Extending the McCumber Cube to Model Network Defense

By Sean M. Price – ISSA member Northern Virginia, USA chapter

This article proposes an extension to the McCumber Cube information security model to determine the best countermeasures to achieve a desired security goal.

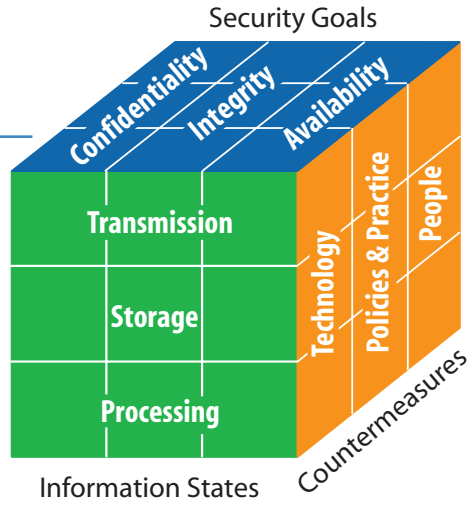

Figure 2 – McCumber Cube

Confidentiality, integrity, and availability are the security services of a system. In other words they are the security goals of system defense, intangible attributes[1] providing assurances for the information protected. Each service is realized when the appropriate countermeasures for a given information state are in place. But, it is not enough to select countermeasures ad hoc. Countermeasures should be selected to defend a system and its information against specific types of attacks. When attacks against particular information states are considered, the necessary countermeasures can be selected to achieve the desired security service or goal. This article proposes an extension to the McCumber Cube information security model as a way for the security practitioner to consider the best countermeasures to achieve the desired security goal.

Security models

Models are useful tools to help understand complex topics. A well-developed model can often be represented graphically, allowing a deeper understanding of the relationships of the components that make the whole. A formal security model is broadly applicable and rigorously developed using formal methods.[2] In contrast, an informal model is considered lacking one or both of these qualities. There are a variety of informal models in the information security world which are regularly used by security practitioners to understand basic information and concepts.

One such informal model is the generally accepted risk assessment framework. This model is used to assess risk by estimating asset values, vulnerabilities, threats with their likelihood of exploiting a vulnerability, and losses. Figure 1 illustrates this model. Note that this commonly used model

Figure 1 – Risk Assessment Model

requires a substantial amount of estimating on the part of the risk assessment participants. This is problematic when reliable estimates cannot be obtained. Another problem with this model is that it does not guide the participants on how best to secure risky aspects of the system. By extending the McCumber Cube, another informal security model, this article will discuss one way to reduce reliance on inexact estimates and improve risk by focusing the assessment on attacks while deriving explicit countermeasures.

McCumber Cube model

John McCumber developed the McCumber Cube as a way to model risk management.[3] This model provides the security practitioner with a means to graphically evaluate and manage risk for a system (see Figure 2).

Viewing the cube from different angles provides a security practitioner with a way to consider risk from different perspectives. The three primary aspects of the cube involve:

1 Security goals often lack explicit definitions and are difficult to quantify. They are usually based on policies with broad interpretations and tend to be qualitative. It is true that security goals emerge from the confluence of information states and countermeasures which have measurable attributes. But, the subjective nature of security goals combined with informal modeling characterizes their attributes as intangible.

2 P. T. Devanbu and S. Stubblebine, "Software Engineering for Security: A Roadmap," *Proceedings of the Conference on The Future of Software Engineering* (2000), 227-239.

3 J. McCumber, *Assessing and Managing Security Risk in IT Systems: A Structured Methodology* (Boca Raton, FL: Auerbach, 2004).

Information states – These represent the various forms in which information can be found within a system. Information is the fundamental aspect of what it is that must be protected.

- *Processing* – Information held in volatile memory or currently manipulated through the processor
- *Storage* – This generally refers to non-volatile storage such as files on hard drives or backup media
- *Transmission* – Information transiting network media

Countermeasures – These are elements which can be used to defend a system from attack, which can be used to protect information in its various states.

- *People* – All individuals associated with a system to include administrators and users
- *Policies and practices* – Documented policies and procedures used to guide people interacting with the system; work flows, separation of duties, and least privilege
- *Technology* – Hardware and software which comprise the system such as operating systems, applications, networking devices, and security tools

Security services – These are the ultimate security goals of a system. They are not concrete but intangible.

- *Confidentiality* – Protecting information from an unauthorized or unintended disclosure
- *Integrity* – A quality which prevents the unauthorized alteration or destruction of information
- *Availability* – The ability to retrieve requisite information in a timely manner for an authorized user

The McCumber Cube can be used by selecting a desired security service and considering what countermeasures must be implemented to protect the affected information states. For example, suppose we need to defend a network against all compromises to information confidentiality. An approach would be to begin enumerating all the different types of controls which could be used to protect information confidentiality for each of the information states. Some of these items would include:

- **Encryption** – Protects information at rest or in transit
- **Antivirus** – Identifies malicious code which might steal and retransmit information
- **Periodic port scanning** – Identifies unauthorized or suspicious ports within the system
- **Identification and authentication** – Used to support access control and accountability for information accessed
- **Vulnerability scanning** – Identifying exploitable weaknesses in the system
- **Incident response** – Procedures used to respond to confidentiality breaches
- **Configuration management** – Ensuing appropriate access controls are implemented to protect information from unauthorized access
- **System documentation** – Identifies all countermeasures in place to protect information confidentiality within the network
- **Awareness training** – Informing users of their responsibilities to protect information from exposure as well as escalation of suspected or actual information exposures

Extending the McCumber Cube

Managing from such an abstract list is daunting at best. Even when the list is subdivided according to the countermeasures it can still be difficult to decide if all of the necessary countermeasures are in place. Achieving a more granular approach requires a minimization of the view from all three information states to each individually. This reduction allows the security practitioner to focus on the risk implications associated with the implementation of countermeasures for a given information state and a particular security service.

Figure 3 – Proposed Extension to McCumber Cube

One way to consider the appropriateness and completeness of a countermeasure is to match it with attacks which might be used against the system. In this way, a risk-based decision can be made regarding each possible attack and the types of countermeasures which might best be used as a basis for defense. A graphical representation of this concept is given in Figure 3. Here we see that an individual attack for a particular information state is combined with the appropriate countermeasures. When these three items are properly merged the applicable security concept is implied.

Although this concept reduces the total view of the McCumber Cube, it simultaneously extends its functional aspects. Extensions of the McCumber Cube are not new. The Information Assurance Model extends the McCumber Cube by adding the security services of authentication and non-repudiation.[4] It also adds the dimension of time as a consideration for risk-based activities for information assurance. Security practitioners are encouraged to seek new ways to view existing paradigms.

Reducing the scope of the view of the McCumber Cube can enhance risk-based decisions for the countermeasures needed to protect against specific attacks. The elements in Figure 3 are defined as follows:

4 W. V. Maconachy, C. D. Schou, D. Ragsdale, and D. Welch, "A Model for Information Assurance: An Integrated Approach," *Proceedings of the IEEE Workshop on Information Assurance and Security* (2001), 301-310.

- **Attacks** – A particular technique exploiting a system weakness
- **Information states** – What it is that needs to be protected
- **Countermeasures** – Those things which can be implemented to defend the network – it is important to note that a weakness presented in one of the associated countermeasures could reduce the ability to achieve the stated security goal
- **Security services** – The goal achieved when attacks to a given information state are mitigated with the identified countermeasures

The model created by McCumber does not require the use of three types of countermeasures. This provides the model user with flexibility. However, this is not an advisable practice. Ideally, a system is designed with appropriate defense-in-depth to enable a security service to continue when a particular countermeasure fails. The extension proposed in this article requires the security practitioner to identify controls for each of the countermeasure classes of *people*, *policies and practices*, as well as *technology*.

Model extension use scenarios

The following scenarios consider a strategy which enables each of the three security services. Each focuses on the transmission information state regarding network defense. Given a particular attack, potential countermeasures are selected which supports the implication that the security service is in effect. A security practitioner could easily compile this information into a table as a form of reference for a given system. Each scenario is accompanied by a table to illustrate this point.

Confidentiality on the network

Sensitive information commonly transits many networks. Multitudes of threat agents actively seek to capture sensitive information. Preventing the unauthorized or unintentional exposure of sensitive information is an important part of the security program of many organizations. Figure 4 illustrates *Sniffers* as a type of attack tool which could be mitigated with select countermeasures.

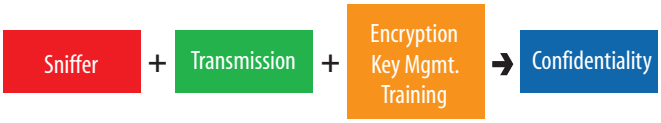

Figure 4 – Confidentiality Model Extension

Attack: Sniffers used to record network traffic.[5]

Countermeasures:

- *Technology* – Encryption is used to protect information from an unintended exposure. This may involve encryption between network nodes or other implementation such as those which are file-based to enable protection.
- *Policies and practices* – Cryptographic key management is necessary to ensure only those authorized access to the information are allowed to decrypt it.
- *People* – Users should be trained on what information should be transmitted through encrypted channels and how it should be accomplished.

Attack Vector	Information State	Countermeasures		Security Goal
Sniffer	Transmission	Technology	Encryption	Confidentiality
		Policy	Key Management	
		People	Training	

Table 1 – Sniffer against Transmission

Clearly, encryption is an excellent choice to use when protecting the confidentiality of information transmitted through a network. However, encryption is of little use if keys are not properly managed and people are not aware of its appropriate use. Table 1 lists the elements of Figure 4.

Integrity for network information

Information traversing a network might be modified in transit. Encryption provides an excellent means to detect modification to the information. However, encryption is not the best control to use in every circumstance. In this scenario an attacker uses *ARP spoofing* to redirect traffic. This allows an attacker the ability to redirect traffic to a particular network node where data packets could be manipulated. Figure 5 illustrates the aspects of this scenario.

Figure 5 – Integrity Model Extension

Attack: ARP spoofing is a known method facilitating network traffic redirection.[6]

Countermeasures:

- *Technology* – Scanning tools configured to look for peculiar ports and unauthorized duplicate MAC addresses is essential. Tools which conduct reverse ARP evaluations are the best to use.
- *Policies and practices* – The scanning should be conducted periodically. Automated scans are best. However, the results of any scan will need to be regularly evaluated.
- *People* – Administrators and security personnel should be trained on the use of the tools and techniques necessary to investigate suspicious activity.

5 Z. Trabelsi and H. Rahmani, "Detection of sniffers in an Ethernet network," *Lecture Notes in Computer Science, 3225* (2004), 170-182.

6 S. J. Templeton and K. E. Levitt, "Detecting Spoofed Packets," *Proceedings of the DARPA Information Survivability Conference and Exposition, 1* (2003), 164-175.

Attack Vector	Information State	Countermeasures		Security Goal
ARP Spoofing	Transmission	Technology	Port scanning	Integrity
		Policy	Periodic scans	
		People	Investigators	

Table 2 – ARP Spoofing against Transmissions

Attacks against network integrity, such as those using ARP spoofing, are interesting problems which might seem unlikely to occur. However, consider the possibilities of attacks such as pharming against network information integrity.[7] Unauthorized changes to dynamic naming servers (DNS), hosts files, and networking device configurations are similar in affect to ARP spoofing. Each of these could be used to redirect traffic to locations where the information could be tampered with or removed entirely form the system. Although the outcome is likely to be the same, different countermeasures would need to be considered for each aforementioned case since the target methodology is different. Table 2 shows the aspects of Figure 5.

Network availability

The inability to access information resources reduces the usefulness of a system. In some situations a lack of availability can directly affect the viability of an organization. Attacks which prevent users from accessing information resources in a timely manner are a continuing problem. Defending against a denial of service (DOS) attack is not always simple. Detection of these types of attacks is an important capability needed to preserve the availability of many information systems. Figure 6 presents one approach which can be used to counteract DOS attacks.

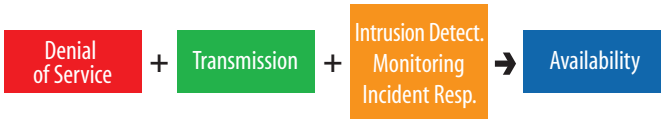

Figure 6 – Availability Model Extension

Attack: DOS prevents timely access to information or systems.

Countermeasures:

- *Technology* – Intrusion detection can be used to identify events indicative of a DOS attack.
- *Policies and practices* – Processes and procedures should be documented and regularly followed to identify DOS activity.
- *People* – Individuals need to be trained to effectively use intrusion detection tools and interpret their output. Incident response skills will also be needed to respond to actual DOS events. Those assigned tasks to identify and respond to DOS activity should periodically practice incident response activities.

In the information security realm detection must always be used when prevention cannot. But, is it necessary to also detect when preventative measures are implemented? The answer is a resounding, *yes!* Due to the possibility that a countermeasure might be bypassed or fail, detection must always continue. The most likely source of a DOS will come from outside of an organization. Firewalls are tools which are an acceptable countermeasure against a DOS attack.[8] However, these tools are of little use when the attack originates from inside a protected enclave. The pervasiveness of Trojan horses and bots allows attackers to launch any assault they desire.[9] As such, internal monitoring for a DOS will still be needed. Although detection must be used when prevention cannot, it should also be implemented when prevention is in place because it is unlikely that the preventative controls will be absolute. No tool or solution is a silver bullet which solves all associated security problems. Table 3 lists the considerations of the attack and the countermeasures selected for the information state and security goal.

Attack Vector	Information State	Countermeasures		Security Goal
Denial of Service	Transmission	Technology	Intrusion detection	Availability
		Policy	Monitoring	
		People	Incident response	

Table 3 – Denial of Service against Transmissions

These scenarios demonstrate a means to designate potential countermeasures for a given attack. The examples listed should not be interpreted to be fully inclusive. A complete solution requires a careful evaluation of the environment which may reveal multiple areas which need countermeasures. Minimally, at least one countermeasure for technology, operations, and people should be implemented as a way to achieve defense-in-depth.[10]

Extension used with risk assessments

The primary purpose of this article is to discuss an extension to the McCumber Cube which associates a specific attack with a selected information state and particular security service. This new model could also be used in a risk framework to ascertain the level of risk present for any given situation in a network environment. Figure 7 suggests that perceived threats coupled with their likelihood with this McCumber Cube extension could be used to evaluate system risk.

7 A. Emigh, "Phising Attacks: Information Flow and Chokepoints," in M. Jakobsson and S. Myers (eds.), *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*, pp. 31-63 (Hoboken, NJ: John Wiley and Sons, 2007).

8 C. L. Schuba, I. V. Krusl, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a Denial of Service Attack on TCP," *Proceedings of the 1997 IEEE Symposium on Security and Privacy* (1997), 208-223.

9 D. Geer, "Malicious Bots Threaten Network Security," *Computer, 38*(1) (2005), 18-20.

10 "Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments" (2008). Retrieved July 1, 2008, from www.nsa.gov/snac/support/defenseindepth.pdf.

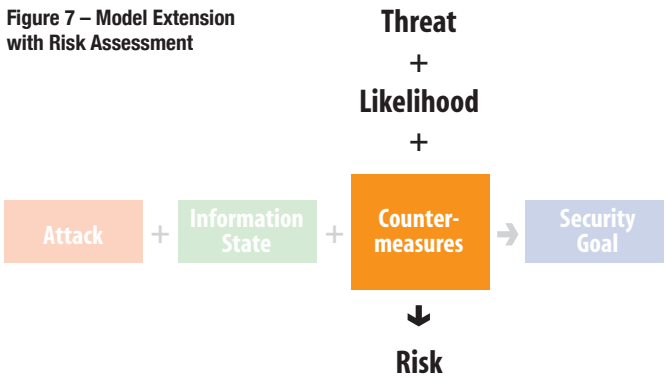

Figure 7 – Model Extension with Risk Assessment

The proposed extension to the McCumber cube takes risk assessment from a different angle. Why not consider specific threats and the estimate of their likelihood and then identify countermeasures that should be in place to defend against them. A lack of existing countermeasures from a defense-in-depth perspective (which is a vulnerability) equates to more risk for the system. Risk assessments do not generally consider countermeasures in the equation. Perhaps this is an intuitive exercise on the part of the assessors, but existing models in the literature seldom discuss it in detail. Popular risk assessment models often include too many estimates which devalues their worth. A model which is closer to a state of reality as opposed to something which relies on estimates is preferable. Often the estimates used in risk assessments have little research or quantitative results to support their assertions. The extension expressed in this article minimizes the estimates and focuses the risk assessment on explicit countermeasures for a specific threat.

Popular risk assessment models often include too many estimates which devalues their worth.

Conclusion

Using models is one way to consider methods to defend a network. The McCumber Cube is a robust, yet informal, model which provides a security practitioner with a graphical means to understand and evaluate system risk. This article proposed an extension to the McCumber Cube which can be used to associate security services, countermeasures, and information states with specific attacks. Using this type of model allows a more discrete identification of countermeasures needed to defend a network against specific types of attack. It can also be used as a new way to evaluate risk in a system.

About the Author

Sean M. Price, CISA, CISSP, is an independent security researcher and consultant living in northern Virginia. He specializes in designing and evaluating organizational information assurance programs and system security architectures. Research interests include insider threat, information flows, and applications of artificial intelligence to information assurance problems. Prior publications include the Information Security Management Handbook, Official (ISC)[2] Guide to the CISSP CBK, *IEEE Computer magazine, as well as other journals and conferences. You can reach him at sean.price@sentinel-consulting.com.*