

Wireless Systems Security

EE/NiS/TM-584-A/WS

Bruce McNair
bmcnair@stevens.edu

EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-1/35

Week 3: Security Topics

EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-2/35

This week, we will begin the discussion of security topics. The focus will be general, but I'll include relevance to wireless systems along the way.

What is “Security”

- Quality has been defined to be “Meeting (or exceeding) customer’s expectations”
 - Assumes no sentient forces to deny the desired outcome
 - natural failures and accidental shortcomings/oversights only

Before we discuss security, we have to define what we mean by the term. The problem is that this area means many different things to different people.

To start, let me introduce a term that has been discussed in great depth that has some interesting relationship to security. This is the term “quality.”

There have been major efforts in several industries to improve the quality of their products and processes, so when I had the job of defining security in one of my jobs, I thought I would see what I could learn from the quality efforts.

The typical definition used for quality deals with satisfying the customer – they get to define whether a product or service meets their idea of quality.

One important aspect of quality is that it assumes that the customer satisfaction has only the careful attention of the supplier to depend on. The supplier has to anticipate what might go wrong in building the product or how the product might break in normal usage, but there are no evil forces trying to undo their efforts.

What is “Security”

- Quality has been defined to be “Meeting (or exceeding) customer’s expectations”
 - Assumes no sentient forces to deny the desired outcome
 - natural failures and accidental shortcomings/oversights only
- An operative definition of security for this course:
 - “Meeting (or exceeding) customer’s expectations in the presence of the actions of an adversary.”
 - Parenthetical extension is especially important here – it addresses cases where customer has not thought through implications of system and its potential impact on their operations.
 - Open ended definition implies ongoing need to address evolving threats

If we try to apply the quality definition to security, one important difference is that with security, we anticipate that there will be bad guys trying to destroy what we put together. If we can continue to meet the user’s needs, even when the enemy is trying to break the system in some manner, we have built a secure system. Later, we will examine what the dimensions of security may be, since this definition does not address that.

There are two important points to this definition that bear examination:

- (1) The customer doesn’t always clearly state what their needs are. They may not have even thought of them. For this reason, the requirement that the design exceed customer’s expectation is stated.
- (2) Before the Internet existed, there were criminals, so it is no surprise that criminals use the Internet to attempt to defraud users. However, as the Internet was being defined, no one anticipated that misspellings, spoofed addresses, redirected web addresses, forged email addresses, viruses in executable attachments, etc. would become as widespread as they have become. For this reason, the definition needs to be open ended, changing to meet new threats as the environment changes. In the same manner, the definition of quality is open ended – as the market evolves and competitors find new and better ways to build their product, the customer’s expectations may increase. The bar is thus raised as to what constitutes a quality product and what is considered shoddy merchandise.

What is “Security”

- Quality has been defined to be “Meeting (or exceeding) customer’s expectations”
 - Assumes no sentient forces to deny the desired outcome
 - natural failures and accidental shortcomings/oversights only
- An operative definition of security for this course:
 - “Meeting (or exceeding) customer’s expectations in the presence of the actions of an adversary.”
 - Parenthetical extension is especially important here – it addresses cases where customer has not thought through implications of system and its potential impact on their operations.
 - Open ended definition implies ongoing need to address evolving threats
- Other quality-derived concepts that are especially pertinent to security:
 - Root cause analysis of faults
 - Continuous process improvement
 - Pareto principle (80/20 rule)
 - “Quality is Free” (refer to Phil Crosby book of same title)

EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-5/35

Finally, in using this quality definition, there is some useful “spin-off” that can be applied to security.

One important lesson learned from looking carefully at quality processes is the idea of continuous process improvement. You can never find the last bug in complex software or remove the last product issue in an assembly process. What you can do, however, is to fix the serious problems, and continue to look for the next worst problem. In this manner, the system design will always be getting better, but it is recognized that it will never be completely perfect.

What you do need to do, however, is to avoid fixing the superficial symptoms and, instead, get at the underlying cause of the problem, the so-called root-cause.

A concept from economics, the Pareto principle, suggests that the majority of wealth is held by a minority of the population, the so-called 80/20 rule. In quality terms, this concept suggests that a few root causes are responsible for a majority of system problems. The good news is that you don’t have to fix everything to make a big improvement, just the few issues that cause all the difficulties.

These quality lessons also teach us about security. When a security issue is found, the underlying cause must be fixed, not simply patched, or it will reoccur. We will often find that there are a few basic issues that reoccur in system after system. Once you begin to recognize the commonality, you can make major advances in fixing new systems.

Finally, the reference to Phil Crosby’s book is especially relevant – making a system secure should not be looked at as an expensive annoyance. Security (or quality) issues discovered early in the design cycle will add cost, but these costs will be more than offset by expenses avoided later in the system lifecycle.

How Much Security Is Enough?

A security assessment model

Perpetrators

Who might try to steal the assets?

- What resources do they have?
- Where and how might they be able to attack?
- What might they be after?
- What are their motivations?

Assets at Risk

What might be worth stealing?

- Assets may be resources, capabilities, etc. that the system has, controls, or influences
- Tangible assets
 - Intangible assets

EE584
2/16/2011

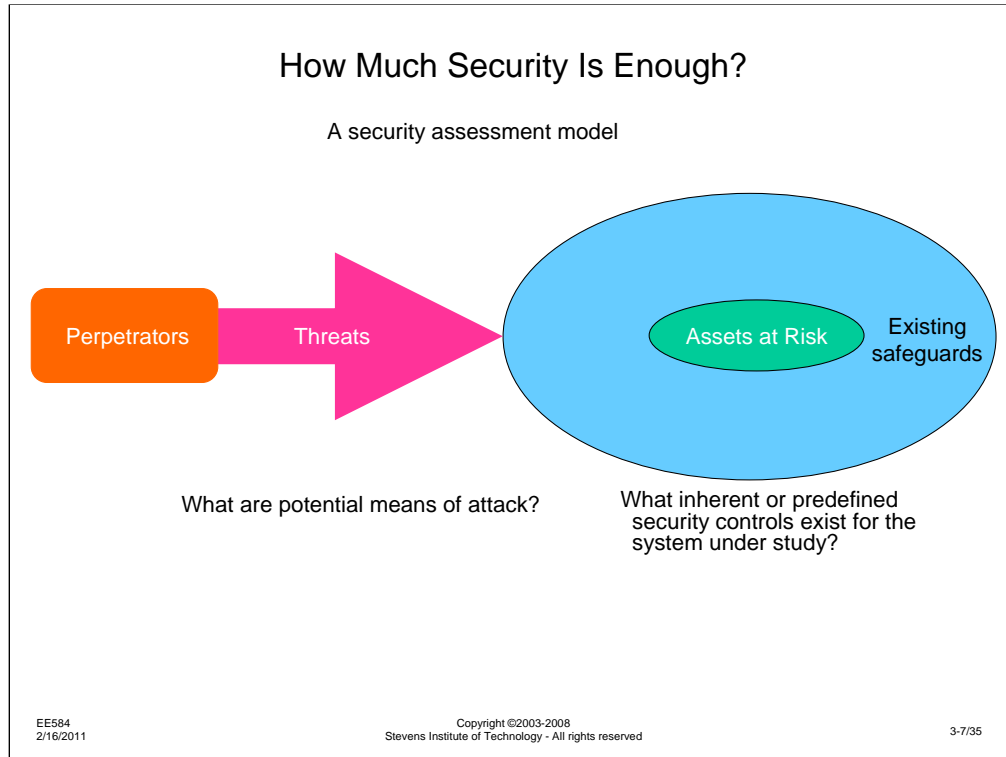
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-6/35

So how can we decide if a system has serious security issues or if we have just identified a possible problem that is really just theoretical. For this, I will present a security assessment model that we will be using extensively for the later half of this course.

To begin to examine security in a system, we must first think about who might be attacking the system. This gives us a picture of their capabilities, their motivation, and what they might try to attack. There is no sense protecting something that no one is ever going to steal.

Next, we must examine what there is in the system under study that someone might want to steal. It is important to recognize that what the designer or user of the system value may not always be what the attacker values. As an example, consider the story told by Cliff Stoll in "The Cuckoo's Egg," an examination of attacks on computer systems at UC Berkeley. The attacker stole miniscule amounts of computing resources on the system that Cliff Stoll was administering. What the systems provided the attacker, however, was connectivity and a means to hide their origin. Connectivity existed to sensitive computing systems at MITRE and the military that the attacker could exploit. By transiting through Stoll's systems, the attacker masked their true identity and location. The lesson is that when examining a system's assets, one must take the broadest view of what might be valuable. In the words of Hank Kluepfel, a computer security investigator from AT&T Corporate Security, the defender has to learn how to "think like a thief."



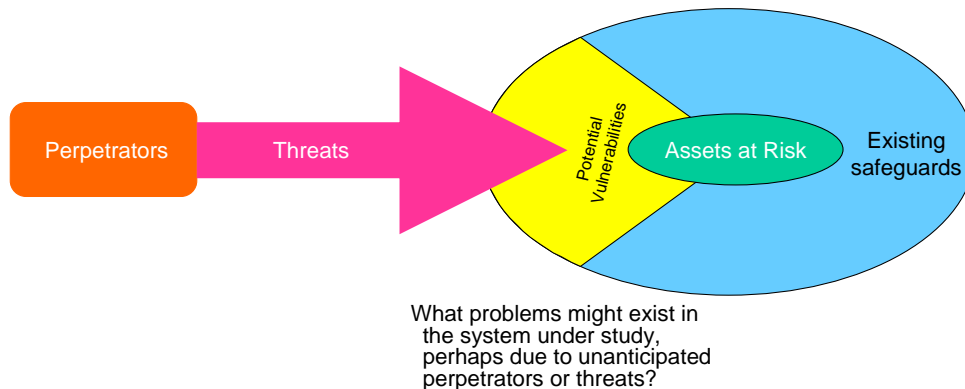
Having identified the people who might attack the system and the assets they may be attacking, we can start to examine the threats – HOW they might attack the system. Again, it is important to be open minded here: a common pitfall that system designers often fall into is: “I am smart. I don’t see any way to attack my system. Therefore it is secure.” Too often, the system designer looks for attacks against the front door, where he or she knows protection has been studied. The attacker finds the unlocked back door that no one ever considered.

As we examine the system under attack, it is valuable to consider the safeguards that have been built into the system. They will certainly protect against some attacks. Perhaps they are more than enough for 90% of the threats we can envision. This makes the job easier. We only have to focus on the 10% of the threats that might bypass the existing safeguards.

While I am presenting this assessment model in a very linear fashion: First look at A, then B, then C; in fact, the process MUST be quite nonlinear. As threat is identified, it is often necessary to go back and see if there was a perpetrator who had not been considered who might be capable of mounting the new threat. Perhaps, there is a system asset that got overlooked. Only when the safeguard that protects it is identified do we remember the asset that the safeguard is supposed to protect. Thus, there are often repeated iterations through the assessment process.

How Much Security Is Enough?

A security assessment model



EE584
2/16/2011

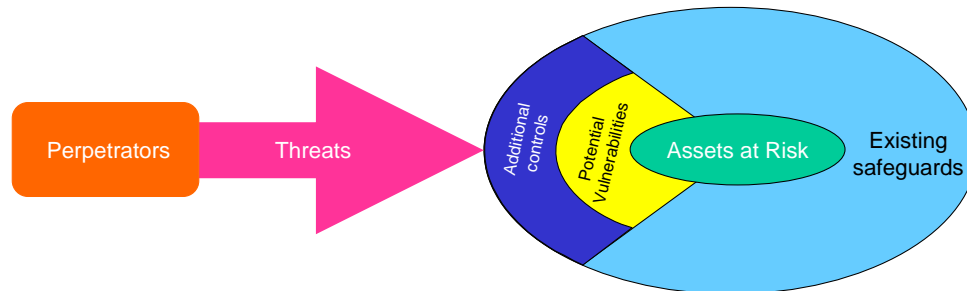
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-8/35

The next step in the assessment model is to identify potential vulnerabilities. These are holes in the armor of the existing safeguards. They are POTENTIAL vulnerabilities because there may not be a real threat that a perpetrator could use to exploit the vulnerability. If we think of existing safeguards as the pickets of a fence around a house with vulnerabilities being the spaces between the pickets, and the assets as targets on the house, the combination of threat/vulnerability/asset is only an issue if the perpetrator could shoot arrows (threats) between the pickets and hit a target. If there is a misalignment between the combination, the threat exists, but cannot be exploited. On the other hand, perhaps the perpetrator will see that he cannot hit the target today and will move to a better vantage point tomorrow from which the target can be hit. This requires the security assessor to anticipate how the threat may evolve in the future.

How Much Security Is Enough?

A security assessment model



What problems could be averted by adding additional security controls to the system design?
Does the risk of attack justify the cost of defending against it?

EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-9/35

Finally, if there are holes in the existing safeguards that are serious, we need to figure out a way to plug them. This requires that we increase the system security with additional controls. However, before we do this, there are two questions that need to be asked.

- (1) How much does it cost to add this additional control versus how valuable is the asset that is going to be protected?
- (2) How serious is the threat? How expensive will it be for the attacker to exercise the threat versus what will be gained by compromising the asset.

For these questions, we must make value/cost estimates of

- (a) Adding security controls that may not exist yet
- (b) Assets that may be tangible quantities (cash) or intangible (corporate reputation)
- (c) Assets that may have a different value to the owner than the attacker (e.g., what is the dollar value to the owner of an irreplaceable photograph?)
- (d) An attack that cannot be directly translated into dollars (e.g., what is the time of a bored teenager worth when stealing a document that could be bought for \$20?)

Other Security Terms

- Security policy
 - A concise, high level statement of issues that will be dealt with in security the system under consideration
- Security domain
 - The scope of authority or scope of responsibility for security of the system. Think of this as corresponding to the security perimeter or edges of a physical system.
- Security architecture
 - A high-level description of the system under consideration, including all security-relevant capabilities, features, etc. and security controls, described in a way that is conducive to analysis of the system.
 - **System security cannot be discussed without a view of the system architecture!**

EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-10/35


Some other security terms we will be using in this course are listed above. Most are self explanatory, but I will give one physical example that might help clarify the concept of a security domain.

If you consider protecting your valuables (jewels, cash, identity documents, etc.) think about the levels of control that you might exert. Your house is probably locked and provides a moderate level of protection against the casual attacker. However, locks can be picked, doors and windows can be broken, so the protection is not absolute. You do use this level of protection for the majority of your possessions, however. It is very likely that within your house, you have a locked desk drawer, a strong box, or a hidden cookie jar where the things that are more important than your shoes are kept. Because this second level of protection is smaller, it is possible to provide a greater level of protection. The security perimeter is smaller, which generally translates into lower cost to offer a higher level of protection for a smaller volume.

When we examine securing wireless communications systems, the same reasoning will be used. A wide domain, e.g., the Stevens campus network, has a low to medium level of protection. There is (or should be) a consistent set of procedures within this domain. Within this domain, there may subdomains with additional levels of protection and different authorities to determine what is and what is not allowable.

This concept of nested security domains is commonplace in physical systems and we will see it is quite useful for electronic systems as well.

Approaching a Discussion of Security for a System

- Assume that it is not really needed
 - or –
 - Assume that it already exists
 - Test it in
 - Add it on
 - Design it in
- 
- Decreasing final cost

EE584
2/16/2011

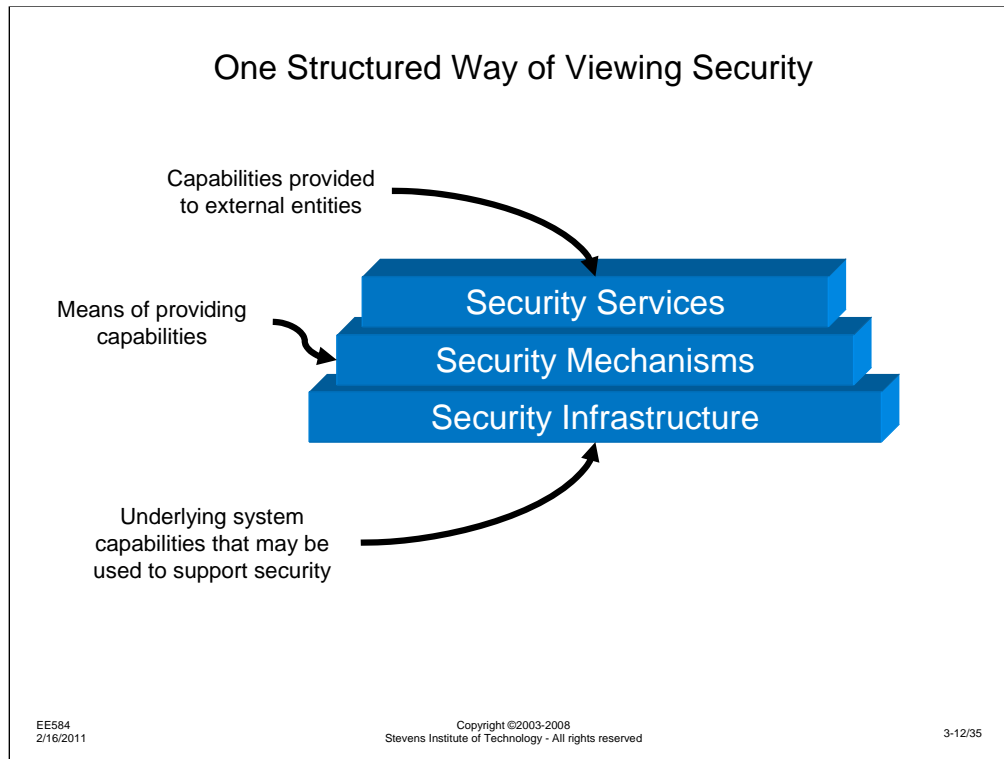
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-11/35

As we examine security concerns in complex systems, my emphasis will be to design security in from the initial concept of the system. There is certainly an obvious cost in taking the time to examine security as system requirements are being defined that one may often wish to avoid. Invariably, this leads to greater costs later in the product lifecycle, as the security gaps are discovered and exploited. Imagine that there are 1000s of units in the field when the first security bug is found. The fix has to be found and distributed to all the fielded systems. This is generally an expensive and error prone process that is not always followed correctly (how many of the security patches for Windows XXX have been loaded onto your computer?)

Sometimes the security fixes made after the fact in a manner that allows them to be added on. This is generally more expensive than designing them in. More expensive yet, is to test the security into the system – let it break and see why.

Worst of all is when the assumption is made that security is not really needed or that it already exists in the system. These systems are very likely to be expensive to maintain. I won't mention any multibillion dollar West Coast-based developers of operating systems here.



What we have discussed about security up until now is more process oriented, since I feel that security really needs to be an inherent part of the development process. What I want to introduce now is some of the more structural parts of the topic.

I have found the diagram above in explaining what the different pieces of security are:

On the top, security services are security-related capabilities that are made available to, for example, users. We will spend a bit of time later examining what these security services may be.

Security services need some technologies to enable them. These technologies are the security mechanisms.

Not actually part of the security of a system, but an important foundation element is the security infrastructure. This is a set of capabilities in the underlying system that can be called upon to provide functions that are needed to build a secure system.

Some Security Infrastructure Capabilities

- Time-of-day, time synchronization across network
- Naming infrastructure
- Directory infrastructure
- Registration authority
- Network management

EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-13/35

Listed here are some security infrastructure functions. Let's start with time-of-day: what does that have to do with security? Again, using the "Cuckoo's Egg" example, Cliff Stoll was trying to trace the path of an attacker as they hit his system and other systems. Knowing that an attack was made against his system at 6:01 pm in California while a related attack was occurring at 5:59 pm in Washington DC isn't very useful if the two computer clocks differ by 20 minutes. If they are synchronized, this might tell us which led to which and, thus, provides important security support.

The naming and (system) directory infrastructure are important elements of any computing system. If we can base user identification (a security service) on the naming infrastructure, and if consistent naming conventions are maintained across the network, this too, can be used in maintaining system security. Is bmcnair on Campus Pipeline the same entity as bmcnair on the ECE department koala system? If they are, we can correlate activities on the two systems to identify attack methods. If there is no system wide naming infrastructure, we don't know if separate events are related or coincidence.

Categories of Security Mechanisms

- *Prevent* occurrence of compromise
- *Detect* occurrence compromise
- *Correct* after-effects of compromise

EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-14/35

Next, let's examine security mechanisms. As I stated earlier, these are the technologies that we can use to enable security services. In considering security mechanisms, I have found it useful to break them into three groups, based on the point in time they are effective: before the attack, during the attack, or after the attack (past, present and future. If we had a mechanism for time travel, I suppose we would have to include the subjunctive case).

Mechanisms that are intended to protect an asset from compromise and are in place before the attack occurs are preventative mechanisms (just like brushing your teeth to prevent bacteria from creating decay). Sometimes it is not possible to prevent an incident ahead of time, or we want additional protection, just in case the preventative control fails. For this, we use detection mechanisms. These mechanisms detect an attack in progress, allowing a timely response, or at least knowing what has been compromised (as dentists use dental x-rays to detect cavities in their early stages). Sometimes, the effectiveness of the detection mechanism is so great that the attacker knows there is no sense in trying, so the detection mechanism becomes a deterrent, preventing the attack. Finally, there are after-the-fact correction mechanisms. The attack has occurred, we didn't detect it in time to prevent damage, we now need to get things back to the state they were in before the attack, or as close as possible (as a last resort, the tooth is pulled and replaced with a piece of plastic).

Security mechanisms are used at all stages. Prevention is the best alternative, but depending on the particular security issue, there may be no prevention mechanism.

Some Security Mechanisms and the Security Services They Could Enable

Service: Mechanisms:	ID	Auth	AC	Conf	Integ	Avail	NR
Cryptography/Encryption		✓		✓	✓		✓
Quality of Service Controls						✓	
Audit Logs			✓ *	✓ *	✓ *	✓ *	✓
Trusted Software			✓	✓	?	?	?
Security Policies	✓	✓	✓	✓	✓	✓	✓
Biometrics	✓	✓					
Smart Cards	✓	✓	✓	✓	✓		✓
System Backups					✓		✓
Security Assessment	✓	✓	✓	✓	✓	✓	✓

List of mechanisms is not meant to be exhaustive

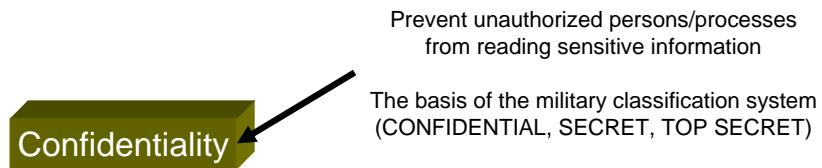
EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-15/35

Listed here (on the left) are several security mechanisms that exist. Listed across the top are the 7 security services we will be discussing in a few slides. I have indicated the applicability of various mechanisms to the different services. For instance, encryption technology can be used to provide authentication services, as well as confidentiality, integrity and non-repudiation. It is not particularly applicable to providing availability.

One Structured Way of Viewing Security



Security Services

EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

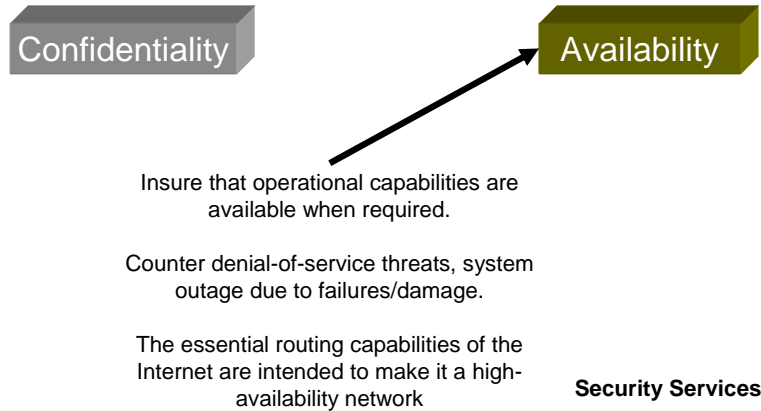
3-16/35

Let's now begin to examine the security services. I will start with Confidentiality, since it is one service most people think of when they discuss security.

The idea of keeping information confidential is to keep unauthorized persons from being able to see or read the information content. Trade-secrets, proprietary information, and classified military information are examples of information that requires that confidentiality be provided.

There are 6 more dimensions of security that we will discuss, but many people do not look further than confidentiality.

One Structured Way of Viewing Security



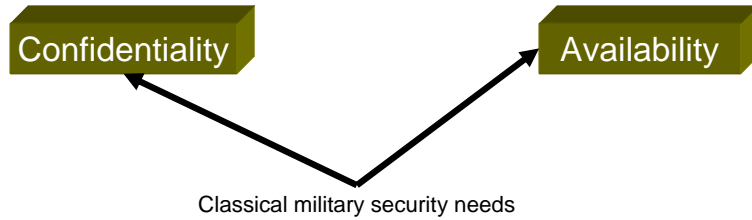
EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-17/35

Another security service is availability. Denial-of-service attacks, like recent Internet worms are examples of denial-of-service attacks intended to compromise the availability of a system.

One Structured Way of Viewing Security



Security Services

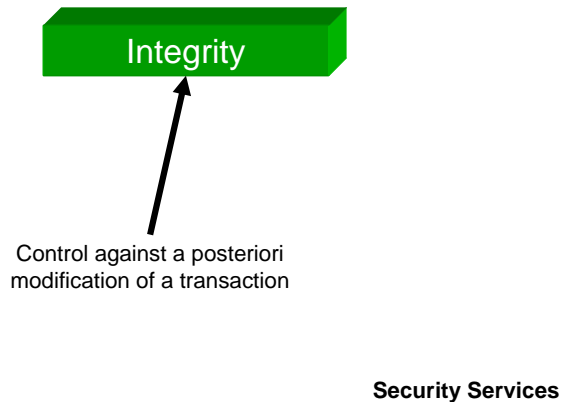
EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-18/35

When we consider the combination of confidentiality and availability, this set of services defines the classical military view of security. In general, up until the Internet boom, these security issues were generally not of concern to commercial users.

One Structured Way of Viewing Security



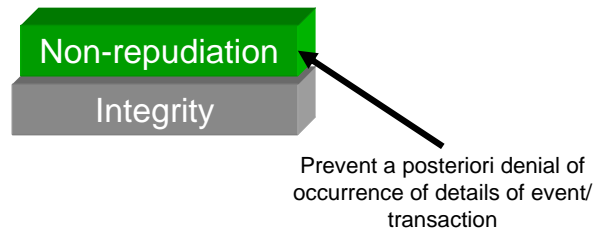
EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-19/35

Integrity is the next security service. Protecting the integrity of a communication protects the message from unauthorized modification. In conventional, non-electronic transactions, since the integrity of a transaction was of paramount importance to commerce, this aspect of security has received the greatest attention. Banking methods like summing and comparing columns and rows of transaction ledgers, special purpose check-writing devices, and using paper that reveals modification are some of the methods used to ensure the integrity of non-electronic transactions. If we move from paper commerce to electronic commerce, the same controls are needed.

One Structured Way of Viewing Security



Security Services

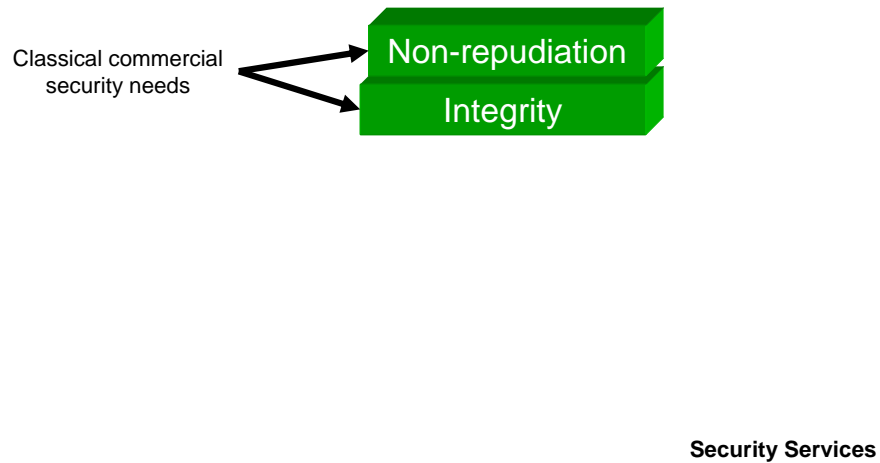
EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-20/35

The next service, and another with historical roots in paper transactions is the Non-repudiation service. Non-repudiation provides protection against one party denying having engaged in a transaction. Non-electronic systems use written signatures (in ink), wax seals, and the embossed seal of a government agency or notary public to ensure a document signature cannot be denied. In electronic systems, as well as in paper-based systems, the only way to create a meaningful non-repudiation control is to build it on top of an integrity control. By analogy, one would never sign a check that was written in pencil, lest they take a chance that the amounts or payee might be changed.

One Structured Way of Viewing Security

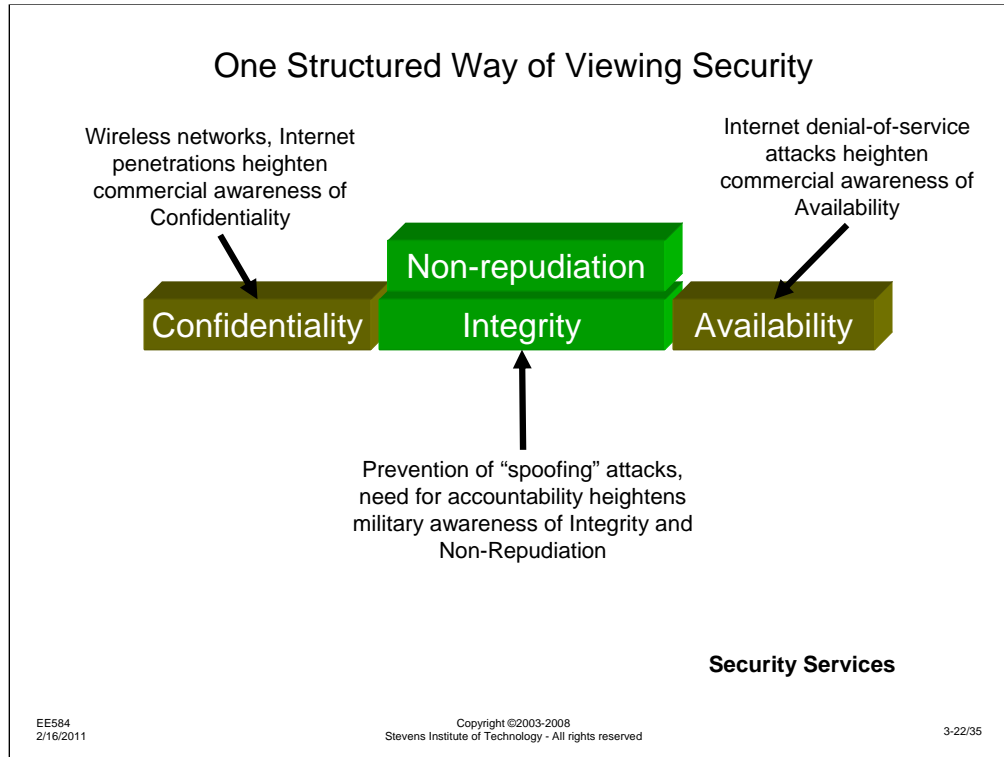


EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

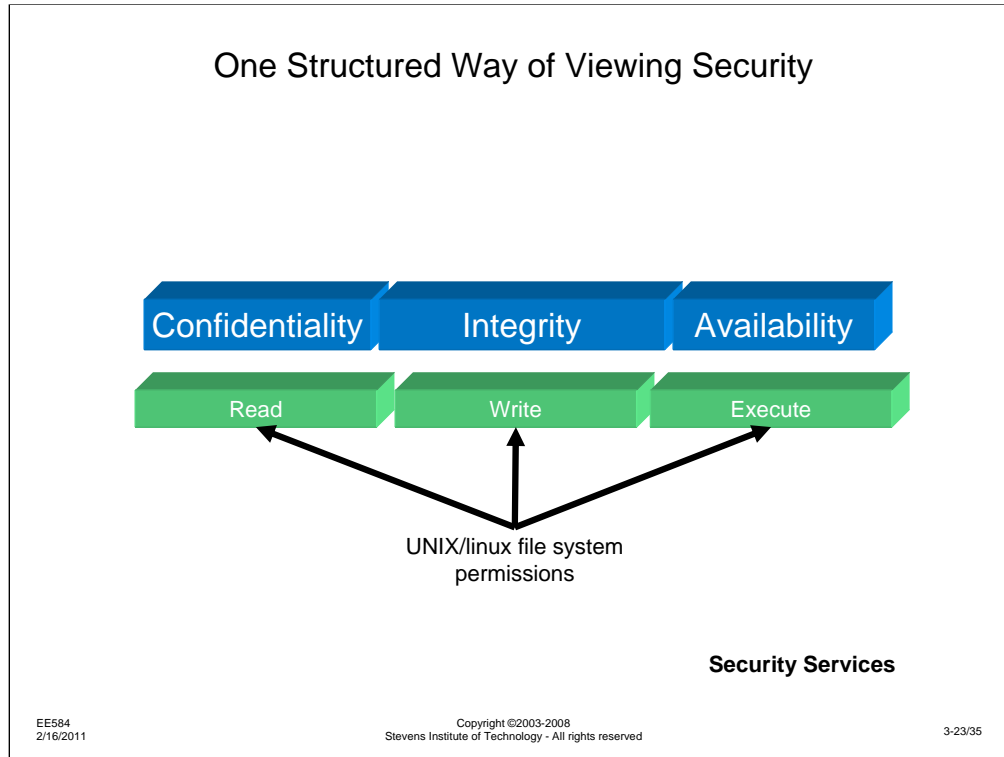
3-21/35

While the military has traditionally focused on confidentiality and availability, commercial needs have generally focused on the integrity and non-repudiation of transactions.



When we put together these sets of needs, we see the top layers of security services. However, as the electronic systems have matured and new threats have evolved, the security concerns of military and commercial users have begun to overlap. As previously mentioned, Internet works have created denial-of-service threats that have disrupted commercial networks. For an information-centric business (e.g., a telecommunications company or a stock broker), when information stops flowing, so does revenue. This has made availability a commercial concern. Likewise, with the attacks against web sites where user credit card numbers have been compromised, commercial operators have become more concerned about confidentiality of the information they manage.

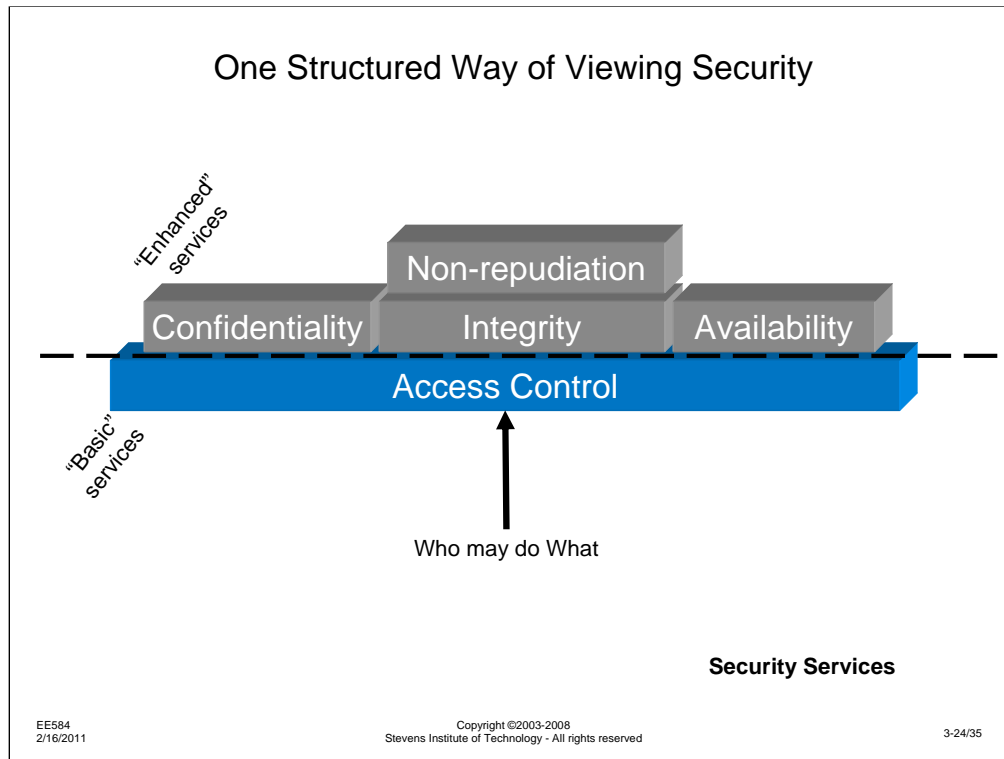
At the same time, as the military has moved to electronic systems for command, control, communications, and intelligence, their reliance on the correctness of information and the ability to verify who provided information or generated a command becomes even more important. Thus, the distinction between the security concerns of military and commercial are moving closer.



An aside: I created the security architecture we are discussing here in the context of a security group I was managing in Bell Labs in the late 1980s. Since international standard committees had been studying this area for some time and had not come to the same viewpoint (e.g., they had not identified Availability as a necessary security service), I felt that I had to validate the architecture. When reasoning about a subject as abstract as security can be, it is difficult to prove or disprove the correctness of an architecture. Instead, for this part of the architecture, I found that there was an independent path to the same conclusion.

The UNIX operating system and the linux OS that was built to a common specification (POSIX), both provide file system permissions to control use and access to resources. These operating systems use a Read-Write-Execute set of file permissions to control access. It turns out that the R-W-X flags directly correspond to the Confidentiality, Integrity, and Availability security services in controlling who can read or modify a file or who can execute a command, influencing the use of system resources.

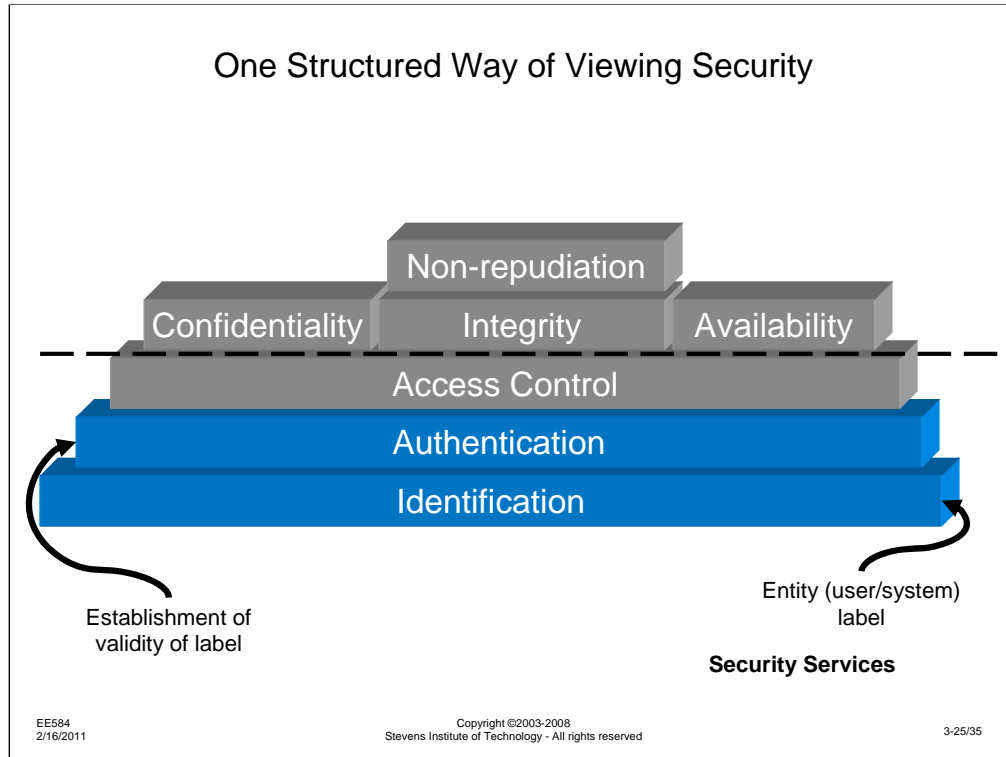
While this does not PROVE the logical completeness of these three security services, the independent path to a parallel solution certainly lends credibility to the completeness of this set of services. In addition, although I am constantly looking for any missing pieces or inconsistency, I have not found one in several years of study.



The security services we have discussed up to now are what I refer to as “Enhanced services.” Not everyone will need all of the services, but they may pick and choose which are important for their particular system.

There are lower level “basic services” that these higher level services are based on. Just as it is not possible to have Non-repudiation without Integrity (or, I could prove that you signed something, but we can’t agree on what was signed), it is not possible to have the higher layer services without a foundation. Working our way down the structure, we come first to the Access Control service.

The Access Control service specifies who may do what. In essence, this service binds the individual person or process specified by a lower level service to the permissions of the higher level services. For instance, in the UNIX or linux system, there is a set of read-write-execute permissions that exist at the individual, group, or system level. Separate permissions may be set for different groups of users.

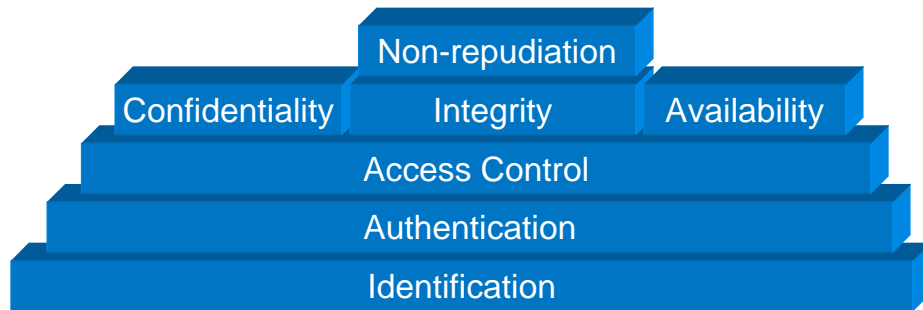


Below the Access Control service are two foundation services that are critical to any security system – the Identification service provides a method to associate a user with their name or identity; the Authentication service provides a way to prove the association.

In terms that most everyone is familiar with, consider the user login and password. The user login is a public piece of information which NAMES the individual within the context of the system they are accessing. Anyone can make an identity claim by stating the user login name. What makes this identity claim authentic is the secret password. Only the valid user should know the password, so only they can authenticate themselves to the system.

A similar technique is used with an ATM card. Possession of the card and inserting it into the ATM machine makes an identity claim as to the user of the card. Here, the card number is the user login. The secret information the user provides, equivalent to the password, is their Personal Identification Number (PIN). Actually, it should be called the Personal Authentication Number, but we won't go into that.

One Structured Way of Viewing Security



Security Services

EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-26/35

So, this is complete set of security services. Six of the security services were identified in ISO-7498-2:1989, "Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture." That document did not include Availability, since it was written from the perspective of an equipment provider and not a network operator, where denial-of-service attacks have been more visible. It also did not include the structural relationship between the security services.

As stated earlier, this set of services has withstood constant scrutiny: are the services independent of each other, or can one be stated in terms of the other? Are there any other security related issues that don't cleanly fall within one service or the other, e.g., are there gaps in the coverage? Is the relationship between services correct, or might there be dependencies that this architecture is missing? I haven't found any cases that lead me to think this architecture needs revising, but I am always open to suggestion. Discussion topic: can you think of any issues that "fall in the cracks"?

What Security Issues Can Be Addressed By Cryptography and Related Techniques?

- Cryptography is NOT the solution to all security problems, but
- It does provide an enabling technology for many issues.
- If intelligently applied (balanced against other issues and needs) it can be of substantial value
- It provides a good place to start discussing detailed security technologies in an Information System

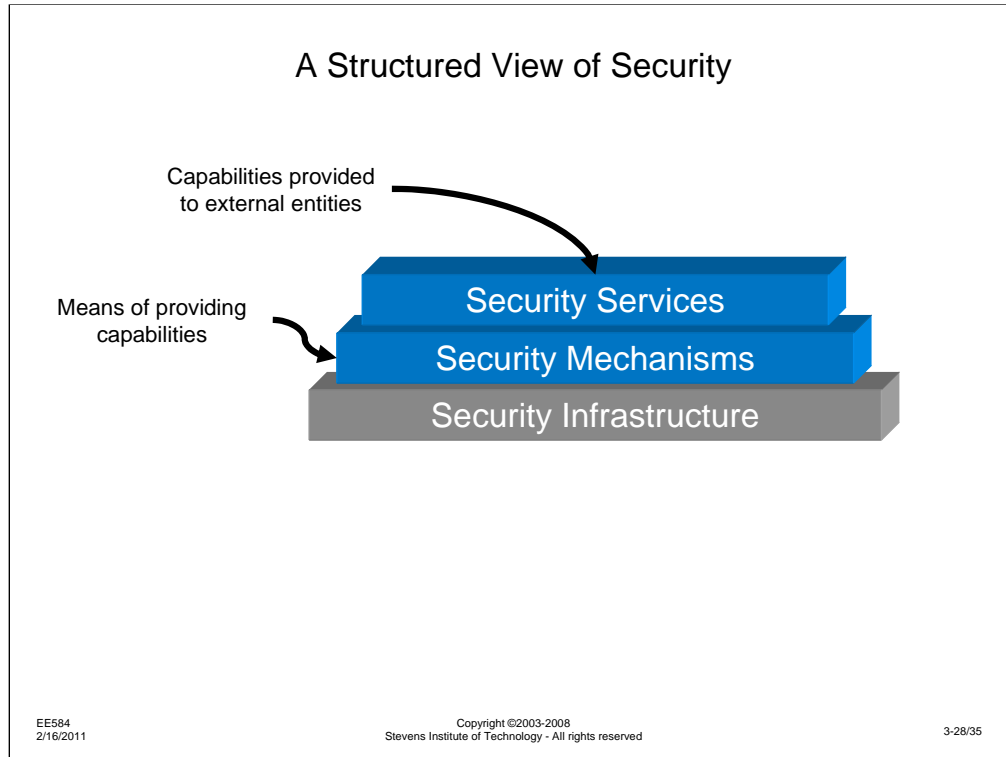
EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-27/35

Let's turn now to a discussion of security mechanisms. In particular, I'll start with cryptography. There are a couple of reasons I start here: I have been interested and involved in this area for most of my career in one way or another; I think it is an area that is still rich with research and applications topics; and it forms the basis of a lot of security in modern systems.

Cryptography is an important technology for confidentiality. I might go so far as to say that you really can't provide confidentiality in an electronic system without some form of cryptography. It is also valuable to provide other security services, as we will discuss later. On the other hand, cryptography does not solve ALL security issues. For instance, it doesn't really do much good against a denial-of-service attack. In some cases, it could make such an attack worse.



Going back to the earlier model, we will examine cryptography as one security mechanism and discuss what services it can provide and how.

Categories of Security Mechanisms And Those That Can Be Addressed By Cryptography

- *Prevent* occurrence of compromise
- *Detect* occurrence compromise
- *Correct* after-effects of compromise

From the previous discussion, I identified the three types of security mechanisms and when they are effective. Security mechanisms built on cryptography can be used to prevent attack or detect the occurrence of an attack, but are generally not useful as a mechanism to correct the damage from an attack.

Some Security Mechanisms and the Security Services They Could Enable

Service: Mechanisms:	ID	Auth	AC	Conf	Integ	Avail	NR
Cryptography/Encryption		✓		✓	✓		✓
Quality of Service Controls						✓	
Audit Logs			✓*	✓*	✓*	✓*	✓
Trusted Software			✓	✓	?	?	?
Security Policies	✓	✓	✓	✓	✓	✓	✓
Biometrics	✓	✓					
Smart Cards	✓	✓	✓	✓	✓		✓
System Backups					✓		✓
Security Assessment	✓	✓	✓	✓	✓	✓	✓

List of mechanisms is not meant to be exhaustive

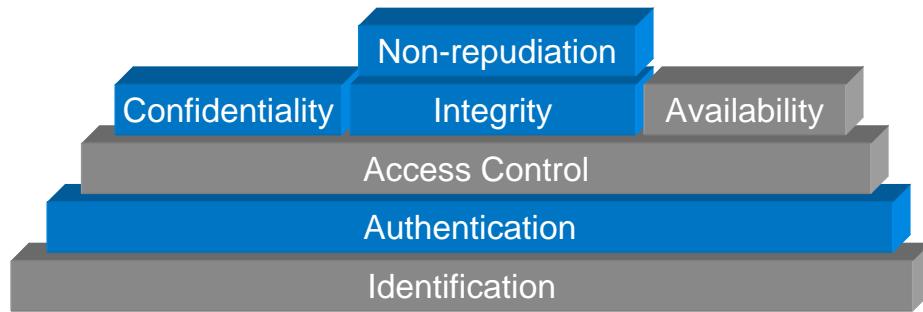
EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-30/35

As seen earlier, cryptography can support several of the security services. In next week's material I will discuss exactly how one might apply encryption to providing authentication, confidentiality, integrity and non-repudiation.

One Structured Way of Viewing Security
And Security Services Addressed By Cryptography



Security Services

EE584
2/16/2011

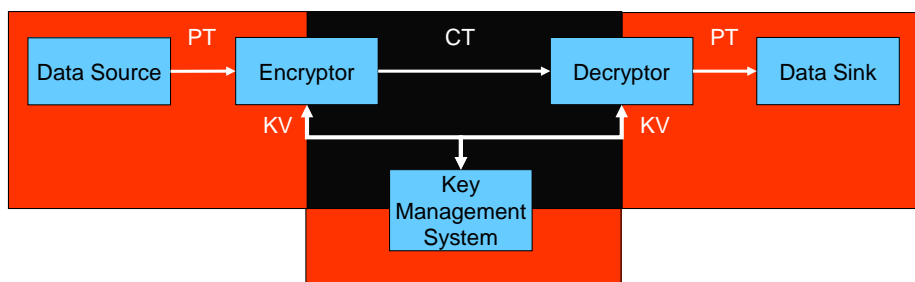
Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-31/35

Looking back at the set of security services, I have highlighted the services cryptography can support.

Cryptography Terminology

- Plaintext (PT) – unprotected source material (images, text, data, etc.)
- Ciphertext (CT) – Plaintext that has been enciphered (encrypted)
- Key Variable (KV) – Parameter of cryptographic system that selects, specifies, or controls key stream
- Key Management – Process for providing corresponding key variable(s) to sender and receiver



EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-32/35

To finish up this week's material, I want to introduce some of the terms used in cryptographic systems.

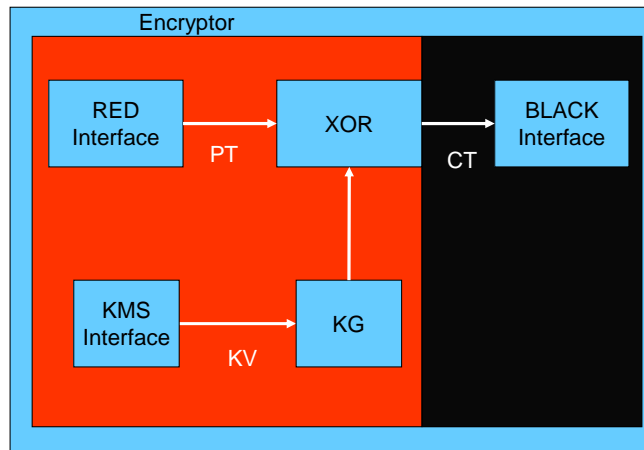
In almost any discussion of cryptography, particularly in military systems, the terms “red” and “black” will come up. As is normally the case, “red” signals the need for caution or is used to highlight a dangerous condition. Here, red information is information that has not yet been protected by the cryptographic system and is in danger of being stolen. Black information is encrypted information. It is assumed that the enemy has full access to all black information. The proper design of the encryption system ensures that access to black information does not, in any way, create the potential for compromise of red information.

Information that has not been encrypted is referred to as Plaintext. After being encrypted, the information is Ciphertext. As we will see later, we would like to use one single cryptographic system for a variety of installations or applications. For this reason, we want to be able to change the parameters that protect the information. The parameter that selects which of a large family of cryptographic functions will be used at any one time is the Key Variable.

Finally, key variables must be coordinated between the sender (encryptor) and receiver (decryptor). The key management system makes this coordination possible.

Cryptography Terminology - Continued

- Key Stream (Key Sequence) (KS) – (Pseudo)random string of symbols used to encrypt and/or decrypt plaintext
- Key Generator (KG) – Device that generates the key stream for a stream encipherment device



EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-33/35

If we open up the encryptor, inside we will find a fairly simple architecture. The key variable controls the behavior of the Key Generator. The key generator creates a stream of seemingly random data known as the Key Stream. This key stream is combined with the plaintext to form ciphertext with a very simple process based on the Exclusive-Or function (XOR). The XOR has the property that if the bit coming from the key generator is a 0, the plaintext is passed through unchanged. If the input from the key generator is a 1, the plaintext is inverted, that is 1's become 0's and 0's become 1's. As you will see, if the key sequence used at the transmitter and receiver is identical, $PT(XOR)0(XOR)0 = PT$, while $PT(XOR)1(XOR)1 = PT$, so the message is unchanged. However, if the key sequence is not known (e.g., by the enemy) or if the key sequence is out of step at the transmitter or receiver, the seemingly random sequence of 1's and 0's that the key generator creates essentially makes the ciphertext appear to be a random string of 1s and 0s, containing no discernable pattern or information.

Miscellaneous Cryptography Terminology

- Affine:
 $F(x) = \alpha x + \beta$
- Linear:
 $F(x) = \gamma x$
 $F(\alpha x + \beta y) = \alpha F(x) + \beta F(y)$ [superposition]
- Nonlinear:
Superposition does not apply
- Permutation:
Reordering of inputs, e.g., $P(\{a,b,c,d\}) = \{c,b,a,d\}$
- Substitution:
Functional mapping, non necessarily 1-1 or onto

EE584
2/16/2011

Copyright ©2003-2008
Stevens Institute of Technology - All rights reserved

3-34/35

There are some other terms that we will use in the discussion of cryptographic systems that I have listed here.

Cryptographic systems are not linear transformations from input to output. If they were, it would be fairly easy to gather bits of information and gradually break the system. In particular, the nonlinear functions that are typically used in cryptographic systems are the functions of permutation and substitution. The permutation operation takes a set of inputs and reorders them. For instance, when a deck of cards is shuffled, the order of the cards is permuted. The same cards appear in the deck, but their order is different than it was before shuffling.

The substitution function is a mapping from an input space to an output space. It is not necessary that the two spaces be the same size, that is, we could map the 52 cards in a deck of cards to a set of 10 numbers. Clearly there will be at least two distinct cards that are mapped to the same number. On the other hand, we might map the set of 52 cards to a set of numbers from 0 to 99. In this case, there must be at least 48 numbers that are never used. Or there might still be two cards that map to the same number, depending on how we choose the mapping.

In general, to be cryptographically useful, the mapping functions used in a substitution or permutation function should not be simple or straightforward. The choice of what makes a good function is beyond the scope of this course, however, and has made for some interesting PhD theses.

Wireless Technical Paper Assignment

- Access procedures have been changed, and will probably change in the future... Currently, (Spring 2011) you can go to the Library page (www.stevens.edu/library) and click on "on-line services." From there, clicking on the link to the IEEE library (conveniently located under "I") will prompt you for the Ezproxy login, if needed and get you to the IEEE
- Access the IEEE library of publications
- On the IEEE Ixplorer® site, click on the Table of Contents Journals and Magazines, on the left side
- The complete contents of the IEEE Transactions on Wireless Communications is available by clicking on the W from the list of letters across the top of the page and following the link to "Wireless Communications, IEEE Transactions on"
- Pick a Wireless Communications Transactions paper that interests you from any of those available from the last 5 years
- Write a 3-5 page report on the paper. Report should include:
 - Citation of the paper you are using
 - Summary of fundamental ideas presented in the paper
 - Issues paper addresses and how they have been addressed in the past
 - Discussion of 1 or 2 core ideas of paper
 - Identification of any security-related issues brought up in the paper (there may not be any)
 - Potential applications of technology presented
 - Future opportunities created by the technology

Note: The IEEE Transactions on Wireless Communications IS NOT the same as the IEEE Wireless Communications magazine. Be sure to use the Transactions for this assignment.