# CompTia Notes: Application, Data, and Host Security

* Application Security Controls and Techniques
  + Fuzzing
    - Trying to crash a program by putting in random data over and over again
    - Kali-Linux, CERT BFF
  + Kali Linux and Pen Testing Tools
    - Install on VMWare and explore applications
  + Secure Coding Concepts
    - Balance between time to market and security
    - Input validation
      * Sanitize and validate
      * Mitigate attacks via XSS
      * OWASP and CERT
  + XSS and XSRF
  + Application Baseline Configuration and Application Hardening
    - Everything is up to date and patched
    - All unnecessary features, ports, services, etc. are disabled and removed
  + Multi-tiered Approach and Application Patching
    - 2 tier: client and database
    - 3 tier: client, webserver, database server
    - Applications should be routinely patched as part of a monthly maintenance cycle, as well as able to be manually patched if necessary
  + SQL vs. NoSQL databases
    - Table of related data
    - NoSQL is good for big data, mongoDB, Google BigTable , non-relational or distributed database, document based, key value pairs, graph,
  + Server-side vs. Client-side validation
    - Client-side is faster than server side
    - Can be bypassed by disabling JavaScript in the browser or intercepting HTTP post and modifying before its sent to the server
    - Server-side talks longer but is more secure as it can’t be bypassed by the client
* Mobile Security concepts and Technologies
  + Device Security
    - Challenges:
      * Full Device Encryption
      * Remote Wiping
      * Lockout
      * GPS
      * Storage segmentation
      * Things getting lost/stolen
      * Being compromised on public Wi-Fi
      * Asset tracking
      * Application management
    - Things like airwatch and mobile iron allow you to partition off a piece of a laptop or phone to be under corporate control. Makes it easier to BYOD and for corporate to control just what they need to.
    - Require strong passwords, constantly enabled and required
  + Key Credential Management and Authentication
    - Manage device content, access and authentication is critical to providing a secure environment
    - Digital certificates are used to authenticate users to access resources.
    - Allows certificate to be revoked if user leaves company, gets phone stolen, etc.
  + Geo-tagging
    - Pictures are geotagged when taken on most devices
    - Shows where phone has been, could be problematic when photos are uploaded to other websites
  + Transitive Trusts
    - A=B and B = C then A = C
    - If we allow this, we must make sure all transitive trusts are secure
  + BYOD Concerns
    - Data ownership
    - Support ownership
    - Patch management
    - Must have a clearly defined agreement with the employee
    - Forensics
    - Antivirus management
    - On-boarding/off-boarding
    - Infrastructure considerations
    - Legal concerns
    - Acceptable use policy
* Establishing Host Security
  + Operating System Security and Settings
    - Patch
    - Disable unnecessary applications
    - Disable unnecessary services
    - Enable Firewall, possibly set up extra firewalls
  + OS Hardening
  + Patch Management
  + White Listing and Black Listing Applications
  + Trusted OS
    - Evaluation Assurance levels are on a scale of 1 to 7
    - Most OS are at 4 for commercial use
    - Higher EAL is more secure
  + Host Based Firewalls
    - ZoneAlarm will allow you to see all the different types of connections going in and out of a network
  + Host Based Intrusion Detection
  + Hardware Security
  + Host Software Baselining and Virtualization
    - Can use VMWare to take snapshots of OS and can be saved
    - Can be used for testing upgrades, patches, and adjustments to the OS, applications or settings
    - Makes restoration very easy
    - Can do P2v (physical to virtual) to clone systems
    - Times to use it:
      * Testing Patch Compatibility
      * Regression testing
      * Better host availability/ elasticity
      * Test scale, see what happens when use goes up
      * Makes isolated environment (sandbox) to test when viruses get introduces to the system
* Appropriate Controls to Ensure Data Security
  + Cloud Storage
    - Ensure that the cloud service you use has good security
  + Storage Area Networks
    - External Fiber Channel, ISCSI, or FCoE
    - Appears as a local storage to the host
    - Zoning and masking creates security boundaries, only shows whose WWNs are in the zone can see the storage
  + Data Encryption
    - Full Disk
      * Data at Rest Encryption encrypts the entire contents of a hard disk to prevent access without proper credentials
    - Database
      * Transparent Data Encryption encrypts the contents of an individual database (data at rest)
      * Cell Level encryption encrypts individual cells (data at rest and in transit)
    - Individual Files
    - Removable Media
    - Mobile Devices
      * Can be encrypted locally and via a VPN and SSL
  + Hardware Based Encryption
    - TPM: Trusted Platform Module, built in
    - HSM: Hardware Security Module, can be external/added later
    - USB Encryption
    - Hard Drive, bitlocker
  + Types of Data to Secure
    - Data in transit
    - Data at rest
    - Data in use
  + Permissions/ALCs Data Policies
    - Access control lists
      * Only give as much access as required to do the task
      * Periodically audit to ensure compliance
  + Data Policies
    - Wiping
      * Policies should be in place to dictate how data is destroyed. Wiping could be 1-pass, 3 –pass, 7-pass etc
    - Disposing
      * Drives should be wiped or degaussed before disposal
    - Retention
      * Varies by company/industry.
    - Storage
      * Policies can include where data is stored, i.e. locally, remotely, SAN, NAS, off-site, cloud, etc.
      * If stored using a cloud provider, where the data is replicated should be documented and approved as well.
* Mitigate Security Risks in Static Environments
  + SCADA Systems
    - Supervisory Control and Data Acquisition
    - Usually refer to centralized systems which monitor and control entire sites, or complexes of systems spread out over large areas
    - RTU: Remote Terminal Unit, connects to sensors that convert the sensor information to digital data (pipe pressure)
    - PLC: Programmable logic Controller, similar to RTU, more versatile
    - HMI: Human machine interface, presents data to a human who then acts upon it
    - MTU: Master Terminal Unit, aggregates all data
    - Used to be closed off, progression:
      * Monolithic
      * Distributed
      * Networked
      * Internet of Things
    - These attacks can be used to degrade or destroy critical infrastructure
  + Embedded Systems, Printers, Smart TV’s and HVAC systems
    - Embedded systems can be exploited to get into a network
  + Mobile Operating Systems
    - iOS has tight control on development, compared to Android
    - Very few viruses /malwares
    - Runs on only Apple hardware
  + Main frames
    - Specialized hardware/software
    - Attacks are usually very specific and generated internally (not large attack area)
    - Most Viruses/malware are targeted at PC/Servers, not mainframe systems,
    - Much smaller worldwide footprint
  + Game Consoles
    - Full-blown computers running specialized versions of Microsoft Windows and Linux
    - Security concerns to do inability to patch manually or customize features
    - Newer systems have cameras and microphones to capture video and speech
  + In-vehicle Computing Systems
    - Always on and connected
    - Can track location, speed, travel history, etc.
    - Myriad of in-vehicle metrics
    - Remote access and control of vehicle features (get text messages through car)
    - It’s possible to start a vehicle, or disable it remotely
    - Must coach employees to stay updated patches
  + Network segmentation
    - Segment network to separate management network from data network
    - Separate networks that contain PII
    - Use firewalls to break up networks
  + Security Layers and Manual Updates’
    - Each layer of security adds more hurdles for an attacker to have to get through
    - Network and host intrusion detection and prevention systems
    - Application and network firewalls
    - Physical as well as technological controls
    - Application Firewalls can block and filter traffic and look for specific commands within an application
  + Firmware version control
    - Target adoption rate sets a percent of products that have installed a firmware update by a certain date.
  + Wrappers, Control Redundancy, and Diversity
    - TCP wrappers used to filter traffic coming in and out. Can be used on embedded systems as well.
    - Control redundancy
      * Use multiple backup and failover systems from different vendors to ensure diversity