BEYOND PASSWORDS: USAGE AND POLICY TRANSFORMATION

THESIS

Alan S. Alsop, Major, USAF

AFIT/GIR/ENV/07-M1

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/07-M1

BEYOND PASSWORDS: USAGE AND POLICY TRANSFORMATION

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Alan S. Alsop, BS

Major, USAF

March 2007

AFIT/GIR/ENV/07-M1

BEYOND PASSWORDS: USAGE AND POLICY TRANSFORMATION

Alan S. Alsop, BS
Major, USAF

Approved:

//signed//	05 Mar 2007
Dennis D. Strouble (Chairman)	date
//signed//	06 Mar 2007
Alan R. Heminger (Member)	date
//signed//	05 Mar 2007
Brian G. Hermann (Member)	date

Abstract

The purpose of this research is to determine whether the transition to a two-factor authentication system is more secure than a system that relied only on what users "know" for authentication. While we found that factors that made passwords inherently vulnerable did not transfer to the PIN portion of a two-factor authentication system, we did find significant problems relating to usability, worker productivity, and the loss and theft of smart cards. The new authentication method has disrupted our ability to stay connected to ongoing mission issues, forced some installations to cut off remote access for their users and in one instance, caused a reserve unit to regress 10 years in their notification and recall procedures. The best-case scenario for lost productivity due to users leaving their CAC at work, in their computer, is costing 261 work years per year with an estimated cost of 10.4 million payroll dollars. Finally, the new authentication method is causing an increase in the loss or theft of CACs, our primary security mechanism for accessing DoD installations, at a rate of 28,222 a year. A single tool, such as the CAC, for all systems and services, carries much power, are we prepared for the responsibility?

To Destiny

Table of Contents

Page

List of Figures

List of Tables

BEYOND PASSWORDS: USAGE AND POLICY TRANSFORMATION

I. Introduction

Background

Currently, the primary method for network authentication on the Air Force's unclassified network has revolved around an authentication method known as "What I Know." (Singh 1985) That is, in order to access our networks, any individual only has to know two things, the username (i.e. logon ID) and password. Research has shown that relying strictly on a password based authentication method has inherent flaws and vulnerabilities that are related to the human factors associated with retaining and recalling multiple passwords (Martinson 2005). As such, user authentication is a significant source of vulnerabilities for Air Force computer networks and systems (Martinson 2005). The vulnerabilities became very apparent in August of 2005 when the Air Force announced that 33,319 Air Force Personnel files, containing sensitive Privacy Act information, were compromised by the unauthorized use of the username and password of a valid user. As such, recent efforts have been focused on ways to bolster security through stronger user authentication processes and methods (Hafemeister 6 Mar 2006). These efforts often require the introduction of unique systems and processes that can change the way that we use the systems and the policies that govern them. As of March of 2006, the Air Force began to move away from a network authentication model that relies on just a username

and password to a network authentication method that requires the use of a token (i.e. Smart card) and a personal identification number (PIN).

With the transformation of user authentication, the question is whether the human factors that create vulnerabilities in the "What I Know" verification method transfer to the two-factor "What I Know" and "What I Have" user authentication method. Additionally, will new vulnerabilities and risks be created by the new system? With the new system, one PIN will be associated with the user's smart card. We know that users have PIN numbers for multiple systems. If the Air Force allows the member to create their own PIN, would it be likely that they would choose a PIN number that they are comfortable with? If the Air Force issues them a PIN, what is the likelihood that they will write it down? Additionally, there will be problems associated with having a token in order get network access. If the user is mobile, how will he get network access as not all computers have smart card readers attached? Additionally, what if the user's smart card is lost, how long before the user is able to access the network again? During the week, this would be quickly handled, but what about over the weekend, or on temporary duty (TDY) at another location?

Problem Statement

With the move towards a new user authentication technique, will the Air Force increase its ability to determine whether or not the user logged on is valid or not. Adding additional security mechanisms appears to help, but the real answer lies in a thorough analysis the usage and policies that come with the new authentication technique.

Research Questions

With the transformation of user authentication in order to decrease the password burden on the user while enhancing security, will users adhere to the new policies concerning smart cards and PIN numbers and will these new security measures ensure that Air Force networks as such are safer because of them?

Purpose Statement

The purpose of this research is to determine whether the new user authentication methods will have an impact on the security of our networks. Specifically, the human factors issues concerning password retention and policy guidance identified by Martinson will be studied to determine whether they apply to the new authentication technique. Next, the introduction of smart cards' to the authentication process will be looked at to determine if new vulnerabilities will be introduced because of this transformation.

Methodology

To collect data, an instrument was developed to question individuals that use the new authentication technique. They answered a series of survey questions related to PIN memorization and smart card usage. These survey questions were very similar to the questions developed by Martinson for his research, but were adapted to the new authentication measures. Additionally, several new questions were added specifically relating to the user's active control of smart cards. Before administration, the new instrument was pilot tested first on the Information Resource Management (IRM) faculty members and current IRM students in order to ensure reliability and content validity. After the data was collected, it was summarized in the form or histograms and frequency

of responses and then compared to data collected by Martinson using statistical analysis tests to determine significance of any changes.

Assumptions/Limitations

The sample for this research was restricted to personnel working for the U.S. Air Force (active duty and civilian). The data collected was restricted to only those sampled personnel who are actively using the new authentication method as required for them to access resources for work. Because this research utilized a survey method, there were certain threats to the internal validity that needed to be negated. Since the survey asked direct questions about their adherence to policy and procedures, the respondent might answer in the expected way according to current policy out of fear of reprisal. While this was a concern, the results from Martinson's research showed that 71 percent of the sampled population of military members admitted during the survey that they had written passwords down, a clear violation of organizational policy. With that in mind and due to the anonymous nature the survey, the reassurance that none of the data will be tractable to the individual, the integrity of the individual military members, and the fact that the sampling population is similar to Martinson's population base, the error will be negligible.

Research Hypotheses

1) The implementation of a two-factor authentication technique will increase the effectiveness of network authentication as related to human factors.
2) The vulnerabilities that affect a strictly password based authentication method will not have an effect on the PIN portion of a two-factor authentication method?

3) Individuals will be more likely to adhere to policy guidance under the new authentication method as compared to password authentication.
4) The new authentication technique will contribute to a loss in worker productivity and smart cards.
5) Accessibility of the networks will decline as individuals find it more difficult to perform job tasks away from the primary workplace (i.e. TDY, Leave) due to the requirement of having a token to authenticate.

Scope

The focus of this research looked specifically at usage and policy issues affecting the new network authentication methods being implemented by the United States Air Force (USAF). Additionally, it looked at how policy and other guidance are adhered to and whether or not PINs would make a difference in regards to adherence. Additionally, it looked at whether or not the use of smart cards affects accessibility. The results were then compared with previous research.

Significance

Network security is a growing concern. With recent compromises of data, the USAF is now implementing new network authentication methods in an effort to negate some of the vulnerabilities associated with the old system. My research looked to see what vulnerabilities will apply to the new authentication method and if any additional weaknesses are introduced. This information can be used as a tool for the USAF in order to assess the level of increased security and guide them to develop policies that will limit the propagation of new vulnerabilities. This research can also be used to determine whether more secure authentication methods are required.

Thesis Overview

This chapter served as an introduction and review of the subject matter to include current issues and previous research associated with password based authentication. It also covers the purpose of this research and gives an overview of the method on which this study was undertaken. Chapter Two contains a review of the of the literature pertaining to the username and password authentication technique in addition to PINs, smart card usage, and the human factors that affect both of those. Chapter 3 contains the research method used. Chapter 4 contains an analysis of the raw data that resulted from the instrument and an in-depth analysis of the data and its significance. Chapter 5 will discuss conclusions, recommendations, and additional findings during the study and provide suggestions for further research.

II. Background

This chapter reviews username and password based authentication to include the definitions of a strong password, password policies, vulnerabilities, strategies in developing strong passwords, and the inherent human factors that attribute to their weakness. Additionally, this chapter will review the emergence of smart cards to authenticate to include their history, technology, security, and the Department of Defense's (DoD) implementation.

History of Password Problems

Before discussing the benefits or changes that a smart card logon technique will provide, it helps to understand the vulnerabilities and problems that plagued the previous authentication technique. For many years, passwords have provided the first line of defense against intruders into computers and their networks (Gehringer 2002; NIPC 2002; Wakefield 2004; Martinson 2005). As such, organizations have required users to have a username and password to authenticate to the information system and they have employed system administrators to oversee the users (Gehringer 2002). In the 1980's, normal password creation policies consisted of telling users to use polysyllabic dictionary words (Martinson 2005). By the 1990's, computers were getting more powerful and dictionary-based attacks were beginning to appear. As such, the typical guidance for a good, or strong, password transformed to the point that they needed to contain upper and lower case letters, numbers, punctuation characters, be seven or eight characters in length, and be easy to remember (Gehringer 2002). At the time, access to organizational

networks was still somewhat more restricted and difficult to access, and brute force attacks on username and password systems were less common (Gehringer 2002).

With the exponential increase in the speed of personal computers, following Moore's Law, and the growth of the Internet, the definition of what makes a strong password had to evolve even further. Unfortunately, even in light of the increasing capabilities of our computing resources, the users' perception of what constitutes a secure password do not always keep pace with the advances in technology. Additionally, guidance to users on how to create strong passwords and enforcing those policies has been hit or miss at best. It is the responsibility of the organizations system administrators to keep the network secure and part of this is ensuring that users understand the latest techniques of developing strong passwords. Current guidance defines a strong password as one that is at least eight characters in length, contains a mix of upper- and lower-case letters, numbers, and symbols. Additionally, it cannot contain a name or dictionary word, be a variation of a previous password, or use symbols that are similar to the characters they are replacing (e.g. 3 instead of E)(Jianxin Yan 2000; Wakefield 2004; Martinson 2005; Microsoft 2006). What we are seeing here is a trend in strong password definitions trying to stay ahead of the technology, systems, and techniques that are used compromise them.

A username and password scheme based on letters and numbers, which comprise of 62 character variations, can be compromised using brute-force password attack scheme in a minimal amount of time by using resources that are available today (see figure 1). In this case, the number of combinations for an 8-character length password is 218 Trillion. With a powerful enough computer, a brute force attack can crack the password in a little

over 60 hours.

62 Characters

Mixed upper and lower case alphabetic characters plus numbers.

Mixed Alpha and Numerals	0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz						
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	3,844	Instant	Instant	Instant	Instant	Instant	Instant
3	238,328	23 Secs	< 3 Secs	Instant	Instant	Instant	Instant
4	15 Million	24½ Mins	2½ Mins	15 Secs	< 2 Secs	Instant	Instant
5	916 Million	1 Day	2½ Hours	15¼ Mins	1½ Mins	9 Secs	Instant
6	57 Billion	66 Days	6½ Days	16 Hours	1½ Hours	9½ Mins	56 Secs
7	3.5 Trillion	11 Years	1 Year	41 Days	4 Days	10 Hours	58 Mins
8	218 Trillion	692 Years	69¼ Years	7 Years	253 Days	25¼ Days	60½ Hours

Figure 1 - 62-Character Based Password Recovery Times (LockDown 2006)

Attempts to overcome these types of vulnerabilities entailed changing the definition for a strong password and the policies for creating them to a 96-character based password (Figure 2) schema. This includes adding special characters to the 8-character password requirement. This increased the number of available permutations from 218 Trillion to 7.2 Quadrillion, which is approximately 33-times the number of combinations that a brute-force attack would have to compute in order to compromise the password of a 62-character based schema. While it would take a very powerful single computer almost three months to complete this task, a network of computers, which could include several hundred machines, could crank through all the combinations significantly faster.

96 Characters

Mixed upper and lower case alphabet plus numbers and common symbols.

Mixed Alpha, Numerals & Symbols	0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz <SP>!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~						
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	9,216	Instant	Instant	Instant	Instant	Instant	Instant
3	884,736	88½ Secs	9 Secs	Instant	Instant	Instant	Instant
4	85 Million	2¼ Hours	14 Mins	1½ Mins	8½ Secs	Instant	Instant
5	8 Billion	9½ Days	22½ Hours	2¼ Hours	13½ Mins	1¼ Mins	8 Secs
6	782 Billion	2½ Years	90 Days	9 Days	22 Hours	2 Hours	13 Mins
7	75 Trillion	238 Years	24 Years	2½ Years	87 Days	8½ Days	20 Hours
8	7.2 Quadrillion	22,875 Years	2,287 Years	229 Years	23 Years	2¼ Years	83½ Days

Figure 2 - 96-Character Based Password Recovery Times (LockDown 2006)

In order to ensure that users develop passwords that are less susceptible to compromise, system administrators utilize password development policies, some of which are automated to ensure they are enforced. One of the key techniques to ensure that users are following strong password creation policies is making certain that users are trained so that they understand the vulnerabilities and risks to the system (Wakefield 2004). Additionally, organizations need to provide feedback to the users so that they understand what information is sensitive and considered an asset to the organization. If the organization does not do this, then users tend to develop their own understanding of what is actually sensitive information, which may or may not be correct (Anne Adams 1999). This kind of behavior can lead to the user's belief that certain information is not at risk, and as such, contribute to the their indifferent attitude towards security.

Additionally, users need to know how to develop strong passwords and understand why they need to create them. Inadequate knowledge of password procedures, content, and cracking lies at the root of user's "insecure" behaviors (Anne Adams 1999). According to Martinson, 36 percent of users either did not know or felt there were no negative consequences to not changing a password on a regular basis. This means that implementing effective password policies must entail ensuring that users understand why these policies are in effect in the first place. Thus, in order to maintain the security of username and password based authentication systems, there is a critical balancing act between users and system administrators between having enough rules for good security, but not so much as to be viewed as an unnecessary burden by the users (Gehringer 2002; Martinson 2005). One of the most common password policies is the forced password change mechanism by which a user must change their password every

60 or 90 days. The problem here is when users must change their passwords frequently they tend to come up with techniques or patterns that assist them in recalling the password but are inherently less secure. Forcing restrictions on users without letting them know why they are necessary will eventually lower the user's regard for overall security (Anne Adams 1999). In one study, it was found that when users were forced to change their passwords frequently and were prevented from using previous passwords, the users would cycle through a multitude of passwords very quickly in order to exhaust their password history list and get back to their favorite password (Jianxin Yan 2000). While the purpose of this policy as implemented was intended to reduce the impact of a potential undetected security breach, a consequence of it led to the reduction of the overall security of the network due to the recycling of familiar passwords (Anne Adams 1999). Other strategies that have been used to ensure stronger password development include training users to create passwords using pass-phrases (Gehringer 2002; Wakefield 2004) and to have users test their passwords against password strength testing tools (Microsoft 2006).

The point here is that password policies and the reasons for them need to be clearly communicated to the user in order to ensure compliance. If the user does not understand why nor what they need to do to ensure that their username and password is secure, their use and regard for security in general will wane and vulnerabilities to the organizational networks will propagate.

Why do we need to have secure passwords? In addition to brute force attacks, which test every possible password combination, username and password based authentication techniques are also susceptible to other vulnerabilities. Every year,

thousands of computers are illegally accessed because of weak passwords. Common weak password choices include: using a dictionary word, dictionary words followed by two numbers, using names of people, places, or things, and using the default passwords on systems. Unfortunately, hackers are aware of these types of vulnerabilities and target them first (NIPC 2002). Some common password attack schemes used by hackers that target weak passwords include educated guessing (e.g. dictionary attacks) of passwords and deriving passwords (e.g. common names) (Neumann 1994). As far back as 1990, hackers were creating dictionaries of 60,000 or more words for the express purpose of attacking username and password based authentication systems. By 2000, these dictionary based cracking systems were also testing permutations of words to include substituting special characters and capitalizing non-initial characters (Gehringer 2002).

Another vulnerability to password authentication that is common today is their susceptibility to spyware attacks. Common advice to users is to refrain from typing passwords on computers that they do not control or are in insecure environments. This includes those computers that are located at internet cafes, computer labs, and airport lounges. These systems are unsafe as criminals can try to get users password information by using inexpensive keystroke-logging devices that take only a few moments to install. In addition, users are advised not to install software on their home systems unless they are confident of the source of the file as the file could be a Trojan (i.e. appears to do one thing while in reality it is capturing users keystrokes). These spyware programs can allow someone to remotely access all information that is typed on the compromised system (Microsoft 2006). To compound this, hackers know that a password for one system is likely to access many other accounts by that same user. This can be especially

dangerous on systems where the user has resorted to using a password management system, or "wallet", such as "Microsoft Passport" or "Darn! Passwords!" These programs are inherently vulnerable to attacks by spyware and viruses and anyone with access to the computer would have access to all the passwords in the wallet (Gehringer 2002). Once a hacker has one password, the security of the rest of their accounts thus becomes compromised (NIPC 2002).

The greatest vulnerability of username and password based authentication schemes lies ultimately in the user. Human error is the principal cause of security breaches in the computing security sector of organizations. They accounted for 84% of the security breaches in 900 private and public American organizations in 2001 (CompTIA 2002; Christina Braz 2006). Martinson's survey of password usage found that: 96% of users recycle or use similar passwords for multiple applications, 71% of users write their passwords down, 39% of users have shared their passwords, 29% of users use familiar names, places, or dates for their passwords, and 68% of users have changed a password so that it is easier to remember. Additionally, regardless of the guidance given to users via training and corporate policies, a small percent of users will ignore sound password advice for convenience (Jianxin Yan 2000). Part of this lies in the fact that users do not understand why they need to follow security policies and some lies in the fact that users don't understand the threats to the systems and how exactly their systems could be compromised. Users still tend to think that password cracking is done on a "personal" basis, and they perceive the risk to be low because their role in the system is not important (Anne Adams 1999). Additionally, users do not understand how password cracking programs work and thus do not understand what comprises a secure

password (Anne Adams 1999). Another reason for these human vulnerabilities is that humans by nature have limited capabilities (e.g. short-term capacity of around seven plus or minus two items) for memorizing sequences of items (e.g. passwords)(Jianxin Yan 2000). Additionally, when humans remember sequences of items, those items cannot be drawn from arbitrary or unfamiliar ranges, but must be familiar 'chunks' such as words or familiar symbols (Jianxin Yan 2000). With so many accounts, complex password requirements, lockout policies, and short password lifetimes, system administrators are ensuring that users come up with techniques that will assist their ability to memorize the password at the cost of compromising security (Gehringer 2002; Martinson 2005). One of the most common examples of this is when users have multiple accounts with different passwords, they will feel inclined to write their password down in order to prevent getting locked out (Gehringer 2002; NIPC 2002; Wakefield 2004)

Another weakness of username and password based authentication schemes is our susceptibility to social engineering techniques designed to gather the password authentication information. Hackers pay more attention to the human link in the security chain than security designers do. This is demonstrated by the social engineering techniques used to obtain passwords (Anne Adams 1999). Common social engineering methods include: sending a Trojan program as an email attachment, posing as a new employee needing help, offering a prize for registering at a Web site with a username and password, and posing as a vendor or systems manufacturer calling to offer a system patch or update (Mitnick 2002).

Each of these attacks can be successful and are inherent of any authentication scheme that relies solely on methods in which users must recall information as opposed

to providing some form of physical proof that the network can validate. Our networks are essential to the success of our war fighting missions and the protection of our privacy information. Unauthorized access, fraud, tampering, eavesdropping and data theft all pose a threat to these systems. One of the key weaknesses of our network is the use of passwords that many of us have grown accustomed to using. As described previously, conventional passwords are vulnerable to attack and allow adversaries to access our systems at will and move about freely, posing as legitimate users from the safety of their own base of operations (SPO 2006). In order reduce the impact of these human factors based vulnerabilities and better secure the network, authentication systems need to ask for more than just what a user knows before they allow them network access, which brings us to the introduction of smart cards in the authentication process.

Smart Cards (a.k.a. CAC)

The DoD implementation of the smart card, known as the common access card (CAC), is designed to provide for that increased security. The advantage of this type of authentication system, commonly referred to as "two-factor authentication", is that it requires something you have, (e.g. CAC), and something you know, (e.g. PIN) (SPO 2006) as opposed to just something you know, which is the basis for the username and password authentication system.

A smart card is a complex embedded system that takes advantage of state of the art silicon technologies and microprocessors. In addition to processors, they normally have several types of data storage to include non-volatile memories such as read only memory (ROM), electrically erasable programmable read only memory (EEPROM), Flash, and random access memory (RAM). They also include communications

interfaces, which can be contact-less (i.e. radio frequency identification (RFID)), analog parts and sensors, which protect the chip against attacks, and embedded software that includes secure operating systems, virtual machines, firewalls, cryptography and other specific applications (Philippe Proust 2004). The term "smart card" has been associated with any credit card-sized card with more memory than the traditional magnetic stripe. For this research, the "true" smart card has the data storage and has an on-board embedded processor or smart chip (Katherine Shelfer 2002). Anything less than that is really just a storage card and provides no security features to protect its data from being read out. A true smart card not only provides a way to store its data, but can also function as a small computer with built-in security features to guard against unauthorized access to its data and functions (Scheuermann 2002).

For the DoD, the CAC will be using integrated technologies to perform standard identification, physical access, and logical access. Some of the initial applications designated to be using the CAC are identification, network authentication, and physical access. Other applications currently under development or evaluation include dining services, finance, travel, medical and dental readiness, deployment readiness, equipment accountability, and training (DoD 2003).

The idea of placing processors in plastic cards was the idea of German inventors, Jergen Dethloff and Helmut Grotrupp, who patented the idea in 1968. In 1974, Roland Moreno filed for a patent on the integrated circuit (IC) card, later dubbed the "smart card." Moreno received a first patent in France in 1975 and a U.S. Patent (number 4,092,524) in 1978 (Katherine Shelfer 2002). While the concept of the smart card was established, it was not until 1977 that technology caught up to the idea and Motorola

produced the first smart card circuit chip. The first commercial use of the smart card was attempted in 1980 by the French banking association, Bancaires, when they used smart card technology in an attempt to reduce fraud from criminals who were counterfeiting credit cards by copying the magnetic stripes. Because of this initiative, credit card fraud rates in France from those cards dropped tenfold. By 1992, the French financial institutions decided to replace magnetic stripe cards with smart cards and as such, benefited from a 75% reduction in credit card fraud over a five-year period (Katherine Shelfer 2002). This shows that by adding another layer of security, more secure than just a magnetic strip card, can lead to quantifiable benefits in regards to reducing unauthorized use of the card. Since 1993, the Department of Defense (DoD) has been conducting evaluations of smart card technology. Initially tested as an updateable data storage device, it has evolved to require an interoperable, backward compatible device for secure on-line data transfer and on-line transactions (DoD 2001; White-House 2004). In September of 1999, the Deputy Secretary of Defense (DEPSECDEF), Dr. John Hamre, and the Defense Management Council (DMC) decided to adopt the smart card, or CAC, as the new DoD identification card (DoD/ACO 2000). In November of 1999, the DEPSECDEF published a memorandum titled, “Smart Card Adoption and Implementation”. This directed the DoD to use smart card technology for identification, physical access, an authentication token for the DoD PKI, and access to DoD computer networks (DoD/ACO 2000). By the beginning of October 2000, the DoD began issuing the new CAC (DoD 2001). Guidance for the use of the new smart card was then incorporated into DoD Directive 8190.3, dated 31 Aug 2002:

4.2 Smart card-based technology and systems shall be used to transform and improve security in DoD processes and mission performance thereby enhancing readiness while also improving business processes.
4.5 Smart card technology shall be applied in the form of a Department-wide common access card (CAC) that shall be:
4.5.1 The standard identification card for active duty uniformed services personnel (to include the selected reserve), DoD civilian employees, eligible contractor personnel, and eligible foreign nationals
4.5.2 The department's primary platform for the public key infrastructure authentication token used to access DoD computer networks and systems in the unclassified environment and, where authorized by governing security directives, the classified environment
4.5.3. The principal card enabling physical access to building facilities, installations, and controlled spaces

In August of 2004, the White House published a Homeland Security Presidential Directive, HSPD-12, which adopted the use of a CAC as identification for all federal employees and the contractors that work for the federal government. This was in response to a need to reduce risk of terrorism to Federal and other facilities due to wide variations in quality and security of the forms of identification (White-House 2004). Key features of this new identification card and a timeline for implementation were outlined in sections 3 and 4 of the document:

Section (3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verify an individual employee's identity: (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process.
Section (4) Not later than 4 months following promulgation of the standard…identification issued by departments and agencies to Federal employees and contractors meets the standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the standard, the departments and agencies shall require the use of identification by federal employees and contractors that meets the standard in gaining physical access to

> federally controlled facilities and logical access to federally controlled information systems (White-House 2004).

In response to HSPD-12, the National Institute of Standards and Technology Computer Security Division initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. Federal Information Processing Standard (FIPS) 201, entitled Personal Identity Verification (PIV) of Federal Employees and Contractors, was developed to satisfy the requirements of HSPD-12. It was approved by the Secretary of Commerce and issued on February 25, 2005 (CSRC 2006).

The CAC has evolved from its original intent as an updatable data storage device in 1993 to become an interoperable, backward compatible processing and data storage device with secure logical authentication and physical access capabilities. Additionally, it is now the standard identification and Geneva Convention Card for active duty and Selected Reserve members of the Uniformed Service, DoD civilian employees, and eligible contractor personnel. The mandatory compliance date for all agencies to produce and provide CACs that are compliant with the first stage of PIV standards as set forth in FIPS 201, is mid 2007 (DMDC 2005). One of the most visible aspects of these changes is the institution of the secure logon requiring use of the CAC and a PIN. The Air Force's deadline for enforcing smart card logon (SCL) was 31 July 2006. As of 7 August 2006, only 53% of Air Force users were compliant (AFCA 2006).

To understand how a smart card is going to help us provide a more secure computing environment, we need to understand the technology that underlies it. As I noted above, smart cards have been used for many years in Europe. One of their key

benefits is the familiar package that they come in. They are in essence credit-card-sized computers with a rugged and familiar form that fits nicely into a wallet or pocket and can take lots of physical stress (David Sims 1999).

A smart card typically consists of three components: a plastic card, a microprocessor, and a communication interface. Generally, the plastic card contains one or more embedded integrated circuit chips (ICC) (a.k.a. microprocessor) in addition to other data, display, storage, or transfer technologies such as a photograph, hologram, linear barcode, two-dimensional barcode, magnetic stripe, radio frequency antenna, and biometrics. They normally support multiple applications, such as storing personal data, calculating values, validating biometric identification, performing digital certification, and encrypting information (DoD 2001).

The plastic card acts as a convenient package for the microprocessor and provides a place to print text and graphics (see figure 3). The smart card chip is located near the edge of the plastic card. This is done to protect the chip if the card is twisted or bent and to accommodate backward compatibility for systems that used to require a magnetic stripe (i.e. credit cards) or bar code on the backside of the card (see figure 4)(Katherine Shelfer 2002). This versatility for multiple technologies allows a single card to meet different needs and allows the smart card to be phased into existing systems (Nelson 1993). In the case of the USAF, the CAC will be used to replace the existing identification card, giving the user additional capabilities and still providing the same benefits and privileges as its predecessors (DoD 2001).

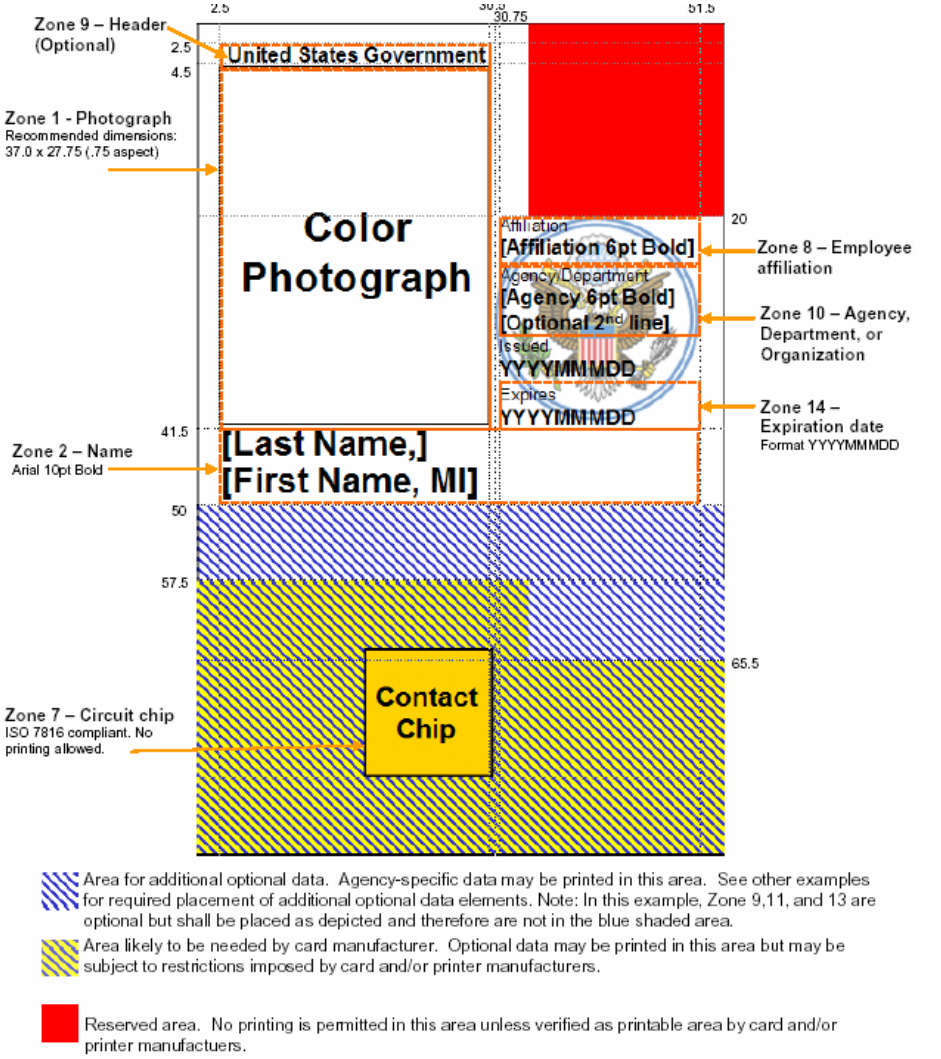

Figure 3 - Smart Card Front (CSD 2005)

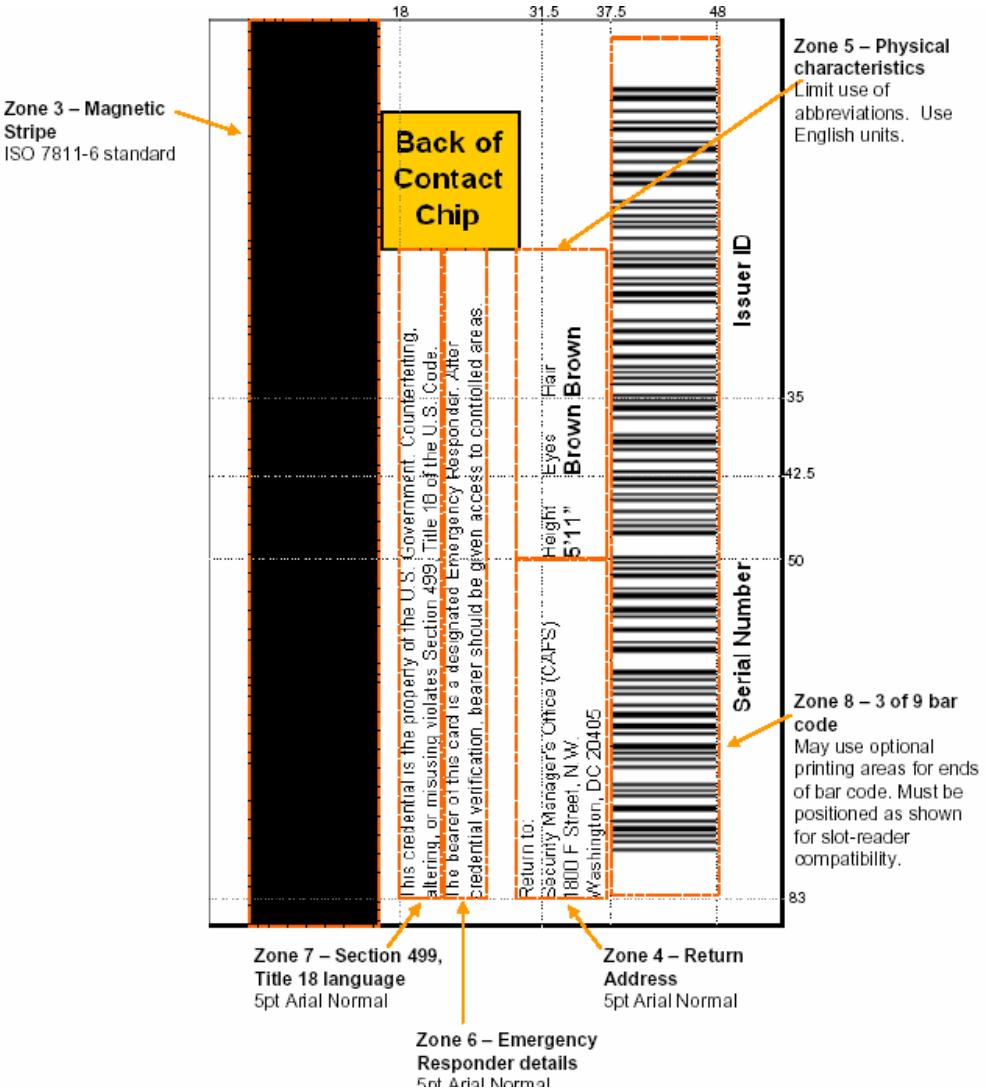

Figure 4 - Smart Card Back (CSD 2005)

The microprocessor portion of a smart card is a programmable microcomputer that incorporates a CPU, memory, communication port, and control logic on a single chip. The ICC is a small piece of semi-conducting material on which the integrated circuit is embedded. A typical chip can contain millions of electronic transistors (DoD/ASD 2002). Usually such cards have an embedded 8-, 16-, or 32-bit processor. Even the 8-bit microprocessor-based smart card is as powerful as the desktop PCs of the

early 1980s (Katherine Shelfer 2002). This microprocessor is a really a computer that has the capability to read, write, and perform various operations to its' onboard memory (DoD 2000). Additionally, included on most ICCs is an on-board cryptographic co-processor that allows signing and key generation to be done entirely on the card. This ensures that the private key data never needs to be offloaded or revealed (David Sims 1999). This cryptographic co-processor allows the smart card to serve as an authentication device for the PKI identity, email, and encryption certificates (DoD 2003). The microprocessor stores its' programs and data in ROM, RAM, EPROM, and EEPROM (Nelson 1993; Katherine Shelfer 2002). The RAM provides storage for temporary data, the EPROM provides programmable, permanent information storage for fixed information, and the EEPROM is nonvolatile read/write memory and is similar to a computer disk drive. It is the storage location for data and application program files (Nelson 1993). Currently, the data contained on a smart card can be stored reliably for a maximum of 10 years (Katherine Shelfer 2002).

The smart card is not a self-contained computer; it requires power and timing signals from an external source. Card-Acceptor devices (CADs) provide the physical interface between the smart card and other devices. The CAD holds the smart card in place and includes a set of contacts that correspond to the "communication interface" on the smart card. The most widely used, and the ones that the US Air Force are currently using, smart cards have metal surface pads and are called "contact smart cards." Smart cards with subsurface leads are called "contactless smart cards." These cards receive their power through inductive coils and exchange signals through capacitive plates (Nelson 1993).

What will these advances in technology provide in regards to increasing the level of security during network authentication? A smart card has the following general security functions: cryptographic applications, user authentication via PIN, and device authentication (Scheuermann 2002). The capabilities of smart cards allow them to authenticate themselves without having to interface with a centralized computer system (Nelson 1993). This prevents secure data from the vulnerability of traveling over the network.

Integrating smart cards, biometrics and public key cryptography provides a solid foundation for developing secure applications and communication systems. The highest level of security uses three-factor authentication: something you know (PIN), something you have (smart card, magnetic stripe card or a physical key) and something you are (biometric) (David Sims 1999). The next level of security incorporates two of those factors. In the case of the CAC and PIN, a two-factor authentication system, authorization is given based on something the user knows and something the user has. As such, neither possession of the card alone nor knowledge of the password alone is sufficient to allow an impostor to masquerade as the authorized user (Keok Auyong 1997). Smart cards provide an environment that enables secure processing that is associated with network user authentication to occur only within the trusted device, which is always under the physical control and protection of the user. This improves system security in three ways: It requires a user to provide both something he or she possesses (i.e. smart card) as well as something he or she knows (i.e. PIN). Either item alone is useless. This greatly reduces the risk that was shown to exist on username and password based authentication systems of password borrowing or theft. It also ensures

that security related data is encrypted while on the user's workstation. A malicious Trojan program can obtain no sensitive information from it (Keok Auyong 1997).

Additionally, if the user loses the smart card, the card is inoperable without the PIN. Guessing a smart cards PIN will be frustrated because the processor on the smart card normally will have a routine that locks the card after three or four incorrect PIN attempts (Chadwick 1999; DoD/ACO 2000; SPO 2006). Another factor that contributes to the increased security of smart card is the decreased possibility of copying the smart card's private key because it never leaves the card. The smart card uses its microprocessor to compute the transmitted data's digital signature (Chadwick 1999). Additionally, smart cards can contain on-board cryptographic co-processors that allow signing and key generation to be done entirely on the card, so that the private key never leaves the card and thus eliminates the possibility of the key pair being snooped out during transmittal. The cryptographic co-processor performs tasks such as key generation and verification, secure signing, hashing, and encryption (David Sims 1999). Thus, to access data on the chip, or utilize the certificates on the chip, a PIN must be entered (DoD/ACO 2000).

In order to ensure the security of DoD computer systems, access to them will be granted only when all of the following are present: the CAC, PIN, valid certificate, and authorization to that particular computer or system. Any application that wants to read and write data to and from the card must be registered and digitally signed by the U.S. Government. If the keys for this process are not present, the smart card processor will not allow the data to be accessed (DoD/ACO 2000). Additionally, in order to prevent the CAC from being counterfeited for physical access based on just identification, the DoD

CAC contains visual anti-counterfeiting components to include the use of holograms and ghost images. The card and its chip are also made more tamper-resistant by the use of dual-sided lamination, which prevents the modification of the printed information or images (DMDC 2005). The goal of these security measures is to negate the use of stolen or borrowed cards to gain access and provide appropriate security to the entire identity proofing and authentication process (CSD 2005).

Table 1 - Overview of Smart Card Security Features (Nelson 1993)

Logical Security Features
Data is not written or read directly by a reader; rather it is written or retrieved using command requests from a host system, with the smart card's microprocessor controlling access to the data
Data access authorizations (e.g., read and write) are protected with password data access control
The Operating system protects internal security information in hidden data areas
The PINs and keys never leave the card, so that they cannot be captured and analyzed
Cards "lock up" after successive invalid PIN entries
Authority access matrices determine whether an instruction executed in one memory area can access data stored in another area
Physical Security Features
Memory, CPU, and logic are integrated onto a single IC with no external bus that can be monitored
Tamper detection devices disable the microprocessor when card tampering is detected
Tamper protection by card layering, microprocessor embedding, protective coatings, and epoxy technologies prevent compromise through layer and IC removal
Leads used for IC testing are fuse connected, then blown before the cards are issued
The smart cards and ICs are manufactured in secure facilities where the chip wafers are accounted for, tested, and assigned a unique serial number

The overarching goal of implementing the smart card for network authentication is to increase the security of critical communications resources. Based on the research, this would appear to be the case. The question that I'll be answering is whether or not the human factors associated with usage and policy are going to have a positive or negative affect on our security posture as we transition to this new technology.

III. Methodology

Procedures

Data was collected via a 40-item survey accessed by U.S. Air Force military and civilian respondents. The surveys were distributed to the organizational members through a web-based interface. To encourage participation in addition to ensuring the anonymity of participants, each survey included a forward that informed them that only personnel directly involved in the research would have access to the raw data. Additionally, the personal data collected by the survey was limited to age, gender, occupation (officer, enlisted, civilian, contractor), and whether or not they have worked in the computer security field. The data collected from the surveys were stored in a database at the Air Force Institute of Technology. The survey period lasted from 14 December 2006 to 11 January 2007.

Participants

The expectations of survey participants were explained on the first page of the survey. Furthermore, the survey summarized the fundamental purpose for the data collection and encouraged everyone's participation in the study. Participants were also instructed to direct any questions to the researchers using provided contact information.

The survey was sent via email to a representative sampling of members of a United States Air Force (USAF), a population of approximately 491,786 (AFPC 2006) military and civilian members, located throughout the world with an initial representative sample of 4,831 members. The survey only targeted military and civilian members of the USAF, but 18 contractors did respond. This is probably due to outdated information on the Air Force Global Email Address directory. Of those, 301 of the surveys did not make

it to their recipients due to errors such as delivery refused, out of office responses, remote host not found, mailbox no longer exists, and mailbox full. With the delivery failures factored in, the number of surveys sent out is reduced to 4,530. 749 recipients took the survey and 725 of those provided usable data, resulting in a 16 percent response rate and a sample size of $n = 725$. Due to a technical error with the data collection tool, 412 of the 725 completed surveys were missing responses for questions 2 through 6, although all the other data for those surveys were collected. Results for questions 2 through 6 will be analyzed using a sample size of $n = 313$.

Design

The survey design was longitudinal between-cases panel design. In this study, the cases are defined by the independent variable of whether the participant is using a username and password authentication technique or a CAC and PIN based authentication technique. The dependent values were measured only once, Martinson has already collected the data for the case of username and password authentication and this research collected the data for the case of CAC and PIN based authentication.

Surveys are more susceptible to certain internal validity threats such as demands on participants, researcher effects, history and maturation, systematic trends, causal direction, predispositions, and similarity in measurement. As such, these issues must be addressed in order to limit their impact and effect on the results (Schwab 2005). Demand effect was controlled by having an independent variable that was not measured during the survey, thus participants did not respond based on expected relationships between the independent variable and the dependent variable. Researcher expectation effects will be limited due to the anonymous nature of the survey, as discussed previously, and the lack

of any interaction between researcher and participants. History, maturation, and systematic trends may pose a concern as security issues, such as the theft of Air Force personal information mentioned previously, may have increased participant awareness of security policies and practices. Causal direction will not be a concern as the usage characteristics, or dependent variables, do not determine the authentication technique. In this survey, temporal precedence is conceptually clear in regards to authentication method determining usage characteristics as opposed to vice versa. Participant predispositions should not be a concern, as the sampled populations are similar, both being military related, and the sample sizes, Martinson has 338 responses and I had 725 (n = 313 for questions 2-6) responses, are significant enough for a normal population distribution. Additionally, the survey was tested for face validity, content validity, and reliability to ensure that the measures were construct valid. Face validity was determined through surveys given to representative sample, pilot group, of participants and the construct was judged content valid by the research team. Additionally, since the causal relationship is clear, internal validity is not a serious concern (Schwab 2005).

Measures

The survey was designed to measure three dimensions of CAC usage in addition to participant individual characteristics. The three dimensions included CAC and PIN usage, CAC control, and CAC and PIN guidance. The participant characteristics of interest included age, gender, occupation, and involvement in the computer and network security field. The survey used is attached as Appendix B. The questions can be cross-referenced with Martinson's survey (Appendix C) and the research hypotheses outlined in chapter 1 using the matrix in Table 2.

Table 2 - Research Hypothesis versus Survey Questions Matrix

Martinson	Alsop	Research Hypothesis
1	1	Validates respondent to survey
	2	Not applicable to study due to PIN policy
8	3	1, 2
2	4	1
3	5	1, 2
4	6	1, 2
5	7	1, 2
6	8	2
7	9	Insight into common techniques
10	10	3
11	11	1, 2
	12	4
	13	4
	14	4
	15	4
	16	Usability Issue
	17	4
	18	4
	19	4
	20	1, 2
	21	5
	22	5
12	23	3
14	24	3
13	25	3
	26	5
	27	5
	28	AFCA request
	29	AFCA request
	30	AFCA request
	31	AFCA request
	32	Future Research
	33	Future Research
	34	Future Research
	35	Future Research
16	36	Comments

Survey questions 3 through 11 and questions 23 through 25 for this research directly matched questions that were asked during Martinson's research. These investigative questions will serve to compare the changes in usage and policy as affected by the implementation of the CAC and PIN authentication method. Questions 12 through 22 and questions 26-27 will answer additional questions and confirm hypothesis relating specifically CAC control. Questions 28 through 31 were added specifically at the request of the research sponsor, the Air Force Communications Agency. Questions 37 through 40 serve to identify participant characteristics.

The data from the survey were imported into Excel 2003 Spreadsheet and analyzed using MINITAB statistical analysis software. The analysis was directly compared against results for Martinson's research questions:

- Do you use passwords?
- Has your password ever been compromised?
- Do you recycle or use similar passwords for different applications?
- In the last year, have you written down a password?
- In the last year, have you ever shared a password with friends, family, co-workers or others?
- How do you remember passwords?
- Have you ever voluntarily changed a password so that it is easier to remember?
- Do you feel that password procedures and parameters are a nuisance?
- How many passwords are you currently remembering/using?
- How would you characterize your organization's training and education relating to the creation of passwords?
- Do you follow the password procedures based on organizational guidance?
- Do you feel the password policies of your organization are burdensome?

Limits of the Data

The data was gathered using a format that does not allow participants to go back and change their answers. This technique therefore does not guarantee that the

participant's feelings at the end of the survey represent how exactly they answered the question during the survey. In other words, it does not capture participants change in attitudes or second thoughts about previous questions based on questions that are encountered later in the survey. One question that was not represented in this survey that was asked in Martinson's research was, "Are there any negative consequences to not changing passwords regularly?" This question did not relate to any of the research hypotheses in this study. In Martinson's research, he noted that the question, "Has your password ever been compromised?" was ambiguous, as the user might not know whether their password has been compromised. This is also true with the research question in this study, "Has you PIN ever been compromised?" I am keeping this question in the study in order to determine whether the participants' confidence in the PIN is similar to the confidence levels shown for passwords in Martinson's research.

Additionally, because the data collected pertained to a two-factor authentication method that had implemented only six months prior to the survey period, we cannot be sure that this data positively reflects the steady state.

All data was inspected for errors and omissions before analysis.

Chapter Overview

This research study will use an anonymous web-based survey of active duty and civilian military members that are using the CAC and PIN authentication method for network access control. The survey was designed as a longitudinal between-cases panel study with the independent variable for the cases being the authentication method. Threats to internal and construct validity were also addressed. The measures of the study

and the limits of the data were then identified, as were the methods for comparison in order to answer the research hypotheses in chapter 1.

IV. Analysis

In this chapter, we analyze the data collected and compare applicable questions directly to the results of Martinson's research. First, we will review the responses for each survey question in detail. We then analyze each of the research hypotheses, directly comparing our results against the results of Martinson's research where appropriate, with statistical analysis tests.

Survey Question Response Overview

Survey Question One

The first investigative question asks, "Do you use a Common Access Card (CAC, aka Military ID) and Personal Identification Number (PIN) to access the network at work?" Possible answers for this question were "Yes" and "No". There was a 100 percent response to this question with 96.8 percent of the participants answering "Yes". This question serves to identify those individuals who are the target of this research. Those who answered 'No' did not take the rest of the survey.

Survey Question Two

The second investigative question asks, “Were you issued a PIN, or did you pick your PIN yourself?” This question will serve to determine whether choosing your own PIN has an affect on PIN usage. The results show that 96.4 percent of the respondents were able to pick their own PIN number. This is consistent with the technique in which the USAF uses to assign PIN numbers to CACs (DMDC 2006). Eleven respondents stated that they did not pick their own PIN, which is at odds with the CAC issuance procedures and leads me to believe that they did not understand the question.

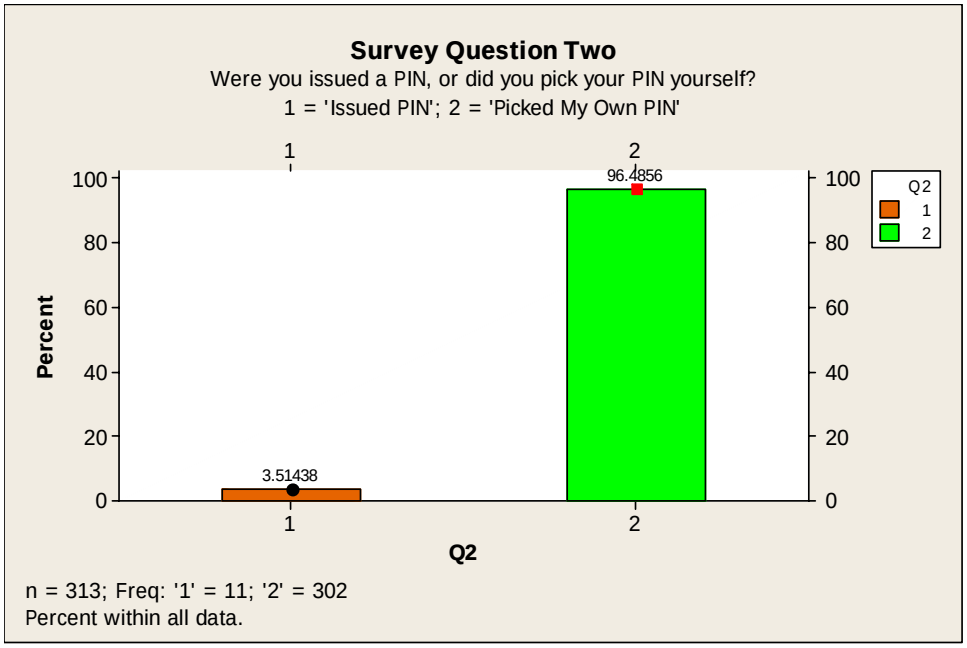

Figure 5 - Were you issued a PIN, or did you pick your PIN yourself?

Survey Question Three

The third investigative question asks, “Have you ever changed your PIN so that it is easier to remember?” This question was similar to a question asked during Martinson’s research, “Have you ever voluntarily changed a password so that it is easier to remember?” Martinson’s research showed that 68.6 percent answered “Yes”, 30.2 percent answered “No”, and 1.2 percent answered “Don’t Know.” In our research, there is a reversal of this trend, with 25.2 percent of respondents stating that they have changed their PIN so that it is easier to remember. This could be due to the fact that users do not have to change their PIN on a regular basis and are allowed to select their own PIN during the CAC issuance process.

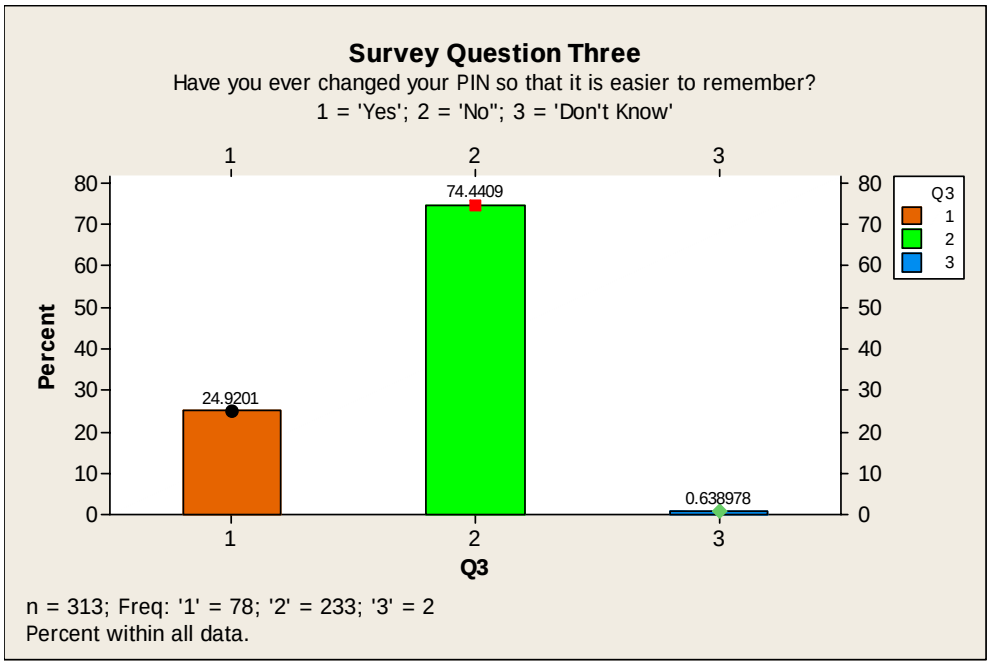

Figure 6 - Have you ever changed your PIN so that it is easier to remember?

Survey Question Four

The fourth investigative question asks, “Has your PIN ever been compromised?” This question was similar to a question asked during Martinson’s research, “Has your password ever been compromised?” Martinson’s research showed that 5.3 percent answered ‘Yes’, 69.5 percent answered ‘No’, and 25.1 percent answered ‘Don’t Know’. In our research, respondents tend to be much more confident in the integrity of their PINs with 93.9 percent answering ‘No’ to this question.

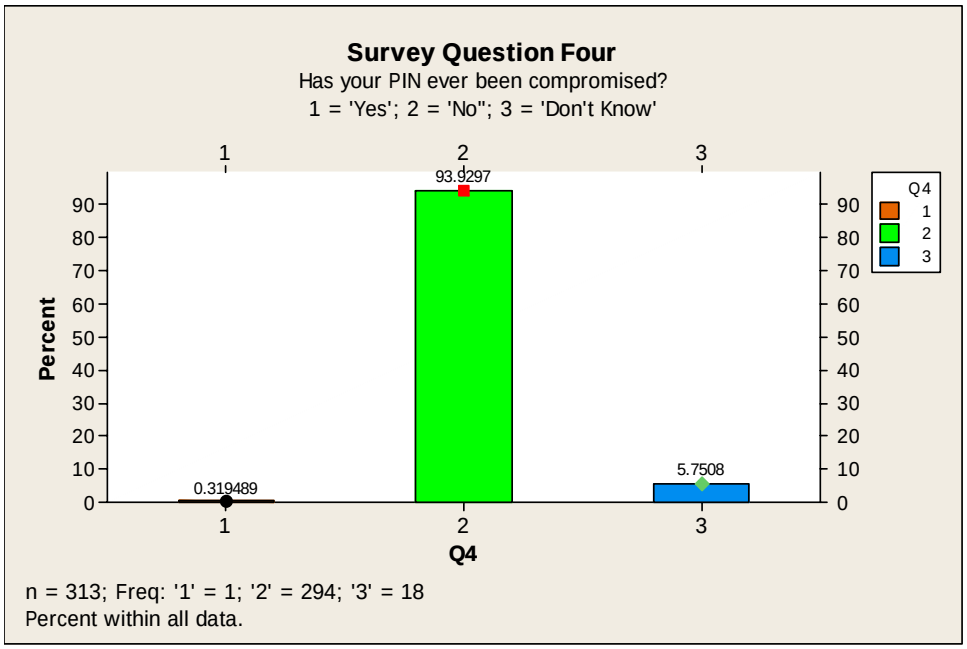

Figure 7 - Has your PIN ever been compromised?

Survey Question Five

The fifth investigative question asks, "Do you use the same PIN for multiple applications? Example: ATM card, Online accounts, Credit Cards." This question is similar to a question asked during Martinson's research, "Do you recycle or use similar passwords for different applications?" Martinson's research showed that 96.2 percent answered 'Yes'. In our research, only 25.6 percent answered 'Yes' and 74.4 percent of the respondents answered 'No', a distinct difference from the results in Martinson's research and an indicator that a CAC and PIN authentication technique can increase the level of security of a network by reducing the vulnerability to PIN compromise.

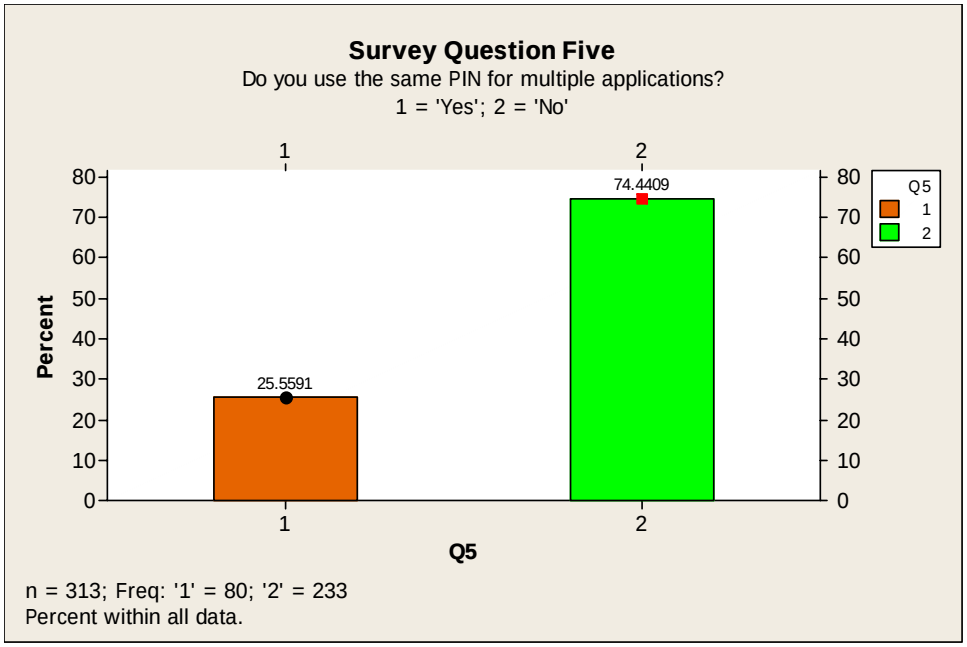

Figure 8 - Do you use the same PIN for multiple applications?

Survey Question Six

The sixth investigative question asked, “In the last year, have you written down your PIN(s)?” This question was similar to a question asked during Martinson’s research, “In the last year, have you written down a password?” Martinson’s research showed that 71.3 percent answered ‘Yes’ and 28.7 percent answered ‘No’. In our research, the results were reversed with 21.4 percent answered ‘Yes’ and 78.6 percent answering ‘No’. Again, it appears that the respondents treat their PINs more securely than they did their passwords.

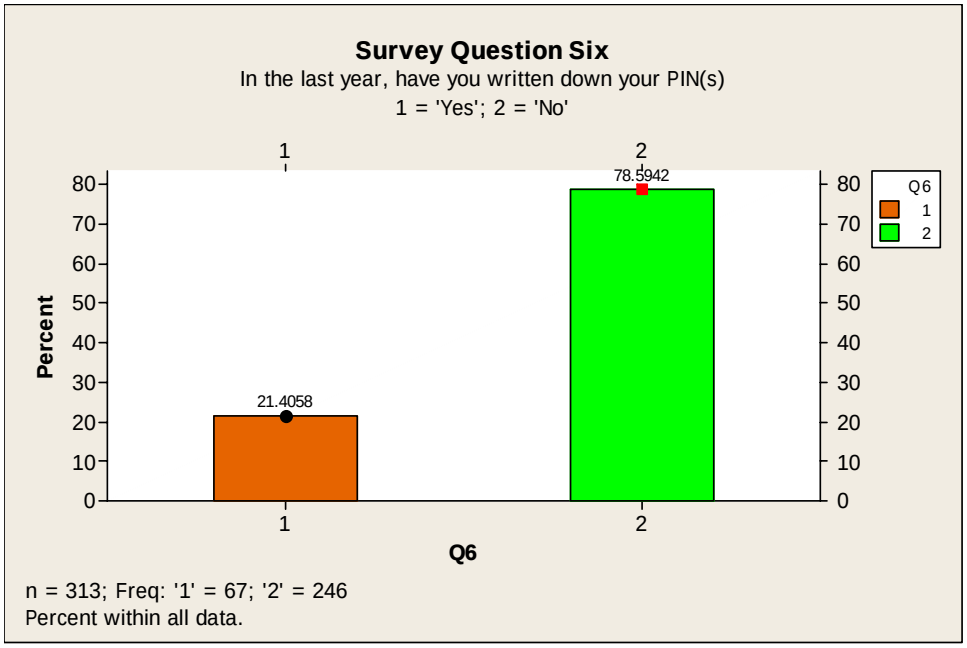

Figure 9 - In the last year, have you written down your PIN(s)?

Survey Question Seven

The seventh investigative question asked, “In the last year, have you shared a PIN with friends, family, co-workers, or others?” This question was similar to a question asked during Martinson’s research, “In the last year, have you ever shared a password with friends, family, co-workers or others?” Martinson’s research showed that 39.1 percent answered ‘Yes’ and 60.9 percent answered ‘No’. In our research, the results showed that only 3.6 percent answered ‘Yes’ and 96.1 percent answering ‘No’. This could be attributed to the fact that PINs are useless without the associated CAC and users are less likely to share their CAC with others as it could affect their ability to access the base and base services.

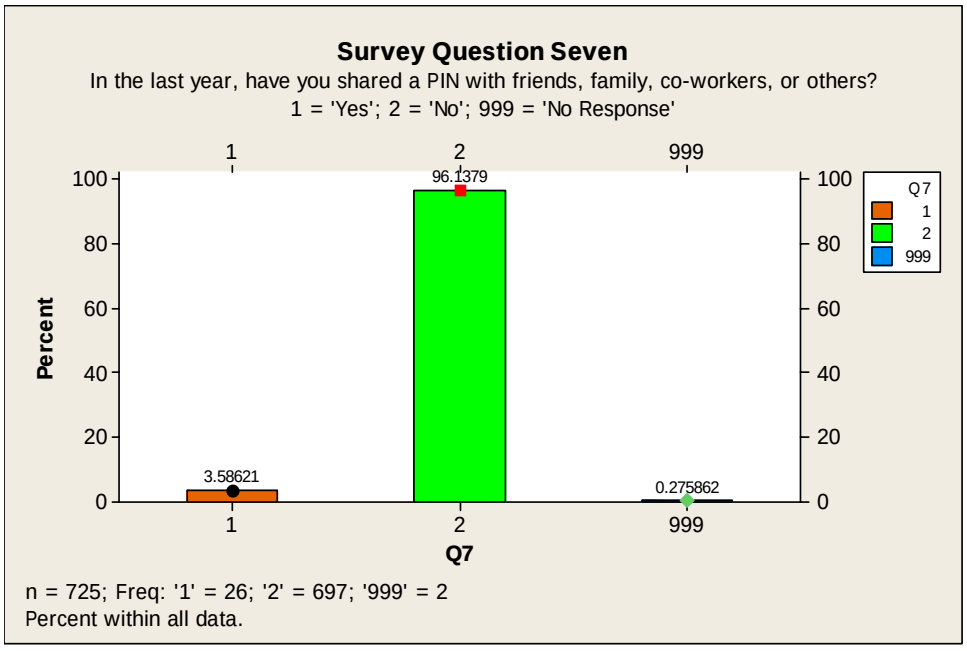

Figure 10 - In the last year, have you shared a PIN with friends, family, co-workers, or others?

Survey Question Eight

The eighth investigative question asked, “Do you use a familiar date, age, SSN, sequence (i.e. 1234), telephone number, street address, or pattern to remember your PIN?” This question was similar to a question asked during Martinson’s research, “How do you remember your password?” Martinson’s research showed that almost 100 percent of the respondents used some technique to remember their password. In our research, the results showed an almost even split with 47 percent answered ‘Yes’ and 52.7 percent answering ‘No’. This question may have confused the respondents as 76.2 percent of the 382 that answered this question ‘No’, then answered question 9 of the survey, “What “Technique” do you use?” with the technique that they used. Unless they are writing their PIN down (21.4 percent according to question six), they would need to use some technique in order to recall the PIN later. The techniques identified in question 9 are included in Appendix D.

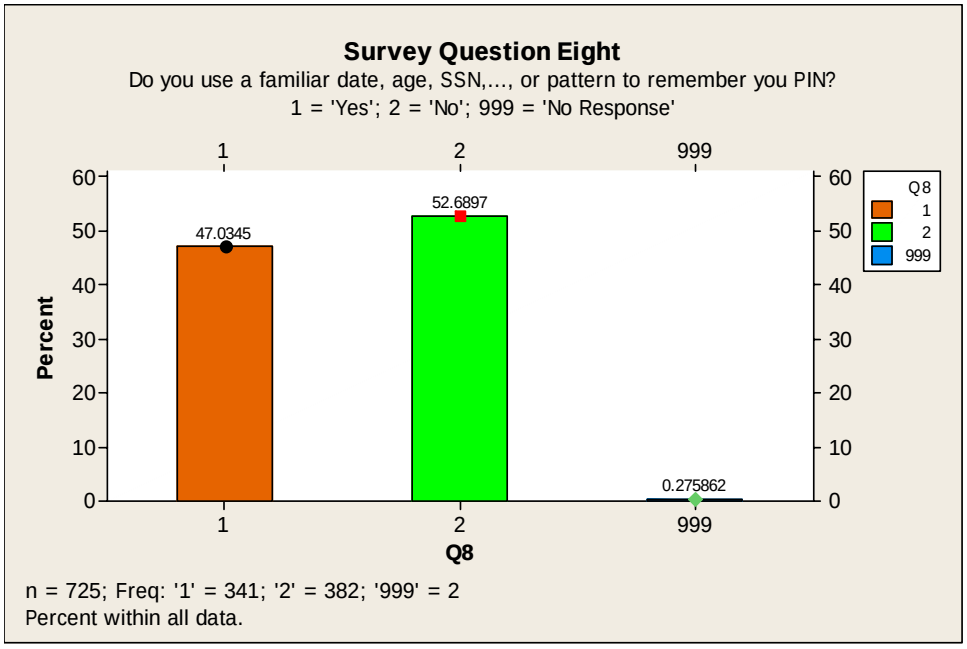

Figure 11 - Do you use a familiar date, age, SSN, sequence, phone number, address, or pattern to remember your PIN?

Survey Question Ten

The tenth investigative question asked, “Do you feel that the CAC and PIN network authentication procedures and parameters are a nuisance?” This question is related to question 24, “Do you feel the PIN policies (creation and use) are burdensome?”, and question 26, “Do you feel that using the CAC and PIN authentication method is burdensome?” of this survey. Additionally, it was similar to a question asked during Martinson’s research, “Do you feel that password parameters are a nuisance?” Martinson’s research showed that 62.1 percent answered ‘Yes’ and 36.7 percent answered ‘No’. In our research, the results were reversed with 34.2 percent answered ‘Yes’ and 57.7 percent answering ‘No’. This implies that the password policies, such as the requirement for long complex passwords and the requirement to change them frequently were more of a nuisance than the burdens imposed under the new authentication technique.

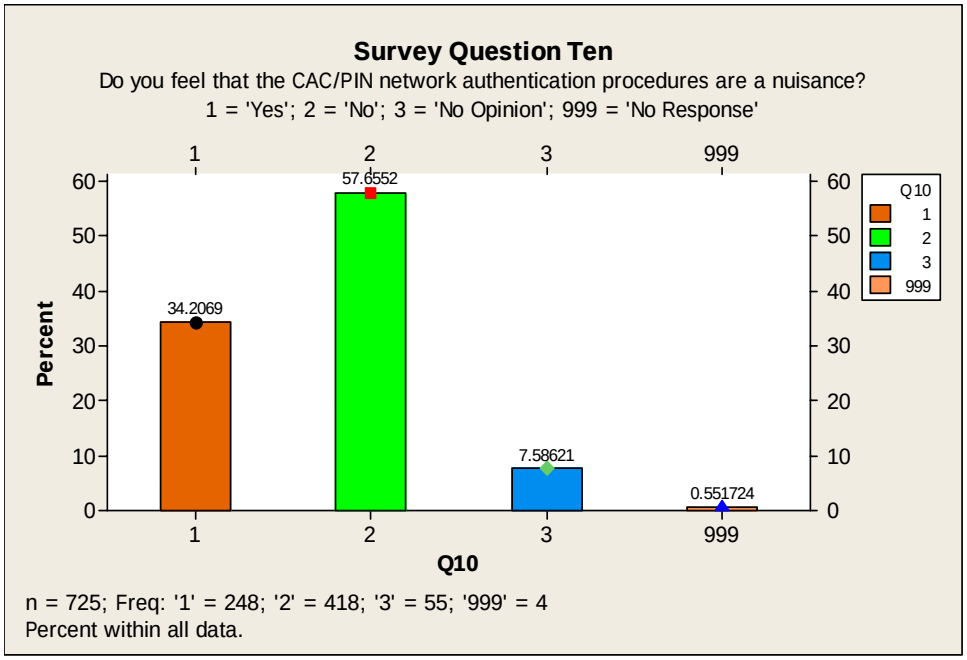

Figure 12 - Do you feel that the CAC and PIN network authentication procedures and parameters are a nuisance?

Survey Question Eleven

The eleventh investigative question asked, "How many PINs (in addition to the one for your CAC) are you currently using?" This question was similar to a question asked during Martinson's research, "How many passwords are you currently remembering/using?" Martinson's research showed that 19.8 percent were remembering up to four passwords, 50.6 percent were remembering 5 to 10 passwords, and 22.5 percent were remembering 11 to 20 passwords. In our research, the results showed that 40.6 percent were remembering 1 to 4 PINs, 42.3 percent were remembering 5 to 10 PINs, and 16.7 percent were remembering more than 10 PINs. It appears that remembering a PIN will be less of a burden than trying to remember a password, as users typically have a fewer number of PINs that they have to remember.

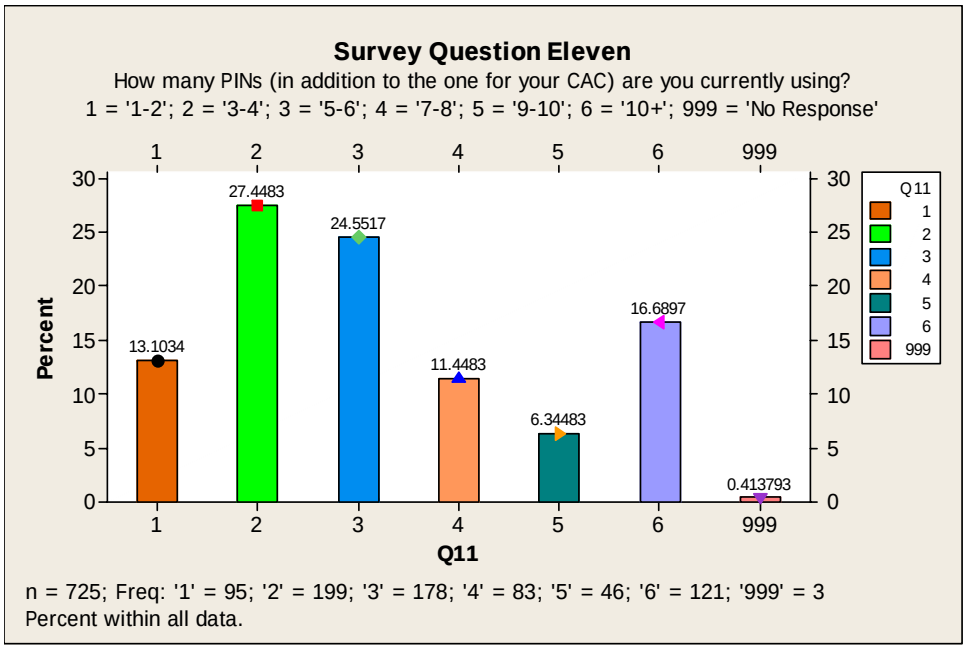

Figure 13 - How many PINs (in addition to the one for your CAC) are you currently using?

Survey Question Twelve

The twelfth investigative question asked, “With the new CAC/PIN authentication, do you have to leave your CAC in the card reader while accessing the network?” In our research, the results showed that 86 percent of the respondents have to leave their CAC in the card reader while they are logged in to the network. 6.9 percent of respondents say that they do not have to leave their CAC in the reader and 6.8 percent state that they only have to do it sometimes. The respondents that have to leave their CAC in the reader in order to stay logged in will be more likely to feel certain adverse affects of the new authentication technique.

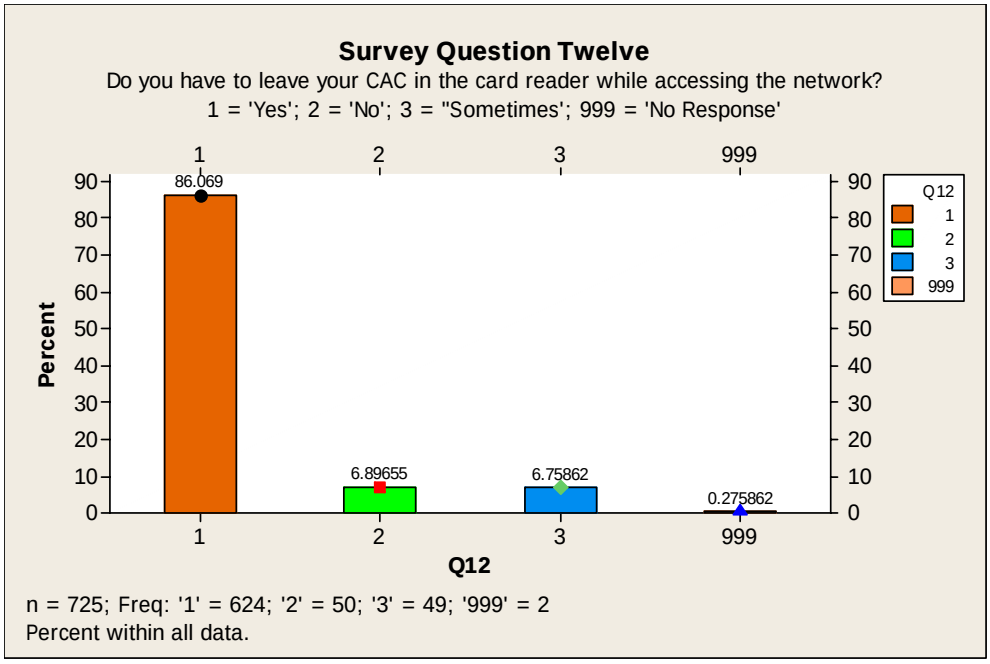

Figure 14 - Do you have to leave your CAC in the card reader while accessing the network?

Survey Question Thirteen

The thirteenth investigative question asked, "In the last 6 months, have you inadvertently left your CAC behind in the computer?" In our research, the results showed that 66.8 percent of the respondents have left their CAC behind. As the CAC is the primary method of accessing the base and base services, this can have a profound effect on the respondent's quality of life. Without the CAC, they will now have to return to work to retrieve the CAC if they want to access any of the base services, and if they have already left the military base, they will have to find someone to escort them back onto the base. Additionally, they now are no longer in control of their card, which then poses a physical security risk.

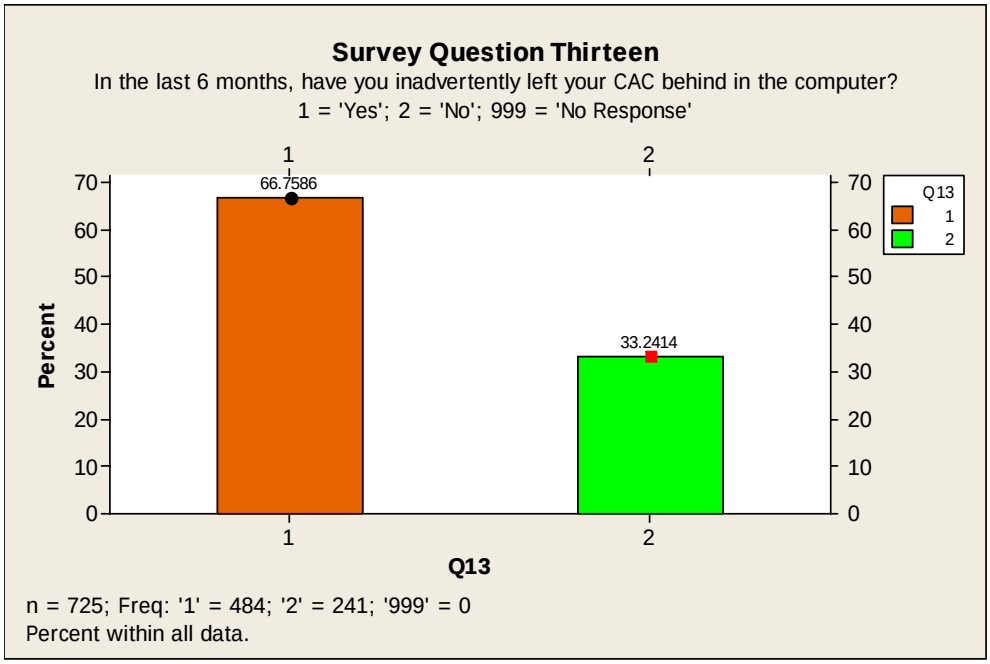

Figure 15 - In the last 6 months, have you inadvertently left your CAC behind in the computer?

Questions fourteen, fifteen, and sixteen were only asked to those who responded 'Yes' to question thirteen, "Have you inadvertently left your CAC behind in the computer?" For these questions, our sample size was n = 484.

Survey Question Fourteen

The fourteenth investigative question asked, "In the last 6 months, how many times have you left your CAC at work, in the computer?" For those individuals that have left their CAC behind, we wanted to get an idea of how frequently this occurred during the last six months. In our research, the results showed that 19 percent of the respondents have left their CAC behind five or more times and 78 percent of the respondents have left their CAC behind more than once. Being the primary method of access to military bases and base services, this could be a potential security threat and an inconvenience to the user.

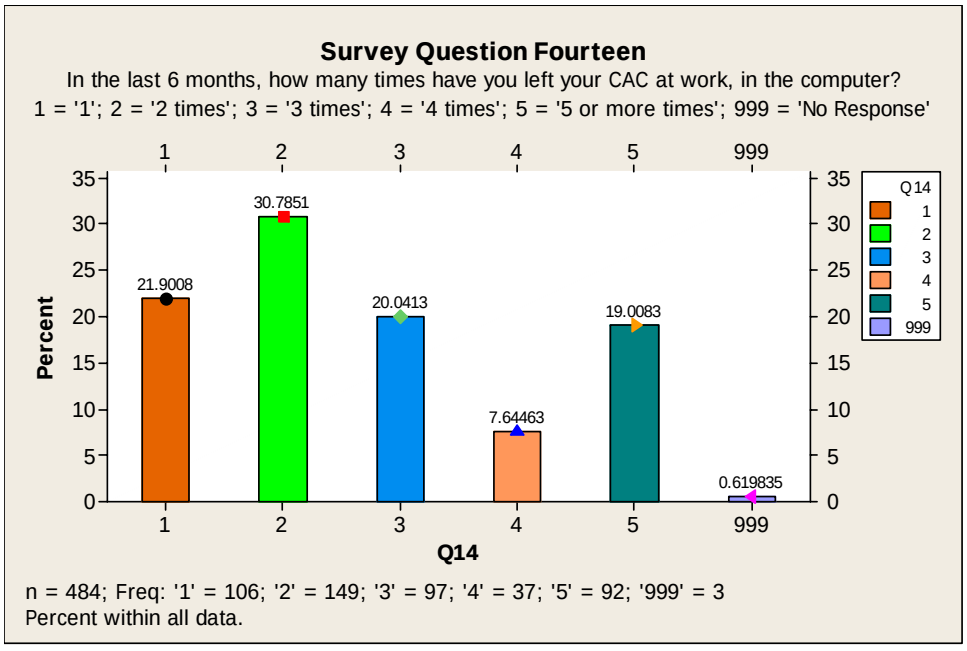

Figure 16 - In the last 6 months, how many times have you left your CAC at work, in the computer?

Survey Question Fifteen

The fifteenth investigative question asked, “How much did the new CAC/PIN authentication technique contribute to this?” 69.4 percent of the respondents stated that the new CAC/PIN authentication technique contributed ‘Greatly’ to them leaving their CAC behind, with an additional 20.2 percent saying that it was at least a factor. It appears that users are still adjusting to having to use their CAC for network authentication and as such, habits such as remembering to take their CAC out of the reader are not yet ingrained.

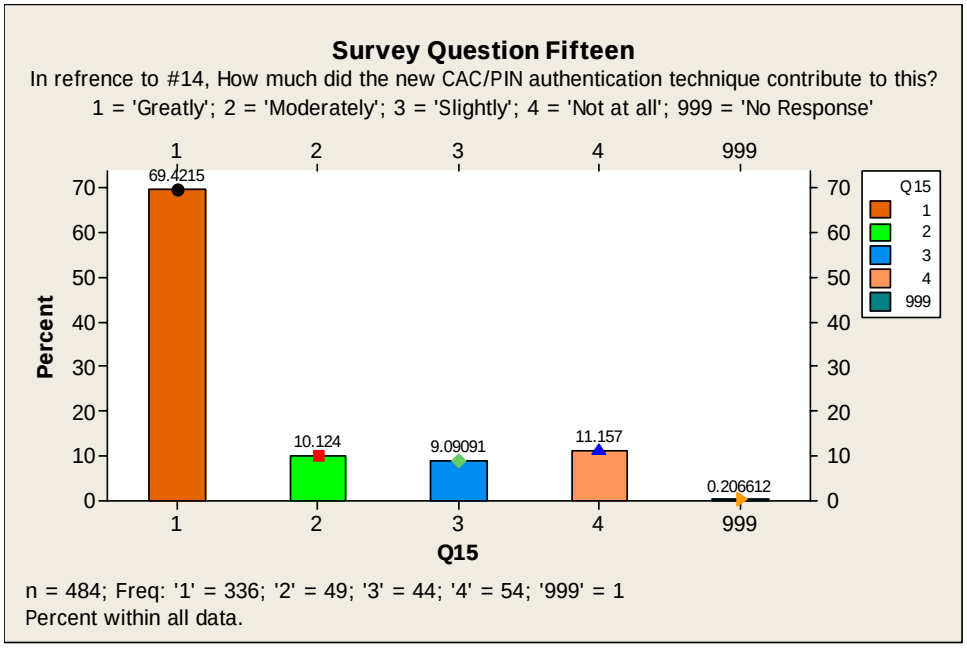

Figure 17 - In reference to #14, How much did the new CAC/PIN authentication technique contribute to this?

Survey Question Sixteen

The sixteenth investigative question asked, “When you left your CAC at work, did it cause you problems in accessing the base or base services?” 62.6 percent of the respondents had problems accessing the base or base services due to leaving their CAC behind in the computer. It appears that there are certainly problems associated with having users use their primary identification method for network authentication.

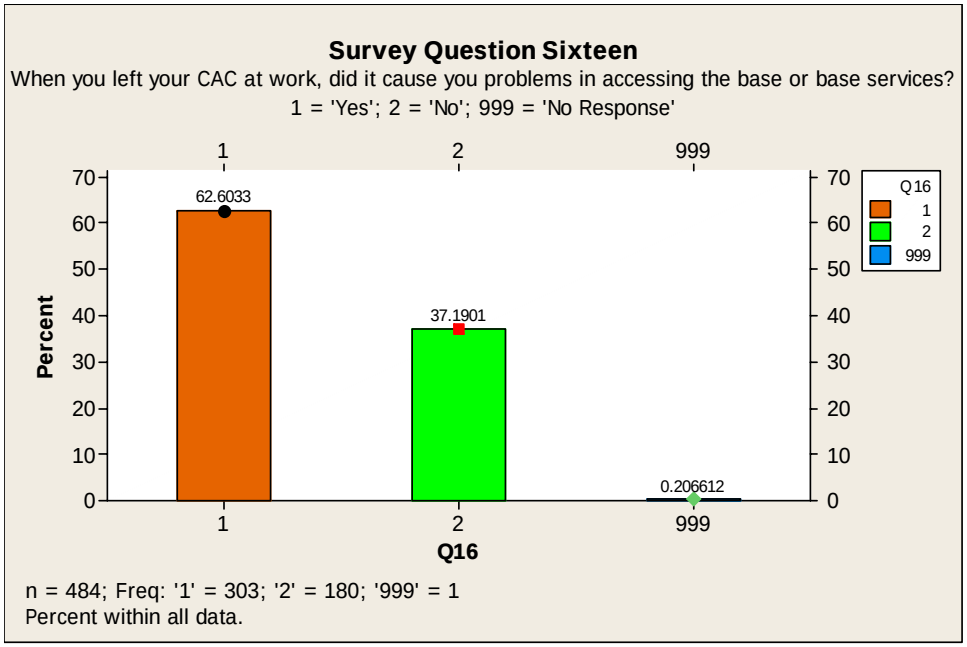

Figure 18 - When you left your CAC at work, did it cause you problems in accessing the base or base services?

Survey Question Seventeen

The seventeenth investigative question asked, “Since implementation of the CAC and PIN to authenticate on the network, has your CAC been lost, stolen, or misplaced?” Results showed that 6.1 percent of the respondents have had their CAC lost or stolen.

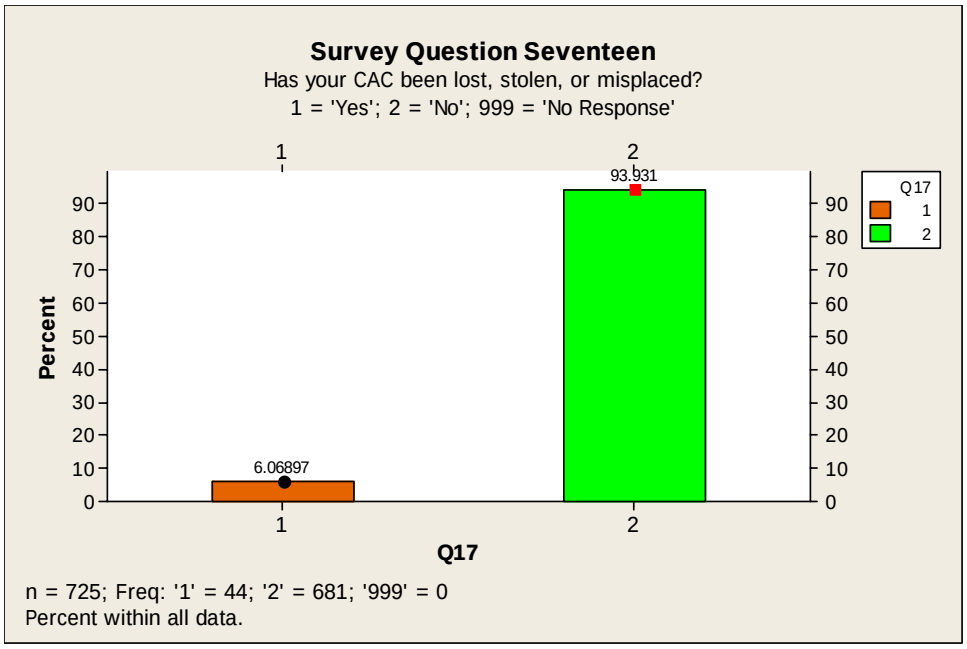

Figure 19 - Has your CAC been lost, stolen, or misplaced?

Questions eighteen and nineteen were only asked to those who responded ‘Yes’ to question seventeen, “Since implementation of the CAC and PIN to authenticate on the network, has your CAC been lost, stolen, or misplaced?” For these questions, our sample population was $n = 44$.

Survey Question Eighteen

The eighteenth investigative question asked, “In reference to the previous question, how many times has your CAC been lost, stolen, or misplaced?” 77.3 percent of the respondents only had their CAC lost, stolen, or misplaced once.

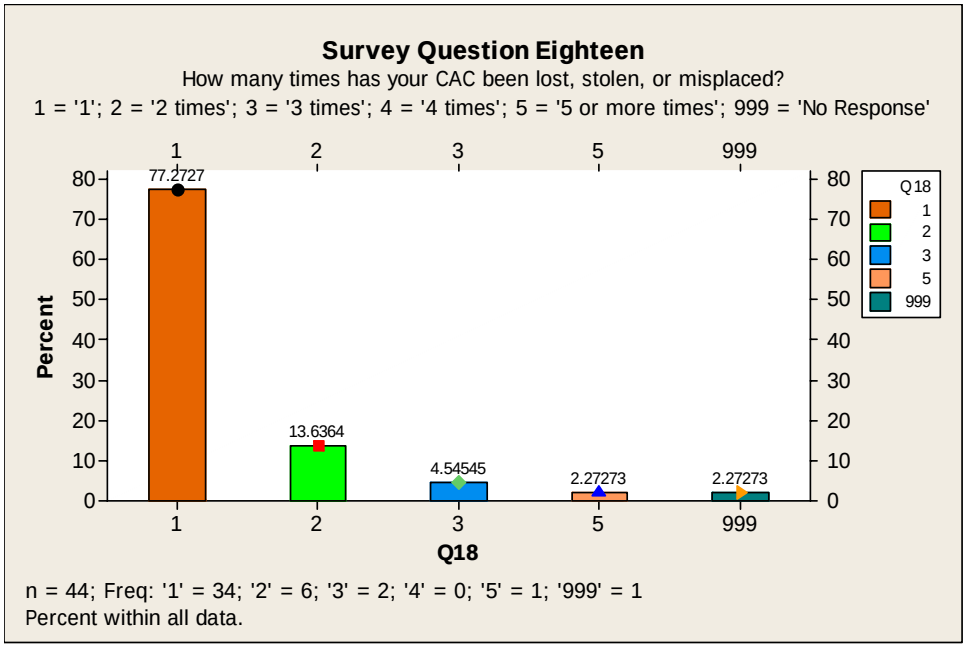

Figure 20 - How many times has your CAC been lost, stolen, or misplaced?

Survey Question Nineteen

The nineteenth investigative question asked, “In reference to the previous question, how much did the new CAC/PIN authentication technique contribute to the loss, theft, or misplacement?” Our results showed that the new CAC and PIN authentication method contributed to 40.9 percent of the CAC loss and thefts. The implication here is that the new authentication technique will cause an approximately 72 percent increase in the number of CACs that are lost or stolen and will require replacement. With the average CAC issuance taking anywhere from 12 to 15 minutes, not including wait times, this can cause a significant additional burden on the Military Personnel Flight as well as a significant loss in productivity of the user.

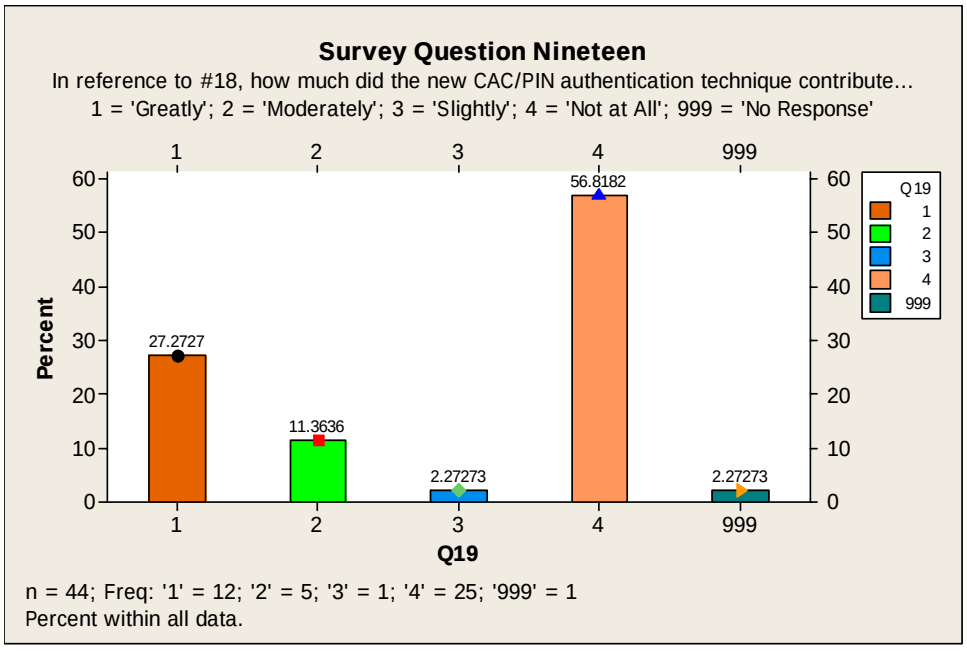

Figure 21 - In reference to #18, how much did the new CAC/PIN authentication technique contribute?

Survey Question Twenty

The twentieth investigative question asked, “In the last year, have you let someone (Co-worker, Friend) borrow your CAC?” This question is related to question seven of our survey, “In the last year, have you shared a PIN with friends, family, co-workers, or others?” and together is similar to a question asked during Martinson’s research, “In the last year, have you ever shared a password with friends, family, co-workers or others?” In order for respondents to share their network account with another user, they would have to let someone borrow their CAC and share their PIN with them. Martinson’s research showed that 39.1 percent answered ‘Yes’ and 60.9 percent answered ‘No’. Our results showed that only 1.2 percent of the respondent has shared their CAC in the last year. This was similar to the response for question 7, where 3.6 percent of the respondents have shared their PIN. It appears at this point that the sharing of user accounts has decreased dramatically due to the new authentication method.

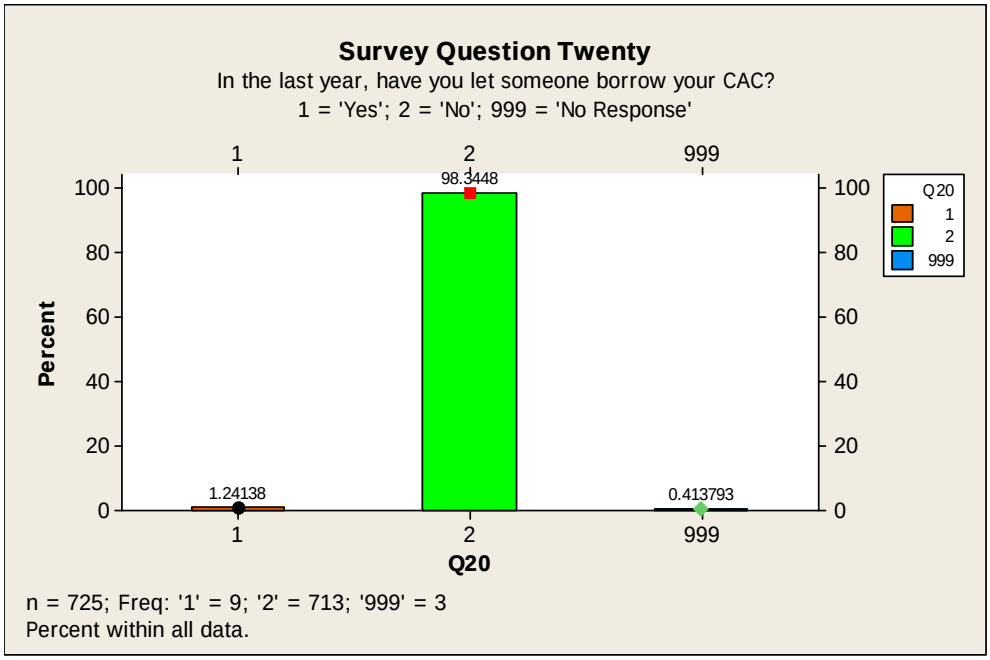

Figure 22- In the last year, have you let someone borrow your CAC?

Survey Question Twenty-One

The twenty-first investigative question asked, “To access your work email account remotely (e.g. Home, TDY, In Transit), do you have to use a CAC reader?” Results showed that 42.9 percent of respondents are required to have a CAC reader present in order for them to access their work email accounts from remote locations. All other respondents either do not try, and thus do not know, to access their work email accounts from remote locations or are still allowed to logon remotely via Webmail or a Virtual Private Network (VPN) connection without the need for a CAC.

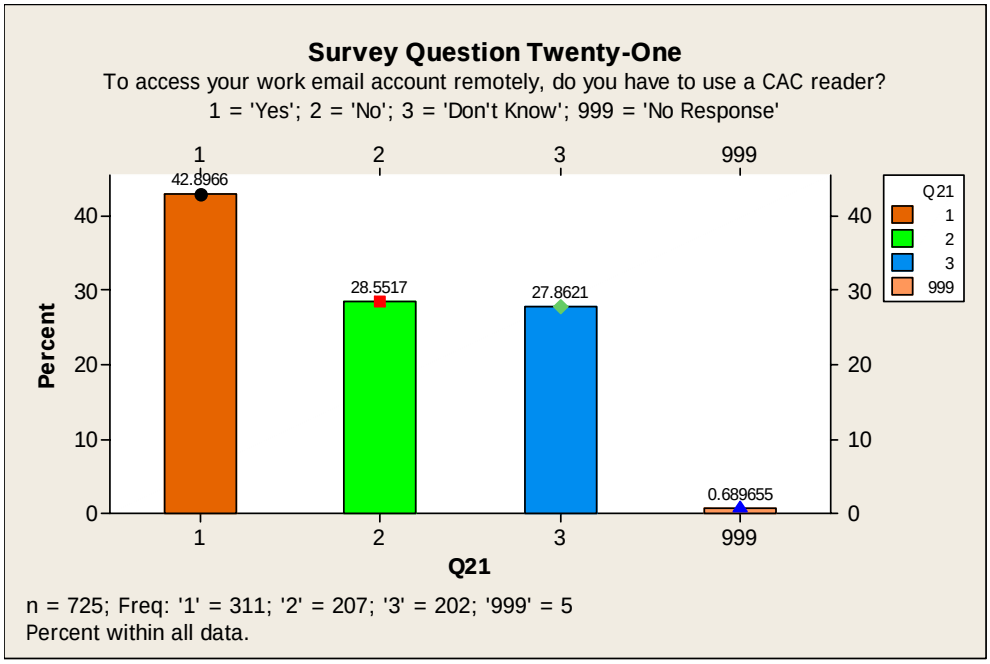

Figure 23- To access your work email account remotely, do you have to use a CAC reader?

Survey Question Twenty-Two

The twenty-second investigative question asked, “Since implementation of the CAC/PIN authentication, how would you rate the ease of accessing the network remotely?” In figure 24, our results are based on all respondents’ answers regardless of whether remote access requires a CAC. In figure 25, our results are based only on those that have to use a CAC reader to remotely access their work email (i.e., they answered ‘Yes’ on question twenty-one). It appears that mandatory CAC use from a remote location has a significant impact on the user.

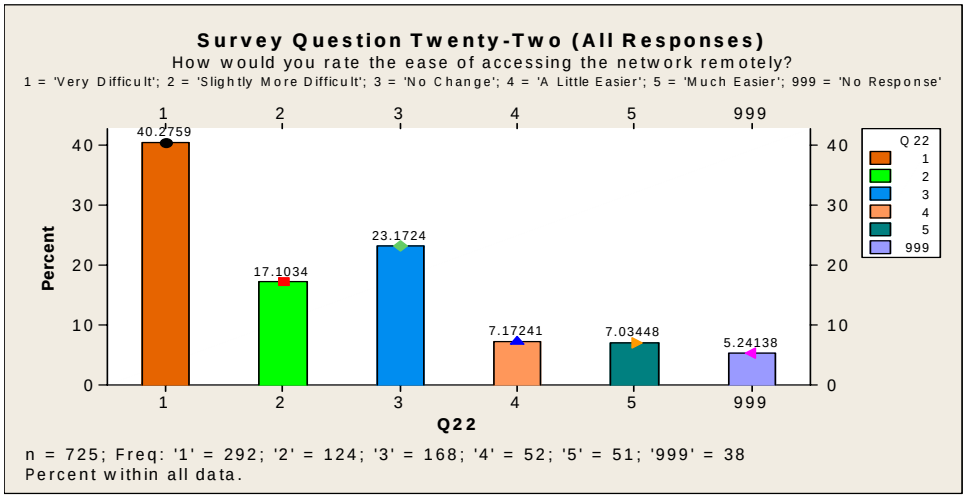

Figure 24 - How would you rate the ease of accessing the network remotely?

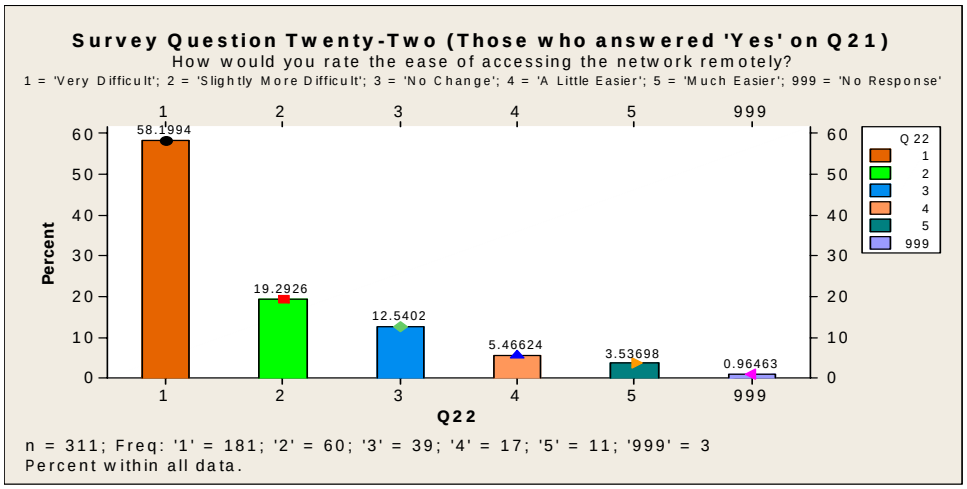

Figure 25 - How would you rate the ease of accessing the network remotely?

Survey Question Twenty-Three

The twenty-third investigative question asked, “How would you characterize your organization’s training and education relating to the creation of PINs and the use of the CAC card for network authentication?” This question was similar to a question asked during Martinson’s research, “How would you characterize your organization’s training and education relating to the creation of passwords?” Martinson’s research showed 7.7 percent thought is was ‘Outstanding’, 31.7 percent rated it ‘Good’, 45 percent rated it ‘Adequate’, 8.6 percent rated it ‘Needs Improvement’, and 5 percent rated it ‘Poor’. This is very similar to our findings (see figure 26). It appears that the level of training related to the new authentication technique has not changed significantly from the training for the previous authentication method.

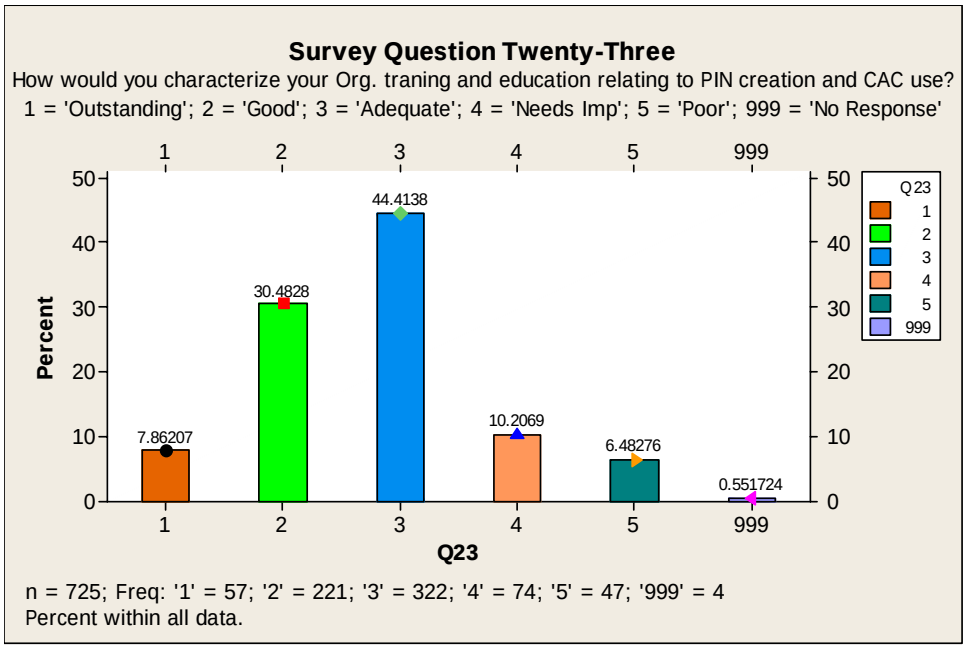

Figure 26 - How would you characterize your Org. training and education relating to PIN creation and CAC use?

Survey Question Twenty-Four

The twenty-fourth investigative question asked, "Do you feel the PIN policies (creation and use) are burdensome?" This question is related to survey question ten and survey question twenty-six and is similar to a question asked during Martinson's research, "Do you feel the password policies of your organization are burdensome?" Martinson's research showed that 50.9 percent considered the password policies a burden and 44.4 percent did not consider it a burden. In our research, the results showed a decline with only 32.3 percent of the respondents considering the PIN policies a burden.

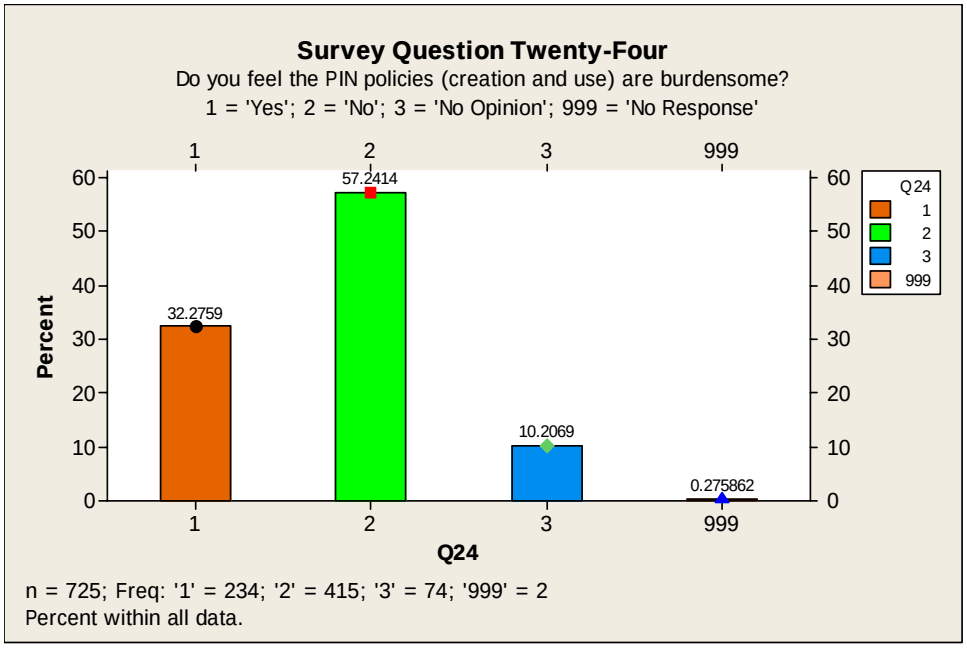

Figure 27 - Do you feel the PIN policies (creation and use) are burdensome?

Survey Question Twenty-Five

The twenty-fifth investigative question asked, “Do you follow CAC/PIN procedures based on organizational guidance?” This question was similar to a question asked during Martinson’s research, “Do you follow the password procedures based on organizational guidance?” Martinson’s research showed that 84 percent answered ‘Yes’. Our results were very similar with 81.8 percent of respondents answering ‘Yes’.

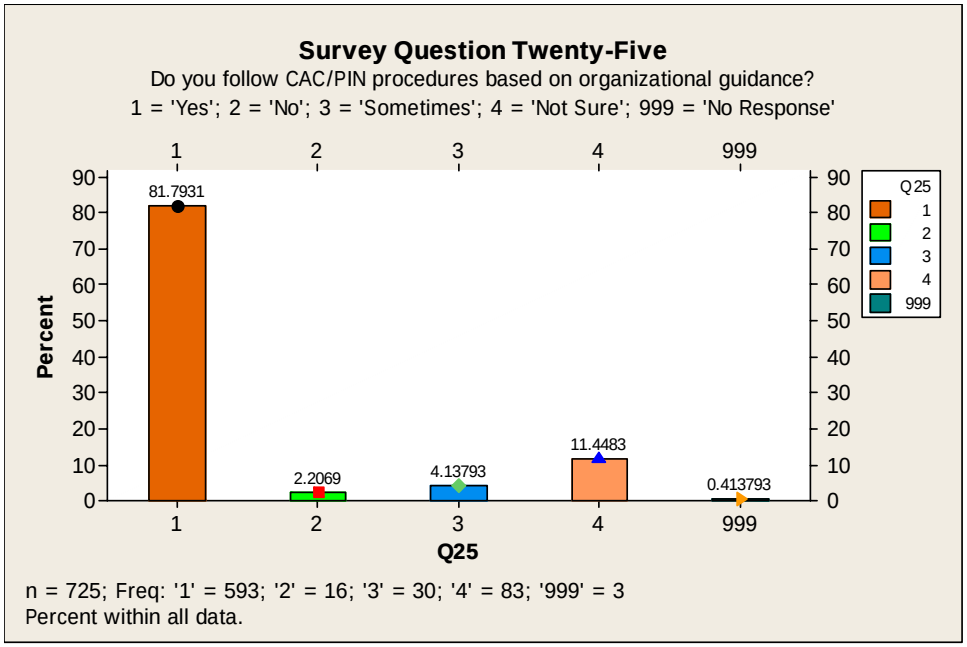

Figure 28 - Do you follow CAC/PIN procedures based on organizational guidance?

Survey Question Twenty-Six

The Twenty-sixth investigative question asked, “Do you feel that using the CAC and PIN authentication method is burdensome?” This question is related to survey question ten, “Do you feel that the CAC and PIN network authentication procedures and parameters are a nuisance?”, and survey question twenty-four, “Do you feel the PIN policies (creation and use) are burdensome?”, and is also similar to a question asked during Martinson’s research, “Do you feel the password policies of your organization are burdensome?” Martinson’s research showed that 50.9 percent considered the password policies a burden and 44.4 percent did not consider it a burden. In our research, the results showed a decline with only 37.1 percent of the respondents considering the PIN policies a burden.

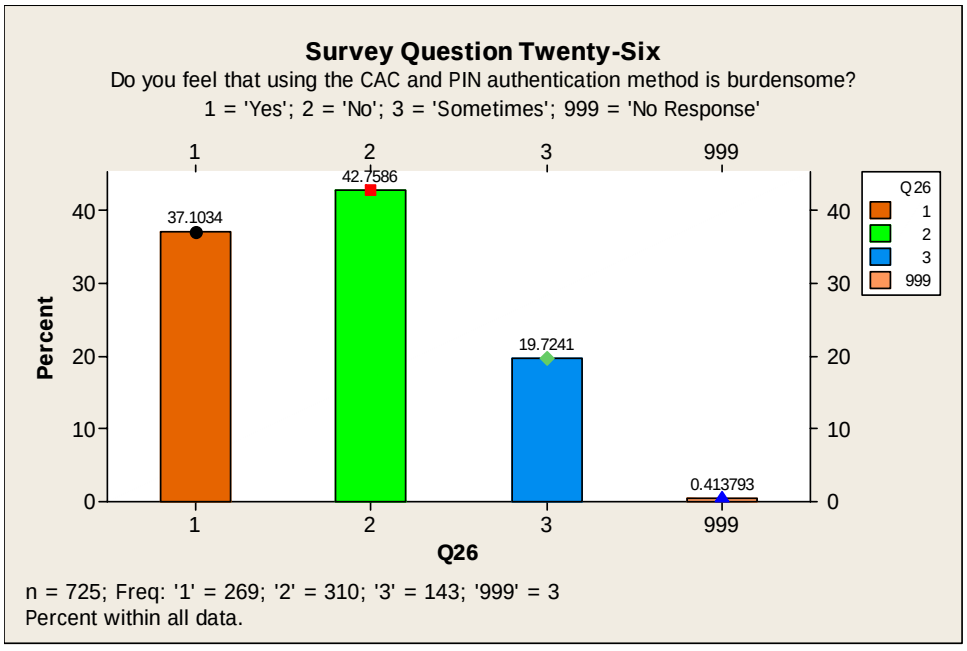

Figure 29 - Do you feel that using the CAC and PIN authentication method is burdensome?

Survey Question Twenty-Seven

The Twenty-seventh investigative question asked, "If you think it is burdensome (referring to the previous question), why?" Seven choices and a comment field followed this question. The users were allowed to select more than one reason. The results of the selectable options are located in figure 30. Respondent comments were categorized and the number of responses for each category are located in figure 31.

Percent (n=725)	*Reason (selecting all that apply)*
36.4	Small errands in the office require taking the CAC with me
35.5	Accessing my email remotely is more difficult
32.6	If I forget or lose my CAC, I can't access the network to do my job
24.8	Have to get CAC from wallet, purse, etc.
21.4	I'm always forgetting to take the CAC card out of the card reader
19.7	I don't think it is burdensome
19.5	Other Reasons

Figure 30 – If you think CAC/PIN authentication is burdensome, why?

Response # (n=170)	*Written responses under category "other" (generalized categories)*
37	Remote access to email is difficult or impossible
24	Takes too long to Logon/Unlock computer
18	Have to enter PIN multiple times
15	Have to get CAC from wallet, purse, etc.
12	Concerns about physical vulnerability of the CAC
11	CAC is being damaged by constant use
8	MPF replacement takes forever

Figure 31 - If you think CAC/PIN authentication is burdensome, why? Comments

Questions twenty-eight through thirty-one were included in the research study at the behest of the sponsoring organization, the Air Force Communications Agency. While the results provide insight into the respondent's views between the Logon ID and Password authentication technique and the new CAC and PIN authentication method, they are not directly related to the purpose of this study.

Survey Question Twenty-Eight

The twenty-eighth investigative question asked, "Do you believe the previous method of securing network access (Logon ID and Password) was a sufficient means of ensuring network security?" The results showed that 62.5 percent of the respondents believed that the old authentication technique to be sufficient for network security.

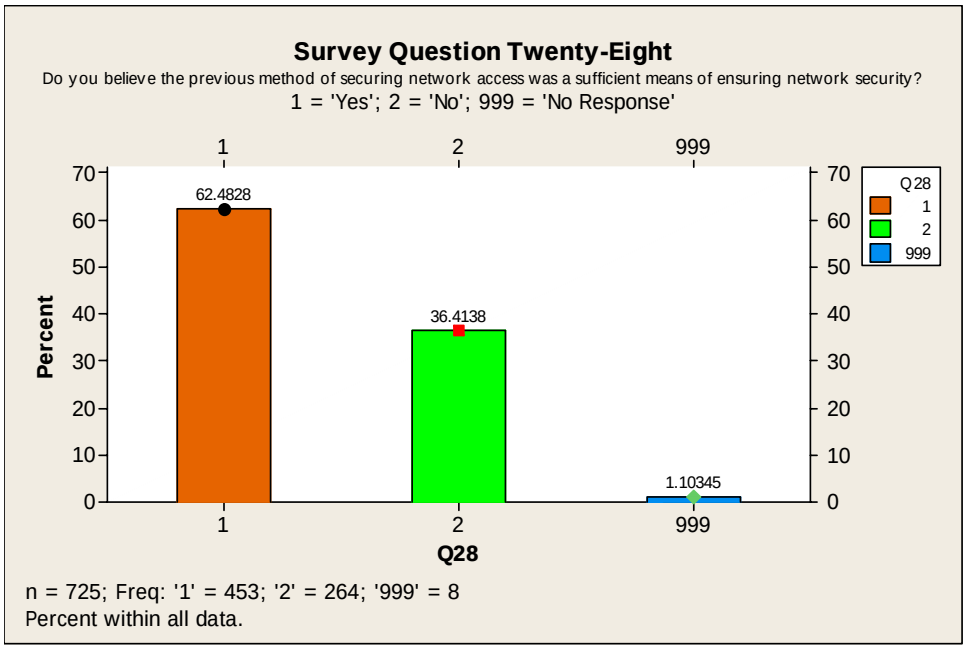

Figure 32 - Do you believe the previous method of securing network access was a sufficient means of ensuring network security?

Survey Question Twenty-Nine

The twenty-ninth investigative question asked, “Do you believe that using a CAC to logon to the network is more secure than Logon ID and Password?” The results showed that 65.1 percent of the respondents believed that the CAC and PIN authentication technique is more secure than the Logon ID and Password authentication technique.

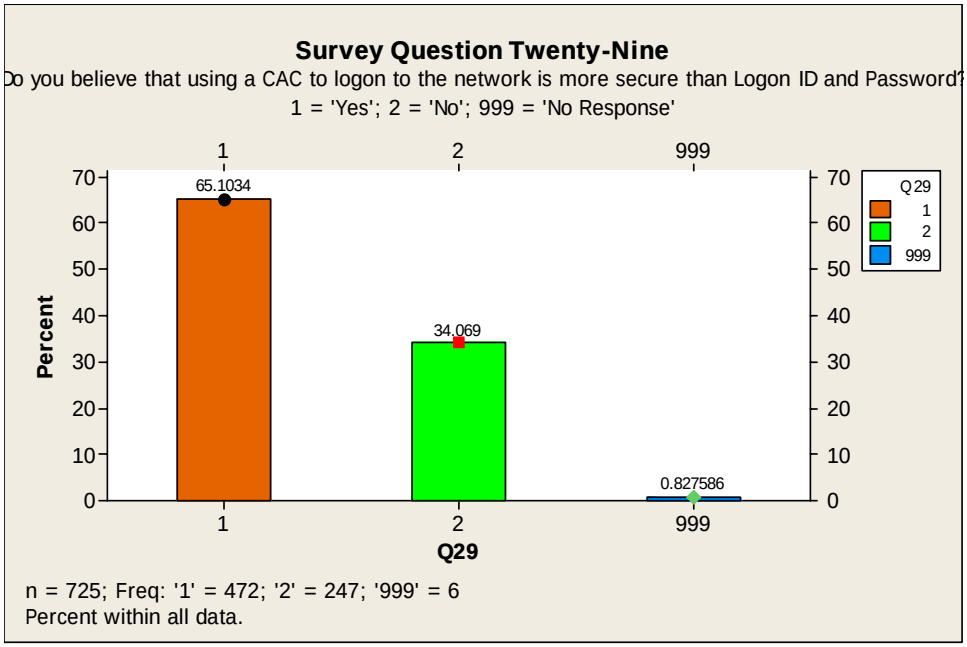

Figure 33 - Do you believe that using a CAC to logon to the network is more secure than Logon ID and Password?

Survey Question Thirty

The thirtieth investigative question asked, “Do you believe using the CAC to logon to the network is: (choose one):”, and then offered two options. The results showed that 26.5 percent of the respondents believed that the CAC and PIN authentication technique is “An Inconvenience’ and 71.4 percent believe it to be “A Necessary Security Evolutionary Requirement.’

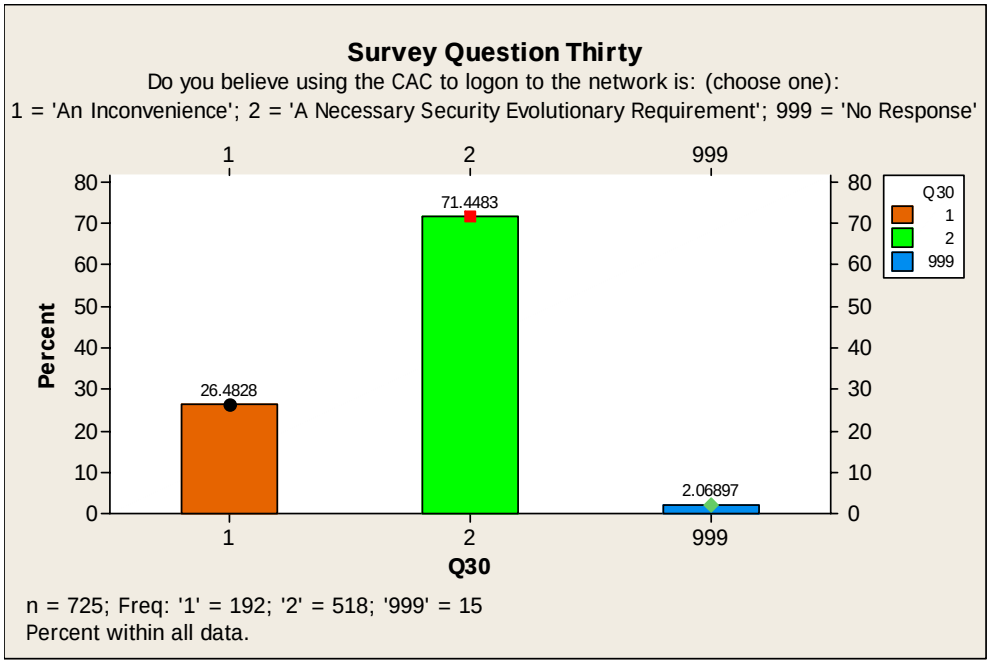

Figure 34 - Do you believe using the CAC to logon to the network is: (choose one):

Survey Question Thirty-One

The thirty-first investigative question asked, “Do you believe that network access conveniences take priority over security?” The results showed that 11.2 percent of the respondents believed their convenience takes priority over network security.

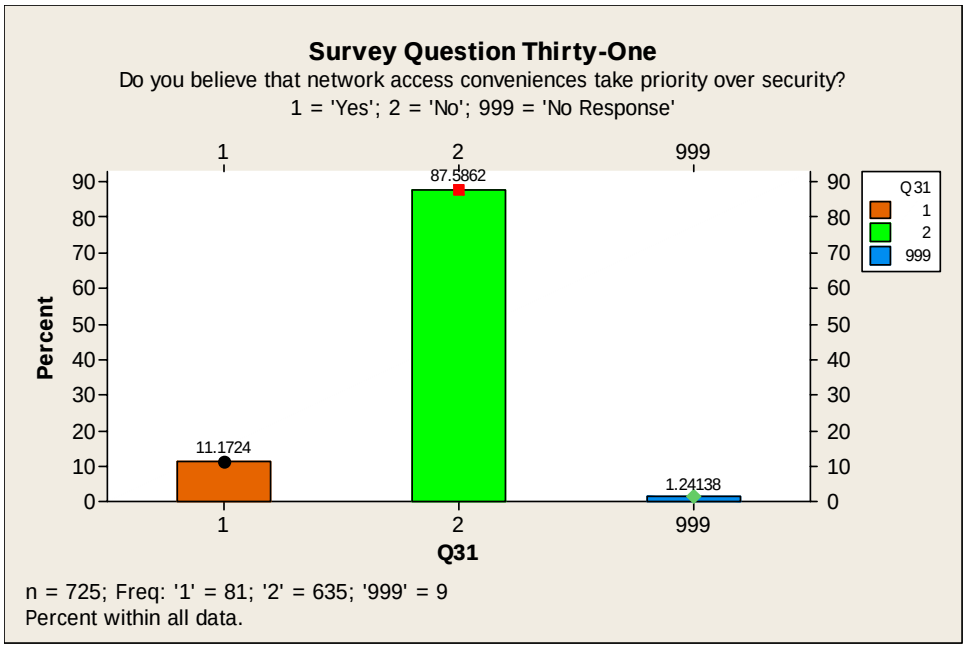

Figure 35 - Do you believe that network access conveniences take priority over security?

Questions thirty-two and thirty-three were included to determine respondent's interests in possible future authentication techniques.

Survey Question Thirty-Two

The thirty-second investigative question asked, "If you had a choice of methods to gain access to the network, which would you prefer?" Our results showed 38.2 percent, the highest proportion, of the respondents are interested in utilizing their fingerprints for authentication. This is higher than the Logon ID and Password technique at 17.66 percent and the CAC and PIN authentication technique at 24.1 percent.

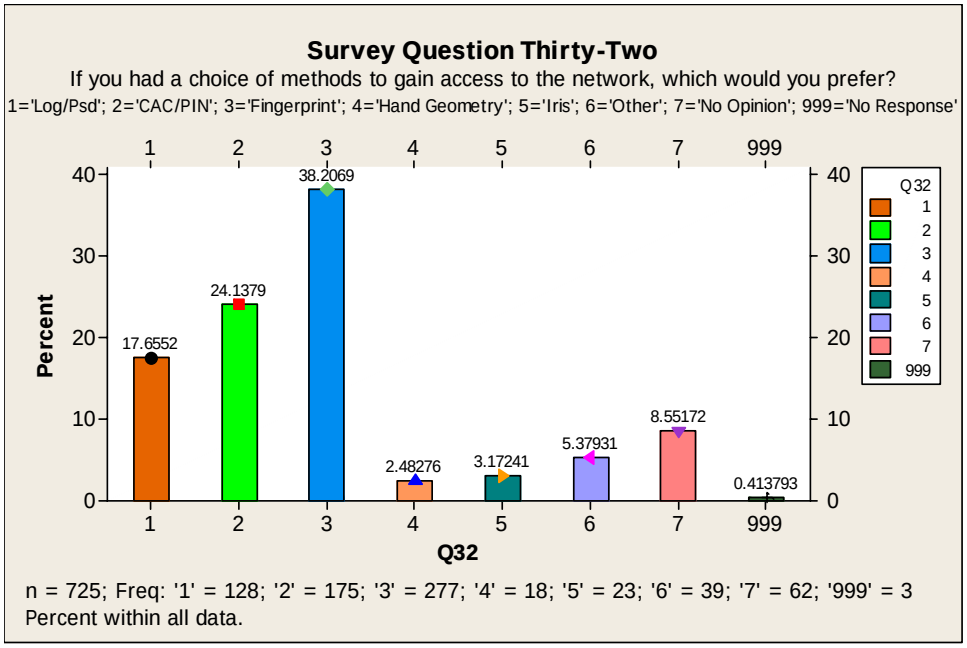

Figure 36 - If you had a choice of methods to gain access to the network, which would you prefer?

Survey Question Thirty-Three

The thirty-third investigative question asked, "Would you prefer a separate card (similar to CAC, but not for ID) specifically for network authentication?" Our results showed that 54.8 percent of the respondents did not want a separate card for network authentication.

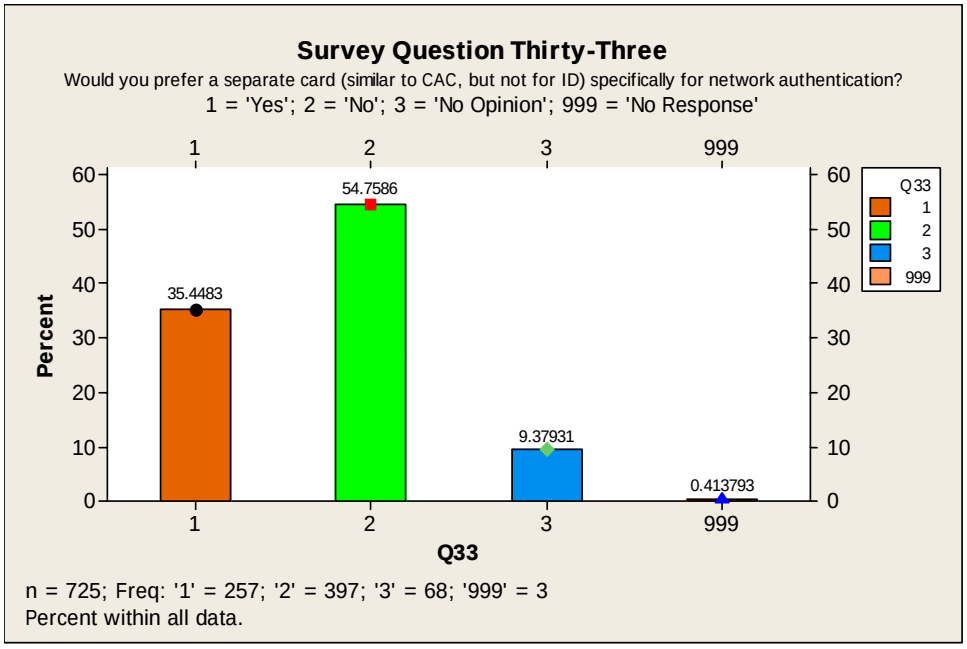

Figure 37 - Would you prefer a separate card (similar to CAC, but not for ID) specifically for network authentication?

Questions thirty-four to thirty-six asked respondents for their general comments regarding the CAC and PIN authentication technique in addition to specific inquires about increasing security and usability. I think that I might have biased the results slightly as many respondents stated that they like the ideas mentioned in questions 32 and 33 of the survey. The results are summarized below. I removed responses that identified specific organizations or included inflammatory comments.

Survey Question Thirty-Four

The thirty-fourth investigative question asked, "What do you think could increase usability/accessibility of the CAC/PIN method without sacrificing security?" The list below represents the common responses to this question. It should be noted that some responses did not fit this question as they are related to other authentication techniques (e.g. biometrics). Those responses belonged under question thirty-five.

- Ability to remove card after logon (swipe card/RFID enable cards)
- Ability to logon to more than one computer (and more than 1 at a time)
- Build more durable cards (increased use forcing replacement sooner)
- Speed up logon/unlock process (currently takes up to 30 sec)
- CAC enable more DoD sites (users still have to remember passwords)
- Reduce the number of CAC authentications (should only have to authenticate CAC once when you logon, then it should be good for all other locations, websites that you visit)
- Ease remote access capability (many users are frustrated with inability to check their email while away from the office)
- Allow base to base use (should be able to access email from any military/DoD installation with your CAC)
- One email address that follows users everywhere (would reduce requirement to reset CAC every time you PCS and allow you to access encrypted emails from previous assignments)
- Disable login ID and password (some users still have to change a password every ninety days, even though they use the CAC and PIN authentication technique)
- Another card for network access separate from our ID card
- Allow lanyards to be attached to CAC (requires hole punch)

Survey Question Thirty-Five

The thirty-fifth investigative question asked, "What do you think could increase security without sacrificing usability?" The list below represents the common responses to this question.

- Implement Biometric authentication techniques (many respondents were concerned about inability to access base or network if they did not have

their CAC on them. Biometrics would reduce number of CACs left in office and would not require someone to return home if they forgot their CAC)

- Greater flexibility with PIN creation (remove guidelines)
- Implement a two-tiered authentication method that uses a USB based token. This would eliminate the need to install a CAC reader at remote location as most computers come standard with USB ports.
- Implement a three-tiered authentication system (what I know, what I have, what I am). This would require the use of a PIN, CAC, and a Biometric.
- Standardize CAC and PIN authentication across commands/bases (depending on where you go, implementation standards are determined by command and local installation policies)
- Block familiar PIN patterns (SSN, Birthdate, etc)

Survey Question Thirty-Six

The thirty-sixth investigative question asked, "Please share any additional comments?" The list below represents the highlights of those responses that are not addressed in the previous two questions.

- **CAC/PIN are causing a physical security problem**
  - "Many people in the section leave their CACs in the reader when they step out of the office for a few minutes"
  - "I have left my CAC card in for short periods of time (e.g. go to the bathroom, get a cup of coffee)"
  - "Most of us will not pull our CAC every time we leave our computers because we just don't think about it and it takes so long to log back on…"
  - What kind of screening is done on maintenance, housekeeping and cleanup personnel? As these people have access to most areas, it would be very easy for one of them to pocket an ID left in a CAC reader and sell it to someone whose intentions are bad
- **Respondents suggested ways to reduce CAC leave behinds**
  - Have computers emit an audible warning during the logout process if the card is left in the reader
  - Organizations post signs by the exits reminding people to take their CAC with them when they leave the building
  - Automatically locking the machine when user removes their CAC
  - Use keyboards with attached CAC readers
- **Concerns about the different treatment based on rank**

    - Burdens go unnoticed by senior leadership because most senior officers have Blackberries that allow them to send/receive emails without the use of mandatory CAC login
- **More remote access concerns**
    - "Do we really all need to check email at home? ... If someone really needs you they can use a phone. For senior officers and commanders, maybe we can find a way to access email from home, but NOT the entire network."
    - "And lack of remote access (while TDY/on leave) is significantly slowing down our communication while away from home station. That needs to be fixed ASAP. I'm a large squadron CC and remote access (web or Blackberry) greatly helps getting/providing timely direction, especially during crisis events."
    - "Since the implementation of CAC card authentication, I can access the Outlook Web Access (OWA) only through my work PC, and that really defeats the mobility purpose of OWA access."
    - "Even if you have a USB plug-in CAC reader the user level that non-IT people set on most networked computers will not allow hardware to be added"
- **Inconsistent application of standards**
    - "My only issue is the command policy of maintaining a password that I never use and cannot remember."
    - "Please push activation of CAC/PIN login for OWA access"
    - "There has been no determination as to who can and will receive CAC readers; so most of the population has been locked out"
    - "I'm a Squadron CC and I can't get OWA at home because I don't have a CAC reader at home and the AF hasn't issued one. The AF should pay for it-not me. With a busy lifestyle this should be afforded to CCs. You axe my access, but don't give me the out. I'll figure it out and get a CAC reader, but good grief."
    - "While we are required to use the CAC/PIN we are still required to change passwords every 60 days. The only time you use that password is if there is a problem and you CAC/PIN are not working."
    - "Why is it that we still have to log in with user name and password plus the CAC/PIN."
    - "Here at ----- AFB, we cannot access .mil email accounts remotely…"
- **CAC transportability**
    - Current method of certificate based on e-mail leads to the danger of losing valuable information if it was sent encrypted and my e-mail address changes, i.e. when I PCS."
- **Unique environments and the CAC**

- "When you have to jump on and off the network on different machines all day, it's easy to forget your card and difficult to use the network"
- I work in an environment where we dedicate computers to a specific duty position. There are times when a person at a specific position has to leave the office. If that vacant position is then tasked with a request and another person needs to fill that position, the vacated computer may or may not be available for use. Additionally, it is very difficult to do so because the person trying to cover dual positions doesn't have 2 CACs.
- "I am a reservist and civilian who needs to access to separate networks and can not."
- "Unable to obtain Host Nation approval for issuance of CAC cards to local national employees in some countries due to concerns over biometric data that is required"
- "big issue with allowing local nationals having CAC…many still do not feel that they should have to use one. Their feeling is that the card contains personal information that should not be made available."

- **CAC a single point of failure?**
  - "I am very uncomfortable having everything tied to a single item like the CAC/ID card. It represents a single failure point for many uses all of which become very difficult should the ID be stolen, damaged or lost."

Demographics

The typical respondent was a 41-50 years old (38.6 percent), male (70.2 percent), and does not work in computer or network security (82.5 percent). The results are in figures 38 to 41. One item of note: each participant works for the military in either an active or a civilian capacity. This will lend credibility to the findings as these individuals are respected for their integrity and ability to follow rules and policies (Martinson 2005).

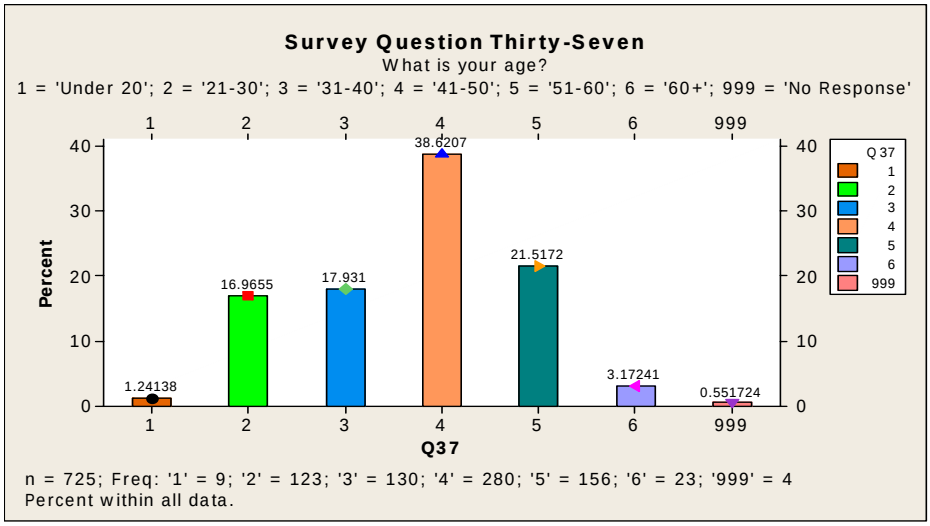

Figure 38 – What is your age?

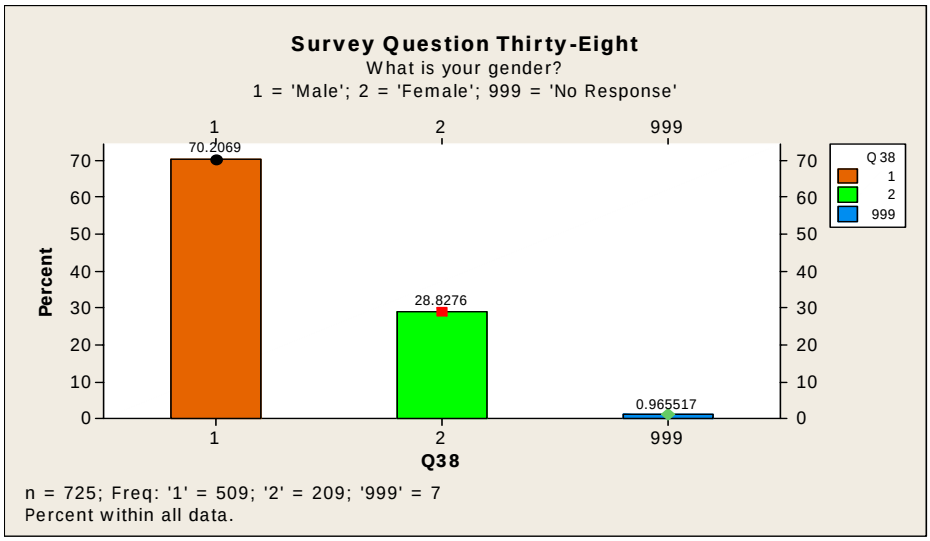

Figure 39 – What is your gender?

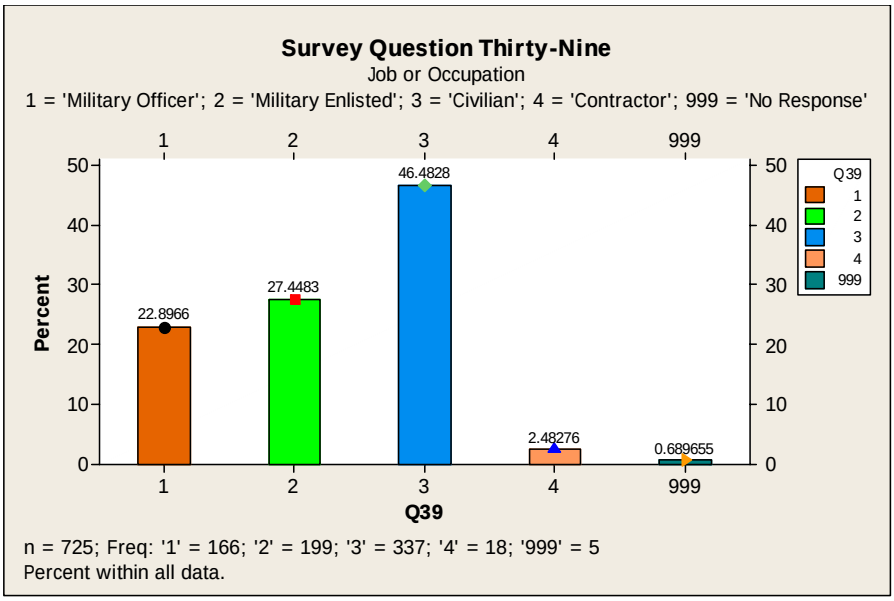

Figure 40 – Job or Occupation

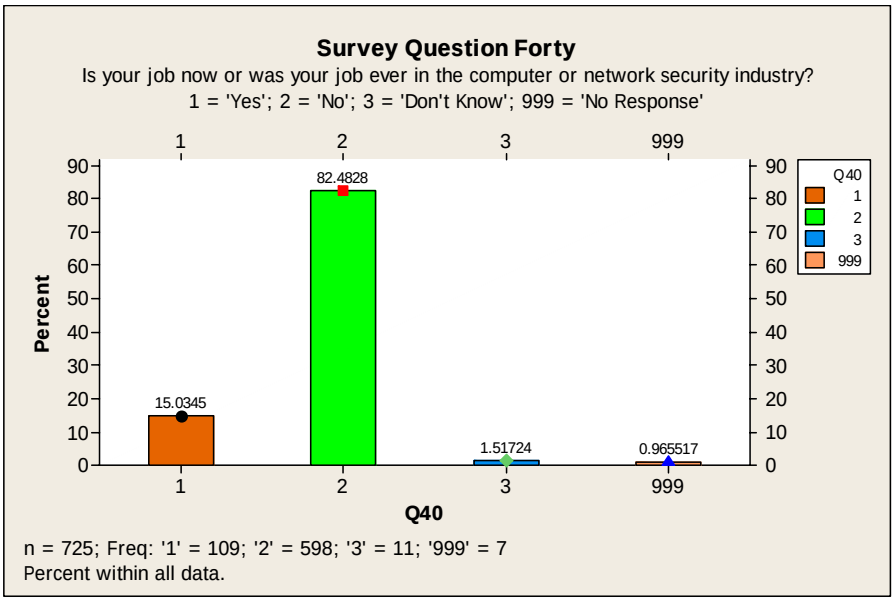

Figure 41 – Is your job now or was your job ever in the computer or network security industry?

Data Analysis

This section is dedicated to analyzing the results of the survey against the research hypothesis of this study. Once again, the research hypotheses are:

1) The implementation of a two-factor authentication technique will increase the effectiveness of network authentication as related to human factors.
2) The vulnerabilities that affect a strictly password based authentication method will not have an effect on the PIN portion of a two-factor authentication method?
3) Individuals will be more likely to adhere to policy guidance under the new authentication method as compared to password authentication.
4) The new authentication technique will contribute to a loss in worker productivity and smart cards.
5) Accessibility of the networks will decline as individuals find it more difficult to perform job tasks away from the primary workplace (i.e. TDY, Leave) due to the requirement of having a token to authenticate.

Research Hypotheses One and Two

Survey questions 3-7, 11, and 20 of this research pertained specifically to the first hypothesis, "The implementation of a two-factor authentication technique will increase the effectiveness of network authentication as related to human factors." Survey questions 3, 5-7, 11, and 20 of this research pertained specifically to the second hypothesis, "The vulnerabilities that affect a strictly password based authentication method will not have an effect on the PIN portion of a two-factor authentication method?" We analyzed these hypotheses with a direct comparison of the survey results

between Martinson's research and ours (Table 3). Because the independent variable (i.e. the authentication technique) is nominal (or categorical) as is the dependent variables (i.e. yes, no, don't know), I will use a Chi-Square Goodness-of-Fit test to analyze each of the related questions and whether or not the results are significant around $\alpha = .05$. The initial indications seem to show that the CAC and PIN authentication technique enhances authentication effectiveness and that some of the vulnerabilities highlighted during Martinson's research show a decline with this new authentication method.

In response to the question, "Have you ever changed your PIN/Password so that it is easier to remember?" The hypotheses are:

- H_o: The proportion of password changes and PIN changes are the same
- H_a: The proportion of password changes and PIN changes are different

The proportion of users answering 'Yes' to this question dropped from 68.6 percent to 24.9 percent (Table 3). Utilizing the chi-square analysis (Table 4), we get a chi-square of 291.2 and a p-value of 0.000. We must reject the null hypothesis and conclude that the proportion of password changes and PIN changes for ease of remembrance are significantly different. Fewer users changing their PIN to some pattern (e.g., SSN, birthdates, etc…) that would allow them an easier ability to remember, reduces the vulnerability to an outside user guessing the PIN based on some familiar aspect of the user.

Table 3 - Research Hypothesis 1/2 Raw Data Analysis

Question Asked (M - Martinson; A - Alsop)	Question Number	Response			
		Yes	No	Don't Know	No Response
*Have you ever changed your Password(**M**)/PIN(**A**) so that it is easier to remember?*	M-Q7	68.6	30.2	1.2	
	A-Q3	**24.9**	**74.4**	0.6	
*Has your Password(**M**)/PIN(**A**) ever been compromised*	M-Q2	5.3	69.5	25.1	
	A-Q4	**0.3**	**93.9**	5.8	
*Do you use the same Password(**M**)/PIN(**A**) for multiple applications*	M-Q3	96.2	3.6		0.3
	A-Q5	**25.6**	**74.4**		0
*In the last year, have you written down your Passwords(**M**)/PINs(**A**)?*	M-Q4	71.3	28.7		
	A-Q6	**21.4**	**78.6**		
*In the last year, have you shared a Password(**M**)/PIN(**A**) with friends, family, co-workers, or others?*	M-Q5	39.1	60.9		0
	A-Q7	**3.6**	**96.1**		0.3
In the last year, have you let someone (Co-worker, Friend) borrow your CAC?	A-Q20	**1.2**	**98.3**		0.4
		1-4	**5-10**	**10+**	**No Response**
*How many Passwords(**M**)/PINs(**A**) are you currently using?*	M-Q10	19.8	50.6	22.5	0.3
	A-Q11	40.6	42.3	16.7	0

In response to the question, "Has your PIN/Password ever been compromised?" The hypotheses are:

- H_o: Password and PIN susceptibility to compromises are the same
- H_a: Password and PIN susceptibility to compromise are different

The proportion of users answering 'Yes' to this question dropped from 5.3 percent to 0.3 percent (Table 3). More remarkable is the increase of users responding 'No' from 69.5 percent to 93.9 percent. Utilizing the chi-square analysis (Table 4), we get a chi-square of 88.4 and a p-value of 0.000. We must reject the null hypothesis and conclude that Password and PIN susceptibility to compromise are different. It appears that in addition to a significant drop in the instances of compromise, there is significant increase in user's confidence that their PIN was not compromised.

Table 4 - Research Hypothesis 1/2 Chi-Sq Analysis

Question Asked (M - Martinson; A - Alsop)	Chi-Sq Analysis					
Chi-Sq Analysis	Cat.	O(n)	Hist(n)	Hist(%)	E(n)	Chi-Sq
Have you ever changed your Password(M)/PIN(A) so that it is easier to remember?	Yes	78	232	68.6	214.8	87.2
	No	233	102	30.2	94.5	203.2
n=313 ; Chi-Sq = 291.2; P-Value = 0.000	DK	2	4	1.2	3.7	0.8
Has your Password(M)/PIN(A) ever been compromised	Yes	1	18	5.3	16.7	14.7
	No	294	235	69.5	217.6	26.8
n=313 ; Chi-Sq = 88.4; P-Value = 0.000	DK	18	85	25.1	78.7	46.8
Do you use the same Password(M)/PIN(A) for multiple applications	Yes	80	325	96.4	301.9	163.06
	No	233	12	3.6	11.1	4416.12
n=313 ; Chi-Sq = 4579.18; P-Value = 0.000						
In the last year, have you written down your Passwords(M)/PINs(A)?	Yes	67	241	71.3	223.2	109.3
	No	246	97	28.7	89.8	271.5
n=313 ; Chi-Sq = 380.8; P-Value = 0.000						
In the last year, have you shared a Password(M)/PIN(A) with friends, family, co-workers, or others?	Yes	26	132	39.1	282.4	232.7
	No	697	206	60.9	440.6	149.1
n=723;n*=2;Chi-Sq=381.9;P-Value = 0.000						
In the last year, have you shared (CAC+PIN)/Password with friends, family, co-workers, or others?	Yes	4	132	39.1	282.4	274.4
	No	719	206	60.9	440.6	175.8
n=723;n*=2;Chi-Sq=450.2;P-Value = 0.000						
How many Passwords(M)/PINs(A) are you currently using?	0-4	294	67	21.3	154.1	127.1
	5:10	307	171	54.5	393.2	18.9
n=722;n*=3;Chi-Sq=162.5;P-Value = 0.000	10+	121	76	24.2	174.8	16.5

Cat. = Category/Response to question
O(n) = Observed (Alsop's Results)
Hist = Historical (Martinson's Results)
E(n) = Expected in O(n) based on Hist (%)
DK = Don't Know

In response to the question, "Do you use the same PIN/Password for multiple applications?" The hypotheses are:

- H_o: Reuse of PIN(s) and Password(s) are the same
- H_a: Reuse of PIN(s) and Password(s) different

The proportion of users answering 'Yes' to this question dropped from 96.2 percent to 25.6 percent (Table 3). It appears that users are much less likely to reuse a PIN

as they are to reuse a password. This trend enhances the security of the network by reducing the vulnerability of a user's PIN being compromised through a successful attack on a different network or system. Utilizing the chi-square analysis (Table 4), we get a chi-square of 4579.2 and a p-value of 0.000. We must reject the null hypothesis and conclude that the proportion of users that reuse PIN(s) and the proportion of users that reuse password(s) are different.

In response to the question, "In the last year, have you written down your PIN(s)/Password(s)?" The hypotheses are:

- H_o: The proportion of users writing down their PIN is the same as the proportion of users writing down their password
- H_a: The proportion of users writing down their PIN is different than the proportion of users writing down their password

The proportion of users answering 'Yes' to this question dropped from 71.3 percent to 21.4 percent (Table 3). It appears that users are much less inclined to write down a PIN, as they are to write down a password. This enhances the security of the network by reducing the vulnerability of a user's PIN being compromised through observation or inadvertent discovery. Utilizing the chi-square analysis (Table 4), we get a chi-square of 380.8 and a p-value of 0.000. We must reject the null hypothesis and conclude that the proportion of users writing down their PIN(s) is different from the proportion of users writing down their password.

In response to the question, "In the last year, have you shared a PIN/Password with friends, family, co-workers, or others?" The hypotheses are:

- H_o: The proportion of users sharing their PIN is the same as the proportion of users sharing their password
- H_a: The proportion of users sharing their PIN is different than the proportion of users sharing their password

The proportion of users answering 'Yes' to this question dropped from 39.1 percent to 3.6 percent (Table 3). It appears that users are much less inclined to share their PIN as they were in sharing their password. This could be related to the fact that in order for a user's PIN to be useful, they would also have to share their CAC, leaving the user without the ability to access the base and base services. Utilizing the chi-square analysis (Table 4), we get a chi-square of 381.9 and a p-value of 0.000. We must reject the null hypothesis and conclude that the proportion of users sharing their PIN is significantly different from the proportion of users sharing their password. Since a user would also have to lend out their CAC with their PIN in order to grant someone unauthorized access to Air Force networks, we also performed this analysis for users that shared their CAC and their PIN. In this instance, only four respondents stated that they had shared their CAC and their PIN. Utilizing the chi-square analysis based on this data (Table 4), we get a chi-square of 450.2 and a p-value of 0.000 on the hypothesis that users are likely to share their network account independent of the authentication technique used. In this case, we reject the null hypothesis and conclude that the likelihood of users sharing their network account is dependent on the authentication technique of the network. In this case, the CAC and PIN authentication technique is significantly less prone to the account sharing than the logon ID and password network authentication.

In response to the question, "How many PINs/Passwords are you currently using?" The hypotheses are:

- H_o: The number of PINs that a user must recall is the same as the number of passwords that they must recall
- H_a: The number of PINs that a user must recall is different from the number of passwords that they must recall

The data shows that the number of PINs that respondents say they use is less than the number of passwords that they were using. We see an increase in the "1-4" category from 19.8 percent of users to 40.6 percent. This corresponds to the decreases in the "5-10" category and the "10+" category. With a higher proportion of users having to remember fewer PINs, users are going to be less inclined to write them down. Utilizing the chi-square analysis (Table 4), we get a chi-square of 162.5 and a p-value of 0.000. We must reject the null hypothesis and conclude that the number of PINs that a user must recall is different from the number of passwords that they must recall.

Research Hypothesis Three

Survey questions 10 and 23-25 of this research pertained specifically to the third hypothesis, "Individuals will be more likely to adhere to policy guidance under the new authentication method as compared to password authentication" We will analyze this hypothesis with a direct comparison of the survey results between Martinson's research and ours (Table 5). For questions 10 and 23-25, the independent variable (e.g. the authentication technique) is nominal (or categorical) as are the dependent variables (see Table 5). We will use a Chi-Square Goodness-of-Fit test to analyze each of the related questions and whether or not the results are significant around $\alpha = .05$.

In response to the question, "Do you feel that the CAC and PIN network authentication procedures and parameters are a nuisance?" The hypotheses are:

- H_o: The proportion of users that consider network authentication a nuisance is independent of the authentication technique
- H_a: The proportion of users that consider network authentication a nuisance is dependent on the authentication technique

The proportion of users answering 'Yes' to this question dropped from 62.1 percent to 34.2 percent (Table 5). Before analyzing the data using the Chi-Square Goodness-of-fit test, we realized there was a distinct different between the answers "No Opinion" and "Don't Know." When Martinson asked this question, the possible answers were "Yes", "No", and "Don't Know". When we asked this question, our possible answers were "Yes", "No", and "No Opinion". Because of the contextual difference of these answers, we decided to treat all answers in categories of "Don't Know" for Martinson's research and "No Opinion" for our research as null responses and did not use them to compute the Chi-Square. Utilizing the chi-square analysis (Table 6), we get a chi-square of 187.5 and a p-value of 0.000. We must reject the null hypothesis and conclude that the proportion of users that consider the new CAC and PIN authentication method a nuisance is significantly less than the proportion of users that considered password based network authentication parameters and procedures a nuisance.

In response to the question, "Do you feel the PIN policies (creation and use) are burdensome?" The hypotheses are:

- H_o: The proportion of users that consider PIN policies a burden is the same as the proportion of users that consider password policies a burden
- H_a: The proportion of users that consider PIN policies a burden is different then the proportion of users that consider password policies a burden

The proportion of users answering 'Yes' to this question dropped from 50.9 percent to 32.3 percent (Table 5). Before analyzing the data using the Chi-Square Goodness-of-fit test, we realized there was a distinct different between the answers "No Opinion" and "Don't Know." When Martinson asked this question, the possible answers were "Yes", "No", and "Don't Know". When we asked this question, our possible

answers were “Yes”, “No”, and “No Opinion”. Because of the contextual difference of these answers, we decided to treat all answers in categories of “Don’t Know” for Martinson’s research and “No Opinion” for our research as null responses and did not use them to compute the Chi-Square. Utilizing the chi-square analysis (Table 6), we get a chi-square of 88.4 and a p-value of 0.000. We must reject the null hypothesis and conclude that the proportion of users that consider PIN policies a burden is significantly less than the proportion of users that consider password policies a burden.

Table 5 - Research Hypothesis 3 Raw Data Analysis

Question Asked (M - Martinson; A - Alsop)	Question Number	Response					
		Yes	No	NO/DK	*		
Do you feel that the Password(M)/CAC & PIN(A) procedures & parameters are a nuisance?	M-Q10	62.1	36.7	0.9	0.3		
	A-Q10	**34.2**	**57.7**	7.6	0.6		
Do you feel the Password(M)/PIN(A) policies are burdensome?	M-Q14	50.9	44.4	3.3	1.5		
	A-Q24	**32.3**	**57.2**	10.2	0.3		
		Yes	No	Some	Unsure	*	
Do you follow the Password(M)/CAC & PIN(A) procedures based on organizational guidance?	M-Q13	84	4.4	8.9	2.1	0.5	
	A-Q25	**81.8**	**2.2**	4.1	11.4	0.4	
		O	G	A	NI	P	N/A *
How would you characterize your organization's training and education relating to the creation of Passwords(M)/PINs and the use of the CAC card for network authentication(A)?	M-Q12	7.7	31.7	45	8.6	5	2.1
	A-Q23	7.9	30.5	44.4	10.2	6.5	0.6
NO - No Opinion; DK - Don't Know; * - No Response							
O - Outstanding; G - Good; A - Adequate; NI - Needs Improvement; P - Poor							

In response to the question, “Do you follow CAC/PIN procedures based on organizational guidance?” The hypotheses are:

- H_o: The proportion of users that follow CAC/PIN procedures based on organizational guidance is the same as the proportion of users that follow password procedures based on organizational guidance
- H_a: The proportion of users that follow CAC/PIN procedures based on organizational guidance is different from the proportion of users that follow password procedures based on organizational guidance

Table 6 - Research Hypothesis 3 Chi-Sq Analysis

Question Asked (M - Martinson; A - Alsop)	Chi-Sq Analysis					
Question/Chi-Sq Analysis	**Cat.**	**O(n)**	**Hist**	**Hist %**	**E(n)**	**Chi-Sq**
Do you feel that the Password(M)/CAC & PIN(A) procedures & parameters are a nuisance?	**Yes**	248	210	62.3	449.3	117.90
	No	418	124	36.8	265.3	69.60
n=666 ; n*=59; Chi-Sq=187.5 ; P-Value = 0.000	**DK**					
Do you feel the Password(M)/PIN(A) policies are burdensome?	**Yes**	234	172	53.4	346.7	36.62
	No	415	150	46.6	302.3	41.99
n=649 ; n*=76 ; Chi-Sq = 88.4 ; P-Value = 0.000	**DK**					
Do you follow the Password(M)/CAC & PIN(A) procedures based on organizational guidance?	**Yes**	593	284	84.5	610.3	0.49
	No	16	15	4.5	32.2	8.18
	Some	30	30	8.9	64.5	18.43
n=722 ; n*=3 ; Chi-Sq = 334.124 ; P-Value = 0.000	**NS/DK**	83	7	2.1	15.0	307.04
How would you characterize your organization's training and education relating to the creation of Passwords(M)/PINs and the use of the CAC card for network authentication(A)?	**O**	57	26	7.9	56.6	0.00
	G	221	107	32.3	233.1	0.63
	A	322	152	45.9	331.1	0.25
	NI	74	29	8.8	63.2	1.86
n=721;n*=4;Chi-Sq = 5.42; P-Value = 0.247	**P**	47	17	5.1	37.0	2.68

Cat. = Category/Response to question; O(n) = Observed (Alsop's Results); Hist = Historical (Martinson's Results)
E(n) = Expected in O(n) based on Hist (%); DK = Don't Know
O - Outstanding; G - Good; A - Adequate; NI - Needs Improvement; P - Poor

The proportion of users answering 'Yes' to this question dropped from 84 percent to 81.8 percent (Table 5), those answering "No" dropped from 4.4 percent to 2.2 percent, and those answering "Sometimes" dropped from 8.9 percent to 4.1 percent. The most significant change was the increase in the number of users that are unsure about whether they are following their organization's guidance. Those answering "Don't Know" or "Not Sure" increased from 2.1 percent to 11.4 percent. This change contributed the most to the chi-square score. Utilizing the chi-square analysis (Table 6), we get a chi-square of 334.1 and a p-value of 0.000. We must reject the null hypothesis and conclude that the

proportion of users that follow CAC/PIN procedures based on organizational guidance is significantly different from the proportion of users that follow password procedures based on organizational guidance.

In response to the question, "How would you characterize your organization's training and education relating to the creation of PINs and the use of the CAC card for network authentication?" The hypotheses are:

- H_o: Organizational training and education relating to the creation of PINs and the use of the CAC is the same as organizational training and education relating to the creation of passwords.
- H_a: Organizational training and education relating to the creation of PINs and the use of the CAC is different from organizational training and education relating to the creation of passwords.

In analyzing the results (Table 5), it appears that there is little difference in the organizational training and education between the creation of passwords and the creation and use of PINs and CACs. Utilizing the chi-square analysis (Table 6), we get a chi-square of 5.42 and a p-value of 0.247. We cannot reject the null hypothesis that organizational training and education relating to the creation of PINs and the use of the CAC is the same as organizational training and education relating to the creation of passwords.

Research Hypothesis Four

Survey questions 12-15, and 17-20 of this research pertained specifically to the fourth hypothesis, "The new authentication technique will contribute to a loss in worker productivity and smart cards." We analyzed this hypothesis by evaluating the respondent's answers to two questions. One that pertained specifically to the issue of users leaving their CAC behind in a card reader and another question that determined

CAC loss or theft attributed to the new authentication technique. While we have no data about previous CAC loss or theft prior to the implementation of the mandatory CAC and PIN authentication method, we do know that there were few requirements in which users had to take their CAC out of their wallet or purse except for identification. We used the number of CACs that were identified as lost and or stolen that were not attributed to the new CAC and PIN authentication system as a baseline in order to determine the relative increase in lost or stolen CACs as a result of the new authentication technique.

Chi-Square Goodness-of-Fit Test for Observed Counts in Variable: Q13 vs Q12

Left CAC Behind	Must Leave CAC in Card Reader YES	NO	Test Proportion	Expected	Contribution to Chi-Sq
YES	412	32	0.64	399.36	0.400064
NO	212	18	0.36	224.64	0.711225

N	DF	Chi-Sq	P-Value
624	1	1.11129	0.292

Figure 42 - CAC in reader vs. CAC left behind

An interesting side note is that whether the user is required to leave their CAC in the card reader while on the network appeared to have no effect on whether they left their CAC behind in the computer or not (Figure 42). Based on the results of this chi-square analysis, whether the user has to leave their CAC in the card reader in order maintain access to the network will have little impact on whether the user forgets to take their CAC with them when they leave.

To predict the number of CACs left behind based on a population of 491,786 military and civilian members (AFPC 2006), we used regression analysis to determine a 95 percent prediction interval and a fitted value. This regression model gave us 841,539 +/- 43,149 CACs left behind during a six month period (figure 43).

Table 7 - Research Hypothesis 4 Raw Data Analysis

Question Asked	Question Number	Response						
		n	Yes	No	Some	*		
With the new CAC/PIN authentication, do you have to leave your CAC in the card reader while accessing the network?	**A-Q12**	*725*	86.1	6.9	6.8	0.3		
In the last 6 month, have you inadvertently left your CAC behind in the computer?	**A-Q13**	*725*	66.8	33	n/a	0		
			1	**2**	**3**	**4**	**5+**	*
In the last 6 months, how many times have you left your CAC at work, in the computer?	**A-Q14**	*484*	21.9	31	20	7.6	19	0.6
			G	**M**	**S**	**NAA**	*	
How much did the new CAC/PIN authentication technique contribute to this?	**A-Q15**	*484*	69.4	10	9.1	11.2	0.2	
			Yes	**No**	*			
Since implementation of the CAC and PIN to authenticate on the network, has your CAC been lost, stolen, or misplaced?	**A-Q17**	*725*	6.1	94	0			
			1	**2**	**3**	**4**	**5+**	*
How many times has your CAC been lost, stolen, or misplaced?	**A-Q18**	*44*	77.3	14	4.5	0	2.3	2.3
			G	**M**	**S**	**NAA**	*	
How much did the new CAC/PIN authentication technique contribute to loss, theft, or misplacement?	**A-Q19**	*44*	27.3	11	2.3	56.8	2.3	

* = No Response/Null; G = Greatly; M = Moderately; S = Slightly; NAA = Not At All; A - Alsop Survey

Regression Analysis: CACsLeftBehind versus N

```
The regression equation is
CACsLeftBehind = 6.9 + 1.71 N

Predictor      Coef  SE Coef      T      P
Constant       6.93    10.98   0.63  0.548
N           1.71118  0.08775  19.50  0.000

S = 25.2238   R-Sq = 98.2%   R-Sq(adj) = 97.9%

New
Obs       N
  1  491786

Predicted Values for New Observations
Obs        Fit    SE Fit          95% CI                  95% PI
  1  841539.02  43148.64  (739508.69, 943569.35)  (739508.67, 943569.37)XX

XX denotes a point that is an extreme outlier in the predictors.
```

Figure 43 - CACs Left Behind for Air Force Active Duty Mil/Civ

Using the fitted value of 841,539 instances in which users left their CAC behind, unsecured at a computer workstation during a six-month period, we extrapolated the value for a one-year period to be 1,683,078. Building on that number to determine how much productive time was lost from the mission gives us the following equation:

CACs left behind in 1 year		1,683,078.00
Q16:User having problems accessing base	x	62.03%
Lost work time (user and helper) per incident in minutes	x	30
Total lost work time per year (in minutes)		31,320,398.50
Total lost work time convert to work years		**261.00**

Figure 44 - Time lost in one year due to CAC leave behinds

Here we have incorporated the results of question 16, "When you left your CAC at work, did it cause you problems in accessing the base or base services?" Additionally, we determined the lost time per incident, 30 minutes total. We assume a loss of 15 minutes for the person attempting to access the base, and 15 minutes for the co-worker that has to go to the base entrance to either return their CAC or sign them onto the base. The results show that we lose the equivalent of 261 work years, per year, to grant individuals access to the base due to the new CAC and PIN authentication technique. If the average salary for personnel were 40,000 dollars a year, this would equate to 10.44 million payroll dollars a year spent on individuals to wait at the gate and signing people onto the base.

Additionally, there were several incidents where the CAC was lost or stolen due to this new authentication technique. The results of question 19, "How much did the new CAC/PIN authentication technique contribute to loss, theft, or misplacement?", showed that 40.91 percent of the CACs that were lost or stolen in the last 6 months were the result of the new CAC and PIN authentication technique. Using the number of CACs

that were lost or stolen and were not attributed to the new authentication technique (58 percent) as the baseline, shows us an increase of 72 percent. To predict the number of CACs lost or stolen based on a population of 491,786 military and civilian members (AFPC 2006), we used regression analysis to determine a 95 percent prediction interval and a fitted value. The regression model (figure 45) gives us 14,111 +/- 2,132 CACs that were lost or stolen in the last 6 months due specifically to the new CAC and PIN authentication technique.

Regression Analysis: CACsStolenLost versus N

```
The regression equation is
CACsStolenLost = 0.578 + 0.0287 N

Predictor      Coef   SE Coef     T      P
Constant     0.5776    0.5428  1.06  0.323
N          0.028692  0.004336  6.62  0.000

S = 1.24637   R-Sq = 86.2%   R-Sq(adj) = 84.2%

New
Obs       N
  1  491786

Predicted Values for New Observations

New
Obs        Fit    SE Fit          95% CI                 95% PI
  1  14110.656  2132.083  (9069.081, 19152.231)  (9069.080, 19152.232)XX

XX denotes a point that is an extreme outlier in the predictors.
```

Figure 45 - CAC lost or stolen in last 6 months

This also incurs a cost in regards to time lost from accomplishing the mission. Using the fitted value of 14,111 instances in which users had their CAC lost or stolen during a six-month period, we extrapolated the value for a one-year period to be 28,222. Building on that number to determine how much productive time was lost from the mission gives us the following equation (Figure 46):

CACs stolen/lost due to CAC/PIN in 1 year		28,222.00
Lost work time per incident in minutes	x	60
Total lost work time per year (in minutes)		1,693,320.00
Total lost work time convert to work years		**14.11**

Figure 46- Time lost in one year due to CAC loss/theft

For lost time per incident, we have assumed a value of 60 minutes total for an individual to go to the military personnel flight and replace their CAC. This is a generous estimate as it assumes that the individual does not have to wait, nor does it include the time that the personnel specialist has to spend creating the new card. The results show that we lose the equivalent of 14.11 work years, per year, to replace lost or stolen CACs due to the new CAC and PIN authentication technique. If the average salary for personnel were 40,000 dollars a year, this would equate to 564,400 payroll dollars a year spent on individuals just to replace their CAC card because theirs was lost or stolen due to the new authentication technique.

Research Hypothesis Five

Survey questions 21, 22, and 26 of this research pertained specifically to the fifth hypothesis, "Accessibility of the networks will decline as individuals find it more difficult to perform job tasks away from the primary workplace (i.e. TDY, Leave) due to the requirement of having a token to authenticate." In Table 8 and Figure 47, you can see that users that must use a CAC reader to access their email accounts from remote locations find the ease of remote access more difficult than those who are not required to use a CAC reader. In Table 8, we broke out the responses for questions 22 and 26 from those individuals that must use a CAC reader remotely. To analyze the significance of

the difference, we utilized the Kruskal-Wallis H-Test for question 22 and the Chi-Square Goodness of Fit test for question 26.

Table 8 -Research Hypothesis 5 Raw Data Analysis

Question Asked	Question Number	Response						
		n	Yes	No	DK	*		
To access your work email account remotely (e.g. Home, TDY, In Transit), do you have to use a CAC reader?	Q21	*725*	42.9	28.6	27.9	0.7		
			VD	SD	NC	LE	ME	*
Since implementation of the CAC/PIN authentication, how would you rate the ease of accessing the network remotely (All responses)	Q22	*725*	40.3	17.1	23.2	7.2	7	5.2
Since implementation of the CAC/PIN authentication, how would you rate the ease of accessing the network remotely (CAC required for remote access)	Q22	*311*	58.2	19.3	12.5	5.5	3.5	1
Since implementation of the CAC/PIN authentication, how would you rate the ease of accessing the network remotely (CAC not required for remote access)	Q22	*207*	33.8	16.4	29.5	8.7	9.2	2.4
			Yes	No	Some	*		
Do you feel that using the CAC and PIN authentication method is burdensome? (All Responses)	Q26	*725*	37.1	42.8	19.7	0.4		
Do you feel that using the CAC and PIN authentication method is burdensome? (CAC required for remote access)	Q26	*311*	44.1	33.4	22.2	0.3		
Do you feel that using the CAC and PIN authentication method is burdensome? (CAC not required for remote access)	Q26	*207*	34.3	46.9	18.4	0.5		
VD = Very Difficult; SD = Slightly More Difficult; NC = No Change; LE = Little Easier; ME = Much Easier								

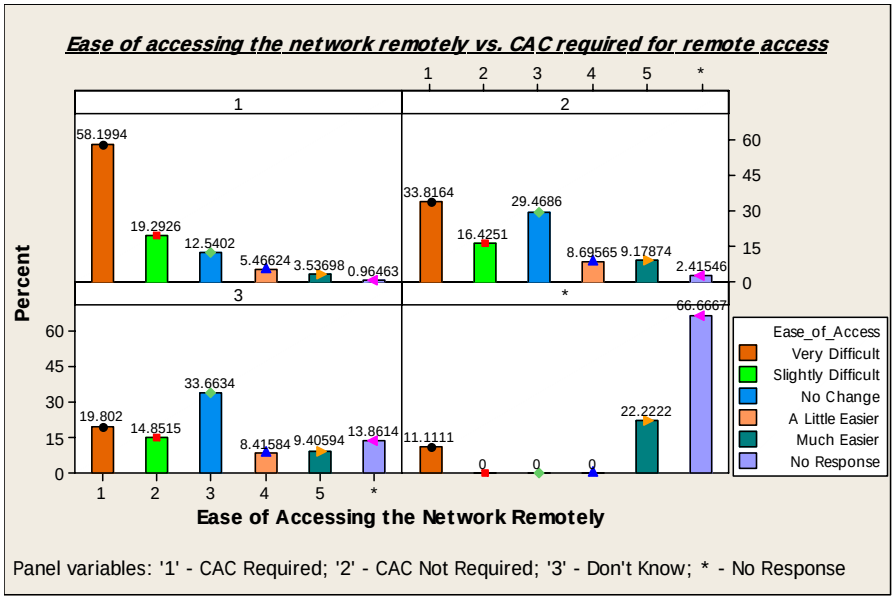

Figure 47 – Ease of Remote Email Access

For the question, “Since implementation of the CAC/PIN authentication, how would you rate the ease of accessing the network remotely?” the hypotheses for Kruskal-Wallis H-test are:

- H_o: The population probability distributions between users that have to use a CAC remotely, those who do not, and those who don’t know, is identical
- H_a: At least two of the 3 probability distributions are different

Kruskal-Wallis Test: Q22 versus Q21

```
684 cases were used
45 cases contained missing values


Kruskal-Wallis Test on Q22:How Would You Rate the Ease of Accessing The Network Remote
Possible Values for Question 22:
  1 - Very Difficult
  2 - Slightly More Difficult
  3 - No Change
  4 - A Little Easier
  5 - Much Easier

CAC Req.   N  Median  Ave Rank      Z
"Yes"    308       1     275.1  -8.07
"No"     202       2     377.3   2.98
"Unsure" 174       3     421.3   6.09
Overall  684             342.5

H = 69.78  DF = 2  P = 0.000
H = 77.41  DF = 2  P = 0.000  (adjusted for ties)
```

Figure 48 - Kruskal-Wallis Test of “Ease of Use” vs. CAC Required

By looking at the median answer for question 22, “Since implementation of the CAC/PIN authentication, how would you rate the ease of accessing the network remotely?” in regards to each response for question 21, “To access you work email account remotely, do you have to use a CAC reader?” We see that those who answered ‘Yes’ to having a CAC required for remote access had a median answer of ‘Very Difficult’ regarding the ease of accessing the network remotely. This contrasts with those who do not need their CAC for remote access, who had a median answer of “Slightly

More Difficult". The H-statistic for this analysis is 77.41 and the p-value is 0.000. We must reject the null hypothesis and conclude that the two of the three probability distributions are different. In this case, it is apparent that users that can only access the email remotely via the use of a CAC reader find this new authentication technique to be significantly more difficult than those who do not have to use the CAC reader.

In response to the question, "Do you feel that using the CAC and PIN authentication method is burdensome?" I wanted to analyze the results based on the respondents answer to question 21, "To access you work email account remotely, do you have to use a CAC reader?" The hypotheses for this test are:

- H_o: The burden felt by the users from the CAC and PIN authentication method is independent of whether they need a CAC reader to access their email remotely
- H_a: The burden felt by the users from the CAC and PIN authentication method is dependent of whether they need a CAC reader to access their email remotely

It appears from the data in figure 49, that there is a trend in which users that require a CAC to access their email account remotely (Figure 49: Panel 1), consider the new CAC and PIN authentication method more burdensome than users that do not require a CAC. This is consistent with our analysis of question 22 (Figure 47). Utilizing the chi-square analysis (Figure 50), we get a chi-square of 23 and a p-value of 0.000. With the $\alpha = .05$, we must reject the null hypothesis and conclude that the burden felt by the users from the CAC and PIN authentication method is dependent of whether they need a CAC reader to access their email remotely.

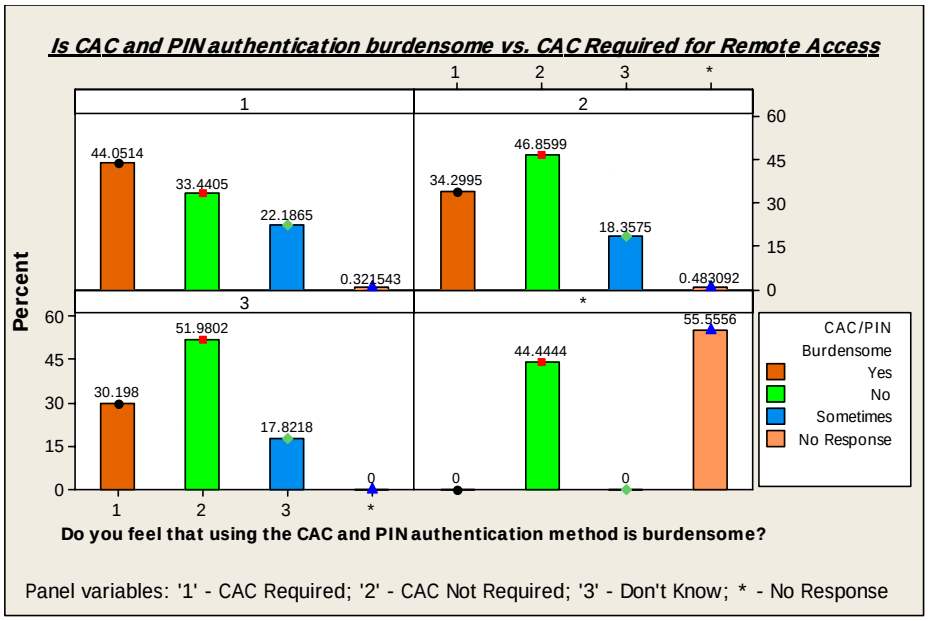

Figure 49 - CAC / PIN burden due to remote access ability

Chi-Square Goodness-of-Fit Test for Observed Counts in Variable: C2

Using category names in
"Is CAC/PIN A Burden"

Is CAC/PIN A Burden?	CAC Required For Remote Access	CAC Not Required For Remote Access	Test Proportion	Expected	Contribution to Chi-Sq
Yes	137	71	0.344660	106.845	8.5109
No	104	97	0.470874	145.971	12.0678
Don't Know	69	38	0.184466	57.184	2.4413

N	DF	Chi-Sq	P-Value
310	2	23.0201	0.000

Figure 50 - Chi-Square Analysis Q26 vs. Q21

Chapter Overview

In this chapter, we analyzed the data collected and compared applicable questions directly to the results of Martinson's research. We reviewed the responses for each survey question in detail and then we analyzed each of the research hypotheses, directly comparing our results against the results of Martinson's research, where appropriate, with statistical analysis tests.

V. Discussion, Conclusions and Recommendations

In this chapter, we discuss our conclusions, recommendations, and suggestions for future research. I will step through each of the research hypotheses and the respective data analysis that supports them to draw their overarching conclusion.

Conclusions

In chapter one, I proposed five hypotheses for this research. The first two were:

1) The implementation of a two-factor authentication technique will increase the effectiveness of network authentication as related to human factors.
2) The vulnerabilities that affect a strictly password based authentication method will not have an effect on the PIN portion of a two-factor authentication method?

In analyzing the data related to the first and second hypotheses, we had (Table 3; Table 4) the following key findings:

- (RH 1/2) Users were less likely to change their PIN to familiar pattern
- (RH 1) The PIN has not been compromised as often as the password
- (RH 1/2) Users do not recycle their PIN as often as they recycle passwords
- (RH 1/2) Users do not write down their PIN as often as they write down passwords
- (RH 1/2) Users do not share their CAC or their PIN nearly as often was the case for passwords in the password based authentication method (Martinson 2005)
- (RH 1/2) The number of PINs that users must recall is less than the number of passwords that users had to recall

Based on these results, we conclude that the vulnerabilities that affect the password based authentication systems (sharing, recycling, recall burden, and writing them down) are significantly reduced in the PIN portion. In addition, the complexity of a

PIN is significantly less than that for a password. A PIN is typically composed of a series of six to eight numbers (i.e. ten character set vs. a passwords 96 character set) and does not have to be changed at regular intervals. Due to the reduced vulnerabilities identified in the data supporting the second hypothesis, the reduced complexity of PINs, and the observation that PINs have not been compromised as often as passwords, we conclude that the two-factor authentication technique implemented by the DoD will increase the effectiveness of network authentication as it relates to human factors.

The third hypothesis in this study was:

3) Individuals will be more likely to adhere to policy guidance under the new authentication method as compared to password authentication

In analyzing the data related to this hypothesis, we had (Table 5; Table 6) the following key findings:

- The CAC and PIN authentication technique is less of a nuisance than the logon ID and password technique
- PIN (creation and use) policies are less burdensome than the password parameters of the logon ID and password technique
- While the number of users that follow CAC and PIN procedures is consistent with the number of users that followed password procedures, the number of users that are unsure about whether they follow organizational guidance has increased significantly.
- Training and education for the CAC and PIN authentication method is similar to that of the logon ID and password authentication technique.

Based on these results, we conclude that the two-factor authentication technique implemented by the DoD will increase user adherence to policy guidance based on the construct that if users believe the technique to be less of a ‘nuisance’ or ‘burden’, then they will be less likely to develop a technique that circumvents policy and guidance. There is some concern about the number of users that are unsure about whether they are

following policy. This could be because the CAC and PIN authentication method has only been mandatory for the sample population for approximately six months when the survey had been given. In contrast, the logon ID and password authentication technique had been in place for many years when Martinson did his research.

The fourth hypothesis in this study was:

4) The new authentication technique will contribute to a loss in worker productivity and smart cards.

In analyzing the data related to this hypothesis, we had (Table 7; Figures 42-46) the following key findings:

- 67 percent of users left their CAC behind in the reader in the last 6 months
  - Approximately 841,539 unattended CACs in the last 6 months
  - 261 work-years per year in lost productivity (approx $10.4M)
- 6 percent of users had their CAC lost or stolen in the last 6 months
  - 41 percent of users attributed theft/loss to new CAC authentication
    i. 72 percent increase in lost/stolen CACs
    ii. 28,222 more CACs lost or stolen each year
    iii. 14.11 work-years per year in lost productivity ($564K)
- Requiring the CAC to be in the card reader to maintain network access to has little impact on whether the user leaves their CAC behind

Based on these results, we concluded that the use of a CAC and PIN authentication technique as implemented by the DoD has contributed to a loss in worker productivity and an increase in the loss or theft of CACs due to the increased insecure handling of the CAC.

The fifth hypothesis in this study was:

5) Accessibility of the networks will decline as individuals find it more difficult to perform job tasks away from the primary workplace (i.e. TDY, Leave) due to the requirement of having a token to authenticate.

In analyzing the data related to this hypothesis, we had (Table 8; Figures 47-50) the following key findings:

- Users that are required to use the CAC in order to access their email remotely find it significantly more difficult and burdensome than those who are not required to use the CAC

Based on these results, in addition to the results of question 27, where 35.5 percent of respondents stated that accessing email remotely is more difficult, we conclude that the network accessibility while away from their primary workplace has declined significantly due to the increased level of difficulty of getting access. This was also a topic of concern in the comment sections of questions 27, 34, and 36. Most users find that the inability to access their email from locations other than their primary workplace significantly hampers their ability to do their job and be responsive. After closing the survey, I was still getting emails from users that wanted to participate. As an example, one of these requests was from the officer in charge (OIC) of a reserve unit that stated, "The introduction of the CAC card for home use has decimated the communications channels that our reserve unit has spent years developing. We are now looking at going back to paper bulletins with stamps." This was their primary method of disseminating information and maintaining recall information for all the reservists in the unit. Due to the loss of ubiquitous remote email access capability, due to the requirement for a CAC, their normal communication capabilities were severely hampered.

Additional Findings

Based on user responses, we found that leaving behind the CAC contributes to more than just the physical security threat of lost or stolen CACs, it also has consequences in regards to lost productivity. The number of CACs that were left behind

also had an effect on respondent's ability to access the base or base services. We found this contributed to a loss of 261 work years, per year, in lost productivity. This figure does not include the additional 14 years of lost productivity in cases where users had to take time out of work to replace their CAC. Combined these losses contribute to a total of 11 million payroll dollars spent on individuals going to and from the gate and waiting at the personnel flight.

Another finding of this research was an apparent interest, and in some cases a plea, for a move towards an authentication system that utilizes the fingerprint, a biometric, as opposed to the logon ID and password and the CAC and PIN techniques. This was clear by the response to question 32 and the comments on questions 35 and 36. Most of the reasoning behind this trend is the hope to reduce the number of times that people are unable to do their job or access the base because they left their CAC at home or they left their CAC at work, in the computer. If they left their CAC at home, they found that they could not access the base network unless they returned home to retrieve it. If they left their CAC at work, they had to have someone (i.e. coworker) come to the gate to either bring them their CAC or grant them access to the base. By moving to an authentication system that relies on who the person "is", a biometric, rather than what they "have", you eliminate any issues regarding network access when they do not "have" the required item.

The new CAC and PIN authentication technique is also causing concerns in regards to personal information. Respondents were concerned about leaving their CACs unattended during short errands around the office. The slow logon times due to CAC certificate validation is apparently contributing to this trend as users find it inherently

frustrating waiting to log back on, so instead they just leave their CAC in the reader. In other instances, due to fast-paced work environments, they just forget to take their CAC with them on short errands. The fact that their name, Social Security Number, and date of birth are easily accessible on the CAC poses privacy concerns, especially with the increase in identity theft in recent years. While the majority of individuals that have access to military bases and facilities have some type of clearance, there are exceptions, such as contracted cleaning and maintenance staff. Additionally, while any compromised CACs are unlikely to allow an unauthorized user access to the DoD networks, they could potentially be used to gain access to the base by unauthorized personnel.

Another issue that is causing concerns is the apparent inconsistencies of applying a common standard for accessing email remotely under the new CAC and PIN authentication technique. Some users responded that their bases had not implemented any remote email access capability, regardless of whether they had a CAC reader. Other locations have implemented remote access with a CAC reader, but have not issued users CAC readers, thus putting the onus on the user to buy a reader so that they can be more productive for the USAF. In contrast, other users, 29 percent of respondents, stated that they had access to their email remotely just using a logon ID and password. One thing is clear; denying users the ability to access to their email accounts remotely has caused a significant amount of frustration and reduced their ability to respond promptly.

Another issue addressed by more than a few respondents was the inability of the CAC and PIN authentication system to serve unique operational requirements. While most users on the network sit in one location and work on one computer. Many situations require users to operate multiple workstations at once. As such, requiring users

to logon with their CAC causes significant usability hardships. Another unique environment issue involved local foreign nationals. Apparently issuing these users a CAC in order for them to do their job runs into problems when trying to get host nation approval to issue a CAC for their citizens. Apparently, according to the responses, some host nations have reservations with the data (e.g. privacy act, biometric) that is needed for the CAC validation and issuance.

Recommendations

While the CAC and PIN authentication method has increased the effectiveness of network authentication and user's adherence to policy guidance, the implementation of the technique has also caused serious problems in regards to usability, productivity, and CAC loss.

The usability of the system in regards to accessibility to work email accounts, especially from remote locations such as home or while TDY has encountered serious setbacks. Implementing CAC remote access and issuing card readers for remote use to those that need it, perhaps through a virtual private connection, could maintain the same level of security while allowing the users more flexibility in using the system to accomplish the mission. Additionally, allowing users located temporarily, TDY or deployed, at other federal installations, should be able to access their home base domain, if at least, just for email purposes. The remote locations typically are equipped with computer and card reader necessary for certificate validation. We should be able to allow Microsoft Outlook Web Access (OWA) via CAC and PIN authorization at these locations. Accessing these remote computers that are not part of our normal domain should be as easy as validating the certificate on our CAC and granting the user "Guest"

access. We could even load the CAC with the date of our last information assurance training.

A simple way to resolve several other burdens placed upon users would be to allow all users to logon to a computer using their CAC via RFID. This is analogous to showing our CAC at the gate to gain access. We take the CAC out (perhaps on a lanyard), logon to the network, and then return the CAC to where it came from. We never have to place the card into the computer and wait. This way we maintain increased authentication security to the network in addition to allowing the user to keep their primary form of identification secure and on their person. The will eliminate the problem of cards left behind in the card reader and the associated burdens thrust on the user due to forgetfulness, such as the embarrassing call to a coworker to come to the gate and "escort" them onto the base. It would also reduce the amount of wear and tear caused by card readers and subsequent replacement that the CAC is currently subjected too. Additionally, this would allow users, such as network technicians, to logon to more than one computer at a time without having to resort to methods that would circumvent security (i.e. have an exception to CAC and PIN authentication such as a logon ID and password).

Until we allow everyone to move away from leaving the CAC in the reader while logged on scenario, respondents suggested several ways to reduce the problems associated with leaving the CAC behind. They suggestions are; using keyboards with attached CAC readers, having computers emit a warning during logout if the CAC is still in the reader, and posting signs by all the exits reminding users to remember to take their CAC with them before they leave.

Another possibility would be to transition our authentication technique to a biometric based system. This would serve the same purpose and garner the same benefits as a CAC logon scheme that utilized RFID. Additional benefits would come from untangling network access to a token that we constantly have to carry with us, and serves as a roadblock to access if we lose it. Of course, if we did not provide fingerprint readers for remote access, we would still have the same problems with usability. Perhaps issuing the fingerprint reader, via hand receipt, similar to the way we issue laptops, would allow users to access to their accounts from those remote sites. What would the cost of this endeavor be? Looking online, I found that smart card readers and fingerprint readers to be approximately the same costs, 40 dollars. In order to provide a universal serial bus (USB) fingerprint reader, at a cost of approximately 40 dollars each, to 491,786 military and civilian members of the USAF, the cost would be about 20 million dollars. Compared to the approximately 10.4 million dollars a year in lost productivity, this could be recouped in two years. Of course, I am comparing apples and oranges here. Payroll dollars are going to be paid whether we implement this technology or not, whereas the money for fingerprint readers will have to come from a budget somewhere. But in light of the recent force shaping initiatives, we should be looking at ways to eliminate as much wasted productive time as possible. Additionally, wouldn't it be a good idea to eliminate the increased vulnerability to our primary form of identification sooner rather than later.

Just standardizing email access via the CAC and PIN through a virtual private connection, and issuing CAC readers, would solve many problems in regards to allowing people remote access to their accounts. The results of the survey show this to be one of

the biggest frustrations that users have with the CAC and PIN authentication method. It seems that we have regressed 10 years in our communications ability in this regard.

Suggestions for Further Study

This study addressed the changes in authentication security measures when moving from a logon ID and password based system to a CAC and PIN based mechanism as they relate to usage and policy. Additionally, this research has shown some of the usability issues that occur when moving from a purely knowledge based authentication method to one that requires additional hardware (i.e. card reader and CAC). Before implementing further changes in the authentication procedures, studies should be done in order to determine their affects on all users of the system. Considerations that do not address unique requirements tend to leave some users with fewer capabilities than previously attained. This loss could affect productivity and in some cases, severely hamper the business processes.

Additionally, because this survey was taken only six months after mandatory implementation of the CAC and PIN authentication method, we cannot be certain it reflects the steady state. A possible future study could administer this survey again to determine if the results are different after the "growing pains' of implementation are worked out.

Another potential topic could look at the incorporation of additional authentication measures. Technologies that are already included in the CAC are contactless interfaces (RFID) and biometric data (i.e. fingerprint). The fingerprint data stored on CACs is already being used to authenticate the user during CAC replacement. An analysis on whether moving to a three-factor based authentication system, to include a

discussion on implementing remote access on such a system, would address the perceived increased security while also ensuring that such an implementation would reduce the negative effects on productivity and network access. Future research could also look at how the lack of remote access via the CAC and PIN authentication technique has affected productivity of users in different job classifications.

Chapter Overview

In this chapter, we reviewed each of the five hypotheses and our findings from the research. We found that the two-factor authentication technique does increase the level of security of the network and that users will be more likely to adhere to policy guidance under the CAC and PIN authentication method as opposed to the logon ID and password based system. We also showed that The new authentication technique will contribute to a loss in worker productivity and smart cards as users are made to remove and leave their CAC unsecured while they are logged on to the network. We also showed that remote access to critical communications has been severely hampered by the requirement to use a CAC to authenticate from those remote locations. Finally, we highlighted some additional issues that were revealed during our research, made recommendations on how to rectify some of the most pressing problems, and suggested future areas in which to research.

Last Word

For the DoD, the CAC was supposed to replace all other tools that performed standard identification, physical access, and logical access to DoD installations and networks. The implementation of the CAC and PIN authentication method for network access has increased security, but at the cost of availability of the network and

productivity of the user. There are plans to incorporate using the CAC for finance, medical and dental readiness, deployment readiness, and training. Before this is undertaken, it would be in the best interest of the USAF to analyze exactly 'how' the CAC is going to be used in order to reduce further vulnerabilities to loss, theft, damage, or misplacement. While having a single tool such as a CAC to access all these systems and services can make our lives easier, all considerations should be given to ensuring that users have it secured at all times. Any item with this much power represents a potential single point of failure and losing or misplacing it can seriously disrupt the capability and productivity of the owner.

Appendix A: Definition of Terms and Acronyms

AFCA – Air Force Communications Agency

CAC – Common Access Card (a.k.a. Smart Card)

CAD – Card Accepting Device

CPU – Central Processing Unit

DEPSECDEF – Deputy Secretary of Defense

DMC – Defense Management Council

DoD – Department of Defense

EEPROM – Electrically Erasable Programmable Read Only Memory

EPROM – Erasable Programmable Read Only Memory

FIPS – Federal Information Processing Standards

HSPD – Homeland Security Policy Directive

ICC – Integrated Circuit Card

IRM – Information Resource Management

PIN – Personal Identification Number

PKI – Public Key Infrastructure

PIV – Personal Identification Verification

PC – Personal Computer

ROM – Read Only Memory

RAM – Random Access Memory

TDY – Temporary Duty

USAF – United States Air Force

Appendix B: Alsop Survey Instrument

The following information is provided as required by the Privacy Act of 1974:

Purpose: To gather information relating to how respondents adhere to policy and guidance relating to the use of personal identification numbers (PINs) and smart cards.

Routine Use: The results of this study will help to determine whether or not the new authentication methods being implemented by the Air Force will increase the security of their network resources.

Analysis of individual responses will be conducted, and only members of the Air Force Institute of Technology research team (Dr. Strouble, Dr. Hermann, Dr. Heminger and Maj. A. Scot Alsop) will have access to the raw data.

Participation: Participation is voluntary. No adverse action will be taken against any member who does not participate in this survey or who does not complete any part of the survey. All data gathered will be completely confidential and no attempt to identify respondents will take place. No raw data will be seen by those in your chain of command.

Instructions

1. Base your answers on your own experiences.
2. Verify you have selected the correct answer before moving on as there is no ability to go back and change it.
3. Any identifying information gathered will only be used to identify trends within subsets of the population. It will NOT be used to identify individuals and their responses.

Contact Information: If you have any questions about this request, please contact Dr. Dennis Strouble (Primary Investigator) – Phone (937) 785-3355 x3323; Email – dennis.strouble@afit.edu or Maj. A. Scot Alsop (Graduate Student) – Phone (617) 308-7653; Email – aalsop@afit.edu.

Common Access Card (CAC) and Personal Identification Number (PIN) Usage
Please take a couple of minutes to fill out this short survey. All information will be kept strictly confidential and will not be seen by chain of command in its raw form. Thank you for your participation.

1. Do you use a Common Access Card (CAC, aka Military ID) and Personal Identification Number (PIN) to access the network at work?
    a. Yes
    b. No
2. Were you issued a PIN, or did you pick your PIN yourself?
    a. Issued PIN
    b. Picked my own PIN
3. Have you ever changed your PIN so that it is easier to remember?
    a. Yes
    b. No
    c. Don't Know
4. Has your PIN ever been compromised?
    a. Yes
    b. No
    c. Don't Know
5. Do you use the same PIN for multiple applications? Example: ATM card, Online accounts, Credit Cards
    a. Yes
    b. No
6. In the last year, have you written down your PIN(s)?
    a. Yes
    b. No
7. In the last year, have you shared a PIN with friends, family, co-workers, or others?
    a. Yes
    b. No
8. Do you use a familiar date, age, SSN, sequence (i.e. 1234), telephone number, street address, or pattern to remember your PIN?
    a. Yes
    b. No
9. What "Technique" do you use? Do NOT write down your PIN.

    _____

10. Do you feel that the CAC and PIN network authentication procedures and parameters are a nuisance?
    a. Yes
    b. No
    c. No Opinion
11. How many PINs (in addition to the one for your CAC) are you currently using?
    a. 0-4
    b. 3-4
    c. 5-6

d. 7-8
e. 9-10
f. 10+

CAC Usage/Control

12. With the new CAC/PIN authentication, do you have to leave your CAC in the card reader while accessing the network?
    a. Yes
    b. No
    c. Sometimes
13. In the last 6 months, have you inadvertently left your CAC behind in the computer?
    a. Yes
    b. No
14. In the last 6 months, how many times have you left your CAC at work, in the computer? (If NO, you will be automatically skipped to question 17 upon submission)
    a. 1
    b. 2 times
    c. 3 times
    d. 4 times
    e. 5 or more times
15. In reference to the previous question (# of times you left your CAC at work), how much did the new CAC/PIN authentication technique contribute to this?
    a. Greatly
    b. Moderately
    c. Slightly
    d. Not at all
16. When you left your CAC at work, did it cause you problems in accessing the base or base services?
    a. Yes
    b. No
17. Since implementation of the CAC and PIN to authenticate on the network, has your CAC been lost, stolen, or misplaced? (If NO, you will be automatically skipped to question 20 upon submission)
    a. Yes
    b. No
18. In reference to the previous question (17.has your CAC been lost, stolen, etc.), how many times has your CAC been lost, stolen, or misplaced?
    a. Never
    b. 1
    c. 2
    d. 3
    e. 4
    f. 5+

19. In reference to the previous question (17. number of times CAC was lost, stolen, etc.), how much did the new CAC/PIN authentication technique contribute to the loss, theft, or misplacement?
    a. Greatly
    b. Moderately
    c. Slightly
    d. Not at all

20. In the last year, have you let someone (Co-worker, Friend) borrow your CAC?
    a. Yes
    b. No
21. To access your work email account remotely (e.g. Home, TDY, In Transit), do you have to use a CAC reader?
    a. Yes
    b. No
    c. Don't Know
22. Since implementation of the CAC/PIN authentication, how would you rate the ease of accessing the network remotely?
    a. Very Difficult
    b. Slightly More Difficult
    c. No Change
    d. A Little Easier
    e. Much Easier

CAC and PIN Guidance

23. How would you characterize your organization's training and education relating to the creation of PINs and the use of the CAC card for network authentication?
    a. Outstanding
    b. Good
    c. Adequate
    d. Needs Improvement
    e. Poor
24. Do you feel the PIN policies (creation and use) are burdensome?
    a. Yes
    b. No
    c. No Opinion
25. Do you follow CAC/PIN procedures based on organizational guidance?
    a. Yes
    b. No
    c. Sometimes
    d. Not Sure

26. Do you feel that using the CAC and PIN authentication method is burdensome?
    a. Yes
    b. No
    c. Sometimes
27. If you think it is burdensome, why? (Select all that apply)
    a. I don't think it is burdensome
    b. Have to get CAC from wallet, purse, etc.
    c. If I forget or lose my CAC, I can't access the network to do my job
    d. Accessing my email remotely is more difficult
    e. Small errands in the office require taking the CAC with me.
    f. I'm always forgetting to take the CAC card out of the card reader.
    g. Other (If "other" please explain:_____

Additional Feedback

28. Do you believe the previous method of securing network access (logon ID and Password) was a sufficient means of ensuring network security?
    a. Yes
    b. No
29. Do you believe that using a CAC to logon to the network is more secure than logon ID and password?
    a. Yes
    b. No
30. Do you believe using the CAC to logon to the network is: (choose one):
    a. An inconvenience
    b. A necessary security evolutionary requirement
31. Do you believe that network access conveniences take priority over security?
    a. Yes
    b. No
32. If you had a choice of methods to gain access to the network, which would you prefer?
    a. Login ID/Password
    b. CAC/PIN
    c. Fingerprint
    d. Hand Geometry/PIN
    e. Iris Scan
    f. Other (If "Other", please explain)_____
    g. No Opinion
33. Would you prefer a separate card (similar to CAC, but not for ID) specifically for network authentication?
    a. Yes
    b. No
    c. No Opinion

34. What do you think could increase usability/accessibility of the CAC/PIN method without sacrificing security?
    a. _____
       _____
35. What do you think could increase security without sacrificing usability?
    a. _____
       _____
36. Please share any additional comments
    a. _____
       _____

Personal Information

(Only AFIT research team will see any of the raw data)

37. What is your age?
    a. Under 20
    b. 21-30
    c. 31-40
    d. 41-50
    e. 51-60
    f. 61+
38. What is your gender
    a. Male
    b. Female
39. Job or Occupation
    a. Military Officer
    b. Military Enlisted
    c. Civilian
    d. Contractor
40. Is your job now or was your job ever in the computer or network security industry?
    a. Yes
    b. No
    c. Don’t Know

Appendix C: Martinson's Survey Instrument

The following information is provided as required by the Privacy Act of 1974:

Purpose: The purpose of this study is to gather information on how respondents choose, remember and use passwords.

Routine Use: The results of this study will help to determine if individuals are using similar patterns or memory techniques when choosing passwords.

Analysis of individual responses will be conducted and only members of the Air Force Institute of Technology research team will be permitted access to the raw data.

Participation: Participation is VOLUNTARY. No adverse action will be taken against any member who does not participate in this survey or who does not complete any part of the survey.

Instructions

- Base your answers on your own thoughts & experiences
- Please make your answers clear and concise when asked to answer in a response or when providing comments
- Be sure to select the correct option button when asked because when you move on you cannot come back

Contact information: If you have any questions about this request, please contact Dr. Dennis Strouble (Primary Investigator) – Phone (937) 785-3355 x3323; E-mail – dennis.strouble@afit.edu or Lt Kurt Martinson (Graduate Student) - Phone (937) 429-3404; E-mail – kurt.martinson@afit.edu.

Start Survey

Notice and Consent Banner:
Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

Password Choice

Please take a few minutes to fill out this survey on password usage. We welcome your feedback, and your answers will be kept confidential. Thank you for your participation.

General Information

1. Do you use passwords?

○ Yes ○ No ○ N/A

2. Has your password ever been compromised?

○ Yes ○ No ○ Don't Know

3. Do you use recycle or use similar passwords for different applications? Example: Personal E-mail, Work E-mail, Online Banking, Online Ordering, etc.

○ Yes ○ No

4. In the last year, have you written down a password?

○ Yes ○ No

5. In the last year, have you ever shared a password with friends, family, co-workers or others?

○ Yes ○ No

Password Choice

6. How do you remember your password(s)?

○ Names, Places, ○ Keyboard Pattern ○ Sports Reference ○ Certain letters in a familiar sentence ○ Other (please explain below)

7. Please share your memory technique. DO NOT write down your password.

_____

_____

_____

8. Have you ever voluntarily changed a password so that it is easier to remember?

○	○	○
Yes	No	Don't Know

9. Are there any negative consequences to not changing passwords regularly?

○	○	○
Yes	No	Don't Know

10. Do you feel that password procedures and parameters are a nuisance?

○	○	○
Yes	No	Don't Know

11. How many passwords are you currently remembering/using?

○	○	○	○
0 to 4	5 to 10	11 to 20	Over 20

Password Guidance

Many organizations have a password policy. For example, users must create passwords that are upper/lower case, contain symbols and words not found in the dictionary. Based on this, please answer the following.

12. How would characterize your organization's training and education relating to the creation of passwords?

○	○	○	○	○	○
Outstanding	Good	Adequate	Needs improvement	Poor	N/A

13. Do you follow the password procedures based on organizational guidance?

○	○	○	○
Yes	No	Sometimes	Don't Know

14. Do you feel the password policies of your organization are burdensome?

○	○	○
Yes	No	Don't Know

Additional Feedback

15. Please write down any <u>old</u> passwords that you have used but <u>are not</u> using today. The purpose is to determine if individuals are using similar patters or characteristics.

_____

_____

16. Please share any additional comments.

_____

_____

Personal Information

17. What is your age?

○	○	○	○	○	○
Under 20	21-30	31-40	41-50	51-60	Over 60

18. What is your gender?

○	○
Male	Female

19. Job or Organization?

○	○
Military Officer	Military Enlisted

20. Is your job now or was your job ever in the computer or network security industry?

○	○	○
Yes	No	Don't Know

Thank you for taking the time to fill out our survey. Your input is greatly appreciated.

Appendix D: Survey Comment Data

Quest. 8	*Question 9*
1	#'s I remember due to personal history
1	4-digit PIN I have used often; with added four numbers for variation.
1	A Birthday of someone I know.
1	A combination of a street address (not mine) and another number.
1	a combination of familiar dates and sequence
1	A combination of my birthday.
1	A combination of numbers that I can remember.
1	a combination of parts of old telephone numbers and important dates
1	A combination of some of the items mentioned above.
1	a date
1	A date easy to remember
1	A date for a child's birthday (scrambled).
1	a familiar date
1	A familiar sequence since I have 15+ passwords to remember (not including PINS/passwords for personal use)
1	a friends birthdate.
1	A jumbled combination of important dates though none of them are my personal info: birthdays, anniversaries, etc.
1	a mix of address numbers
1	A number sequence. Thats the only way I can remember it. I have to remember about twenty password between my job and home use.
1	a number used for something else
1	A numeric version of a madeup word that amuses me.
1	a pattern
1	a portion of a family member's SSN
1	a series of favorite numbers
1	a series of repeating numbers
1	A set of numbers that have no meaning no very familiar to me.
1	A special date and time of a personal event
1	A variation on my wife's birthday.
1	Acronym from telephone dial buttons
1	Added additional numbers to a date familiar to me.
1	ADDRESS
1	Ages and initials of family members
1	Alsop Test
1	An old address from my home of record.
1	An old military ID #
1	an old phone number
1	An old phone number that no one else would know.
1	An old phone number, pre-service.

1	An order of preference for a sequential series of familiar numbers. i.e. Say for example Fruits: Apple, Nectarine, Orange, Pear. Alphabetically they are A, N, O, P. But I like (for example) Nectarines first, then Pear, then Apple, then Orange. So if A, N, O, P correspond to 1,2,3,4 then my preference is 2,4,1,3 which would be a PIN 2413. Kinda complex but it works for me.
1	anniversaries
1	Base the PIN off familiar number sequences significant in my life.
1	Based on a personal experience
1	Birth dates
1	birth year month, date
1	birthdate
1	birthdate of child
1	birthdates
1	Birthday
1	birthday
1	Birthday of an historical figure.
1	birthday, using #'s for day, month, year, of sibling
1	brith dates of members
1	Can't say without giving it away.
1	certain digits from mine and spouses SSNs
1	child's dob
1	Codes (letters to numbers)
1	combination names and ages
1	Combination of a few previous street addresses
1	combination of familiar numbers
1	combination of famillar dates in a certain sequence
1	Combination of family member's birthdays
1	Combination of numbers using an old zip code as part of the pin
1	Combination of personal numbers
1	Convert one of may childrens names to digits using a telephone key pad.
1	date
1	date
1	date
1	date
1	date
1	date
1	date
1	Date
1	Date Combination
1	Date of an event
1	date of birth of a special family member, not my own
1	dates
1	Dates
1	Dates I remember or even sometimes a random number that I have already memorized
1	Daughter Birthdays
1	daughters dob
1	Depending on the work location, used something directly related to the work area to remind me of the pin.

1	Digits are added, or subtracted, at multiple place holding positions in a familiar and easily remembered number sequence.
1	Dog's birthdate.
1	Don't feel comfortable answering this question.
1	don't understand the question
1	Drivers license number
1	Easy date to remember
1	exact same basic PIN and change the special character(s) at front, moving left to right on the qwerty keyboard.
1	familiar date
1	familiar date
1	familiar date
1	Familiar date
1	familiar date
1	familiar date
1	familiar date
1	familiar date
1	familiar date
1	familiar date
1	familiar date (scrambled)
1	Familiar date, in an uncommon order (not the usual YYYY/MM/DD format) Also combinations of Licence plates, VINs and telephone #'s and AFSC's
1	familiar date/pattern
1	Familiar number
1	Familiar number sequence
1	Famillliar date
1	Family member birth date
1	family member's birthday
1	FAMILY MEMBERS PHONE #
1	For my pin I use something that has meaning to me.
1	For this PIN I selected the numeric day each of my three family members were born.
1	For us "Old farts," a perfect pin was no problem. We once had service numbers before we went to the SSAN!
1	former street addresses
1	High school mascot and jersey numbers from football and basketball; first and only pin I have ever used with all my accounts requiring a PIN
1	I associate an application with an old number that I used to use frequently enough that I can still recall it without much extra effort
1	I currently use a combination of old addresses. Previously, I used a friends old telephone number.
1	I end up with whatever I can get the system to take.
1	I have a password / pin formula (different for each) that is known only to me. I pick a "seed" word or number sequence that is familiar to me (e.g., old license number, scout troop number) and transform it through the formula. The result is a password / pin that meets requirements. Occasionally, I will change the formula. Neither formula nor "seed" is ever written down.
1	I have a system.
1	I have an interest in history, I currently use the dates and places of events from the 14th and 15th century to derive my PINs.
1	i just know it
1	I just remember where i met my wife, how many kids i have and my grandmother's birthday.

1	I listed all of the house numbers I have ever lived at in my entire life, in a certain order.
1	I randomly pick area codes that i know and put them together in a particular sequence that only I know
1	I remember phone numbers more from the pattern they make on the keypad, rather than the actual numbers, so I used the same thought and picked a pattern on the number pad.
1	I use a combination of an old phone number and street address.
1	I use a combination of frequently used other pins.
1	I use a combination of numbers that easily come to mind due to a hobby I have.
1	I use a fairly distant relative's birthday for my CAC PIN. Use other sequences for personal accounts.
1	I use a number I had on my high school ID
1	I use a pin number that I frequently use in everyday life so that its easy to remember.
1	I use a street address I haven't lived at for 10 years; then, add unrelated numbers.
1	I use family birthdate combinations.
1	I use family members' dates of birth, like father, sister, etc.
1	I use my cell phone # all mixed around.
1	I use phone numbers that are familiar to me but not directly associated with me (e.g., friends' phone numbers).
1	I use the date of when my husband and i met.
1	I use the sail number of my recreational sailboat
1	I used the cell phone number of another person that I would not forget.
1	I used the Gregory-Newton Formula of Interpolation to compute a value--of some personal significance--from a common logarithm of exponential and hyperbolic functions and substituted a number for the decimal in the log cos 10
1	I would rather not say.
1	If I told you, you'd know my pin!
1	I'm not telling you.
1	important dates
1	important dates
1	Info from my other personality.
1	initials+year
1	It is a significant date to me.
1	just a social i know
1	Keyboard pattern
1	keyboard pattern
1	Keyboard pattern
1	keyboard pattern in a shape that I can recall.
1	keypad on the right of the keyboard and put it in like i'm dialing a phone number.
1	Last 2 digits of my birth year plus the 4 digits of a year mentioned in a particular favorite song of mine.
1	last 4 from my childhood phone number
1	last 6 SSN
1	Last to First Familiar
1	Math Functions
1	Memory
1	multiple, sometimes patterned sequence to correlate tele pad words (like texting)
1	My birth year, my husband's birth year, year of our wedding are used as the basis of the CAC PIN. However, the numbers are adjusted so that they are not employed in a way that is obvious and easily detected.
1	My college dorm address plus the room number
1	My old street address number.

1	No Comment
1	NONE
1	None of your business or one of the above from number 8
1	NUMBEERS BACKWARDS
1	Number not associated with me, but one that I'm unlikely to forget.
1	numbers
1	numbers from a phone number that a family member once had for 50 years
1	Numbers from SSan
1	Numbers I can remember
1	Numbers in a pattern (related to my anniversary date)...
1	numbers of birthdays in my family
1	numbers of previous units
1	Numerical sequence
1	Numerical Sequence
1	obsolete addresses, phone numbers, etc.
1	Old family secret
1	Old High School Football Number to start and finish PIN
1	OLD PHONE
1	Old phone number, no longer in use.
1	OLD STREET ADDRESS
1	Old telephone number
1	old telephone number
1	Old telephone number and year
1	One that I can easily remember. I have 21 diferent pins for AF use; that is ridiculious.
1	Parents phone number
1	Part alteration of my birth date and part keyboard pattern.
1	Part of an obscure phone number.
1	Parts of old telephone numbers
1	past event in my life
1	Past squadrons I have been assigned to.
1	pattern
1	Pattern
1	pattern
1	pattern on keypad
1	Pattern on numbered key pad.
1	PERSONAL NUMBER
1	Personal references condensed into either some form of abbreviations, or acronyms that are easily remembered.
1	ph #
1	PHONE
1	Phone
1	PHONE
1	phone #
1	phone #
1	Phone # from old assignment
1	PHONE FRIEND
1	phone number
1	phone number

1	phone number
1	phone number
1	phone number
1	Phone number for loved one.
1	portion of SSN
1	prefix of two different phone #'s
1	Random scrambled addresses
1	Ref question 8. I have a number that is meaningful to me but does NOT contain date, age, SSN... My "method" is a compilation of unrelated information but again, I've been able to personalize.
1	relative birthdays
1	religious significance
1	Repeat home address twice
1	repeat numbers
1	repetetive motion
1	same 4 number punched in two times
1	Sequence
1	Sequence
1	Sequence of special events.
1	Sequence/pattern of numbers that I am familier with.
1	Sequence/repeating numbers
1	significant date
1	significant date
1	SIGNIFICANT NUMBER AND DATE
1	Significant year groupings from events in my life that would not be obvious to someone who does know my methodology
1	Significant years, but not a single date
1	similarity with other pin
1	Since CAC pin is 8 digits I use a combination of to other 4 digit pins that I use frequently.
1	slip my age in there and my initials
1	something familiar to both my husband and myself; not SSN, phone, or DOB
1	something I can remember.
1	something that is an important date in my life.
1	Something unique in everyday use to remember the pin...due the other numerous passwords we ain the Air Force have to have for CBT sites & everything else!
1	Spatial Pattern
1	Sports dates of significance
1	SSN
1	SSN
1	ssn, atm pin numbers, debit card numbers
1	street address
1	Street Address
1	Symmetry, repetition
1	take a date familiar to me and re-arrange the alpha-numerical order
1	TELE
1	telephone
1	TELEPHONE #
1	telephone number
1	telephone number

1	Telephone number
1	telephone number
1	telephone number
1	Telephone number from when I was a young child growing up.
1	Telephone number of someone from the phonebook
1	Telephone number pad based pattern.
1	the birthdate of a family member
1	the combination of the first bicycle lock I ever owned
1	the day of the month of the birth of myself, my spouse, and one of my daughters
1	The numerical date of my wife's birthday.
1	The year I graduated from College, the squadron I was in, and my last 4
1	unused phone numbers or addresses
1	Use a GPS coordinate technique
1	Use familiar numbers.
1	used number combinations familiar to me but not easily traceable to me.
1	variation of SSN
1	Variety of SSN numbers.
1	Very old telephone number
1	wedding anniversary date, child birthday etc.
1	wedding date
1	With the requirement here to have multiple passwords for nirpnet, siprnet, JWICS and CAC cards - you need to develop a system to remember the sequence. Most folks just change the last letter - or right it down somewhere to remember the number.
1	With trying to remember so many different PINs, I try to keep them simple so I wont forget.
1	year of birthdays of family members
1	Years of birth of certain people.
1	Zip Code + repeat last digit
2	?
2	8 character pattern +2 digits, characters or special characters
2	A combination of dates that marked significant events during my military career
2	a combination of familiar numbers from different sources
2	A common number to me entered twice.
2	A date that is meaningful to me but is unknown to others; in no records or files
2	A mix of family bithdates.
2	A number from way back in my past
2	a number i will remember
2	a number relating to a memorable date
2	A numercial sequence that is significant to me so it will be easy to remember.
2	A pattern that I move around the keyboard each time I must change my PIN.
2	A random combination of numbers
2	A series of numbers easy for me to remember
2	A series of numbers that form a pattern.
2	a series of numbers that i remember
2	A series of numbers that I remember, not related to SSN, b-day or any identifying information
2	a significant date
2	a significant number that relates to a familiar event in my life
2	a special sequence of my favorite 2-digit number

2	A variety of numbers
2	Acromym converted to digital sequence
2	Add a number to the front and back of an existing PIN.
2	an account number
2	An easily rememberde series
2	an old telephone number (4 numbers) from an assignment many years ago and a couple more random digits
2	an random bunch of numbers I memorized.
2	Another memorable number
2	Any combination of numbers which I'll remember but not address, phone number or SSN..those are to easy to break
2	association - number "couples" mean something to me personally; a part of a specific date that is sentimental in nature
2	Association of time/dates of my own personal experience.
2	Based on familiar (to me) information from my past.
2	b-day
2	birth years of persons I know
2	Birthday of relative.
2	Boy Scout troop
2	change last two numbers, if we weren't required to change every 60 days,then we would have to write them down. I could understand if it was compromised. When you have several different accounts with different pins, how in the crap do you remember them without writing them down.
2	Childhood friends/pets
2	classified!
2	Close my eyes and pick numbers or letters on my keyboard and if it is aceptable I memorize it.
2	combination of birth dates of 2 of my 4 children.
2	combination of college student id number
2	combination of dates
2	Combination of easy numbers for me which add up to nothing
2	combination of important dates
2	Combination of old zip codes, phone numbers, and a personal number that I use. Again, all very old - just nmbers that come back to me easily.
2	Combination of previously assigned unit designations.
2	Combination of significant personal numbers.
2	Combination of things that will be easy for me to remember, yet comply with 9 alpha-numeric/character requirement.
2	Combination of two numbers that I know well that together equal the minimum number of characters
2	combinations of unrelated birth months and years from different family members
2	Combine number patterns that have meaning for me but are NOT related to any personal info such as SSN, address, phone etc
2	Combined numbers of squadrons that I've known since high school. Some are real world, others are fictional.
2	Committed to memory
2	Concatenation of some remembered prime(s and yy or 100-yy or yyyy or 10000-yyyy for some memorable year(s)} in a remembered permutation of these items.
2	Convert an important word to me + numbers into a pin
2	created group of familiar numbers
2	dates
2	Devise an eight to nine word sentence and use the first letter of each word. Always use one word that represents each a number and special character to fullfill that requirement.

2	digits of interest
2	Do not write down CAC pin On other passwords save on travel drive. I have over 125 passwords
2	dont know
2	Don't recall using a technique or where I got the number...was something easy for me to remember.
2	easy
2	easy number to remember
2	Easy to remember
2	Easy to remember number combinations from my life.
2	Event dates and times
2	EXAMPLE: #1438JpQUI
2	Familiar number
2	familiar number with variation
2	familiar/favorite # sequence....ie size of car engine from teenage years
2	Famous sports figures.
2	Favorite words in a song.
2	First wife's day and year of birth (no month) combined with the last 4 of her SSAN. Comment on question 10: They are a necessary nuisance.
2	Former unit's numerical designations
2	friends b-day
2	ghtdr
2	have my own
2	I am using a passpharse method.
2	I CAN NOT TELL YOU
2	I can't remember numbers only finger positions on a key pad. It is a physical technique.
2	I chose numbers that have a specific meaning to me in relationship to sports.
2	I currently use a very important date in my life. It's something I will never forget therefore, I don't ever have to write it down.
2	I derive a number from familiar numbers, being careful to not make an obvious pattern. The same goes for more complex PINs to include upper and lower case keys.
2	I do not have a "technique" other than building one that is not obvious.
2	I don't have a technique...
2	I don't remember how I came up with the number, to be honest.
2	I duplicated a familiar 4 digit number used when I was in high school.
2	I easily remeber numbers and use the last 4 digits of the telephone numbers from 2 two of my friends from middle school.
2	I have a portion of a very old phone number that I use only for my CAC pin.
2	I have a sequence that I can identify with easily
2	I have numbers that hold significance but are not related to dates
2	I just remember some Numbers.
2	I just used a random technique, based on keyboard layout to facilitate ease of typing in the PIN
2	I occassionaly spell out a word on a phone and use the corresponding numbers.
2	i picked random numbers out of a hat until i had a pin
2	I rather keep this to myself
2	I relate the numbers to the musical tones on the phone and I link the "tone" PIN to songs I like
2	I strongly believe you should not ask this ?
2	I tend to use a combination of significant dates.
2	I think of it as a internal clock.

2	I think of things I would only know that I experienced and was too ashamed to let anyone know.
2	I use #'s that are easy for me to remember.
2	I use 2 meaningful dates, no birthdays, anniversaries, etc.
2	I use a combination of two different numbers that are familiar to me.
2	I use a favorite number, a favorite date along with random numbers and letters as required by whatever program requires
2	I use a strong password and convert it to the PIN using the telephone pad letter to numbers format.
2	I use a technique of the current event happen in my life right now.
2	I use all the number down the middle of the keypad.
2	I use an anniversary date.
2	I use an old phone extension from my house that I grew up in. It is no longer associated with my family. I repeat the 4 numbers twice.
2	I use my favorite numbers that have no relation to telephone, street or birthdate.
2	I use something important to me, makes it easier to remember.
2	i use the current rules but in a combination that is meaningful to me
2	I use the last 6 digits of a very old overseas telephone number.
2	I use the one potato... two potato method...
2	I use the same PIN which I use for banking.
2	I used a random set of numbers and commited them to memory. I have to use this pin many times per day so its was not hard to commit it to memeory.
2	IAW Air Force instructions
2	important date
2	Important dates (not birthday, anniversary, etc) something obscure to me only
2	Important family dates.
2	Important occurance in personal life
2	important personal date
2	initals converted to numbers twice
2	Initials of family members and the year I graduated. Just things that are easy to remember
2	Is this a trick question? Please.....
2	It was an id number that I had from an airline job, that met all the requirements of a pin.
2	It'a variation of different dates.
2	It's a serial number for a machine
2	It's just a number I came up with about 10 years ago and now consider it to be "my number."
2	Jusr remember it.
2	Just a set of numbers that I have memorized as long as I use it on a regular basis
2	Just memory
2	just picked numbers.
2	Just simple, easy to remember pattern. But not easy enough for anyone to figure out, I hope.
2	keyboard sequence
2	last 4 of ex-husbands SSN plus mmyy of ex-anniversary
2	last four of my childhood phone number plus my lucky number.
2	Letter/number patterns from keyboard.
2	letters that I can convert to numbers in a logical manner
2	Linked to something only I'd know.
2	locker combination from highschool
2	Made up numbers, no sequence
2	Made up PIN.
2	Make up a phrase and use the first letter of the phrase.

2	Mathematical formula to generate the digits.
2	memoriable numbe
2	Memorization
2	memorization
2	memorization
2	Memorization.
2	Memorization.
2	memorization.
2	Memorize
2	Memorize it.
2	memory
2	Memory
2	memory
2	Memory
2	Memory
2	Memory of the past
2	Memory....if I don't hvae to change this every time I wake up, remembering it is easy
2	Military arms designations
2	mind over matter
2	Mix of important numbers
2	My favorite band's album title.
2	My line numbers for promtion to SMSgt and CMSgt.
2	My own.
2	My pin is related to a fond memory. So old no one would ever figure it out.
2	n/a
2	N/A
2	NAMES OF OLD PETS, SPORTS TEAMS, CARTOON CHARACTERS
2	No technique
2	no technique
2	no technique - thought of one and remember it....
2	No technique utilized.
2	No technique. I just memorized it.
2	No technique. I just used random numbers and memorized them.
2	Non sequential set of numbers and letters.
2	none
2	None
2	none
2	none
2	none
2	none - random
2	None of your business
2	None of your business.
2	None specific just make one up
2	None YA BUSINESS
2	none.
2	None...originated from Bank's pin numbering techniques. Something else to consider, my technique in the past has depended on the number pad being used. I've used a designs and patterns.

2	nonsence word
2	Not to tell anyone
2	Nothing special, other than using the same PIN for a long period of time, so I can do it in my sleep.
2	number associated with phone number letters
2	Number familarization
2	number pad strokes
2	Number pattern, but not sequential.
2	numbers and letters
2	numbers from jersey I wore in sports
2	Numbers similar to another password
2	Numbers that are siginificant to my family
2	Numbers that flow together easily in my mind and not consecutive numbers (e.g. 1,2,3,4)
2	numbers that I will remember
2	Numbers that mean something to me and would only be known by me.
2	Numbers which popped into my head.
2	obscure birthdays
2	Old ID # from high school
2	Old number that means something to me, but not to anyone else. i.e. not documented
2	Old PIN from a bank account closed 18 years ago.
2	old security code
2	one that is easy for me to remenmber
2	Part SSAN Part phone mixed up
2	pattern
2	pattern sequence of numbers on keypad
2	Personal only known to me
2	phone key alpha translation; pick a word association
2	pick whatever pops into my head at the time and hope I remember it.
2	Picked numbers that had personal meaning to me, followed by a year that had meaning also.
2	Picked the last four digits of an old work telephone number and added to other digits in front of it.
2	ramdom number, letters and special charactors
2	random
2	random
2	random
2	random
2	random
2	random
2	Random
2	Random
2	Random #s
2	random 7 numbers
2	Random character generator
2	random characters
2	random number
2	random number
2	random numbers
2	random numbers
2	random numbers

2	Random numbers
2	random numbers
2	Random numbers
2	Random numbers
2	Random numbers on a telephone keypad.
2	Random numbers selection
2	Random numbers.
2	random numbers...
2	random pick of numbers and letters
2	Random sequence
2	Random sequence of characters.
2	random sequence of numbers and alpha characters that are extracted from my immediate faimily members names, dates of birth and cell phone numbers.
2	random words and numbers
2	Random, progressive combination
2	randomly chose 7 numbers
2	randomly generated lotto numbers
2	Rember the PIN number
2	Right now it is part of my old phone number growing up, a long long time ago
2	scrabble tiles with reverse precedence starting at the letter Q. Random draw.
2	scrambled memorized numbers
2	sequence numbers
2	Sequence on the keypad I can remember.
2	Series of #'s and letters upper & lower case mixed around.
2	Set of common numbers I can easily remember. Lab #, notebook #, ect
2	several rows of the keyboard and use upper or lower case
2	Significant numbers to me
2	some numbers correspond to letters that are part of a word that means something to me and the remaining numbers are numbers that mean something to me
2	some thing from my past
2	Something easily remembered.
2	Something easy to remember
2	Something easy to remember
2	something for me to remember
2	something I easily remember and no one else can guess
2	something that I can remember easily
2	spell a word
2	Strictly thought out process.
2	That's personal
2	The calendar date I was drafted.
2	The name of a former pet converted to numbers via telephone number buttons. I set my own PIN the day I received my first CAC card and have used this same PIN only for my CAC since that time (2002).
2	Thing that are for me eazy to remember
2	This is not a question that should be asked. If I answer correctly you can obtain my PIN.
2	two credit card pin numbers pushed together
2	up and down
2	Use the same one for everything I can

2	Used a variation of a current pin that I've used for 20 years.
2	Utilize a number that has significance to me only.
2	Various
2	very old telephone number (last 4)
2	We have so many (red that as WAY TOO MANY) pins and passwords that I believe anyone who says they don't wite them down is less than honest.
2	Whatever comes to mind at the time I am selecting a new PIN
2	whatever is easiest for me to remember and meets system requirement

Bibliography

AFCA (2006). MAJCOM Network Tasking Order Status Report S. U. A. 06.ppt. Scott AFB, IL, Air Force Communications Agency.

AFPC (2006). Air Force Demographics Snapshot. A. F. P. Agency.

Anne Adams, M. A. S. (1999). "Users Are Not The Enemy." Association for Computing Machinery, Communications of the ACM **42**(12): 40-46.

Chadwick, D. (1999). "Smart Cards Aren't Always the Smart Choice " Computer **32**(12): 142-143.

Christina Braz, J.-M. R. (2006). Security and Usability: The Case of the User Authentication Methods. IHM. Montreal, Quebec, Canada, Association of Computing Machinery.

CompTIA (2002). Committing to Security: A CompTIA Analysis of IT Security and the Workforce. Oakbrook Terrace, IL (US), Computing Technology Industry Association.

CSD (2005). Personal Identity Verification (PIV) for Federal Employees and Contractors: Federal Information Processing Standards (FIPS) Publication 201. C. S. D. C. I. T. Laboratory, National Institute of Standards and Technology.

CSRC (2006). Personal Identity Verification (PIV) of Federal Employees / Contractors. C. S. D. C. S. R. C. (CSRC), National Institute of Standards and Technology.

David Sims, B. H. (1999). "Smart Cards and Biometrics: Your Key to PKI." Linux Journal(59).

DMDC (2005). HSPD-12 Implementation Plan. D. M. D. Center, Defense, Department of.

DMDC (2006). DoD Common Access Card (CAC) Issuance Policy. D. M. D. Center, Defense, Department of.

DoD (2000). New Identification Card Uses "Smart" Technology. o. Defense, US Department of Defense**:** 1.

DoD (2001). Department of Defense Common Access Card White Paper. D. o. Defense, Department of Defense.

DoD (2003). Department of Defense Common Access Card Fact Sheet. D. o. Defense, Department of Defense.

DoD/ACO (2000). DoD Smart Card Information Briefing. D. o. D. A. C. Office, Department of Defense.

DoD/ACO (2000). Security of the Common Access Card. D. o. D. A. C. Office, Department of Defense.

DoD/ASD (2002). DODD 8190.3 - Smart Card Technology. D. o. Defense, Department of Defense.

Gehringer, E. F. (2002). Choosing Passwords: Security and Human Factors. 2002 International Symposium on Technology and Society (ISTAS'02). Piscataway, NJ, USA.

Hafemeister, R. (6 Mar 2006). Smart Cards Become Key to Computer Access. Air Force Times**:** 12.

Jianxin Yan, A. B., Ross Anderson, Alasdair Grant (2000). The memorability and security of passwords - some empirical results. M. Kuhn. Cambridge, UK, University of Cambridge - Computer Laboratory**:** 11.

Katherine Shelfer, J. D. P. (2002). "Smart Card Evolution." Comminications of the ACM **45**(7): 83-88.

Keok Auyong, C.-L. C. (1997). "Authentication services for computer networks and electronic messaging systems." ACM SIGOPS Operating Systems Review **31**(3): 3-15.

LockDown (2006). Password Recovery Speeds-96. c. b. passwords, LockDown**:** Password Recovery Speeds of a 96 Character based password scheme.

Martinson, K. W. (2005). Passwords: A survey on Usage and Policy. Systems and Engineering Management, Air Force Institute of Technology. **Master of Information Resource Management:** 63.

Microsoft. (2006, 14 Jun 2006). "Strong Passwords: How to create and use them." from http://www.microsoft.com/athome/security/privacy/password.mspx.

Mitnick, W. L. S. K. D. (2002). The Art of Deception, Wiley Publishing, Inc., Indianapolis, Indiana.

Nelson, R. A. (1993). Smart Card Multiple Function. Security Technology Symposium. U. S. D. o. Energy. Virginia Beach, Virginia, U.S. Department of Energy.

Neumann, P. G. (1994). "Risks of Passwords." Association for Computing Machinery, Communications of the ACM **37**(4): 126.

NIPC, N. I. P. C. (2002). "Password Protection 101." National Infrastructure Protection Center Publications.

Philippe Proust, J.-P. T., Laurent Sourgen, Fabien Germain (2004). High Security Smart Cards. Design, Automation and Test in Europe Conference and Exhibition. Europe, IEEE.

Scheuermann, D. (2002). "The smartcard as a mobile security device." Electronics & Communication Engineering Journal: 205-210.

Schwab, D. P. (2005). Research Methods For Organizational Studies. Mahwah, New Jersey, Lawrence Erlbaum Associates, Inc.

Singh, K. (1985). "On improvements to password security." ACM SIGOPS Operation Systems Review **19**(1): 53-60.

SPO, A. P. (2006). Smart Card Logon is Coming to Your Network. A. F. P. K. I. S. P. Office, USAF.

Wakefield, R. L. (2004). "Network Security and Password Policies." The CPA Journal **LXXIV**(7).

White-House (2004). Homeland Security Presidential Directive/HSPD-12.

Vita

Major Alan Scott Alsop graduated from South Whidbey High School in Langley, Washington. He enlisted in the Air Force in March 1991. After graduating from Apprentice Communications-Computer Systems Programming Training, he went to work for the 1500 Computer System Group at Scott Air Force Base (AFB), Illinois. While at Scott AFB, Major Alsop competed for and won a Reserve Officer Training Corp scholarship that led him to Central Washington University in Ellensburg, Washington. Major Alsop graduated from Central Washington University, "Magna Cum Laude", with a Bachelor of Science degree in Computer Science in June 1996. Major Alsop was then assigned to the National Air Intelligence Center (NAIC) as a Project Manager and Analyst for the Information Systems Branch (SCDA) of NAIC. In June 1999, Major Alsop was assigned to the Electronic Systems Center at Hanscom AFB, Massachusetts. There he became the Chief of the Integration and Evaluation Branch where he was involved with cutting edge research and development technologies in the Common Operational Picture (COP) and Joint Battlespace Infosphere (JBI) programs. While assigned to ESC, he deployed to the Joint Task Force-Southwest Asia at Prince Sultan Air Base, Saudi Arabia. There he led the J6 Coalition Program Office. In June of 2002, Major Alsop was assigned to the 305th Communications Squadron, McGuire AFB, New Jersey. While there, he served as the Flight Commander for the Mission and Information Systems Flights. In August 2005, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
23-03-2007	Master's Thesis	Mar 2006 – Mar 2007

4. TITLE AND SUBTITLE

Beyond Passwords: Usage and Policy Transformation

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Alsop, Alan S., Maj, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 P Street, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/07-M1

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFCA/ECAI (Attn: Martin Solis, Maj, USAF)
203 West Losey St., Room 2000
Scott AFB, IL 62225-5222
DSN 779-5898
Email: Martin.Solis-02@scott.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The purpose of this research is to determine whether the transition to a two-factor authentication system is more secure than a system that relied only on what users "know" for authentication. While we found that factors that made passwords inherently vulnerable did not transfer to the PIN portion of a two-factor authentication system, we did find significant problems relating to usability, worker productivity, and the loss and theft of smart cards. The new authentication method has disrupted our ability to stay connected to ongoing mission issues, forced some installations to cut off remote access for their users and in one instance, caused a reserve unit to regress 10 years in their notification and recall procedures. The best-case scenario for lost productivity due to users leaving their CAC at work, in their computer, is costing 261 work years per year with an estimated cost of 10.4 million payroll dollars. Finally, the new authentication method is causing an increase in the loss or theft of CACs, our primary security mechanism for accessing DoD installations, at a rate of 28,222 a year. A single tool, such as the CAC, for all systems and services, carries much power, are we prepared for the responsibility?

15. SUBJECT TERMS
Computer Networks, Identification, Recognition, Verification, Smart Card, Network Authentication, Password

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			Dennis D. Strouble, PhD (ENV)
U	**U**	**U**	**UU**	147	**19b. TELEPHONE NUMBER** *(Include area code)* DSN: 785-3355 x3323 email: Dennis.Strouble@afit.edu