EVALUATING INFORMATION ASSURANCE CONTROL EFFECTIVENESS ON AN AIR FORCE SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEM

THESIS

Jason R. Nielsen, Major, USAF

AFIT/GCO/ENG/11-10

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GCO/ENG/11-10

EVALUATING INFORMATION ASSURANCE CONTROL EFFECTIVENESS ON AN AIR FORCE SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEM

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

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

Jason R. Nielsen, MS

Maj, USAF

March 2011

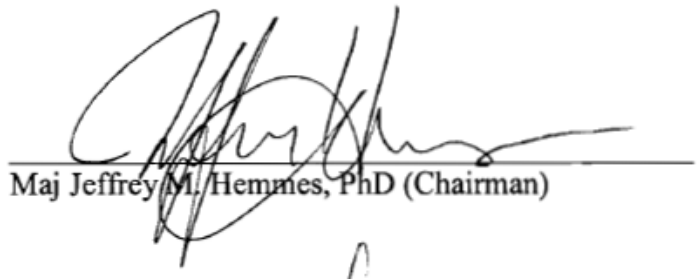
AFIT/GCO/ENG/11-10

EVALUATING INFORMATION ASSURANCE CONTROL EFFECTIVENESS ON AN AIR FORCE SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEM

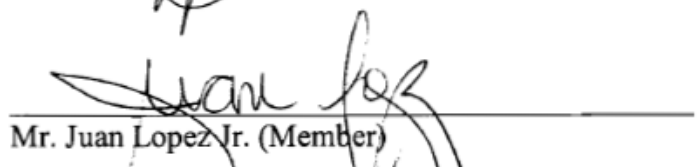
Jason R. Nielsen, MS

Maj, USAF

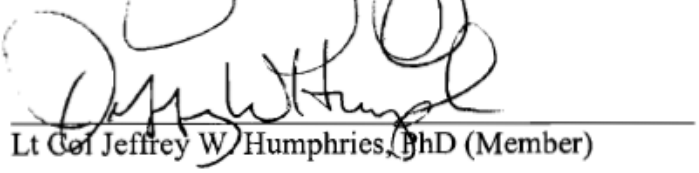
Approved:



Maj Jeffrey M. Hemmes, PhD (Chairman) — 9 Mar 2011 Date



Mr. Juan Lopez Jr. (Member) — 7 Mar 2011 Date



Lt Col Jeffrey W. Humphries, PhD (Member) — 3 Mar 2011 Date

Abstract

Supervisory Control and Data Acquisition (SCADA) systems are increasingly being connected to corporate networks which has dramatically expanded their attack surface to remote cyber attack. Adversaries are targeting these systems with increasing frequency and sophistication. This thesis seeks to answer the research question addressing which Information Assurance (IA) controls are most significant for network defenders and SCADA system managers/operators to focus on in order to increase the security of critical infrastructure systems against a Stuxnet-like cyber attack. This research applies the National Institute of Science and Technology (NIST) IA controls to an attack tree modeled on a remote Stuxnet-like cyber attack against the WPAFB fuels operation. The probability of adversary success of specific attack scenarios is developed via the attack tree. Then an impact assessment is obtained via a survey of WPAFB fuels operation subject matter experts (SMEs). The probabilities of adversary success and impact analysis are used to create a Risk Level matrix, which is analyzed to identify recommended IA controls. The culmination of this research identified 14 IA controls associated with mitigating an adversary from gaining remote access and deploying an exploit as the most influential for SCADA managers, operators and network defenders to focus on in order to maximize system security against a Stuxnet-like remote cyber attack.

To my Wife, Children & Family

Acknowledgements

I would like to express my sincere gratitude to my research committee, Maj Jeff Hemmes, Lt Col Jeff Humphries, and Mr. Juan Lopez. Many thanks to Maj Hemmes, as my thesis advisor for your patience, support and guidance throughout this effort. Thank you Lt Col Humphries for the two courses you taught and your feedback. Mr. Juan Lopez, thank you for sharing your deep knowledge of critical infrastructure as well as your research expertise and patience. I appreciate your continuous guidance and numerous course corrections on the path to this final product. Also a big thanks to Mr. Juan Nogueras for acting as my liaison with his WPAFB fuels personnel as well as AFMC fuels subject matter experts. Without your assistance and the efforts of your personnel this thesis would not have been possible.

Lastly, thank you to my wife, daughter and son for your love and support. To my wife, thank you for your time and patience in supporting me throughout this effort. Also, thank you for your countless hours reviewing my writings and acting as a sounding board for my ideas. You and the kids are my continuing inspiration and motivation.

Jason R. Nielsen

Table of Contents

List of Figures

Page

List of Tables

Page

EVALUATING INFORMATION ASSURANCE CONTROL EFFECTIVENESS ON AN AIR FORCE SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEM

I. Introduction

The frequency and sophistication of cyber attacks against critical infrastructure continues to escalate. A complex computer worm discovered in June 2010 effectively disabled Iran's nuclear program for more than a year (Barnes, 2010). The highly secure Iranian nuclear facilities were located underground, physically and electromagnetically isolated from insecure networks, also known as air gapped from the Internet. It is suspected that the worm propagated from universal serial bus (USB) thumb drives that technicians carried in and out of the facility which closed the air gap and allowed the worm to penetrate the SCADA system. The highly complex computer worm, called Stuxnet, was designed to jump from computer to computer until it found a specific control system that it targeted (Barnes, 2010). Computer experts examining the worm have described it as the first weaponized computer virus. According to Ralph Lagner, the computer expert who first sounded the alarm about Stuxnet, it is "like the arrival of an F-35 into a World War I battlefield" (Barnes, 2010).

According to Warden (1998), when applying his five-ring system model of the adversary it is imperative to approach the enemy as an interdependent system versus an opposing army, navy and air force. The concentric rings of his model point to the relative importance as they radiate out from the center which contains the leadership, see Figure 1. Critical infrastructures fall within the second, system essentials ring and third, infrastructure ring of the five-ring

systems model, making them relatively more important than population and fielded military (Warden, 1998). Modern societies and militaries have become increasingly dependent on critical infrastructure such as electrical power generation/distribution, petroleum refining/distribution, telecommunications. These critical infrastructures also form a critical vulnerability to the industries that make modern societies and economies flourish. They also provide the logistical support to allow a nation to successfully prosecute war.

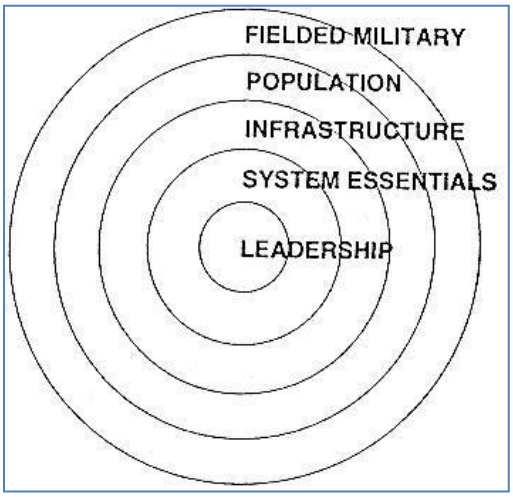


Figure 1. Warden's Five Rings (Warden, 1995)

Background

The systems that control critical infrastructures are Industrial Control Systems (ICS) which encompass several types of control systems including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other smaller control systems such as Programmable Logic Controllers (PLC) (Stouffer, Falco & Scarfone, 2008). Industries associated with critical infrastructure include power generation and distribution, oil and gasoline refining and distribution, water and waste systems, chemical processing and transport, manufacturing, telecommunications, and banking infrastructures (Munro, 2008). In

the past, these systems were isolated from corporate networks and the Internet, which insulated them from remote cyber attacks and provided security through obscurity. However, these systems are increasingly being connected to corporate networks in order to increase operating efficiencies and reduce costs (Stouffer et al., 2008). Also, open source technical information on SCADA systems is readily available to attackers (Stouffer et al., 2008). This has dramatically increased the attack surface of SCADA systems to remote cyber attack. Note: Throughout this thesis, Industrial Control Systems will be referred to as Supervisory Control and Data Acquisition (SCADA) systems for consistency.

SCADA systems typically require high system availability due to the safety of ongoing industrial processes. Disruption of system processes can cause an enormous negative financial impact and even potential for loss of life. Because of the critical nature of these systems they are prime targets for terrorists, or a nation state adversary, especially during wartime. According to a MacAfee survey of over six hundred IT executives, the majority, 59% believe that foreign governments are already involved in cyber attacks against their critical infrastructure (Baker, Waterman & Ivanov, 2010). Additionally 80% of the respondents acknowledge connecting their SCADA systems to an IP network despite the risks. Finally, the survey also revealed that less than 50% of the critical infrastructure providers implement basic security measures (Baker et al., 2010). The MacAfee report highlights the widespread vulnerability of critical infrastructures world-wide. There is significant room for improvement in securing SCADA systems from cyber attack. The federal government has recognized it has an important role to ensure critical infrastructures are protected. The federal government has developed policies and partnerships with private industry in an effort to secure critical infrastructures through a number of executive orders, laws, and plans.

The National Institute of Standards and Technology (NIST) Special Publication 800-82 describe Information Assurance (IA) controls that apply to information systems in support of the Federal government. These IA controls are the management, operational, and technical controls that are considered industry best practices and government recommendations and guidance. They serve to protect the confidentiality, integrity, and availability of the system and its information. IA controls are the primary means through which SCADA systems are made defensively strong to withstand cyber attacks. NIST recommends a defense-in-depth approach of layering IA controls in order to achieve an effective cyber security posture (Stouffer et al., 2008). The defense-in-depth approach employs successive layers of policy, operational procedures and technology in a variety of methods to secure systems to achieve multilayer, multidimensional protection, like the defenses of a medieval castle (Ashley & Jackson, 1999).

Research Goals

Current literature does not show an indication of the degree to which IA controls increase the security of SCADA systems. My research will apply NIST IA controls in an attack tree to evaluate the effectiveness of the IA controls. Attack trees are graphically represented by an up-side down tree with the root node as the overall goal of the attack (Schneier, 1999). Sub goals and leaf nodes provide different paths to the root. The cyber attack is based on the recent Stuxnet exploit (Mills, 2010). The attack tree model is based on the Wright-Patterson Air Force Base (WPAFB) fuels operation. This operation is a small, government owned, contractor operated Air Force base fuels operation. According to the Fuels flight contract branch chief, the WPAFB fuels operation represents 70% of the Air Force fuels flight implementations in the CONUS. Air Force Fuels Policy Directive 08-002, dated 10 November 2008 directs implementation of fuels Automated Information Technology (AIT) hardware and software

(Hession, 2008). The Fuels Manager Defense (FMD) SCADA system is operated and maintained by nearly all of the CONUS AF fuels operations (DLA, 2009). By examining the probability of adversary success of specific attack scenarios along with WPAFB fuels operation subject matter experts (SMEs) impact assessment, an overall risk is produced which highlights the most significant groups of IA controls which contribute to increased security.

This research seeks to answer the research question: Which group of NIST 800-82 IA controls are most significant for network defenders and SCADA system managers/operators to focus on in order to increase the security of the WPAFB Fuels flight critical infrastructure systems against a Stuxnet-like remote attack? Since Stuxnet is currently recognized as the most advanced exploit against critical infrastructure, this research is timely in order to identify IA controls which are most effective to mitigate a Stuxnet-like attack.

Thesis Organization

The purpose of this thesis is to determine which group of IA Controls are most effective to mitigate a particular type of cyber attack against an Air Force fuels operation. The introduction provided background material, established the research goals and introduced the research question. Chapter 2 provides background on critical infrastructures and related research. It describes SCADA systems along with polices that govern their security. It compares and contrasts SCADA systems with traditional information technology systems and describes recent cyber attacks against critical infrastructure. Additionally, this chapter provides background on attack trees and explains how they function. Finally, it introduces the Stuxnet exploit. Chapter 3 discusses the research methodology. It describes what data was collected and how the data was used. Also, how the results will be analyzed. Chapter 4 presents the analysis of the data. Critical aspects of a risk matrix are examined and the most influential IA controls

are identified. Chapter 5 presents the conclusions, recommendations for future work and limitations to this approach.

"Throughout the Entire Course of History, Warfare is Always Changing." --Andre Beaufre

II. Literature Review

Chapter Overview

The purpose of this chapter is to provide background information on SCADA systems in general and review previous research in the area of SCADA systems. Also, it provides information on the Stuxnet worm, IA Controls, Fault trees, and Attack Trees.

Supervisory Control and Data Acquisition Overview

Industrial Control Systems (ICS) encompass several types of control systems including SCADA systems, Distributed Control Systems (DCS), and other smaller control system components such as Programmable Logic Controllers (PLC) (Stouffer et al., 2008). Figure 2 shows a high level view of a typical SCADA system architecture.

SCADA systems are defined as a collection of systems, software and equipment that allows an operator in a remote location to maintain situational awareness and exert control of portions of, or an entire, industrial operation (Carlson, 2002). SCADA systems were designed to enable control of large scale industrial processes and provide a means for their safe and efficient operation and delivery (Munro, 2008). SCADA systems are typically geographically dispersed and contain many data collection points. As an example, eighty percent of the United States' power is generated by 270 utilities. Each utility has its own SCADA system that contains up to 50,000 telemetry collection points (Fernandez and Fernandez, 2005). In some cases, the number of data collection points are in the 100,000 range, and a few instances near 1 million (Daneels and Salter, 1999).

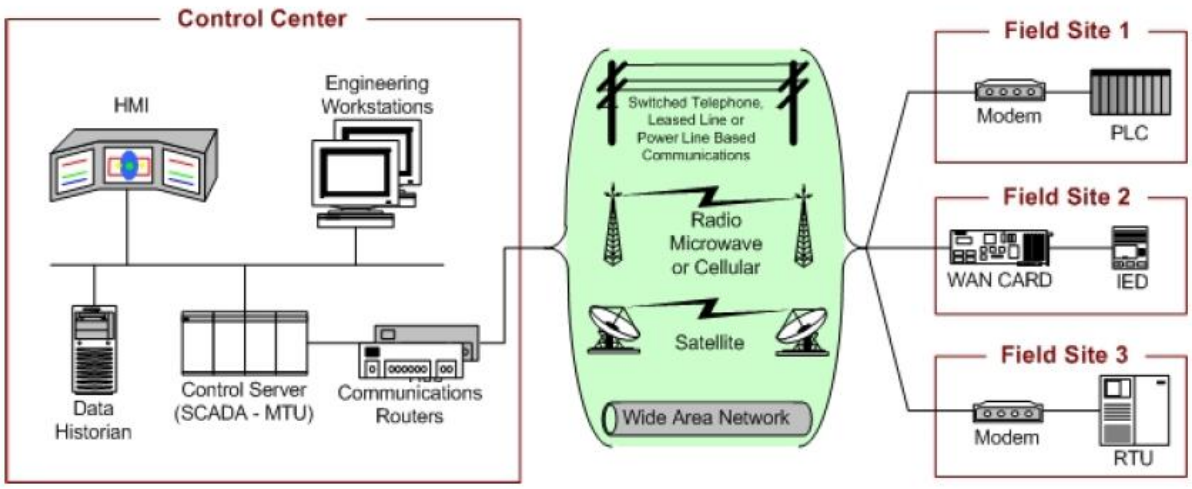


Figure 2. High level view of SCADA system Architecture (Stouffer et al., 2008)

These systems typically require total and absolute system availability (Gold, 2009). Absolute system availability is required due to the safety of ongoing industrial processes. Disruption of these processes can also cause enormous negative financial impacts and even potential for loss of life. For instance, a large gas line explosion would cost the parent company financial loss and also has the potential for human injury or death, depending on the location (Carmody, Hammerschmidt, Goglia & Black, 2002). For instance, on 20 September 2010, a gas line explosion in San Bruno, California killed 6 peoples and destroyed 30 homes (Hennessy-Fiske, 2010). Also, on 19 January 2011, an explosion of a gas line in Philadelphia, Pennsylvania killed one person, injured five and burned two homes (Stamm, 2011). The underlying cause of both explosions are still under investigation as of this writing.

Many industries utilize SCADA systems. Some of these industries include power generation and distribution, oil and gasoline refining and distribution, water and waste systems, chemical processing and transport, manufacturing, telecommunications, and banking infrastructures (Munro, 2008). They form centers of gravity for societies and governments.

According to the DOD Dictionary of Military Terms (2010), a center of gravity is the source of power that provides a nation the moral or physical strength, freedom of action, or will to act (Mullen, 2010). They provide the life blood for modern societies to operate efficiently. Indeed, critical infrastructures form a center of gravity for the U.S. Approximately 90 percent of the U.S. critical infrastructure is owned by private companies (Stouffer et al., 2008).

A great deal of SCADA systems in operation today were installed 15 to 20 years ago, when attack threats were more physical (Gold, 2009). Information security was not a significant concern when most SCADA systems were initially installed. Today these networks are threatened electronically when they are connected to a corporate network, which is typically connected to the Internet.

Government Role in SCADA security

The U.S. government has recognized the important role that critical infrastructures play in the functioning of government, the economy, and society in general. The federal government has a responsibility in ensuring these infrastructures are protected. It has taken steps, in the form of policy and regulation, to facilitate increased security of these critical systems. The next several sub-paragraphs present in chronological order many of these policies and other initiatives the U.S. government has taken to facilitate critical infrastructure security.

Critical Infrastructure Protection

On 15 July 1996, President Clinton signed Executive Order 13010. The purpose of this order was to develop a strategy to protect critical infrastructures. The order established the President's Commission on Critical Infrastructure Protection (PCCIP), and a number of associated committees, whose mission was to examine the problem of securing critical infrastructures. The Infrastructure Protection Task Force (IPTF) was also established to identify

and coordinate existing expertise in the public and private sector. The PCCIP along with related committees and the IPTF were all temporary in nature and terminated on or before seven months after the executive order was signed (Clinton, 1996).

Presidential Decision Directives 62 and 63

On 22 May 1998 President Clinton signed Presidential Decision Directives (PDD) 62 and 63. Both seek to strengthen the nation's defenses. The directives dealt with emerging unconventional threats and protection of U.S. critical infrastructure. A key tie-in between the two, described in PDD-62 is the establishment of the office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The two sections below provide additional details of the two PDDs.

Protecting America's Critical Infrastructure

On 22 May 1998, President Clinton signed Presidential Decision Directive/NSC-63 to further address critical infrastructure protection. PDD-63 clearly identified critical infrastructures as physical and cyber systems that are essential to the minimal operations of both the economy and government (Clinton, 1998). Additionally, the directive identified telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private as examples of critical infrastructure sectors. The intent of this document was to ensure that the United States would take necessary steps to eliminate significant vulnerabilities to critical infrastructures, with an emphasis on cyber systems. PDD-63 also emphasized that the protection of critical infrastructures is a shared responsibility and partnership between the commercial entities and the government. Finally, the directive designated lead agencies for 15 specific sectors and functions of critical infrastructure.

Combating Terrorism

On 22 May 1998, President Clinton also signed PDD 62, "Protection against Unconventional Threats to the Homeland and Americans Overseas", which reaffirms PDD-63 vs. policy on Counter Terrorism. This classified document creates a more systematic approach to fighting the terrorist threat. It clarifies the activities of many U.S. agencies charged with roles in defeating terrorism. In order to achieve a heightened level of coordination, it also established the Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism (Clinton, 1998).

Critical Infrastructures Protection Act of 2001

Section 1016 of the Patriot Act is referred to as the Critical Infrastructures Protection Act of 2001. It establishes the National Infrastructure Simulation and Analysis Center (NISAC) to serve as the source of national competence to address critical infrastructure protection and continuity. The act also further clarified the definitions of critical infrastructures as:

> Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Bush, 2001).

Critical Infrastructure Protection in the Information Age

On 16 October 2001 President Bush signed Executive Order 13231, Critical Infrastructure Protection in the Information Age. EO 13231 established the President's Critical Infrastructure Protection Board. The board is responsible for recommending policies and coordinating programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems (Bush, 2001).

Patriot Act of 2001

On 26 October 2001, the Patriot Act of 2001 was approved by President Bush. The Patriot Act of 2001 significantly increased the ability of law enforcement agencies to search telephone and e-mail communications, medical, financial, and other records. Additionally, it eased restrictions on foreign intelligence gathering within the United States and broadened the discretion of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts. Finally, the act expanded the definition of terrorism to include domestic terrorism (Bush, 2001).

National Strategy for Homeland Security, 2002

In July 2002, President Bush published the National Strategy for Homeland Security. This was the first document of its kind. The purpose of the Strategy was to mobilize and organize in order to secure the nation form terrorist attacks. It laid out three priorities: 1) Prevent terrorist attacks within the United States, 2) Reduce America's vulnerability to terrorism, and 3) Minimize the damage and recover from attacks that do occur (Bush, 2002).

National Strategy for Physical Protection of Critical Infrastructures and Key Assets

In February 2003, the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets was signed by President Bush. It seeks to facilitate the strategic planning process for core mission areas and reduce the nation's vulnerability by protecting our critical infrastructures and key assets from physical attack. It aligns homeland security efforts into six critical mission areas: intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructures and key assets, defending against catastrophic terrorism, and emergency preparedness and response. It also provides a unified

organizational structure and identified specific initiatives to protect critical infrastructures (Bush, 2003).

Homeland Security Presidential Directive 7

On 17 December, 2003 the Homeland Security Presidential Directive 7 was signed by President Bush. It established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. It defines terms and asserts 31 policy statements. These policy statements provide additional detail of and define the roles various federal, state, and local agencies will play in carrying out the directive (Bush, 2003). See Appendix A for listing of Roles and Responsibilities of Sector-Specific Federal Agencies.

National Strategy for Homeland Security, 2007

In October 2007, an updated National Strategy for Homeland Security was published by President Bush. It addressed safeguarding and preserving the nation's Critical Infrastructure and Key Resources (CIKR). The Strategy builds directly from the first National Strategy for Homeland Security published in 2002. This updated Strategy incorporates lessons learned from exercises and real-world catastrophes. It also complements the National Security Strategy and the National Strategy for Combating Terrorism, both published in 2006. The purpose of the strategy is to guide, organize, and unify U.S. homeland security efforts on four goals: 1) prevent and disrupt terrorist attacks, 2) protect the American people, our critical infrastructure, and key resources, 3) respond to and recover from incidents that do occur, and 4) continue to strengthen the foundation to ensure long-term success. Table 1 identifies 17 sectors of critical infrastructure and key resources established by the 2007 strategy.

Table 1. 17 Sectors of Critical Infrastructure and Key Resources (Bush, 2007), (Bush, 2003)

Sectors of Critical Infrastructure and Key resources	Description
Agriculture and Food	The supply chains for feed, animals, and animal products; Crop production and the supply chains of seed, fertilizer, and other necessary related materials; and post-harvesting components.
Banking and Finance	Variety of physical structures, to include buildings and financial utilities, as well as human capital. Also payment, clearing and settlement systems and electronic and physical transfer of assets.
*Chemical	Manufactures of products such as fertilizer, chlorine, and polymers. Depends on raw materials, manufacturing plants and processes, and distribution systems, research facilities, transportation and electricity.
*Commercial Facilities	Commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct commercial transactions, or recreation.
*Commercial Nuclear Reactors, Materials, and Waste	Robust containment buildings, redundant safety systems, and sheltered spent fuel storage facilities.
*Dams	Larger Dams provide water and electricity to cities, and agriculture. The federal government is responsible for roughly 10 percent of the dams whose failure could cause significant property damage or have public health and safety consequences.
Defense Industrial Base	Private industries supporting the DOD.
Drinking Water and Water Treatment Systems	Fresh water supply and wastewater collection and treatment. These utilities depend on reservoirs, dams, wells, and aquifers, treatment facilities, pumping stations, aqueducts, and transmission pipelines.
Emergency Services	Fire, rescue, emergency medical service, and law enforcement organizations that are employed to save lives and property in the event of an accident, natural disaster, or terrorist incident.
Energy	Generation, production, distribution and command and control of electricity and oil and natural gas.
Government Facilities	Federally owned or operated facilities, including DOD and the Department of Veterans Affairs.
Information Technology	Information systems, networks, Communication systems, Internet, facilities, human and intellectual capital, networks, communications lines, infrastructures and IT services.
*National Monuments and Icons	Diverse array of national monuments, symbols, and icons that represent our Nation's heritage, traditions and values, and political power.
Postal and Shipping	Depends on a transportation fleet composed of both service-owned and contractor-operated vehicles and equipment. Mail also travels daily by commercial aircraft, truck, railroad, and ship.
Public Health and Health Care	State and local health departments, hospitals, health clinics, mental health facilities, nursing homes, blood-supply facilities, laboratories, mortuaries, and pharmaceutical stockpiles.
Telecommunications	Provides voice and data service to public and private users through a complex and diverse public-network infrastructure encompassing the Public Switched Telecommunications Network (PSTN), the Internet, and private enterprise networks.
Transportation Systems	Aviation, maritime traffic, rail, pipelines, highways, trucking and busing, and public mass transit.
** Denotes sectors added by 2007 Strategy*	

National Infrastructure Protection Plan

In 2009, the National Infrastructure Protection Plan (NIPP) was signed by Michael Chertoff. It seeks to make U.S. critical infrastructures and key resources more resilient to disruption. The NIPP also lays out a risk management framework which enables risk-informed decision making to mitigate effects of terrorist attacks through risk management actions. It also contains the most current mapping of sector-specific agency to critical infrastructure sector. Table 2 provides a mapping of government agency to critical infrastructure (Chertoff, 2009).

Table 2. Government agency to Critical Infrastructure mapping (Chertoff, 2009)

Sector-Specific Agency	Critical Infrastructure and Key Resources sector
Department of Agriculture Department of Health and Human Services	Agriculture and Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Healthcare and Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Water
Department of Homeland Security Office of Infrastructure Protection	Chemical Commercial Facilities, Critical Manufacturing, Dams, Emergency Services, Nuclear reactors, Materials, and waste
Office of Cybersecurity and Communications	Information Technology Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration United States Coast Guard	Transportation Systems
Immigration and Customs Enforcement Federal Protective Service	Government Facilities

Defense Critical Infrastructure Program

On January 14, 2010, DOD Directive (DODD) 3020.40 established the Defense Critical Infrastructure Program **(**DCIP). It established the responsibilities of the DOD, pursuant to Homeland Security Presidential Directive 7 and the National Industrial Security Program DODD

5220.22 of 2004. The DCIP sought to align DOD efforts in support of the National Infrastructure Protection Plan. DCIP contains DOD sector-specific agency responsibilities for the national Defense Industrial Base (DIB) sector (Lynn, 2010).

Summary of Government Role in SCADA security

The U.S. government has recognized the important role that critical infrastructures play in the functioning of government, the economy, and society in general. The previous sections described a number of steps it has taken via policy and regulation to facilitate increased security of critical infrastructures. These extensive efforts by the federal government highlight the relevance of this research on the effectiveness of IA controls. The next section compares and contrasts characteristics of SCADA and IT systems.

Comparing SCADA and IT systems

Information Technology (IT) and SCADA systems were built for different purposes and are governed by different core principles. When SCADA systems were created, the primary concern was for reliability, maintainability, and availability (RMA) (Byres et al., 2003). SCADA systems were created to support critical infrastructure control processes. Security was considered from the standpoint of physical security, consisting of closed systems with controlled access to the network and consoles. This method required attackers to have access and be able to come in physical contact with the equipment they were attempting to affect. In contrast, IT systems' core principles are confidentially, integrity and availability (CIA) (Bishop, 2003). See Figure 3 for graphical representation of RMA and CIA core principals. Computers were originally networked together to support research efforts. Now the Internet is primarily used for communications, information, commerce and entertainment.

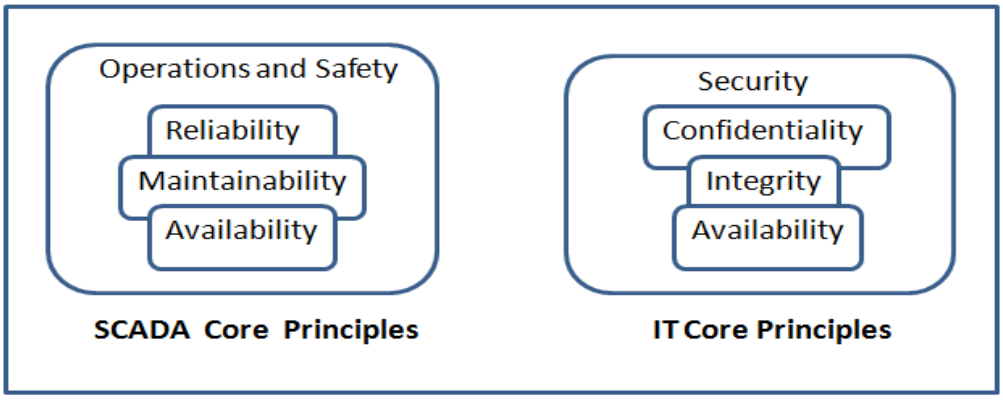


Figure 3. RMA and CIA core principles (Byres et al., 2003), (Bishop, 2003)

Perhaps the most significant differences between SCADA and IT networks are their requirements for availability, latency, and security. IT network users tolerate periodic outages where service is not available. However, SCADA systems are required to operate uninterrupted for months and in some cases years (Byres and Lowe, 2004). Furthermore, IT systems typically operate with considerable variation in communication path latency. However, SCADA systems cannot tolerate increased latency due to proprietary protocols and safety requirements for timely human interaction (Byres and Lowe, 2004). Another significant difference between the two is illustrated with the end devices. In an IT network there is a high tolerance for periodic end device, ie. computer outages. There is a greater concern of keeping the core network servers operating in the network operations center. In SCADA systems, however, the end device is extremely important in that it provides telemetry to the central facility. If telemetry is not available, then serious problems can arise (Byres and Lowe, 2004). Since SCADA systems are now being connected to IT networks the security vulnerabilities inherent to SCADA systems can

now be exploited via the IT network. Table 3 summarizes some of the differences between IT systems and SCADA systems.

Table 3. Differences between IT and SCADA systems (Stouffer et al., 2008)

Characteristic	IT System	SCADA System
Performance Requirements	Non-real-time Response must be consistent High throughput is demanded High delay and jitter maybe acceptable	Real-time Response is time-critical Modest throughput is acceptable High delay and/or jitter is a serious concern
Availability Requirements	Responses such as rebooting are acceptable Availability deficiencies can often be tolerated	Rebooting may not be acceptable Outages must be planned and scheduled well in advance Exhaustive pre-deployment testing required
Risk Management Requirements	Confidentiality and integrity is paramount Fault tolerance is less important – momentary downtime is not a major risk Delay of business operations is major risk	Human safety paramount, followed by process protection Fault tolerance is essential, downtime not acceptable Major risk impact is regulatory non-compliance, loss of life, equipment, or production
Architecture Security Focus	Primary focus is protecting the IT assets, and the information stored on or transmitted Central server may require more protection	Primary goal is to protect edge clients (e.g., field devices such as process controllers) Protection of central server is still important
Unintended Consequences	Security solutions are designed around typical IT systems	Security tools must be tested to ensure that they do not compromise normal ICS operation
Time-Critical Interaction	Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary	Response to human, other emergency interaction is critical Access to ICS should be strictly controlled, yet not hamper human-machine interaction
System Operation	Systems are designed for use with typical operating systems Upgrades are straightforward	Differing and custom operating systems often without security capabilities Software changes must be carefully made
Resource Constraints	Systems are specified with enough resources to support the addition of third-party applications such as security solutions	Systems are designed to support the intended industrial process, with minimal memory and computing resources to support the addition of security technology
Communications	Standard communications protocols Mostly wired networks with some wireless Typical IT networking practices	Many proprietary and standard communication protocols Many types of comm. media used including wire/wireless Complex networks, require expertise of control engineers
Change Management	applied in a timely fashion in the presence of good security policy and procedures. The Procedures are often automated.	Must be thoroughly tested and deployed incrementally throughout a system. ICS outages must be scheduled days/weeks in advance
Managed Support	Diversified support styles	Usually single vendor
Component Lifetime	3-5 years	15-20 years
Access to Components	local and easy to access	isolated, remote, and require extensive physical effort to gain access to them

With such significant differences among the key characteristics of IT and SCADA systems, it follows that joining the two together in a networked environment may lead to

negative consequences. One consequence is unintentionally exposing SCADA systems to exploitation and electronic attack.

Risk Factors

There are several factors which increase the risk associated with SCADA systems. These include: 1. standardized protocols and technologies, 2. connectivity to other networks, 3. insecure and rogue connections, and 4. widespread availability of technical specifications (Stouffer et al., 2008). These factors increase the attack surface of SCADA systems. They are each discussed further in the next four sections.

Standardized Protocols and Technologies

Vendors are openly publishing their equipment specifications to allow third parties to generate compatible add-ons. They are also transitioning from proprietary systems to open systems to reduce cost and remain competitive. Increasing in popularity standard technologies like Microsoft Windows® and common network protocols like TCP/IP. Standardized protocols and networking technology vulnerabilities and exploitation techniques are widely published on the Internet. The increased use of standard protocols increases the risk to SCADA systems (Stouffer et al., 2008).

Connectivity to other networks

Many organizations have connected their SCADA systems to a corporate network in order to improve ease of access to resources by operational personnel to conduct maintenance and diagnostics. Connectivity to the SCADA system allows management to make operational and purchasing decisions. Connecting the SCADA network to a corporate network exposes all of the SCADA components to the corporate network. The corporate network in-turn has

network connections to the Internet and in many cases other corporate partner networks as well. An adversary can use these connections to attack the SCADA system (Stouffer et al., 2008).

Insecure and rogue connections

Modems are typically used by vendors to perform maintenance, diagnostics and system health monitoring. These connection points introduce a significant risk to SCADA systems. While modems provide great reach-back capability at significant cost savings, they also provide an entry into the SCADA network. If the modem does not use an authentication scheme, it can be easily exploited. In some cases, systems come pre-installed with modems that are configured with a default password that is never changed (Stouffer et al., 2008). The same is true for some wireless connections (Stouffer et al., 2008). Some wireless encryption is very weak and leave networks susceptible to a determined hacker. Also, connections opened for vendors to do temporary work are a risk, especially if they are forgotten about (Stouffer et al., 2008). Additionally, hard-wired connections that do not have strong authentication and encryption can also be easily breeched (Stouffer et al., 2008).

Widespread availability of technical specifications

Technical information for SCADA system components are widely available to the public for free or purchase. This information aids industry professionals to maintain their expertise and assists in development of future control systems. Anyone with access to the Internet can gain specific technical information and in some cases operating manuals for vendor specific equipment. With this widespread availability of information, it is possible for a determined attacker who has little knowledge of SCADA systems to utilize automated attack tools against them (Stouffer et al., 2008).

Vulnerabilities of SCADA Systems

It is becoming increasingly common for critical infrastructure sectors to connect their SCADA system to enterprise or corporate networks which inadvertently act as a gateway to the Internet (Stouffer et al., 2008). The Internet connection provides another avenue for attackers targeting SCADA systems. Since SCADA systems are connected to an IP network, they are vulnerable to most of the IP exploits that hackers use. In addition to physical access and connection to IP networks as attack vectors, SCADA systems are also vulnerable to attack through telephone modems, wireless networks, laptop computers, and trusted vendor connections (Byres et al., 2003). According to Ken Munro, managing director of SecureTest, they have discovered a new vulnerability in every SCADA test they have conducted (Munro, 2008)[1].

The Department of Homeland Security staged an experiment called Aurora in March 2007, at the Department of Energy's (DOE) Idaho Lab (Meserve, 2007). A video recording demonstrated how a large industrial generator commonly deployed in the nation's power grid could be destroyed by a remotely connected computer hacker. Multiple, simultaneous attacks such as this could knock out power over a large geographical area for months, causing significant harm to the U.S. economy. Scott Borg, an economist working on federal government projects, stated that if a third of the country lost power for three months, it would cost $700 billion, causing greater damage than the great depression (Meserve, 2007).

The DOE Aurora experiment demonstrated how an adversary can cause significant damage to the power grid by cyber means with only a few lines of code. In a SCADA environment, something as ordinarily mundane as a network scan can be enough to cause

---

[1]SecureTest is a provider of expert penetration and security testing, with over 500 clients across the private, public sectors (SecureTest, 2010).

equipment to malfunction (Fernandez and Fernandez, 2005). Unlike IT systems, which are routinely patched as needed, SCADA systems are only patched every few years due to high demand of availability (Fernandez and Fernandez, 2005). SCADA systems are also highly vulnerable to malformed packets, causing them to stop functioning, as compared to IT networks which would merely discard them.

The National Institute of Standards and Technology's Guide to Industrial Control Systems points out that vulnerabilities can exist in policy and procedures, platform configuration, platform hardware, platform software, malware protection, network configuration vulnerabilities, network hardware, network perimeter, network monitoring and logging, communications, and wireless connections (Stouffer et al., 2008). In the past the hacker community lacked expertise in exploiting SCADA systems. However now that SCADA systems can be reached from the Internet, hackers will likely have interest in exploiting them.

In July 2009, the Department of Homeland Security (DHS) Control Systems Security Program (CSSP) issued a report titled "Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments" that present the results from 15 ICS assessments performed from 2004 through 2008. The purpose of the assessments was to provide information to critical infrastructure providers on vulnerabilities, so they could increase the security of their SCADA systems. Vulnerability information was collected and analyzed. Common vulnerabilities were grouped into general categories. The analysis of the data collected found that poor network protocol implementations, information disclosure, and authentication problems occurred with the most frequency (DHS, 2009). Table 4 contains a listing of the common vulnerabilities discovered from the assessments.

Table 4. Summary of Common CSSP ICS assessment findings (DHS, 2009)

Category	Common Vulnerability
Poor Code Quality	Use of potentially dangerous functions in proprietary ICS application
Vulnerable Web Services	Poor authentication
	Directory traversal enabled
	Unauthenticated access to Web server
Poor Network Protocol Implementations	Lack of input validation: Buffer overflow in ICS service
	Lack of input validation: Lack of bounds checking in ICS Service
	ICS protocol uses weak authentication
	ICS protocol uses weak integrity checks
	ICS product relies on standard IT protocol that uses weak encryption
Poor Patch Management	Unpatched or old versions of third-party applications incorporated into ICS software
	Unpatched operating system
Weak Authentication	ICS uses standard IT protocol that uses weak encryption
	Use of standard IT protocol with clear-text authentication
	Client-side enforcement of server-side security
	Improper security configuration
	No password required
	Weak passwords
	Weak password requirements
Least User Privileges Violation	Unauthorized directory traversal allowed
	Services running with unnecessary privileges
Information Disclosure	Unencrypted proprietary ICS protocol communication
	Unencrypted nonproprietary ICS protocol communication
	Unencrypted services common in IT systems
	Open network shares on ICS hosts
	Weak protection of user credentials
	Information leak through unsecure service configuration
Network Design Vulnerabilities	Lack of network segmentation
	Firewall bypassed
Network Component Configuration Vulnerabilities	Access to specific ports on host not restricted to required IP addresses
	Port Security not implemented on network equipment

ICS Security Controls

According to Stouffer et al. (2008), security controls are one of various security mechanisms which when implemented correctly can impede an adversary by mitigating system

vulnerabilities. Security controls consist of management, operational, and technical safeguards or countermeasures put in place for an information system to protect the confidentiality, integrity, and availability of the system and its information (Ross, Stoneburner, Porter, Rogers, Swanson, Graubart et al., 2007). Organizations need to determine which security controls are needed to protect their information systems and operation. They must also determine the needed level of assurance. These controls are measured when put in place to ensure they are providing the protection desired. Security controls are recommended for use by organizations for protecting their information systems and should be employed as part of a larger well-defined and documented information security program (Ross et al., 2007). Table 5 lists the classes and families of the 17 Security Controls.

Table 5. Security Control Families and Classes (Ross et al., 2007)

FAMILY	CLASS
Access Control	Technical
Awareness and Training	Operational
Audit and Accountability	Technical
Certification, Accreditation, and Security Assessments	Management
Configuration Management	Operational
Contingency Planning	Operational
Identification and Authentication	Technical
Incident Response	Operational
Maintenance	Operational
Media Protection	Operational
Physical and Environmental Protection	Operational
Planning	Management
Personnel Security	Operational
Risk Assessment	Management
System and Services Acquisition	Management
System and Communication Protection	Technical
System and Information Integrity	Operational

ICS specific security control guidance is found in Appendix I of NIST Special Publication 800-53. It takes the guidance for IT systems and tailors it specifically for ICS. These changes recognize the differences in ICS and IT systems and provide additional focus to the need for real-time response and extremely high availability, predictability, and reliability (Ross et al., 2007).

Threats to SCADA Systems

A threat is defined as an indication of imminent danger (Merriam-Webster, 2010). SCADA systems are subject to threats similar to that of computer systems and telecommunications networks. These threats can come from both electromagnetic and physical means. Threats can come from people, natural disasters, accidents, and equipment failures (DHS, 2005). Adversarial threats are a subset of threats consisting of people motivated to negatively impact SCADA systems. Other forms of threats like natural disasters and equipment failures are important to plan for in order to protect SCADA systems, but are not the focus of this literature review. The adversarial threats along with their description and motivations are listed in Table 6.

Table 6. Adversarial Threats to ICSs and motivations (DHS, 2005), (Grimes, 2005)

Threat agent	Description	Motivation
Malicious intruders	Remote Hacking once required a fair amount of skill or computer knowledge, attackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.	Destruction, Activism, Recreation
Criminal groups	Organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud.	Financial advantage
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities.	Espionage, Enable future attacks
Insiders	The disgruntled insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data.	Financial advantage, Revenge
Hostile Governments	Several nations are aggressively working to develop information warfare doctrines, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power–impacts that could affect the daily lives of U.S. citizens.	Espionage, Warfare
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence.	Ideology
Industrial Spies	Industrial espionage seeks to acquire intellectual property and know-how by clandestine methods	Financial advantage

A threat may be known to exist, but not significant. For instance, a company may know of industrial spies targeting them from a competitor, but the company may deem the threat as non-existent for specific portions of their infrastructure. For example, risk analysis may reveal that an outlying control station that is operating with 20 year old technology is not a likely target. It is unlikely that the competition would target this facility. Assigning additional security resources to the remote control station is unwarranted. Therefore, in order to properly assign resources, the severity of the threat must be determined.

Severity of Adversarial threat

Some industry experts speculate that since SCADA systems are typically custom made for specific sector applications, that it requires a great deal of specific knowledge on a particular

system and the specific industry in order to attack it. Furthermore, that the "specialized knowledge" requirement will limit the number of attackers perhaps explains why SCADA attacks are not nearly as common as attacks on other computer networks (Chikuni and Dondo, 2007). Although successful SCADA attacks are infrequent to date, there are indications of increased interest by adversaries. In 2002, U.S. investigators found evidence on browser logs showing Al-Qaeda operatives spending time on sites that offer programming for switches that run critical infrastructures (Gellman, 2002). Also, during interrogations, Al-Qaeda prisoners have expressed the organizations interest in targeting critical infrastructures (Gellman, 2002).

In September 2009, McAfee conducted a survey of critical infrastructure IT executives in fourteen countries (Baker et al., 2010). The 600 respondents were asked a number of questions, such as 'How long before you expect a major cyber incident affecting critical infrastructures in your country?' and 'Are current laws in your country insufficient against cyber attacks?' Two figures in the survey were particularly telling. Figure 4 shows the percentage of respondents that believe that foreign governments have been involved in cyber attacks against critical infrastructure in their country. The largest responder was China with 75 percent. The lowest was Spain with 42 percent. The United States responded with 60 percent. The vast majority believe that foreign governments are already attacking their critical infrastructures.

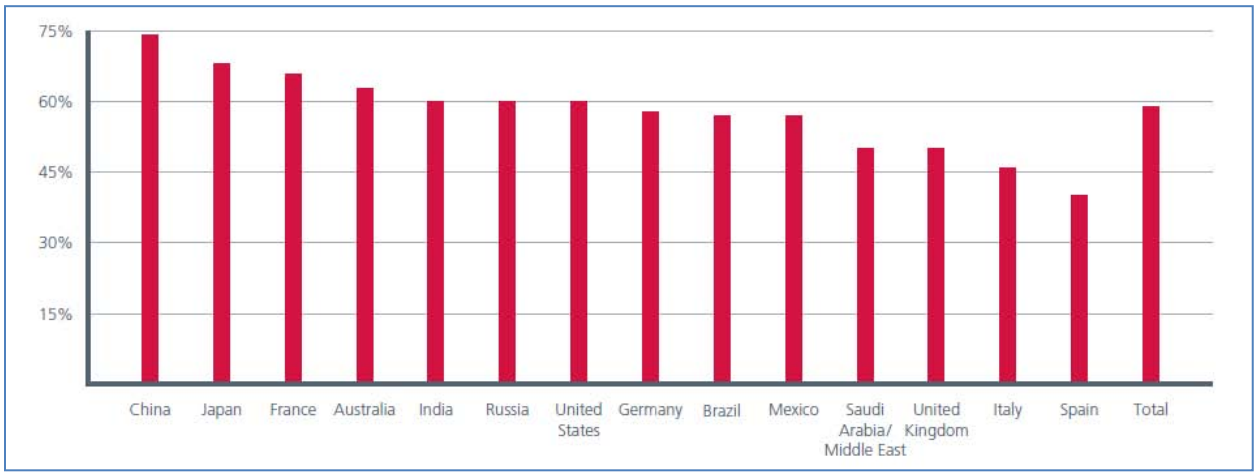


Figure 4. Suspected Cyber Attacks on Critical Infrastructure (Baker et al., 2010)

Another significant graph, Figure 5, from the McAfee study describes the percentage of large scale Distributed Denial of Service (DDoS) attacks that selected countries have experienced and their frequencies. Of the 13 countries listed on the graph 12 countries indicated that they experience DDoS attacks daily. Approximately 55 percent of the respondents reported large scale DDoS at least annually. However, these DDoS attacks only resulted in a damage to reputation, service interruption, or critical breakdown 23 percent of the time overall (Baker et al., 2010). These responses indicate that the adversary threat against critical infrastructure is high.

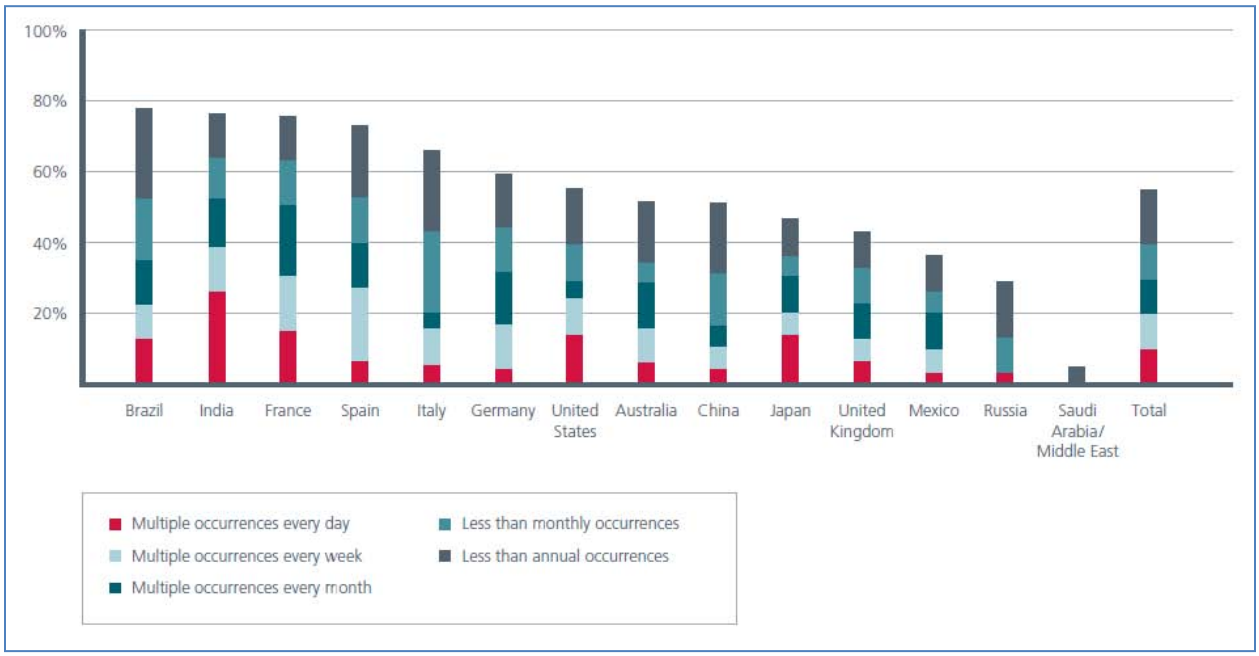


Figure 5. Suspected Large Scale DDoS Attacks and Frequency (Baker et al., 2010)

Although there are similarities between IP networks and SCADA systems, there are significant differences in the negative impact that results when these systems are successfully attacked by an adversary. For example an interruption to an Internet Service Provider (ISP) will typically result in a loss of revenue to customers. However, a similar interruption to a SCADA system could cause the loss of proprietary information, damage to the economy, damage to the environment and potentially significant loss of life (Stouffer et al., 2008).

IT systems connected to the Internet get attacked frequently. According to the DoD, their computer networks are scanned and probed by external parties millions of times per day (CBS/AP, 2009). These reconnaissance activities usually precede attacks. According to the Carnegie-Mellon's Computer Emergency Response Team Coordination Center (CERT/CC) there were 7,236 Computer system/IP vulnerabilities reported in 2007 and 44,074 vulnerabilities

reported since they started keeping statistics in 1995 (Carnegie-Mellon CERT, 2010). Since 1998, the number of incidents reported to CERT/CC has increased significantly. Figure 6 shows the number of reported incidents for the years 1990 through Q3 2003 for IP systems (Carnegie-Mellon CERT, 2010). The CERT/CC also notes that computer intrusion incidents are underreported. For instance, some businesses may not want system hacks known publically, because it could damage their reputation and result in the loss of current and future customers. The trend for increasing incidents shows no sign of slowing. The Internet grew by 380 percent from the year 2000 to 2009 and new vulnerabilities are routinely discovered (Internet World Stats, 2010). As the Internet continues to grow, so does the attack surface, making yet more incidents possible.

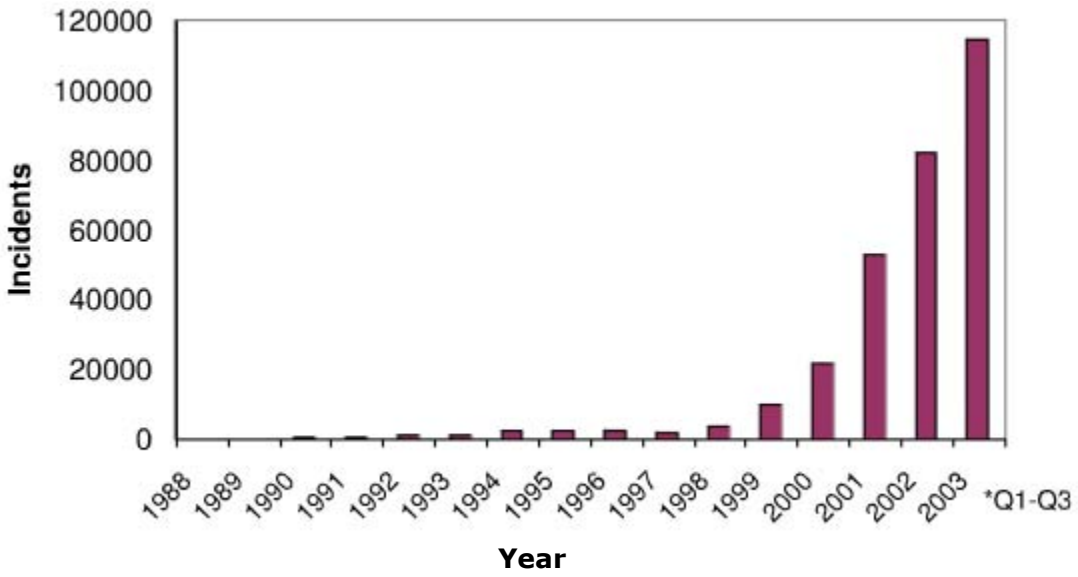


Figure 6. Information Security Incidents: 1990–2001 (Carnegie-Mellon, 2010)

A handful of incidents occurred where critical infrastructures were negatively impacted. The British Columbia Institute of Technology (BCIT) tracks network security incidents that directly impact ICS and SCADA systems in their database (Byres et al., 2003). The BCIT estimate there are approximately 100 cyber related incidents per year (Hildick-Smith, 2005). According to the BCIT Industrial Security Incident Database for the year 2004, there was a sharp increase in the number of incidents reported annually starting in 2001. Figure 7 shows the Industrial Security Incidents from 1982 through 2006 as recorded in the BCIT.

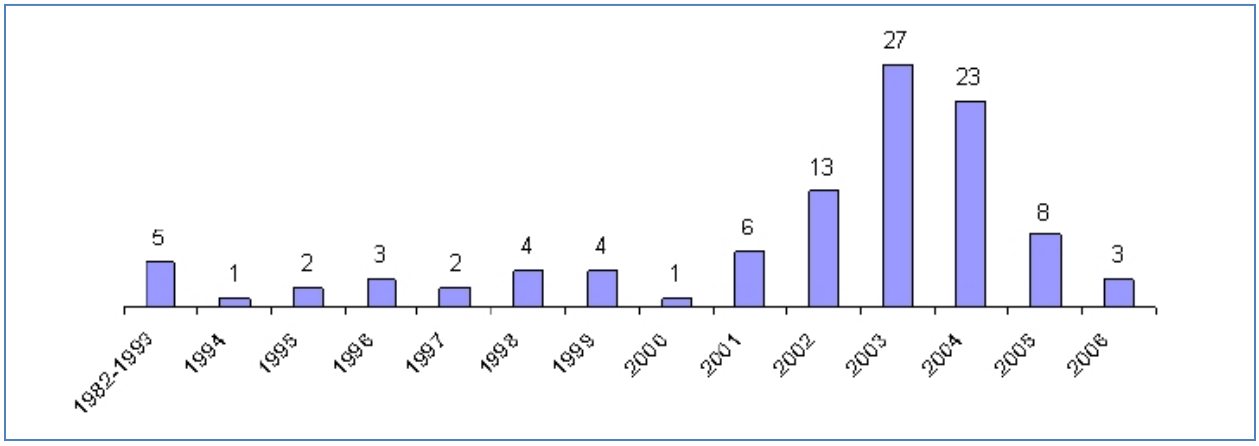


Figure 7. Industrial Security Incidents by Year (Stouffer et al., 2008)

Additionally, prior to 2001, 70 percent of the attacks originated from insiders. From 2001 forward, there was a notable shift with 70 percent of the attacks originating from external sources (Byres and Lowe, 2004). This shift in attack origin is likely due to increased connectivity of SCADA networks to the Internet, thus dramatically increasing the attack surface of these systems. As of September 2009, it is estimated that 80 percent of critical infrastructure operators connect their SCADA systems to an IP network despite the security risks (Baker et al., 2010). A

determined individual with an internet connection, phone line, or wireless connection could attack SCADA systems and cause damage. Recent history provides numerous examples of attacks against SCADA systems running across the threat spectrum from teenage recreational hacker, to terrorist, to disgruntled insider.

Recent SCADA attacks

The preponderance of malicious cyber attacks have occurred on non-SCADA computer networks. The numbers of reported and verified malicious attacks against SCADA systems are small when compared to attacks against computer networks. One problem in verifying malicious SCADA attacks is the difficulty of establishing attribution of the act to the attacker (Stouffer et al., 2008). In recent years many malicious cyber attacks against SCADA systems worldwide have caused significant monetary cost. The following are a number of impressive examples of SCADA related utility outages. Although some were caused by acts of nature, or accidents, they are instructive of the effects that are possible by attacking critical infrastructures.

1. 1997, Worcester Air Traffic Communications - In 1997, a juvenile accessed the phone system operated by New York – New England Telephone Company (NYNEX). As a result the telephone service was disrupted to the Federal Aviation Administration Tower at the Worcester Airport, to the Worcester Airport Fire Department and to other related entities. Additionally, aircraft were unable to send an electronic signal to activate the runway lights on approach. Telephone service, including the 911 service, was also disabled throughout the local area (Stouffer et al., 2008).
2. 1999, Bellingham Washington Gas Pipeline rupture - In June 1999 a steel gas pipeline ruptured near Bellingham Washington, killing two children and an 18 year old, injuring eight others and causing $45 million in property damage. There were numerous

contributing factors to the accident including a SCADA system that became unresponsive allowing pressure to build up beyond safety parameters. The National Transportation Safety board concluded that if the SCADA system operated correctly the rupture would not have happened (Carmody et al., 2002).

3. 2000, Maroochy Shire sewage control system - The Maroochy Shire, Queensland computerized waste management system was hacked into by a disgruntled former employee and caused millions of liters of raw sewage to spill out into local parks, rivers and the grounds of a Hyatt Regency hotel. The attack was conducted by an employee of the subcontractor that installed the SCADA system and was later turned down for job with the local government. He accessed the network through a wireless connection. The cost of the incident was estimated at greater than $1 million (Smith, 2001).
4. 2003, Ohio Davis-Besse nuclear power plant - The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January 2003 and disabled a safety monitoring system for nearly five hours and a plant process computer for six hours. The worm gained entry through a T1 line that bypassed the business network firewall. The nuclear power plant was offline at the time and both systems had redundant analog backups that were unaffected (Poulsen, 2003).
5. 2003, Northeast Blackout - On August 14, 2003, the largest power blackout in North American history affected an area with an estimated 50 million people and 61,800 mega-watts (MW) of electric load in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut and New Jersey, and the Canadian province of Ontario. The series of events that contributed to the blackout started with a failure of an alarm processor in First Energy's SCADA system. A short time later multiple high

voltage lines in Ohio tripped due to contact with trees. This caused overloading of additional high voltage lines which led to eventual failure of the power grid. The blackout left some parts of the country without power for up to 4 days. The estimated cost to the U.S. ranged between $4 billion and $10 billion (Liscouski et al., 2003).

6. 2003, DoS attack on an Israeli power plant - Iranian hackers attempted to hack into the Israel Electric Corporation's computers and launch a denial of service attack to disrupt the power supply in Israel. The attackers were foiled before any damage was inflicted (Yamini, 2003).
7. 2003, CSX train service outage - In August 2003, the Sobig computer virus brought down train signaling systems throughout the east coast of the U.S. The virus infected the computer system at CSX Corporation's Jacksonville, Florida headquarters, shutting down signaling, dispatching and other systems. This caused a number of train cancellations and delays of long distance trains ranging from four to six hours (Hancock, 2003).
8. 2005, Taum Sauk Dam Failure – The dam was overtopped during a night time pump-back operation. More than 1 billion gallons of water were released when the Dam failed. The overtopping was caused in large part due to improperly secured sensors that reported false water levels to the SCADA operators (King and Calcagno, 2010).

Although not all of these mishaps were caused by a malicious party, it is clear from the recent history that the consequences of utility interruptions are significant. An attacker with sufficient motivation and knowledge could conduct a devastating attack against critical infrastructures resulting in tremendous financial loss as well as the potential for loss of life.

Attack Countermeasures

In order for a cyber attack to succeed, an attacker, vulnerability and a means of exploiting the vulnerability must exist. If one or more of these don't exist then a successful attack is unlikely. An attacker is also referred to as a threat. From a defensive standpoint it is very difficult to eliminate a threat. Likewise exploits built to take advantage of vulnerabilities are beyond the influence of defenders. SCADA systems defenders install countermeasures like IA controls in order to mitigate known vulnerabilities (Stouffer et al., 2008). So, the primary factor under the control of the SCADA systems operators is making their systems defensively strong through countermeasures like implementing IA controls. According to MacAfee (2010), basic security measures are not widely adopted by critical infrastructures around the world. It describes a basic security measures adoption rate ranging from 62 percent on the high end to 40 percent on the low end (MacAfee, 2010). Also, the sector with the highest adoption rate was banking and energy and the lowest water/sewage (MacAfee, 2010). DOD security measure adoption rates are likely higher across all sectors due to directive regulations, but objective data was not available to support this assertion. The next section describes future trends in SCADA systems.

Future Trends

The spectrum of threats to SCADA systems will continue to evolve. Terrorist groups and governments will continue to refine their tools, techniques and procedures (TTP) for targeting SCADA systems. Governments will increasingly recognize that cyber attacks against SCADA systems are an evolving area of warfare and national influence. China is currently investing considerable effort into developing its cyber capabilities. The Chinese government has also engaged in rhetoric toward other countries about their ability to adversely affect critical

infrastructures by cyber means. There have been numerous cases in the recent past of Chinese hackers breaking into U.S. government systems. As part of their military evolution, China is seeking to achieve electronic dominance over its global competitors by the year 2050 (Coughlin, 2010).

Governments have three main challenges regarding the protection of critical infrastructures. They must modify governmental organization structure to properly handle cyber threats, find effective ways to share sensitive threat and vulnerability information, and deploy capabilities to assist critical infrastructures for their common defense (Baker et al., 2010).

As the interest in SCADA systems increases, additional vulnerabilities will be discovered over time. Safeguarding SCADA systems to ensure the functioning of the government, the economy and society will continue as a core area of concern with the U.S. government. The pursuit of SCADA systems security will continue to grow. Since SCADA systems are increasingly connected to other networks, ease with which exploits are built against SCADA systems will increase as well. The future is ripe for discovering new vulnerabilities and exploitation of SCADA systems.

Related Research

In Mendezllovet's (2010) work titled "Codifying Information Assurance Controls for DOD SCADA Systems", the primary goal of the research was to compare and map IA controls from the NIST SP 800-82 to the DOD IA Control framework. The primary tool in Mendezllovet's research was a survey from Civil Engineer SMEs. A relative ranking was produced within the three categories of Management, Operational and Technical IA controls. Additionally, respondents strongly favored four of the eight new IA controls they considered for potential inclusion into DOD regulations. This research in evaluating the effectiveness of IA

controls may also provide additional insight into disconnects identified in Mendezllovet's (2010) research. For example, in his research, Civil Engineer (CE) SMEs rated Certification and Accreditation low as a management control and rated encryption high as a technical control. Both of these issues were identified as out of synch with published information security guidance. These potential touch points are examined in the conclusion of this research.

In Igure's (2007) doctoral thesis, a taxonomy of security vulnerabilities in SCADA protocols, he addressed the problem of security assessment of SCADA communication protocols. He used known SCADA protocol vulnerabilities to construct a taxonomy that provides a method for security assessment of other SCADA protocols. As part of future work he suggested that his research could support the effort to find relative risks of the various vulnerabilities of the system. The paths of his taxonomy could be assigned numeric values. These relative values would provide a risk grading on individual attacks and vulnerabilities (Igure, 2007). This research will use a different tool in a similar manner as described by Igure in order to determine security effectiveness of groupings of IA controls against a specific category of attack and attack vector. This will also give a partial ranking of a group of IA controls.

Byres et al. (2004) describe the application of an attack tree methodology to a common SCADA protocol. The goal is to use the attack tree as a method to assess the security risks in the protocol to identify flaws that could cause damage to the SCADA system. The authors developed 15 attacker goals, then built attack trees. They speculated that since there is very little security inherent in SCADA protocols that any moderately skilled hacker would be able attack the system if access is achieved. They made a number of important observations that are directly applicable to this research. Attackers typically engage in reconnaissance activity prior to launching an attack. Also, the clear precursor to a cyber attack is gaining network access to the

target system. The team of authors believe that the technical difficulty is the most critical indictor of attack success. Lastly, the authors suggested as future work an approach that better aggregates attack tree subordinate node values and site specific parameters such as known vulnerabilities and countermeasures. This research will address a portion of Byres et al (2004) future work by incorporating an aggregation of subordinate leaf node values and IA control site specific countermeasures into the attack tree.

Logistics Compliance Assessment Program

The Logistics Compliance Assessment Program (LCAP) is an evaluation program to ensure units key logistics processes are performed in a safe, standardized, repeatable and technically compliant manner. In the Air Force, Major Commands (MAJCOMs) conduct LCAP evaluations of subordinate units to assess their logistics proficiency. Air Force Instruction 20-111, Logistics Compliance Assessment Program (LCAP) standardizes the breadth, depth, frequency, grading, and reporting requirements (Reno, 2009). The LCAP applies to AF units performing duties across the spectrum of logistics to include fuels operations. Acceptable quality levels are used to minimize subjectivity in LCAP evaluations and describe allowed discrepancies. LCAP functional checklists are developed by AF/A4L in coordination with MAJCOMs. The checklists serve as a guide for inspectors in assessing logistics units (Reno, 2009). The AFMC Fuels Management LCAP checklist was reviewed in order to glean aspects of the operation which are vulnerable to a cyber attack. The following items may be susceptible to cyber attack: accuracy of inventory, proper documentation of inspections and procedures, documentation of training, certifications and qualifications, operational checklists and fuels operating Instructions.

Stuxnet

In June 2010, a complex computer worm was discovered which effectively disabled Iran's nuclear program for more than a year. Later this worm was given the name Stuxnet. It is suspected that the worm initially propagated from thumb drives that were carried by personnel from one computer to another, even broaching Iranian air gapped systems. For almost 17 months, Stuxnet targeted a specific Siemens centrifuge control component to moderate the speed at which the nuclear facilities' centrifuges rotated in order to damage, but not destroy them (Barnes, 2010). The worm is also capable of masking its own actions, making troubleshooting for the root cause extremely difficult. Even though the Iranians are aware that their systems are infected with the worm and have spent substantial resources in cleaning-up, the worm is so virulent that they continue to be plagued by it (Barnes, 2010).

Stuxnet uses a digitally signed kernel-mode rootkit. It has approximately 4,000 functions which is comparable to some commercial software products (ICS-CERT, 2010). Stuxnet takes advantage of 4 zero day exploits. Two of the zero days have since been patched. It also uses the same exploit as the Conficker worm (ICS-CERT, 2010). It appears that a thumb drive is the primary means of propagation, but the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has noted that it can also spread via network shares, STEP7 Project files, WinCC database files, and a print spooler vulnerability (ICS-CERT, 2010). As of October 2010, Symantec estimates that over 100,000 computers are infected with Stuxnet worldwide, with 60% of those infections in Iran (Jarema, 2010).

Computer experts at Microsoft who examined the worm estimate that it took 10,000 man-hours to build. Others conclude that it must have been developed by a nation state due to its sophistication and ability to target very specialized proprietary vendor equipment (Barnes, 2010).

Experts have a long way to go to discover all of the intricacies of the exploit as reverse engineering work continues. The Stuxnet worm is an interesting and relevant real-world exploit to choose as part of this research.

NIST IA Controls

The purpose of NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, is to provide guidance for securing ICS, SCADA systems, DCS, and other systems performing control functions in critical infrastructure operations. It recommends security countermeasures via a list of many different methods and techniques for securing SCADA systems in order to mitigate associated risks. The guide encourages readers to perform a risk-based assessment on their systems and to tailor the recommended guidelines and solutions to meet their specific security, business and operational requirements (Stouffer et al., 2008). Security controls are defined as the management, operation, and technical safeguards and countermeasures identified to protect the confidentiality, integrity, and availability of the information and system (Katzke et al. 2006). The 30 IA controls as described in NIST SP 800-82 are listed in Table 7. These security controls will be incorporated into the attack tree described later in Chapter 3.

Table 7. ICS Security Controls (Stouffer et al., 2008)

Management Controls
Risk Assessment
Planning
System and Service Acquisition
Certification, Accreditation, and Security Assessments
Operational Controls
Personnel Security
Physical and Environmental Protection
Control Center/Control Room
Portable Devices
Cabling
Contingency Planning
Disaster Recovery Planning
Configuration Management
System and Information Integrity
Malicious Code Detection
Intrusion Detection and Prevention
Patch Management
Media Protection
Incident Response
Awareness and Training
Technical Controls
Identification and Authentication
Password Authentication
Physical Token Authentication
Role-Based Access Control
Web Servers
Virtual Local Area Network
Dial-up Modems
Wireless
Audit and Accountability
Encryption
Virtual Private Network

Different critical infrastructure operations may implement only a subset of the IA controls. Depending on the degree to which the ICS is integrated into the operation, implementation of some IA controls is not possible. For instance, if an operation does not

possess any portable devices then the operational control for portable devices is not implemented.

Fault Trees

Fault Tree Analysis (FTA) is a tool used for safety and reliability evaluations to analyze and visually display failure paths in a system. It provides a means for systems level risk evaluations via a tree structure (Ericson, 1999). FTA is about 50 years old as of this writing and is widely used around the world. The failure behavior of the system is modeled in a visual fault tree. The simple set of logic rules and symbols within the tree structure make qualitative and quantitative evaluation of very complex systems possible (Ericson, 1999). The construction of fault trees is simple, but Ericson (1999) warns that if the tree becomes too complex, they become much more difficult to solve. He states that the ability to evaluate is directly related to fault tree size, complexity and computer capacity. It's important to briefly discuss fault trees as the precursor from which attack trees evolved. Attack trees take advantage of all of the features of fault trees plus additional capabilities.

Attack Trees

Attack trees, just like fault trees are models of reality (Ericson, 1999). They provide a simplified representation of complex real world drivers. The accuracy underlying the drivers and future analysis depend on time/effort spent studying them and assumptions made.

In an attack tree, the attacks against the target are represented by an upside down tree structure with the goal as the root node and different ways of achieving that goal as sub-goals and leaf nodes as the lowest level tasks (Schneier, 1999). The leaf nodes contain user-definable values called indicator values to store attributes of that leaf node. It is possible to assign multiple user-defined variables in the form of Boolean, continuous, or explicitly specified values to the

leaf nodes. For instance, a Boolean value could take the form of breach of trust, either true or false, a continuous value such as cost, from zero to potentially millions of dollars and explicitly specified values such as 1 for low to 4 for high. There are many other possibilities for continuous node values to include, but not limited to - technical difficulty, technical ability, noticeability, impact of attack, probability of apprehension, likelihood of attack success, site conditions and installed countermeasures (Byres, 2004). This research uses, in part, publically available attack data as a source to populate indicator values in the attack tree. For a large attack tree there can be thousands of potential attack scenarios if all possible paths are followed in order to read the root goal. In order to narrow down the number of attacks to better match the potential threat, a threat agent profile is applied to the tree. In the SecureITree software a threat agent profile defines the capabilities of the attacker. The threat agent profile is user defined with operators on the indicator values which describe the capabilities and limitations of the specific attacker, thus reducing the number of potential paths that are available to reach the root goal (Ingoldsby, 2010).

The attack tree includes both physical and cyber attacks for completeness. It shows the touch points between the two and how they affect one-another. Additionally, it highlights the mutually exclusive physical and cyber aspects of possible attacks. Just like fault trees, if the attack tree becomes too complex, the utility is lost. Therefore, only cyber attacks are evaluated in this research. Also to ensure the tree is not too complex, the lowest level tasks are kept at a course level of description. For instance, the low level task of "searching the Internet" for target information could include the sub-task of accessing the Internet, navigating to Google, navigating to target website, etc…. However, the task is left as "searching the Internet" for

better utility. The tasks are broken down to the point where further subdividing them does not contribute to the overall research effort to reveal the IA control system security effectiveness.

Attack trees are compelling tools for a number of reasons. Attack trees provide a methodical way of describing the security of systems, based on varying attacks and attacker profiles (Schneier, 1999). The use of attack trees allows the comparison of technical and non-technical attacks which leads to a more comprehensive analysis of threats and vulnerabilities (Franz et al., 2004). They also capture knowledge in a reusable form and are scalable, so the creator does not need to be an expert in everything (Schneier, 1999). Attack trees also focus analysis on measureable goals that can ultimately be translated into specific tests against real world implementations (Byres, 2004). For instance if an organization experienced significant financial loss over a period of time due to physical theft of property, they may develop the goal of reducing financial loss due to theft. The use of an attack tree can reveal specific areas to further develop security courses of action in order to reduce the likelihood of theft and thus reduce future financial loss. Attack trees also allow for a structured elaboration of events in order for an attack to be successful (Byres, 2004). These distinctive capabilities of attack trees make the tool well suited to answer security related questions.

Limitations of Attack Trees

There are a number of disadvantages to attack trees. The main disadvantage of attack trees is that they provide only the choice between and/or nodes. This limits the ways a goal can be broken down into sub-goals (Buhan, Bazen, Hartel & Veldhuis, 2006). Another limitation is that attack trees may not consider secondary factors. For instance, a robust insider threat monitoring program may catch a malicious insider and prevent an incident. Also, a realistic estimation of the indicator values at the leaf node level is difficult to get exactly right (Opel,

2005). Additionally, it may be difficult to break the leaf node actions into totally independent steps (Piètre-Cambacédès & Bouissou, 2010). Lastly, the creation of a complete Attack Tree is virtually impossible. They can give a false sense of security. Some attack vectors may be overlooked. It is always limited by the skills and depth of knowledge of the creator (Opel, 2005). Although attack trees have limitations, they have numerous characteristics which make them well suited for modeling purposes in this research.

Attack Tree Modeling Software

Modeling software can significantly assist in the creation and enumeration of attack trees. SecureITree software was purchased by AFIT in order to facilitate research in the Center for Cyberspace Research (CCR). This software provides the capability to model attack trees in a visual manner. It further incorporates the application of various indicator values to the leaf nodes. Additional operations are available to analyze attack scenarios, threat agents, risk, and allows the propagation of indicator values up the tree. An example of an attack tree with the root goal called Root is displayed in Figure 8. In order for an AND node to be true, all subordinate leaf nodes must be true. Conversely for an OR node to be true, only one of the subordinate leaf nodes need be true. Finally, since the root node is the ultimate goal of the attacker, the indicators associated with it reflect the resources required to compromise the system (Byres, 2004).

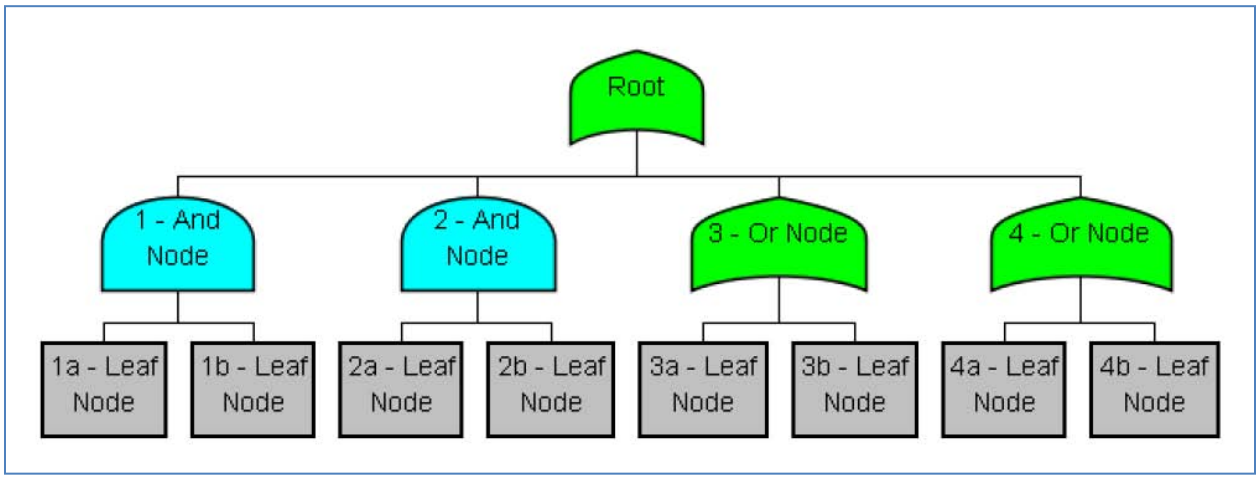


Figure 8. Example Attack Tree

Oil and Gas Pipeline sector

The specific critical infrastructure for this research is fuels operations, which is part of the oil and gas pipeline sector. This is a high interest area for the government and military. Access to petroleum and its associated operations are literally the fuel that enables war and drives modern civilization. This sector was chosen due to existing research efforts supported by HQ AF A4/A7 and an established relationship between the CCR and the local WPAFB fuels flight. The local fuels operation was utilized as the foundation of the attack tree model and appropriate NIST SP 800-82 IA controls were incorporated.

Chapter Summary

This chapter provided a summary of the current state of critical infrastructure control systems protection and exploitation. The compelling cost and operational benefits continues to drive increased connectivity of control systems to corporate networks. This increased connectivity also increases the attack surface of control systems. It is highly probable that motivated adversaries will attack SCADA systems. Since critical infrastructure owners and

operators worldwide are seeing increased attack activity, governments are eager to partner with private entities to ensure their continued function.

"I am tempted to make a slightly exaggerated statement: that logistics is all of war-making, except shooting the guns, releasing the bombs, and firing the torpedoes."
- ADM Lynde D. McCormick, USN

III. Methodology

Chapter Overview

This chapter describes the research methodology for the IA control system security effectiveness effort. It describes the approach, data sources, building the attack tree, understanding probability, and limitations. It concludes with a brief outline of how results are interpreted in the data analysis chapter.

Introduction

This research will provide insight into which IA controls are most significant for network defenders and SCADA systems operators to focus on in order to ensure the security of critical infrastructures against a Stuxnet-like exploit. Since the attack vector is the most advanced exploit found to date against critical infrastructure, this research is timely to identify those critical IA controls which are most effective in mitigating a successful attack.

Approach

This study continues the Air Force Institute of Technology (AFIT) AF/A4/7 – Logistics, Installations & Mission Support sponsored research effort into critical infrastructure protection. A portion of the framework in Risk Assessment section of NIST 800-30, Risk Management Guide for Information Technology Systems is used to develop a Risk Level Matrix and then recommend particular IA controls. The Likelihood determination, step five of the guide, is developed via a cyber attack tree modeled on the WPAFB fuels operation. The attack tree is generated from operator checklists, annual rate of occurrence from significant mission impacting

events, the NIST IA controls, existing survey data and direct researcher observation of operations. Next, a meaningful way to represent the probability of attacker success is determined. It will then be used to develop the probability values related to IA controls and individual attacker actions which culminate in an overall probability of adversary success. Then an analysis is performed on the paths an attacker can take in order to achieve the overall goal and five specific, different attack scenarios are chosen. The attack scenarios will allow the attacker to produce specific adverse impacts against the SCADA system. Next an impact analysis, step 6 of the guide, is performed to determine the adverse impact resulting from a successful attack. The impact analysis data is obtained via a survey instrument of six WPAFB Fuels SMEs. Then a risk determination, step 7 of the guide, is made using the SME responses along with the probability of adversary success to develop a risk matrix. Finally the risk matrix will point to the group of IA controls which most significantly contributes to system security against a Stuxnet-like cyber attack, producing the IA control recommendations, step 8 of the guide.

Understanding Probability of Adversary Success

Attack trees are particularly useful in estimating the risk for situations where the event happens infrequently or has not occurred before. Attack trees greatly improve risk estimation by incorporating not only knowledge of the defender's system, but also the adversary that will attack it. Risk is an expression of the likelihood that a threat actor will exploit a vulnerability of a target (Byres, 2004).

Ingoldsby (2010) identifies a number of different types of risk that are expressed as equations in the SecureITree software. The various types of risk include attack risk, attack scenario relative risk, absolute risk, probabilistic risk, capitalistic risk, and total risk. All of the risk calculations in the SecureITree software require subjective input from the user. In an effort

to reduce the amount of subjective data introduced into this research, it was desirable to seek another way to calculate risk that was more objective. Ayyub, McGill & Kaminsky (2007) introduced an equation to describe risk with only three variables. The probability of adversary success, P_s is described as one minus the system security effectiveness (1 - E_s), multiplied by both the probability of attack success, P_k and the probability distribution of hazard intensity imparted on the target, Q. This equation, $P_s = (1 - E_s) P_k Q$, is used as the starting point and modified in order to arrive at an equation to describe the overall probability of adversary success of a specific cyber attack using the attack tree. The equation is reduced by recognizing that Q has no meaning at the task level. The expression of the hazard intensity only has meaning at the root node of the cyber attack tree where all of the sub-tasks come together and the effect of the attack takes place. For this research Q will be held at the value of 1. The modified equation describing the probability of adversary success is $P_s = (1 - E_s) P_k$.

The above equation describes the probability of adversary success for a specific leaf node action with one IA control applied. Therefore the total probably of adversary success for a specific leaf node, P_{leaf}, with multiple IA controls applied is represented as the sum of all of the P_s's, divided by n, the number of IA controls which impact the particular leaf node, see Figure 9.

$$P_{leaf} = [\sum_{n}^{1} (1 - E_n) P_k]/n$$

Figure 9. Probability of Adversary success for specific leaf node

Next, it is necessary to calculate the probability at each of the OR and AND nodes below the root node. The probability is calculated as the average of the leaf nodes for an AND node.

OR node probabilities are calculated as the minimum of its leaf nodes. These probability rules then propagate up the tree to the root node. Finally the probability generated at the root node is the overall probability of adversary success for a specific attack scenario.

Method for Creating Attack Tree

In order to build an effective attack tree, it is desirable to follow a methodical, structured process in an iterative manner to guide thought. Schneier provides a straightforward method for creating an attack tree (Schneier, 1999). The steps are displayed graphically in Figure 10 and outlined below as follows:

Steps to Create an Attack Tree

1. *Identify possible attack goals*
2. *Form a separate tree for each goal, they may share subtrees or leaf nodes*
3. *Brainstorm attacks against each goal*
4. *Add these attacks to the tree*
5. *Repeat steps 3 and 4 until tree is complete*
6. *Give to someone else for review/additions*
7. *Add to/refine tree as necessary over time*

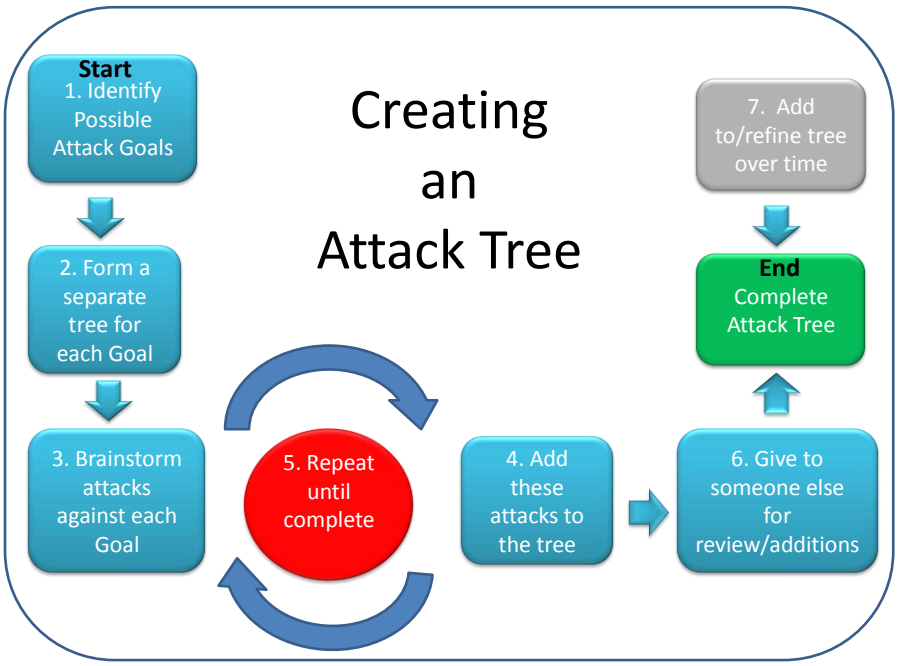


Figure 10. Creating an Attack Tree (Schneier, 1999)

Data Collection

In order to ensure the attack tree is as thorough and complete as possible, a number of source documents are utilized to assist in its construction.

- *Fuels flight operating instructions*
- *Quality checklists (QCL)*
- *Inspector General inspection results*
- *Various DoD and AF level petroleum regulations*
- *Fuels Manager Defender documentation*
- *Direct observations of fuels flight operation*
- *Amenaza SecureITree software references*
- *NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations*
- *NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security*
- *NIST SP 800-30, Risk Management Guide for Information Technology Systems*

The broad variety of sources and their thoughtful consideration used to create the attack tree ensures it is sufficiently complete.

Building the Attack Tree

In this research, the attack tree root goal is to cause a disruption of fuels operations. The result of a successful attack makes it possible for the attacker to deny, degrade, destroy, disrupt, deceive or delay aspects of the fuels operation. Potential threat agents against critical infrastructure include the broad categories: natural, accidental and malicious (Bundbury, 2009). The variation in potential threat agent attacks against critical infrastructure is expansive, running the gambit from teenage hacker, nation state actor, industrial accidents, terrorist attacks, disgruntled employee, and hurricane to heat wave and points in between. This research focuses on those attacks that are believed most common. According to MacAfee (2010), more than half of the executives surveyed said they had experienced large scale denial of service attacks and "stealthy infiltration" by a high level adversary like organized crime, or a nation state against

their critical infrastructure operation. Furthermore, fifty-nine percent of those surveyed believe that foreign governments had already been involved in attacks and infiltrations in their countries (Baker et al., 2010). Additionally the computer experts reverse engineering the Stuxnet worm suspect the worm was generated by a nation state (Barnes, 2010). The prevailing belief is that attacks on critical infrastructures by a well-organized nation state adversary with specific goals are common. Additionally, according to Byres (2004), 70 percent of the security incidents on critical infrastructures were from an external source during the years of 2001-2003. The majority of those attacks, 51 percent originated remotely via the Internet. Therefore, for this research the primary threat agent applied to the attack tree is a sophisticated, wealthy, remote and anti-social adversary. The adversary is highly technically competent and has substantial resources at their disposal. Lastly, the threat agent only attacks remotely and does not engage in physical attacks, nor social engineering.

The major sub-trees of the attack tree was built using the cyber attack methodology outlined in the book *Counter-Hack Reloaded* as a base-line in order to capture all the steps which typically occur in a cyber attack (Skoudis & Liston, 2006). Additionally, specific Stuxnet-related vulnerabilities were incorporated consistent with those described in US-CERT and ICS-CERT (2010). The attack tree was ported to SecureITree software. See Appendix B for the complete base stuxnet attack tree.

Indicator Values

The attack tree leaf nodes contain user-definable values called indicators to store characteristics of that leaf node. The necessary indicator values were determined and each leaf node was assigned indicators values as shown in Table 8.

Table 8. Leaf node Indicator variables (Ingoldsby, 2010)

Indicator Name	Type	Value Range
Probability of adversary success	Continuous	0..1
System security effectiveness	Continuous	0..1
Probability of attack Success	Continuous	0..1
Technical Difficulty	Specified	0 - Unlikely, .1 - Difficult, .5 - Moderate, .9 - Trivial, 1 – None
Physical presence	Boolean	T/F
Breach of trust	Boolean	T/F

Description of Indicator Values

The following paragraphs describe the indicator values and how values were determined for specific leaf nodes. The probability of adversary success was calculated as the values propagate up the tree. All other calculations of indicator values were done outside of the SecureITree software. See Appendix E for Indicator Value Summary.

Probability of adversary success: The probability of adversary success is the average of the probability of adversary successes as they propagate up the tree. See Figure 9 for equation. For a specific attack scenario there is only one overall probability of adversary success value at the root node. The lower the value the less likely the adversary will be successful.

System security effectiveness: The system security effectiveness is the degree to which the IA control is effective in defending the system. This value was obtained by extrapolating it from existing survey data. See appendix G further explanation (Freyre et al., 2010). The system security effectiveness value is the E_s value in the equation described in Figure 9. The larger the value, the more security the IA control provides for the system.

Probability of attack success: The probability of attack success describes the probability that a particular leaf node action will be successful. It equals the technical difficulty for that leaf node. The lower this value, the lower the likelihood of attack success. See Appendix H for Probability of Attack Success Matrix.

Technical difficulty: This indicator is used to determine the probability of attack success. According to Byers (2004) the technical difficulty of an attack is the most critical indicator of attack success. The higher the technical difficulty, the lower the probability of successful attack execution. See Table 9 for enumeration of the different tiers of technical difficulty. Objective data was not available to determine these values, therefore technical difficulty was determined and assigned by the researcher. Recognizing that the precise values of technical difficulty were not of critical importance, the researcher sought to assign values that were appropriate to the leaf node actions relative to each other. An effort was made to ensure the values assigned were consistent with the Threat Likelihood scale provided in NIST 800-30, Risk Management Guide for Information Technology Systems, pg 25.

Table 9. Description of Technical Difficulty (Byres, 2004)

Technical Difficulty		
Name	**Description**	**Value**
None	No technical skill required	1
Trivial	Little technical skill required	.9
Moderate	Average cyber hacking skills required	.5
Difficult	Demands a high degree of technical expertise	.1
Unlikely	Beyond the known capability of today's best hackers	0
Not Applicable	Not Applicable	-

Physical presence: Physical presence is a Boolean indicator that describes the need for an attacker to be physically present at the target in order to accomplish the leaf node action. If this indicator is false, then the action is executed remotely.

Breach of trust: Breach of trust is a Boolean indicator that describes the insider threat. If this value is true, then an insider is necessary for the leaf node action to succeed. If the value is false, then an insider is not necessary for success.

Associating IA Controls with Leaf node actions

The leaf nodes of the attack tree and the IA controls were associated with each other via a matrix with the leaf node actions on the vertical and the IA controls listed horizontally. Further, the values for the systems security effectiveness and technical difficulty where input. See appendix H for Probability of attack success matrix. The association of leaf node actions and IA controls were assigned as determined reasonable by the researcher. The NIST 800-82, Guide to Industrial Control Systems (ICS) Security was used as a source to assist in determining which IA controls are associated with the leaf node actions. Where the IA control had influence over the leaf node action, a partial probability of adversary success was calculated at that junction. For leaf nodes which were impacted by multiple IA controls, the average of the probability of adversary success was taken for that leaf node. Additionally the IA controls associated with each leaf node were annotated in the notes section in SecureITree.

The attack tree was passed to AFIT faculty and students who are knowledgeable in attack tree creation. Step six of Figure 10 directs that the attack tree be given to someone else for review/additions. The attack tree created for this research was provided to four AFIT faculty and a master's student who attended the SecureITree training to conduct a review for completeness. Two of the faculty instructors were cyber operations officers, each with over 18 years of

experience. The third faculty member has been an instructor at AFIT for 7 years and a IT security professional for 25 years. The fourth faculty member is a cyber security research engineer specializing in critical infrastructure. The final reviewer was a master's student with 10 years experience in Information Management who is also using an attack tree in his research. Following through with this step ensures that the attack tree captures a more complete picture of possible attacks and is rooted in operational reality. Feedback was incorporated into the final attack tree going forward in the remainder of this research.

Survey

The purpose of the survey is to seek USAF fuels subject matter experts (SME) ranking of cyber incidents against the fuels Automated Information System (AIS). This data, in conjunction with the probability of adversary success, will be used to determine which IA controls are most influential in securing the fuels AIS against a specific cyber attack. It will be administered to six personnel who work in fuels operations/management.

Population

The target population is USAF Fuels subject matter experts (SMEs). The sample was drawn from WPAFB Fuels flight personnel due to an existing research relationship. Also HQ AFMC/A4RE personnel were included due to proximity as targets of opportunity. The personnel participating met the following criteria:

- They possess extensive experience in fuels operations
- They have fuels SCADA system experience
- They volunteered to participate in the study

Survey Overview

The survey instrument consists of three parts. Part one consists of demographics which asks questions about years of experience, computer security/network security training, industry certifications and affiliation with the government. Part two asks respondents to assign an impact rating of low, medium or high to given incidents. The definitions provided for low, medium and high are derived from NIST SP 800-30, Risk Management Guide for Information Technology Systems, pg. 23. The respondents are rating the incidents in the right column of Table 10. Mapping of Vulnerability Leaf Nodes to Incidents. Part three asks respondents to further refine each incident they ranked in Part two. They are directed to consider all other incidents they can think of that fall within the same category and provide a value for the incident. These values range from: Low (1 to 10); Medium (11 to 50); High (51 to 100), derived from NIST SP 800-30, pg. 25. See Appendix I for full survey instrument.

Table 10. Mapping of Vulnerability Leaf Nodes to Incidents

Network Device Leaf Node	Stuxnet vulnerability Leaf node	Effect
Exploit vulnerable application	Step 7 Project files	Alter Fuels Manager Defense (FMD) database data
Exploit vulnerable application	Exploit Vulnerable WinCC	Alter FMD real time Human-Machine Interface (HMI) data
Exploit vulnerable Windows XP Operating System	Exploit Print Spooler vulnerability	Cause the computer hard drive where FMD resides to crash
Network Server	Exploit vulnerable Server Service	Transmit a false report to the Fuels Enterprise System
Network Server	Exploit Vulnerable Network Shares	Disrupt FMD Communications

Risk Matrix

The purpose of the NIST 800-30, Risk Management Guide for Information Technology Systems is to provide a structure for the development of an effective risk management program.

It provides descriptions and practical guidance needed for assessing and mitigating risks discovered within IT systems. The ultimate goal of the guide is to assist organizations to better manage IT-related mission risks (Stoneburner et.al, 2002). This guide contains recognized industry best practices and recommendations from NIST. The risk matrix is obtained from NIST 800-30, pg 25. There is no comparable risk matrix currently available specifically for SCADA systems, so this information systems risk matrix is used.

The risk matrix combines the results obtained from the attack tree and the survey. For the purposes of this research the threat likelihood is replaced with the probability of adversary success. The verbiage is different, but they both describe the same thing, the probability that the overall adversary attack succeeds. The values for the probability of adversary success are placed along the Y axis were threat likelihood is shown in Figure 11. In a similar manner the SME impact from the survey is placed along the X axis on the risk matrix. The resulting intersections will be plotted in a graph and analyzed in chapter 4. The scale of the X and Y axis are pulled directly from NIST 800-30 without modification. There is no need to deviate from the scale provided because it is a recognized guideline for best practices and fits well within the research methodology.

Threat Likelihood	Impact		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Figure 11. Risk Level Matrix (Stoneburner et al., 2002)

Limitations of this approach

Attack trees are subjective, because they reflect the thought process of their creator. Also, it holds true that "more heads are better than one" in building attack trees. This ensures that there are differing individual thought processes applied to the same problem, resulting in a stronger tree. The attack tree in this research was created by a single individual and validated by peer review. The review made the tree stronger, but it may not be as robust as an attack tree generated by a group. Also, data for the technical difficulty and probability of attack success were determined subjectively because objective data were not available. Since there was no objective data there was no way to evaluate the underlying probably distribution. Therefore, no assumption was made about the underlying probability distribution. Also, the manner in which the probably of adversary success was propagate up the attack tree may not be optimal. Averaging the probabilities fit well into the risk level matrix management tool, but also likely smoothed out the probabilities which may skew the results. Once again, objective data could shed additional light on a better way to propagate the probabilities up the tree. Additionally, due

to the thousands of available attack scenarios within the tree, a small subset of specific attack scenarios were selected for examination consistent with available attack trend data. As a consequence, potentially relevant data within those discarded scenarios are not included. Finally, inclusion of commercial proprietary data may make the attack tree applicable to a larger cross section of the critical infrastructure community. But due to its sensitive nature, proprietary data was not available for this research.

Data Analysis Procedure

The methodology presented here utilizes an attack tree based on WPAFB fuels operations. The probability of adversary success associated with each of the lowest level tasks contributes to the overall probability of adversary success of the specific attack. The probability of adversary success will vary depending on which leaf node actions are taken to reach the root goal and their corresponding IA controls. A survey of fuels operations SMEs provides the impact rating of specific incidents which are possible after a successful attack. These impact ratings are then coupled with the earlier probability to develop the risk matrix. The data points in the matrix will fall into one of nine quadrants, as in Figure 11. By examining the data points in the matrix, it will reveal the most influential IA controls. These IA controls will appear where the probability of adversary success is lowest. Therefore, the most influential IA controls will fall into the lower portion of the matrix, meaning those defensive IA controls are most effective. Also, the further to the right on the impact axis, the more significant the impact of the event. So, the closer to the lower right-hand portion of the matrix, the more significant the associated IA controls to reducing risk and increasing systems security.

Chapter Summary

This chapter provided the methodology for determining the most significant IA controls to secure a fuel operation SCADA system against a specific cyber attack. It described the data sources used to populate an attack tree based on a fuels operation. The process of building the attack tree and narrowing down the IA controls associated with specific attacks is described. Then an equation describing probably of attack success was modified in a number of steps to get to the final equation to describe the probability of adversary success. Next, potential limitations to this approach are addressed. Finally, the data analysis procedure was described. The next chapter describes the analysis of data.

IV. Data Analysis

Chapter Overview

This chapter presents an analysis of the survey data collected from the WPAFB fuels operations SMEs. It also examines the probability of adversary success of the five specific attack scenarios. Next, the probability of adversary success from the attack scenarios and the incident impact are combined into a risk matrix. Finally, the risk matrix is analyzed to determine the most influential IA controls in securing the SCADA system.

Survey

Six members of the WPAFB fuels operation and HQ AFMC/A4RE were surveyed to obtain SME rankings on specified incident impacts for a cyber attack on the fuels operation. The following paragraphs analyze and discuss the responses to the WPAFB fuels operations survey. See appendix I for the full survey instrument.

Part I - Demographics

There were four questions in the demographics section. The first question asked how many years of experience does the respondent have in operating or managing fuels industrial control systems. The respondents in the survey all had at least 11 years and the majority had over 21 years of experience, see Figure 12.

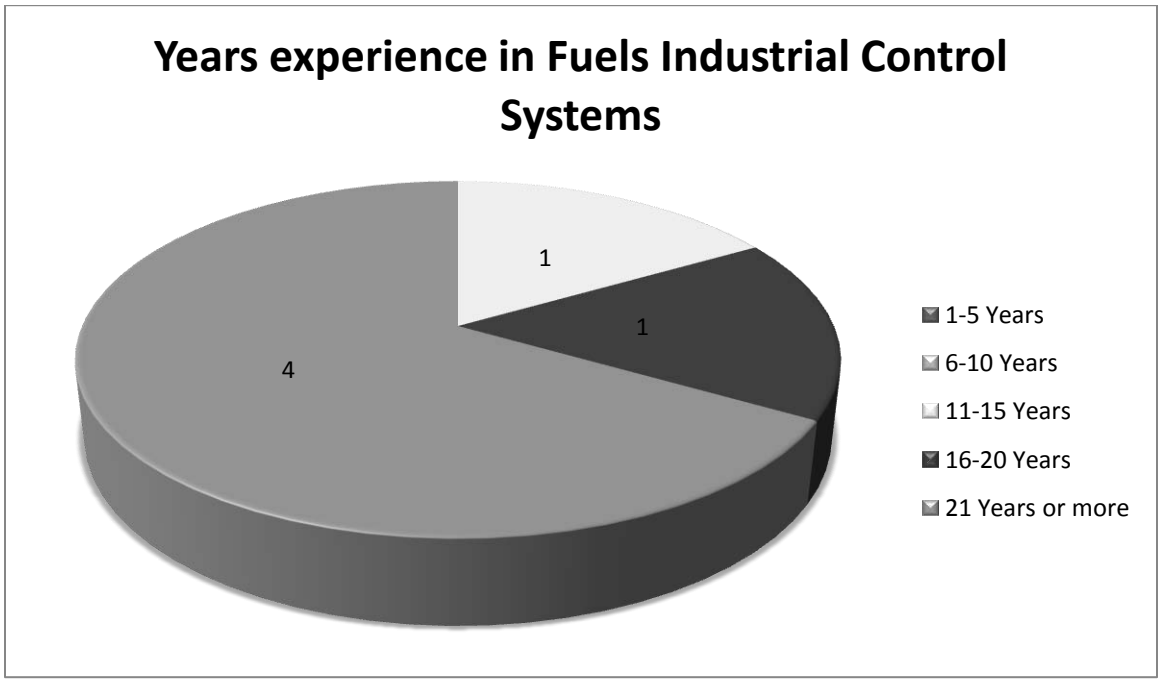


Figure 12. Years experience in Fuels Industrial Control Systems

Question two asked for all computer security or network security training completed in the last five years. Table 11 lists the Computer Security or Network Security Training respondents have received in the last five years. Most of the respondents listed both Information Assurance Awareness and Information Protection training. Only one respondent did not indicate Information Protection training. This is likely an oversight, because it is a requirement in order to use the Air Force network. Respondents did not indicate any additional training outside of annual AF training requirements.

Table 11. Computer Security or Network Security Training in Last 5 Years

Computer Security/Network Security Training	Number
DoD Information Assurance Awareness	6
Information Protection	5
Total	11

Question three asked for a list of all industry certifications successfully completed in the last five years. See Table 12 Industry certifications in last 5 years. The low number of certifications is surprising. One respondent had both the Level I and II Quality Assurance Certifications and another had a Fuels Manager Defense (FMD) 6.0 certification. The Air Force requires quality assurance certifications in order to manage contracted operations. Also, it makes sense a current fuels operator would have an FMD certification. There were four out of the six respondents who listed no industry certifications in the last five years. It may be the case that the respondents have additional certifications they obtained more than five years ago.

Table 12. Industry Certifications in Last 5 Years

Industry Certifications	Number
Level I Quality Assurance Certification	1
Level II Quality Assurance Certification	1
Fuels Manager Defense 6.0	1
Total	3

The final question asks respondents about their primary affiliation with the government. The respondents were evenly split with two civil servants, two military and two contractors. See Figure 13 for Primary Affiliation with Government.

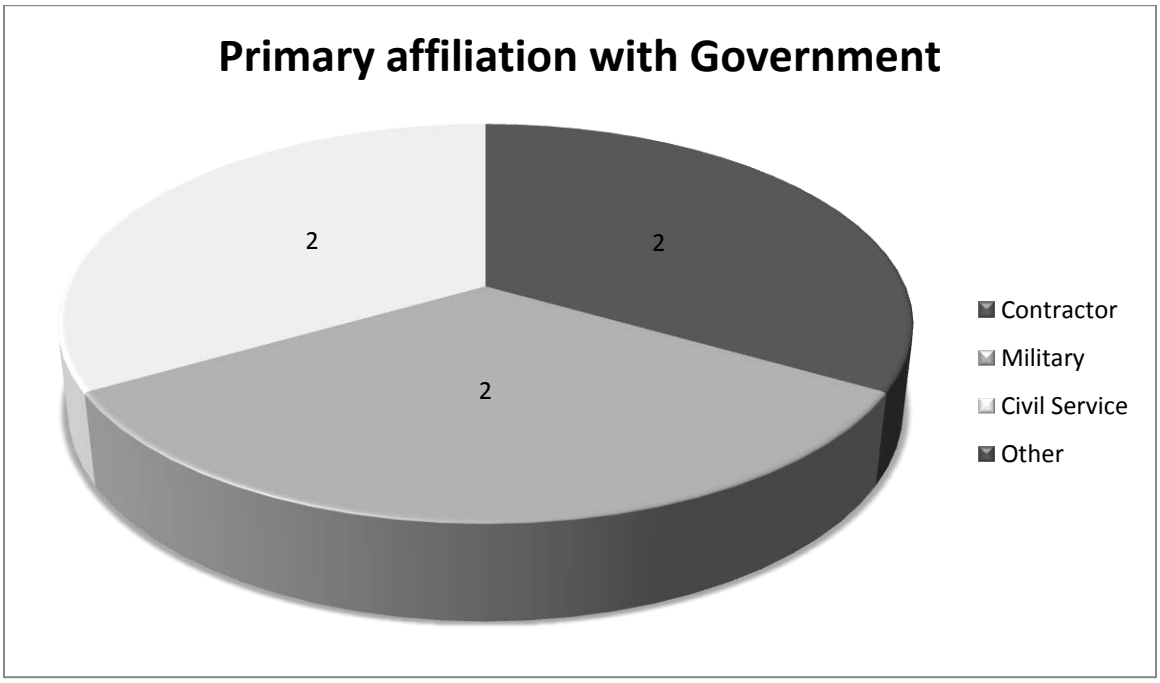


Figure 13. Primary Affiliation with Government

Part II – Impact Rating

This section of the survey asked respondents to rate the impact magnitudes for the five incidents. The incidents were rated as Low, Medium or High impact. The definitions for these ratings were taken directly from NIST 800-30 Risk Management Guide for Information Technology systems, page 23. The mode is also displayed for each incident. See Table 13. Incident Impact Ratings.

Table 13. Incident Impact Ratings

Incident Impacting the Fuels Mission	Respondent (Low, Med, High)						Mode
	1	2	3	4	5	6	
Alter Fuels Manager Defense (FMD) database data	L	H	M	H	H	H	H
Alter FMD real time Human-Machine Interface (HMI) data	M	M	M	M	H	H	M
Cause the FMD computer hard drive to crash	L	H	M	M	M	L	M
Transmit a false report to the Fuels Enterprise System	L	M	M	M	M	L	M
Disrupt FMD Communications	L	M	L	L	M	M	L/M

Part III – Impact Category refinement

This section of the survey asked respondents to further score the incident impact within the rating they assigned in Part II. Scores were assigned in the following guidelines: Low impact (1 to 10), Medium impact (11 to 50), High impact (51 to 100). Respondents were to take into account all other events that can occur in that magnitude of impact category. These scores are averaged in the rightmost column of Table 14.

Table 14 shows the fuels SMEs rated almost all incidents medium with one high. The data shows that the respondents put a high degree of importance on the accuracy of the data in their database. The impact of real-time data on the HMI and the computer hard drive failure averaged to medium. Lastly, the respondents attach a much lower importance on the accuracy of data in and communications to systems external to their own. This concludes the analysis of the survey, the next section discusses reduction of IA controls in the attack tree.

Table 14. Incident Impact Scores

Incident Impacting the Fuels Mission	Respondent Impact (Low, Med, High)						Average Rating
	1	2	3	4	5	6	
Alter Fuels Manager Defense (FMD) database data	10	80	50	100	70	60	61.7
Alter FMD real time Human-Machine Interface (HMI) data	35	30	50	15	75	75	46.7
Cause the FMD computer hard drive to crash	10	85	50	45	40	5	39.2
Transmit a false report to the Fuels Enterprise System	3	20	50	40	25	5	23.8
Disrupt FMD Communications	3	40	10	5	15	20	15.5

Reduction of IA controls in attack tree

In building the attack tree, some of the IA controls were eliminated either because they were not implemented by the WPAFB fuels operation, or because the particular attack was not impacted by the IA control. For instance, at the time of this research, the wireless point of sale devices were non-operational. Therefore the wireless IA control was not considered. Also, since this research focuses on a specific type of cyber attack, any IA controls associated with physical security and breach of trust were not considered as well. This process eliminated 14 IA Controls, see Table 15. IA Controls Eliminated for non-applicability.

Table 15. IA Controls Eliminated for Non-applicability

Management Controls
Planning
Operational Controls
Personnel Security
Physical and Environmental Protection
Control Center/Control Room
Portable Devices
Cabling
Contingency Planning
Disaster Recovery Planning
Media Protection
Technical Controls
Physical Token Authentication
Virtual Local Area Network
Wireless
Encryption
Virtual Private Network

Specific attack scenarios were chosen which broadly matched attacks listed in the SANS (SysAdmin, Audit, Network, Security) Institute top 20 security risks for 2007 (Safier, Rouse, Paller, Kotkov, Sarwate, Skoudis, et al., 2007). The probability of adversary success for each of these attack scenarios will form the Y-axis of the risk matrix. The specific attack tree leaf node actions were examined within the five chosen cyber attacks. See Appendix F for Leaf Node, Effect Mapping for mapping of attack tree vulnerabilities to attacker effects.

After eliminating IA controls that are not applicable, the remaining IA controls which are associated with the 5 cyber attack scenarios are listed in Table 16.

Table 16. IA Controls Associated with 5 Cyber Attack Scenarios

Management Controls
Risk Assessment
System and Service Acquisition
Certification, Accreditation, and Security Assessments
Operational Controls
Configuration Management
System and Information Integrity
Malicious Code Detection
Intrusion Detection and Prevention
Patch Management
Incident Response
Awareness and Training
Technical Controls
Identification and Authentication
Password Authentication
Role-Based Access Control
Web Servers
Dial-up Modems
Audit and Accountability

Attack Tree Analysis

The five attack scenarios were derived from the Reduced Base Stuxnet Attack Tree in the SecureITree software. See Appendix C for Reduced Base Stuxnet Attack Tree. The probability of adversary success at the root node and the eight major sub-trees were calculated, see Table 17. A number of observations emerge from the calculated probability of adversary success values. One, the variability between the highest scenario probability and the lowest is .13 on a 0 to 1 point scale. So the probabilities of all of the 5 scenarios fall within a small 13% band of the scale. Looking at the major sub-trees for all of the attack scenarios, there is a significant range in values from the lowest to the highest probability. For all the attack scenarios the range is .9219, which covers approximately 92% of the scale. Finally, most of the major sub-trees within the attack scenarios when compared to each other have little variability. This is a product of the how

the attack tree was created. Many of the major sub-trees have only AND nodes, or few OR nodes which dramatically reduces the potential values of the probability of adversary success of that sub-tree.

Table 17. Probability of Adversary Success of Specific Attacks

Attack Scenario	Probability of Adversary Success per Major Sub-tree								Overall Probablity of Adversary Success
	Select Exploit	Reconnaissance	Scanning	Gain Access	Deploy Exploit	Covering Tracks and Concealment	Maintain Access	Execute Exploit	
Step 7 Project Files	0.1000	0.3515	0.4863	0.0781	0.4910	0.2769	0.3840	1.0000	0.3960
Vulnerable WinCC	0.1000	0.4930	0.4863	0.0781	0.0540	0.2769	0.3840	0.5075	0.2975
Print Spooler	0.1000	0.3515	0.4863	0.0781	0.0540	0.2769	0.3840	1.0000	0.3414
Server Service	0.1000	0.4930	0.4863	0.0781	0.4910	0.2769	0.3840	1.0000	0.4137
Network Shares	0.1000	0.3515	0.4863	0.0781	0.0540	0.2769	0.3840	1.0000	0.3414

The IA controls which influenced the success of the five attack scenarios are listed in Table 18. For the specific implementation at the WPAFB fuels operation, these 16 IA controls influence the success of the five attack scenarios.

Table 18. IA Controls Influential in Securing against Remote Cyber Attack

Management Controls
Risk Assessment
System and Service Acquisition
Certification, Accreditation, and Security Assessments
Operational Controls
Configuration Management
System and Information Integrity
Malicious Code Detection
Intrusion Detection and Prevention
Patch Management
Incident Response
Awareness and Training
Technical Controls
Identification and Authentication
Password Authentication
Role-Based Access Control
Web Servers
Dial-up Modems
Audit and Accountability

Risk Level Matrix

The responses from Part III – Impact Category Refinement of the survey and the probability of adversary success from the attack trees of the five attack scenarios were combined into the Risk Level Matrix, Figure 14. In the matrix, all of the risk values lie in the medium-medium area of the graph except attack #1, which falls into the high-medium area. The IA controls associated with the actions of all the attack scenarios have very little variation, so it is difficult to draw meaningful information about the significance of IA controls from this Risk Level Matrix. In order draw a meaningful result, it is necessary to break the attack scenarios apart into the major sub-trees in a modified risk level matrix.

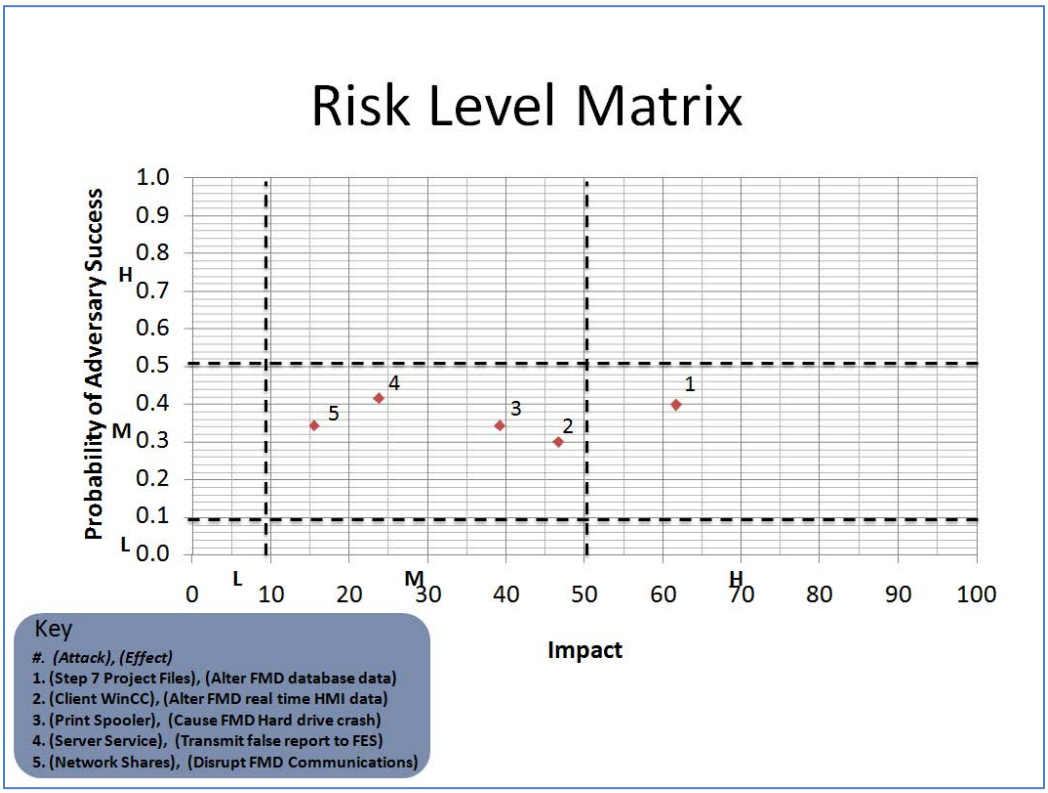


Figure 14. Risk Level Matrix

The probabilities of the major sub-trees of the attack scenarios were graphed separately in Figure 15. Modified Risk Level Matrix.

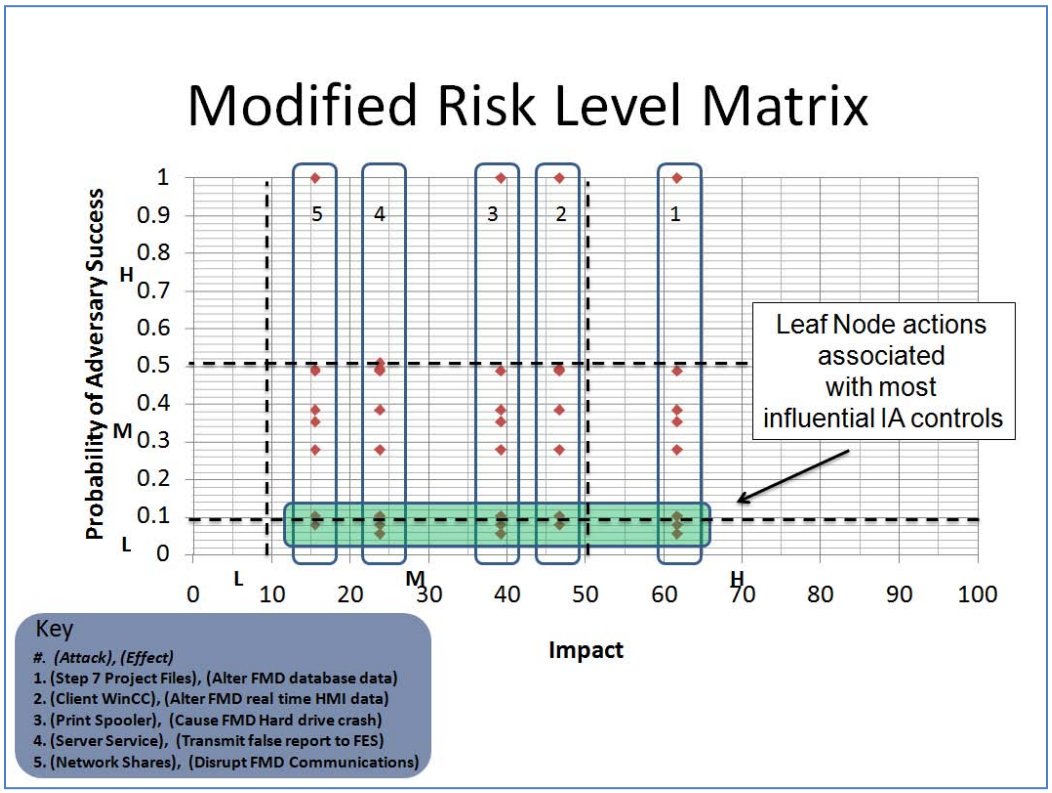


Figure 15. Modified Risk Level Matrix

When broken into its constituent parts, there is much variability in the probability of adversary success values of the major sub-trees. Also, some of the actions are not possible for the victim to defend against. For instance, the select exploit sub-tree has a very low probability of adversary success, but provides no data regarding the strength of IA controls. There are no IA controls that affect the adversary in this case because all of the actions the adversary takes are separate from the target network and organization. For the sub-trees that do have IA controls associated with them, the lower the probability of adversary success, the more significant the IA control is to defending the system. The tasks and IA controls that fall into the low portion of the risk level matrix are the most significant in defending the system. In Figure 15, the area shaded in green contains the major sub-trees that contain the most influential IA controls. The gain

access and deploy exploit are the only sub-trees that fall within the low area on the Modified Risk Matrix, see Figure 16.

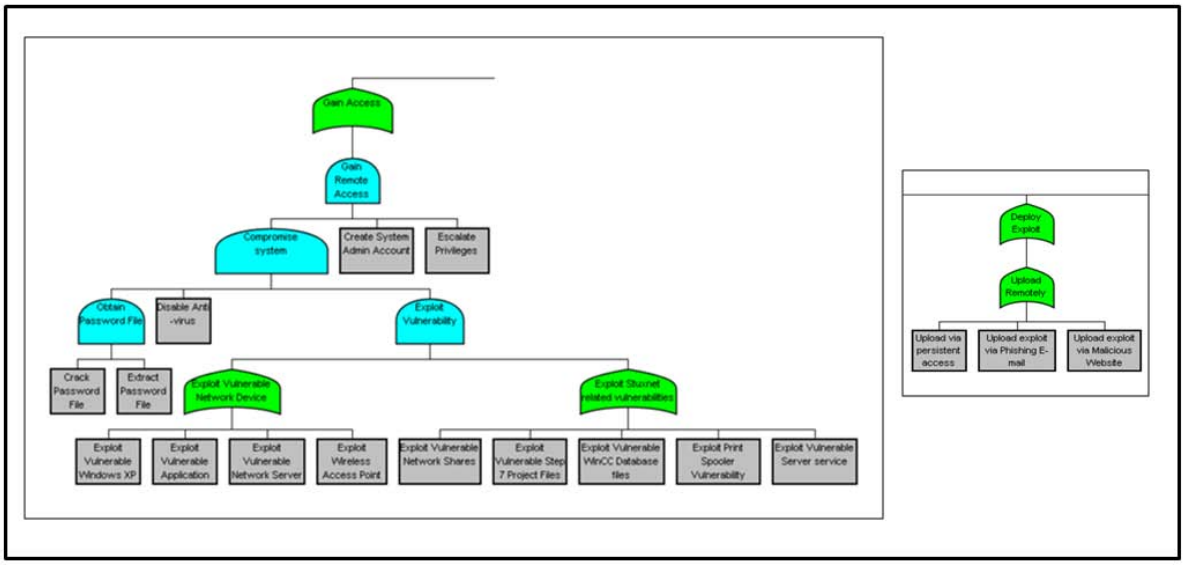


Figure 16. Gain Access and Deploy Exploit major sub-trees

The 14 most influential IA controls in securing the fuels SCADA system against a Stuxnet-like attack are listed in Table 19. Most Influential IA Controls.

Table 19. Most Influential IA Controls

Management Controls
Risk Assessment
Certification, Accreditation, and Security Assessments
System and Service Acquisition
Operational Controls
Awareness and Training
Configuration Management
Incident Response
Intrusion Detection and Prevention
Malicious Code Detection
Patch Management
System and Information Integrity
Technical Controls
Audit and Accountability
Identification and Authentication
Password Authentication
Role-Based Access Control

Chapter Summary

This chapter presented an analysis of the data collected in the WPAFB fuels operations SMEs survey. It then examined the probability of adversary success of the five specific attack scenarios. These two sets of values were then combined to create the X and Y axis of the risk level matrix. The risk matrix was then analyzed to determine the most influential IA controls in securing the SCADA system. The next chapter describes conclusions and recommendations for future work.

V. Conclusions and Recommendations

Conclusions

This research provided insight into which IA controls are most significant for network defenders and SCADA systems managers/operators to focus on in order to ensure the security of critical infrastructures against a Stuxnet-like exploit. An attack tree was built based on the WPAFB fuels operation. The attack tree was populated with IA controls which were then associated with leaf node actions. System security effectiveness values and the probability of attack success was determined for each leaf node and applied to the attack tree. The overall probability of adversary success for the five specific attack scenarios were determined using SecureITree software. The incidents associated with the five specific attack scenarios were rated by AF fuels operation SMEs. Finally, the probability of adversary success and SME impact were incorporated into a risk level matrix. The risk level matrix provided additional insight into the most significant IA controls.

All actions in the attack tree are not necessary to achieve a successful attack. Certain sets of leaf node actions are more significant to achieving success than others. The probability of success of a critical sub-tree of a cyber attack is a significant indicator of the overall probability of adversary success. A critical sub-tree with a low probability of success was the limiting factor of the five specific attack scenarios. Barring physical access or insider assistance/knowledge, a cyber attack is not possible without the exploitation of a vulnerability, therefore the IA controls that deal with preventing an attacker from gaining access are very significant to the security of the SCADA system. This research shows that the key actions of a remote cyber attack is gaining access to the target computer via the exploitation of a vulnerability and deploying malicious

code. The IA controls associated with these leaf node actions are the most influential IA controls.

The results of this study are useful for managers who make the ultimate decision on which IA controls provide the greatest return on investment in securing a SCADA system. If an organization cannot implement all of the IA controls, they should focus on controls listed in Table 20. in order to protect against a Stuxnet-like cyber attack.

Table 20. Most influential IA Controls

Management Controls
Risk Assessment
Certification, Accreditation, and Security Assessments
System and Service Acquisition
Operational Controls
Awareness and Training
Configuration Management
Incident Response
Intrusion Detection and Prevention
Malicious Code Detection
Patch Management
System and Information Integrity
Technical Controls
Audit and Accountability
Identification and Authentication
Password Authentication
Role-Based Access Control

The IA controls have been designed primarily to address IT systems security issues. SCADA systems are slowly transitioning toward IT-like systems, but the move has not fully occurred. Caution is warranted when introducing these solutions to a SCADA environment and

they may need to be specially trailed in order to work properly (Stouffer et al., 2008). Therefore the operational reality facing SCADA operators makes implementation of a number of the most influential IA controls listed in Table 20 problematic. SCADA operators are less likely to fully implement patch management, role-based access controls, malicious code detection, and intrusion detection and prevention. According to a number of ICS security assessment conducted by DHS (2009), poor patch management and weak authentication were among the top ICS software vulnerabilities observed. This indicates that SCADA operators are less inclined to implement proper patch management and role-based access controls. Furthermore, there is concern that the malicious code detection IA control will cause latency due to computational overhead affecting the real-time performance of SCADA systems. Also, that updating virus signatures further exposes the SCADA system to attacks from the Internet (Krutz, 2006). Finally, it is unlikely the intrusion detection and prevention IA control will be implemented in an effective manner because most IDS' are not capable of monitoring SCADA protocols for suspicious behaviors (Stamp, Campbell, Depoy, Dillinger & Young, 2004).

The research methodology applied in this study is a sound approach to identify which IA controls are most influential to SCADA system security. The methodology partially addresses the future work described by Igure (2007) to find relative risks of the various vulnerabilities of the system. The methodology also incorporates factors called for by Byres et al. (2004) to use an attack tree to aggregate subordinate node values and site specific parameters such as known vulnerabilities and countermeasures. In Mendezllovet's (2010) research in codifying IA controls for DOD SCADA systems, there was perfect agreement among survey respondents that certification and accreditation was ranked last as an effective IA control. They also ranked encryption as a high technical control. He suspected there is a disconnect in how the CE and IT

communities view the relative importance of these controls. This research shows that certification and accreditation is important in defending against a cyber attack. Similarly, encryption was not found to be a significant IA control in defending against a cyber attack. This study shows evidence supporting his suspicion of a disconnect of the ranking of IA controls within the IT and CE communities.

Recommendations for Future Research

Based on known limitations and current constraints, four extensions of this study are proposed. One potential extension of this research is to conduct research on a SCADA operation where the AIS is more tightly integrated into the physical control mechanisms of the operation. An examination of such an operation might produce a greater range of risk and may include the IA controls that were not included in this study. Also, as a related item, a metric that describes the degree to which a SCADA system is coupled into the physical infrastructure could be developed.

A second research option is to focus on the remote aspects of other cyber attacks. There is an opportunity to apply other known cyber exploits in a similar manner using the same methodology. Additionally, the study of physical access components of an attack would show which IA controls are most significant to physical security.

A third extension is to take the attack tree developed in this research and refine it by including a source of data to more objectively assign values to both the system security effectiveness and the probability of attack success. Also, the addition of more technical details may answer technical issues related to securing SCADA systems.

Finally, another researcher could take the results and extend them to fuels operations across the DOD or other critical infrastructures. The inclusion of commercial industry, proprietary data would assist in extrapolating to a more general case.

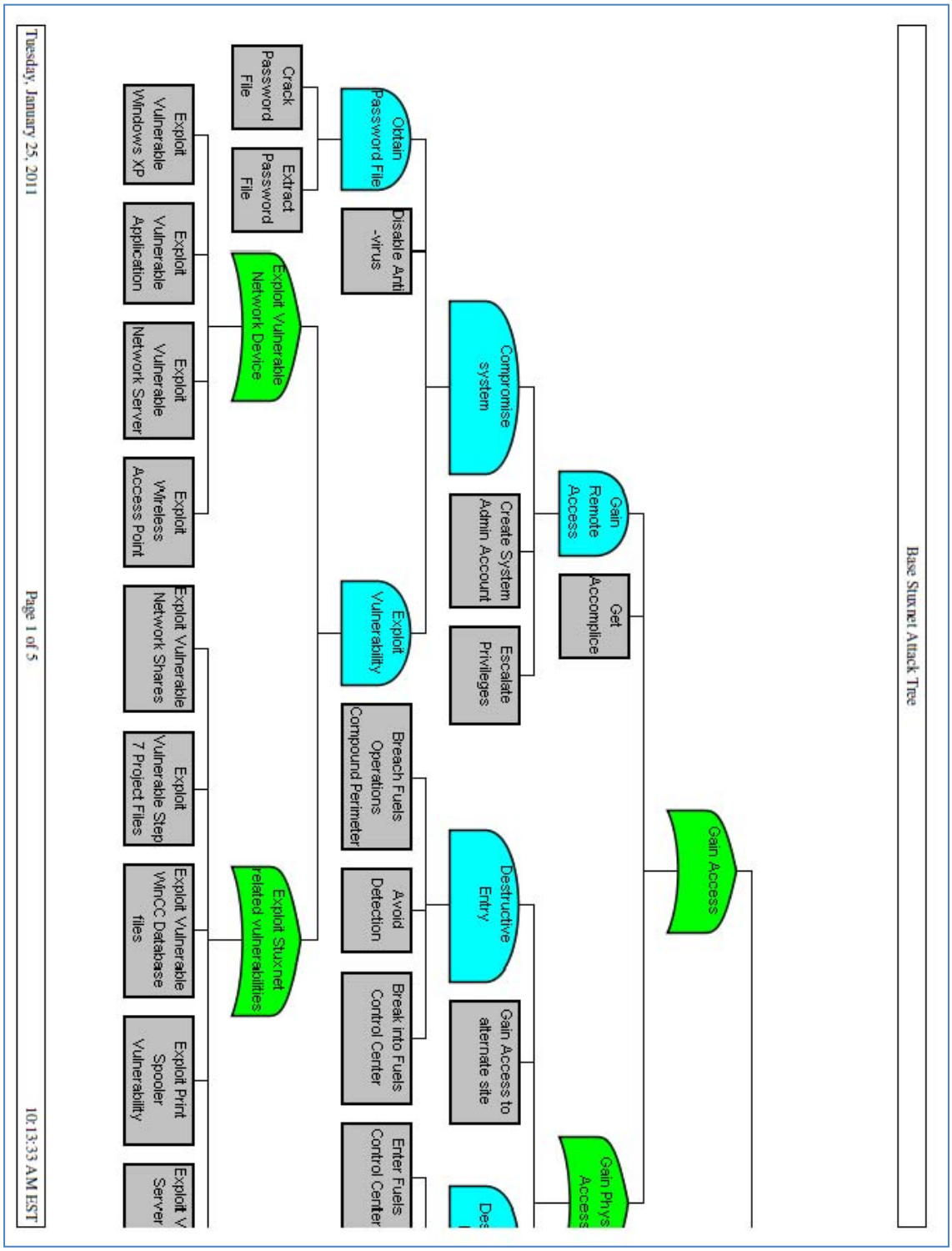
Summary

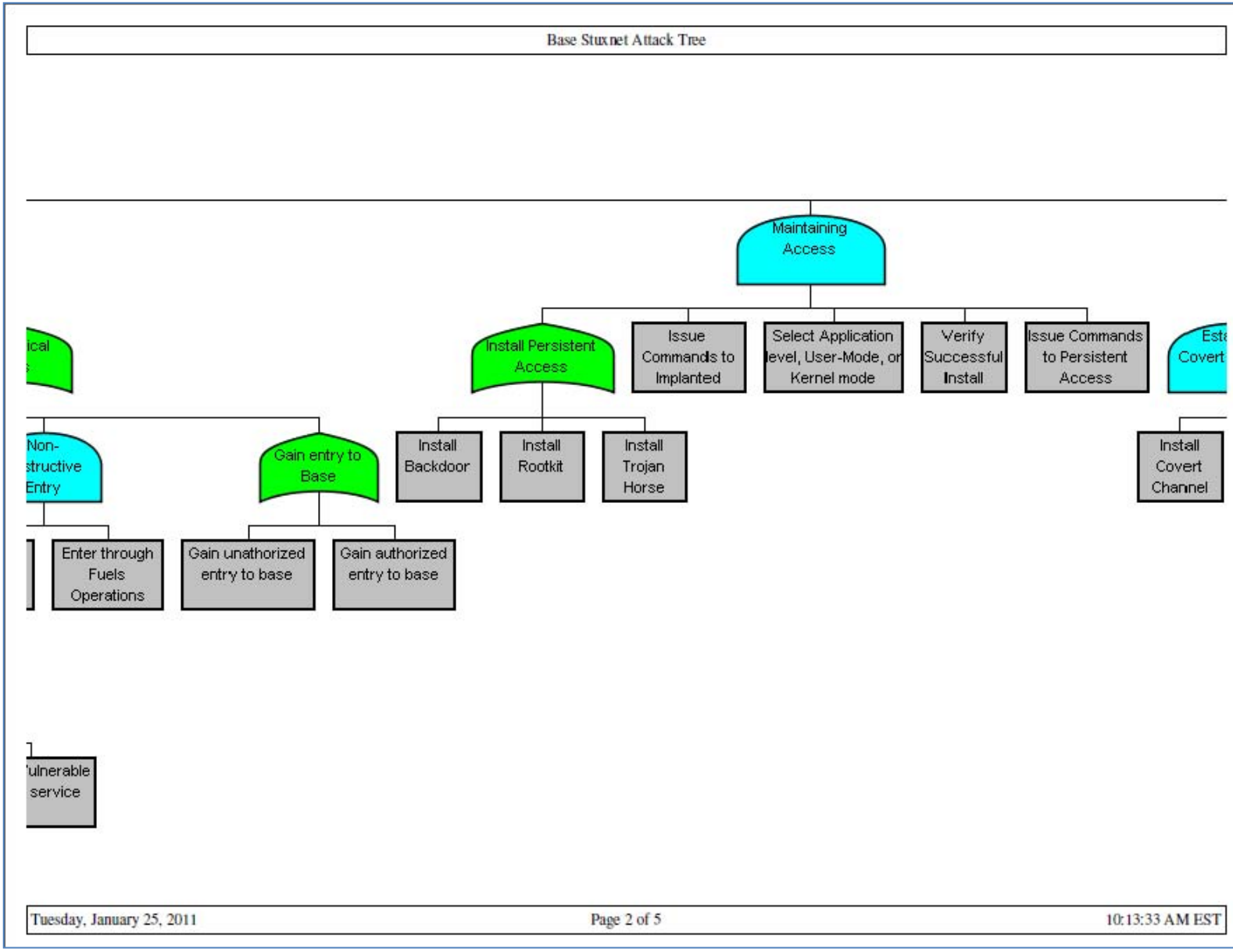
This research showed which IA controls are most influential for network defenders and SCADA system managers and operators to focus on in order to ensure the security of critical infrastructures against a Stuxnet-like exploit. Since this attack vector is the most advanced exploit found to date against critical infrastructure, this research is timely and relevant in identifying the critical IA controls which are most effective in preventing a successful attack. Just as significant the methodology used in this research is a sound approach to answering questions about system security. It provides a broadly applicable and flexible framework to answer other systems security questions for both IT and SCADA systems with only minor modification.

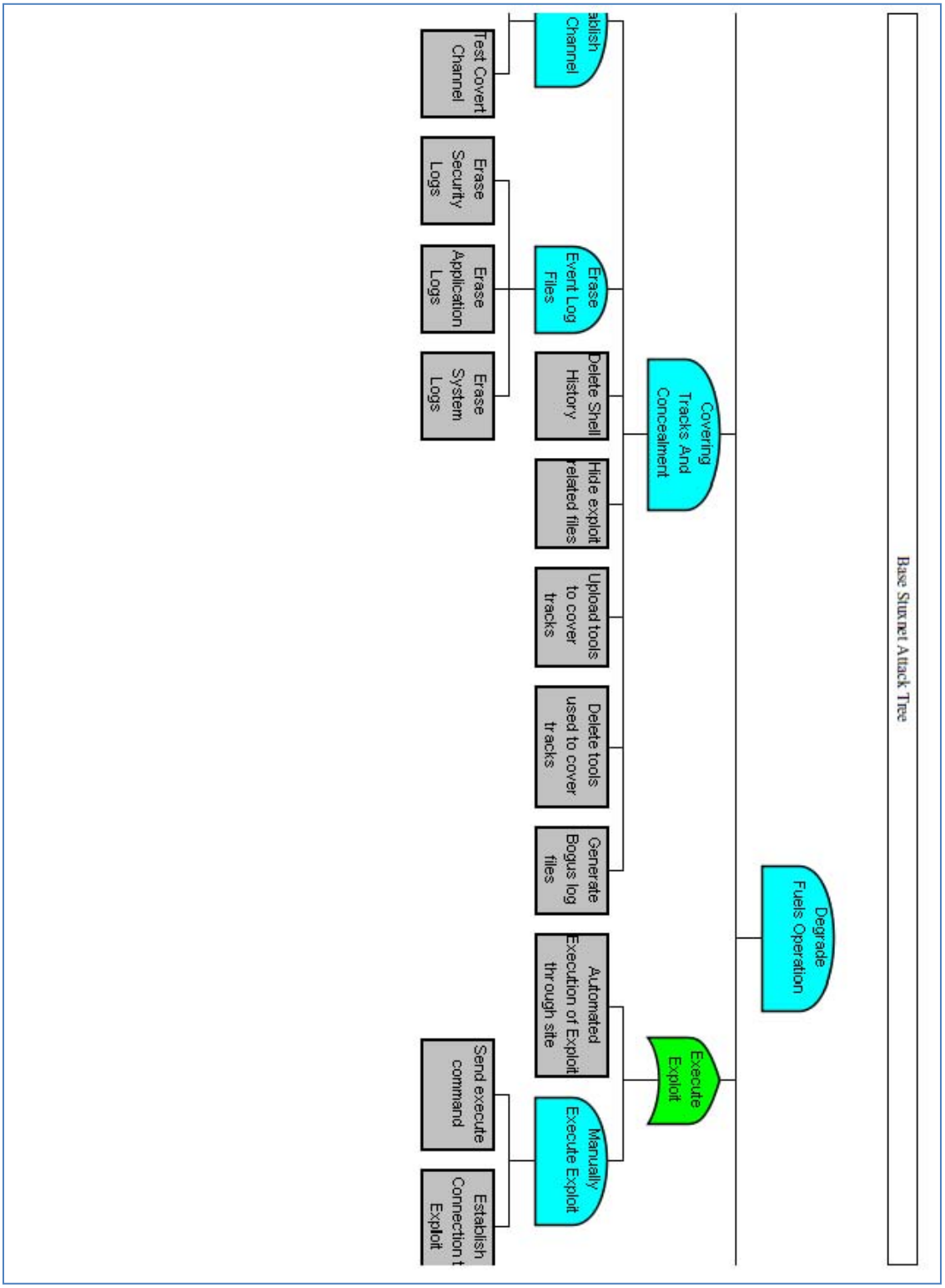
Appendix A: Roles and Responsibilities of Sector-Specific Federal Agencies (Bush, 2003)

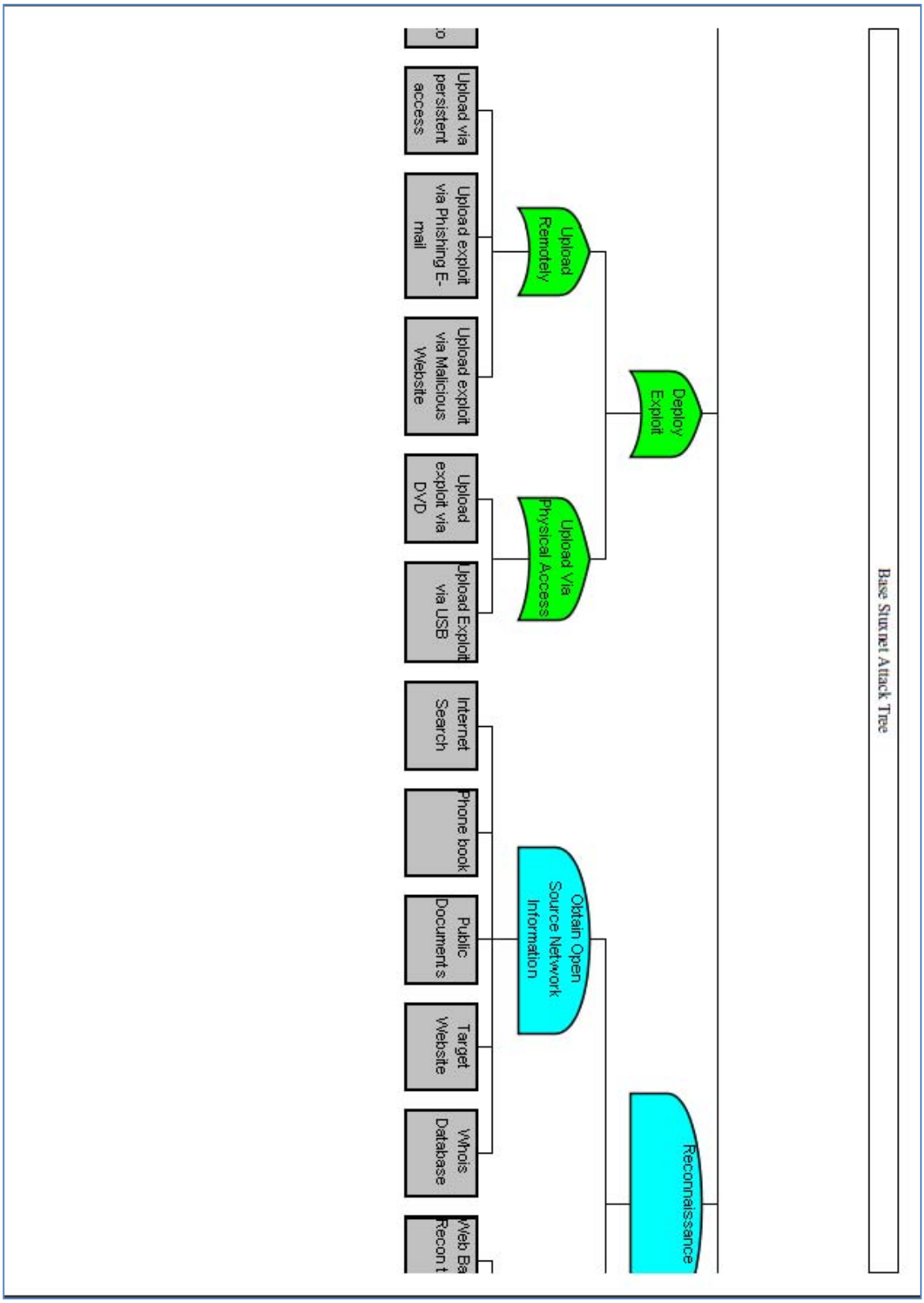
Federal Agency	Sector
Department of Agriculture	Agriculture, food (meat, poultry, egg products)
Health and Human Services	Public health, healthcare, and food (other than meat, poultry, egg products)
Environmental Protection Agency	Drinking water and water treatment systems
Department of Energy	Energy, including the production refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear power facilities
Department of the Treasury	Banking and finance
Department of the Interior	National monuments and icons
Department of Defense	Defense industrial base

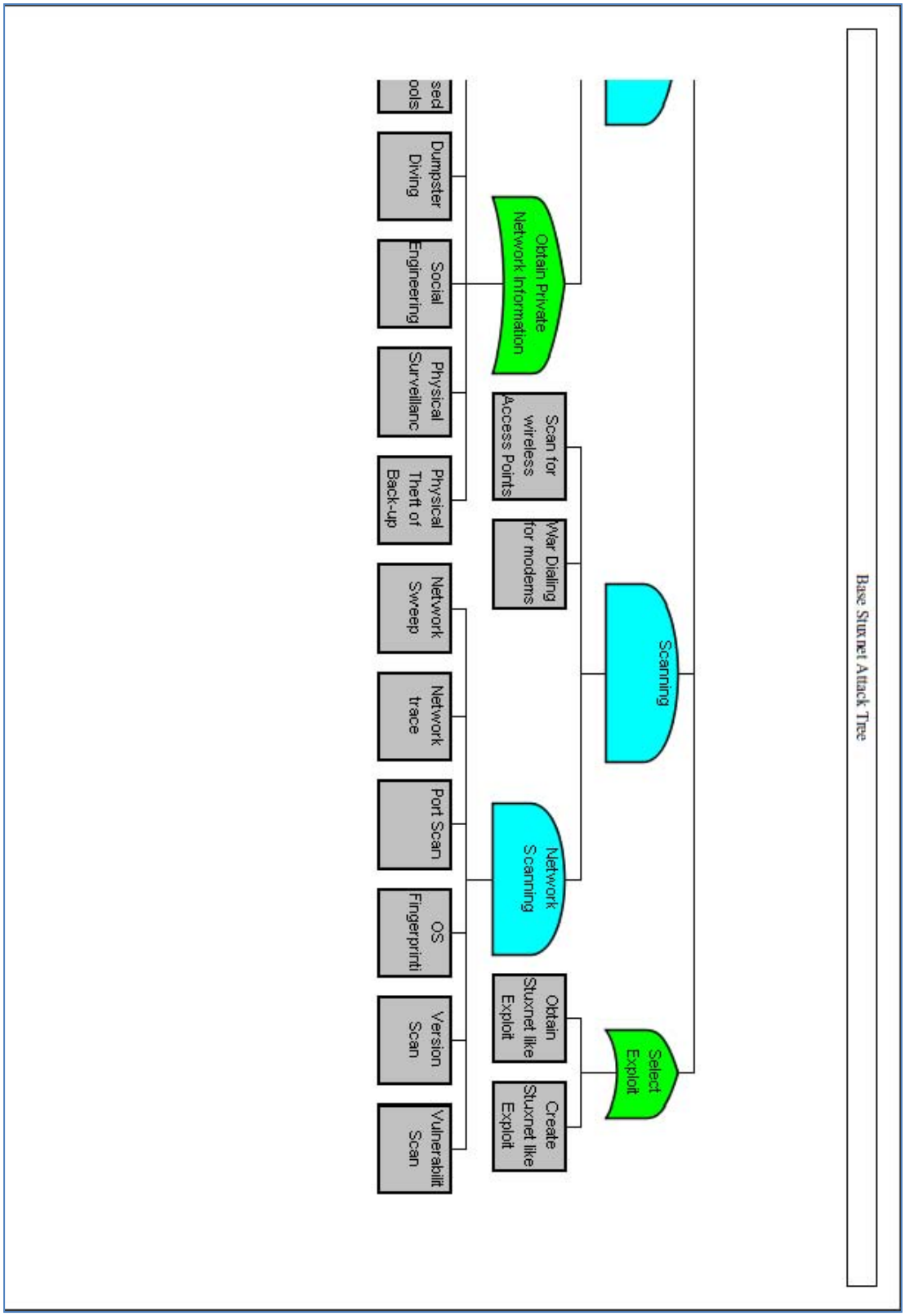
Appendix B: Base Stuxnet Attack Tree



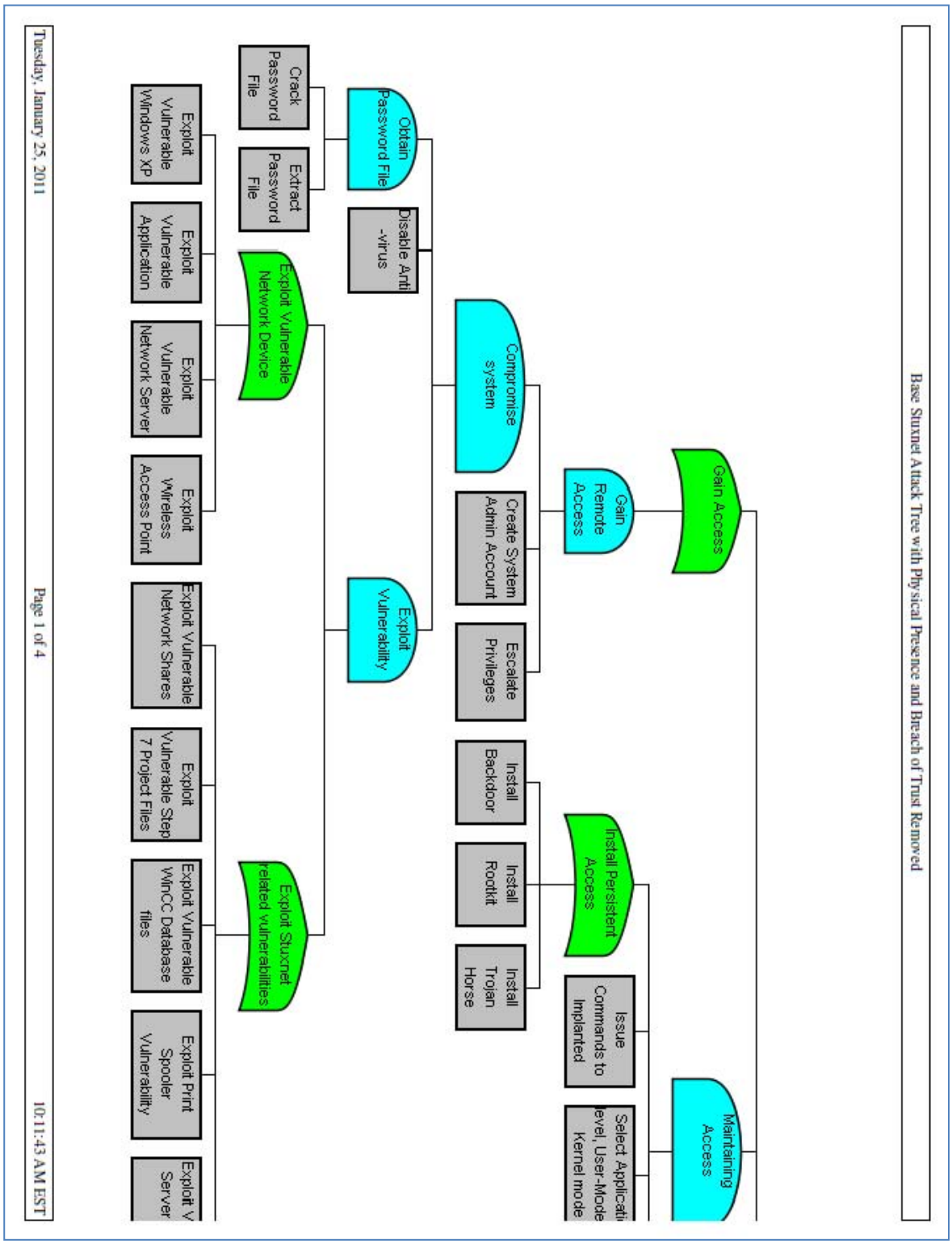

Base Stuxnet Attack Tree
Maintaining Access
ical
Install Persistent Access
Issue Commands to Implanted
Select Application level, User-Mode, or Kernel mode
Verify Successful Install
Issue Commands to Persistent Access
Este
Covert
Non-structive Entry
Gain entry to Base
Install Backdoor
Install Rootkit
Install Trojan Horse
Install Covert Channel
Enter through Fuels Operations
Gain unathorized entry to base
Gain authorized entry to base
ulnerable service
Tuesday, January 25, 2011
Page 2 of 5
10:13:33 AM EST

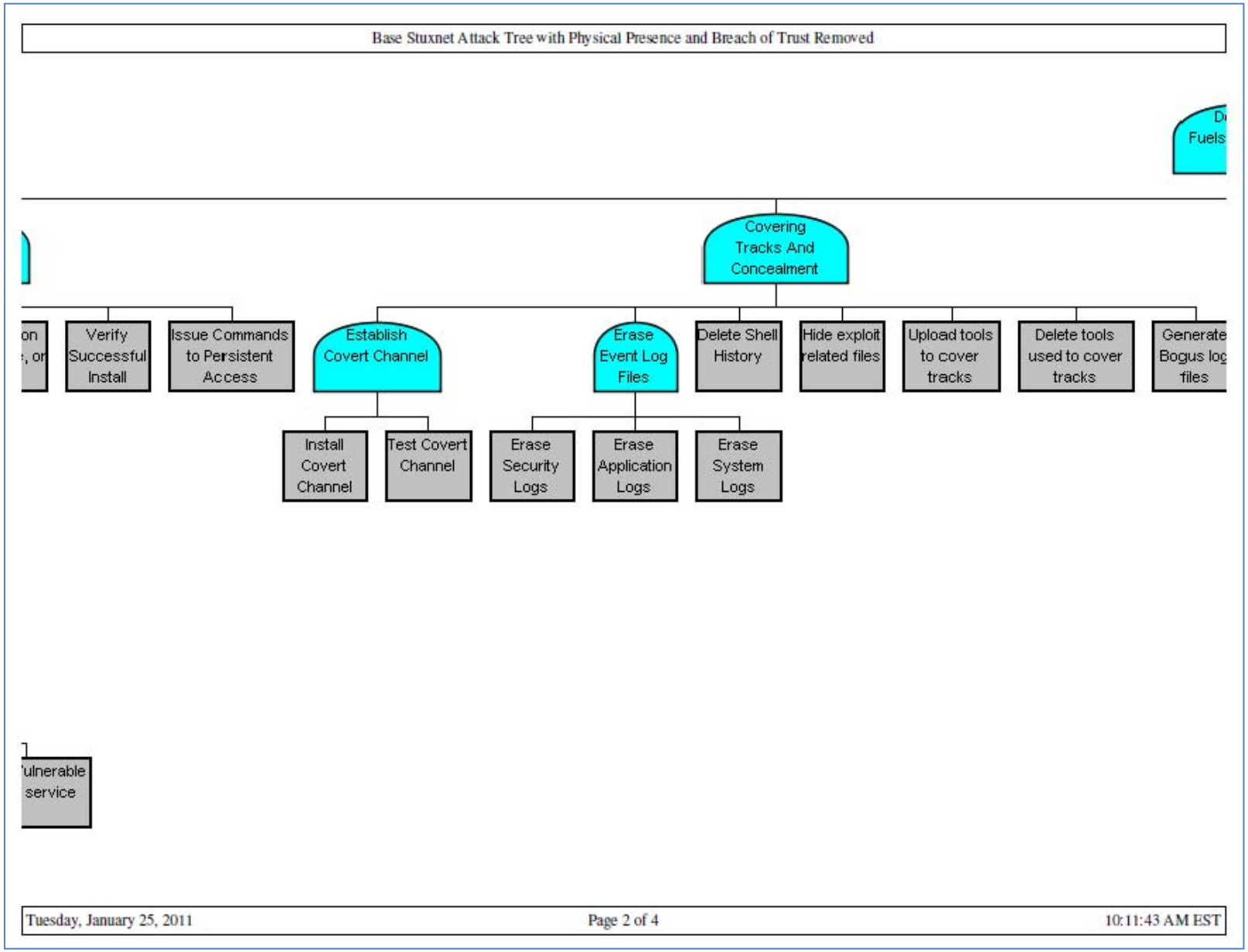

Base Stuxnet Attack Tree
Degrade Fuels Operation
Execute Exploit
Covering Tracks And Concealment
Automated Execution of Exploit through site
Manually Execute Exploit
Delete Shell History
Hide exploit related files
Upload tools to cover tracks
Delete tools used to cover tracks
Generate Bogus log files
Erase Event Log Files
Erase Security Logs
Erase Application Logs
Erase System Logs
ablish Channel
Test Covert Channel
Send execute command
Establish Connection t Exploit

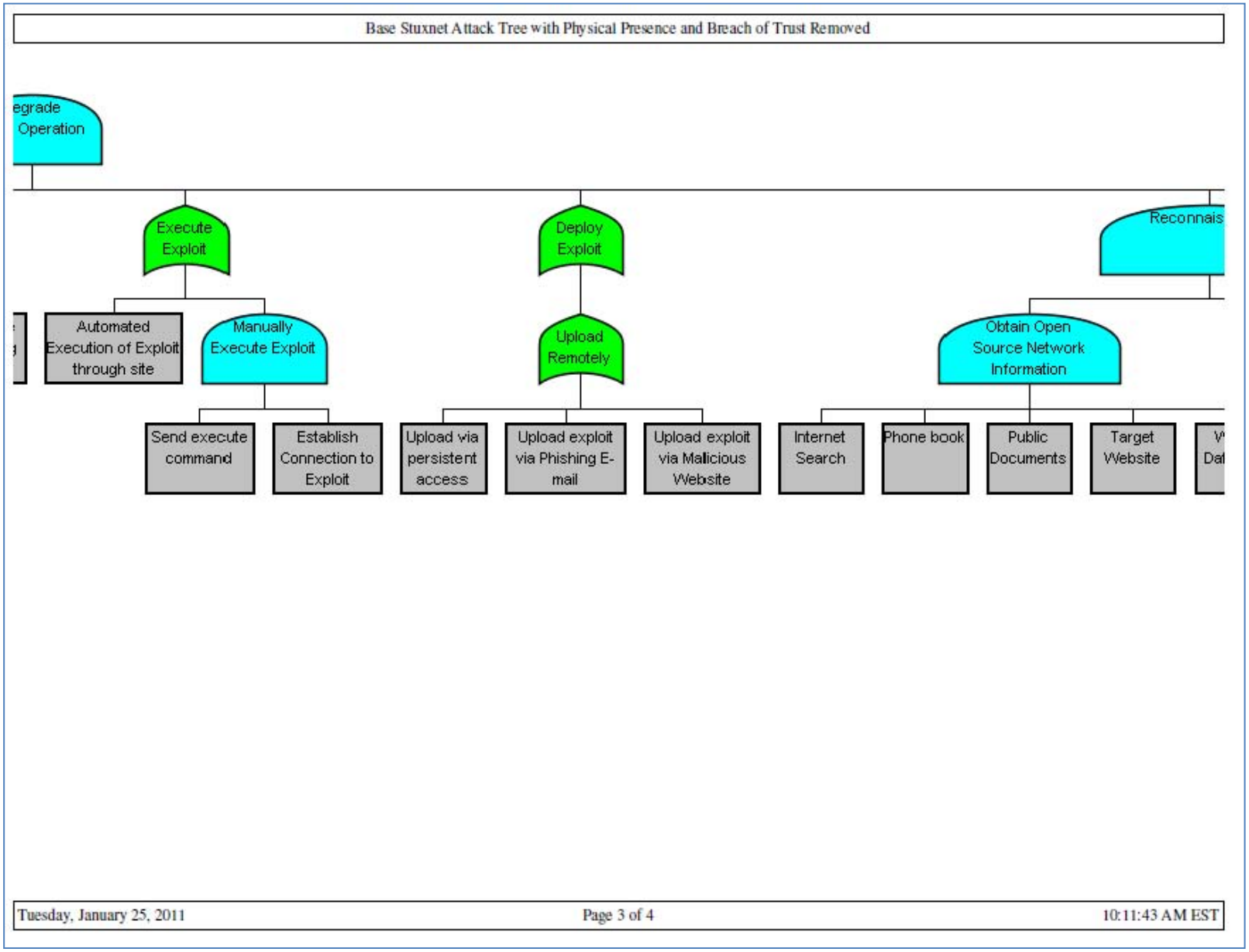

Base Stuxnet Attack Tree
Reconnaissance
Obtain Open Source Network Information
Whois Database
Target Website
Public Documents
Phone book
Internet Search
Deploy Exploit
Upload Via Physical Access
Upload Exploit via USB
Upload exploit via DVD
Upload Remotely
Upload exploit via Malicious Website
Upload exploit via Phishing E-mail
Upload via persistent access


Base Stuxnet Attack Tree
Scanning
Select Exploit
Obtain Private Network Information
Network Scanning
Obtain Stuxnet like Exploit
Create Stuxnet like Exploit
Scan for wireless Access Points
War Dialing for modems
Physical Surveillanc
Physical Theft of Back-up
Social Engineering
Dumpster Diving
sed ools
Network Sweep
Network trace
Port Scan
OS Fingerprinti
Version Scan
Vulnerabilit Scan

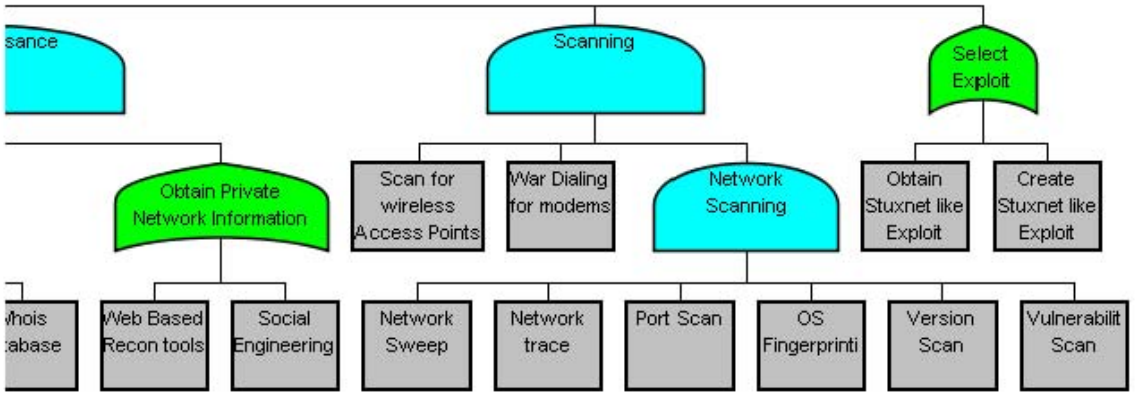
Appendix C: Reduced Base Stuxnet Attack Tree




Base Stuxnet Attack Tree with Physical Presence and Breach of Trust Removed
Fuels
Covering Tracks And Concealment
Verify Successful Install
Issue Commands to Persistent Access
Establish Covert Channel
Erase Event Log Files
Delete Shell History
Hide exploit related files
Upload tools to cover tracks
Delete tools used to cover tracks
Generate Bogus log files
Install Covert Channel
Test Covert Channel
Erase Security Logs
Erase Application Logs
Erase System Logs
service
Tuesday, January 25, 2011
Page 2 of 4
10:11:43 AM EST

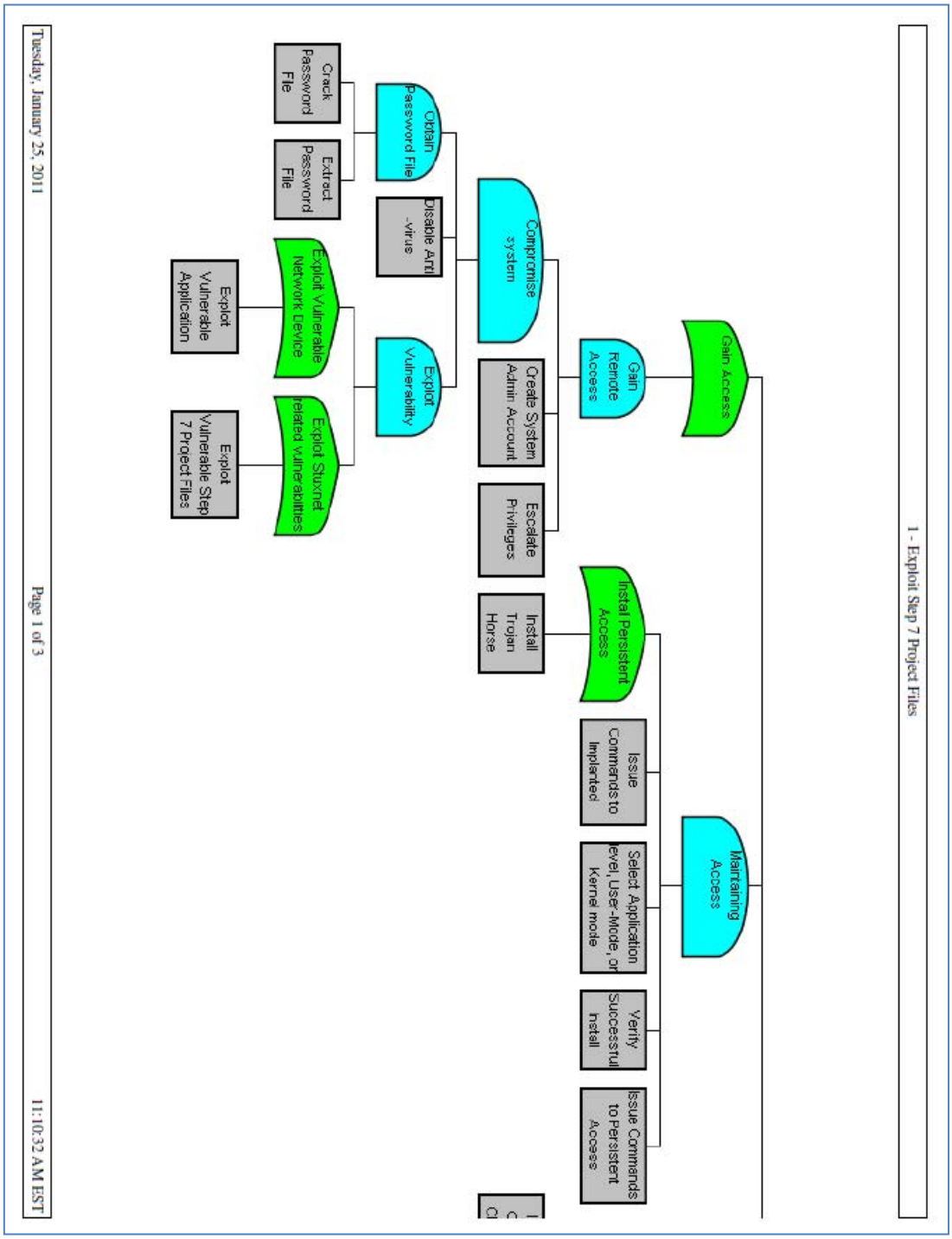

Base Stuxnet Attack Tree with Physical Presence and Breach of Trust Removed
egrade Operation
Execute Exploit
Deploy Exploit
Reconnais
Automated Execution of Exploit through site
Manually Execute Exploit
Upload Remotely
Obtain Open Source Network Information
Send execute command
Establish Connection to Exploit
Upload via persistent access
Upload exploit via Phishing E-mail
Upload exploit via Malicious Website
Internet Search
Phone book
Public Documents
Target Website
Tuesday, January 25, 2011
Page 3 of 4
10:11:43 AM EST

Base Stuxnet Attack Tree with Physical Presence and Breach of Trust Removed

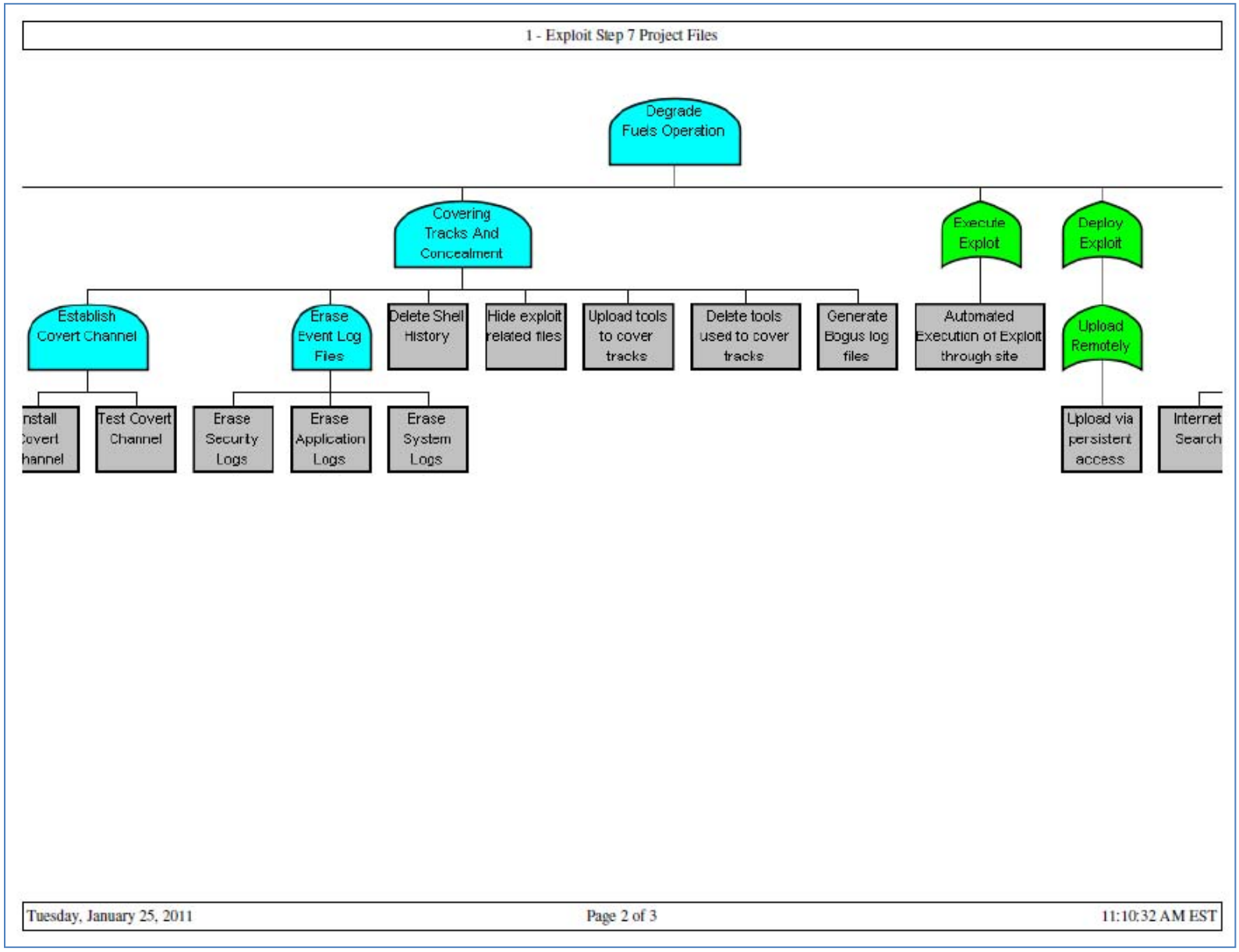


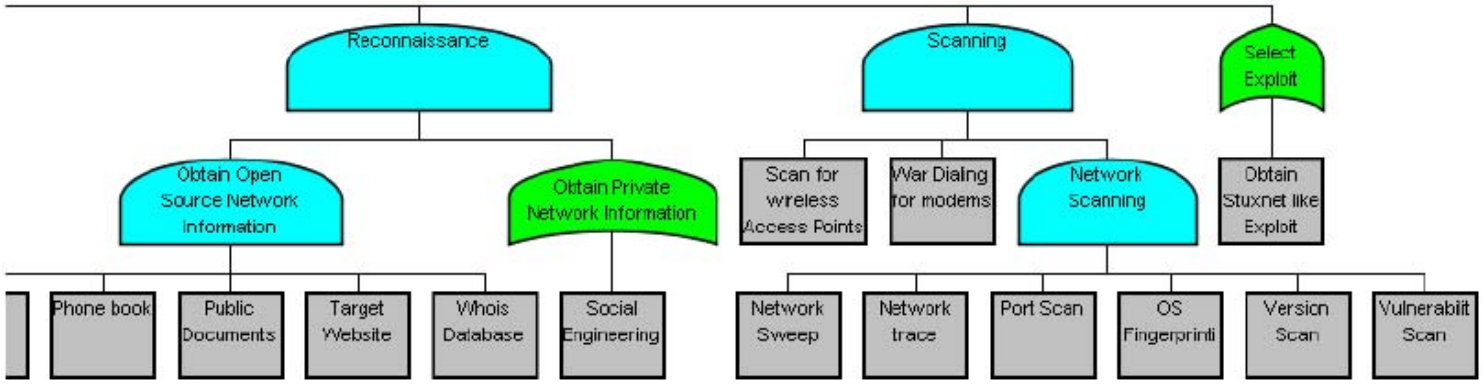
Appendix D: Five Chosen Attack Scenarios

Step 7 Project Files Attack Scenario

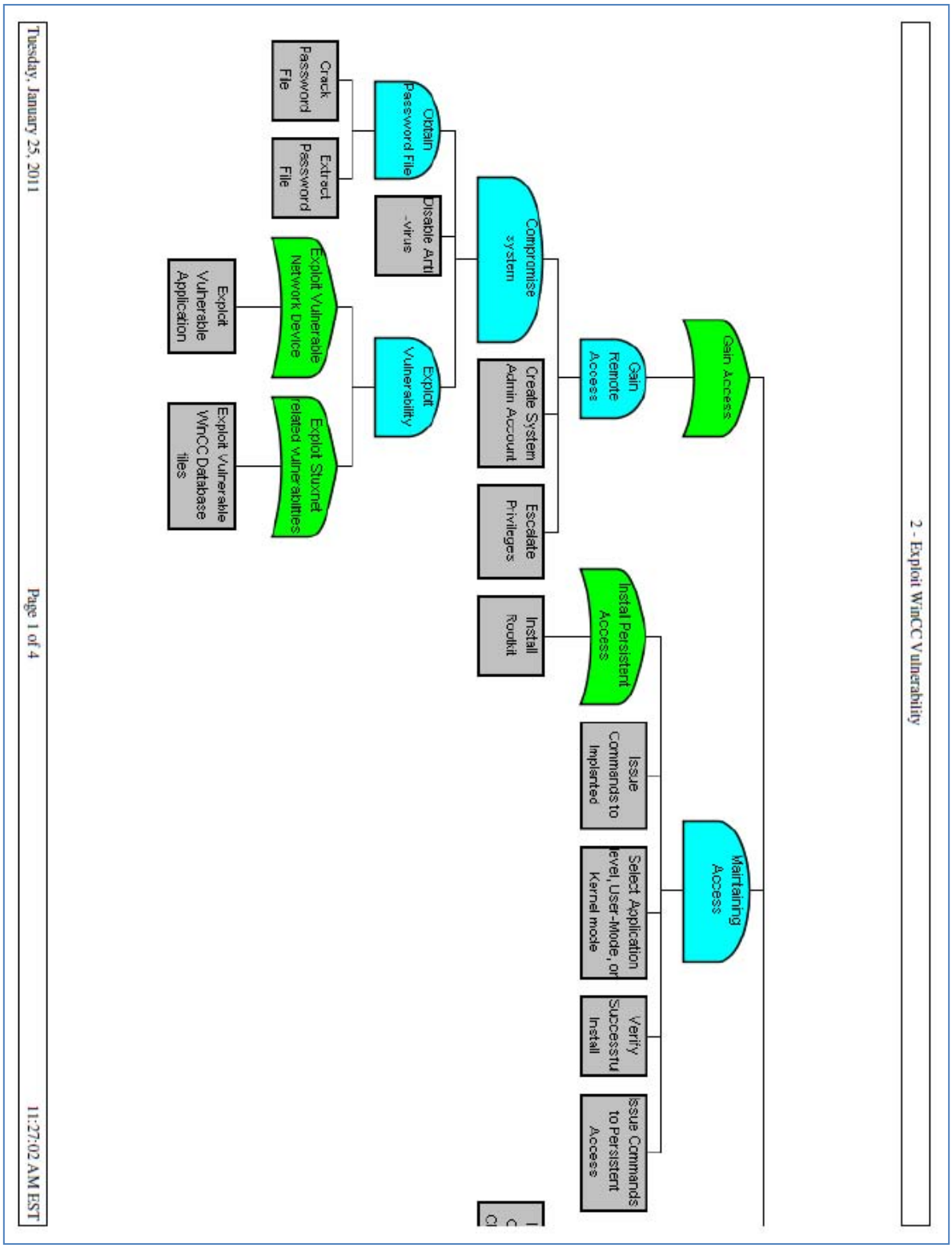


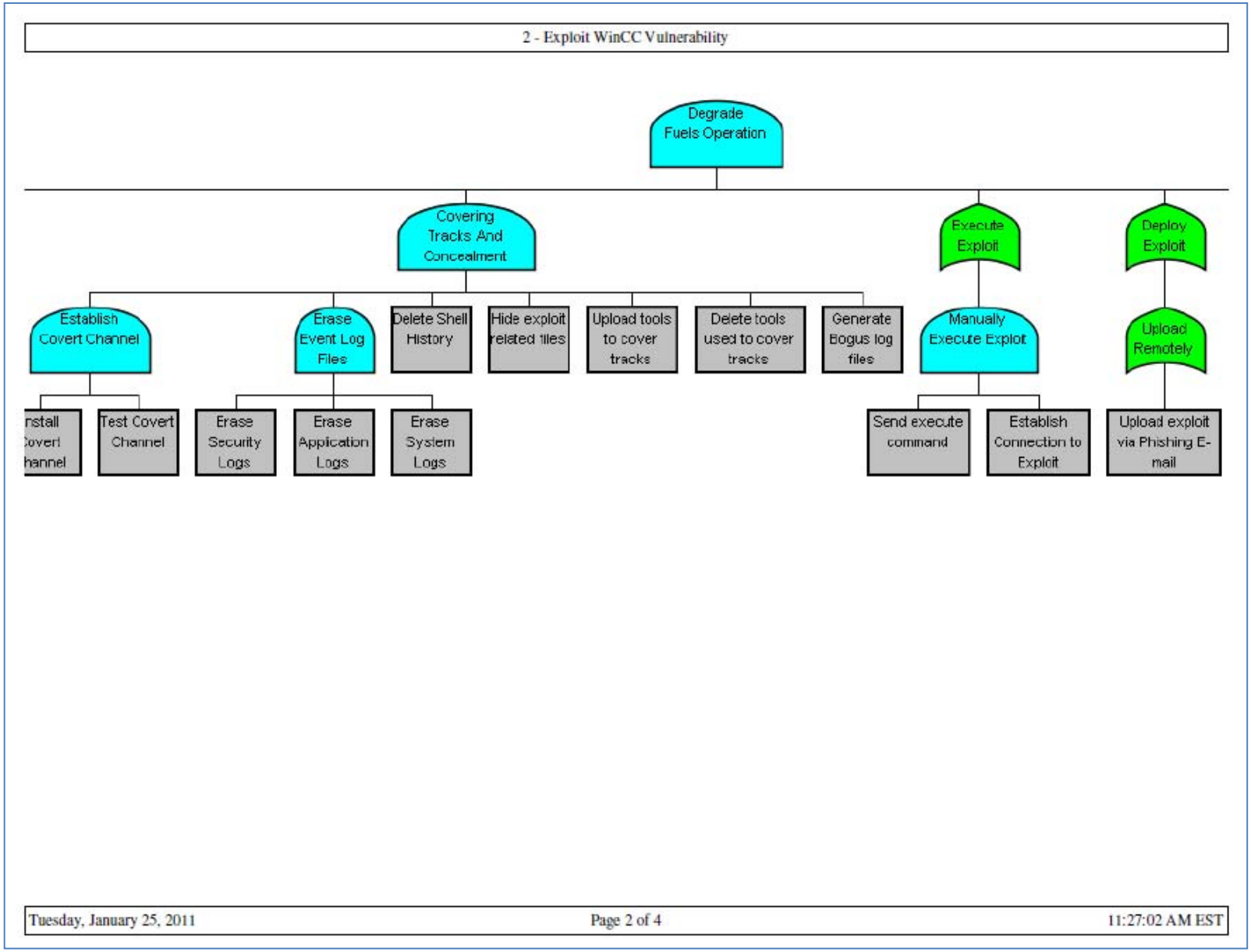
Page 1 of 3


1 - Exploit Step 7 Project Files
Degrade Fuels Operation
Covering Tracks And Concealment
Execute Exploit
Deploy Exploit
Establish Covert Channel
Erase Event Log Files
Delete Shell History
Hide exploit related files
Upload tools to cover tracks
Delete tools used to cover tracks
Generate Bogus log files
Automated Execution of Exploit through site
Upload Remotely
nstall Covert hannel
Test Covert Channel
Erase Security Logs
Erase Application Logs
Erase System Logs
Upload via persistent access
Internet Search
Tuesday, January 25, 2011
Page 2 of 3
11:10:32 AM EST


Reconnaissance
Scanning
Select Exploit
Obtain Open Source Network Information
Obtain Private Network Information
Scan for wireless Access Points
War Dialing for modems
Network Scanning
Obtain Stuxnet like Exploit
Phone book
Public Documents
Target Website
Whois Database
Social Engineering
Network Sweep
Network trace
Port Scan
OS Fingerprinti
Version Scan
Vulnerabiit Scan

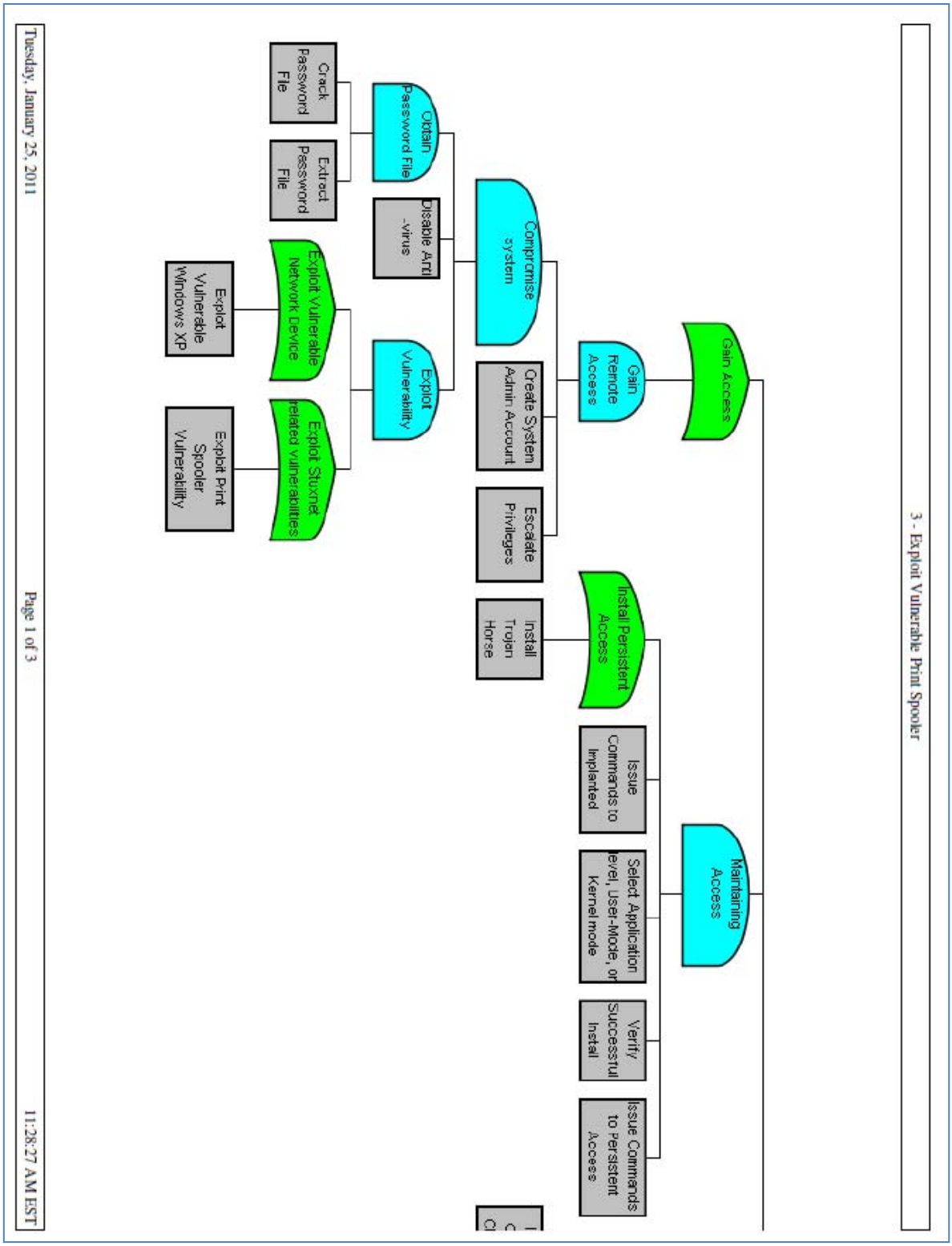
WinCC Attack Scenario

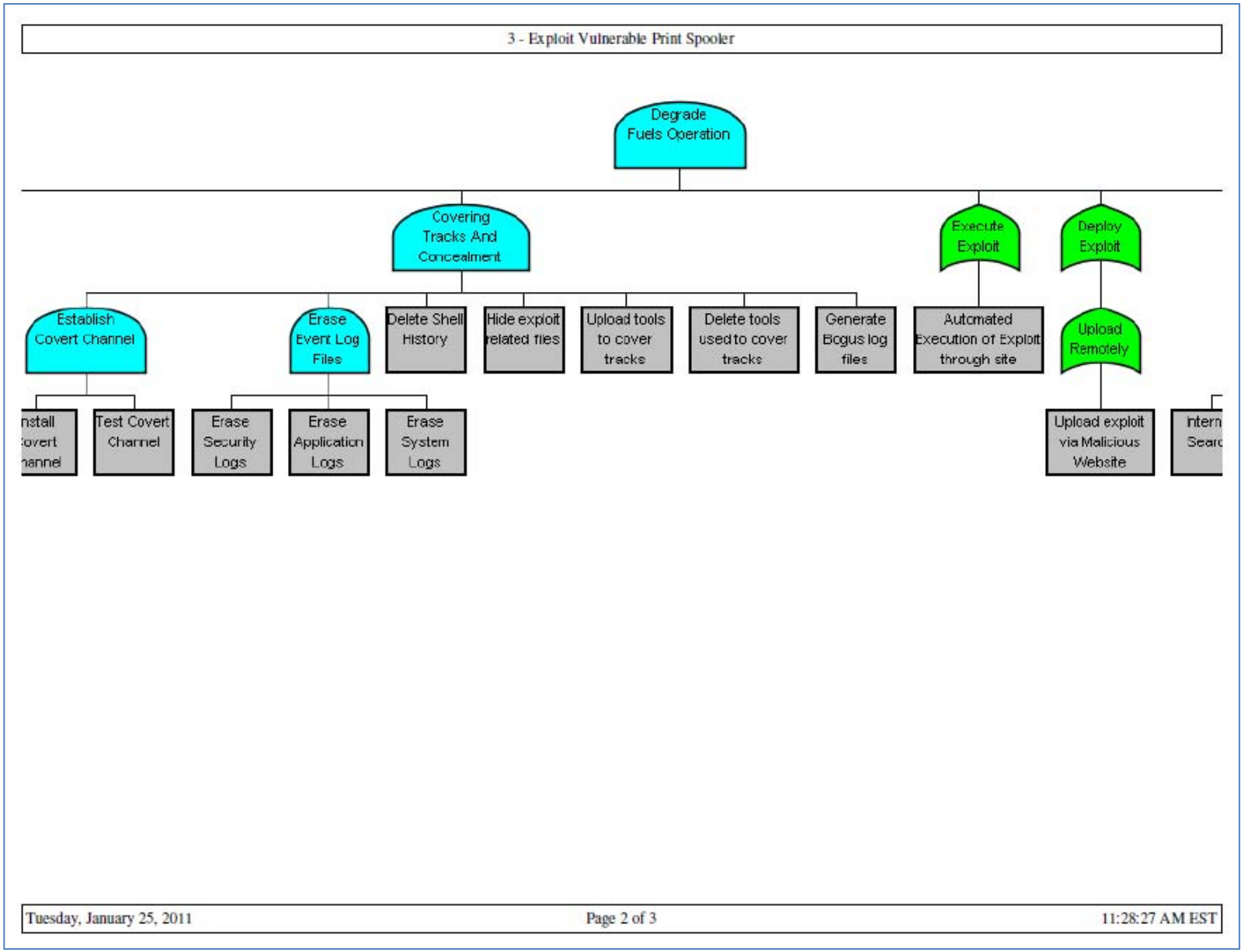



2 - Exploit WinCC Vulnerability
Degrade Fuels Operation
Covering Tracks And Concealment
Execute Exploit
Deploy Exploit
Establish Covert Channel
Erase Event Log Files
Delete Shell History
Hide exploit related files
Upload tools to cover tracks
Delete tools used to cover tracks
Generate Bogus log files
Manually Execute Exploit
Upload Remotely
nstall Covert hannel
Test Covert Channel
Erase Security Logs
Erase Application Logs
Erase System Logs
Send execute command
Establish Connection to Exploit
Upload exploit via Phishing E-mail
Tuesday, January 25, 2011
Page 2 of 4
11:27:02 AM EST

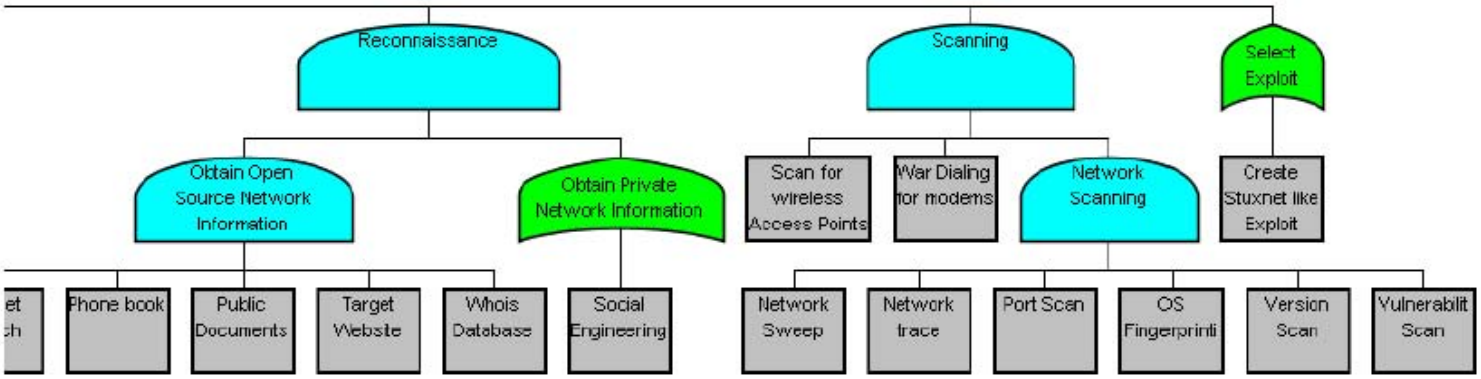
2 - Exploit WinCC Vulnerability
Reconnaissance
Obtain Open Source Network Information
Internet Search
Phone book
Public Documents
Target Website
Whois Database
Obtain Private Network Information
Web Based Recon tools
Scanning
Scan for wireless Access Points
War Dialing for modems
Network Scanning
Network Sweep
Network trace
Port Scan
OS Fingerprinti
Version Scan
Vulnerabilit Scan
Select Exploit
Obtain Stuxnet like Exploit
Tuesday, January 25, 2011
Page 3 of 4
11:27:02 AM EST

Print Spooler Attack Scenario

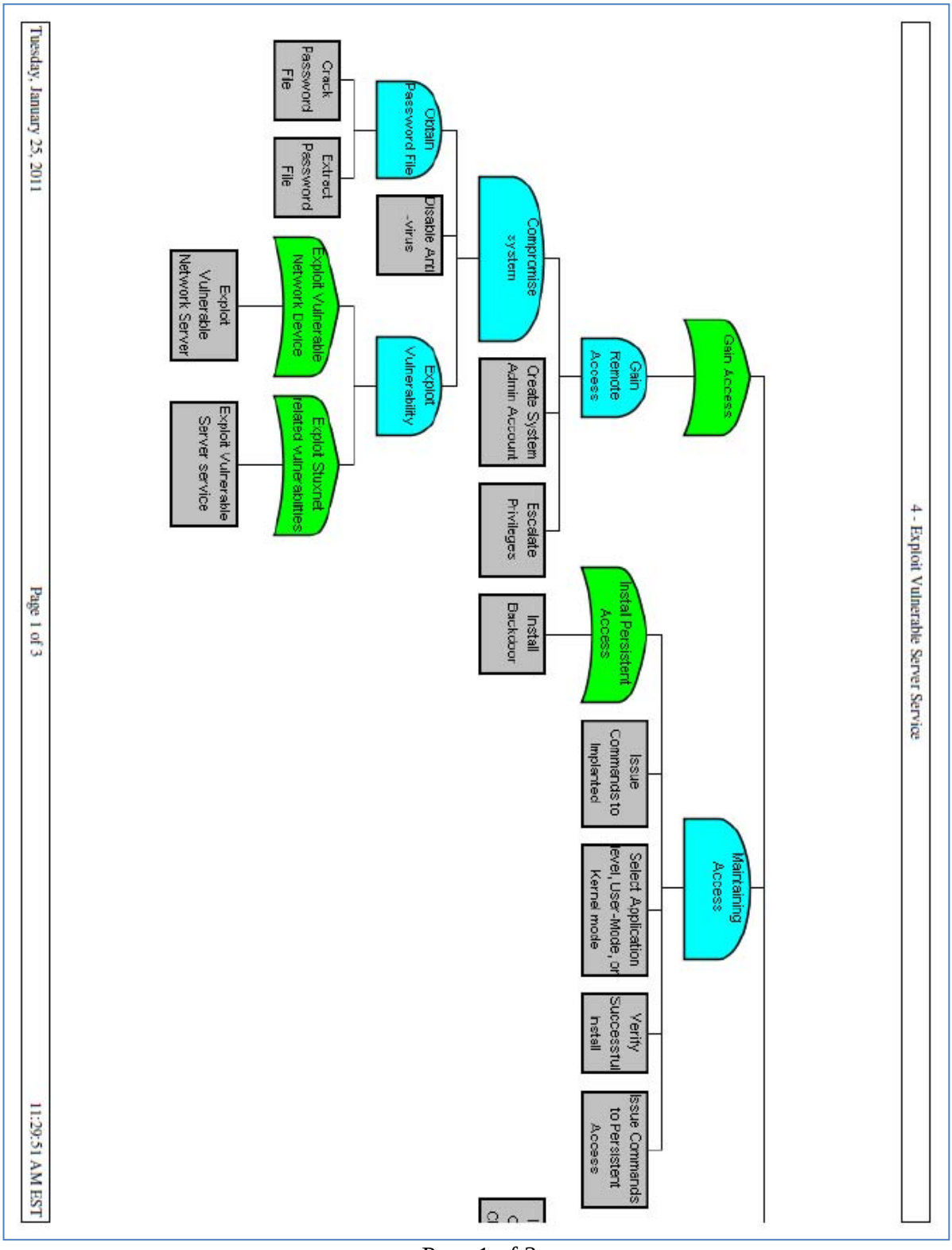


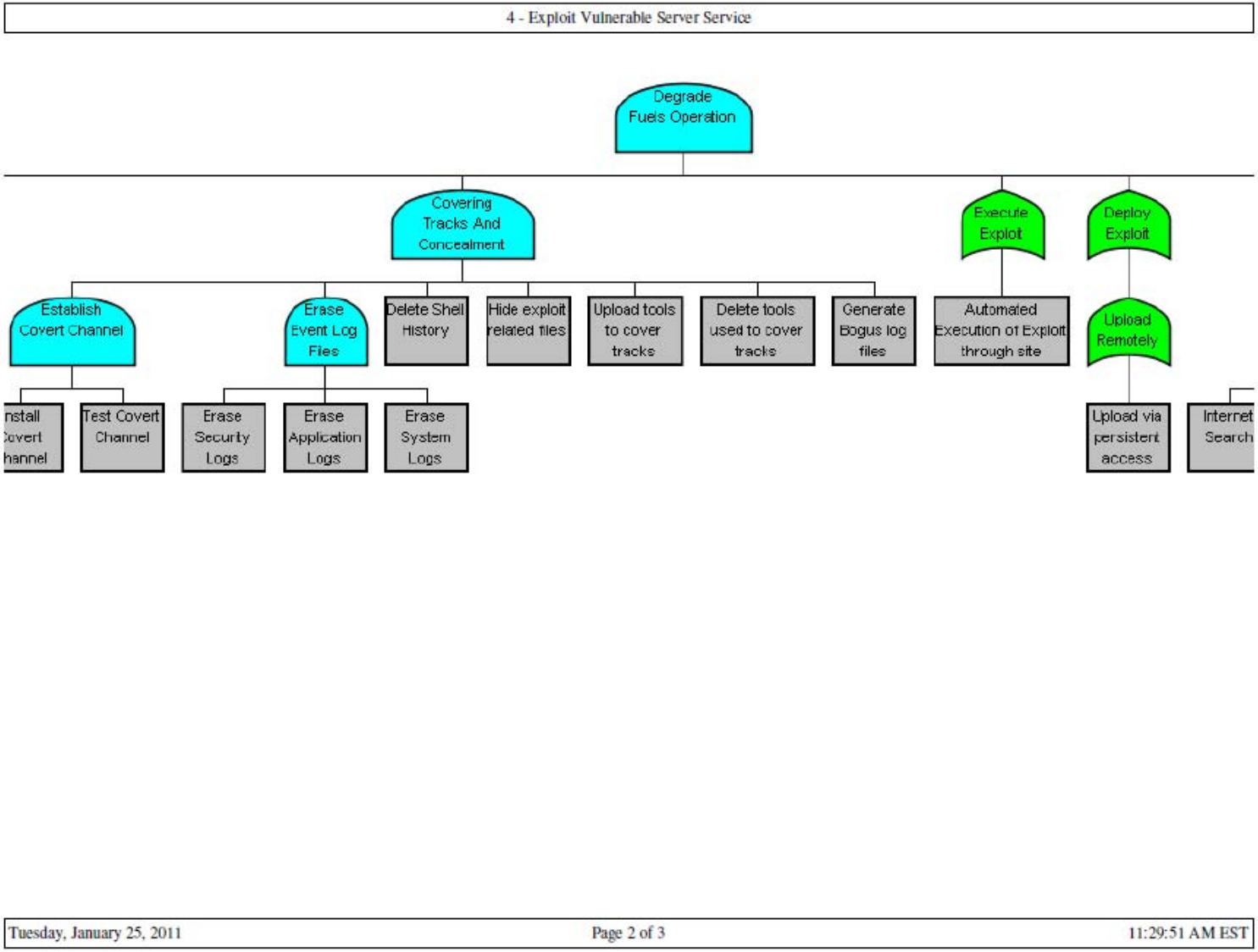

3 - Exploit Vulnerable Print Spooler
Degrade Fuels Operation
Covering Tracks And Concealment
Execute Exploit
Deploy Exploit
Establish Covert Channel
Erase Event Log Files
Delete Shell History
Hide exploit related files
Upload tools to cover tracks
Delete tools used to cover tracks
Generate Bogus log files
Automated Execution of Exploit through site
Upload Remotely
nstall overt hannel
Test Covert Channel
Erase Security Logs
Erase Application Logs
Erase System Logs
Upload exploit via Malicious Website
Intern Searc
Tuesday, January 25, 2011
Page 2 of 3
11:28:27 AM EST

3 - Exploit Vulnerable Print Spooler

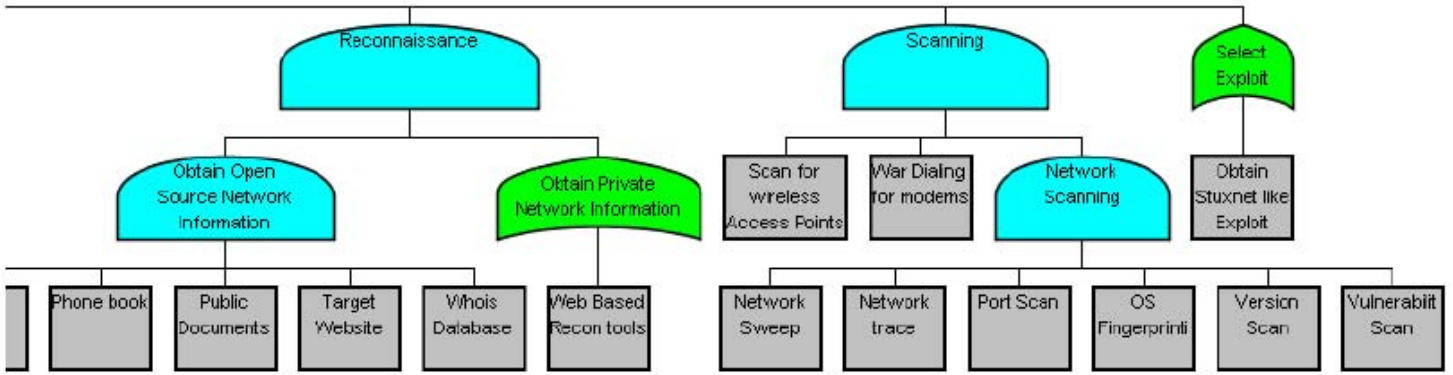


Server Service Attack Scenario



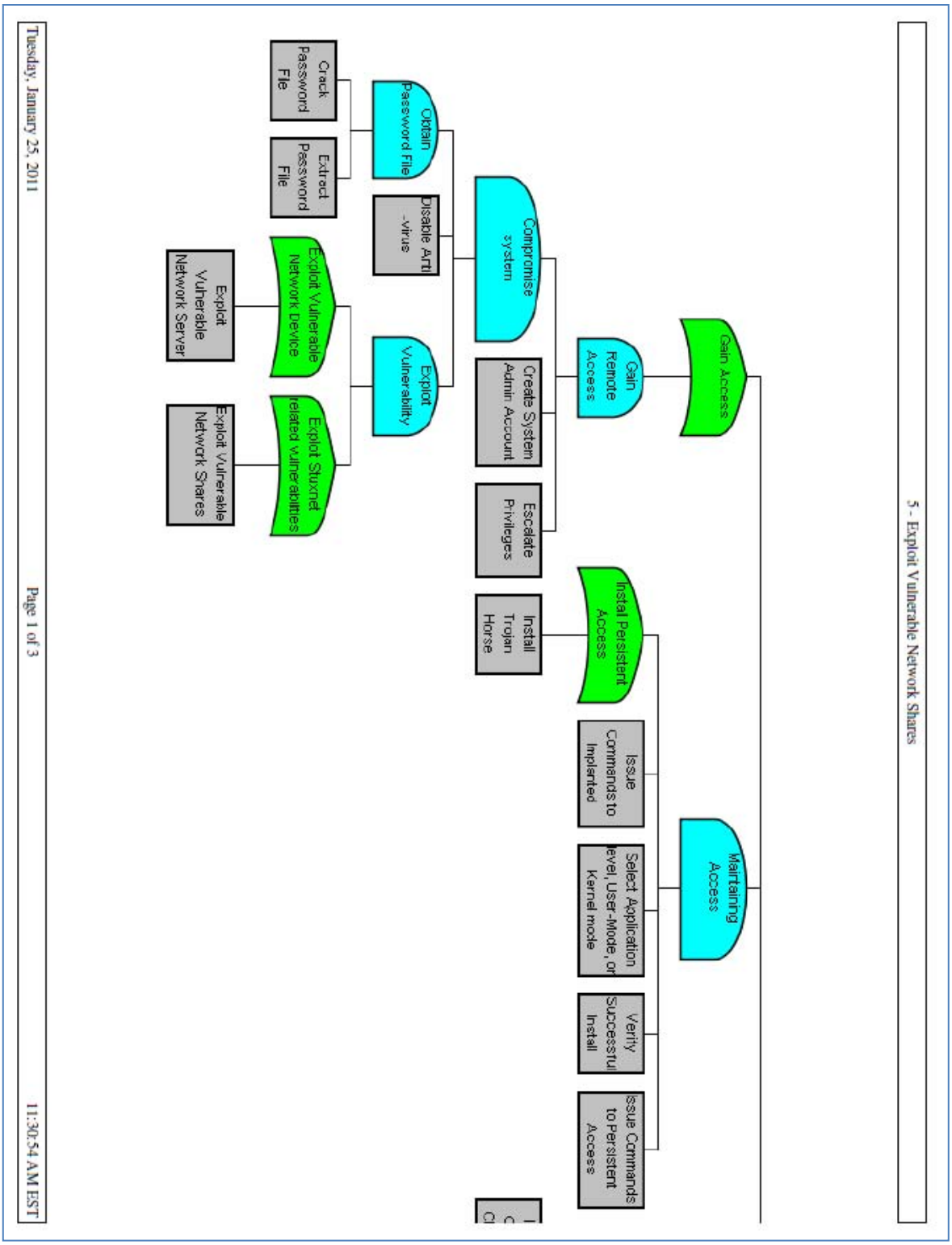

4 - Exploit Vulnerable Server Service
Degrade Fuels Operation
Covering Tracks And Concealment
Execute Exploit
Deploy Exploit
Establish Covert Channel
Erase Event Log Files
Delete Shell History
Hide exploit related files
Upload tools to cover tracks
Delete tools used to cover tracks
Generate Bogus log files
Automated Execution of Exploit through site
Upload Remotely
nstall Covert hannel
Test Covert Channel
Erase Security Logs
Erase Application Logs
Erase System Logs
Upload via persistent access
Internet Search
Tuesday, January 25, 2011
Page 2 of 3
11:29:51 AM EST

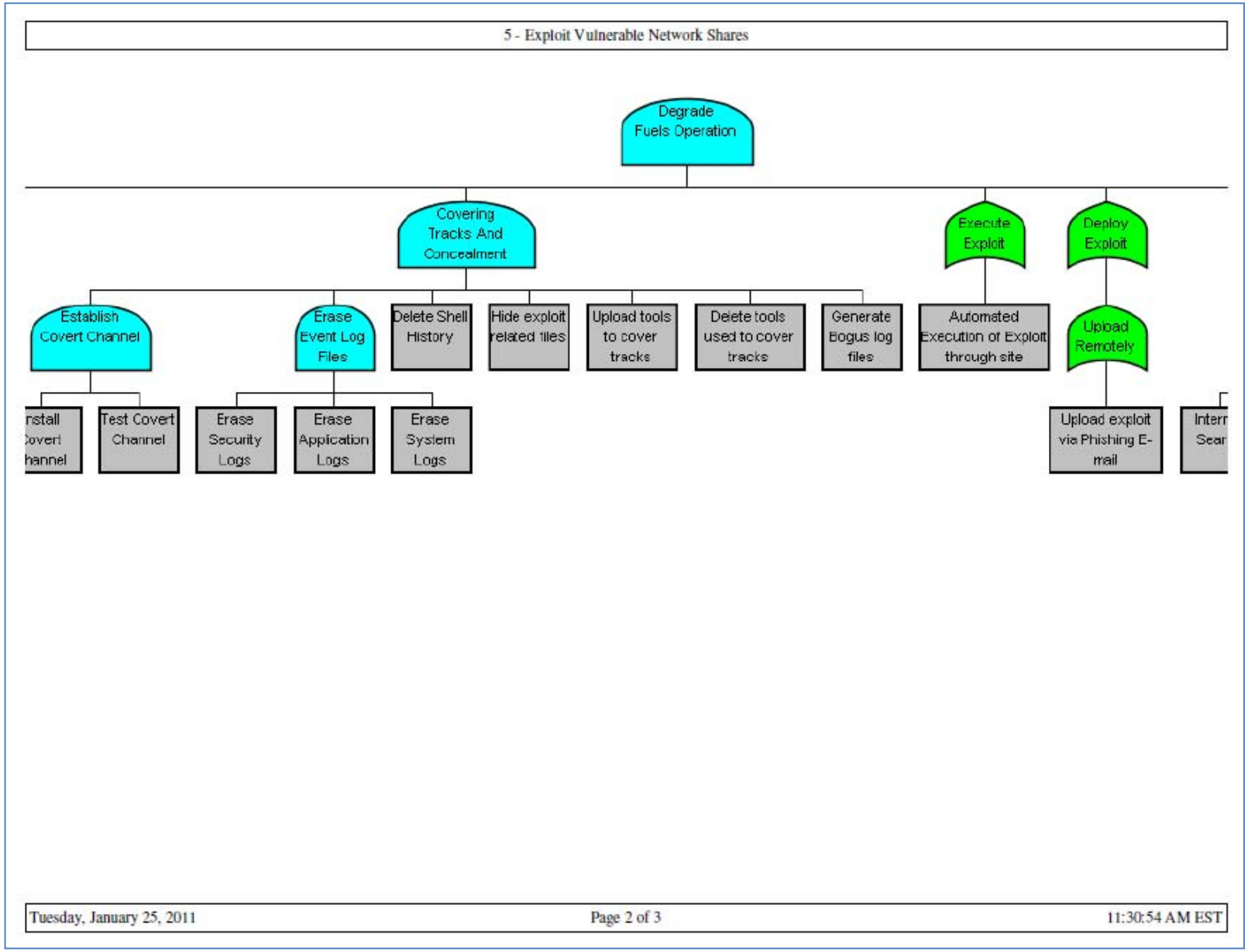
4 - Exploit Vulnerable Server Service



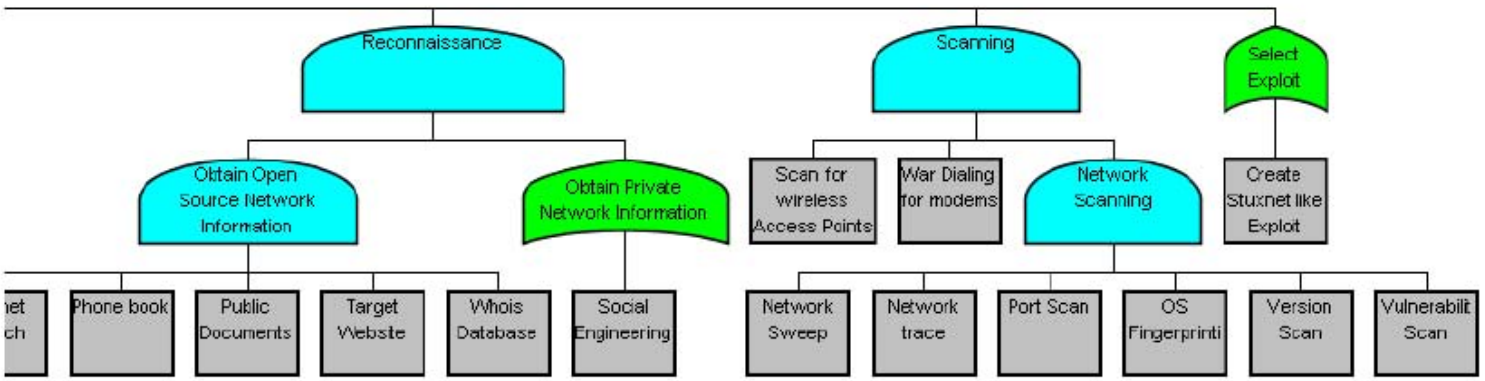
Tuesday, January 25, 2011 Page 3 of 3 11:29:51 AM EST

Network Shares Attack Scenario




5 - Exploit Vulnerable Network Shares
Degrade Fuels Operation
Covering Tracks And Concealment
Execute Exploit
Deploy Exploit
Establish Covert Channel
Erase Event Log Files
Delete Shell History
Hide exploit related files
Upload tools to cover tracks
Delete tools used to cover tracks
Generate Bogus log files
Automated Execution of Exploit through site
Upload Remotely
rstall Covert hannel
Test Covert Channel
Erase Security Logs
Erase Application Logs
Erase System Logs
Upload exploit via Phishing E-mail
Interr Sear
Tuesday, January 25, 2011
Page 2 of 3
11:30:54 AM EST

5 - Exploit Vulnerable Network Shares



Tuesday, January 25, 2011 Page 3 of 3 11:30:54 AM EST

Appendix E: Summary of Indicator Values

 SecurITree http://www.amenaza.com

Indicators for tree: Base Stuxnet Attack Tree.rit

Name	Type	Subtype	OR	AND	SAND	Units	Range
Breach of Trust	Behavioral	Capability	boolean OR	boolean OR			0 - 1
Physical Presence	Behavioral	Capability	boolean OR	boolean OR			0 - 1
Probability of Adversary Success	Behavioral	Capability	minimum of vertices	average of vertices			0 - 1
Probability of Attack Success	Behavioral	Capability	minimum of vertices	average of vertices			0 - 1
Security System Effectiveness	Behavioral	Capability	minimum of vertices	minimum of vertices			0 - 1
Technical Difficulty	Behavioral	Capability	maximum of vertices	maximum of vertices			Named Values

Details:

Name: Breach of Trust
Type: Behavioral
Subtype: Capability
OR: boolean OR
AND: boolean OR
Units:
Range: 0 - 1
Default value for new LEAF nodes: 1.0
Notes:
TRUE - Insider actions required.
FALSE - No insider actions required.

Name: Physical Presence
Type: Behavioral
Subtype: Capability
OR: boolean OR
AND: boolean OR
Units:
Range: 0 - 1
Default value for new LEAF nodes: 1.0
Notes:
TRUE - Physical access required.
FALSE - Physical access not needed.

Name: Probability of Adversary Success
Type: Behavioral
Subtype: Capability
OR: minimum of vertices
AND: average of vertices
Units:
Range: 0 - 1
Notes:
Meaningful at the root node as the combination of the probability of attack success of all of the leaf nodes for a specific attack scenario.

Name: Probability of Attack Success
Type: Behavioral
Subtype: Capability
OR: minimum of vertices
AND: average of vertices
Units:
Range: 0 - 1
Notes:
Describes the probability that a particular leaf node action will be successful.

Name: Security System Effectiveness
Type: Behavioral
Subtype: Capability
OR: minimum of vertices
AND: minimum of vertices
Units:
Range: 0 - 1
Default value for new LEAF nodes: 0.5
Notes:
The degree to which the applied IA controls
are effective at defending the system at a specific leaf node.

Name: Technical Difficulty
Type: Behavioral
Subtype: Capability
OR: maximum of vertices
AND: maximum of vertices
Units:
Named Values:

- Unlikely : 0
- Difficult : 0.1
- Moderate : 0.5
- Trivial : 0.9
- None : 1

Default value for new LEAF nodes: 0.1
Notes:
Describes the technical difficulty associated with particular leaf node.

Sunday, January 23, 2011 Page 1 of 1 11:25:34 AM EST

Appendix F: Leaf Node, Effect Mapping

Network Device Leaf Node	Stuxnet vulnerability Leaf node	Effect
Exploit vulnerable application	Step 7 Project files	Alter Fuels Manager Defense (FMD) database data
Exploit vulnerable application	Exploit Vulnerable WinCC	Alter FMD real time Human-Machine Interface (HMI) data
Exploit vulnerable Windows XP Operating System	Exploit Print Spooler vulnerability	Cause the computer hard drive where FMD resides to crash
Network Server	Exploit vulnerable Server Service	Transmit a false report to the Fuels Enterprise System
Network Server	Exploit Vulnerable Network Shares	Disrupt FMD Communications

Appendix G: System Security Effectiveness Values

How effective do you consider each of the following technologies in place at your organization in detecting and/ or countering security events? (Scale: Very effective, Somewhat effective, Not very effective, Not at all effective, Don't know, Not applicable-don't use) (Base: experienced a cyber security event during the past 12 months)		**Management Controls**	Risk Assessment	Planning	System and Service Acquisition	Certification, Accreditation, and Security Assessments	**Operational Controls**	Personnel Security	Physical and Environmental Protection	Control Center/Control Room	Portable Devices	Cabling	Contingency Planning	Disaster Recovery Planning	Configuration Management	System and Information Integrity	Malicious Code Detection	Intrusion Detection and Prevention	Patch Management	Media Protection	Incident Response	Awareness and Training	**Technical Controls**	Identification and Authentication	Password Authentication	Physical Token Authentication	Role-Based Access Control	Web Servers	Virtual Local Area Network	Dial-up Modems	Wireless	Audit and Accountability	Encryption	Virtual Private Network
Percent "Very" or "Somewhat" Effective	**2010**																																
Statefull firewalls	86%																														0.65		
Electronic access control systems	82%																																
Access controls	80%																																
Password complexity	79%																						0.59										
Encryption	76%																															0.57	
Heuristics-based SPAM filtering	74%																																
Application layer firewalls	71%																																
Host-based firewalls	68%																																
Network-based antivirus	68%																0.51																
Identity management Systems	67%																						0.50										
Network IDS/IPS	66%																	0.50			0.50												
Policy-based network connections & enforcement	66%			0.50																													
RBL-based SPAM filtering	66%																																
Surveillance	66%								0.50																						0.50		
Wireless encryption/ protection	66%										0.50																			0.50		0.50	
Automated patch management	65%																0.49		0.49														
Host-based antivirus	63%																0.47																
Badging	62%							0.47																									
Change control/configuration management systems	62%														0.47																		
Network-based policy enforcement	62%																																
Rights management	62%																																
Multi-factor/strong authentication	61%																						0.46		0.46								
Network access control (NAC)	60%																																
Role-based authentication	57%																									0.43							
Host-based policy-enforcement	56%																																
Application configuration monitoring	53%														0.40	0.40																	

- Denotes System Secruity Effectiveness value for particular IA control

How effective do you consider each of the following technologies in place at your organization in detecting and/ or countering security events? (Scale: Very effective, Somewhat effective, Not very effective, Not at all effective, Don't know, Not applicable-don't use) (Base: experienced a cyber security event during the past 12 months)		**Management Controls**	Risk Assessment	Planning	System and Service Acquisition	Certification, Accreditation, and Security Assessments	**Operational Controls**	Personnel Security	Physical and Environmental Protection	Control Center/Control Room	Portable Devices	Cabling	Contingency Planning	Disaster Recovery Planning	Configuration Management	System and Information Integrity	Malicious Code Detection	Intrusion Detection and Prevention	Patch Management	Media Protection	Incident Response	Awareness and Training	**Technical Controls**	Identification and Authentication	Password Authentication	Physical Token Authentication	Role-Based Access Control	Web Servers	Virtual Local Area Network	Dial-up Modems	Wireless	Audit and Accountability	Encryption	Virtual Private Network
Percent "Very" or "Somewhat" Effective	**2010**																																
Host-based IDS/ IPS	53%																	0.40															
Manual patch management	53%																		0.40														
Host-based SPAM	51%																																
Network-based monitoring/forensics/ESM tool	51%									0.38																							
Software development tools (& processes)	50%				###																												
Host based anti-SPAM	47%																																
Data tracking	46%															0.35														0.35		
Host base configuration management/change control	45%														0.34																		
Application monitoring & trending	44%		0.33																											0.33		
Digital signatures	43%															0.32																	
One-time passwords	43%																						0.32					0.32					
Wireless monitoring	41%										0.31																		0.31				
Data loss prevention (DLP) tools	39%												0.29																				
Application signing	38%																																
Automated integrity controls	38%															0.29							0.29										
Anomaly detection system	32%									0.24								0.24															
Biometrics	30%																								0.23								
Keystroke monitoring	24%																													0.18			

=(Percent "Very" or "Somewhat" Effective) * .75

Survey percetnages are multiplied by .75 consistent with the mid value between very effective and somwhat effective per the scale below.

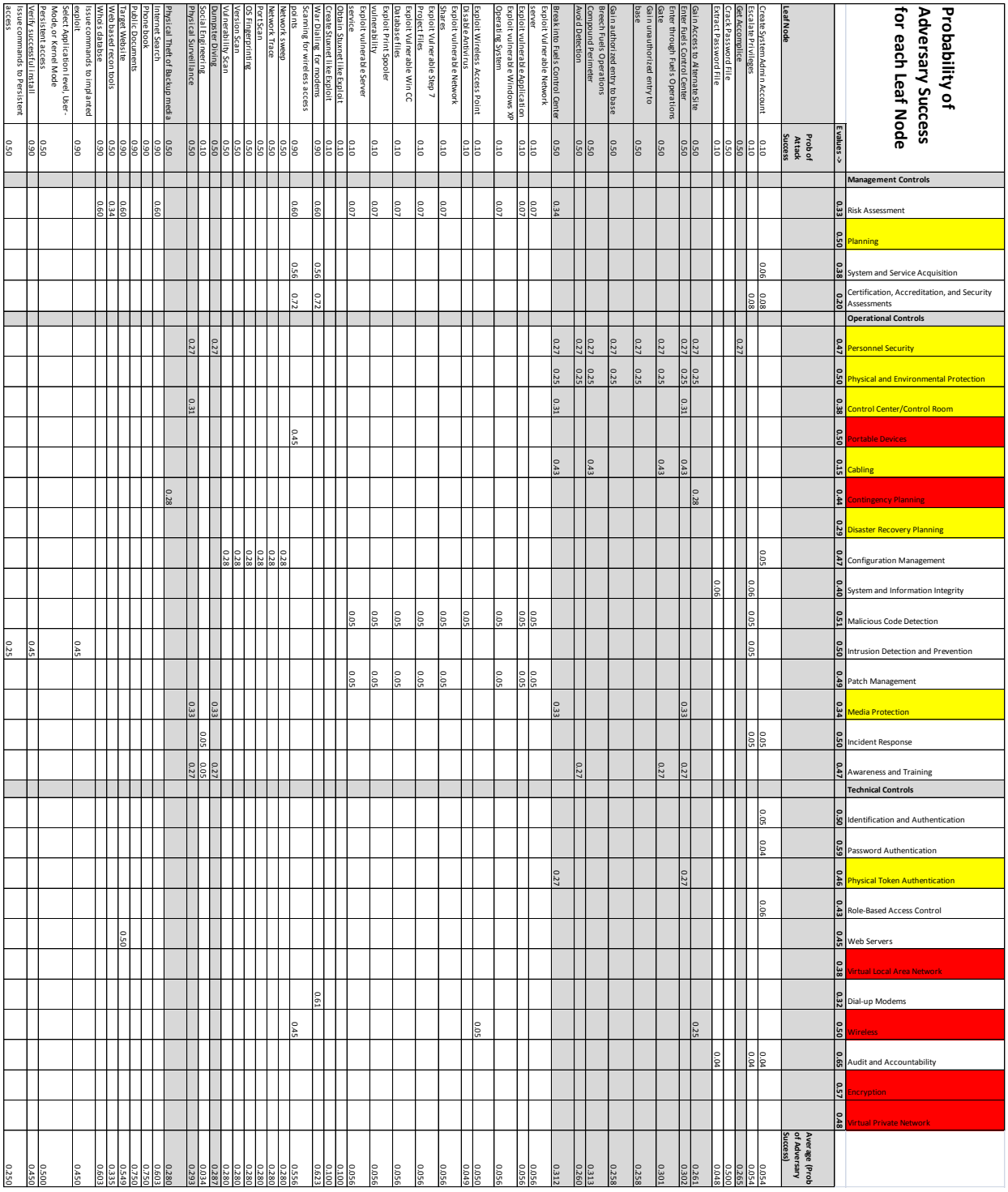
Security System effectiveness

1. Very effective (value .9)
2. Somewhat Effective (value .6)
3. Not very effective (value .3)
4. Ineffective (value .1)
5. Not applicable (value 0)

- Denotes System Secruity Effectiveness value for particular IA control

IA Control	System Secuirty Effectivness value (E)	
Management Controls		
Planning	0.5	
System and Service Acquisition	0.38	
Risk Assessment	0.33	
Certification, Accreditation, and Security Assessments	0.2	*(4 of 4)
Operational Controls		
Malicious Code Detection	0.51	
Physical and Environmental Protection	0.5	
Portable Devices	0.5	
Intrusion Detection and Prevention	0.5	
Incident Response	0.5	
Patch Management	0.49	
Personnel Security	0.47	
Awareness and Training	0.47	*(8 of 15)
Configuration Management	0.47	
Contingency Planning	0.44	*(10 of 15)
System and Information Integrity	0.4	
Control Center/Control Room	0.38	
Media Protection	0.34	*(13 of 15)
Disaster Recovery Planning	0.29	
Cabling	0.15	*(15 of 15)
Technical Controls		
Audit and Accountability	0.65	
Password Authentication	0.59	
Encryption	0.57	
Identification and Authentication	0.5	
Wireless	0.5	
Virtual Private Network	0.48	*(6 of 11)
Physical Token Authentication	0.46	
Web Servers	0.45	*(8 of 11)
Role-Based Access Control	0.43	
Virtual Local Area Network	0.38	*(10 of 11)
Dial-up Modems	0.32	
* Values on Items in blue are extrapolated		
from Mendezlovett's (2010) work in ranking		
IA controls.		

Appendix H: Probability of Attack Success Matrix



Probability of Adversary Success for each Leaf Node

Leaf Node	Prob. of Attack Success	Evalues ->	Risk Assessment 0.33	Planning 0.50	System and Service Acquisition 0.38	Certification, Accreditation, and Security Assessments 0.20	Personnel Security 0.47	Physical and Environmental Protection 0.50	Control Center/Control Room 0.38	Portable Devices 0.90	Cabling 0.15	Contingency Planning 0.44	Disaster Recovery Planning 0.29	Configuration Management 0.47	System and Information Integrity 0.40	Malicious Code Detection 0.51	Intrusion Detection and Prevention 0.50	Patch Management 0.49	Media Protection 0.34	Incident Response 0.50	Awareness and Training 0.47	Identification and Authentication 0.50	Password Authentication 0.59	Physical Token Authentication 0.46	Role-Based Access Control 0.43	Web Servers 0.45	Virtual Local Area Network 0.38	Dial-up Modems 0.32	Wireless 0.50	Audit and Accountability 0.65	Encryption 0.57	Virtual Private Network 0.48	Average (Prob of Adversary Success)
Management Controls																																	
Install Rootkit		0.50													0.30	0.25	0.25								0.29								0.270
Install Backdoor		0.50													0.30	0.25	0.25								0.29								0.270
Install Trojan Horse		0.50													0.30	0.25	0.25								0.29								0.270
Upload exploit via DVD		0.90													0.54	0.44	0.25		0.59														0.525
Upload exploit via USB		0.90													0.54	0.44	0.25		0.59														0.525
Upload exploit via persistent access		0.90													0.54	0.44																	0.491
Upload exploit via Phishing E-mail		0.10													0.06	0.05	0.25				0.05												0.054
Upload exploit via Malicious Website		0.10													0.06	0.05					0.05												0.041
Automated Execution of Exploit through site conditions		1.00																															1.000
Send execute command		0.90																															0.750
Establish connection to exploit		0.50													0.30	0.25	0.25																0.265
Delete Shell history		0.10											0.05																				0.053
Hide exploit related files		0.50																							0.29								0.285
Upload tools to cover tracks		0.10													0.06	0.05	0.05																0.053
Delete tools used to cover tracks		0.90																															0.750
Test Covert Channel		0.50																															0.500
Generate Bogus Log Files		0.50																															0.175
Install Covert Channel		0.50													0.30	0.25	0.25								0.29								0.270
Erase Security Logs		0.50																		0.25					0.29						0.18		0.237
Erase Application Logs		0.50																		0.25					0.29						0.18		0.237
Erase System Logs		0.50																		0.25					0.29						0.18		0.237

* - IA Controls in Red are not part of the fuels flight implmentation

** - IA Controls in Yellow are part of the Fuels flight implementation, but either do not appreciably impact on cyber leaf node actions, or impact physical leaf node actions.

Appendix I: Survey Instrument

Incident Impact Rating of Fuels Operators

Primary Investigators: Maj Jeffrey Hemmes and Mr. J. Lopez Jr.
Student Researcher: Maj Jason R. Nielsen
Research Institution: Air Force Institute of Technology, Wright Patterson AFB, Ohio.
Research Sponsor: HQ USAF A4/7
Purpose: Collect impact ratings for specific incidents affecting DoD Fuels Operations.
Background: This research effort seeks to discover which Information Assurance (IA) controls are most influential for defending the networked Fuels industrial control systems against a specific cyber attack. By examining the success probability of specific attack vectors along with the impact of potential incidents, an overall risk metric can be calculated. This survey requests Air Force Fuels SMEs to provide an impact rating to specific cyber incidents that could impact the operational mission of a Fuels Management organization.

The survey is organized into three parts: (1) Demographics, (2) Impact rating and (3) Impact category refinement.

Disclaimer: This research was conducted in compliance with DoD requirements regarding the protection of human subjects

PART I - Demographics:

1. How many years of experience in operating or managing Fuels Industrial Control Systems do you have? (round values up, place an X next to only one)

   ___ 1-5 years
   ___ 6-10 years
   ___ 11-15 years
   ___16-20 years
   ___ More than 21 years

2. List all computer security or network security training you have completed in the last 5 years.

   _____

   _____

   _____

3. List all industry certifications you have successfully completed in the last 5 years. (e.g. Quality Assurance Certification, Project Management Professional, Security+)
   _____

   _____

   _____

4. What is your primary affiliation with the government? (place an X next to only one)

   ___ Contractor
   ___ Military (Reserve, Guard, or Active Duty)
   ___ Civil Service employee
   ___ Other (Describe) _____

PART II – Impact Rating:

Instructions: This portion of the survey will ask you to rate the impact magnitude of various incidents on the Fuels mission according to the definitions provided in Table 1. Read through Table 1 before proceeding.

Table 1. Magnitude of Impact Definitions (source: NIST SP 800-30)

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability: (1) May result in the ***highly costly*** loss of ***major tangible*** assets or resources; (2) May ***significantly violate***, harm, or impede an organization's mission, reputation, or interest; or (3) May result in ***human death*** or serious injury.
Medium	Exercise of the vulnerability: (1) May result in the ***costly*** loss of ***tangible*** assets or resources; (2) May ***violate***, harm, or impede an organization's mission, reputation, or interest; or (3) May result in ***human injury***.
Low	Exercise of the vulnerability: (1) May result in the ***loss of some*** tangible assets or resources or (2) May ***noticeably affect*** an organization's mission, reputation, or interest.

Note: You can make the following assumptions when determining the impact ratings:

1. The incidents are listed in random order.
2. The incidents are mutually exclusive events.
3. Only one incident can occur at a time.
4. An incident is considered a singular event, meaning they can only occur once.
5. One incident will not cause another event to occur.

Please proceed to the next page to provide impact ratings.

Instructions: Provide your response in the "Impact Rating" column for each incident listed in table 2 below. Select only one impact rating for each incident (e.g. Low, Medium, or High) according to the definitions provided in table 1.

Table 2. Mission Impact Rating

Incident Impacting the Fuels Mission	Impact Rating (Low, Med, High)
Alter Fuels Manager Defense (FMD) database data (For example - change status of training for personnel, change status of fuel truck maintenance, alter fuel temperature conversion calculation, falsify report from lab, cause billing errors, cause errors in fuels inventory)	
Alter FMD real time Human-Machine Interface (HMI) data (For example - change visual indicator of tank fuel level)	
Cause the computer hard drive where FMD resides to crash (For example – cause non-recoverable computer hard drive crash)	
Transmit a false report to the Fuels Enterprise System	
Disrupt FMD Communications (For example – prevent in-bound and out-bound FMD communications with external systems)	

PART III – Impact Category Refinement:

Instructions: For each incident ranked L, M, or H in Part II, give it a numeric score within the defined range. Scores should take into account all other events that can occur in that magnitude of impact category. Assign scores using the following guidelines: Low impact (1 to 10), Medium impact (11 to 50), High impact (51 to 100). Refer back to Part II as needed for the rank (L,M,H) you assigned.

Examples:

> *Low impact:* At the post office the impact of running out of "forever" stamps is low. So the score must fall within 1 to 10. Other incidents that have a low impact include long wait times (2), customer complaints (1), and a new federal holiday (3). Among all of the possible low impact incidents, running out of forever stamps scores 5.
>
> *Medium impact:* At the post office the impact of a broken mail sorting machine is medium. So the score must fall between 11 and 50. Other incidents that have a medium impact include postal employee calling in sick (20), snow storm (40), and a mail truck in maintenance depot (25). Among all of the possible medium impact incidents, a broken mail sorting machine scores 30.
>
> *High impact:* At the post office the impact of the roof caving in high. So the score must fall within 51 to 100. Other incidents that have a high impact include a phoned-in bomb threat (80), power outage (75), and a point of sale outage (55). Among all of the possible high impact incidents, the roof caving in scores 70.

Score the following - Low (1 to 10); Medium (11 to 50); High (51 to 100):

Mission Impacting Rating Refinement	Score
Alter Fuels Manager Defense (FMD) database data	
Alter FMD real time Human-Machine Interface (HMI) data	
Cause the computer hard drive where FMD resides to crash	
Transmit a false report to the Fuels Enterprise System	
Disrupt FMD Communications	

Thank you for your participation in this survey. If you have any follow-on questions you can contact Maj Jason Nielsen at (318) 834-6662 or Mr. Lopez at (937) 255-6565 at extension 4637. If this survey was E-mailed to you, please E-mail it back attached to a signed E-mail to jason.nielsen@afit.edu.

Disclaimer: This research was conducted in compliance with DoD requirements regarding the protection of human subjects

Appendix J: AFIT IRB Exemption Approval Letter

DEPARTMENT OF THE AIR FORCE
AIR FORCE INSTITUTE OF TECHNOLOGY
WRIGHT-PATTERSON AIR FORCE BASE OHIO

18 JAN 2011

MEMORANDUM FOR JEFFERY M. HEMMES, PH.D.

FROM: Alan Heminger, Ph.D.
AFIT IRB Research Reviewer
2950 Hobson Way
Wright-Patterson AFB, OH 45433-7765

SUBJECT: Approval for exemption request from human experimentation requirements (32 CFR 219, DoDD 3216.2 and AFI 40-402) for study titled "Security Effectiveness of Information Assurance Controls for AF Fuels Industrial Control Systems"

1. Your request was based on the Code of Federal Regulations, title 32, part 219, section 101, paragraph (b) (2) Research activities that involve the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior unless: (i) Information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and (ii) Any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.

2. Your study qualifies for this exemption because you are not collecting sensitive data, which could reasonably damage the subjects' financial standing, employability, or reputation. Further, the demographic data you are collecting cannot realistically be expected to map a given response to a specific subject.

3. This determination pertains only to the Federal, Department of Defense, and Air Force regulations that govern the use of human subjects in research. Further, if a subject's future response reasonably places them at risk of criminal or civil liability or is damaging to their financial standing, employability, or reputation, you are required to file an adverse event report with this office immediately.

//SIGNED//
ALAN HEMINGER, PH.D.
AFIT Research Reviewer

cc. Maj Jason R. Nielsen, USAF
Co-investigator
Judith Copler, Contractor
AFIT Sponsored Programs Office

Bibliography

Ashley, B. K., Jackson, L. (1999). *Information Assurance Through Defense in Depth,* Information Assurance Technology Analysis Center, IA Newsletter, Vol 3 No 2, Fall 1999. Retrieved on 10 December 2010 from http://iac.dtic.mil/iatac/download/Vol3_No2.pdf

Ayyub, B., McGill, W., Kaminsky, M. (2007). *Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework,* Risk Analysis, No. 4, 2007.

Baker, S., Waterman, S., Ivanov, G. (2010). *In the Crossfire: Critical Infrastructure in the Age of Cyber War,* McAfee, Inc., 2010. Retrieved 20 October 2010 from http://newsroom.mcafee.com/images/10039/In the Crossfire_CIP report.pdf

Barnes, E. (2010). *Mystery Surrounds Cyber Missile That Crippled Iran's Nuclear Weapons Ambitions*. Retrieved 1 December 2010 from http://www.foxnews.com/scitech/2010/11/26/secret-agent-crippled-irans-nuclear-ambitions/#

Bishop, M. (2003). *Computer Security.* Boston, Massachusetts: Addison Wesley.

Buhan, I., Bazen, A., Hartel, P., Veldhuis, R. (2006). *A false rejection oriented threat model for the design or biometric authentication systems.* Advances in biometrics: international conference, ICB 2006, Hong Kong, China. Retrieved on 2 March 2011 from http://doc.utwente.nl/57029/1/00000130.pdf

Bundbury, P. (2009). *Moving from Compliance-based security to a risk-based security model,* Computer Fraud & Security, September 2009.

Bush, G. W. (2001). *Executive Order 13228 Establishing the Office of Homeland Security and the Homeland Security Council,* Washington DC: GPO.

Bush, G. W. (2001). *Executive Order 13231 Critical Infrastructure Protection in the Information Age*, Washington DC: GPO.

Bush, G. W. (2002). *National Strategy for Homeland Security.* Washington DC: GPO.

Bush, G. W. (2007). *National Strategy for Homeland Security.* Washington DC: GPO.

Bush, G. W. (2003). *The National Strategy for the Physical Protection of Critical Infrastructures and Key assets.* Washington DC: GPO.

Byres, E., Franz, M., Miller, D. (2004). *The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems,* International Infrastructure Survivability Workshop (IISW'04), Institute of Electrical and Electronics Engineers.

Byres, E. J., Kay, J., Carter, J. (2003). *Myths and Facts Behind Cyber Security and Industrial Control.* Retrieved on 12 February 2010 from http://www.pimaweb.org/conference/april2003/pdfs/ MythsAndFactsBehind CyberSecurity.pdf

Byres, E. J., Lowe, J. (2004). *The Myths and facts behind cyber security risks for industrial control systems.* Berlin, Germany: VDE 2004 Congress.

Carlson, R. (2002). *High-Security SCADA LDRD Final Report*. Sandia Labs.

Carnegie-Mellon CERT. (2010). Carneigie-Mellon Computer Emergency Response Team, 2010. Retrieved 16 February 2010 from http://www.cert.org/stats/

Carmody, C. J., Hammerschmidt, J. A., Goglia, J. J., Black, G. W. Jr. (2002). *Pipeline Rupture and Subsequent Fire in Bellingham, Washington June 10 1999,* National Transportation Safety Board. Washington DC.

CBS/AP. (2009). *Pentagon Bill To Fix Cyber Attacks: $100M.* Retrieved 20 February 2010 from http://www.cbsnews.com/stories/2009/04/07/tech/main4926071.shtml

Chertoff, M. (2009). *National Infrastructure Protection Plan,* Department of Homeland Security, Washington, DC: GPO.

Chikuni, E., Dondo, M. (2007). *Investigating the Security of Electrical Power Systems SCADA.* AFRICON.

Clinton, W. J. (1998). *Critical Infrastructure Protection.* Washington, DC: GPO.

Clinton, W. J. (1996). *Executive Order 13010 Critical Infrastructure Protection.*, Washington, DC: GPO.

Clinton, W. J. (1998). *Presidential Decision Document 62 – Combating terrorism.* Washington, DC: GPO.

Contracts, (2006). Retrieved 20 February 2010 from http://www.defense.gov/Contracts/Contract.aspx?ContractID=3229

Coughlin, C. (2010). *China will soon have the power to switch off the lights in the West,* The Telegraph. Retrieved 18 February 2010 from http://www.telegraph.co.uk/comment/6924710/China-will-soon-have-the-power-to-switch-off-the-lights-in-the-West.html

Daneels, A., Salter W. (1999). *What is SCADA?* International Conference on Accelerator and Large Experimental Physics Control Systems.

DHS. (2009). *Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments,* Department of Homeland Security, Washington DC.

DHS. (2005). *Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity.* Washington, DC. GPO.

DHS. (2003). *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection.* Department of Homeland Security, Washington DC: GPO.

DLA-DESC. (2009). *Base Level Support Application (BLSA) Administrator Procedures,* Defense Logistics Agency, Defense Energy Support Center. Memorandum DESC-I-23, 17 Dec 2009.

Ericson, Clifton, A. II. (1999). *Fault Tree Analysis - A History,* 17th International System Safety Conference. Retrieved 13 January 2011 from http://www.fault-tree.net/papers/ericson-fta-history.pdf

Fernandez, J. D., Fernandez, A. E. (2005). *SCADA Systems: Vulnerabilities and Remediation.* Consortium for Computing Sciences in Colleges.

Franz, M., Convery, S., Cook, D. (2004). *An Attack Tree for the Border Gateway Protocol*, 2004. Internet Engineering Taskforce. Retrieved 20 October 2010 from http://tools.ietf.org/html/draft-ietf-rpsec-bgpattack-00

Freyre, J., Holmlund, L., Kimberland, K., Mucisko, D. (2010). *Cybersecruity Watch Survey*. Retrieved 30 November 2010 from http://www.csoonline.com /documents/ pdfs/2010CyberSecurityResults.pdf

Gellman, B. (2002). *U.S. Fears Al-Qaeda Cyber Attacks*, Washington Post. Retrieved 11 February 2010 form http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/ AR2006061200711.html

Gold, S. (2009). *The SCADA challenge: Securing critical infrastructure. Network Security*, (8), 18-2.

Grimes, M. (2005). *SCADA Exposed*. Retrieved 14 February 2010 from http://www.toorcon.org/2005/slides/mgrimes/mgrimes-scadaexposed.pdf

Hancock, D. (2003). *Virus Disrupts Train signals.* Associated Press. Retrieved 14 February 2010 from http://www.cbsnews.com/stories/2003/08/21/tech /main569418.shtml

Hennessy-Fiske, M. (2010). *San Bruno fire chief puts explosion death toll at 6.* Retrieved 1 March 2011 from http://latimesblogs.latimes.com/lanow/2010/09/san-bruno-fire-chief-puts-explosion-death-toll-at-6.html

Hession, K. P. (2008). *Automated Information Technology Implementation*. Air Force Fuels Policy Directive 08-002.

Hildick-Smith, A. (2005). *Security for Critical Infrastructure SCADA Systems.* SANS institute, 23 February.

ICS-CERT. (2010). *ICS-CERT ADVISORY ICSA-10-272-01—PRIMARY STUXNET INDICATORS*, September 29. Retrieved 4 December 2010 from http://www.us-cert.gov/control_systems/pdf/ICSA-10-272-01.pdf

ICS-CERT. (2010). *ICS-CERT ADVISORY ICSA-10-238-01B—STUXNET MALWARE MITIGATION Update B"*, September 15. Retrieved 4 December 2010 from http://www.us-cert.gov/control_systems/pdf/ICSA-10-238-01B.pdf

Igure, V. M. (2007). *A taxonomy of security vulnerabilities in scada protocols,* School of Engineering and Applied Science, University of Virginia.

Ingoldsby, T. (2010). *Attack Tree-based Threat Risk Analysis.* Amenaza Technologies Limited.

Internet World Stats. (2010). *Internet Usage Statistics*. Retrieved 16 February 2010 from http://www.internetworldstats.com/stats.htm

Jarema, J. (2010). *What is the Stuxnet Malware?* Retrieved 13 January 2011 from http://www.suite101.com/content/what-is-the-stuxnet-malware-a295260

Katzke, S., Stouffer, K., Abrams, M., Norton, D., Weiss, J. (2006). *Applying NIST SP 800-53 to Industrial Control Systems.* ISO EXPO: 17-19.

King, W. B., Calcagno, F., Evans, J. H., Gross, E., Lovullo, T. J., Peters, M., et al. (2010). *Taum Sauk Pumped Storage Project, Dam Breach Incident*. Retrieved 12 February 2010 from http://www.ferc.gov/ industries/hydropower/safety/projects /taum-sauk/staff-rpt.asp

Krutz, R. L. (2006). *Securing SCADA Systems*. Wiley Publishing, Inc.: Indianapolis, IN.

Liscouski, B. E., William, J. S. E., Purdy, A., Hendershot, H., Schmidt, S., Kolevar, K., et al. (2003). *Interim Report: Causes of the August 14th Blackout in the United States and Canada, US.* U.S.-Canada Power System Outage Task Force.

Lynn, W. J. III. (2005). *Defense Critical Infrastructure Program (DCIP),* Department of Defense Directive 3020.40, Washington DC: DOD.

Mendezllovet, E., (2010). "Codifying Information Assurance Controls for Department of Defense (DOD) Supervisory Control and Data Acquisition (SCADA) systems." Air Force Institute of Technology Graduate School of Engineering and Management.

Merriam-Webster. (2010). Retrieved on 10 February 2010 from http://www.merriam-webster.com/

Meserve, J. (2007). *Staged Cyber Attack Reveals Vulnerability in Power Grid*. Retrieved on 12 February 2010 from http://www.cnn.com/2007/US/09/26/power.at.risk/index.html

Mills, E. (2010). *Symantec to Congress: Stuxnet is 'wake-up call'.* CNet News. Retrieved on 29 Nov 2010 from http://news.cnet.com/8301-27080_3-20023124-245.html

Mullen, M. (2010). *DOD Dictionary of Military and Associated Terms.* Washington, DC: GPO.

Munro, K. (2008). *SCADA - A critical situation.* Network Security, Volume 2008, Issue 1, January.

Opel, A. (2005). *Design and Implementation of a Support Tool for Attack Trees.* Otto-von-Guericke University Magdeburg. Retrieved on 2 March 2011 from http://www.toengel.net/internship/data/internship_thesis.pdf

Piètre-Cambacédès, L., Bouissou, M. (2010). *Beyond Attack Trees: Dynamic Security Modeling with Boolean Logic Driven Markov Processes (BDMP).* European Dependable Computing Conference, pp. 199-208, 2010 European Dependable Computing Conference.

Poulsen, K. (2003). *Slammer Worm Crashed Ohio Nuke Plant Network.* SecurityFocus News. Retrieved on 14 February 2010 from http://www.securityfocus.com/news/6767

Reno, L. M. (2009). *Logistics Compliance Assessment Program (LCAP).* Air Force Instruction 20-111. Department of the Air Force. Washington DC: GPO.

Ross, R., Stoneburner, G., Porter, E., Rogers, G., Swanson, M., Graubart, R., et al. (2007). *Recommended Security Controls for Federal Information Systems.* National Institute of Standards and Technology.

Safier, A.,Rouse, A., Paller, A., Kotkov, A., Sarwate, A., Skoudis, E., et al. (2007). *SANS Top-20 2007 Security Risks (2007 Annual Update).* Retrieved on 5 December 2010 from http://www.sans.org/top20/2007/top20.pdf

Schneier, B., (1999). "Attack Trees." Dr. Dobbs Journal, Retrieved Oct 21, 2010 from http://www.schneier.com/papers-attacktrees-ddj-ft.htm

SecureTest. (2010). Retrieved on 22 Feb 2010 from http://www.securetest.com/about-us.aspx

Skoudis, E., Lisston, T. (2006). "Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses." Prentice Hall; 2 edition.

Smith, T. (2001). *Hacker jailed for revenge sewage attacks, 2001.* Retrieved on 10 February 2010 from http://www.theregister.co.uk/2001/10/31/hacker_ jailed_for_revenge_sewage/

Stamm, D. (2011). *Gas Explosion Rocks Philly Neighborhood.* Retrieved from http://www.nbcphiladelphia.com/news/breaking/Tacony-Explosion-114177649.html

Stamp J, Campbell P, Depoy J, Dillinger J, Young W. (2004). *Sustainable security for infrastructure SCADA.* Sandia National Laboratories report SAND2003-4670, presented at 2004 power systems conference in Clemson, SC.

Stoneburner, G., Goguen, A., Feringa, A. (2002) "Risk Management Guide for Information Technology Systems." Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

Stouffer, K., Falco, J., & Scarfone, K. (2008). *Industrial Control Systems (ICS) Security.* Gaithersburg, MD: National Institute of Standards and Technology Special Publication 800-82.

USA PATRIOT Act. (2001). *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*.

Warden, J. A. III (1998). Air Theory for the Twenty-first century. *Battlefield of the future: Twenty-first century warfare issues* (chap. 4). Montgomery, AL: Air University Press. Retrieved on 29 November 2010 from http://www.airpower.maxwell.af.mil/ airchronicles/battle/chp4.html

Yamini, G. (2003). *Iranian hacking attempt to electric corporation foiled*. Retrieved on 13 February 2010 from http://www.haaretz.com/hasen/pages/ShArt.jhtml?itemNo=346272&contrassID=1&subContrassID=7&sbSubContrassID=0&listSrc=Y

Vita

Major Jason R. Nielsen graduated from California State University of Sacramento in Sacramento, California with a B.S. degree in Computer Engineering in 1995. He was commissioned through OTS in 1997. After completing BCOT, his first assignment was at Maxwell AFB, Gunter Annex at SSG as a Systems Engineer. During this time he graduated with a M.S. degree in Justice and Public Safety from Auburn University at Montgomery, Alabama.

In September 2003 Maj Nielsen was reassigned to Andrews AFB, 789th Communications Squadron. In route to his new assignment he attended Squadron Officers School in residence. At Andrews he served as Operations Flight Commander, Airborne Communications Program Director, and Support Flight commander, 89th Communications Squadron. During his tour at Andrews AFB he deployed in support of OIF/OEF to Camp Arifjan Kuwait, as the CFLCC/C6 AF Liaison.

In June 2006 he was reassigned to the Barksdale AFB, 8 AF Det 1, Air Force Network Operations Center (AFNOC). There he served as Chief Combat Operations Division and Chief, Standardization and Evaluation. During his tour at AFNOC he deployed to HQ USCENTCOM TNOSC as a watch officer at MacDill AFB, FL.

In August 2009, Maj Nielsen entered into the Graduate School of Engineering and Management, Air Force Institute of Technology, Wright-Patterson AFB, OH, as a Masters Student majoring in Cyber Operations. There he served as a Section Leader for 16 graduate students and was inducted into Eta Kappa Nu (HKN), an electrical and computer engineering honor society. Upon graduation, he will be assigned to the Air Force Intelligence, Surveillance and Reconnaissance Agency, Lackland AFB, TX.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
24-03-2011	Master's Thesis	September 2009 – March 2011

4. TITLE AND SUBTITLE

Evaluating Information Assurance Control Effectiveness on an Air Force Supervisory Control and Data Acquisition (SCADA) System

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Nielsen, Jason R., Major 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 Hobson Way, Building 640
WPAFB OH 45433-8865

8.PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GCO/ENG/11-10

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

INTENTIONALLY LEFT BLANK.

10.SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION/AVAILABILITY STATEMENT

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Supervisory Control and Data Acquisition (SCADA) systems are increasingly being connected to corporate networks which has dramatically expanded their attack surface to remote cyber attack. Adversaries are targeting these systems with increasing frequency and sophistication. This thesis seeks to answer the research question addressing which Information Assurance (IA) controls are most significant for network defenders and SCADA system managers/operators to focus on in order to increase the security of critical infrastructure systems against a Stuxnet-like cyber attack. This research applies the National Institute of Science and Technology (NIST) IA controls to an attack tree modeled on a remote Stuxnet-like cyber attack against the WPAFB fuels operation. The probability of adversary success of specific attack scenarios is developed via the attack tree. Then an impact assessment is obtained via a survey of WPAFB fuels operation subject matter experts (SMEs). The probabilities of adversary success and impact analysis are used to create a Risk Level matrix, which is analyzed to identify recommended IA controls. The culmination of this research identified 14 IA controls associated with mitigating an adversary from gaining remote access and deploying an exploit as the most influential for SCADA managers, operators and network defenders to focus on in order to maximize system security against a Stuxnet-like remote cyber attack.

15. SUBJECT TERMS

SCADA, ICS, IA Controls, Supervisory Control and Data Acquisition, Industrial Control Systems

16SECURITY CLASSIFICATION OF:			**17.LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**THIS PAGE**			Jeffrey M. Hemmes Maj, USAF (ENG)
u	**u**	**u**	**UU**	139	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-3636, ext 4619 (jeffrey.hemmes@afit.edu)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18