Security Architecture and Engineering

Implement and manage engineering processes using secure design principles

Designing and managing secure computer systems breaks out into 4 layers: hardware, kernel and device drivers, operating system, applications. Perimeter defenses is physical security. There should be multiple layers of defense at each component that needs to be protected.

Understand the fundamental concepts of security models

- Access control and least privilege - Bella-lapadula model
- Complex environments - Lattice-based access control
- Integirty - Biba Model, Clark-Wilson
- Conflict of Interest - Chinese Wall Model

Select controls based upon systems security requirements

NIST document for selecing controls Generally a framework is used to categorize the information system or business, and then it will tell you which controls or standards are applicable.

Understand security capabilities of information systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

- Access control - ring model is used. Ring 3 is user, ring 0 is Kernel.
- Memory Protection - prevents a program from affecting the integrity, availability, and confidentiality from another
- TPM - a processor at harware level that allows computer to do cryptographic operations. If TPM, can do secure boot and full disk encryption
- Encryption - can provide confidentiality and integrity depending on type of cryptography used

Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

- Client-based systems - when user downloads content or has a vulnerable browser on a malicious website
- Server-based systems - clients attacking systems accepting connections/commands
- Database systems - data mining, polyinstantiation, inference and aggregation
- Cryptographic systems - weak IV, key size, key exchange, or symetric encryption algorithm used. good crypto is mathematically difficult
- Industrial Control Systems (ICS) - generic term that refers to anything from a thermostat to a chemical processing monitor
- Cloud-based systems - A company that stands up several servers for outsourcing. Pay them money to get the below examples
    - Infrastructure as a Service(IaaS)=Linux Server Hosting
    - Platform as a Service(PaaS)=Web Service hosting
    - Software as a Service(SaaS)=Web mail

- Distributed systems - use lots of devices that aren't necessarly high performance. think Docker swarm or beowolf cluster
- Internet of Things (IoT) - embedded systems that do only set few things. Smart TV, fridge, thermostat, etc. often built on linux kernel, has libraries that alow basic functionality like ping, store data, and query APIs.

Assess and mitigate vulnerabilities in web-based systems

Types of code run in web browsers

- Applets - small pieces of mobile code embedded in web browsers to display content. executables that are run locally. write them in java.
- Java script - scripts that can be embedded in web pages to make your browser do certain things. everyone uses java script
- DOM/CSS - There are DOM/CSS vulnerabilities you have to watch out for. attackers can inject their own code here.
- ActiveX - same as applets but use digital certificates instead of sandbox like java. microsoft only

Want to fix?

- Look at OWASP. See if any of your web app is vulnerable of the things. scan it with OWASP ZAP.
- Update hosting software. use secure libraries. follow OWASP rules. use a static analysis tool. run OWASP zap on it. update web browser.

Types of Vulns?

- Web hosting software vulns
- hard coded credentials
- inpropper permissions and redirects
- badauthentication
- bad session management
- bad encryption
- SQL injection
- cross site scripting (XSS)
- cross site forgery requests
- local/remote file inclusion
- API information disclosure

Assess and mitigate vulnerabilities in mobile systems

Mobile devices are actually a real problem. Should manage them with "mobile device manager" to push policies out. Can also remotely wipe them, and put full disk encryption on them.

Assess and mitigate vulnerabilities in embedded devices

Should see what track the device flows across the network. See if you can connect to any ports. See if they have any CVEs or a security program for their products.

Apply cryptography

OWASP CHEATSHEET LINK

- Cryptographic life cycle (e.g., key management, algorithm selection)
    - key management: how are you going to store all of your private/public keys? are there backups? who do you trust
    - algorithm selection: need to know if you need CIA? Speed? How much strength do you need?
- Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves)
    - symmetric: one key that encrypts and decrpts
    - asymmetric: each person has their own public and private key. Private decrypts, public encrypts
    - elliptic cures: a type of math model used to gennerate commputationally difficult private/public key pairs
- Public Key Infrastructure (PKI) - leverages all three forms of encryption to provide and manage digital certificates. Users have confidentiality, integrity, non-repudiation
- Key management practices: Have certificate authority for managaging and signing certificates
- Digital signatures - uniquely represents who someone is
- Non-repudiation - can't deny that you did something
- Integrity (e.g., hashing) - proving that the data hasn't been altered
- Understand methods of cryptanalytic attacks - analyzing initilzation vectors, key exchanges, symmetric encryption, etc for weaknesses that could be exploited
- Digital Rights Management (DRM) - systematic approach for protecting digital rights

Apply security principles to site and facility design

Need to know about physical security like: doors, locks, walls, fences, lights, guards, badges, gates, man traps, sensors, alarms, seucrely failing, emergency protocols.

Implement site and facility security controls

- Wiring closets/intermediate distribution facilities -
- Server rooms/data centers - could need shielded racks, cabling, seperation of equipment, locks, temperator monitors
- Media storage facilities - encryption
- Evidence storage - classification and access control
- Restricted and work area security
- Utilities and Heating, Ventilation, and Air Conditioning (HVAC)
- Environmental issues
- Fire prevention, detection, and suppression - know which fire extenguishers put out different fires

Home Page
To next domain! - D4 - Communication and Networking Security