Global Information Assurance Certification Paper

Security Issues When Data Traverses Information Domains: Do Guards Effectively Address the Problem?

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b – Option 1
Charles Maney
May 18, 2004

1. Abstract

The sharing of information has become an integral part of our society. Because of this, it has become increasingly important to protect that information as well as the resources that facilitate the information exchange. This is particularly important when considering the sharing of information within government and military agencies. Different agencies share different types of information that are restricted from access by certain users. When this data must travel between networks of different security classifications, there arises the need for a guarding solution. A guard, simply stated, is a component or multiple components placed between networks to protect them and the information that passes between them. Government and military agencies use guarding solutions to further secure their networks and the information they contain. For the purposes of this document, the term *government* refers to the U.S. Federal Government.

This paper is intended to present an overview of guards and the security considerations they intend to address. A description of information domains will be followed by an explanation of the need for security when they must be interconnected. The paper will then describe some of the security issues that are inherent in sharing data across those information domains. Finally, it will discuss the methods by which guards attempt to address those security issues and briefly describe some existing solutions to determine if guards are a solution to the problem.

2. Introduction

In order to understand guarding technology, the subject of information domains needs to be discussed. This section will present an overview of information domains as they relate to government and military networks. Guards will then be introduced and defined with an explanation of why they are needed in the government sector.

2.1. What are Information Domains?

Information domains can be described as entities that encompass data of a certain classification, the authorized users of that classification environment and the governing security policy imposed on that classification environment. This paper will focus on an information domain representing a network of a particular data classification. The Department of Defense (DoD) separates data into classification levels, depending on the sensitivity of the data. The more sensitive the data, the higher the classification level it will carry. The Department of Defense defines the following five classifications:

- TOP SECRET – this is the highest security level, and is defined as information which would cause "exceptionally grave damage" to national security if disclosed to the public. This classification is most often subdivided on the basis of "need to know", and includes such information as the design of cutting-edge weaponry, etc.
- SECRET– the second highest classification may include, for example, details of other security measures and procedures. It is defined as information that would cause "serious damage" to national security if disclosed.
- CONFIDENTIAL – is the lowest classification level. It is defined as information that would "damage" national security if disclosed.
- SENSITIVE BUT UNCLASSIFIED (SBU) – data which is not related to national security but whose disclosure to the public could cause some harm; such data includes personal demographic information from recent censuses, for example. This category is often referred to as Unclassified/FOUO or for official use only. Personal data, and information which requires confidentiality such as contract negotiations, will often fall in this category as well.
- UNCLASSIFIED – not technically a "classification", this is the default, and refers to information that is not sensitive and can be freely disclosed to the public. Information that was previously classified under one of the above levels is often declared "unclassified" at a certain time because its age has made its classification no longer necessary.[1]

The preceding list of levels is not exhaustive; other classifications exist, however, they are subclassifications. For each classification, there is a network operating at that level that must be secured. Each of these networks or information domains will often share data with other information domains. This sharing of data between networks needs to be secured as well.

2.2. Why the Need for Security Between Information Domains?

The compromise of sensitive information can have serious ramifications that can threaten national security or even cause loss of life. Therefore, sensitive information needs to be protected, especially when it is being shared between

[1] "Classified information." Wikipedia. 23 Feb. 2004 <http://en.wikipedia.org/wiki/Classified_information>.

different information domains. When protecting data, three aspects of the data need to be addressed: confidentiality of the data, integrity of the data, and availability of the data. Confidentiality refers to ensuring that the data is not disclosed to unauthorized individuals, processes or devices. Integrity refers to the protection against the unauthorized modification or destruction of information. Availability pertains to the timely and reliable access to data and systems.[2]

The confidentiality, integrity and availability of information that resides on a network is always at risk of being compromised. That risk increases when data traverses different networks. Let's say, for example, that there are two networks of different classifications that want to share data, a TOP-SECRET network and an UNCLASSIFIED network. The TOP-SECRET network will be referred to as the 'high side', since it is the higher classification of the two networks. The UNCLASSIFIED network will subsequently be referred to as the 'low side'. Each of these is a separate information domain. Without protection between these two domains, an unauthorized user on the low side could potentially retrieve sensitive information from the high side. Another scenario would be that the high side could potentially be exposed to malicious code, such as a virus, sent from the low side that could damage critical information or system processes. In the simplest terms, you want to keep 'bad things' from getting to the high side and keep 'sensitive things' from getting to the low side. The use of a guard to facilitate the data exchange is one way to address these security concerns.

3. What is a Guard?

A guard is a combination of hardware and software that is used to provide secure data transfer between two information domains. There are many different types of guards with different functionalities, but the basic functionality of every guard is the same: protect the networks at the boundary and secure the data transfer between those networks. Because guards control data flow at the network boundary, they are sometimes confused with firewalls. Before describing different types of guards and their functionalities, it is important to make the distinction between guards and firewalls.

3.1. Guards Are Not Firewalls

While guards can perform the same functions as firewalls, guards generally provide much more functionality than firewalls in order to address the problems of data exchange between information domains. Kenneth A. Minihan, Lieutenant General, USAF writes:

---

[2] Hayden, Michael V. Committee on National Security Systems (CNSS). CNSS Instruction No. 4009. May 2003. 23 Feb. 2004 <http://www.nstissc.gov/Assets/pdf/4009.pdf>.

> "Guards are distinguished from firewalls in three major ways:
> (i) Guards have an application filtering capability that is much stronger than a typical application filtering firewall. Guards use a reclassifier application to control what data is passed from one enclave to another. The reclassifier application uses a collection of filters to review application content.
> (ii) Guard software is generally developed to meet higher assurance requirements.
> (iii) Guards undergo a much more extensive test and evaluation (e.g. source code analysis, unconstrained penetration testing, and design documentation review) to provide a signifcantly higher level of confidence that they will work correctly."[3]

Here, Lt. General Minihan uses the term *enclave* to refer to an information domain. Generally, firewalls filter packets at the network level, although some have application filtering capabilities. Guards, however, filter data packets at several levels and can therefore offer other services such as content checking, filtering based on data labeling and virus protection. Also, depending on the requirements of the system and the environment in which it will be deployed, the guard will be required to be evaluated and possibly accredited by the appropriate government agency in order to be considered for use. The evaluations will be briefly described later.

3.2. Multiple Single Levels of Security (MSL) or Multi-level Security (MLS)?

Confusion often arises when trying to understand and differentiate MSL and MLS. The terms seem to have similar meaning, but they are very different with respect to guard design and architecture. MSL is an architecture that incorporates a defense-in-depth approach to security between information domains. This design consists of a guard that joins the information domains, but the domains are completely separated except for their connection points to the guard. The guard prevents unauthorized access to the data on the interconnected networks and controls the data that passes through it to the other domain. This architecture can incorporate several components that perform additional security functions to ensure a defense-in-depth strategy. A key feature of this design is that the classification levels reside on separate networks.

MLS describes an architecture that allows data of different classification to reside on the same system or network. While this architecture also incorporates a defense-in-depth security strategy, it manages the different data classification with the use of data labels. Labelling describes the process of applying a label to

---

[3] Minihan, Kenneth A. National Security Telecommunications and Information Systems Security Committee (NSTISSC). NSTISS Advisory And Information Memorandum On The Role Of Firewalls And Guards In Enclave Boundary Protection. Dec. 1998. Mar. 2004 <http://www.nstissc.gov/Assets/pdf/NSTISSAM COMPUSEC1-98.pdf>.

each data object that defines its classification.[4] The guard and its systems have the capability to control labelled data and access to it through the use of mandatory access controls (MAC) and role-based access controls (RBAC). This design incorporates a trusted operating system such as Trusted Solaris to facilitate the data labelling and MAC and RBAC processes. To illustrate this design, a user with TOP SECRET clearance and a user with SECRET clearance both have access to the same network with the same computer. The TOP SECRET user can access TOP SECRET information and any classification below it. The SECRET user can only access SECRET information and any classification below it. The SECRET user is restricted from access to TOP SECRET information even though it is on the same computer on the same network. The key aspect of MLS architecture is that data from of different classifications exists in the same processing environment.

Because these terms are often confused, guards are sometimes categorized incorrectly. Most guards fall into the MSL category and full MLS operablility has yet to be achieved in many functional areas. MLS guards exist, however, much work remains to meet the requirements of users in the Department of Defense and other government agencies.

3.3. Low to High Guards

A low to high guard is one in which the information is transferred in one direction from the information domain of lower classification to the domain of higher classification. The direction of the data transfer is referred to as the data flow. When the data flow is restricted to one direction, guards are sometimes referred to as one-way filters.

Although the functionality of a low to high guard will differ depending on the requirements of the intended users or agency, in general, this implementation restricts the flow of data from the high side to the low side and uses the Bell Lapadula model to ensure confidentiality of high side information. This is achieved with access controls that enforce a 'write up, read down' policy. This means that users cannot read from a higher data classification level than their own and they cannot write to a lower data classification level than their own. This ensures that sensitive information from the high side will not be disclosed to the low side.[5]

There may be other security precautions that need to be addressed in this implementation, such as the blocking of malicious code, prevention of disruption of service on the high side or damage to the high side system. The low to high

---

[4] Fahs, Rainer , and Simon R. Wiseman. Defence Research Agency. Re-Floating the Titanic: Multi Level Security in Contemporary Environments. Mar. 2004 <http://www.eicar.org/download/titanic.doc>.

[5] Cole, Eric, et al. SANS Security Essentials with CISSP CBK Version 2.1. 2nd ed. Vol. 1. N.p.: SANS Press, 2003. 390-391.

implementation lacks the ability to ensure the integrity of the data being transferred, so this type of guard is usually deployed in environments that do not require integrity checks for file corruption or manipulation. An example of this type of data would be weather data needed by ships at sea or pilots. This data is updated and passed through often and repeatedly, so it may not need to be checked for integrity.

3.4. High to Low Guards

High to low guards, or one-way filters, ensure the transfer of data in one direction only, from the high side to the low side. This policy is 'write down' but still must protect the confidentiality of the high side information. Basicly, the guard ensures that only information that is of the low side classification or lower can pass through from the high side. This implementation is a bit more complicated in that the data being sent must be checked for its classification, whereas with a low to high guard, it is already coming from a lower classification. These checks sometimes involve verifying the sensitivity label of a file, searching for specific content in a file (sometimes referred to as 'dirty-word searching') or checking for allowable file types as determined by site-specific policy.

Some of the security checks performed in a high to low architecture require the review of a human to ensure that unauthorized disclosure of sensitive information does not occur. Other functions of the human reviewer are sanitization and downgrading.[6] These involve 'cleaning' the data so that it can be downgraded to a lower classification level. Most guards lack the technology to handle these functions without the human review component and are considered semi-automated guards.

3.5. Bi-directional Guards

Bi-directional guards allow the transfer of data in both directions between the low side domain and the high side domain. This type of guard is much more complex than a one-way implementation because it must enforce the restrictions of both low to high and high to low implementations within the same architecture. The components that can make up a bi-directional guard include: virus scanners, filetype checkers, trusted operating systems, intrusion detection devices, audit loggers as well as human reviewers. While there is a need for an efficient, fully automated guard that satisfies all the security requirements of the government community, the industry has not yet successfully developed an 'all around' solution.

[6] Multilevel Security in the Department Of Defense: The Basics. Department of Defense Multilevel Security Program. <http://nsi.org/Library/Compsec/sec3.html>.

3.6. Evaluation and Regulation

Several government agencies evaluate guards and their components to provide a level of confidence in the security claims of the products. The required assurance of the guards is very high and the evaluations are specified to thoroughly test those high standards. The Department of Defense in particular, regulates the procurement, operation and maintenance of all information technology systems that will be used within the Defense Information Infrastructure (DII).

The Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) defines the procedure for formally evaluating a guard that will potentially be deployed in the DII. A Designated Approving Authority (DAA) oversees the process, which often includes other government agencies that carry out specified procedures. The National Security Agency (NSA) is one example that performs the Verification Phase, consisting of testing the system against a set of predefined security requirements.[7]

The particular evaluation or accreditation that a guard will require depends on the environment in which it will be deployed. Other regulation policy and evaluation criteria include Secret and Below Interoperability (SABI), Director of Central Intelligence Directive (DCID) 6/3 and the Common Criteria (CC).

4. Security Issues

There are several security issues to consider when sharing data between information domains. These issues can be described by the threat that is imposed on the confidentiality, integrity and availability of sensitive data and the information systems on which it is contained. Some of the most important threats are discussed in this section.

4.1. Sniffing

Sniffing is the process of using a software tool to capture network traffic. By placing a sniffer on a connected network, an attacker can obtain valuable information such as IP addresses, usernames and passwords. Obviously the attacker could then use the information to masquerade as a user on the classified network. In addition, many sniffers are easy to use with very little technical knowledge.

---

[7] United States. Department of Defense. Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). Dec. 1997. <http://iase.disa.mil/ditscap/DitscapFrame.html>.

This attack compromises the confidentiality of the data. A guard can mitigate this threat by avoiding the broadcasting of network information and most effectively by encrypting the data that is sent over the network.[8]

4.2. Spoofing

Spoofing is the act of impersonating an authorized user by using an IP address, that normally resides on the internal network, from outside of the network. Once this takes place, information that is intended for the authorized user (based on the IP address) will be received by the attacker.

Confidentiality of sensitive data has been compromised here. Guards must employ a properly configured firewall to reduce the risk of this threat. Another mitigation strategy would be to use a key exchange system for authentication. Without the required key, spoofing an IP address gets the attacker nowhere.

4.3. Unauthorized Disclosure

Unauthorized disclosure can be described as an unauthorized user obtaining sensitive information from the high side domain. This can result from poor administration, inaccurate 'dirty-word search' or is the result of another attack.

This can be either an active or passive attack that compromises data confidentiality. Data labelling, mandatory access control, reliable dirty-word and content filtering, automated downgrading and proper security configuration are ways that a guard can be effective in mitigating this type of threat. Although it is reactionary, good auditing can help detect if an unauthorized disclosure of information has occurred.

One company that attempts to address this security concern is DigitalNet. DigitalNet's XTS-400 Trusted Computer System incorporates support for automated downgrading and is designed to be used in guarding solutions. XTS-400 has also been evaluated by NSA.[9]

4.4. Malicious Code

Malicious code is software that can be executed on a target system in an unauthorized fashion for the purposes of causing damage, obtaining information

---

[8] Cole, Eric, et al. SANS Security Essentials with CISSP CBK Version 2.1. 2nd ed. Vol. 1. N.p.: SANS Press, 2003. 173-174.

[9] DigitalNet XTS-400 Trusted Computer System Technical Overview. DigitalNet Government Solutions, LLC. May 2004 <http://www.getronicsgov.com/solutions/info_sec_sol/pdf/XTS-400TechnicalOverview.pdf>.

or modifying data. Examples are viruses, worms, trojan horses, macro viruses, etc. It can be embedded in e-mail, files or html and can vary greatly in its purpose. This threat has the potential to compromise confidentiality, integrity and availability.

The proper mitigation of this threat it to include a virus scanner that can detect all types of malicious code. The guard must have the capability to easily update the virus definitions used by the scanner in order for it to be effective.

Trusted Computer Solutions counters this issue in its design of the Trusted Gateway System (TGS) (now known as SecureOffice Trusted Gateway). TGS is a one-way low to high guard that runs on the Trusted Solaris operating system and includes a virus scanner among many other security features. It can detect embedded viruses as well. The TGS has gone through the DITSCAP and been evaluated by NSA.[10]

4.5. Denial of Service (DoS)

Shon Harris writes, "A denial of service (DoS) attack is when a system is bombarded with so many requests that it can no longer accept other requests or fulfill them."[11] Examples are distributed denial of service, the smurf attack and the fraggle attack. These all have subtle differences, but share the same goal: overload the system in order to render the system inoperable.

This attack threatens data and system availability. All guards should be designed with the capabilities of avoiding a DoS attack or recognizing a DoS attack and reacting appropriately. Examples would be to not allow the system to be pinged by other systems and proper file handling and maintenance.

5. Conclusion

The government's need to share information between different information domains presents the necessity to understand the security implications associated with such a data transfer. Guards are the culmination of that understanding. User requirements of the government community are steadily increasing which steadily increases the complexity of guarding technology. While many solutions exist that address several of the security issues, there will continue to be a number of obstacles to overcome in developing the ideal guard.

---

[10] SecureOffice Trusted Gateway. Trusted Computer Solutions. May 2004 <http://www.tcs-sec.com/products/1products1_3_2.html>.

[11] Harris, Shon. Mike Meyers' CISSP Certification Passport. Berkeley, CA: McGraw Hill/Osborne, 2002. 366-367.

Success will lie in the balance of maximizing threat mitigation and meeting user needs.

6. References

"Classified information." Wikipedia. 23 Feb. 2004 <http://en.wikipedia.org/wiki/Classified_information>.

Cole, Eric, et al. SANS Security Essentials with CISSP CBK Version 2.1. 2nd ed. Vol. 1. N.p.: SANS Press, 2003. 173-174.

Cole, Eric, et al. SANS Security Essentials with CISSP CBK Version 2.1. 2nd ed. Vol. 1. N.p.: SANS Press, 2003. 390-391.

DigitalNet XTS-400 Trusted Computer System Technical Overview. DigitalNet Government Solutions, LLC. May 2004 <http://www.getronicsgov.com/solutions/info_sec_sol/pdf/XTS-400TechnicalOverview.pdf>.

Fahs, Rainer , and Simon R. Wiseman. Defence Research Agency. Re-Floating the Titanic: Multi Level Security in Contemporary Environments. Mar. 2004 <http://www.eicar.org/download/titanic.doc>.

Harris, Shon. Mike Meyers' CISSP Certification Passport. Berkeley, CA: McGraw Hill/Osborne, 2002. 366-367.

Hayden, Michael V. Committee on National Security Systems (CNSS). CNSS Instruction No. 4009. May 2003. 23 Feb. 2004 <http://www.nstissc.gov/Assets/pdf/4009.pdf>.

Minihan, Kenneth A. National Security Telecommunications and Information Systems Security Committee (NSTISSC). NSTISS Advisory And Information Memorandum On The Role Of Firewalls And Guards In Enclave Boundary Protection. Dec. 1998. Mar. 2004 <http://www.nstissc.gov/Assets/pdf/NSTISSAM COMPUSEC1-98.pdf>.

Multilevel Security in the Department Of Defense: The Basics. Department of Defense Multilevel Security Program. <http://nsi.org/Library/Compsec/sec3.html>.

SecureOffice Trusted Gateway. Trusted Computer Solutions. May 2004 <http://www.tcs-sec.com/products/1products1_3_2.html>.

United States. Department of Defense. Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). Dec. 1997. <http://iase.disa.mil/ditscap/DitscapFrame.html>.

Last Updated: July 26th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS