THE PARKERIAN HEXAD

The CIA Triad Model Expanded

By Georgie Pender-Bey

In fulfillment of the Master of Science in Information Security Program at Lewis University

(This page is left blank intentionally)

Table of Contents

Abstract

The CIA model is a fundamental security model that has been around for more than 20 years. It focuses on three basic areas of information security: confidentiality, integrity, and availability. It is perhaps the most well-known model for securing data and is still taught and preached today. Today, data is more valuable and complex than ever. The amount of data that is stored electronically has grown exponentially over the last few years. In 2011, the amount of data created and replicated will surpass 1.8 zettabytes (1.8 trillion gigabytes) - growing by a factor of 9 in just five years [8]. Technological trends, such as cloud computing and storage and electronic health records, just to name a few, have made protecting data much more a daunting task than ever, and it's only going to continue to get harder. The global move to digitize personal and sensitive information is seemingly outpacing the capabilities of the security measures that have been in place for years. Since 2005, the investment by enterprises in the digital universe has increased 50% — to $4 trillion. That's money spent on hardware, software, services, and staff to create, manage, and store — and derive revenues from — the digital universe [8]. The CIA model also seems very technology driven and does not focus enough on the human element of information security. Humans are the biggest threat to security of data today. These, among other reasons, has led some to question whether the confidentiality, integrity, and availability (CIA triad) model is an adequate model to protect today's data, considering a lot of those measures were put in place with the CIA model in mind. Even though the Parkerian Hexad (PH) is built on the CIA model, its added components provide a more comprehensive and complete model for securing the data today. This paper will provide an in-depth explanation of the PH model and demonstrate its applicability to situations in which the CIA model of data security comes up somewhat short.

Chapter 1 -Introduction

Information Security is almost as old as information itself. Whenever people develop new methods for recording, storing, or transmitting information, these innovations are almost inevitably followed by methods of harnessing the new technologies and protecting the information they process [1]. Dating back more than two decades ago, the confidentiality, integrity, and availability (CIA) model has been the de facto standard by which to design and build your organization's information security architecture around. The CIA Triad is a venerable, well-known model for security policy development, used to identify problem areas and necessary solutions for information security [3]. Figure 1.1 is a graphical presentation of how the CIA triad effectively protects data. The bidirectional arrows in the figure below show the relationship between all three components in the CIA model. Having the dark circle in the middle further re-enforces the point that all three components must be protected in order to comply with CIA. It also stresses the importance of balance in your organization. For example, if you move the center circle more toward the confidentiality and integrity elements, you begin to sacrifice availability, and so on.

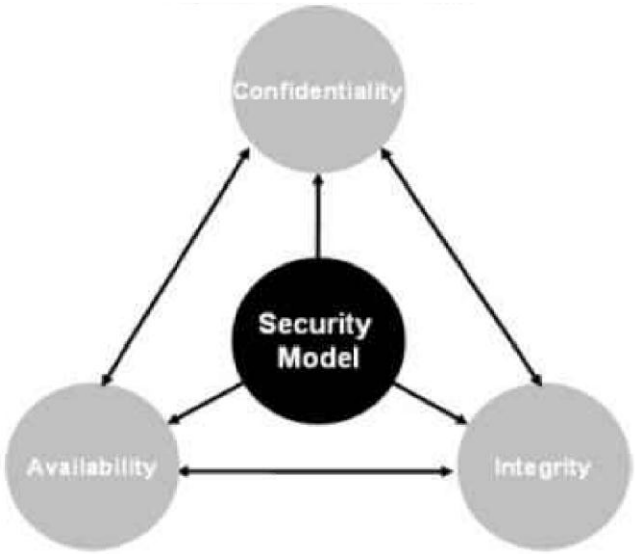

Figure 1.1: The CIA triad [12]

For a very long time it was thought that if a security design meets all of the components of the CIA triad, the data is relatively secure. This way of thinking, however, has changed in recent years for several reasons. So much has changed in the way we store data, where we store it, how we transmit it, and how we secure it. Moreover, ensuring data security and protecting privacy is becoming harder as the information multiplies and is shared ever more widely around the world [6]. The threats to information confidentiality, integrity, and availability have evolved into a vast collection of events, including accidental damage, destruction, theft, unintended or unauthorized modification, or other misuses from human or nonhuman threats [12]. Consider other examples as the move to electronic health records in the medical field, the ability to file your taxes online, cloud storage offerings from companies like Google and Amazon, and the evolution of security threats. These are just a few examples of how our data has become much more complex over the last few years, and the complexity is only going to continue to increase. This new environment of many constantly evolving threats has prompted the development of a

more robust intellectual model that addresses the complexities of the current information security environment [12].

In 2002, Donn B. Parker, currently a retired information security consultant and researcher, introduced an expanded version of the CIA model the added three additional elements. The security model was later renamed to the Parkerian Hexad in honor of Parker. To this day, Parker is highly regarded as one of the great minds on the topic of information security. In fact, he is also known as a great pioneer in the field of information security. He has earned numerous awards for his work in the information security field from several different organizations such as the Information Systems Security Association's Individual Achievement Award, 1994 National Computer System Security Award, MIS Infosecurity News' Lifetime Achievement Award, and the (ISC)²'s Harold F. Tipton Lifetime Achievement Award just to name a few. He has written several books on the topic of Info Security and gives lectures as well.

The Parkerian Hexad is an expression of a set of components added to the CIA triad to form or more comprehensive and complete security model. It aims to change how information security is understood and implemented. The six atomic elements of the Parkerian Hexad are confidentiality, integrity, availability, authenticity, possession or control, and utility. It aims to fill in the gaps of the of CIA model to improve the security of today's information assets. As Figure 1.2 suggests, security isn't as simple as the circle in the previous figure. The hexagon not only symbolizes the six components, it also figuratively suggests that each component fits together perfectly, solving the puzzle of comprehensive information security.

Figure1.2: The Parkerian Hexad [13]

Why did Parker deem it necessary to create a new security model? Are there threats (or threat vectors) that are not adequately covered under the CIA model? Has technology surpassed the CIA model? These issues will be explored in the upcoming chapters as the Parkerian Hexad is broken down and covered in-depth, particularly in regard to how it can address circumstances not covered adequately by the CIA approach.

Chapter 2 – Parkerian Hexad

When Parker introduced his refined security, he also wanted to change the way information security is assessed and understood. To him, the CIA model is simply too simplistic for some applications. Information security has not concentrated sufficiently on the role that people play in perpetuating and defending against information-related loss. Security is about people (and forces or acts of nature such as storms, heat, cold, or tremors), not just technology [7]. One of the limitations of the CIA model is that it focuses too much on the technology protecting information assets and not enough on people. Not only did Parker expand the CIA model, but he felt it was best understood and implemented when the components were grouped together. He suggested that the elements be looked at in the following groupings: *confidentiality and possession, integrity and authenticity, and availability and utility.* These elements are covered in detail below in the order that Parker meant for them to be understood.

2.1 – Confidentiality

Confidentiality is probably the most important element of both the CIA model and the Parkerian Hexad. It refers to the property that information is not made available or disclosed to unauthorized individuals, entities, or processes [4]. If your data is not confidential, it is not secure. Every organization has some form of sensitive information where only certain people should be allowed access to it. If exposed, this information could have damaging effects on the company and/or its customers.

One current example of a breach of confidentiality is the recent attacks on the Sony gaming and Qriocity networks. Some unknown group (or person) managed to gain unauthorized access to the personal information of thousands of Sony's customers. The damage was so severe, the attack forced Sony to disable much of its online services for weeks. Supposedly, Sony completely redesigned and rebuilt the infrastructure that supports their online services. Sony to this day, still isn't completely sure of how much data was exposed. The Director of Communications was forced to release the following statement to the public in April 2011:

> *"We have discovered that between April 17 and April 19, 2011, certain PlayStation Network and Qriocity service user account information was compromised in connection with an illegal and unauthorized intrusion into our network.*
>
> *Although we are still investigating the details of this incident, we believe that an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email address, birthdate, PlayStation Network/Qriocity password and login, and handle/PSN online ID. It is also possible that your profile data, including purchase history and billing address (city, state, zip), and your PlayStation Network/Qriocity password security answers may have been obtained…."* [21]

Today, there is an abundance of methods, technologies, and techniques that can be used to protect the confidentiality of sensitive data. Depending on the organization, some methods may be deemed unnecessary and/or prohibit users from completing their day-to-day responsibilities. Each organization must find which method works best for it.

For example, in the military and government workplaces, information is classified not just to assign value to data, but also as a means to protect its confidentiality. Data classification is a scheme by which the organization assigns a level of sensitivity and an owner to each piece of information that it owns and maintains [22]. The government has three classifications of information: top secret, secret, and confidential. When a document, letter, memo, or other piece of information is created, the owner assigns to it a classification level, which among other things,

defines the security clearance of individuals that can access that information [22]. High-ranking officers are the only individuals that may have access to top secret data, for example. This information could include launch codes, information about foreign relations, military tactics and strategy, etc. Slightly lower-class officers or personnel would have access to secret data. Regular staff members would have access to confidential data, but only on a need-to-know basis. By using this model, individuals need to gain clearance from authoritative officers or members of an organization in order to gain access to data at any of the levels. This is just one way of keeping data confidential.

2.2 – Possession/Control

The *possession/control* component is one of Parker's additions to the CIA model. It was added to protect against the idea that confidential data can be possessed and controlled by an unauthorized individual or party without actually violating or breaching confidentiality. Parker defines this component as:

> *"a state of having in or taking into one's control or holding at one's disposal; actual physical control of property by one who holds for himself, as distinguished from custody; something owned or controlled."* [7]

This component also addresses the protection of public data that may be owned and copy written. Articles, books, news publications, scholarly journals, etc. need to be protected even though they are technically available for anyone to view. Possession/Control is vital because it covers breaches where confidentiality is both key and nonexistent.

There are ways to protect your sensitive data even if the device that houses the data is stolen or lost. One tool that has grown in popularity fairly recently is the encrypted file system (EFS). EFS is a tool that uses both public key encryption in conjunction with symmetric key encryption to provide a strong defense against a breach of confidentiality. But in this case, it can also guard against a breach of possession. When a user wants to encrypt a folder or directory, your computer system generates a symmetric key called the file encryption key (FEK). Once the folder or directory is encrypted using the FEK, the computer then encrypts the FEK with the computer system's public key. As a best practice, the private key should not be stored on the local PC itself. Instead, on server and/or even a portable drive. When a user wants to decrypt a folder/directory, they have to use their private key to decrypt the FEK, and then use the FEK to decrypt the folder/directory.

How can this help protect against a breach in the real world? Just this year, at the Kennedy Space Center, a human resources employee reported that his laptop was stolen from his vehicle as it was parked outside of his home. The laptop is said to have contained the personal information of about 2,300 employees. In addition to Social Security numbers, the information included names, race, national origin, gender, date of birth, contact information, college affiliation and grade-point average [20]. NASA, which owns and runs the KSC, has since released a statement saying the following:

> *"More preventative actions and 'lessons learned' are expected to follow in the coming days and weeks to help stop this from happening again,"*…[20]

If EFS was used to encrypt the directory where the personal information of the employees was stored, it would make it very difficult to retrieve the data from that specific directory, assuming

that the private key was not stored locally on the computer. There will always be cases where employees need to have sensitive company information on a mobile device. The idea here is to protect the data contained on the laptop in the event the laptop is stolen or lost, possession is breached but not confidentiality. Another approach is to evaluate whether or not it is necessary for employees to have the data on their portable devices and explore technologies available that would give employees remote access to the data without having it stored on the device itself. It's safe to assume that EFS, along with many other necessary security policies, were discussed to make sure that they are protected against situations like this in the future.

2.3 – Integrity

Integrity is an original component of the CIA triad. It is defined as the ability to prevent data from being changed in an unauthorized or undesirable manner [24]. This definition is not limited only to unauthorized parties or intrusions. This definition also includes people with authorized access to information assets. It is a known fact that employees are one of the biggest threats to data integrity. Employees sometimes accidentally, delete files, enter inaccurate data, save over the wrong file, edit the wrong files, etc. File corruption is another concern. File corruption can occur while information is being transmitted, stored, or by viruses [4]. To maintain integrity, there not only need to be measures in place to prevent unauthorized and /or undesirable changes to data, but there also needs to be ways to undo or recover from those changes when/if they occur [24].

There are several ways to protect and ensure data integrity such as data verification and validation checks, performing and maintaining backups, and hashing, just to name a few.

Hashing is probably the most common way to protect and ensure data integrity today. File hashing is the process in which a file is read by a special algorithm using the value of its bits to compute a large number called a hash value [24]. The hash value now becomes a numerical representation of that file and its contents. The idea is that if anything changes within the file (i.e. replace a period with a comma, delete a space between two words, etc.) then when that file is hashed again, the hash value would be different from before. Data integrity is very important because inaccurate or altered data is basically useless data. Integrity attacks are not limited to just data. The integrity of websites, computers, and servers can all be compromised. A breach of integrity can have very severe financial and legal repercussions on any organization. Lots of organizations now use some form of hashing or integrity policies to check for data integrity today for these reasons.

Some software has built in tools and packages that can be installed that help to protect data integrity. For example, with oracle there is a package called the DBMS_SQLHASH package that a DBA could use to check the integrity of the results of a query. He/she could run a query on a customer database that returns values that are not normally changed very often such as first name, last name, mailing/shipping address, and credit card number. They could then, using the DBMS_SQLHASH command, to tell the database to calculate a hash value of that query that can be used later for comparing. A DBA could run this simple query as often as they desire and if the query ever returns a different hash value, they could then make sure that the change was a valid one. A hash value change could be due to the authorized deletion or addition of a customer, name change, or address change.

2.4 – Authenticity

Authenticity is another one of Parker's additions to the CIA model. Authenticity refers to the assurance that a message, transaction, or other exchange of information is from the source it claims to be from. Authenticity involves proof of identity [16]. Today, knowing exactly who you are communicating and sharing data with is key when doing business over the web. The internet has enabled us all the ability to do just about anything and everything from our homes such as filing our taxes, performing bank transfers, check credit reports and scores, and paying bills. Because of these abilities, and many others, technologies were developed to give customers the confidence in knowing that the site they are visiting is legitimate and the communication is secure.

As with all of the other components, there are several ways to accomplish the goal of authenticity. One of the most common methods used today is the use of digital certificates. Digital certificates are files that certify the identity of a company being accessed through its website. Digital certificates are issued by entities called certificate authorities. Certificate authorities are mutually trusted companies that verify companies are who they say they are and issue a certificate proving so. They are most often used in public key infrastructure environments and contain the name, address, serial number, public key, expiration date and digital signature, among other information. Companies use these digital certificates to validate their websites and create encrypted connections, also known as secure socket layers (SSL) connections, to secure the communication between the client and the server. This way, when users browse to these sites, they can not only see that the site is validated but they can also have some confidence knowing that their connection and all communication with the site are secure.

Websites are subject to phishing-based spoofing attacks every year. Early in 2011, one of the web portals for the air force was spoofed. Nearly identical to the real site, the fake one aimed to fool people into entering their log-ins and passwords so the information could be captured by illicit sources [19]. They are not sure how many people fell victim to the site, but once it was reported the site was immediately taken down. Had users paid attention to the details of the site, they would have noticed that the site was not issued a Department of Defense digital certificate, or any digital certificate at all for that matter. Attacks like this happen all the time. PayPal is spoofed regularly using the exact same tactics. In 2003, Paypal customers received a phishing email that directed users to a spoofed PayPal website called www.paypal-billingnetwork.net [25]. In 2008, a website called fightidentitytheft.com made it known that PayPal was spoofed again using several other realistic domain names such as www.paypalnet.com, www.paypa1.com, and www.paypalsecure.com [26]. Digital certificates are great but also are useless if they go unnoticed.

2.5 – Availability

Availability is the last component of the original CIA model. Availability is defined as the ability to have resources available when needed. It is one of the simpler components to describe, but ironically, it is one of the most difficult to safegard. Security professionals today are tasked with the responsibility of securing networks and their resources while also maintaining availability. As the old saying goes, the only way to truly achieve total security is to unplug the server and lock it up in a volt. But the fact of the matter is, in today's world, if resources are not available, companies could face very serious consequences such as loss of

revenue, broken client relationships, failure to meet SLAs, danger to patient care (in EHR implementations), and other poor outcomes. Maintaining and ensuring availability of resources has become one of the biggest tasks for any information support or security professional.

The challenge for every information security professional is to achieve the right balance of availability and security. Depending on the level of availability needed, there are several options available to help meet the goal of availability. Two of the more common options are active/active clustering and active/passive clustering. Both help to provide high availability but in slightly different ways. There are several ways to configure them as well. Only one setup will be covered here.

In active/active clustering, all devices in the cluster are in an active mode and may also be load balancing the connections to resources. For example, one of the most important network components used for securing a network are firewalls. If a single firewall is the gateway for a network, it is a single point of failure. If the firewall were to fail for any reason, your entire network could lose connectivity to the internet. One way to protect against this failure is to have multiple firewalls clustering together in an active/active cluster, also known as a high availability pair. With this setup, you not only have load balancing but you also gain protection against any kind of failure. Since both devices are active, they are both able to handle connections a firewall the network logically as one unit. In the event that one fails or is deactivated for any reason, the other device(s) takes over and the experience is totally transparent to the end-users and end-devices in the network.

With active/passive clustering, you have high availability but not the same load balancing capabilities or transparency to the end-users and end-devices. The two devices in this build are

built exactly the same with the exception that one is inactive and one is active. This means that fs one device fails, the other device becomes active and takes over for the inactive device. One of the drawbacks to the active/passive configuration is that the failover tends to be not so transparent to the end-users and end-devices because of the very short amount of time it takes for the inactive device to become active. That short amount of time may not be that big of an issue for most networks but for financial and trading companies, 20 seconds to 1 minute of downtime could cost the company hundreds of thousands of dollars. The inability to process transactions is very detrimental for financial companies, even if the outage is very momentary.

2.6 – Utility

Utility simply refers to the usefulness of data. This is the last fundamental component of the Parkerian Hexad. It focuses on a much overlooked concept when it comes to data. The data may meet five of the six PH components (confidentiality, integrity, availability, authenticity, possession/control), but is it in a useful state? Utility is often confused or assumed with availability but the two are distinct.

Consider the following hypothetical:

> *"An employee is asked to send an encrypted copy of the company's employee database to a data mining company for analysis. The employee goes out and buys an encrypting drive so that any data copied to it needs a decrypting key to access it. The employee copies the database to the drive, assigns a key to it, and sends it to the data mining company. Three days later, the data mining calls and says that they have*

received the drive but does not know the key. The employee that sent the drive forgot the key that was assigned to the drive ....."

In the example above, five out of the six components, except for utility, are met. The sensitive data is confidential, retains its integrity, authentic, possessed/controlled correctly, and available but is not in a useful format or state. Parker gave a good brief description of his reasoning for adding utility as a component:

"Information may be available and therefore usable but it doesn't necessarily have to be in a useful form to be defined as available ." [7]

Utility cannot be overlooked as a vital component to this model. If data it not a in a useful state or form, it is basically useless.

Chapter 3 – CIA vs PH

Parker describes the CIA model as simple and easily and quickly explained to management, information owners and users, and legislative assistants that write our laws. However, we are dangerously deceiving them by its simplicity, errors, and deficiencies [7]. The CIA model is simply too simple a concept to secure today's complex networks and it may leave environments susceptible to threats that they are not prepared to handle. Parker aimed to expand the view of security and include people more into the realm of information security. Below is a comparison between the components as Parker would have us view them.

3.1 – Confidentiality vs Possession/Control

Every breach of confidentiality is a breach of possession/control. Adversely, every breach of possession/control is not a breach of confidentiality. An adversary may steal a memory stick with your private key on it, but they may not have your pass phrase to use it. The confidentiality has not been breached but your adversary now has possession and control of your information asset [5]. Information security has to take the human element more into consideration. Security professionals can spend all their time making sure that the data is confidential, but they must also make sure that those that have appropriate access to data handles it appropriately.

One area that the current CIA model does not address is copyright violations. Data that is meant to be open and exposed to the public still needs to be protected. In this case, exposure and

disclosure is not a breach of confidentiality because there is no confidentiality. But if someone decides to re-use copy written material, there has to be a way to define the violation. This is a violation of control. This is also an example of the CIA model not including human interference enough in the concept.

3.2 – Integrity vs Authenticity

Integrity refers to being correct or consistent with the intended state of information. Any unauthorized modification of data, whether deliberate or accidental, is a breach of data integrity [4]. This is another component that relies heavy on technology and does not look enough into the human element enough. Cyclic redundancy check and hashing algorithms are great, but what about the authenticity of data? Authenticity cannot be assumed because they are two totally different concepts.

For example, integrity does not answer the question of, is this message truly from the sender? Is my banks website actually the website from my bank? If a criminal forges e-mail headers to make it look as if an innocent person is sending threatening e-mail messages, there has been no breach of confidentiality (the thief uses his or her own e-mail account), possession (no information has been taken out of the control of the victim), or integrity (the e-mail messages are exactly as intended by the criminal). What is breached is authenticity: the e-mail is incorrectly attributed to someone else [4]. The CIA model overlooks this important human element.

3.3 – Availability vs Utility

Once a user has access to resources, is it in a state or form that is useable? Implementing redundancy, failovers, and clusters are great for ensuring availability. Protecting against hardware failures and DDoS attacks is very important to maintaining network health and functionality. Availability is not concerned at all with the usability of the outputs.

Utility focuses on the content of data. If a customer sent an email to a retail company in a language that the retail company doesn't recognize, that message may meet the requirements of five of the six PH components except for utility. The complexity of data has made the utility of data even more important. The CIA model fails to acknowledge and overlooks the idea of data utility. These are the reasons that the PH model is a more comprehensive and complete model today.

Chapter 4 – Meeting PH Compliance

One of the great things about the PH model is that organizations can become compliant without having to invest large amounts of money in infrastructure. It really comes down to better policy writing and enforcement, employee education and awareness, and/or leveraging a lot of the technology that is likely already available in most environments. In some situations, one can meet multiple components of the PH model by taking one technological step forward. There are many ways to achieve PH compliance. In the sections below, a few tips for meeting PH are described.

4.1 – Use IPSec VPN tunnels

Using IPSec VPN tunnels satisfies multiple components of the PH model such as data **integrity**, **confidentiality**, and **authenticity**. IPSec works in phases. Authenticity is achieved in both phase 1 and phase 2 of the IPSec process. Using preshared keys is the simplest way to securely authenticate peers. This means that both peers have agreed on symmetrical keys that will be used to negotiate all security association parameters during the initial Internet Key Exchange (IKE) negotiation. Authenticity, confidentiality, and integrity are all achieved in the tunnel itself, during and after phase 2. The level of encryption and the hashing also are generally agreed upon by both peers. The encryption provides the confidentiality. All data packets are encrypted in transit from end to end. The cryptographic hashing algorithm chosen between the peers serves two purposes. HMAC-SHA1, for example, is used to verify the integrity of the data

in transit and to also authenticate the data. The use of IPSec alone satisfies three out of the six components of PH.

4.2 – Limit the amount of data that leaves the organization

Today, remote employees are a very necessary evil for businesses. Home workers and field salesmen often need access to very sensitive data in order to work and function effectively. There are two known issues with remote or field employees: they are either given too much data out of fear that they may not have what they need during crucial presentations and/or sales meetings and the threat of losing sensitive data to theft or accidental misplacement or disclosure. This makes protecting the **possession or control** of data much more difficult.

Thankfully there are technologies available to help keep the data where it is most secure. Technological advancements like citrix allow users to access resources at work from anywhere as long as they have an internet connection. Citrix leverages a combination of proprietary technologies and Microsoft's terminal services to provide users with a work-like experience from anywhere. With this technology, all users see are screenshots of an application running on a server. This eliminates the need to have sensitive data and proprietary applications stored locally on mobile devices or remote PCs. Network administrators can also limit what remote users have access to and when they can access it. Technologies like this help to minimize the risk of a breach of possession or control of data.

4.3 – Configure critical systems for high availability

In a world where access to critical systems and sensitive data are crucial, security is paramount but **availability** cannot be overlooked. There are several ways to tackle ensuring availability of resources. When it comes to virtual environments, high availability can be a lifesaver when/if there are hardware failures. The idea behind availability in virtual environments is simple. Most, if not all, virtual environments have multiple physical servers that host several virtual servers. Should one of the physical servers fail, typically the virtual servers being hosted on that server fail as well. With high availability, should a physical server fail, the hosted virtual servers can be automatically migrated to another physical host server with available resources. The occurrence, in some cases, can be nearly transparent to users and/or active connections currently being handled by the virtual servers at the time of the failure. Availability of resources is preserved and business can continue as usual while the failed server is repaired and re-implemented.

4.4 –Follow the best practices for key management

PKI is a very common set of protocols, polices, and procedures that can be used to encrypt data, authenticate the sender, and verify the integrity of the message. PKI is most commonly used with SSL. When used correctly, it is a very effective process for securing data. One aspect of PKI that can easily be overlooked is the management of the private keys. The private keys associated with digital certificates are a vital component in ensuring the **utility** (or usefulness) of data. For example, with SSL, if for some reason the private key associated with a

certain digital certificate is lost, then any data that is encrypted using the public key cannot be decrypted. This incident essentially renders the data useless.

Proper management and security of private keys should be at the top of the list when it comes to the implementation of PKI. Private keys should nearly be treated as Top Secret data. This means that keystores should have different passwords that are changed regularly with the company's passwords policy. The password should not be the same as the administrative password used on other servers [27]. This would keep every IT professional in the organization from knowing the password to the keystore. Only the administrator who is responsible for managing the keystore should know the password. The password to the keystore should also be changed when the IT professional that was responsible for managing the keystore is reassigned or leaves the organization [27]. The organization should also consider getting new certificates with new private keys in the same instance as well. The keystore should be backed-up regularly and kept off-site like all critical data. Use of an automated key and certificate management system that removes the need for administrators to access keystores directly and the passwords that protect them is also great idea [27].

Chapter 5 – Conclusion

The CIA model has been a very good security model for a very long time. There are several reasons to why the CIA model seems to fall short of being an adequate security model. As threats and technologies change, the understanding of how to secure those technologies and protect against those threats must change. Today, humans are much more of a threat than ever before. Also, data has become far more complex than ever before, which in turn makes securing that data more difficult. The online capabilities introduce new threats that are simply not adequately covered in the CIA model.

The more opportunities humans have to handle data, the more that data is at risk of being loss, stolen, and somehow corrupted. This is especially true for remote and field employees. When data leaves the organization on an employee's laptop or portable storage device, it is up to the organization's information security department to make sure that that data is protected should that device become lost or stolen. Implementing whole-disk encryption or EFS and encrypted portable drives that can self-destruct are a good start. This way, confidentiality is reserved even though possession or control is breached in the event the device is lost or stolen. The harsh fact is that humans are very forgetful and are prone to making mistakes. A better option would be to employ policies and technologies that aid in limiting the amount of data that has to leave the organization. Every breach of confidentiality is a breach of possession or control. But not every breach of possession or control has to be a breach of confidentiality.

The increase in data complexity cannot be ignored when evaluating security models. One of the biggest attributes of data complexity is the growth in the amount data being created,

processed, and secured. The growth in data has drastically changed storage technologies over the last several years. Growth rates and availability demands have led to some to have to implement cloud or SAN storage technologies. As the world becomes more digital, more and more sensitive data will be created and stored. If the data itself is not simple, the security of it can't be simple.

Online capabilities have vastly expanded. People are now able to do anything from file taxes to looking up their medical history. These new capabilities require a new way of thinking when it comes to security. When it comes to patient health information (PHI) or personally identifiable information (PII), authenticating the site you're communicating is vital in protecting yourself from identity theft. On the other end, validating the utility (or usefulness) of the data users are entering into the site vital for business. Using technologies like SSL for authentication (and encryption) has nearly become expected. Companies have also went to great lengths to make sure they are getting useful data from customers by parameterizing fields in online forms and simplifying form questions, for example. The CIA model simply doesn't cover these areas and needed to be expanded.

References

[1] R. Lehtinen, D. Russell, and G.T. Gangemi Sr., "Some Security History", in *Computer Security Basics,* 2nd Edition, O'Reilly, 2006, ch. 2, pp. 22.

[2] J. Hintzbergen, K. Hintzbergen, I. Baars, and A. Smulders, "Information, security, and architecture", in *Foundations of Information Security,* 2nd Edition, Van Haren, 2010, ch. 4, sec. 4.2, pp. 13-14.

[3] C. Perrin. (2008). *The CIA Triad* [online]. Available: http://www.techrepublic.com/blog/security/the-cia-triad/488. Accessed January 12, 2012.

[4] P. Steichen. *Principles and fundamentals of security methodologies of information systems – Introduction* [online]. Available: http://pst.libre.lu/m2ssic-metz/01_intro-art.pdf. Accessed January 23, 2012.

[5] Marinus (2009). *Is the CIA model still relevant?* [online]. Available: http://telicthoughts.blogspot.com/2009/02/when-one-thinks-of-securing-information.html. Accessed 23, 2012.

[6] K. Cukier (2010). *Data, data everywhere*. [online] Available: http://www.economist.com/node/15557443. Accessed February 12, 2012.

[7] D. B. Parker (2010). *Our Excessively Simplistic Information Security Model and How to Fix It* [online]. Available: http://www.issa.org/images/upload/files/Parker-Simplistic%20Information%20Security%20Model.pdf. Accessed February 12, 2012.

[8] L. Mearian (2011). *World's data will grow by 50X in next decade, IDC study predicts* [online]. Available: http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf . Accessed March 11, 2012.

[9] L. King (2009). *IDC: Business security 'must keep pace' with data complexity* [online]. Available: http://www.computerworlduk.com/news/security/16642/idc-business-security-must-keep-pace-with-data-complexity/. Accessed February 12, 2012.

[10] *Security Considerations: How to Ensure Data Authenticity and Integrity [online]. Available: http://etutorials.org/Networking/network+management/Part+I+Data+Collection+and+Methodology+Standards/Chapter+2.+Data+Collection+Methodology/Security+Considerations+How+to+Ensure+Data+Authenticity+and+Integrity/. Accessed February 12, 2012.*

[11] M. Whitman, H. Matord (2009). "Introduction To Information Security," in *Principles of Information Security, 3rd* ed. Boston, Mass. Thomson Course Technology. 2009, pp. 3 – 13.

[12] Y. Bhaiji (2008), *Chapter1: Overview of Network Security*[online]. Available: http://www.networkworld.com/subnets/cisco/072508-ch1-net-security-technologies.html. Accessed February 26, 2012.

[13] L. Marzigliano , *Advice: Security vs. Utility* [online], Available: http://www.zigthis.com/145, Accessed February 26, 2012.

[14] S. Mirjalili, A. Lenstra , *Towards a Structural Secure Design Process* [online], Available: http://infoscience.epfl.ch/record/164556/files/NPDF-48.pdf, Accessed February 26, 2012.

[15] S. Holloway (2010), *Security? What security?* [online], Available: http://www.it-director.com/business/security/content.php?cid=12267, Accessed February 26, 2012.

[16] L. Clemmer (2010), *Information Security Concepts: Authenticity* [online], Available http://www.brighthub.com/computing/smb-security/articles/31234.aspx , Accessed March 11, 2012.

[17] D. Beattie, *Information Security: An Overview* [online], Available: http://www.cybersecureonline.com/KNOWYourRisks/InformationSecurity/tabid/65/Default.aspx , March 11, 2012.

[18] X. Wu (2009), *Security Architecture for Sensitive Information Systems* [online], Available: http://www.csse.monash.edu.au/~srini/theses/Ping_Thesis.pdf , Accessed March 11, 2012.

[19] R. Boland, (2011), *Military Website Spoofing Is No Laughing Matter* [online], Available: http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2814&zoneid=254, Accessed March 2, 2012.

[20] J. Dean, (2012), *KSC employees warned over effects of laptop theft* [online], Available: http://www.floridatoday.com/article/20120317/BUSINESS/303170018/KSC-employees-warned-over-effects-laptop-theft%3Fodyssey?nclick_check=1, Accessed March 29, 2012.

[21] M. Panzarino, (2011), *Playstation Network Hacked and user Information stolen, here's what you have to do[Updated]* [online], Available: http://thenextweb.com/insider/2011/04/26/entire-playstation-network-hacked-and-user-information-stolen-heres-what-you-have-to-do/. Accessed March 26, 2012.

[22] R. Collette, M. Gentile, (2006), *Overcoming Obstacles to Data Classification* [online], Available: http://www.computereconomics.com/article.cfm?id=1117, Accessed March 26, 2012.

[23] *How EFS Works* [online], Available: http://technet.microsoft.com/en-us/library/cc962103.aspx, Accessed March 29, 2012.

[24] J. Andress, "The Basics of Information Security", in *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, Elsevier, 2011, ch. 1, pp. 5-8

[25] P. Roberts, (2003), *PayPal Users Warned of Spoof Site* [online], Available: http://www.pcworld.com/article/111499/paypal_users_warned_of_spoof_site.html, Accessed April 24, 2012

[26] (2008), *PayPal Email Scam – Web Form* [online], Available: http://www.fightidentitytheft.com/paypal_scam_webform.html, Accessed April 24, 2012

[27] P. Turner (2010), *Private Key Management: Best Practice Tips From The Real World* [online], Available: http://www.businesscomputingworld.co.uk/private-key-management-best-practice-tips-from-the-real-world/ , Accessed April 30, 2012.