Homework #7

CECS 378 – Spring 2021 Cappel
Due: Wednesday, May 5th by 11:59 PM
Sergio Vasquez

Chapter 12 – Operating System Security

1. What are the basic steps needed in the process of securing a system?
    a. Assess risks and plan the system deployment
    b. Secure the underlying operating system and then they key applications
    c. Ensure any critical content is secured
    d. Ensure appropriate network protection mechanisms are used
    e. Ensure appropriate processes are used to maintain security
2. What are the basic steps needed to secure the base operating system?
    a. Install and patch operating system
    b. Harden and configure the operating system to adequately address the identified security needs of the system by:
        i. Removing unnecessary services, applications, and protocols
        ii. Configuring users, groups, and permissions
        iii. Configuring resource controls
    c. Install and configure additional security controls, such as anti-virus, host-based firewalls, and intrusion detection system(IDS)
    d. Test the security of the basic operating system to ensure that the steps taken adequately address its security needs.
3. What are the pros and cons of automated patching?
    a. Pros: Minimizes window of vulnerabilities that are exploited to the attackers.
    b. Cons:
        i. The entire system might be crashed if something goes wrong with the patching

ii. The patching sometimes introduce instability, if the patching is not done properly then the system can be unstable

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

    a. consequence both of the multiple operating systems executing side by side.

    b. Both of the presence of the virtualized environment and hypervisor as a layer below the operating system kernels and the security services they provide

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

    a. Logging is important because it ensure that in the event of a system breach or failure, system administrators can more quickly and accurately identify what happened and thus most effectively focus their remediation and recovery efforts.

    b. Its limitations as a security control:

        i. If the desired logs are monitor closely, it will provides an early warning of failures or attacks in development

        ii. Besides, the desired logs only capture the given level of detail which ranges from the maximums detail to none

    c. Pros and cons:

        i. Pros:

            1. Detect the failure quickly in order to recover it from a system crash

            2. Analyze a security incident

        ii. Cons:

            1. The remote logging will not perform if the server goes down

            2. Cause the slow of system since remote logging execute heavy complication jobs.

Chapter 13 – Cloud & IoT Security

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

On-demand self-services:
The Cloud computing services does not require any human administrators, user themselves are able to provision, monitor and manage computing resources as needed.

1.Broad network access:

The Computing services are generally provided over standard networks and heterogeneous devices.

2.Rapid elasticity:

The Computing services should have IT resources that are able to scale out and in quickly and on as needed basis. Whenever the user require services it is provided to him and it is scale out as soon as its requirement gets over.

3.Resource pooling:

The IT resource (e.g., networks, servers, storage, applications, and services) present are shared across multiple applications and occupant in an uncommitted manner. Multiple clients are provided service from a same physical resource.

4.Measured service:

The resource utilization is tracked for each application and occupant, it will provide both the user and the resource provider with an account of what has been used. This is done for various reasons like monitoring billing and effective use of resource.

7. List and briefly define three cloud service models.

Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) is a self-service model for managing remote data center infrastructures. IaaS provides virtualized computing resources over the Internet hosted by a third party such as Amazon Web Services, Microsoft Azure or Google. Instead of an organization purchasing hardware, companies purchase IaaS based on a consumption model. It is like buying electricity. You only pay for what you use

Platform as a Service (PaaS)

Platform as a Service (PaaS) allows organizations to build, run and manage applications without the IT infrastructure. This makes it easier and faster to develop, test and deploy applications.

Software as a Service (SaaS)

Software as a service (SaaS) replaces the traditional on-device software with software that is licensed on a subscription basis.

8. 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 multi-tenant 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.

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.

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

Sensor
Actuator
Microcontroller
Transceiver
Radio-frequency Identification (RFID)

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.

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.

The "smart" in a smart device is provided by a deeply embedded microcontroller.

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.

(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.

10. What is the IoT security framework?

The IoT model is a simplified version of the World Forum IoT Reference Model. It consists of the following levels:

Smart objects/embedded systems
Fog/edge network
Core network
Data center/cloud