**Homework #7 Answers**

**CECS 378 – Spring 2021 Cappel**

**Due:** Wednesday, May 5th by 11:59 PM

**Homework #7 is focused on Chapter 12 and Chapter 14. There are 10 total questions all worth 10 points each (100 pts total).**

**Chapter 12 – Operating System Security**

1. What are the basic steps needed in the process of securing a system?

* assess risks and plan the system deployment.
* secure the underlying operating system and then the key applications.
* ensure any critical content is secured.
* ensure appropriate network protection mechanisms are used.
* ensure appropriate processes are used to maintain security.

1. What are the basic steps needed to secure the base operating system?

* install and patch the operating system.
* harden and configure the operating system to adequately address the identified security needs of the system by:
  + removing unnecessary services, applications, and protocols
  + configuring users, groups, and permissions
  + configuring resource controls
* install and configure additional security controls, such as anti-virus, host-based firewalls, and IDS, if needed
* test the security of the basic operating system to ensure that the steps taken adequately address its security needs.

1. What are the pros and cons of automated patching?

**Pros:** minimizes window of opportunity for attackers when new vulnerabilities are found; is convenient, especially if automated.

**Cons:** patches sometimes introduce instability, especially on change-controlled systems.

1. What are the main security concerns with virtualized systems?

* guest OS isolation, ensuring that programs executing within a guest OS may only access and use

the resources allocated to it, and not covertly interact with programs or data in either other guest

OS’s or in the hypervisor

* guest OS monitoring by the hypervisor, which has privileged access to the programs and data in each guest OS, and must be trusted as secure from subversion and compromised use of this access
* virtualized environment security, particularly in regard to image and snapshot management, which attackers may attempt to view or modify

1. Why is logging important? What are its limitations as a security control? What are pros and cons of remote logging?

Logs provide audit trails of system and application events, and are useful for identifying problems, analyzing security breaches, analyzing system/application failures. In regulated or otherwise controlled environments, logs are usually mandated by industry or governmental auditors. Logs may even, if monitored closely, provide an early warning of failures or attacks in progress.

**Chapter 13 – Cloud & IoT Security**

1. List and briefly define the essential characteristics of cloud computing.

* **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms as week as other traditional or cloud-based software services.
* **Rapid elasticity**: Cloud computing gives you the ability to expand and reduce resources according to your specific service requirement. For example, you may need a large number of server resources for the duration of a specific task. You can then release these resources upon completion of the task.
* **Measured service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.
* **On-demand self-service:** A cloud service consumer (CSC) can unilaterally provision computing capabilities, such as server time and network storage, as needed, automatically, without requiring human interaction with each service provider. Because the service is on demand, the resources are not permanent parts of the consumer’s IT infrastructure.
* **Resource pooling:** The provider’s computing resources are pooled to serve multiple CSC’s using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

1. List and briefly define three cloud service models.

* **Software as a service (SaaS)**: Provides service to customers in the form of software, specifically application software, running on and accessible in the cloud.
* **Platform as a service (PaaS)**: Provides service to customers in the form of a platform on which the customer's applications can run.
* **Infrastructure as a service (IaaS)**: Provides the customer access to the underlying cloud infrastructure.

1. Describe some of the main cloud specific security threats.

* **Abuse and nefarious use of cloud computing**: For many CPs, it is relatively easy to register and begin using cloud services, some even offering free limited trial periods. This enables attackers to get inside the cloud to conduct various attacks, such as spamming, malicious code attacks, and denial of service.
* **Insecure interfaces and APIs**: CPs expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.
* **Malicious insiders**: Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and, in doing so, confers an unprecedented level of trust onto the CP. One grave concern is the risk of malicious insider activity. Cloud architectures necessitate certain roles that are extremely high-risk.
* **Shared technology issues**: IaaS vendors deliver their services in a scalable way by sharing infrastructure. Often, the underlying components that make up this infrastructure (CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multitenant architecture. CPs typically approach this risk by the use of isolated virtual machines for individual clients. This approach is still vulnerable to attack, by both insiders and outsiders, and so can only be a part of an overall security strategy.
* **Data loss or leakage**: For many clients, the most devastating impact from a security breach is the loss or leakage of data. We address this issue in the next section.
* **Account or service hijacking**: Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity, and availability of those services.
* **Unknown risk profile**: In using cloud infrastructures, the client necessarily cedes control to the cloud provider on a number of issues that may affect security. Thus, the client must pay attention to and clearly define the roles and responsibilities involved for managing risks. For example, employees may deploy applications and data resources at the CP without observing the normal policies and procedures for privacy, security, and oversight.

1. List and briefly define the principal components of an IoT-enabled thing.

* **Sensor**: A sensor measures some parameter of a physical, chemical, or biological entity and delivers an electronic signal proportional to the observed characteristic, either in the form of an analog voltage level or a digital signal. In both cases, the sensor output is typically input to a microcontroller or other management element.
* **Actuator**: An actuator receives an electronic signal from a controller and responds by interacting with its environment to produce an effect on some parameter of a physical, chemical, or biological entity.
* **Microcontroller**: The "smart" in a smart device is provided by a deeply embedded microcontroller.
* **Transceiver**: A transceiver contains the electronics needed to transmit and receive data. Most IoT devices contain a wireless transceiver, capable of communication using Wi-Fi, ZigBee, or some other wireless scheme.
* **Radio-Frequency Identification (RFID)**: (RFID) technology, which uses radio waves to identify items, is increasingly becoming an enabling technology for IoT. The main elements of an RFID system are tags and readers. RFID tags are small programmable devices used for object, animal, and human tracking. They come in a variety of shapes, sizes, functionalities, and costs. RFID readers acquire and sometimes rewrite information stored on RFID tags that come within operating range (a
* few inches up to several feet). Readers are usually connected to a computer system that records and formats the acquired information for further uses.

1. What is the IoT security framework?

* Cisco has developed a framework for IoT security that serves as a useful guide to the security requirements for IoT.