Australian Government
Department of Defence
Defence Science and
Technology Organisation

A Perspective on Research Challenges in Information Security

Tamas Abraham, David Adie, Angela Billard, Paul Buckland, Michael Frangos, Ben Long, Martin Lucas, Paul Montague, Dean Philp, Simon Windows

Command, Control, Communications and Intelligence Division

Defence Science and Technology Organisation

DSTO–TN–1035

ABSTRACT

This report considers a number of selected areas of security technology and practice. The focus is on exposing and highlighting research gaps and opportunities in the current security state of the art within these areas, both in terms of implementation practice and of the literature.

Published by

DSTO Defence Science and Technology Organisation
PO Box 1500
Edinburgh, South Australia 5111, Australia

Telephone: (08) 7389 5555
Facsimile: (08) 7389 6567

AR No. 015-129
November, 2011

APPROVED FOR PUBLIC RELEASE

Contents

1 Introduction

As the pace of technological advance continues unbridled, the risks associated with the compromise of information security grow ever more significant. There is a strong pull towards systems becoming increasingly interconnected. New technological areas such as cloud computing, together with the established trends towards mobile computing and a pervasive electronic environment, present new aspects and attack vectors which demand a re-evaluation of security practices and paradigms. Ongoing research in security is therefore an imperative.

With this in mind, this report considers security in a number of selected areas of security technology and practice associated with the current activities and research interests of the authors, namely:

- Unified Security,
- Security Policies and Architectures,
- Critical Information Infrastructure Protection Security,
- Multi-Level Security, and
- Authentication and Authorisation.

The focus is on exposing and highlighting research gaps and opportunities in the current security state of the art within these areas, both in terms of implementation practice and of the literature.

We end the report with a summary of the key opportunities we have identified, and draw these together from across the different domains.

2 Security Policies and Architectures

Security policy and security architectures are closely interrelated. At the highest level, security policy defines the goals that an architecture should achieve. On the other hand, at the lowest level, an architecture implements automated policies to ensure that higher-level security objectives are achieved. As a result, policy and architectures have a degree of mutual dependence whereby the limitations of one can produce similar limitations in the other. For example, a security architecture must be able to support the goals stated by policy or risk becoming inconsistent with it or, at least, less functional than policy requires. Similarly, an architecture may provide the possibility for great flexibility and functionality but a lack of policy and policy mechanisms to appropriately govern such an architecture will produce a system that is less secure than policy requires or significantly less functional than the architecture's capability.

In addition, traditional policy and architecture approaches suffer from similar problems. Manual development, translation and validation processes produce static policy and architectures, as well as difficulty in verifying a cohesive, consistent result. Furthermore, attitudes to risk management have significantly changed in the last decade and traditional risk averse approaches are no longer sufficient to support operational requirements, modern technologies and user expectations. The following sections discuss issues and research challenges in the areas of security policy and security architectures.

2.1 Security Policies

Security policy is a generic term that covers a broad range of documents, procedures and rules whose purpose is to provide a coherent and consistent approach to protecting an organisation's assets. At the highest level, organisational security policy should set out the operational environment of the organisation, the kinds of threats and risks it faces, the security objectives to be achieved and guidelines for achieving them. At the lowest level, security policy may be refined to cover specific practices and procedures for human behaviour and automated rules governing the behaviour of technological systems and system components. In order to be consistently effective, security policy must be correctly implemented at every level and across every domain of an organisation's operation. Figure 1 (based on [Billard & Ozols 2006]) shows a conceptual structure of security policy.

Unfortunately, the comprehensive scope of security policy contributes to making it extremely difficult to manage in itself.

2.1.1 Ambiguity, Inconsistency, Complexity and Effect

Security policy is often ambiguous and complex, and it is difficult to ascertain its effects. To some extent, this is a reflection of the world to which it applies. There are numerous things organisations need to be able to do in order to conduct day-to-day business and numerous ways in which opponents could attempt to foil their efforts. In addition, security policy has a delicate balance to maintain between security and functionality. There is no point in securing assets to a degree that they cannot be used for their intended purpose

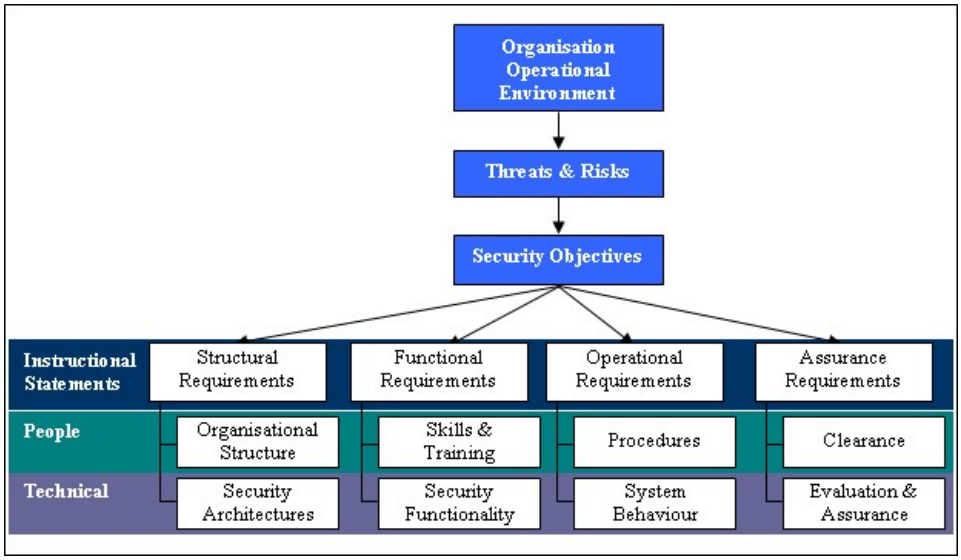

Figure 1: *Conceptual structure of security policy*

and the resulting complexities can make security policy extremely difficult to understand. The use of natural language to express large portions of the whole security policy picture complicates matters further by being imprecise and diversely interpretable. This leads to ambiguities and misunderstandings about how the security policy statements should be applied. Unfortunately, even if the policy could be easily understood, the difficulty in assessing its actual effects means it is hard to have assurance that the policy will be effective in providing the appropriate security guidance or that it will not have unwanted side-effects. Furthermore, a lack of formal modelling and validation of policy statements can result in contradictions and logical inconsistencies within policy. The Australian Government Protective Security Manual (PSM) [Attorney General's Department 2007] provides an example of this in its flowchart for "How to select an appropriate security classification" (Part C, paragraph 6.12) which, if followed, would result in a document containing both 'Highly Protected' information and 'Restricted' information receiving the overall document classification of 'Restricted' instead of 'Secret', as suggested by paragraph 7.19.

Like anything else, security policy needs to be maintained in order to stay up-to-date and relevant to what is going on in the real world. However, traditionally, security policy tends to be very static. This is largely because its lifecycle is based on manual processes. Unfortunately, the real world can change substantially in very short periods of time and so it is very easy for policy to be almost constantly out of date. Small, seemingly limited revisions can have widespread and unexpected side-effects. In addition, when policy is broken up into separate layers or units, maintaining consistency becomes a major challenge. This makes thorough validation of the policy a vital part of its lifecycle.

However, typically, policy is so large and complicated that it is extremely difficult to check as a whole.

2.1.2 Research challenges

There are a range of research challenges in relation to security policy. Automated policies have the advantage of precise specification in a machine interpretable manner. In theory, this should assist in modelling and validation; however, there are still a range of issues that present difficulties:

- The use of a variety of specification languages and implementation mechanisms (influencing how policy is interpreted) make it difficult to draw together a coherent 'big picture' of how policy is implemented across and between systems;
- There is a lack of tools for modelling and analysing security policy that support a wide range of specification languages. Most of the tools that exist use their own languages, thus creating yet another point at which translation is required. Furthermore, these languages are either limited in expressiveness to a particular application domain or so generic that they present a significant learning curve in how to use them in order to accurately express different kinds of problems and properties [Billard et al. 2002].
- As technology is constantly evolving, security policy modelling and analysis tools would need to evolve alongside technology to ensure that gaps don't develop between the kind of policies that are implemented and the kind that can be modelled.
- Many existing verification techniques, such as symbolic modelling, require large amounts of machine resources and a long time in order to exhaustively verify even relatively simple problems. This suggests that these techniques would not cope with the scale and complexity of system-wide security policy validation.

Organisational security policy, which is typically expressed in natural languages, suffers from further issues and challenges:

- The expression of ideas and generic concepts is difficult to translate into precise formal expression, making many parts of organisational-level policy unsuited to modelling and validation. While there are some attempts to analyse natural language policy [Naufel do Amaral et al. 2006] it is unclear how well such analysis would resolve issues with inherent ambiguities in the language.
- Organisational security policy may include parts that are suited to formal modelling and validation; however, most modelling and validation tools require the skills of programmers and/or mathematicians in order to use them. This presents a steep learning curve for policy writers without a mathematical/technical background.

An additional research challenge is the ability to model non-technical factors as part of a cohesive security policy model, including humans and manual procedures. A model that does not include these factors will always be incomplete.

2.2 Security Architectures

Security architectures can be defined as the structures, mechanisms, automated security policies and the interrelationship between these that are required to implement stated security objectives and organisational security policy. The relationship between security policies and security architectures is more difficult to define precisely, since they both aim to achieve the same goals and are mutually dependent. Traditionally, security architectures have been static in nature and therefore limited in their ability to dynamically adapt to changing user requirements, security conditions and resource availability. Such architectures and their component technologies assume that security risks, requirements and resources will not change over time and this often results in inflexibilities that impede the system and its users. As a result, system users are often not provided with the best service possible, nor is the best security employed.

Recent research efforts including "Dynamic Security Architectures" [Billard & Long 2009] and "Security as a Service" [Bertino & Martino 2007] have attempted to address these deficiencies by providing more dynamic and flexible security architectures capable of adapting to changing circumstances. However, there is still a considerable amount of research required in this area, particularly in incorporating dynamic variables such as risk, trust and reputation in access control decisions. These variables change as the underlying factors change, so in order to provide truly 'best fit' security services, such variables need to be calculated on-the-fly, taking into account the relevant factors for a particular situation and context. The security system must then be able to respond appropriately.

2.2.1 Trust and Reputation-based Security

In security systems trust is commonly established either by policy based mechanisms or by reputation based mechanisms. Policy-based trust is based on policy and credentials. Agents are trustworthy if they meet the requirements of the policy (e.g. correct username and password, correct biometrics, 100 points of ID etc.). Reputation based trust mechanisms are not as well established as policy-based trust mechanisms. Security systems that employ reputation-based trust mechanisms estimate the "trustworthiness" of each user based on the user's previous transactions or on referrals from trusted or unknown third parties. Such mechanisms are commonly found in online services such as eBay where ranking systems are used to establish trust between buyers and sellers in online markets. "Dynamic Security Architectures" [Billard & Long 2009] has demonstrated how a simple model of user reputation may be incorporated into access control decisions, however, for real world applications, more complex reputation-based trust models must be explored. Trust models from the field of e-commerce such as [Josang, Ismail & Boyd 2007] show promise in this regard but there is large scope for further research in the area.

2.2.2 Risk-based Security

The National Security Agency (NSA) has realized the importance of incorporating risk in security systems in order to meet the increasingly complex data access and sharing requirements of modern organisations. The concept of Risk Adaptable Access Control (RAdAC) [McGraw 2009] has been developed which extends other earlier access control

models by introducing environmental conditions and risk levels into the access control decision process. RAdAC combines information about a subject's trustworthiness as well as situational and environmental risk factors to create an overall quantifiable risk metric. The particular security policy in place is then adjusted dynamically depending on the measured level of risk. In addition to RAdAC, there are other promising risk-based access control models such as BARAC [Zhang, Brodsky & Jajodia 2006] in which access control decisions are made by comparing the risk of information access with the benefits of information sharing.

The challenges involved in developing security architectures capable of supporting risk-based access control models such as RAdAC and BARAC are immense. Firstly, realistic models for the risk level present in a particular information transaction must be developed. This is not a trivial matter and whilst there has been some research done in this area [Cheng et al. 2007] [Srivatsa, Rohatgi & Balfe 2008] there is still a significant amount of work required. The second major challenge will be to develop security architectures that can dynamically adapt to changes in transactional risk levels. This may require context-aware systems that can dynamically modify security policy and handle any necessary revocation of resources as the level of risk changes.

3 Authentication and Authorisation

3.1 Storage and Protection of Credentials

There is a plethora of credentials which a user is required to present in various scenarios during their typical working day. If these are distinct passwords or pass phrases, and sufficiently complex to avoid being guessed, then this places an inordinate burden on the user's memory. [We shall discuss the use of biometrics in a later section.] Therefore it seems prudent to employ some form of storage device in that case, such as:

- a portable security token, e.g. a smartcard, CodeStick [Defence Science and Technology Organisation 2008] [Grove et al. 2007] or smartphone,
- a "password safe" on a desktop PC or a mobile computer/smartphone, in which multiple passwords are stored under the protection of a single pass phrase [Sourceforge n.d.].

In other scenarios, for example when authenticating using some sort of secret or private key of cryptographic (significant) length instead of a simple password/phrase, the credential, which is then beyond typical human capacity to remember, must typically again be stored in some form of portable security token/device.

3.1.1 Loss of Token

There are some clear issues associated with this storage of credentials in a token. For example, should the security token be lost/stolen, the credential data must remain (a) inaccessible and (b) unusable by a malicious party. Typically this is achieved at the interface level, in the case of a credential stored on a smartcard for example, by requiring the user to authenticate via means of a PIN or biometric before the smartcard will respond to any challenge using the stored credential. [Of course, in relation to credential loss, there is the obvious requirement to retain legitimate access to the data/systems concerned for ongoing operational needs. There exist well known mechanisms to address this issue, and it is out of scope for the purposes of the current discussion.]

In addition, the stored credential data itself should be held under hardware-based protection, such as via proprietary commercial hardware [Ashkenazi 2005] or standards-based approaches such as the Trusted Platform Module (TPM) [*Trusted Computing Group* n.d.]. Though this makes it difficult for an attacker to extract the raw key data, there may be weaknesses in the hardware/software mechanisms [Jackson 2010] or maliciously inserted hardware modules ("Silicon Trojans") [Anderson, North & Yiu 2008] which compromise the user's credentials. Therefore, one opportunity we see for research is the exploration of other mechanisms for additional protection of the credential data in order to mitigate such risks as far as possible in high security application areas, following the fundamental principle of defence in depth. For example, recent work has demonstrated the capability to derive unique and repeatable cryptographic keys from user biometric data [Lan & Hang 2008]. An attacker in control of such a device would still be incapable of accessing the credentials encrypted using such keys without knowledge of the user biometric.

Another issue associated with loss of a security token is, in the case where the token is utilised for encryption of data, some mechanism for recovery of that data in the absence of the credential must be provided. This may typically involve some sort of key escrow so that system administrators may recover the key(s) for decryption of the critical data. However, there are opportunities here for abuse of the system by administrators. Opportunities exist for exploring novel protocols involving threshold-based secret sharing [Desmedt 2005] amongst multiple parties in order to mitigate both the impact of malicious administrators and of loss of administrator tokens.

3.1.2 Protection of Credential on Token During Usage

Ideally, in the case of a credential consisting of a cryptographic key rather than a password, the key itself never leaves the token during usage, but instead is simply used to compute and return a response to a challenge from the system to which the user is attempting to authenticate.

However, there may be information leaked from the device during the computation which can reveal information about the key - for example, the time taken or the power consumed [Kocher, Jaffe & Jun 1999]. A more recent sub-class of these generic "side channel" attacks, called Cache Attacks, [Osvik, Shamir & Tromer 2006*b*] show how easily cryptographic keys in secure processes may be revealed by the state of the CPU cache to unprivileged processes running on the same CPU, even under conditions in which sandboxing, memory protection and virtualisation are employed. Such attacks are exacerbated by the move towards multi-application/multi-level devices and the increasing emphasis on cloud computing solutions, in which malicious applications may manoeuvre to be co-hosted on the same box as a target application. Though various mitigations have been explored, it is clear that more research in this area is required. As Tromer et al. state [Tromer, Osvik & Shamir 2009]: "Indubitably, further side channels in all levels of system architecture will be created and discovered, as hardware grows in parallelism and complexity."

3.1.3 Protection of Passwords During Entry

The preferred mechanism of authentication should involve two or even three factors i.e.

- something the user possesses (e.g. portable security token),
- something the user knows (e.g. pass word or pass phrase) and
- something the user is (biometric).

Whilst we have discussed some of the issues and challenges around tokens and biometrics in this and other sections, the use of human knowledge (e.g. a password) in high security systems seems unavoidable as at least one of the required authentication factors. The protection of passwords during their actual use, i.e. during entry to the system, raises some areas for further research.

For example, the SecHCI (Secure Human-Computer Identification) Project discusses the issues associated with disclosure of a password during its entry into a computer system, either through passive attacks (shoulder-surfing, hidden cameras, keyboard sniffers,

TEMPEST attacks, etc.) or active attacks (fake terminals, subversion of backend servers, etc.) [*The SecHCI Project* n.d.]. Though there are some mechanisms proposed so far, there clearly remains much to be done in improving security and yet retaining acceptable usability for any password-type human authentication system.

Alternatives, of course, include the automatic presentation of passwords held on a user's security token rather than direct human entry. Again, this is a field in which there is much scope for innovation in terms of integrating such mechanisms into often legacy infrastructure, with both a high degree of security in protecting the passwords from compromise and maintaining ease of use for the user.

3.1.4 Web Single Sign-On

Another solution to the multiple credential burden, is to use the same digital identity. There are standards for authenticating users which can be used for access control to log on to different services with the same digital identity where services trust the authentication body. The most popular of these standards is OpenID. This has the advantage of not requiring the user to enter all of their identity information into every site they wish to use. A major disadvantage is that phishing attacks from a malicious relaying party would allow the malicious party access to all other services using the users identity [Oh & Jin 2008]. Also, as a single authentication is used for multiple services, any compromise has a larger impact, and use of strong authentication (such as smart card) would be desirable.

3.2 Privacy and Anonymity

Traditionally, the authorisation of a user to exercise a certain privilege has depended upon their initial authentication, and subsequently based on that authentication, e.g. by consulting an access control list, a decision is made regarding the granting or otherwise of the privilege. Even in cases where a user is granted access based upon a credential attesting to the user possessing a certain role or attribute (e.g. an attribute certificate [Farrell & Housley 2002]), the link to the user's identity is still present, either implicitly or explicitly.

However, such a mechanism is naively at odds with users' understandable concerns regarding their privacy, particularly in an increasingly networked world in which tracking of user activity and deductions/inferences based on such become all too easy for both legitimate and non-legitimate parties. The risks only become exacerbated with the increasing emphasis on cloud computing solutions.

Simplistic approaches such as certified attributes/roles not linked to an identity still allow for tracking and correlation of user activities based on tracking usage of that certificate. The strict goal of privacy is not met.

Whilst such a goal may seem at odds with typical Defence approaches to security, the pervasive tracking of users, whilst beneficial to our own unified security systems [Abraham et al. 2010], should not be facilitated for less trusted or even hostile systems. With increasing coalition activities and the associated use of allied, and perhaps less trusted, systems, together with the trend towards an increasingly "smart" environment in which users must operate, the situation will only get worse. In addition, in a broader whole of

government or even commercial context, privacy becomes an even stronger requirement which must be addressed.

There has been development in the literature regarding anonymous credentials over the years. These cryptographic tokens allow users to claim (and prove) statements about their attributes anonymously. The concepts are very closely related to those of digital cash [Chaum 1985] [Brands 2000]. Some schemes [Camenisch & Lysyanskaya 1991] allow for multiple showings of one credential to remain unlinkable. Though there has been much theoretical development here, we have not yet seen integration of such concepts into practical systems, and hence gaps/opportunities exist.

One other area of application of the above schemes, and itself also an area in which further research opportunities arise, is in limiting the knowledge leaked during certain attestations. For example, in negotiating within a group of users the highest common security clearance of that group, a protocol which limits the leakage of information about the exact clearance levels of each participant would be advantageous, without (or in addition to) restricting this information by simply relying on its confinement to trusted hardware. The problem is not simply related to more traditional "zero knowledge" type scenarios, and, as such, offers challenging opportunities for novel work. Use of anonymous credentials would limit the risks, by anonymising requests and thereby rendering independent protocol runs unlinkable, but other issues remain.

3.3 Biometrics

There are some biometric technologies that are already widely in use, such as Fingerprint, Face, Iris and Speaker recognition, and a large number of additional technologies being researched. These technologies are developed to facilitate a range of functions that can be broadly categorised as verification or identification, and include, for example, physical and logical access control, weapons control, identity management and surveillance operations. A review of biometrics technology was done by DSTO in 2008 [Heyer 2008].

As with other types of verification or identification systems there are many possible security vulnerabilities. Possible areas of attack specific to biometric systems include mimicking valid biometrics, manufacture of fake biometrics, using fake identification to enrol an invalid user, and synthesizing a data input stream and changing it iteratively to achieve better match scores. Further work can be done to resist attacks, improve usability and performance of correct matching. There is more work to be done for some types of biometrics that are not mature enough to be widely used.

The approaches for authentication are typically classed as "something you know" (e.g. a password), "something you have"(e.g. a smartcard), or "something you are" (e.g. a fingerprint). A fourth factor that may be added to this is "somebody you know" [Brainard et al. 2006]. This fourth factor can be used where a user requests another user to vouch for them. This is a method of authentication often used in human relationships, and has some advantages. As this is a social form of authentication, it contains potential vulnerability to social engineering. Further work could be done to make practical use of this factor.

3.4 Secure Localisation and Tracking

Research towards interesting applications of object localisation and tracking remains popular. For instance, secure localisation of objects can be useful in contexts such as secure ad-hoc pairing of devices to provide assurances that paired devices really are the ones present [Kobsa et al. 2009] [Kindberg & Zhang 2002]. Object tracking applications include paradigms such as blue-force tracking and personnel/inventory tracking. Al-Kuwari and Wolthusen point out that these tasks can be achieved through object-based (where an object shares its self-localisation data) or network-based (where one or more reference objects locate another object) means [Al-Kuwari & Wolthusen 2010].

Security considerations relating to object localisation and tracking are less active in related research areas, though secure localisation is an area that provides important robustness guarantees in these systems [Al-Kuwari & Wolthusen 2010], which may be used within sensitive and potentially hostile environments, such as in theatre. Both object-based and network-based means of tracking are currently being researched using the CodeStick device as a platform, through such applications as blue-force tracking and Bluetooth tracking, respectively.

3.5 Relay and Man-in-the-Middle Attacks

The ongoing trend towards the ubiquity of and reliance on wireless communication channels opens up vulnerabilities for would-be attackers to exploit. Interesting exploitation methods include (but may not be limited to): relay, or wormhole, attacks; and man-in-the-middle attacks (MITM).

Defending against these attacks is particularly relevant in contexts where entities need a high assurance that their direct communication counterpart is the expected entity it is claiming to be, instead of an unexpected impostor carrying out an attack. In a passive relay attack, for example, Eve may try to authenticate to Bob, posing as Alice, in order to gain access to a sensitive meeting or resource. She conducts a relay attack in league with Charlie, who simultaneously carries out an authentication procedure with Alice in some less sensitive context. Bob is convinced Eve is actually Alice, allowing Eve escalated access.

In this example, which assumes the same credentials held by Alice would be used in both contexts, use of a mutually authenticated secure channel between Alice and Bob does not improve the situation whatsoever, because the true endpoints of the communication channel are in fact Alice and Bob as they each expect. The middlemen, Eve and Charlie, effectively form part of the communications channel connecting Alice and Bob, such that Eve is able to gain her desired access in lieu of Alice after the transaction is complete.

Active MITM attacks are also possible where entities are not sufficiently vigilant [Stajano, Wong & Christianson 2010]. To illustrate, consider the example where Mallory presents Alice with a fake bank web site. Alice, if not vigilant enough to check the address in her browser, is blissfully unaware that it is not really her bank site. Since Mallory can use a certificate that was issued for her domain, which happens to host the fake site, the browser indicates to Alice everything is OK. However, the site looks (and feels) to Alice like her

bank's site. When she interacts with it, Mallory's server mirrors that interaction on the real bank site, but includes some nefarious activity.

An interesting consideration moving towards the future is that the mutual authentication provided by classical (PKI-based) methods will be susceptible to attack by quantum computers [Shor 1997]. This favours atomic pairing and authentication, which would remain secure in the presence of quantum computing since there is no reliance on cryptographic protocols, for instance by leveraging physical one-way function technologies. Proposed by Ravikanth [Ravikanth 2001], these utilise physical properties of difficult to characterise materials/structures in order to provide a cost-effective physical analogue of cryptographic one-way functions.

4 Unified Security

With the ever increasing focus on organisational security, the convergence of physical and cyber security has seen great advances in recent years [Contos, Hunt & Derodeff 2007, Tyson 2007]. Whilst both of these traditionally separate fields face their own set of challenges, their combination introduces new challenges that necessitate additional effort and guidance from governments, vendor communities and industry associations [US Department of Homeland Security 2003, US Department of Homeland Security 2004, Sarbanes & Oxley 2002, Open Security Exchange 2007, Hamilton 2005]. In addition to covering purely cyber and physical security topics, these ventures also address issues associated with risk management, emergency management, disaster recovery, personnel security, privacy management, auditing and the facilitation of potential forensic investigations.

These efforts all fall under what we call *unified security*, the discipline in which systems are combined to achieve security benefits greater than those of the individual components. However, this definition differs from what is practised, under the more popular term *security convergence*, insofar that security convergence is driven significantly by commercial factors, typically with goals such as:

- risk mitigation: liability reduction, legislation compliance;
- business processes: cost reduction, increased operational efficiency or business value, reduced process lifecycles; and
- other factors such as human interaction, security awareness, improved morale, better image and reputation (brand protection).

Unified security expands on these ideas, keeping 'improved security' as the primary objective, while providing transparent solutions for users that reduce the complexities of following policies and guidelines rigorously. We call this approach *security through convenience*. The challenges presented below reflect this intent and highlight areas for investigation that focus on security compliance whilst mitigating the adverse effects on users' daily routines.

4.1 Security Objectives

Typical security objectives include *confidentiality*, *availability*, *integrity*, as well as *non-repudiation*, *authenticity*, and *utility*, and we find that these objectives can gain new meanings in the context of unified security. For example, confidentiality relates to both digital information and users' physical locations, and availability may affect *safety* objectives in emergencies when physical access control systems are controlled via computer networks.

Much of security convergence is driven by increased security and reduced costs; however, Contos et al. [Contos, Hunt & Derodeff 2007] state that security convergence must include an understanding of the impact on individuals and the ability for them to perform their jobs, i.e., the inconvenience to users. When security measures and policies are too onerous or unnecessarily complex, users (including security operators) are less likely to cooperate [Weir et al. 2009]. Users circumvent security measures accidentally, but also

often deliberately [Adams & Sasse 1999] for the sake of convenience, resulting in potential vulnerabilities that may be exploited by internal or external attackers, rendering security solutions less effective. McIlwraith [McIlwraith 2006] challenges us to develop a comprehensive approach to information security, considering both the human and technical dimensions. A system providing more convenient ways for users to adhere to security policies will more likely meet security objectives. Therefore, we consider convenience to be one of the most critical objectives of unified security as it enables security objectives to be achieved.

4.2 Emerging Technologies

There are several technologies that organisations have considered contributing to convergence, such as physical access control systems, biometric controls, RFID [Lopez et al. 2007], video surveillance, time sheet programs, GPS programs etc.; however, many are treating this level of unification as something to be done at a later stage [Contos & Kleiman 2006]. On the other hand, we consider the unification of such technologies to be essential in the search for convenient new solutions.

Advances in security technologies are frequent and commonplace, necessitated by the ever inventive criminal element ready to circumvent it at every opportunity, and by the need to extend protection to an increasing area of operations. Ongoing commitment by organisations to include more systems into their security frameworks in future is anticipated. The following sections highlight some technologies that we think should, and probably will, receive increased consideration.

4.2.1 Identity Reconciliation

The inclusion of many disparate systems into a unified security system often introduces multiple representations of the same entities. Enterprise Security Management (ESM) systems routinely utilise pre-defined mappings to overcome this difficulty when reasoning. Such approaches can, however, become difficult to administer and maintain. Automating the discovery of the multiple representations of the same identity would therefore become a significant time-saving factor, and is likely to attract ongoing research interest.

4.2.2 Additional Data Sources

The increased availability of data generated by our daily routines should enable better tracking and auditing of our actions and assets. Security issues can be identified promptly by live monitoring of computer activity, traversal through building access control points and asset access records. Logs can be analysed to provide a picture of user behaviour that can be used to finetune policies and facilitate more targeted training. The inclusion of new data sources for investigation and cross-source reasoning will thus become increasingly important elements of security operations.

4.2.3 Convenience Technologies

New security technologies must emphasise convenience to assist users in maintaining secure practices. For example, automating the use of a classified material register, by logging and monitoring each item within, can help better track their location at all times in a busy working environment.

Providing single sign-on solutions for accessing all resources in an office, including computers, telephones, printers and whiteboards, with automatic lock-up mechanisms when the user leaves the area, can minimise security-related human error. Such solutions can also incorporate controls for multi-level security, restricting access based on classification levels.

However, providing more convenient solutions requires considerable research into security design, to ensure the convenience of accessing information is not exploited by malicious intruders. For example, one does not want the existence of office single sign on to create a gaping hole in an existing security in-depth strategy.

4.2.4 Targeted Visuals

Constant feedback of security-related information can be provided by targeted visuals, scoped appropriately for each user. For example, a display in a corridor could show the location of occupants within a workplace, assisting with security monitoring and also compliance with occupational health and safety requirements. A visualisation personalised for a user at their desk may include information about their unsecured assets (or about the users to whom they are talking when on the phone). The same application may trigger an SMS message to the user when the system discovers a security violation involving those assets if still unsecured when he/she leaves the workplace.

4.3 A Comprehensive Approach

Forrester Research defines security convergence to be the integration of security functions and information onto a common IP network [Contos, Hunt & Derodeff 2007]. John Moss, CEO and founder of S2 Security Corp considers security convergence to mean the adoption of IT technologies by the physical security realm and the support by the IT community of physical security requirements [Contos, Hunt & Derodeff 2007]. However, Contos et al. [Contos, Hunt & Derodeff 2007] note that it is functional convergence (the fusing of multiple non-security solutions) that provides new platforms upon which new security solutions may be driven. Therefore, with respect to unified security, it is important to consider the potential for improved security from combinations of both physical and non-physical (or logical), and both security and non-security systems.

Most companies are decomposing the big-picture goal of security convergence into manageable fragments [Forristal 2006], unifying system *functionality* to achieve:

- use of a single ID card for physical and logical access,
- single step card enrolment and termination across all databases, and

- centralised ID-management systems,

but also unifying system *data* in the form of ESM systems [Contos & Kleiman 2006], such as Intellitactics Security Manager, ArcSight ESM and IBM Tivoli. Ideally, a more comprehensive approach to unified security will provide a combination of both *active unification* of functionality and the more *passive unification* of data only.

A comprehensive approach to unified security will encompass all aspects of convergence within a single system, illustrated by Figure 2: a combination of logical and physical systems contribute to security and non-security systems, a combination of security and non-security systems contribute to convergence components or monitoring systems, and a combination of these systems contribute to a unified security system. Furthermore, a unified security system may contribute to other systems.

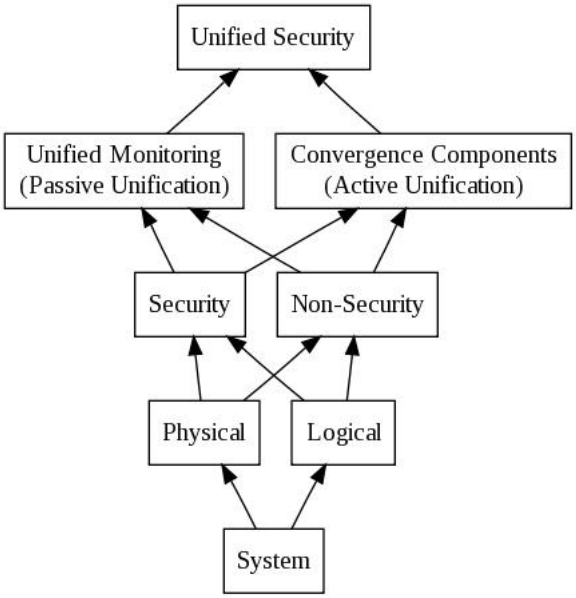

Figure 2: *A Unified Security System*

4.4 Unified Security Frameworks

Some discussions of frameworks for unified security are found in the literature [Campbell et al. 1996, J. Dawkins & Papa 2005, Wilson & Tharakan 2003, Nortel 2005]. However, most are selective and cater for subsets of security convergence (e.g., omitting consideration of monitoring or physical aspects) or describe it either as a set of policies [Indiana Office of Technology 2007] or processes only.

A comprehensive IT security framework is proposed by IBM [Buecker et al. 2009] that includes people and identity, data and information, application and processes as well as network and physical infrastructure, from a business perspective. It also includes a blueprint to match security requirements to proprietary product offerings. This is indicative of the lack of standardisation that currently exists for security in general. Whilst

frameworks to cover the expanded world-view of unified security may be derived from existing proposals, it is also important to consider what is required for their successful implementation.

Implementation issues can present themselves at all levels within the framework. A unified security system is most likely to be heterogeneous, meaning increasingly complex configurations and environments to make everything work. To alleviate these problems, government and industry needs to be proactive in providing solutions that simplify deployment, operations and maintenance. For example, at the hardware level, interfaces can be standardised. At the network level, common languages/protocols can be developed for component communication. At the application level, standard structures/ontology can be provided to describe unified security concepts. Similar initiatives can be carried through to all levels within the framework.

5 Multi-Level Security (MLS)

Ever since the initial application of computer systems within the defence and intelligence communities, Multi-Level Security (MLS) has been a strong driver and significant challenge to system architects and developers. Organisations and users struggle with the conflicting needs of protecting the security of sensitive information at multiple levels, and the need to provide ready access to information by those with appropriate access and need-to-know in order to efficiently and effectively accomplish their mission.

This requirement for rapid, or even real-time, access to sensitive data has been heightened in the post-9/11 era. For example, in the United States, the Department of Homeland Security mandates and initiatives have increased the number of agencies requiring shared access for joint evaluation of sensitive information [Persinos & Evancha 2005].

Despite significant progress in MLS systems, and a strong array of products on the US Unified Cross Domain Management Office's (UCDMO's) Cross Domain Baseline list [Unified Cross Domain Management Office 2007], there are a number of issues and challenges which remain to be fully addressed.

5.1 Write Down

The "no write down" or "*-Property" of the Bell-LaPadula model [Bell & LaPadula 1973] forbids the transport of information downwards (system-high to system-low) in an MLS system. However, strict enforcement of such a policy can lead to isolation of lower-level users from data critical to the success of their mission. For example, in the "sensor to shooter" scenario [Smith 2007a], targeting information based on sensitive reconnaissance data must be passed down to weapons systems on low side networks.

This transfer of information from higher level domains down to lower level domains remains one of the key challenges facing MLS solutions. Though there are a number of products and technologies which aim to address this problem [Unified Cross Domain Management Office 2007], there remain issues with any given approach. For example, automated filters are not 100% accurate in identifying sensitive language/data, whilst human sanitization and review of documents being downgraded in classification is subject to human error (due to oversight or automatic acceptance of tedious repetitive approvals) [Note also that some document formats, such as Microsoft Word, can hide histories of changes, and hence hide potentially sensitive information from a naive reviewer]. The problems are exacerbated in the face of a malicious attack, exploiting known vulnerabilities in the automated and/or human sanitization process.

In addition, it is noted that modification of data by automated sanitization solutions can lead to unnecessary data loss and/or degradation of the quality/precision of the data.

One further aspect which must be taken into account is that of aggregation. This refers to the situation in which individual items of data are unclassified, but, taken as a collection, they convey sensitive data. This obviously presents issues for data guards filtering/sanitising content moving downwards, in that they may need to maintain an awareness of the history of content transferred in order to accurately infer the appropriate sensitivity of the information which they are currently being requested to release.

Finally, one additional area of focus regarding data transfer guards which is of great significance today but on which we feel requires more research is that of support for compartments/caveats, in contrast to the simpler hierarchical models, in light of increase in incidence of coalition operations and the need for sharing information across national boundaries.

Though significant progress is already being made towards automation of the review process during data transfer, as well as supporting increasingly complex data structures and file types, with bi-directional guards supporting many-to-many network connections, there are still opportunities and challenges to be addressed.

5.2 Covert Channels

One of the mechanisms by which a malicious user (or process) may transmit information from the high side to the low side of a system is via a covert channel. For example, information may be embedded using steganographic techniques in an otherwise innocent looking document/image/data stream.

Even variations in disk usage, memory usage or timing of processes may be used to signal between otherwise disconnected domains. For example, Anderson refers to the issue of polyinstantiation [Anderson 2008], where the same file name is used in system high and system low domains. Refusal to create the file in the system low domain, if it already exists in system high, will reveal to a system low user the existence of the file at the system high level, thereby potentially leaking information.

Information may be leaked unintentionally by innocent users/processes as well as by malicious agents—for example, Cache Attacks [Osvik, Shamir & Tromer 2006*a*] show how easily cryptographic keys in secure processes may be revealed by the state of the CPU cache to unprivileged processes running on the same CPU, even under conditions in which sandboxing, memory protection and virtualisation are employed.

Although it is typically not regarded realistic to eliminate ALL covert channels in an MLS system, deliberate introduction of noise in a channel may severely limit its capacity. Accordingly, DCID 6/3 [United States Central Intelligence Agency 1999] simply mandates at the top level (Protection Level 5) that a thorough search for covert channels be conducted (potentially via code review) and that the maximum bandwidth of those channels be determined.

Anderson notes that the DoD target of one bit per second, whilst adequate for preventing leakage of most data types, is clearly inadequate when considering the leakage of cryptographic keys, being relatively small and highly sensitive [Anderson 2008]. This motivates the usage of specialised cryptographic hardware in MLS systems, in order to isolate cryptographic keys, much more so than issues of performance.

Covert channels can emerge when low-level transactions are blocked by high-level transactions. Such covert channels can be avoided by giving priority to the low-level transactions. However, this can cause performance issues. Kaur et al. propose a concurrency protocol to avoid the performance downside of prioritising low-level transactions in an MLS database [Kaur et al. 2007].

Acknowledgement messages from the high side to the low side can also facilitate covert channels. Unfortunately, when acknowledgements are removed from a protocol, data can be lost when transmitted unsuccessfully. Kang et al. describe work on the Naval Research Laboratory (NRL) Data Pump [Kang, Moskowitz & Chincheck 2005], in which the covert channel resulting from allowing for an acknowledgement of message delivery is minimised to an acceptable value.

Based on existing research, we believe the identification, quantification and limiting of covert channels remains an area in which further contributions may be made.

5.3 Cascade Vulnerability Problem

The Cascade Vulnerability Problem(CVP) [Anderson 2008] [Bistarelli, Foley & O'Sullivan 2005], refers to the possibility of breaking security policy by connecting two systems that have been assured to span a set of security levels in such a way that the composite system spans a set of levels outside of the intended range. For example, in Figure 3, system F is evaluated at class B3 in the Orange Book, so it can span levels T through C. However, a malicious user able to break the other systems (evaluated only at class B2) is able to move T level content from System F via a clear path to C level content on System F, thus violating the security goals without ever having to compromise the class B3 system.

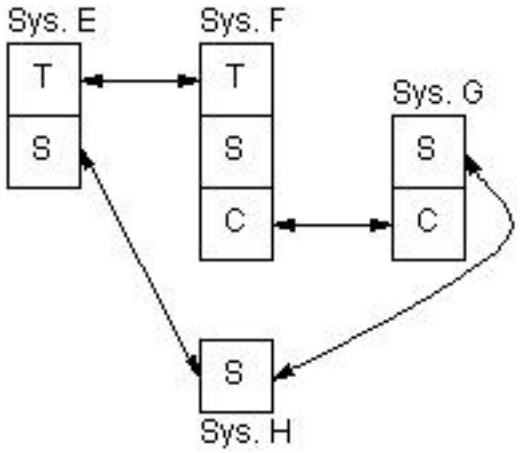

Figure 3: *Cascade Vulnerability Problem*

Bistarelli et al. and Servin et al. propose an approach to address this problem in an MLS system [Bistarelli, Foley & O'Sullivan 2005] [Servin et al. 2007]. Rather than disconnecting all connections on the network, their approach is one of a weighted optimisation, minimising the number of disconnections [Bistarelli, Foley & O'Sullivan 2005] by considering the service impact of those disconnections [Servin et al. 2007].

There is scope for further contribution on such a significant issue. One particular aspect which we have not seen addressed as yet is a solution which can take into account the dynamic ad-hoc nature of modern networks. As the topology and identity of the nodes changes in a network of MLS systems, itself a research area of considerable challenge, the CVP needs to be continually reassessed.

5.4 Multi-Level Applications

The recent trend, due to increasingly affordable network infrastructure, has been towards deployment of Multiple Single Levels of Security (MSLS) systems, in which separate networks are each dedicated to a single security level. Evaluation/assessment focus is then on the data guards mediating data transfers between the networks (see the discussion of the Write Down problem above). Users requiring convenient simultaneous access to data at multiple levels then utilise an access solution [Unified Cross Domain Management Office 2007] providing a single display with separate windows onto each network, together with perhaps limited capabilities for mediated data transfer between the windows. Such solutions reduce the user's 'desktop footprint' and increases ease of use, though there still remain considerable barriers to the user.

The next step of integration for the user, we believe, is to begin to fuse the information together seamlessly, as opposed to its maintenance in separate windows. This path has already been begun, at a very basic level, with Trusted Network Environment's (TNE's) [General Dynamics 2007a] capability to expose different information to different users visiting the same URL, and also the read-only implementation for XML content by solutions such as PeBL/Siftex [McLean 2003] in a room display context. We would anticipate that a generic solution whereby information in a document (web, Word, Excel, etc.) is contained at multiple levels and only that information appropriate to the viewing user's level is visible, would be the next logical step. This would be further extended for multi-user solutions. Some progress towards such a generic planned robust solution for filtered content on a user desktop has recently been made [Owen et al. 2011].

This ability to seamlessly read information in the same generic document at multiple security levels would be a major improvement in the user experience. The additional ability to create and edit such composite level documents at the user terminal (c.f. some specialised creation process) would be an added advantage as a further step. However, we foresee several issues to be resolved by research activity in terms of editing of documents to which a user has only limited visibility, resulting in context-dependent impacts on users at other levels. In addition, problems of inference, already present in the read-only solution, from knowledge of the presence and size of higher-classified sections of information, will need to be addressed.

Such fusion support would be enabled as a particular instance of the development of MLS-capable/MLS-aware applications, i.e. the critical point is that we see the next step in the development of MLS technology as progressing yet further up the "stack". Currently most MLS instances involve generic applications (or even operating systems) running unmodified in a sandboxed environment, with little/no knowledge of any MLS context in which they operate. This further development opportunity has been foreshadowed and promised since the early days of MLS, though has yet to be fully realised.

6 Critical Information Infrastructure Protection Security (CIIPSec)

Critical Infrastructure is the set of systems and services that are essential for society to function in the modern world. The following are examples of Critical Infrastructure: electricity generation, transmission and distribution, food production, financial services, health services, law enforcement, military, oil and gas production and distribution, telecommunication, transportation and water (provision of fresh water and disposal of waste water).

Due to the critical nature of these functions, many governments around the world have put a very high priority on protecting Critical Infrastructure. This has been driven, in large part, by terrorist activities such as the Oklahoma City and World Trade Center bombings and the 9/11 terrorist attacks. A number of low-level attacks have been made to Critical Infrastructure, but to date the damage has been minimal.

Critical Information Infrastructure Protection Security (CIIPSec) defines the measures taken to ensure the protection of the Critical Infrastructure from attack.

Supervisory Control and Data Acquisition (SCADA) is the technology that enables Critical Infrastructure systems to be monitored and controlled. Remote sensors monitor various data points (such as pressures or voltages) in the systems and relay the data to the Control system, which will send control signals to the devices in the system when required.

According to Yardley a number of US Government documents have been published outlining guidelines for protecting Critical Infrastructure in the US [Yardley 2008]. These include "Critical Foundations: Protecting America's Infrastructures" [President's Commission on Critical Infrastructure Protection 1997], "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism" [Committee on Science and Technology for Countering Terrorism, National Research Council 2002] and "Roadmap to Secure Control Systems in the Energy Sector" [J. Eisenhauer & O'Brien 1997].

A number of major laboratories are conducting large-scale research on CIIPSec in the US. These include the Idaho National Laboratory (INL), the Pacific Northwest National Laboratory (PNNL) and Sandia National Laboratory Centre for SCADA Security. These and other major research laboratories have joined together to create the National SCADA Test Bed. This is located within the 2300 km^2 INL, located in south-eastern Idaho and contains nuclear reactors, a working power grid, chemical plants and laboratories used to conduct research into protecting SCADA systems from cyber attack.

Research into SCADA security is also being carried out in numerous universities, by SCADA vendors and SCADA special-interest groups.

6.1 Current research

There is a considerable amount of effort being put into research into improving the security of SCADA systems. Some of the work being done includes:

- significant research on improving the security of SCADA protocols, either by developing more secure versions of SCADA protocols such as DNP3 and MODBUS or by tunnelling the protocol (e.g. using SSL/TLS);
- electricity companies in the US are looking at pushing the monitoring of electricity parameters and control of local appliances out into the customers premises (the so-called Smart Grid [Zetter 2009]). Some research is being done into the security implications of the Smart Grid. It is widely regarded that the Smart Grid is being rolled out before enough research has been done into the security aspects;
- intrusion detection and prevention for SCADA systems [Rrushi 2006];
- measures to improve on the security of SCADA systems as an entity [*Improved Security for SCADA Systems* 2008] and [Naedele 2007];
- modelling SCADA systems and the effect of cyber attacks [McDonald & Richardson 2009], [*The Viking Project* 2009];
- studying SCADA specific malware [Carcano et al. 2008], [Carcano et al. 2009], [K. Baek & Smith 2007].

6.2 Rationale for further SCADA Research

The SCADA systems which are used to monitor and control the Critical Infrastructure systems use protocols that were not designed with security in mind. This was mainly due to the fact that the systems themselves tended to be isolated and physical security was the main issue. When Internet access became readily available, the corporate systems were connected to the Internet. For business purposes, it was useful to connect the Control system to the Corporate system for the purpose of monitoring the status of the system. While this may be convenient for the enterprise, it makes it possible for someone on the Internet to access the Control system. Also in some cases there have been links from the SCADA vendor networks to the Control network, so that the vendor could make modifications to the system without having to visit the site. This presents another attack vector, particularly as in some cases the link has entered behind the Control-Corporate Firewall.

To date there have been no incidents related to cyber attacks on SCADA systems that have resulted in loss of life or large-scale impact to critical services. However, there have been instances where loss of life or loss of critical services has occurred due the SCADA related incidents. These were not due to malicious attacks, but errors in the control system itself or SCADA system performance degradation. Examples are the Bellingham fuel pipeline rupture of 1999 [NTSB 2002] and the major blackout of parts of the NE of the US in 2003 [*The Great 2003 Northeast Blackout and the $6 Billion Software Bug* 2007]. In both cases it was a combination of a number of factors that resulted in the problem, but they both involved serious problems in the control system.

In the case of the Bellingham fuel pipeline rupture there were design flaws as well as a physical defect in the pipeline that had weakened it. The reason that the pressure build-up that caused the rupture was not detected was that the SCADA operator was working on

a new database schema on the live SCADA system. After the operator saved the new schema, the SCADA server became unresponsive and it is presumed that an error in the database schema had caused this. While the system could no longer be monitored the pressure built up in the pipeline and it ruptured, resulting in a little over a million litres of petrol being released into the nearby creek. The petrol ignited and resulted in the deaths of three people.

When the 2003 blackout of a large part of the North East of the US occurred, cyber-terrorism was initially suspected. The blackout was actually triggered by a power cable sagging under heavy load and coming into contact with untrimmed trees. Because of a race condition in an SCADA alarm subsystem, the SCADA operators were not aware of the failure. For this reason, the SCADA operators were not able to inform the neighbouring power utilities about the problem and a cascading failure then occurred.

Another incident happened when a Harrisburg, Pennsylvania water treatment plant was infected by SPAM malware [Hayes 2006]. One of the servers in the plant was infected when an employee's laptop was connected to the Control network. In this case there were no problems with the running of the SCADA system, but if the malware caused the CPU loading on the server to increase, it may have caused problems. And if it was in a nuclear power plant rather than a water treatment plant, the consequences may have been severe.

These examples show that seemingly minor changes to a SCADA system can sometimes result in dramatic unforseen outcomes. It also shows that a cyber attacker does not necessarily need to have an in-depth knowledge of the system to cause enormous damage. There are numerous documented occurrences of breaches of Critical Infrastructure by hackers that have not resulted in any damage, but the potential is there for small modifications to result in catastrophic consequences, whether intended or not.

6.3 Possible new CIIPSec Research

This section outlines new or emerging areas of research in CIIPSec, as well as discussion of some practical security measures. There are two main areas of Critical Infrastructure, those that use SCADA systems (such as Power, Water, Transportation and Oil and Gas) and those that do not (such as Air Traffic Control, Finance and Telecommunications). The following are possible areas for further research and/or development in the securing of SCADA Systems.

6.3.1 Automatic Firewall shutdown or modification of firewall rules in response to cyber attack

The connection of the Corporate and Control networks is present for convenience, so that the status of the Control system can be monitored by management from the Corporate network. The SCADA System does not require this connection and will continue to operate unaffected if the connection is severed. If a possible attack is detected by the Intrusion Detection System (IDS), it may be advantageous to have the firewall between the Control and Corporate systems automatically shut down, to cut any control channel, while the incident is investigated. Alternatively, the firewall rules could just be modified to just

stop some or all of the traffic. However, turning off the firewall would ensure that there was no possibility of a command channel being present.

6.3.2 Better architectures for the SCADA Control-Corporate Interface

The current best practices for the network architecture for Control Systems are outlined in [Idaho National Laboratory 2006]. This is a layered, defence-in-depth strategy with specific zones separated by strategically positioned firewalls and logically placed IDS sensors. While this divides the SCADA enterprise into separate security zones, a misconfigured firewall, very skilled hacker or inside attacker can still potentially access the Control system from the Corporate network. The positioning of data diodes on any connections from the Control network to the outside would allow data on the state of the system to be sent to servers on the Corporate network, but would eliminate the possibility of a control channel into the Control network. This would also mean that SCADA vendors would no longer be able to access the Control system remotely, which would remove another attack vector. Note that sometimes there may be a business imperative for this connection, e.g. spot electricity pricing, and so it is acknowledged that this may be difficult in some systems.

6.3.3 Making SCADA systems more resilient

SCADA systems are comprised of a set of sensors and controllers, linked to the controlling computers. These systems were generally not designed with security in mind and the consequences of minor unintended or accidental changes can have major consequences. There is scope for research into how to make SCADA systems more resilient, so that incidents such as the Bellingham pipeline rupture are less likely to occur. Verissimo discusses the challenges of architecting resilient Critical Information Infrastructures [Verissimo 2008].

6.3.4 Security for Smart Grid systems

The US is in the process of installing smart meters in a large number of sites across the country [Zetter 2009]. This is effectively extending the SCADA systems to millions of homes, factories and offices. An Australian initiative is also underway [*Smart Grid R&D Roadmap for Australia* 2010]. Clementine discusses the vulnerabilities of the Smart Grid [Clementine 2009]. But it would seem that much further research in this area would be of critical import.

6.3.5 Use of application white-listing in SCADA Systems

Application whitelists take the opposite approach to traditional anti-virus (A/V) systems. The whitelist is the list of all programs that are permitted to execute on the computer. The advantages over traditional A/V technology are:

- there is no need to frequently update with new virus signatures,
- the processing overhead of the A/V software will be greatly reduced, and

- there is no need to manually update the virus signatures.

  However, we note that zero day exploits remain an issue.

6.3.6 Draft policies regarding Security of Critical Infrastructure

Currently it seems that the operators of SCADA systems trade off convenience at the expense of security. There is a business case for having the Control system connected to the Corporate system, but this needs to be weighed up against the security implications of connecting a network that uses insecure protocols, commonly with quite old hardware (with a longer refresh cycle than typical for general IT systems), to the outside world. The development of a set of recommended best practices may be useful. This would be based upon the INL best practices [Idaho National Laboratory 2006], but would extend it to include policies such access control, physical security, password standards, restrictions on the use of mobile devices and flash drives onsite, minimum standards for IDS/IPS usage and controls on the software that is permitted to run on Control system computers.

6.3.7 Research on the detection of Insider attacks on SCADA systems

Currently security monitoring of SCADA systems uses IDS technology to detect anomalous network traffic, which may be related to an attempt to hack the SCADA system. In the case of an inside attack, the user will most likely have the authority to make changes to the SCADA system. Detection of such attacks when they occur would be quite difficult and may require fusing of various pieces of information that may seem innocuous when taken in isolation, but when put together suggest the behaviour is anomalous.

7 Summary

In this report, we have identified a number of research opportunities across a range of selected domains and aspects of Information Security.

For Security Policies, the research challenges noted include introducing some commonality in specification languages and implementation mechanism for policies, together with associated practical and usable modelling and analysis tools, and we identified the issues of keeping pace with technological innovation. In relation to Security Architectures, the challenge is to build on initial research in providing dynamic and flexible architectures. In particular, architectures capable of supporting risk-based and reputation-based access control models, for example, within such a dynamic architectural context.

With regard to Authentication and Authorisation, we see the key opportunities in various areas as:

- Protection and Storage of Credentials: Opportunities exist for enhanced protection of credentials on security tokens, improved recovery mechanisms and increased resistance to attacks on credentials during usage.
- Privacy and Anonymity: Though the capability of the protocols to support some of the requirements is available, there remains much to be done in refining/enhancing such schemes and in applying and integrating them into real-world systems. In addition, tying in with Unified Security, there is dichotomy between requirements to track and correlate the activities of individuals with the need for privacy. Moreover, concealing such correlations from less trusted systems, together with requirements to minimise information leakage as much as possible even between trusted systems, offers many opportunities for further research.
- Biometrics: As well as improvements in security, usability and performance of existing and novel biometric schemes, another domain identified is that of social forms of authentication.
- Secure Localisation and Tracking: Securely identifying the location or proximity of a device is a critical issue for a number of scenarios.
- Relay and Man-in-the-Middle Attacks: the use of protocols based on physical properties may present a means to provide for authentication not only resistant to traditional Man-in-the-Middle style attacks, but also address some of the future threats which quantum computers present to conventional protocols.

As regards Unified Security, we assert that further investigation is needed to explore and describe security objectives such as convenience, that focus on ensuring that due care and diligence in secure environments can be exercised whilst minimising the requirements and impact on users. To this end, the two major pursuits we identified in the incorporation of future technologies into unified security are the needs for automation, to help users reduce human error, and simplification, so that user compliance is easier. Furthermore, there is a need to investigate the potential for frameworks to describe the full gamut of unified security as well as describing solutions that will help facilitate their adoption, and we anticipate continued interest in this area from government and industry.

We have outlined a number of areas in which there are immediate and significant research and development opportunities within the MLS space. Though over recent years there has been a continuous improvement in usability, functionality and security of MLS solutions, we believe that there remain to be made significant advances, particularly in the area of usability.

Finally, in the CIIPSec area, research opportunities include focus on improving architectures for control systems via defence-in-depth strategies, together with improved resilience of SCADA systems, whilst also developing appropriate policies and best practices for CIIPSec systems. Tying into the Unified Security domain, opportunities exist to strengthen systems against insider attacks through fusion of information from a variety of sources.

References

Abraham, T., Long, B., Philp, D. & Windows, S. (2010) A unified security framework: Realising security through convenience. Submitted to SEC-2010.

Adams, A. & Sasse, M. A. (1999) Users are not the enemy, *Communications of the ACM* **42**(12).

Al-Kuwari, S. & Wolthusen, S. (2010) Serial hook-ups: A survey of forensic localization and tracking mechanisms in short-range and cellular networks.

Anderson, M., North, C. & Yiu, K. (2008) *Towards Countering the Rise of the Silicon Trojan*, Technical report, Defence Science and Technology Organisation. URL – `http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/9736/1/DSTO-TR-2220%20PR.pdf`. DSTO-TR-2220.

Anderson, R. (2008) *Security engineering*, 2nd edn, Wiley.

Ashkenazi, A. (2005) Security features in the i.mx31 and i.mx31l multimedia applications processors. URL – `http://www.freescale.com/files/32bit/doc/white_paper/IMX31SECURITYWP.pdf`.

Attorney General's Department (2007) Australian government protective security manual. URL – `http://intranet.defence.gov.au/dsa/DSM/chm/scr/forms/PSM.pdf`.

Bell, D. E. & LaPadula, L. J. (1973) *Secure computer systems*, Technical Report MTR-2547 (ESD-TR-73-278), Mitre Corporation. vols I-III.

Bertino, E. & Martino, L. D. (2007) A service-oriented approach to security - concepts and issues, pp. 7 –16.

Billard, A., Howard, A., McLean, P. & Ozols, M. (2002) *A Survey of Security Policy Languages*, Technical report, DSTO.

Billard, A. & Long, B. (2009) *Dynamic Security Architectures: Architecture and Case Studies*, Technical report, DSTO.

Billard, A. & Ozols, M. (2006) *ACSI33 Network Security Analysis*, Technical report, DSTO.

Bistarelli, S., Foley, S. N. & O'Sullivan, B. (2005) A soft constraint-based approach to the cascade vulnerability problem, *Journal of Computer Security* **13**(5), 699–720.

Brainard, J., Juels, A., Rivest, R., Szydlo, M. & Yung, M. (2006) Fourth-factor authenticatin: Somebody you know. URL – `http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/fourth-factor/ccs084-juels.pdf`.

Brands, S. A. (2000) *Rethinking public key infrastructures and digital certificates*, MIT Press.

Buecker, A., Crowther, D., de Valence, F., Monteiro, G., Oosterhof, M., Quap, A., Schuett, M. & Stockmann, K. (2009) Introducing the ibm security framework and ibm security blueprint to realize business-driven security, An IBM RedGuide Publication. URL – http://www.redbooks.ibm.com/abstracts/redp4528.html.

Camenisch, J. & Lysyanskaya, A. (1991) An efficient system for non-transferable anonymous credentials with optional anonymity revocation, *in Adanvces in Cryptology - EUROCRYPT 2001. Lecture NOtes in Computer Science.*, Vol. 2045, Springer, pp. 93–118.

Campbell, R. H., Qian, T., Liao, W. & Liu, Z. (1996) Active capability: A unified security model for supporting mobile, dynamic and application specific delegation, Security White Paper, System Software Research Group, Department of Computer Science, University of Illinois at Urbana, Champaign. URL – http://choices.cs.uiuc.edu/Security/Papers/delegate.ps.

Carcano, A., Fovino, I., Masera, M. & Trombetta, A. (2008) Scada malware, a proof of concept, *in Critis'08*. URL – http://www.springerlink.com/content/a024m666158171m5/.

Carcano, A., Fovino, I., Masera, M. & Trombetta, A. (2009) An experimental investigation of malware attacks on scada systems. URL – http://linkinghub.elsevier.com/retrieve/pii/S1874548209000419.

Chaum, D. (1985) Security without identification: transaction systems to make big brother obsolete, *Communications of the ACM* **28**(10), 1030–1044.

Cheng, P.-C., Rohatgi, P., Keser, C., Karger, P. A., Wagner, G. M. & Reninger, A. S. (2007) Fuzzy multi-level security: An experiment on quantified risk-adaptive access control, *in SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy*, IEEE Computer Society, Washington, DC, USA, pp. 222–230.

Clementine, J. (2009) The security vulnerabilities of the smart grid. URL – http://www.ensec.org/index.php?option=com_contentview=articleid=198:the-security-vulnerabilities-of-smart-gridcatid=96:contentItemid=345.

Committee on Science and Technology for Countering Terrorism, National Research Council (2002) *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. URL – http://www.nap.edu/catalog/10415.html.

Contos, B. & Kleiman, D. (2006) *Enemy at the Water Cooler: Real-Life Stories of Insider Threats and Enterprise Security Management Countermeasures*, Syngress Publishing, Inc.

Contos, B. T., Hunt, S. & Derodeff, C. (2007) *Physical and Logical Security Convergence: Powered by Enterprise Security Management*, Syngress Publishing.

Defence Science and Technology Organisation (2008) Australian defence science. URL – http://www.dsto.defence.gov.au/attachments/ADSVol16No2.pdf. Available online (16 pages).

Desmedt, Y. (2005) Threshold cryptography, *in Encyclopedia of Cryptography and Security*. DBLP:reference/crypt/2005.

Farrell, S. & Housley, R. (2002) An internet attribute certificate profile for authorization.

Forristal, J. (2006) Analysis: Physical/logical security convergence. URL – `http://www.networkcomputing.com/wireless/analysis-physicallogical-security-convergence.php`.

General Dynamics (2007a) Trusted network environment (tne).

Grove, D., Murray, T., Owen, C., North, C., Jones, J., Beaumont, M. & Hopkins, B. (2007) An overview of the annex system. URL – `http://www.acsac.org/2007/papers/29.pdf`. Available online (12 pages).

Hamilton, B. A. (2005) Convergence of enterprise security organizations, Security White Paper, The Alliance for Enterprise Security Risk Management. URL – `http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=43025`.

Hayes, F. (2006) Botnet threat. URL – `http://www.computerworld.com/s/article/271922/Botnet_Threat?taxonomyId=17pageNumber=2`.

Heyer, R. (2008) *Biometrics Technology Review 2008*, Technical report, Defence Science and Technology Organisation. URL – `http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/9704/1/DSTO-GD-0538%20PR.pdf`. DSTO-GD-0538.

Idaho National Laboratory (2006) *Control Systems Cyber Security: Defense in Depth Strategies*, Technical report, Idaho National Laboratory. URL – `http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf`. External Report #INL/EXT-06-11478.

Improved Security for SCADA Systems (2008) URL – `http://www.springerlink.com/content/a024m666158171m5/`.

Indiana Office of Technology (2007) Information security framework state of indiana information resources policy and practices indiana office of technology version 2.0, Indiana State Online Publications. URL – `http://www.in.gov/iot/files/Information_Security_Framework.pdf`.

J. Dawkins, K. Clark, G. M. & Papa, M. (2005) A framework for unified network security management: Identifying and tracking security threats on converged networks, *Journal of Network and Systems Management* **13**(3), 253–267.

J. Eisenhauer, P. Donnelly, M. E. & O'Brien, M. (1997) Roadmap to secure control systems in the energy sector. URL – `http://www.oe.energy.gov/csroadmap.htm`. Available online (58 pages).

Jackson, W. (2010) Engineer shows how to crack a 'secure' tpm chip. URL – `http://gcn.com/articles/2010/02/02/black-hat-chip-crack-020210.aspx`.

Josang, A., Ismail, R. & Boyd, C. (2007) A survey of trust and reputation systems for online service provision, *Decision Support Systems* **43**(2), 618–644.

K. Baek, S. Bratus, S. S. & Smith, S. (2007) *Dumbots: Unexpected Botnets through Networked Embedded Devices*, Technical report, Dartmouth College Computer Science. URL – `http://www.ists.dartmouth.edu/library/342.pdf`. Technical Report TR2007-591.

Kang, M., Moskowitz, I. & Chincheck, S. (2005) The pump: a decade of covert fun, pp. 7 pp. –360.

Kaur, N., Singh, R., Misra, M. & Sarje, A. (2007) A secure concurrency control for mls/ddbss, pp. 41 –46.

Kindberg, T. & Zhang, K. (2002) Validating and securing spontaneous associations between wireless devices.

Kobsa, A., Sonawalla, R., Tsudik, G., Uzun, E. & Wang, Y. (2009) Serial hook-ups: A comparative usability study of secure device pairing methods.

Kocher, P., Jaffe, J. & Jun, B. (1999) Differential power analysis, *in Lecture Note in Computer Science: Advances in Cryptology - Crypto 99 Proceedings*, Vol. 1666, Springer-Verlag.

Lan, N. T. H. & Hang, N. T. T. (2008) An approach to protect private key using fingerprint biometric encryption key in biopki based security system, pp. 1595 –1599.

Lopez, L., Redondo, L., Martinez, J.-F., Ramiro, M., Hernandez, V., Bonilla, F. & Breton, F. (2007) Secuarea: Security in physical and logical areas, pp. 95–100.

McDonald, M. & Richardson, B. (2009) Position paper: Modeling and simulation for process control system cyber security research, development and applications. URL – `http://cimic.rutgers.edu/positionPapers/MichaelMcdonald-paper.pdf`.

McGraw, R. (2009) Risk adaptable access control.

McIlwraith, A. (2006) *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*, Gower Publishing Limited.

McLean, P. (2003) A secure pervasive environment, *in Proceedings of the Australasian Information Security Workshop (AISW'03)*, Vol. 21 of *Conferences in Research and Practice in Information Technology*, Australian Computer Society, pp. 67–75.

Naedele, M. (2007) Addressing it security for critical control systems, pp. 115 –115.

Naufel do Amaral, F., Bazilio, C., Hamazaki da Silva, G., Rademaker, A. & Haeusler, E. (2006) An ontology-based approach to the formalization of information security policies, pp. 1 –1.

Nortel (2005) Nortel unified security framework for corporate and government security, Position paper, Nortel. URL – `http://www.nortel.com/solutions/security/collateral/nn104120-051705.pdf`. Available online (10 pages).

NTSB (2002) Pipeline accident report: Pipeline rupture and subsequent fire in bellingham, washington june 10, 1999, Pipeline Accident Report NTSB/PAR-02/02. URL – `http://www.ntsb.gov/publictn/2002/par0202.pdf`. Available online (88 pages).

Oh, H. & Jin, S. (2008) The security limitations of sso in openid. URL – http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04494089.

Open Security Exchange (2007) Physical/IT security convergence: What it means, why it's needed, and how to get there, White Paper. URL – http://whitepapers.techrepublic.com.com/abstract.aspx?docid=966797.

Osvik, D. A., Shamir, A. & Tromer, E. (2006*a*) *Cache attacks and countermeasures: the case of AES*, Vol. 3860 of *Lecture Notes in Computer Science*, Springer, pp. 1–20.

Osvik, D., Shamir, A. & Tromer, E. (2006*b*) Cache attacks and countermeasures: the case of aes, *in Lecture Note in Computer Science: Proceedings of the Cryptographers' Track (CT-RSA) at the RSA Conference 2006*, Vol. 3860, Springer-Verlag, pp. 1–20.

Owen, C., Grove, D., Newby, T., Murray, A., North, C. & Pope, M. (2011) Prism: Program replication and integration for seamless mils, *in Security and Privacy (SP), 2011 IEEE Symposium on*, pp. 281 –296.

Persinos, J. & Evancha, D. (2005) *Multi-level security strategies for the federal government*, Technical report, Larsten Business Reports.

President's Commission on Critical Infrastructure Protection (1997) Critical foundations: Protecting america's infrastructure. URL – http://fas.org/sgp/library/pccip.pdf. Available online (192 pages).

Ravikanth, P. (2001) Physical one-way functions.

Rrushi, L. (2006) Scada intrusion prevention system. URL – http://perso.telecom-paristech.fr/~legrand/CI2RCO-conf/Article/scada_rrushi.pdf.

Sarbanes, P. & Oxley, M. (2002) An act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes., Congressional Record, Vol. 148. URL – http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html.

Servin, C., Ceberio, M., Freudenthal, E. & Bistarelli, S. (2007) An optimization approach using soft constraints for the cascade vulnerability problem, pp. 372 –377.

Shor, P. W. (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. on Computing* pp. 1484–1509.

Smart Grid R&D Roadmap for Australia (2010) URL – http://www.smartgridaustralia.com.au/uploads/documents/SGA_RD.pdf.

Smith, R. E. (2007a) Introduction to multilevel security.

Sourceforge (n.d.) Password safe. URL – http://passwordsafe.sourceforge.net.

Srivatsa, M., Rohatgi, P. & Balfe (2008) Securing information flows: A quantitative risk analysis approach, *in Military Communications Conference*, pp. 1–7.

Stajano, F., Wong, F. & Christianson, B. (2010) Multichannel protocols to prevent relay attacks.

The Great 2003 Northeast Blackout and the $6 Billion Software Bug (2007) URL – http://www.availabilitydigest.com/private/0203/northeast_blackout.pdf. Available online (7 pages).

The SecHCI Project (n.d.) URL – http://www.hooklee.com/SecHCI/.

The Viking Project (2009) URL – http://www.vikingproject.eu/page1.php.

Tromer, E., Osvik, D. & Shamir, A. (2009) Efficient cache attacks on aes, and countermeasures, *Journal of Cryptology* (1), 37–71. URL – http://www.springerlink.com/content/73876v1qq07q0277/.

Trusted Computing Group (n.d.) URL – http://www.trustedcomputinggroup.org/.

Tyson, D. (2007) *Security Convergence: Managing Enterprise Security Risk*, Butterworth-Heinemann, Newton, MA, USA.

Unified Cross Domain Management Office (2007) *Cross domain inventory 2.1*, Technical report.

United States Central Intelligence Agency (1999) *Director of Central Intelligence directive 6/3: protecting sensitive compartmented information within information systems*, Technical report.

US Department of Homeland Security (2003) Homeland security presidential directive 7: Critical infrastructure identification, prioritization, and protection, Homeland Security Presidential Directive, US Department of Homeland Security. URL – http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.

US Department of Homeland Security (2004) Homeland security presidential directive 12: Policy for a common identification standard for federal employees and contractors, Homeland Security Presidential Directive, US Department of Homeland Security. URL – http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm.

Verissimo, P. (2008) Challenges of architecting resilient critical information infrastructures. URL – http://www.nis-summer-school.eu/nis08/presentations/paulo_verissimo_lecture.pdf.

Weir, C. S., Douglas, G., Carruthers, M. & Jack, M. (2009) User perceptions of security, convenience and usability for ebanking authentication tokens, *Computers & Security* **28**, 47–62.

Wilson, G. & Tharakan, U. O. (2003) Unified security framework, *in Proceedings of the 1st international symposium on Information and communication technologies*, Trinity College Dublin, pp. 500–505.

Yardley, T. (2008) Scada: issues, vulnerabilities, and future directions, *;login:* (6), 14–20. URL – http://www.usenix.org/publications/login/2008-12/pdfs/yardley.pdf.

Zetter, K. (2009) Feds' smart grid race leaves cybersecurity in the dust.

Zhang, L., Brodsky, A. & Jajodia, S. (2006) Toward information sharing: Benefit and risk access control (barac), *Policies for Distributed Systems and Networks, IEEE International Workshop on* **0**, 45–53.

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION DOCUMENT CONTROL DATA	1. CAVEAT/PRIVACY MARKING

2. TITLE	3. SECURITY CLASSIFICATION
A Perspective on Research Challenges in Information Security	Document (U) Title (U) Abstract (U)
4. AUTHORS	5. CORPORATE AUTHOR
Tamas Abraham, David Adie, Angela Billard, Paul Buckland, Michael Frangos, Ben Long, Martin Lucas, Paul Montague, Dean Philp, Simon Windows	Defence Science and Technology Organisation PO Box 1500 Edinburgh, South Australia 5111, Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO–TN–1035	015-129	Technical Note	November, 2011

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. No. OF PAGES	12. No. OF REFS
2011/1105610/1	07/012	CIOG	34	91

13. URL OF ELECTRONIC VERSION	14. RELEASE AUTHORITY
`http://www.dsto.defence.gov.au/publications/scientific.php`	Chief, Command, Control, Communications and Intelligence Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for Public Release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SOUTH AUSTRALIA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS

No Limitations

18. DSTO RESEARCH LIBRARY THESAURUS

Information Security

19. ABSTRACT

This report considers a number of selected areas of security technology and practice. The focus is on exposing and highlighting research gaps and opportunities in the current security state of the art within these areas, both in terms of implementation practice and of the literature.