Cross-Domain Information Sharing in a Tactical Environment

Mel Crocker
General Dynamics Canada

Net-centric warfare in the full spectrum of operations mandates information sharing among non-traditional partners across security domains. This information sharing requires the exploitation of complex technologies and generates significant security challenges. Traditional information assurance solutions to support cross-domain information sharing have focused heavily on preventive measures, restricting information flow and reducing the risk of information compromise. This constraint on information flow directly opposes the duty of the warfighter to share information. A holistic solution involving robust software components, auditing, and permission management will reduce the risks of unauthorized information exposure to adequate levels without imposing severe information flow constraints.

Net-centric warfare is about *employing information age concepts to increase combat power in war and mission effectiveness in operations other than war* [1]. By linking sensor networks, command and control networks, and shooter networks, warfighters can achieve efficiencies in the full spectrum of operations by sharing information in a common operating environment. Unity of effort across organizational, national, technical and spatial boundaries is necessary. Warfighters have a *duty to share* information with others, and in the tactical environment it is not always obvious who needs the information and exactly how that information will be used. In some respects, sharing information is a leap of faith that the recipient will treat the information properly, not abusing the implied trust.

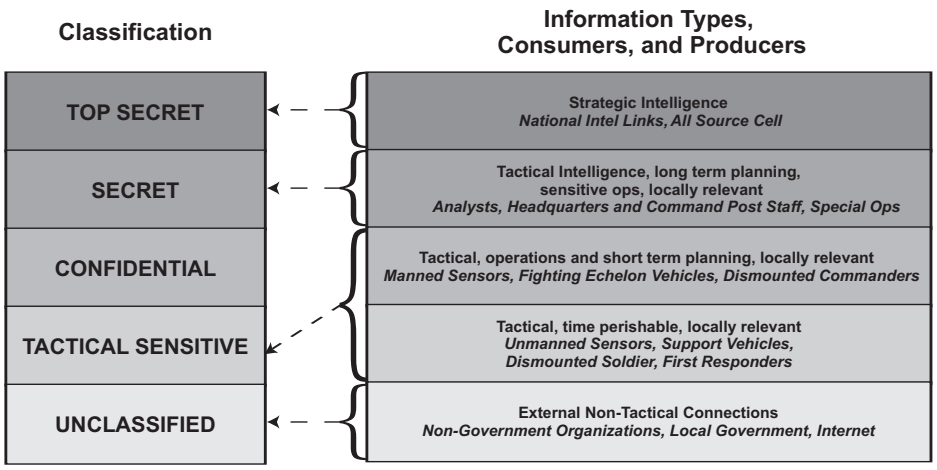
This article introduces aspects of the tactical environment and some of the complexities of sharing information in a tactical network, describes the security challenges and suggests a high-level security architecture that applies adequate measures without compromising the information sharing needs of the warfighter. Secure solutions to these types of complex net-centric problems are made achievable with the increased assurance that can be placed on well-developed and tested software.

The Tactical Information Environment

Information in modern tactical networks is generated from multiple sources: global positioning system receivers, unmanned and manned sensors, observations and recordings of individuals, higher command and intelligence networks, the Internet, and a variety of other sources. In modern operations, information must flow quickly from sensors to fusion processes to analysts and decision makers and, finally, to those who must execute action. Taking more than a few minutes from detection to action often significantly reduces the effectiveness of operations.

Beyond the need for quick and wide information flow, the tactical information environment is also made complex with differences in information sensitivity. As one moves from the fighting echelon of a tactical deployment back to national headquarters, there are fundamental differences in the sensitivity of data. For tactical elements in direct contact with the enemy, the majority of information processed is highly time perishable and generally focused on the following questions: Where am I? Where are my buddies? Where is the enemy, and what are his capabilities? Within a tactical headquarters environment, the information becomes more sensitive as plans are generated, intelligence is analyzed, and the larger tactical environment is monitored. Current government sensitivity labels and handling are based on definitions of sensitivities that were created for nationally sensitive information, only loosely relevant in the tactical environment. Executive Order 12958 describes three subjective classifications based on the damage resulting from compromise: TOP SECRET – *exceptionally grave* damage; SECRET – *serious* damage; and CONFIDENTIAL – damage to the national security [2]. These are relatively subjective groupings based on an interpreter's understanding of the anticipated impact of unauthorized disclosure and centered on national security. There is no time perishable consideration and all consideration is toward the affect on national security, not the impact on tactical operations; national security and tactical operations are related but are not the same thing. Figure 1 illustrates the five types of information and where they likely fit in current classifications. The figure introduces the term *tactical sensitive* for information falling between confidential and unclassified; it describes much of the information handled in a tactical environment.

Figure 1: *Information Sensitivity Classifications in the Tactical Environment*



Beyond the varied information sensitivities, warfighters also face the significant challenge of information overload and determination of correct distribution. To deal with this, Alberts and Hayes suggest that systems must transition from information *push* designs toward information *post* and *smart pull* designs.

> Moving from a push to a post and smart pull approach shifts the

> problem from the owner of information having to identify a large number of potentially interested parties to the problem of having the individual who needs information identifying potential sources of that information. The second problem is a far more tractable one. This is because it is much easier for the individual who has a need for information to determine its utility than for the producer to make this judgment. [3]

This concept does not line up with the security tenet of limiting information distribution based on *need to know* and forces a new paradigm to providing adequate information assurance measures. The tactical environment will always have a need for some information to be pushed to consumers because there are alerts and critical developments that must be pushed to specific subscribers, but this *pushed* information is only a subset of the total information shared in the tactical environment.

When information of a like sensitivity is distributed within a defined community of interest, it is considered an information domain and is managed with a single security policy[1]. Often information must flow between domains; the cross-domain information exchanges must be sufficiently flexible to address the information sharing paradigm shift necessary for net-centric warfare.

Legacy Approaches to Cross-Domain Solutions (CDS)

Cross-domain information flow has always been considered a security-critical event and the risks associated with this type of transfer have been mitigated with a security guard. When the security guard is put into a system context, it is often referred to as a CDS. In the simplest sense, among other functions, a CDS confirms that information has been correctly downgraded when traveling from a higher domain to a lower domain, ensures that malware cannot move from the lower to the higher domain and confirms no information leakage from a higher to a lower domain. They are programmed for specific data formats, formally applying preestablished sets of rules and in general are very expensive. An example of a certified security guard is the software application Radiant Mercury which was developed under contract for the U.S. Navy by Lockheed Martin Corporation. When placed on a suitably trusted platform, this product automatically sanitizes, filters, and downgrades formatted classified documents.

Researchers from the Mitre Corporation have studied the evolution of guards toward better supporting the demands of today's warfighter and have concluded that guards should become more flexible, capable of handling information exchanges with libraries of approved schemas [4]. Mitre also identified critical functionality necessary in the security guard and some functionality that mandates a visibility beyond the guard to the connecting systems (e.g. workstation, server and user identification). Although some of these characteristics would be a large improvement over current guards, the suggested changes fail to address the information requirements of the modern tactical warfighter by constraining the timeliness, reach, and richness of information exchange. A *point* solution such as a security guard cannot effectively satisfy the information sharing demands of the tactical warfighter and a holistic system solution is required.

Beyond that, legacy security guards do little to mitigate the risks posed by insiders. A level of trust is placed in the individual charged with assigning a sensitivity label to information and in those who handle or consume the information. With the asymmetric threat posed by an insider, it becomes even more important to ensure individual trust is not abused[2], and if it is abused, to detect this transgression quickly, prevent further damage and provide an adequate forensic trail to hold the attacker accountable. Previous CDS approaches imposed preventive measures on the unauthorized disclosure of information instead of focusing on the trust placed in the individual. Information that was incorrectly marked and/or carefully prepared to avoid rules was unlikely to be detected by a CDS. Although individuals will always be subject to compromising trust relationships, these transgressions would be more detectable in a system solution.

Security Solution for Tactical Cross-Domain Information Sharing

The tactical environment demands a security solution that provides measures to keep the information protected, and that allows for timely, widely distributed and rich information exchanges. Solutions today must reduce the risks associated with information compromise such that they are significantly outweighed by the benefits of the system, thereby providing commanders with the means to exercise their duty to share information.

A number of significant factors have recently changed, creating the opportunity for new approaches to cross-domain information sharing.

Certification Advances

The suggested architecture has to be certified by appropriate authorities and accredited by commanders for operation in specific environments. Unfortunately, certification and accreditation (C&A) have become significant challenges for systems, leading to solutions such as the security guards discussed earlier. *Instead of being viewed as helpful, C&A is considered a hindrance. It is neither timely nor cost-efficient in an era when technology advances are coming faster than ever* [5]. The Defense Information Assurance Certification and Accreditation Process (DIACAP), still in draft format[3], introduces changes that provide a framework for certifying system solutions … *to support the paradigm shift from* need to know *to* need to share [5]. The DIACAP is applicable to tactical information sharing and introduces a process that could be used to certify and accredit the high-level security solution proposed in this article.

Technology Advances

Several technologies are creating opportunities for better cross-domain security solutions.

1. The Trusted Computing Exemplar (TCX) project is creating a framework for rapid high assurance system development, addressing how high assurance software components can be built [6]. With the system solution envisaged in this article, several high assurance components will be required at various places in the system and the TCX project identifies a process prescribing how these types of components can be built. Moreover, there are a number of companies who have significantly matured their software development processes, achieving the Software Engineering Institute's Capability Maturity Model and Capability Maturity Model Integration Level 5. Beyond mature software development processes, the improvements in verification of software have also been significant and are becoming the focus of intense research [7]. Creating software that predictably and verifiably does what it purports to do and nothing more is becoming achievable within reasonable expense. All these elements are critical to building a system solution.

2. The Advanced Encryption Standard (AES) was approved in Federal Information Processing Standards Publication 197 dated 26 Nov. 2001 to encrypt unclassified U.S. government traffic. In June 2003, the National Security Agency (NSA) approved AES to protect classified U.S. traffic, an unprecedented action in the world of high-assurance encryption [8]. Because the algorithm is publicly available, coalition partners can independently implement the algorithm and with a common key, they can securely exchange information.
3. The Trusted Computing Group (TCG)[4], an alliance of manufacturers, is in the process of establishing a number of relevant security hardware and system standards, effectively creating a framework for secure system solutions. The TCG recognizes the critical link with hardware, and several manufacturers are beginning to market compliant equipment. Regarding the solution suggested in this article, TCG compliant equipment would create an affordable, stable hardware base for the high assurance software components.
4. Persistent information storage is becoming very inexpensive and readily available devices can store immense quantities of information. This is important to support archiving audit logs. Protecting the integrity of and controlling access to the audit logs can be securely accomplished using the measures identified in the Trusted Platform Module specifications. Draft *NIST Special Publication 800-86, Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response*, and draft *Special Publication 800-92, Guide to Security Log Management* provide considerable rigor to audit processes and log management.
5. The Group Security Association Key Management Protocol (GSAKMP) *provides a security framework for creating and managing cryptographic groups on a network* [9]. If information can be tagged for a particular community of interest, access to that information can be managed by cryptographic mechanisms. Warfighters only need to send the information to a community of interest, and the framework provided by GSAKMP will ensure secure access is managed for participants. Separating the complexity of correctly tagging information from distribution decisions will allow for a more efficient information sharing environment.
6. There have been a number of significant advances recently toward certified components leading toward a certified Multiple Independent Levels of Security (MILS) architecture [10]. A MILS architecture leads toward a degree of confidence in the separation of information within the system, avoiding so much technical complexity that the system cannot practically be built. This creates well-enforced system sandboxes where software can be forced to execute only within approved parameters. The High Assurance Platform (HAP) is a computer that provides MILS capabilities using industry standard commercial hardware, software and applications, and should be available to a narrow community in 2007. It is intended to provide NSA certified separation to multiple operating systems running simultaneously in different security domains[5].
7. The Department of Defense (DoD) Discovery Metadata Specification was created to allow for efficient information discovery in US government networks [11]. It includes a number of tags that are relevant to security, including classification, declassification date, dissemination controls, and others. Moreover, search engines have become increasingly more efficient with hybrid designs of crawler/spider based components and human powered directories. Despite the growing quantity of information available, finding relevant information is becoming easier due to the use of metadata labels and strong search engines.

A systemic information assurance approach must provide layered security measures that reduce the need for information content filtering measures. The solution relies on increasing the strength and reliability of accountability, detective and reactive measures, and consequently increases flexibility in information sharing. The following high-level solution builds on the advantages presented by recent maturations in select technologies.

Encryption to support confidentiality and integrity of information flows should be established from source to destination, so devices at the boundary will not be able to examine the contents of packets. This means that some of the traditional functionality of the CDS must be pushed to the information sources, in most cases data terminals. It is important to note that the destination need not necessarily be another data terminal but could be traffic destined for a community of interest.

The following functionality must exist at information source points, often personal computers:

- Trusted identification and access control measures must be resident in the source data terminals. These measures link user triggered actions to individuals and confirm privileges before allowing actions. Systems and protocols provide the means to manage identities across disparate networks with a high degree of confidence and minimum inconvenience to the user community. Regarding authorization, the use of X.509 based attribute certificates and a Privilege Management Infrastructure offers considerable flexibility to handle role based authority [12] and progress has been made extending Public Key Infrastructures into tactical environments.
- Trusted audit measures must be resident on the data terminals to capture all security relevant events. With the establishment of the TCG standards and resulting hardware, the audit logs can be securely protected and with the availability of inexpensive storage, the logs can hold a tremendous amount of information before needing to be rolled over.
- Trusted domain separation must exist on the data terminals. There is considerable research into making trusted operating systems more accessible and commercial operating systems more secure, providing sufficient flexibility to strike the right risk exposure and functionality. Moreover, with the establishment of TCG standards and hardware, the increased confidence in the operating systems and software will be strongly based on trusted hardware. This should make domain separation on desktops achievable and affordable in the near term.
- Trusted encryption measures with an appropriate algorithm must provide adequate confidentiality and integrity protection for information flows between data terminals. Trusted Network Connect from the TCG offers an assured encryption solution and the digital signature, random number generation and protected storage of the Trusted Platform Module, again from the TCG, offers the other necessary primitives for a secure solution.
- Malicious content filtering that detects and prevents the execution of

malware must exist on all data terminals. With host firewalls and advances in malware protection products, networked computers can connect to the Internet with a degree of confidence. In a tactical environment, the risk of attack is far reduced and the potential for successful malware introduction is also reduced.

- There must be trusted, locally controlled interfaces that allow for movement of select data from one domain on a data terminal to another domain on the same terminal. The term *controlled interface* is not carefully defined in this article, but in general, it mediates information exchanges, looking for defined transgressions when moving data between domains. Effectively a controlled interface gives authorized users some flexibility to move data electronically between domains.

Within the connecting network, there must be a number of complimentary services:

- An identity and permission management service must provide complimentary functionality to the capabilities needed at the information sources.
- Network and distributed intrusion detection and reaction services must exist. Other than receiving alerts from network intrusion detection sensors, this service would also receive alerts from host based intrusion detection sensors, collect log data for detailed analysis and react to events based on policy.
- A policy management service provides the needed flexibility for a tactical network. This service would establish policies that relate to the network configuration and security posture. These policies would be dynamic based on changes in information flow requirements, changing threats and various other influences.
- A service that provides security association and key management is needed to support GSAKMP.

A boundary protection system should contain the following functionalities at the network boundaries.

- Identity and access control to ensure the users passing information or drawing information across the domain boundary are authorized to do so.
- Flow control measures that can accommodate the need for supporting quality of service information exchanges such as near real-time graphical collaboration sessions, and control network ingress from unwanted sources and/or unwanted traffic.
- Audit measures that work with intrusion detection and prevention systems to detect malicious activity and/or exposures in a timely fashion and provide non-repudiation of information flows.
- The configuration of boundary protection services must be dynamically configurable by policy, allowing information flow based on tactical conditions.

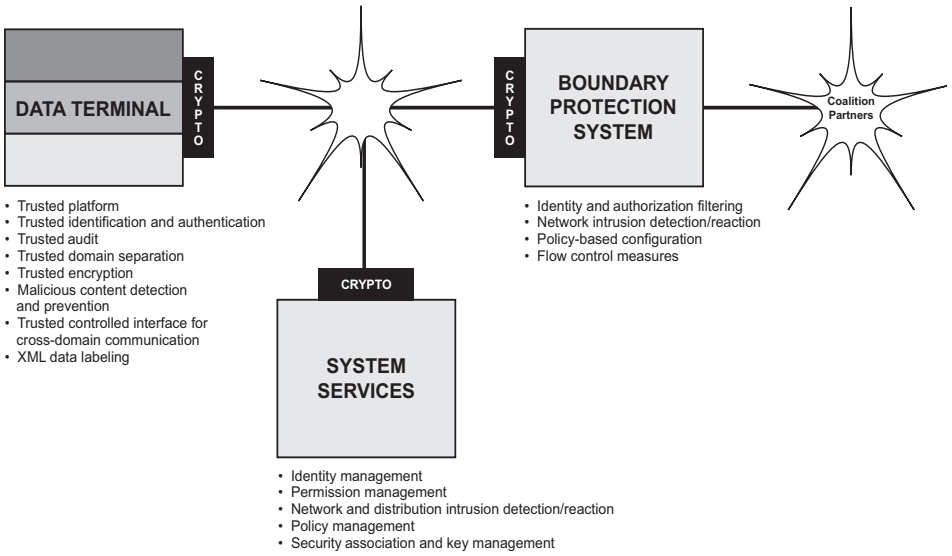


Figure 2: *Suggested High-Level Solution*

This high-level architecture (Figure 2) has a number of implementation challenges that require deeper analysis, but these have not been identified or explored in this article for brevity purposes.

Conclusion

To support the unity of effort necessary in today's combat environment, warfighters have a duty to share information widely and quickly in rich exchanges, some of which must cross security domains. This article suggests a holistic high-level solution to securing cross-domain exchanges that will not excessively constrain the exchanges, taking advantage of advances in technology and policy. The solution effectively takes some of the trust and functionality originally resident in traditional CDS and moves it into information sources, system services, and boundary protection devices.

Although the solution suggested here has been applied to the tactical environment, elements of the system solution may lend itself to other environments with similar problem spaces. Instead of tactical domains, one could consider the domains relevant in medical information systems. Patients must securely share private information with family general practitioners, and occasionally general practitioners must share elements of this information with specialists. The exchange between patient, general practitioner, and specialist creates a small community of interest. At the same time, some of this information may be useful to those needing statistics, but the posting agency may not really be aware of the information needs of the authorized consumers and may not be best able to manage the makeup of the authorized consumers. Managing access might be better placed with others whose primary expertise is privacy, access control, and information presentation. Throughout these exchanges, actions must be logged to ensure violations can be handled quickly.

This article has not proposed any dramatic new technologies; it has simply suggested re-positioning some relatively well-understood security functionality to non-traditional places in the network in the hopes of satisfying the information sharing needs of the warfighter.◆

References

1. DoD. "Network Centric Warfare." DoD Report. 27 July 2001 <www.dod.mil/nii/NCW/>.
2. Bush, George W. Further Amendment to Executive Order 12958 <www.whitehouse.gov/news/releases/2003/03/20030325-11.html>.
3. Alberts, D.S., and R.E. Hayes. "Power to the Edge: Command and Control in the Information Age." CCRP (June 2003): 14-15.
4. Reed, Nancy. "Security Guards for the Future Web." Technical Report 04W0000092. Mitre Corporation,

2004 <www.mitre.org/work/tech_papers/tech_papers_05/05_0166/05_0166.pdf>.
5. Wierum, Jenifer M. "Defense Information Assurance Certification and Accreditation Process and the Global Information Grid Information Assurance Architecture." 10th International Command and Control Research and Technology Symposium The Future of C2, Mar. 2005.
6. Irvine, Cynthia E., Timothy E. Levin, Thuy D. Nguyen, and George W. Dinolt. "The Trusted Computing Exemplar Project." Proc. of the 5th IEEE Systems, Man and Cybernetics Information Assurance Workshop, United States Military Academy, West Point, NY, 10-11 June 2004.
7. Jones, Cliff, Peter O'Hearn, and Jim Woodcock. "Verified Software: A Grand Challenge." IEEE Computer 39.4 (2006).
8. Committee on National Security Systems. "National Policy on the Use of the Advanced Encryption Standard to Protect National Security Systems and National Security Information." U.S. CNSS Policy No. 15 Sheet No 1. June 2003.
9. Internet Engineering Task Force. "Group Secure Association Group Management Protocol." Internet Draft. 2005 <www3.ietf.org/proceedings/06mar/IDs/draft-ietf-msec-gsakmp-sec-10.txt>.
10. Alves-Foss, Jim, Carol Taylor, and Paul Oman. "A Multi-layered Approach to Security in High Assurance Systems." Proc. of the 37th Hawaii International Conference on System Sciences, 2004.
11. Magar, A. "Investigation of Technologies and Techniques for Labeling Information Objects to Support Access Management." Defense Research and Development Canada, Report DRDC Ottawa CR 2005-166. 2005
12. Chadwick, David. "The X.509 Privilege Management Infrastructure." Proc. of the North Atlantic Treaty Organization Advanced Networking Workshop on Advanced Security Technologies in Networking, Bled, Slovenia, June 2003. University of Salford, 2003 <http://sec.isi.salford.ac.uk/Papers.htm>

Notes

1. A security domain is defined by the Internet Security Glossary as *an environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources* <www.ietf.org/rfc/rfc2828.txt>.
2. The John Anthony Walker Jr. story of insider espionage activities over eighteen years can be found at <www.crimelibrary.com/terrorists_spies/spies/walker/1.html>.
3. A draft version of the DIACAP is available at <http://iase.disa.mil/ditscap/ditscap-to-diacap.html#diacap>.
4. More information on the TCG and its standards can be found at <www.trustedcomputinggroup.org>.
5. The HAP is described at <www.gdc4s.com/contacts/user_conf/topics.cfm>.

About the Author

Mel Crocker is the information assurance technical lead for the Land Command Support System program within General Dynamics Canada. He has a master's degree in software engineering from Royal Military College, and a Bachelor of Science in math and physics.

General Dynamics Canada
1020-68th AVE N.E.
Calgary, AB T2E 8P2
Phone: (403) 295-5075
E-mail: melvin.crocker@gdcanada.com