Week 5 Final Assignment: Application Security and Cryptographic Algorithms

Shaun Hoadley

CST316: Information Security Management

Professor Amr Elchouemi

August 9, 2021

There are a number of ways for organizations to support CIANA (Confidentiality, Integrity, Availability, Non-repudiation, and Authentication) and promote security Awareness. One such way is by implentingorganizational security policies and procedures. While there are other componentsan organization may include in their security policies and procedures, this paper will focus on acceptable use policies, password policies, authorization and authentication policies, and security awareness policies, due to easy implementation and high return on investment.

As the name implies, the policies that contain the guidelines for acceptable use of company resources, hardware, and software for security threat mitigation are acceptable use policies. Acceptable use policies support basic security principles with their implementation. Acceptable use policies should clearly state how company resources should and should not be used by the employees as well as visitors. An example from Security by Design Principles according to OWASP, blocking specific websites on company networks can support defense in depth by creating a layer of protection against risky websites (Sveikauskas, 2018).

Password policies are also fairly easy to implement. Password policies dictate the requirements for passwords, as well as regulate how frequently passwords should be reset. The complexity of passwords dictate how challenging it is for an attacker to crack it and thus gain access to a system. Organizations are able to set a baseline of security by requiring passwords meet certail criteria, such as minimum length, uppercase and lowercase letters, numbers, and special characters. Password policies support the principles of establishing secure defaults as well as defense in depth.

Authorization and authentication policies support the principles of defense in depth and principle of least privilege. Authorization and authentication policies are used to verify that a user is who they claim to be (authentication) as well as the amount of access they are allowed in a system (authorization). Organizations may further increase security robustness making it even more difficult to penetrate by using multifactor authentication.

Finally, security awareness policies are used to educate employees about information security principles, avoiding the opening of suspicious emails, clicking links that may be malicious, and how to respond to a suspected threat. Security awareness policies support the principles of least privilege and defense in depth. Organizations further reduce risk by implementing security awareness policies, because their employees are educated about what types of emails, links, and websites may be trusted, and which are “don’t trust” services.

Integrating other security practices alongside acceptable use policies, password policies, authorization and authentication policies, and security awareness policies, establishes the security of the organization. With a security structure in place, the organization minimizes risk of attack and establishes recovery plans allowing rapid recovery in the event of an attack.

An organization that I am affiliated with has implemented an acceptable use policy for their company network that prevents employees and affiliates from accessing personal email accounts and social media sites. The organization does have an isolated guest network so that visitors to the facility, and employees on their break with their own devices, have the ability to check these during downtime (visitors waiting to be seen or employees on break). As part of the acceptable use policy, employees are only permitted to have personal devices in designated areas. With those policies in place, the organization promotes productivity while limiting possible risks to the company network via malicious emails, viruses, and social engineering.

The password policies implemented by the organization are designed to further minimize risk of unauthorized access to the company network. Rather than relying on users to create and update their passwords for the system, the organization has a random password generator that provides and resets user passwords every forty-five days. The random password generator creates a variable length password from twelve to eighteen characters long that includes uppercase and lowercase letters, numbers, and special characters. If a user loses their password they are required to contact a system administrator to be able to have a new password generated for them. The result of the password policy ensures a high level of complexity for passwords that make them less susceptible to being cracked further ensuring the security of the network.

In addition to the password policies, the organization also uses multifactor authentication methods to control access. For physical locations within the building doors require a swipe of an employee badge and a six digit code to unlock the doors. For access to certain parts of the network, in addition to username and password, SecureID is also required. The SecureID is a system that generates a six digit number every sixty seconds on a lcd display on a card or fob.

I am unsure of what additional security awareness policies are in place for employees, but affiliates such as myself are required, within the first thirty days, to submit to a federal background check. Upon passing the background check, a Homeland Security STA (Security Threat Assessment) course must be taken and passed. After the initial background check and STA course, the background check must be renewed every five years and the STA course renewed annually.

To further secure itself, in addition to the policies above, an organization should also utilize network security mechanisms. As stated by Wills, administrators can set rules within DHCP (Dynamic Host Configuration Protocol) to enforce whether or not a device can coonect to the network (2019). Organizations may whitelist or blacklist email addresses and IP addresses to allow or disallow access. To send data securely over the network, IPSec (Internet Protocol Security) should be leveraged (Wills, 2019). Access controls can be used for granting or denying a user to the system as well as track the activities of the user on the system. A common form of access controls is Role-based access control. A role-based access control grants authorization of privileges based on the role that a user is set at (eg. Administrator, manager, user, etc..). The application of email filters can be used to detect and redirect suspicious emails. The use of multifactor authentication (MFA) increases the security of accounts. As stated by Sargent, firewalls and network alerts for abnormal activity should be additional layers of security (2020).

Implementing audits and vulnerability scans can identify possible vulnerabilities in networks and attached devices. Simulated attacks and weak node detection and repair can be done with active scanning. Among some of the tools available for networks that promote active scanning and exposed ports are Trace Route, Port Scanner, IP Scanner and NS Lookup. Regular network activity monitoring can be done with passive scanning to ensure software and firmware are up to date.

To properly secure data, organizations should use cryptographic algorithms. A cryptographic algorithm takes plaintext and converts it to ciphertext. The three major types of cryptographic algorithms are symmetric, asymmetric, and hash function algorithms. Symmetric cryptographic algorithms, sometimes referred to as secret key algorithms, use a single key for encrypting and decrypting data. Because a symmetric cryptographic algorithm uses a single key, if that key is compromised, any data encrypted with that key is also possibly compromised, therefore this method of encryption should be avoided if possible by organizations. An asymmetric cryptographic algorithm uses a public key and private key combination where the public key is mathematically linked to the private key. Because an asymmetric cryptographic algorithm uses two keys for encryption and decryption, it is more secure at the cost of using more computing power. Hash functions, sometimes referred to as one-way encryption, compute fixed-length hash values based on the plaintext (and sometimes a salt value), rather than using a key. Some of the common encryption algorithms used today are 3DES, AES, and RSA.

When it comes to software development and the software development lifecycle (SDLC), an organization can further improve on security by instituting security practices and testing into the traditional software development lifecycle. Doing so makes the SDLC a Secure SDLC, or security development lifecycle. This can be done by using security compliant code and by eliminating code that might allow others to inject code that can compromise the system.

Lastly, organizations should have in place some sort of incident and disaster mitigation plans. One well respected framework for incident response id from the National Institute of Standards and Technology (NIST). According to Wills, the NIST framework includes the following steps, detection, response, mitigation, reporting, recovery, remediation, and lessons learned (2019).

By anticipating security vulnerabilities, having clear security policies and procedures, and incident management and disaster recovery plans, organizations can avoid many security vulnerabilities and breaches. Through adhearance to CIANA, organizations can gain and maintain the trust of their clients as well as investors or stockholders. By promoting security awareness and incorporating security practices in the SDLC, organizations increase their security and lower risks to attacks.

**References**

Sargent, S. A., & Webb, J. P. (2020). The Key to Trust: Social Engineering Fraud and Modern Threat Detection. Benefits Magazine, 57(1), 22.

Sveikauskas, D. (2018). *Security by Design Principles according to OWASP*. ThreatPress. Retrieved from <https://blog.threatpress.com/security-design-principles->owasp/

Wills, M. (2019). [(ISC)2 SSCP Systems security certified practitioner: Official study guide](https://ashford.instructure.com/courses/87741/modules/items/4439845) (2nd ed.). John Wiley & Sons.