Interdependency Analysis

Richard K. McAllister
Sparta Incorporated, Columbia MD.
(410) 381-9400 ext. 231
rmcall@sparta.com

James L. Coyle
Averstar Incorporated, Greenbelt MD
(301) 982-5414 ext. 318
jcoyle@averstar.com

Abstract

In this paper, "Interdependency Analysis" is defined as a technique for evaluating security service strengths of combinations of security mechanisms employed to protect information. Such a technique can provide a valuable tool for assessing the security architectures and implementations of information systems. The technique can also help security administrators better manage security policies and mechanisms.

Keywords

security mechanisms, security evaluations, security architecture, security services, information systems security engineering (ISSE)

1. SCOPE AND FIELD OF APPLICATION

The field of Information Systems Security Engineering (ISSE) needs better methods or techniques for evaluating the security services provided by networks of information systems. Past and present evaluation efforts such as the U. S. Trusted Computer Security Evaluation Criteria [TCSEC] and the Common Criteria [CC] have not (yet) satisfied the needs of system engineers who must select and integrate components and perform security evaluations as the design progresses.

Component evaluation methods vary depending on the technologies of the types of security mechanisms. Indeed, there are different methods used to evaluate locked doors, safes, and surveillance mechanisms. The technique defined here can take advantage of any existing or developing component evaluation method that provides metrics for the strength of the security services provided, including trusted product evaluations.   It can be used to combine the results of those methods into evaluations of large, complex, heterogeneous systems of components.

We define, "Interdependency Analysis" as a technique for evaluating security service strengths of combinations of security mechanisms employed to protect information. Such a technique can provide a valuable tool for assessing the security architectures and implementations of information systems. The technique can also help security administrators better manage security policies and mechanisms.

2. OVERVIEW

In this effort we endeavored to derive simple models and rules for dealing with what we knew to be a complex analytical problem. While there is much to be done in testing, evaluating, and practicing what we have concluded, we have produced what we believe to be the fundamentals of a practical method for system security evaluation.

We actually identified two types of interdependencies. The first is “Security Mechanism Interdependency” and the second is “Security Service Interdependency”. Under security mechanism interdependency we conclude there is a need for all security mechanisms to be **protected** and **supported**. Under security service interdependency we present an **Adversary→Security service→Target** model and **two cases** for combining security mechanisms to derive the effective security service strengths. Next, we integrate the two concepts by adding support and protection mechanisms to the adversary→security service→target model.

This approach would be straight-forward except for the dependence of some internal security mechanisms on the underlying architectures of individual components that contain them. This “weak protection” situation is described and resolved with the interdependency models. Finally, we show examples of combined systems by reducing them into simpler equivalents.

3. SECURITY MECHANISMS INTERDEPENDENCY MODEL

Figure 1 illustrates the fundamental interdependency model for mechanisms.

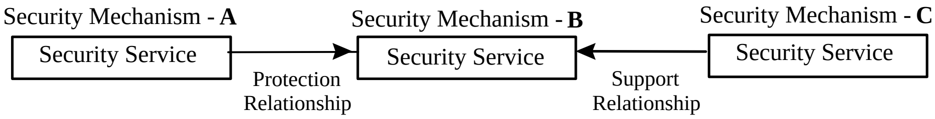


Figure 1. The Mechanism Interdependency Model

We identified two types of mechanism dependencies; protection and support. Security Mechanism A protects Security Mechanism B, while Security Mechanism C provides support. In our model, mechanism A is some combination of physical security and logical security barring direct access to B (a lock and access code). Mechanism C is the control needed by a mechanism B to enable it to provide its service. For example, if mechanism B was providing an access control decision and/or enforcement services it could be dependent upon the support of mechanism C for an authentication service.

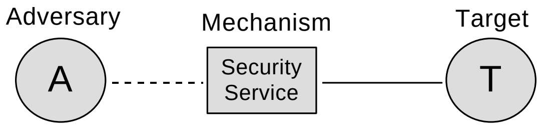
Therefore, the method for ascertaining the strength of the security service provided by mechanism B in Figure 1 must include an evaluation of the protection from mechanism A and the support from mechanism C. This model of mechanism interdependency is iterative for all security mechanisms in a security architecture. The protection mechanism A in Figure 1 also needs to be supported and protected. Furthermore, the support mechanism C in Figure 1 needs to be supported and protected. This creates a relationship of interdependency that extends into a complex molecular-like structure with support and protection threads interconnecting security mechanisms. We have some expectation from analysis that the threads rapidly lead to diminishing contributions to support and protection whereupon additions will be judged to be insignificant, e.g. paint on a steel door.

4. THE SECURITY SERVICE INTERDEPENDENCY MODEL

The information objects that are the targets of adversaries are the logical starting points for the analysis of security services. Guided by security service requirements documented in a security policy, an evaluation of the security services provided by all mechanisms between targets and adversaries can be performed.

Security mechanisms are employed to provide the security services of authentication, access control, confidentiality, integrity, availability, and non-repudiation. There are many types of mechanisms implemented in physical, administrative, personnel, software, and hardware forms. All of these mechanisms are necessary to compose secure information systems. We also consider "security management" to be a security service that is provided by security mechanisms such as users, security administrators, and applications developed for that purpose.

Security services protect the target from the objectives of the adversary, as shown in Figure 2. The ability of a mechanism to resist an attack we call the "service strength" (against that attack) of the mechanism. The ability of an attack to render the mechanism ineffective or to degrade its protection we call a "vulnerability". Note that vulnerability thus defined is an inherent characteristic of the mechanism that is independent of any characteristic of an adversary.



Adversary Objective	**Security Service**	**Target**
False authorization	Authentification	Authentication data/decision
Unauthorized access	Access control	Any data/system component
Disclosure	Confidentiality	Any data/process
Modification/damage	Integrity	Any data/process/component
Denial of service/use	Availability	Any data/process/component
Spoofing/Denial	Non-repudiation	Proof of origin/delivery data
Unauthorized control	Security management	Security management data

Figure 2. The Adversary → Security Services → Target Model

4.1 Security Mechanisms and Security Engineering Assertions

a) Security mechanisms never stand alone in providing security services.
b) Security mechanisms are often capable of contributing to more than one security service.
c) The first test for security mechanisms is for compatibility. Interactions should not cause degradation of service.
d) The strength of a security service depends on the contributions and configurations of all the mechanisms that provide the service.
e) The service strength of a mechanism is type and technology unique. Locked doors and encryption devices can be used for access control but they have different evaluation methods and criteria.
f) Information Systems Security Engineers (ISSEs) must prepare architectural assertions based on the ability of mechanisms in combination to meet the security service requirements.

g) ISSEs must be alert to the danger of assuming that more layers of protection increase the service strength. The total protection will be reduced to the weakest link.
h) The analysis of combined security mechanisms must include the effect of individual, protecting, and supporting mechanism failures.
i) Product vendors must provide the first assertion of security service capabilities provided by the security mechanisms included in their products.

4.2 Two Target Protection Path Configurations

The following diagrams show two different protection path configurations. Both show a combination of mechanisms providing a given security service and are illustrated together in Figure 3.

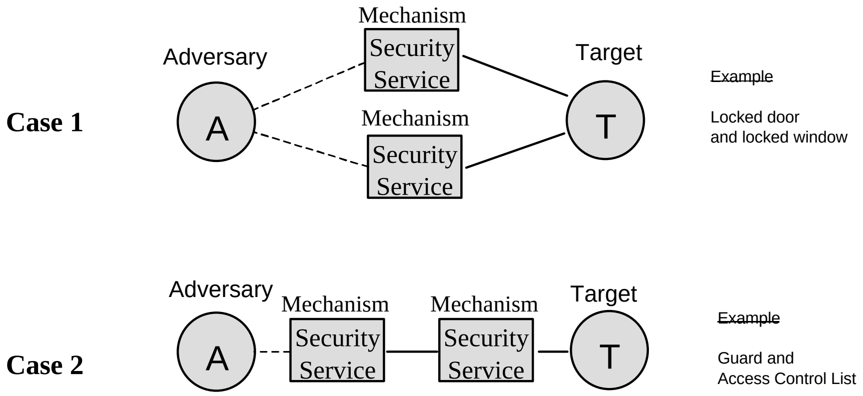


Figure 3. Parallel and Serial Path Cases

Case 1 shows two (or more) security mechanisms providing a security service for a target along separate paths (the parallel case); or as shown in Case 2, they can provide the service along a common path (the serial case).

In Case 1 each mechanism provides the total service so the failure of either mechanism results in a loss of service. An example of Case 1 is a structure with a locked front door and a locked window.

In Case 2 each mechanism provides part of the service and the failure of either mechanism reduces the service to that provided by the remaining mechanism. An example of Case 2 is a guard at the entrance of a building and the access control list in a computer.

It is important to understand that all security mechanisms are analyzed as providing the same security service to the target. Thus, combining the mechanisms in Case 1 results in the weakest mechanism as the effective service strength. In the example, either the door or the window is the weaker mechanism. Combining the mechanisms in Case 2 is accomplished by the addition of the mechanism service strengths if they are independent, i.e. not protecting or supporting.

4.3 The Complete Interdependency Model

Figure 4. combines protection and support mechanisms with the Adversary→Security Service→Target model forming the complete interdependency model. The example of a support mechanism is security control. The security service provided by the security control mechanism is security management. Security management service includes initializing, monitoring, keying, enabling, disabling, function selection, SMIB management etc. The security control mechanism example is a trusted and protected portion of the operating system or a reference monitor [GASSER].

Protection mechanisms are things such as the locked office protecting the entire computer system components or anti-tamper protection for a single computer component.

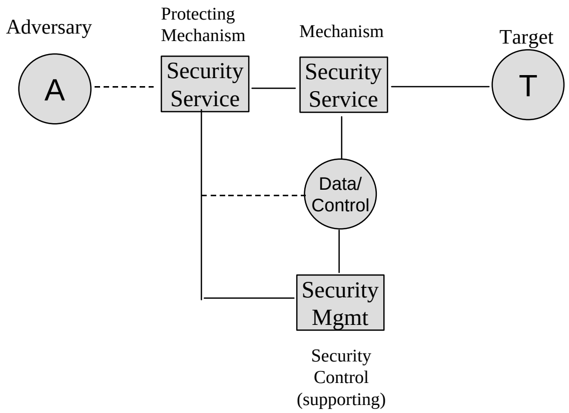


Figure 4. Interdependency Model

Figure 4. illustrates the protection of valid access paths to both the target protecting mechanism and the supporting security management. Invalid access paths are shown as dashed lines. The adversary cannot get to the target without getting through both the security service protection mechanism and the target protection mechanism. However, by attacking the security management mechanism, the adversary need only get through a single protection mechanism. Further, if the security management mechanism is weaker than the mechanism directly protecting the target, then the adversary will logically attack the security management mechanism to weaken or disable the target protecting mechanism. Figure 4 also shows the protection of an invalid path (dashed line) to the data/control. Without protection against the invalid path attack, the modification of the data or control information is probably the easiest attack. Ultimately, analysis of this model will show that the composite service strength protecting the target is only “dependent” upon or limited to the strength of the protecting mechanism or mechanisms.

4.4 Logical And Physical Access Control

Figure 5. illustrates an office environment which has both a physical access control mechanism and a logical access control mechanism. Logical access is permitted to the system via telecommunications channels from outside the distributed office environment. Physical access is permitted to the system by satisfying physical or administrative access control mechanisms.

Both logical and physical access controls satisfy the requirement for “no unauthorized access to the system”. The system normally applies a second access control mechanism which limits users to the standard user interface devices. Inside the system, another mechanism controls access to the target. Where required, Identification and Authorization (I&A) service mechanisms support the access control mechanisms.

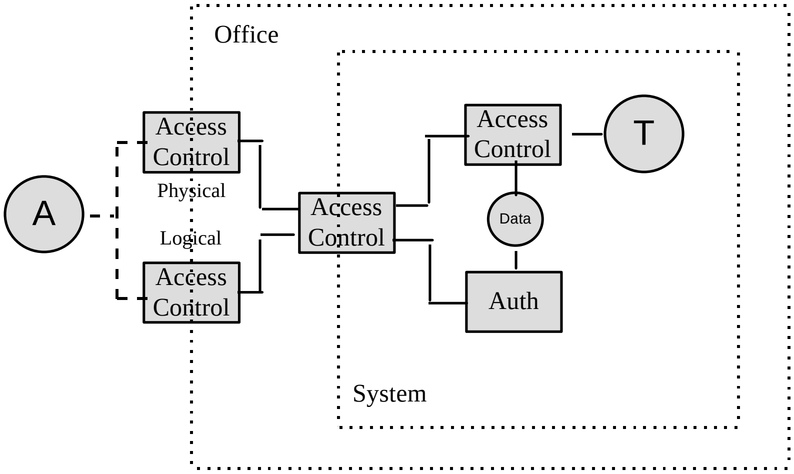


Figure 5. Logical and Physical Access - Mechanisms Protecting Mechanisms

The requirement for I&A is present whenever there is a policy separating authorized and unauthorized users.

5. WEAK PROTECTION PROBLEM

Figure 6. illustrates a situation where the access control service to the target could be lost if the first access control mechanism fails. This could happen because there may be an alternate path around the second access control mechanism. If true, the strength of the first access control mechanism is the total strength of the access control service.

For example, Oracle database privilege control manages access to its files. However it ultimately relies on the underlying operating system to control access to the file system. Oracle can only control access to information it manages, but this same information is part of the file system as well. Therefore, an adversary does not need to defeat the Oracle database software to accomplish their attack objective. They can simply get to the targeted information via the file system manager.

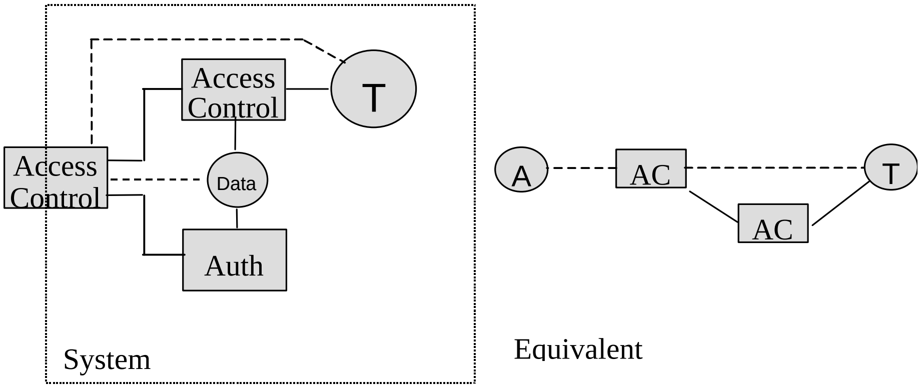


Figure 6. Weak Protection Example

5.1 Architectural Assurance

Figure 7, illustrates the alternative attack paths an adversary can take if the first protection mechanism can be satisfied or defeated.

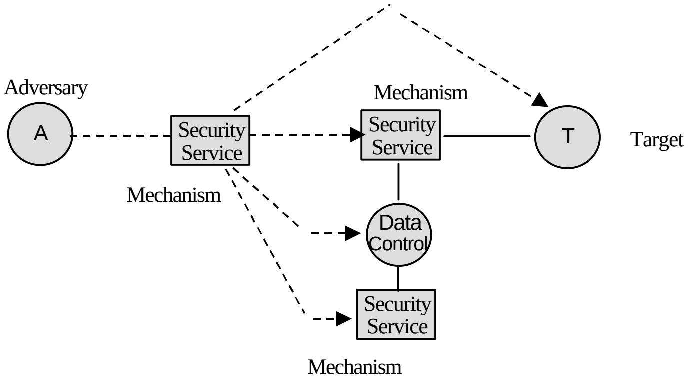


Figure 7. Attack Paths

The protecting mechanism on the far left is protecting everything.
In this case, the system architecture must eliminate the weak protection and close the attack paths. In classic computer security, systems are evaluated according to the sets of design features that give degrees of "assurance" that internal policies are being enforced. The principal assurance is through controlling access to information and security control software. In Figure 8. , the system access control closes all invalid paths to internal software mechanisms and data and all valid paths are controlled by the implemented security mechanisms.

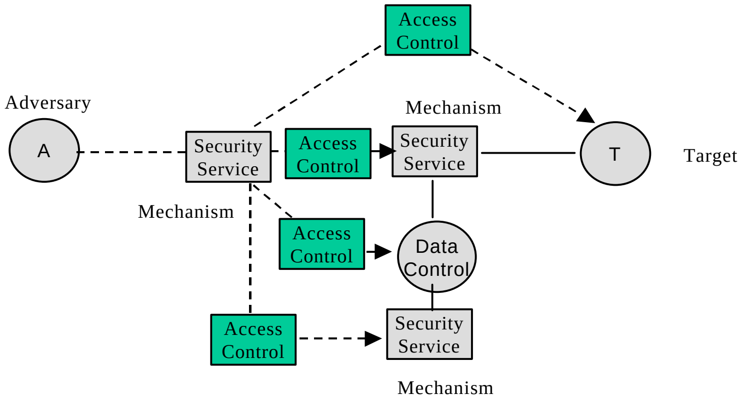


Figure 8. Architectural Assurance.

The value of this system access control or "assurance" is the limiting factor for any security service strength that the component can provide.

Perhaps the better way to view mechanisms and assurances is to consider the underlying component architectural assurance as a part of each security service mechanism internal to the component. This view eliminates the difficulty of a software mechanism having no service strength unless protected by a security component. For the software mechanism, the protection mechanism is not independent of the security service mechanism; it is part of it.

6. SECURITY REQUIREMENTS & METRICS

We expressed security requirements in terms of “security service strengths”. We created coarse security strength metrics of Strong, Moderate, Minimum, and None. These broad metrics are provided so that information owners can easily use them to define their general security service strength requirements. The detailed evaluation of security products, and more particularly of the security mechanisms they contain, needs to be provided by specialists in various security mechanism fields. Given that expert data, a security metric with a separate scale of strength for each particular type of security mechanism can be developed (a much more granular measurement of strength than our coarse metrics). Regardless of the granularity of the expert scales, it is always possible to map each type of evaluated product mechanism to our four coarse strength metrics as shown in Figure 9.

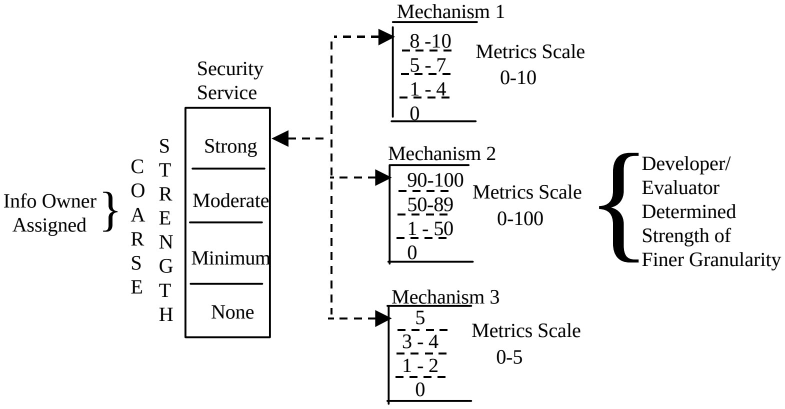


Figure 9. Requirements and Metrics

Scale mapping follows a process. First, the information owner establishes the required strength (strong, moderate, minimum, none) for each security service in each information domain. Second, the rating systems for each class and type of mechanism must be obtained (each may be different based on the technology employed). There need be no direct numerical value relationship between the service requirement strength and the mechanism ratings. However, the security architect must make mechanism selections based on the cost, availability, compatibility, combined effectiveness, and customer priorities. Finally, the security architect maps the security service requirement for each mechanism to be placed within the information system architecture to one or more of the security mechanism scales. Thus, the choice of mechanisms, their compatibility, and their combined effectiveness is assessed through this “Interdependency Analysis”.

This is not a paper about mechanism strengths. It is an approach toward complexity reduction. There is much research to follow in determining how to add strengths or determine the weaker of similar and dissimilar mechanisms. The approach does suggest a degree of subjectivity on the part of an ISSE when mapping combined mechanisms to service requirements. This is unavoidable. To allay the subjectivity of relating service requirement strength to mechanism effectiveness the information owner can place monetary values on the potential information loss. For example, a cryptographic mechanism used to protect government Top Secret information is probably not the right choice for protecting the most important information of a $1M business.

7. SYSTEM EXAMPLES

7.1 Access Control Thread Example

The adversary has the choice to attack the mechanisms that directly protect the target (T) or those that support those mechanisms. Figure 10. depicts a common set of service interdependent mechanisms and possible attack paths.

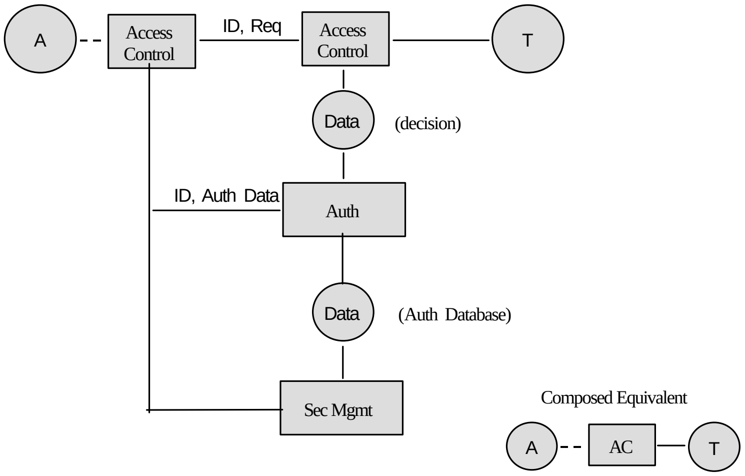


Figure 10. Access Control Thread Example

Assuming that the first AC mechanism is not protecting the other mechanisms, the access control to T will fail if both AC mechanisms fail in providing their service. The composition is accomplished by adding the service strengths of the two AC mechanisms. However, if the authentication service or the security management supporting services is weaker, the AC service is reduced to the weaker of those services. This must be accomplished before adding the two AC services

A distinction should be made here between service failure and mechanism failure. The failure of the authentication mechanism results in a failure to provide the service of access control to T, but the other mechanisms are unaffected and should be viewed as working correctly.

Note, there is a need here for user security context. The ID+Request from a user must be bound to the [ID+Auth Data] sent to the I&A mechanism.   What is not shown (for simplicity) is the Security Management control of the AC mechanisms whereby the user is placed into a security context which confines the users activities and data to at least a logical partition of system resources.

7.2 Crypto Thread Example

Figure 11. illustrates a typical cryptographic mechanism thread to encrypt and decrypt data. The adversary must be prevented from getting to the cryptographic function, and the key management mechanism which support for the cryptographic function. The access control mechanism is the protecting mechanism that prevents the adversary from getting to either of the other mechanisms it protects. This then is just an example of the interdependency model of Figure 4 in which the services are specifically chosen.

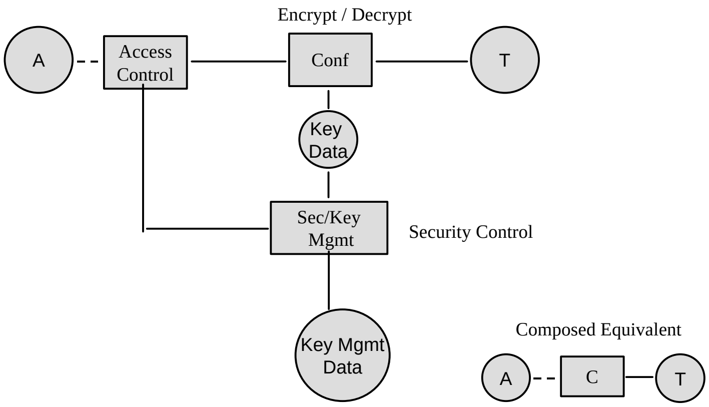


Figure 11. Cryptographic Mechanism Thread

7.3 Composed Services Examples

This example shows both a logical and physical entry/exit gate to the computer system in an office environment.

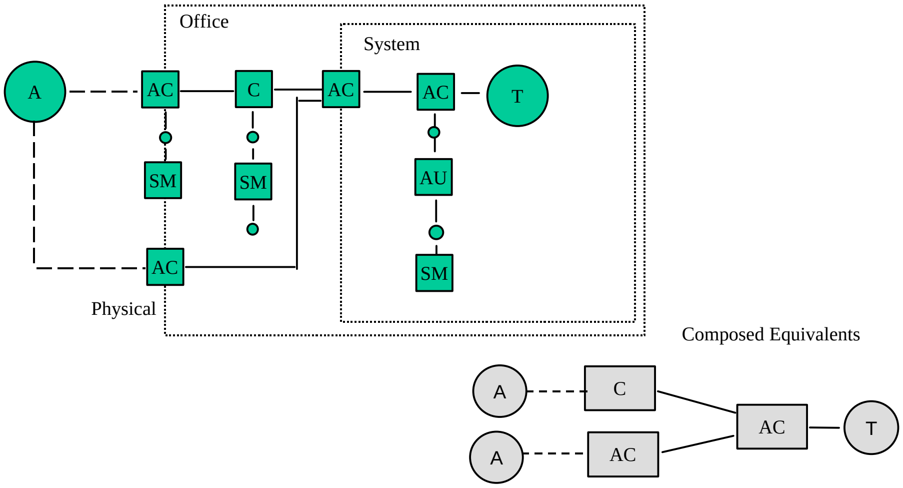


Figure 12. Composed Services Example

The example takes the examples from Figures 10 and 11 and combines the two. The purpose is to illustrate the process of composing and decomposing more complex security systems. The confidentiality mechanism also serves an access control function. The confidentiality path permits authorized remote users to achieve access equivalent to in-office users. The physical access control path is a hurdle for both adversaries and authorized users.

7.4 Two System Example

Figure 13. illustrates the approach to compose two connected systems.

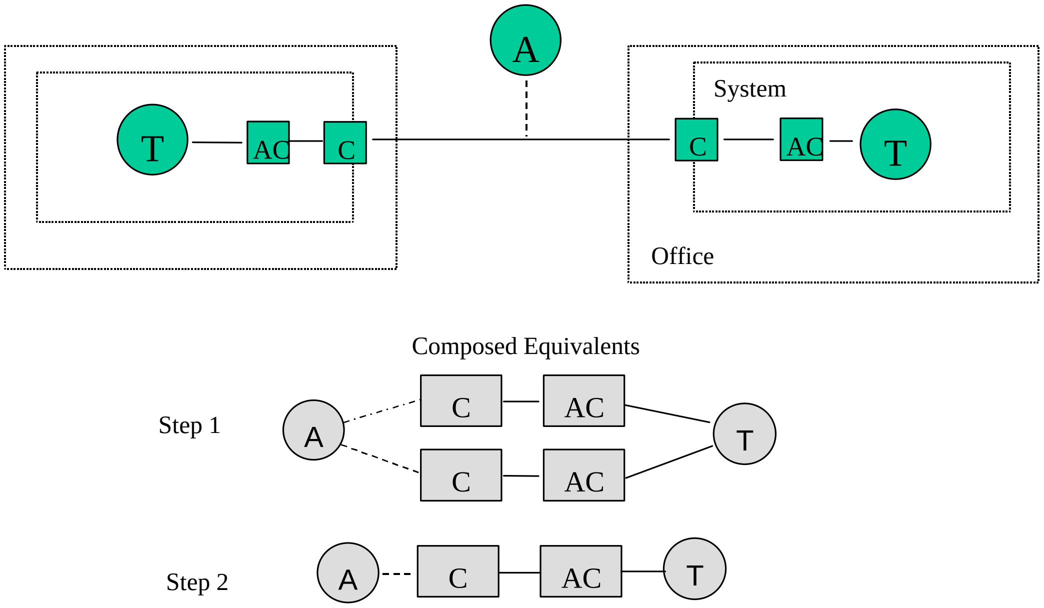


Figure 13. Two System Example

The first simplification is to consider that the two targets are really the same target since the same information may validly be located in both systems. This permits the folding of two systems into the composite of step 1. There are now two parallel paths to the target. In step 2 we choose the weaker of the two paths as the effective protection path. The final combination of the two service mechanisms relies upon the question of which service is being evaluated, confidentiality or access control.

8. CONCLUSIONS

We conclude:

- There are mechanism interdependencies and security service interdependencies.
- All mechanisms require or depend upon protection and support.
- Support includes security management services and other services (e.g., AC services are dependent on an authentication service).
- Security services depend upon the combinations of security mechanisms along parallel and serial paths between adversaries and targets.
- Mechanisms that independently protect other mechanisms can add to the effective security service.

- Support mechanisms and their data/control information must not be more vulnerable (weaker) than the supported mechanisms.
- When composing security architectures, the selection of appropriate mechanisms is driven by the service(s) each provides and their strength of service.
- The strength of service is defined by the security requirements (information protection policies) associated with a given component of the architecture within the information domain.

9. REFERENCES

CC: Common Criteria for Information Technology Security Evaluation
GASSER: Building A Secure Computer System, Morrie Gasser, Van Nostrand Reinhold, 1988
TCSEC: Trusted Computer Security Evaluation Criteria, US National Computer Security Center and the “The Rainbow Series”