Security Models, Information Sharing and Analysis

CS-3113: PRINCIPLES OF CYBER SECURITY

BENJAMIN R. ANDERSON

Trusted System

There are only two possibilities when it comes to being a secure system:

- The system is secure – at all times, from all attacks
- It is not secure – there are types of attacks, or certain times when it is not secure
- Keep in mind that the “time” aspect can be anywhere in the systems lifecycle
  - Can you protect it in manufacturing?
  - Can you protect it, and the information, when the system is decommissioned?

We have not yet been able to develop a secure system

Instead, many security professionals prefer to speak in terms of placing "trust" in a system

There are degrees of trust

- You may trust a family member with access to your computer, or a password
- You would not trust a stranger (or even an acquaintance) with the same access or information

Trusted Computing Base

The term "trusted computing base" (TCB) originated from the Orange Book and does not address the level of security a system provides, but the level of trust, albeit from a security perspective

Trusted Computing Base definition:

- *The trusted computing base (TCB) of a computer system is the set of all hardware, firmware, and/or software components that are critical to its security, in the sense that bugs or vulnerabilities occurring inside the TCB might jeopardize the security properties of the entire system.*
- *https://en.wikipedia.org/wiki/Trusted_computing_base*

Addressing trust is done because no computer system can be totally secure

- The types of attacks and vulnerabilities change and evolve over time
- With enough time and resources, most attacks can become successful

However, if a system meets a certain criteria, it is looked upon as providing a certain level of trust (not security)

All components in the TCB has a responsibility to support and enforce the security policy of that particular system.

Security Policies

As mentioned earlier, security is more than just ensuring hardware and software is secure

The first step in creating a secure system is to establish security policies that identify what you are trying to achieve

- For example, determining which aspect of the CIA Triad is more important
- Confidentiality – like the military
- Integrity – like financial institutions
- Availability – like safety systems

Security Policy: a statement of the security we expect the system to enforce.

An operating system – or other component in a trusted system – is only trusted in relation to its security policy and the aspects of the policy it is expected to satisfy

From *Security in Computing* by Pfleeger and Pfleeger:

Policies do not come in a "one size fits all" template. There are different levels of security policies:

- *Strategic - what is the overall security goal for the organization (e.g. our military versus banking discussion)*
- *Tactical (operational) – more of a statement on how we will implement some aspect of security.*

Password Policies

A security policy that everyone is probably familiar with is the password policy

These policies usually include:

- Length requirements
- Complexity requirements (upper-case, lower-case, number, symbol, etc.)
- How often they have to be changed
- Proper handling/behaviors

Here is a sample password policy provided by the Rhode Island Department of Education via the National Center for Education Statistics:

- https://nces.ed.gov/pubs2003/secureweb/a_e5.asp

Often, where there are policies everyone needs, a standard is developed

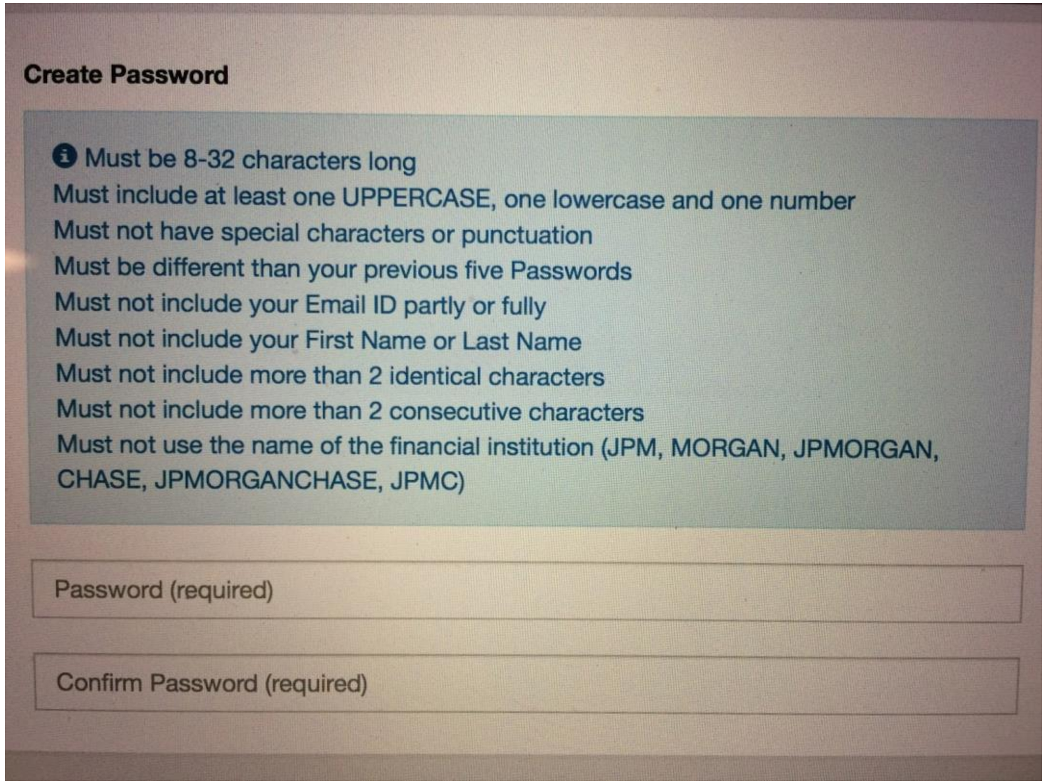
For example, NIST developed NIST SP 800-63b: Digital Identity Guidelines

- https://pages.nist.gov/800-63-3/sp800-63b.html
- Look at section 5.1.1.2 Memorized Secret Verifiers
  - Notice the different length requirements for subscriber-chosen passwords and for randomly chosen passwords
  - Also notice what the passwords should be checked against
    - Previous passwords from breaches
    - Dictionary words
    - Etc.

Password Policies

Here is a password policy that I have run into previously

- As you can see, they don't allow their organization to be used as part of the password
- This way, someone doesn't use:
  - passwordJPMORGAN
  - Essentially, they have added their own organization to the dictionary they check against
- Also note that they don't allow special characters or punctuation
  - This is probably to help prevent injection attacks



Create Password

Must be 8-32 characters long
Must include at least one UPPERCASE, one lowercase and one number
Must not have special characters or punctuation
Must be different than your previous five Passwords
Must not include your Email ID partly or fully
Must not include your First Name or Last Name
Must not include more than 2 identical characters
Must not include more than 2 consecutive characters
Must not use the name of the financial institution (JPM, MORGAN, JPMORGAN, CHASE, JPMORGANCHASE, JPMC)

Password (required)

Confirm Password (required)

TCSEC – The "Orange Book"

The Orange Book is not in use anymore, but provided a lot of the foundations for security requirements

- Its title is the "Trusted Computer System Evaluation Criteria" or TCSEC, but it is generally referred to as the "Orange Book" because its cover was orange
- It was part of a series of standards called "The Rainbow Series" since the different books had different colors for the cover
- https://en.wikipedia.org/wiki/Rainbow_Series

Reference for the standard:

- https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf

From the Orange Book:

- *Requirement 1 - SECURITY POLICY - There must be an explicit and well-defined security policy enforced by the system. Given identified subjects and objects, there must be a set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object. Computer systems of interest must enforce a mandatory security policy that can effectively implement access rules for handling sensitive (e.g., classified) information.[7] These rules include requirements such as: No person lacking proper personnel security clearance shall obtain access to classified information. In addition, discretionary security controls are required to ensure that only selected users or groups of users may obtain access to data (e.g., based on a need-to-know).*

The Orange Book

For a system at the C1 level (DISCRETIONARY SECURITY PROTECTION):

- *2.1.1 Security Policy*
  - *2.1.1.1 Discretionary Access Control*

    The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals or defined groups or both.

For a system at the C2 level (CONTROLLED ACCESS PROTECTION):

- *2.2.1 Security Policy*
  - *2.2.1.1 Discretionary Access Control*

    The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

Notice the additional requirements as we move up in security classes

How does a Linux system accomplish this?

Do the protection/permission bits satisfy this requirement?

Security Policy

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- *A **security policy** is a document that defines the scope of security needed by the organization and discusses the assets that require protection and the extent to which security solutions should go to provide the necessary protection*
- *The security policy is used to assign responsibilities, define roles, specify audit requirements, outline enforcement processes, indicate compliance requirements, and define acceptable risk levels*

Policy vs Model

From OSG:

- *A **security model** provides a way for designers to map abstract statements into a security policy that prescribes the algorithms and data structures necessary to build hardware and software. Thus a security model gives software designers something against which to measure their design and implementation.*

As you can see from the definitions, a security policy contains the abstract goals of security, and the security model provides the details on what (and how) it should be done (or what shouldn't be done)

- Ex: A policy might say "be heathy" and a model would have the details "eat a balanced diet, exercise regularly, don't smoke, etc."

Reference: Certified Information System Security Professional Official Study Guide, Ninth Edition, by Chapple, Stewart, and Gibson

Security Mode Principles

Here are some of the concepts used in security models

- As you read them, compare them to the NSA design principles
- ***Identity***: Can each user, program, object, and resource be uniquely identified?
- ***Accountability***: Can users be held accountable for their actions?
- ***Monitoring***: Is a record maintained of users actions?
- ***Authorization***: Do rules exist to govern which entities may access which objects?
- ***Least privilege***: Are users restricted to the minimal set of resources needed to perform their job?
- ***Separation***: Are the actions of entities prevented from interfering or colluding with the actions of other entities?
- ***Redundancy***: Are copies of hardware, software, and data components maintained to ensure consistency, accuracy, and timeliness of results across locations?

Reference Monitor

From OSG:

- *The part of the TCB that validates access to every resource prior to granting access requests is called the* ***reference monitor****. The reference monitor stands between every subject and object, verifying that a requesting subject's credentials meet the object's access requirements before any requests are allowed to proceed. Effectively, the reference monitor is the access control enforcer for the TCB. The reference monitor enforces access control or authorization based on the desired security model, whether discretionary, mandatory, role-based, or some other form of access control.*

Essentially, the reference monitor is what verifies that a subject (user, application, process, etc.) has authorized access to an object (file, memory location, etc.) before the subject is allowed to access the object

Reference: Certified Information System Security Professional Official Study Guide, Ninth Edition, by Chapple, Stewart, and Gibson

Security Kernel

From OSG:

- *The collection of components in the TCB that work together to implement reference monitor functions is called the **security kernel**. The reference monitor is a concept or theory that is put into practice via the implantation of a security kernel in software or hardware. The purpose for the security kernel is to launch appropriate components to enforce reference monitor functionality and resist all known attacks. The security kernel mediates all resource access requests, granting only those requests that match the appropriate access rules in use for a system.*

From Cloud Academy, CISSP: Domain 8 – Software Development Security – Module 3:

- https://cloudacademy.com/course/cissp-domain-8-module-3/considerations-for-secure-software-development/
- *And the three main requirements of the kernel and the reference monitor include these: the security kernel must provide isolation for the processes carrying out the reference monitor concept and must be tamper-proof, the reference monitor must be invoked for every access attempt and must be impossible to be circumvented, the reference monitor must be small enough to be tested and verified in a complete and comprehensive manner.*

Note: The reference monitor is the abstract concept, while the security kernel is the implementation

OSG Reference: Certified Information System Security Professional Official Study Guide, Ninth Edition, by Chapple, Stewart, and Gibson

Domain

From : *CISSP All-in-one Exam Guide*, chapter 5: Security Models and Architecture

- *A domain is defined as a set of objects that a subject is able to access. This domain can be all the resources a user can access, all the files available to a program, the memory segments available to a process, or the services and processes available to an application. A subject needs to be able to access and use objects (resources) to perform tasks, and the domain defines which objects are available to the subject and which objects are untouchable and therefore unusable by the subject. A security domain has a direct correlation to the protection ring that a subject or object is assigned to. The lower the protection ring number, the higher the privilege and the larger the security domain.*

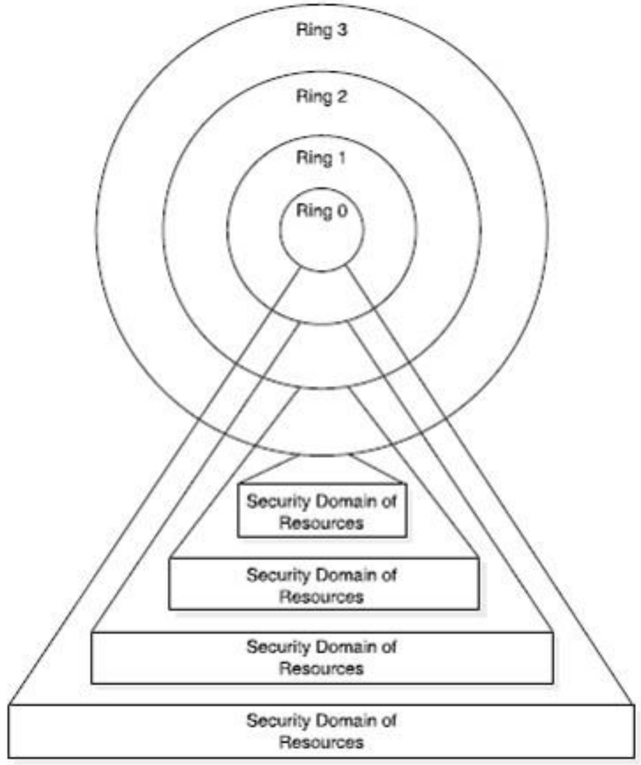

Ring 3
Ring 2
Ring 1
Ring 0
Security Domain of Resources
Security Domain of Resources
Security Domain of Resources
Security Domain of Resources

Figure 5-13 The higher the level of trust, the larger the number of available resources.

Military Security Policy (Clearances)

The primary purpose of a military security policy is confidentiality

- i.e. – Prevent the disclosure of information, particularly classified information
- They are also concerned with integrity and availability, but the highest priority is confidentiality

To implement this, each piece of information is provided a label with its sensitivity level

- For the U.S. Government, there are:
  - Information that isn't classified: Unclassified (U)
  - Information that is classified: Confidential (C), Secret (S), Top Secret (TS)
- These form a hierarchy, with: U < C < S < TS

In addition, there is a requirement for "need to know"

- Just because you are cleared to a certain level doesn't mean you have access to everything at that level – just what you need to know for you roles and responsibilities

Military Security Policy (Clearances)

In addition to levels, there are also compartments

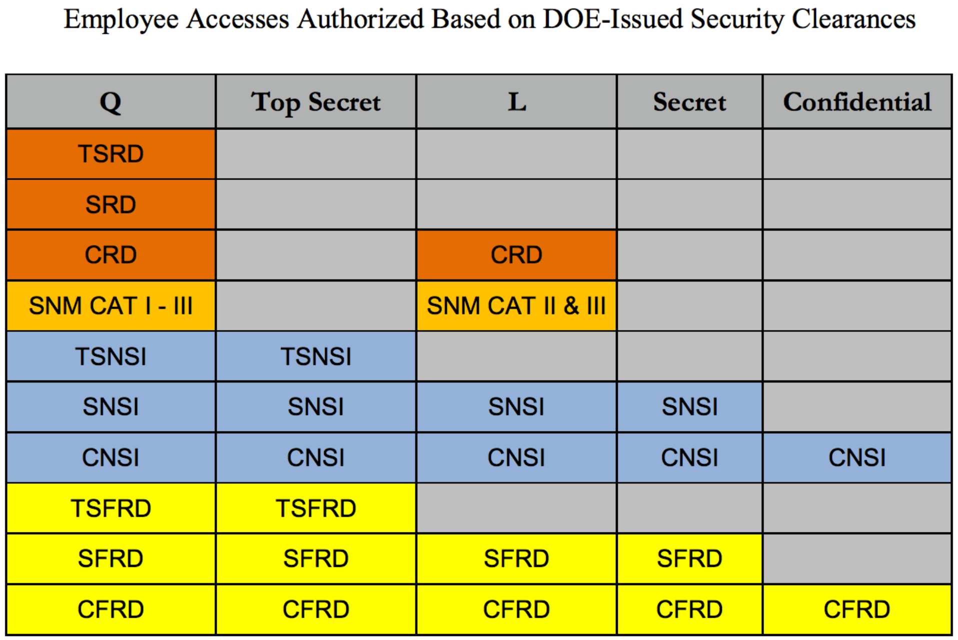
- These are related to need-to-know, but are still separate
- Information may be in one or more compartments and subjects may have access to more than one compartment

The Department of Energy also uses “Categories” – which are like compartments – since they deal with nuclear weapons

- Restricted Data (RD) is nuclear weapon information
- Formerly Restricted Data (FRD) is nuclear weapon data that was designated to be available to the military
- National Security Information (NSI) is information on national security topics

The DOE used “Q” and “L” clearances instead of TS or S since those categories have special clearance requirements

- See the diagram for more details



Employee Accesses Authorized Based on DOE-Issued Security Clearances

Q	Top Secret	L	Secret	Confidential
TSRD				
SRD				
CRD		CRD		
SNM CAT I - III		SNM CAT II & III		
TSNSI	TSNSI			
SNSI	SNSI	SNSI	SNSI	
CNSI	CNSI	CNSI	CNSI	CNSI
TSFRD	TSFRD			
SFRD	SFRD	SFRD	SFRD	
CFRD	CFRD	CFRD	CFRD	CFRD

Image from: https://en.wikipedia.org/wiki/Q_clearance

Military Security Policy

There are also other compartments and restrictions:

- SCI – sensitive compartmented information
  - Not “above” Top Secret
  - This is still a compartment
- NATO – share only with NATO allies
- NOFORN – No Foreign, information can only be shared with U.S. citizens

Dominance Function

The combination of rank (sensitivity level) and compartment is referred to as an object's class or classification.

A clearance is a statement of the level of information an individual is trusted to access.

We can define a dominance function where:

If we have, S(rank, set_of_compartments) and O(rank, set_of_compartments)

S ***dominates*** O if and only if

- O.rank < S.rank ***and*** O.set_of_compartments ⊆ S.set_of_compartments
- ⊆ is the subset operator

Security Models

According to Pfleeger and Pfleeger in their textbook, models can be used to:

- Test a particular security policy for completeness and consistency
- Document a policy
- Help conceptualize and design an implementation
- Check whether an implementation meets its requirements.

In several of the models, maintaining separation between varying levels of security is the chief concern.

This is the multilevel security problem.

Lattice Model

The military security model is an example of a more general scheme known as lattice.

The dominance relation (***dom***) of the security model is the same relation found in the lattice model

- Top Secret dominates Secret, Secret dominates Unclassified, therefore Top Secret also dominates Unclassified (property of a lattice)

There are other similar lattice relationships in the private sector

- *Internal* dominates *Proprietary* which dominates *Public*

Many security models based on lattice model because it naturally represents increasing degrees/levels of security.

Bell-LaPadula Model

This is the model used in the "Orange Book". It describes the traditional approach/concern for the military

- Particular emphasis is on preventing unauthorized disclosure of information.

Simple Security Condition (policy/property)

- Allows a subject read access to an object only if the security level of the subject dominates the security level of the object.

*-Property (star-property)

- Allows a subject write access to an object only if the security level of the subject is dominated by the security level of the object. Also known as the Confinement Property.

These two properties taken together are often referred to as the "No Read Up/No Write Down" policies.

Consider: What does "No Read Up/No Write Down" mean, and how it implements the militaries desire to maintain confidentiality.

Bell-LaPadula Model

No Read Up (the simple security condition):

- This is fairly straightforward.
- An example would be a user cleared for Secret information would NOT be allowed to read a file at a higher classification such as TOP SECRET (thus "no read up").

No Write Down (the *-property):

- This is less obvious
- An example would be a user cleared for TOP SECRET would not be allowed to write to a file or send information to a user only cleared for SECRET (thus "no write down")
- But, what if the TOP SECRET user is only going to write SECRET information to a file or send it to a SECRET user. Why can't the TOP SECRET user do this -- send only SECRET information to a SECRET user?
  - The answer is that the computer is expected to prevent any accident from happening
  - Thus, if a TOP SECRET user is prevented from writing to a file a SECRET user can access, there is no possible way, deliberate or accidental, that the TOP SECRET user can divulge TOP SECRET information to the SECRET user

Commercial Security Policies

While most companies are not concerned with classified data, they still may have different "levels of sensitivity" of data that must be protected

- Example, Public information versus proprietary information

Another difference between commercial and military policies is that commercial entities frequently don't introduce a concept of "clearances" for employees and access cannot be based on some theory of "dominance“

Finally, the military security policy is based on confidentiality because the military is most concerned about disclosure

- In industry, integrity and availability are at least as equally important and often considered more important

There are a number of models that aren’t don’t use confidentiality as the primary concern

Clark-Wilson Security Model

As we have mentioned, the "military security policy" is focused on unauthorized disclosure but in some environments disclosure is not as important as modification (confidentiality –vs– integrity)

Consider a person's bank account or medical records for example

- It is important to keep the account balance information private
- However, it is far more important that another user is unable to change the account balance
- This can also hold in other areas, like medical records – test results should not be changed.
- In these situations, integrity is more important than confidentiality

For the Clark-Wilson Model, integrity is the focus

- The goal is to insure that no user can modify data in a manner that would result in the loss or corruption of assets.

Clark-Wilson Security Model

Clark-Wilson uses 2 mechanisms used to achieve this goal:

- ***Well-formed transactions***: Data can only be modified in very constrained ways
- ***Separation of Duty***: Separates operations into parts and requires each part be performed by a different subject

Auditing is also required in this model

From: *CISSP All-in-One Exam Guide*, Chapter 5: Security Models and Architecture

- *In the Clark-Wilson model, users cannot access and manipulate objects directly, but must access the object through a program. This provides another layer of protection between the subject and the object and further restricts the type of actions that can take place on that object, thus protecting the integrity of the object…*

  Clark-Wilson model prevents authorized users from making modifications by requiring them to go through programs to modify objects. It also prevents authorized users from making improper modifications by enforcing separation of duties, and maintains an audit log for external transactions.

Biba Integrity Model

The Biba Integrity Model, like the Clark-Wilson model, is based on integrity

- At its most basic level, Biba ignores the issue of secrecy, instead concentrating on integrity
- Some environments are concerned more with the validity of information as opposed to maintaining confidentiality
- Sometimes Biba is thought of as the "dual" of the Bell-La Padula model

Biba defines "integrity levels" which are analogous to the sensitivity levels in the Bell-LaPadula model

Biba is based on the fact that a subject can only have the amount of trust in an object equal to the level of integrity for the lowest subject

If you can’t trust an individual

- You can’t trust the data that the individual has had the ability to modify

Biba Integrity Model

Biba supports 5 different integrity principles:

1. ***Low-Water Mark Policy***: The integrity level of a subject immediately following an observed access to an object is set to be the lower of the integrity levels for the subject and the object
2. ***Low-Water Mark Policy for Objects***: Similar to previous except works on objects.
3. ***Low-Water Mark Integrity Audit Policy***: Introduces the concept of ***corruption level*** to measure possible corruption of data, corruption level set to lowest integrity level of subjects and objects.
4. ***Ring Policy***: Enforces a strict, unmodifiable integrity level for the life of subjects and objects (you can't modify files of "higher" classification and you can't execute programs of a higher classification level).
5. ***Strict Integrity Policy***: Includes the previous principle (ring policy) and adds another stipulation

   A subject can't observe an object with a higher classification level

Comparison of Bell-LaPadula and Biba

From : *CISSP All-in-one Exam Guide*, chapter 5: Security Models and Architecture

- *The Bell-LaPadula model is used to provide confidentiality. The Biba model is used to provide integrity. The Bell-LaPadula and Biba models are informational flow models because they are most concerned about data flowing from one level to another. Bell-LaPadula uses security levels and Biba uses integrity levels.*

Goals of Integrity

From : CISSP All-in-one Exam Guide, chapter 5: Security Models and Architecture

- *There are three main goals of integrity:*

  Prevent unauthorized users from making modifications

  Prevent authorized users from making improper modifications

  Maintain internal and external consistency

  Clark-Wilson addresses each of these goals in its model. Biba only addresses the first goal.

Non-interference Models

Reference: *CISSP All-in-one Exam Guide*, chapter 5: Security Models and Architecture

Multilevel security properties can be expressed in other ways, one being noninterference. This concept is implemented to ensure that any actions that take place at a higher security level do not affect, or interfere, with actions that take place at a lower level.

This type of model does not concern itself with the flow of data, but with what a subject knows about the state of the system.

- *So if an entity at a higher security level performs an action, it cannot change the state for the entity at the lower level.*
- *If a lower-level entity was aware of a certain activity that took place by an entity at a higher level and the state of system changed for this lower-level entity, the entity might be able to deduce too much information about the activities of the higher state, which in turn is a way of leaking information.*
- *Users at a lower security level should not be aware of the commands executed by users at a higher level and should not be affected by those commands in any way.*

Chinese Wall Security Model

Also known as Brewer and Nash Model

This is a commercial confidentiality policy

- Involves controls required to protect against conflicts of interest
- A conflict of interest exists if a person in one company can access information about an individual, product, or services in another company.

Utilizes 3 levels of abstraction:

- ***Objects***: lowest level, includes items such as files which can contain information concerning only one company.
- ***Company groups***: Contains all objects concerning a particular company.
- ***Conflict classes***: clusters of groups of objects for competing companies.

A person can access information only if information for a different group in the same conflict class has never been accessed.

Chinese Wall Security Model

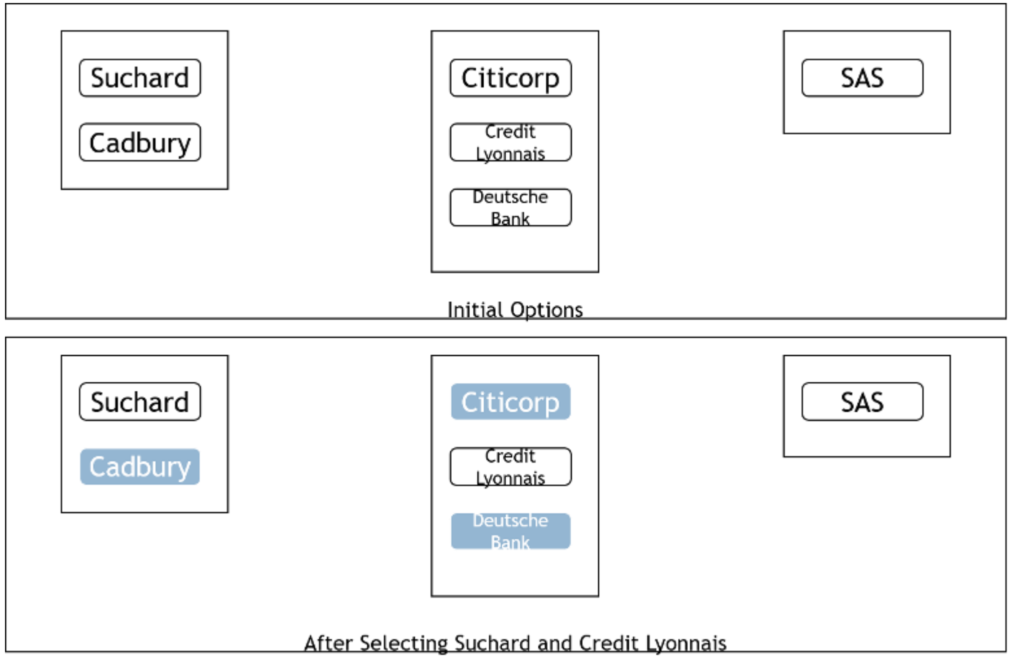


Figure 5-5 from Security in Computing by Pfleeger and Pfleeger

In this diagram we see there are three conflict classes:

- Suchard, Cadbury
- Citicorp, Credit Lyonnais, Deutsche Bank
- SAS

From the second part of the diagram we can see that once a user accesses Suchard, they are no longer able to access Cadbury

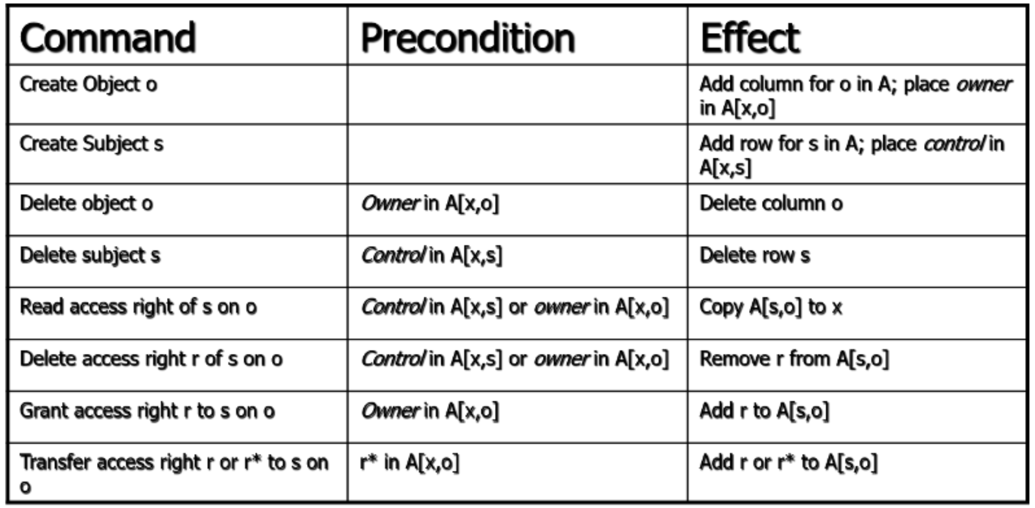
The same is true for Citicorp and Deutsche Bank once a user accesses Credit Lyonnais

This model is preventing any conflict of interest that could occur between those organizations

Graham-Denning Model

Provides rules that can be used to model the access control mechanisms of a protection system

A[s,o] is the access control matrix with a row for each subject and a column for each subject and object



Command	Precondition	Effect
Create Object o		Add column for o in A; place *owner* in A[x,o]
Create Subject s		Add row for s in A; place *control* in A[x,s]
Delete object o	*Owner* in A[x,o]	Delete column o
Delete subject s	*Control* in A[x,s]	Delete row s
Read access right of s on o	*Control* in A[x,s] or *owner* in A[x,o]	Copy A[s,o] to x
Delete access right r of s on o	*Control* in A[x,s] or *owner* in A[x,o]	Remove r from A[s,o]
Grant access right r to s on o	*Owner* in A[x,o]	Add r to A[s,o]
Transfer access right r or r* to s on o	r* in A[x,o]	Add r or r* to A[s,o]

Table 5-2 from Pfleeger and Pfleeger

Harrison-Ruzzo-Ullman Model

The HRU Model is a variation on the Graham-Denning model

- Based on commands with each command consisting of parameters, conditions, and primitive operations.

Primitives are:

- Create subject
- Create object
- Destroy subject
- Destroy object
- Enter right r into A[s,o]
- Delete right r from A[s,o]

Two important results from the HRU model:

- If commands are limited to **one operation each**
  - It is possible to determine if it is possible for a given subject to ever have access to a given object
  - Allows you to determine in advance if a proposed scheme would ever have the possibility of allowing, for example, a User cleared for at most Secret data to access Top Secret info.
- If commands are not limited to only one operation, then it may be an unsolvable problem to determine the above.

Take-Grant Model

Contains only 4 primitive operations:

- Create
- Revoke
- Take
- Grant

Create and revoke are similar to Graham-Denning model.

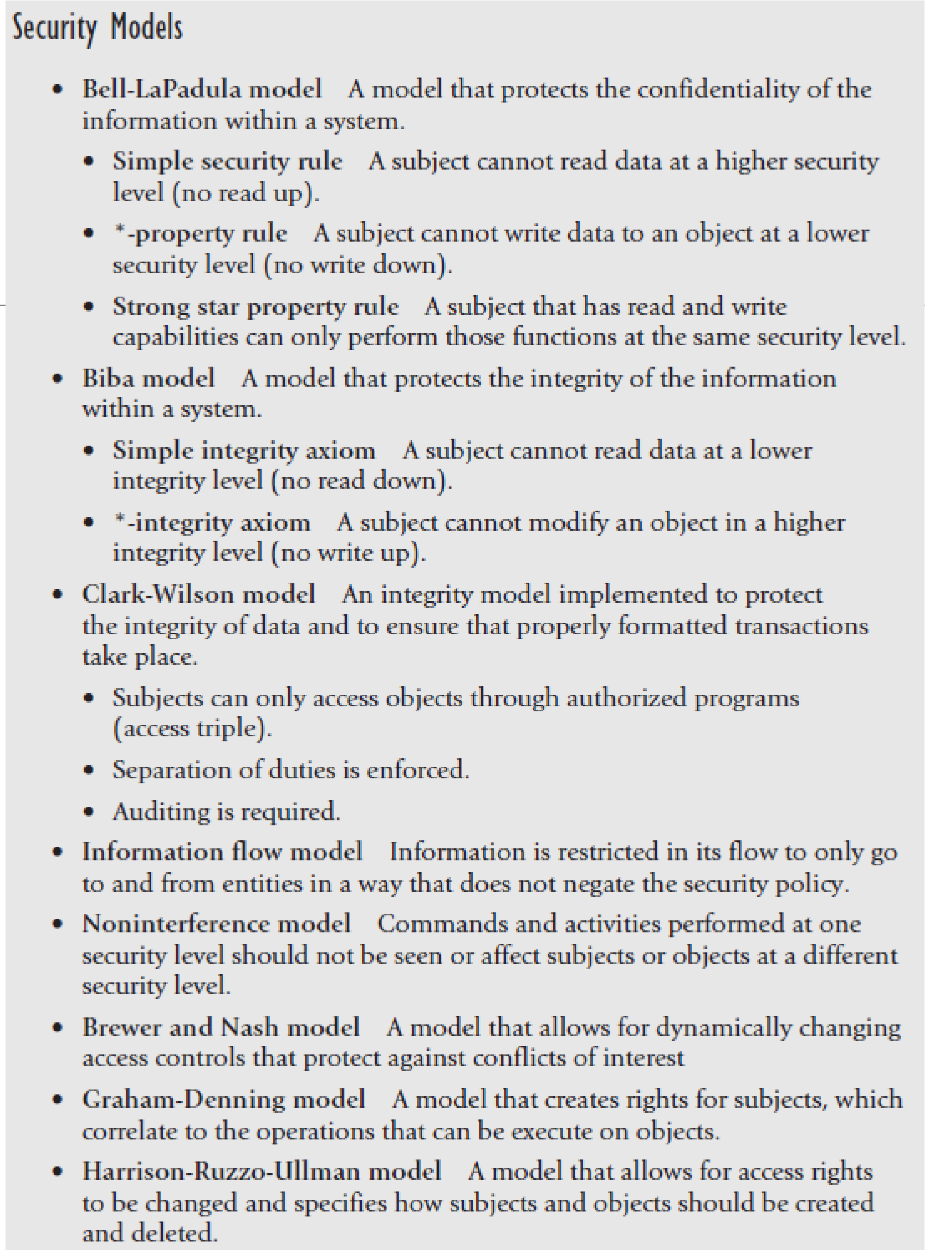
- ***Grant***: Subject s grants to object o access rights r on p. Remember that the set of objects consist of both subjects and objects (e.g. users and files)
- ***Take***: Subject s takes from object o access rights r from p.

In this system it has been shown that certain access rights questions are decidable

- Can we decide whether a given subject can share an object with another subject?
- Can we decide whether a given subject can steal access to an object from another subject?

Security Models Summary

Diagram from : *CISSP All-in-one Exam Guide*, chapter 5: Security Models and Architecture



Security Models

- **Bell-LaPadula model** A model that protects the confidentiality of the information within a system.
  - **Simple security rule** A subject cannot read data at a higher security level (no read up).
  - ***-property rule** A subject cannot write data to an object at a lower security level (no write down).
  - **Strong star property rule** A subject that has read and write capabilities can only perform those functions at the same security level.
- **Biba model** A model that protects the integrity of the information within a system.
  - **Simple integrity axiom** A subject cannot read data at a lower integrity level (no read down).
  - ***-integrity axiom** A subject cannot modify an object in a higher integrity level (no write up).
- **Clark-Wilson model** An integrity model implemented to protect the integrity of data and to ensure that properly formatted transactions take place.
  - Subjects can only access objects through authorized programs (access triple).
  - Separation of duties is enforced.
  - Auditing is required.
- **Information flow model** Information is restricted in its flow to only go to and from entities in a way that does not negate the security policy.
- **Noninterference model** Commands and activities performed at one security level should not be seen or affect subjects or objects at a different security level.
- **Brewer and Nash model** A model that allows for dynamically changing access controls that protect against conflicts of interest
- **Graham-Denning model** A model that creates rights for subjects, which correlate to the operations that can be execute on objects.
- **Harrison-Ruzzo-Ullman model** A model that allows for access rights to be changed and specifies how subjects and objects should be created and deleted.

Security Modes of Operation

Reference: *CISSP All-in-one Exam Guide*, chapter 5: Security Models and Architecture

A system can operate at different types of modes depending on the sensitivity of the data being processed, the clearance level of the users, and what those users are authorized to do. The mode of operation describes the security conditions under which the system actually functions. There are four modes of operations a system can function under.

- *A system is operating in a* ***dedicated security mode*** *if all users have the clearance and formal need-to-know to all data processed within the system. All users have been given formal access approval for all information on the system and have signed nondisclosure agreements pertaining to this information. The system can handle a single classification level of information.*
- *A system is operating in* ***system-high security mode*** *when all users have a security clearance or authorization to access the information but not necessarily a need-to-know for all the information processed on the system. So the difference between the dedicated security mode and the system-high security mode is that in the dedicated security mode, all users have a need-to-know pertaining to all data on the system; in system-high security mode, all users have a need-to-know pertaining to some of the data.*
- *A system is operating in* ***compartmented security mode*** *when all users have the clearance to access all the information processed by the system, but might not have the need-to-know and formal access approval. In compartmented security mode, users are restricted from being able to access some information because they do not need to access it to perform the functions of their jobs and they have not been given formal approval to access this data. In this mode, users can access a segment, or compartment, of data only. The objective is to ensure that the minimum possible number of people learn of information at each level. Compartments are categories of data with limited number of subjects cleared to access data at each level.*
- *A system is operating in* ***multilevel security mode*** *when it permits two or more classification levels of information to be processed at the same time when all the users do not have the clearance or formal approval to access all the information being processed by the system. The Bell-LaPadula model is an example of a multilevel security model because it handles multiple information classifications at a number of different security levels within one system.*

Information Sharing

One definition that has dropped out of regular usage is:

- ***CI/KR: Critical Infrastructure and Key Resources***: An umbrella term referring to the assets of the United States essential to the nation's security, public health and safety, economic vitality, and way of life. Simply put, it's power grids and water filtration plants; national monuments and government facilities; telecommunications and transportation systems; chemical facilities and much more.
  - https://www.dhs.gov/blog/2009/11/19/cikr
- This is still referred to in documentation (like HSPD-7) but has usually been shortened to just "critical infrastructure"

To assist with the protection of critical infrastructure, the U.S. established a national cybersecurity information sharing ecosystem

Information Sharing

From CISA:

- *Information sharing is essential to the protection of critical infrastructure and to furthering cybersecurity for the nation. As the lead federal department for the protection of critical infrastructure and the furthering of cybersecurity, the Cybersecurity and Infrastructure Agency (CISA) has developed and implemented numerous information sharing programs. Through these programs, CISA develops partnerships and shares substantive information with the private sector, which owns and operates the majority of the nation's critical infrastructure. CISA also shares information with state, local, tribal, and territorial governments and with international partners, as cybersecurity threat actors are not constrained by geographic boundaries.*
- https://www.cisa.gov/information-sharing-and-awareness

Information Sharing

To assist with information sharing, a public-private partnership was created

- These are called Information Sharing and Analysis Centers (ISACs)

ISACs:

- *Sector-specific Information Sharing and Analysis Centers (ISACs) are non-profit, member-driven organizations formed by critical infrastructure owners and operators to share information between government and industry. While CISA Central works in close coordination with all of the ISACs, a few critical infrastructure sectors maintain a consistent presence within CISA Central.*
- https://www.cisa.gov/information-sharing-and-awareness

ISACs specifically mentioned by CISA:

- Multi State Information Sharing and Analysis Center (MS-ISAC)
- ISAC for state, local, tribal, and territorial (SLTT) governments
- Financial Services ISAC (FS-ISAC)
- Aviation ISAC (A-ISAC)

Information Sharing

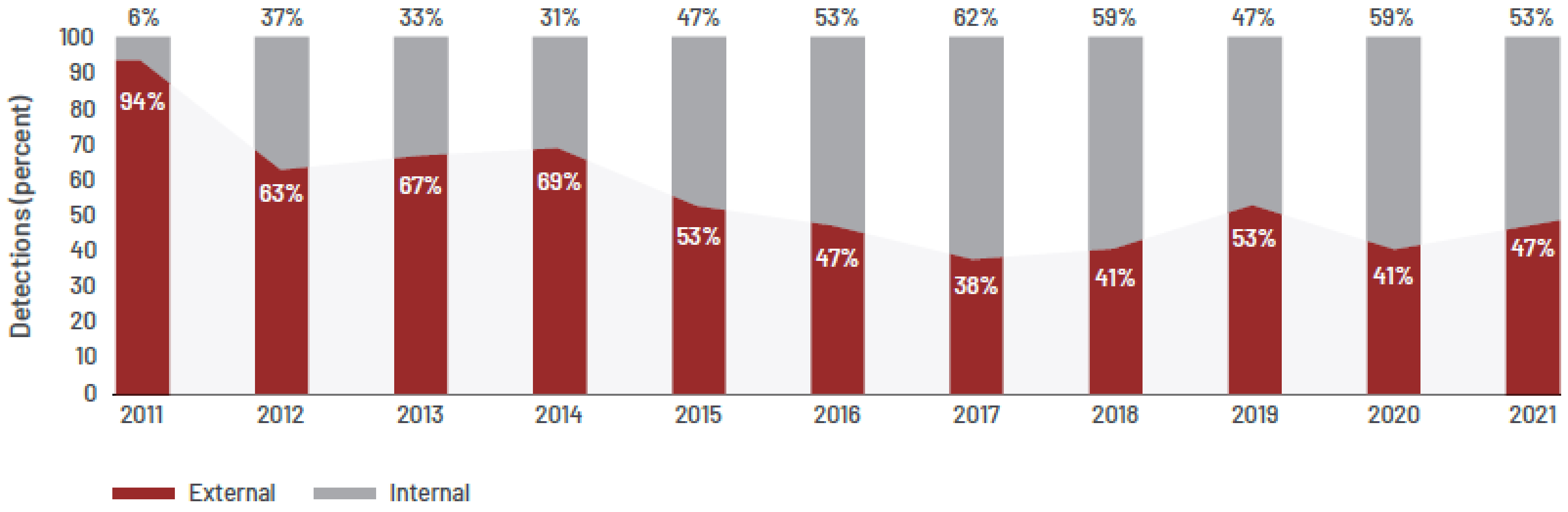
One important reason for information sharing is the large number of incidents detected by external parties

In addition, if an attacker compromised one financial organization, they can notify other banks of indicators of compromise (IoCs), lessons learned, and any other information about the attackers

- This allows the other banks to update their defenses to keep the attacker out
- Find the attacker quickly if they are already there
- Immediately respond effectively

Information Sharing

Detection by Source, 2011-2021



In APAC and EMEA, the majority of intrusions in 2021 were identified externally—a reversal of what was observed in 2020. The detection by source for Americas held steady with most intrusions continuing to be detected internally.

From: M-Trends 2022 – Mandiant Special Report

Information Sharing and Analysis Organizations (ISAOs)

Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, directs DHS to:

- *Develop a more efficient means for granting clearances to private sector individuals who are members of an ISAO via a designated critical infrastructure protection program;*
- *Engage in continuous, collaborative, and inclusive coordination with ISAOs via CISA Central, which coordinates cybersecurity information sharing and analysis amongst the Federal Government and private sector partners; and*
- *Select, through an open and competitive process, a non-governmental organization to serve as the ISAO Standards Organization. This ISAO Standards Organization will identify a set of voluntary standards or guidelines for the creation and functioning of ISAOs.*

The ISAO Standards Organization was formed in October 2015:

- *The Awardee for the ISAO Standards Organization Cooperative Agreement is the University of Texas at San Antonio (UTSA) with support from the Logistics Management Institute (LMI) and the retail Cyber Intelligence Sharing Center (R-CISC).*
- https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos

ISAC/ISAO Sharing Models

Information Sharing and Analysis Center (ISAC): The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government.

- From: PRESIDENTIAL DECISION DIRECTIVE/NSC-63 May 1998

Information Sharing and Analysis Organizations (ISAO): The Secretary of Homeland Security (Secretary) shall strongly encourage the development and formation of Information Sharing and Analysis Organizations (ISAOs) for the purposes of: (I) gathering and analyzing cybersecurity information; (ii) distributing cybersecurity information; and (iii) collaborating with members or customers, other ISAOs, or other private sector, Federal, State, local, tribal, territorial, and international entities to respond to cyber threats and mitigate cyber risk.

- From: EXECUTIVE ORDER February 2015

Motivation For Inclusion of ISAOs

ISAC approach originally focused on critical infrastructure sectors

- Simple first step
- In-line with risk management prioritization efforts at the time

There are some drawbacks:

- ISACs are Mainly Sector Based
- Not all companies fit neatly into any sector
- No Baseline Membership Standards across ISACs
- Dependent on Industry for Sub-sector Outreach
- Few options for "Less Cyber Capable Companies

Some types of organizations don’t fit well into the ISAC sectors

For example:

- HVAC Vendors
- Law Firms
- Mega Churches
- Electronic Crime Investigators
- National Assoc. Of MBAs, National Associations of Accountants
- Construction Companies
- Small town businesses wanting to associate with each other / not sector based
- Small Bio-tech Laboratories

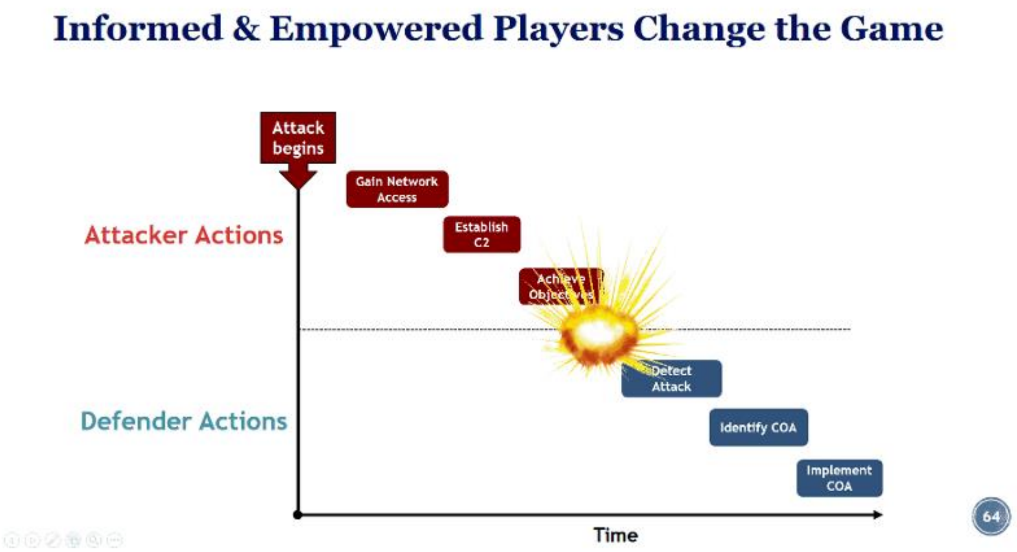
Motivation For Inclusion of ISAOs

The cyber threat is one of the most serious economic and national security challenges we face as a Nation.

- President Barack Obama, March 2010

Mission: Improve the Nation's cybersecurity posture by identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents and best practices.

Vision: A more secure and resilient Nation that is connected, informed and empowered.



Informed & Empowered Players Change the Game

ISAO Information Sharing

The types of information an ISAO might share include:

- Security relevant incident data (in real-time is the ultimate goal). Analysis that drives actions or improves situational awareness
- Cyber Threat Indicators
- Vulnerabilities and/or exploits that could impact the ISAO members
- Defensive Measures
- Best practices
- Security training / awareness
- Trends or new technology that might impact the members of the ISAO

The goals of the ISAO and the needs of its members will determine what information is shared, and what organization it is shared with

- Could share with other ISAOs, government
- Could assist with incident response, or SOC operations

ISAO

The ISAOs mean that, instead of a few dozen sector ISACs, you can have 100s of potential sharing entities

- Some can be large companies – like auto manufactures
- Some can be small organizations, but a large number of entities – like private schools

Some example types:

- Commercial or Sector ISAO
  - Shoe Retailers ISAO
  - U.S. Catholic Churches ISAO
- "Tiered" ISAOs for a given industry
  - National Association of Mariachi Bands ISAO
  - SW U.S. Mariachi Bands ISAO
  - Mariachi Bands of South Texas ISAO
- Geographically based ISAOs
  - State of Texas ISAO
  - City of San Antonio ISAO
- ISAO Service Providers
  - Providers of services to ISAOs
  - Providers of services to individual organizations not part of an ISAO
- ISAOs for a limited event
  - (e.g. Super Bowl, Olympics)

ISAO – Interesting Possibilities

Credit Union ISAO

- There is already an ISAC which they could be a member of (and in many cases, are already a member of)

South Texas Mariachi Band ISAO

- Do these folks really need to be part of an information sharing organization?
  - Yes: They could have websites or social media pages
  - Yes: If they collect credit card information or personal (contact) information?
  - Yes: They use computers for bookings, and finances
- Then they might benefit from coming together to discuss cyber security in their environment

Cannabis Growers of Oregon

- May not want to share with government agencies

Energizing an Information Sharing Ecosystem

ISACs have helped dramatically improve the cybersecurity of critical infrastructures

Helps build a broader ecosystem that meets the needs of everyone else

Various types of ISAOs

- Industry- and Sector-Based
- Geographically-Based
- Event-Based
- Informal Group-Based

Private- and public-sector entities

For-profit and not-for-profit organizations

International entities

A decentralized network of networks built on trusted sharing

Flexible, scalable, and ***aligned with organizational self-interest***

Forming an ISAO

An ISAO is for anybody who wants to be part of the ecosystem in order to be more informed about cyber security issues

- States (some states have already formed an info sharing entity)
- Communities within the states
- Industry sectors

You may elect to be part of multiple ISAOs

- Geographic and functional
- Tiered ISAOs (national, regional, local)

You may contract to have a service provider provide some/most services

The services offered by an ISAO will vary and will depend on the goal of the ISAO and what its members want:

- Sharing across ISAOs
- Sharing with government
- Pooling resources for incident response
- Creating a 24/7 SOC

Final Thoughts on ISAOs

ISAOs are NOT just Mini-ISACs.

- They do NOT need to provide the same services or be as robust

ISAOs do NOT need to share with the government

- There may be benefits to doing so, but what is shared will be up to the members of the ISAO

ISAOs do NOT need to share with other ISAOs

- There may be benefits in sharing some information, but what an ISAO will share will be up to its members

ISAOs do NOT need a 24/7 SOC, have incident response capability, or perform extensive threat analysis

- They can simply share information that is relevant to your members
- There is a benefit in having all of these, but the ability to offer these services is up to the members

ISAOs do NOT need to charge a membership fee, this is up to the members

- An income source may allow providing enhanced services for the members but this is NOT required to be an ISAO

What an ISAO will do will depend on its members and the charter it develops

Building a Common Body of Knowledge

Developing a CBOK was a task given to UTSA/CIAS

- To build the body of knowledge for the community through the development of standards, guidelines, and best practices

Initial guidance was published 30 September 2016

- ISAO 100-1, Introduction to ISAOs
- ISAO 100-2, Guidelines for Establishing an ISAO
- ISAO 300-1, Introduction to Information Sharing
- ISAO 600-2, U.S. Government Relations, Programs, and Services

Now the foundational documents are in place for implementation

Can broaden the focus to growing the ecosystem and improving capability

ISAO

ISAO 100-1:
Introduction to Information Sharing and Analysis Organizations (ISAOs)
v1.01

October 14, 2016

ISAO

ISAO 100-2:
Guidelines for Establishing an Information Sharing and Analysis Organization (ISAO)
v1.01

October 14, 2016

ISAO

ISAO 300-1:
Introduction to Information Sharing
v1.01

October 14, 2016

ISAO

ISAO 600-2:
U.S. Government Relations, Programs, and Services
v1.01

October 14, 2016

Other ISAO Documents

ISAO 100 Series: ISAO Creation & Operation

- ISAO 100-1: Introduction to ISAOs
- ISAO 100-2: Guidelines for Establishing an ISAO
- ISAO 100-3: Guidelines for Operating an ISAO
- Tax-Exempt Structuring: 501(c)3 or 501(c)6?

ISAO 300 Series: Information Sharing

- ISAO 300-1: Intro to Information Sharing
- ISAO 300-2: Automated Information Sharing

ISAO 500 Series: ISAO Analysis

- ISAO 500-1: Introduction to Analysis
- ISAO 500-2: Analytical Methods

ISAO 700 Series: Global Information Sharing

- ISAO 700-1: Introduction to Global Sharing
- ISAO 700-2: International Issues

ISAO 200 Series: ISAO Capabilities & Services

- ISAO 200-1: Intro to ISAO Capes & Services
- ISAO 200-2: ISAO Capabilities
- ISAO 200-3: ISAO Services

ISAO 400 Series: Privacy and Security

- ISAO 400-1: Practices to Advance Consumer Privacy
- ISAO 400-2: Privacy Guidelines
- ISAO 400-3: Security Guidelines

ISAO 600 Series: Government Relations

- ISAO 600-1: The Role of Government
- ISAO 600-2: US Government Relations, Programs & Services
- ISAO 600-3: State, Local & Tribal Issues

ISAO 800 Series: Legal Issues

- ISAO 800-1: General Counsel Considerations

Information Sharing Resource Library

The ISAO Library can be found here:

- https://www.isao.org/

The list of information sharing groups can be found here:

- https://www.isao.org/information-sharing-groups/
- The groups can be filter off of types of organization:
  - Geographic
  - Industry/Sector
  - Other
  - Special Interest
- It can also filter off of Location and Area of Interest

Next Steps

The issues the ISAO SO is facing:

Growth is good, but organized growth is better

- We need to promote effective collaboration among sectors and regions

All-source intelligence model

Action items feed CBK and conferences

Identify how to advance methods and technologies

- Community Body of Knowledge
- Common Marketplace
- Public Forum for Exchanging Ideas

Goal: A decentralized network of networks built on trusted sharing