CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

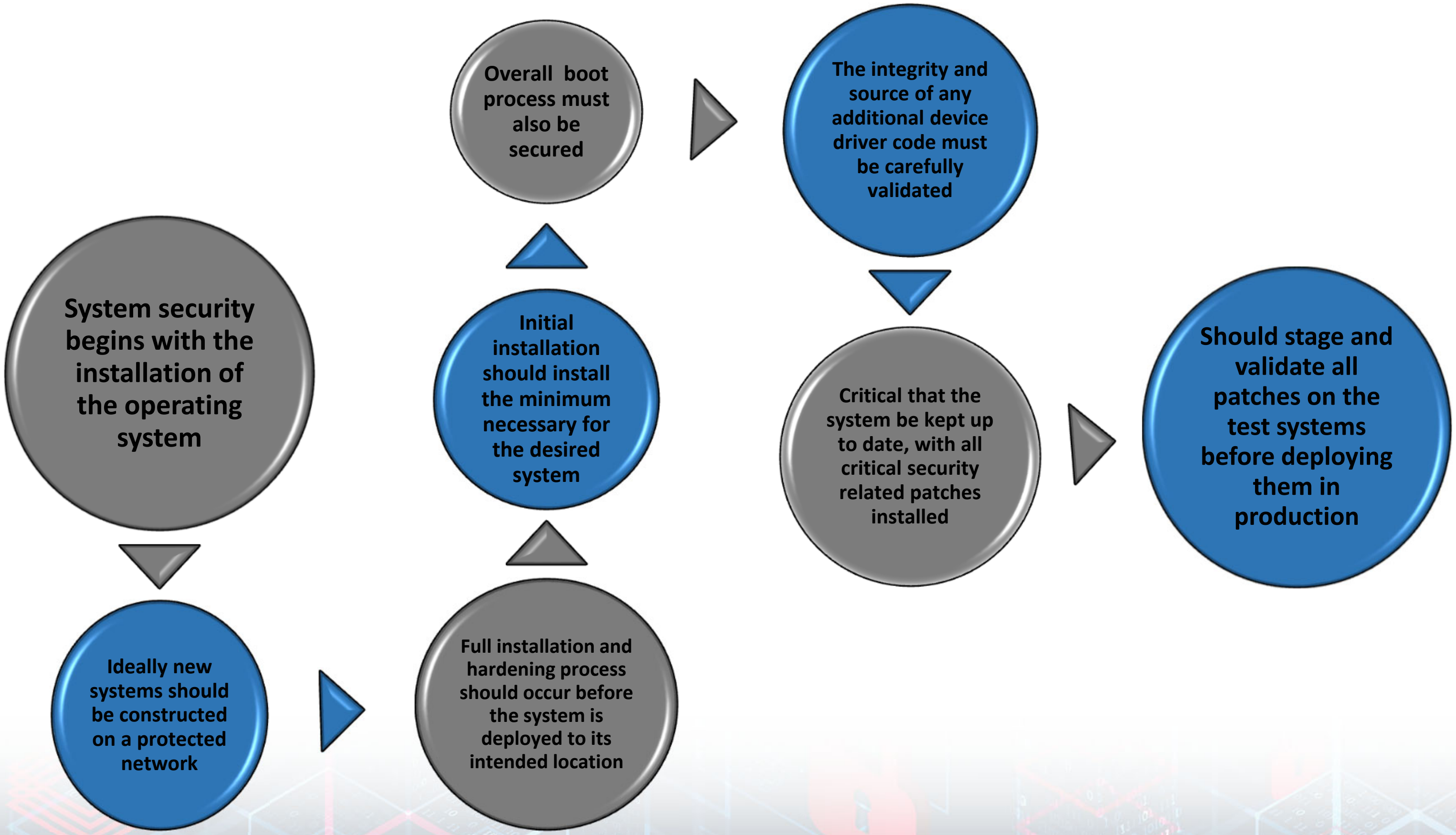
# User Authentication, Access Control, and Operating System

Operating System Security

# Video Summary

- OS Initial Setup and Patching
- OS Application Configuration
- Encryption Technology
- Security Maintenance
- Logging and Backup

# Initial Setup and Patching



System security begins with the installation of the operating system

Ideally new systems should be constructed on a protected network

Full installation and hardening process should occur before the system is deployed to its intended location

Initial installation should install the minimum necessary for the desired system

Overall boot process must also be secured

The integrity and source of any additional device driver code must be carefully validated

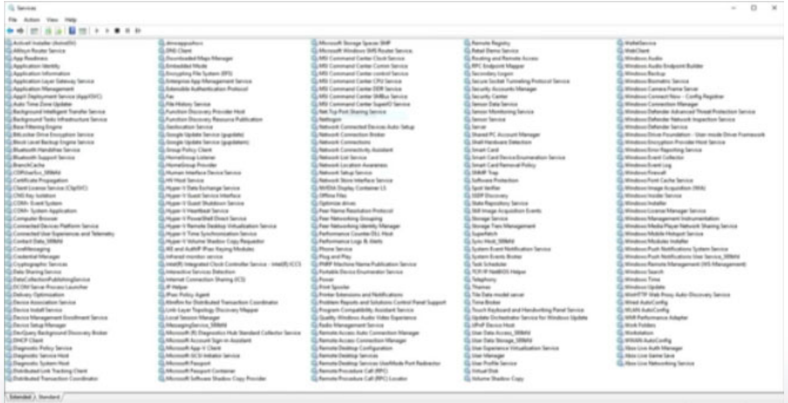
Critical that the system be kept up to date, with all critical security related patches installed

Should stage and validate all patches on the test systems before deploying them in production

# Remove Unnecessary Services, Applications, Protocols

- When performing the initial installation the supplied **<u>defaults should not be used</u>**
  - Default configuration is set to maximize ease of use and functionality rather than security
  - Windows 10 has over 240 services by default
  - If additional packages are needed later they can be installed when they are required

- If **<u>fewer software packages</u>** are available to run the risk is reduced



ActiveX Installer (AxInstSV)
AllJoyn Router Service
App Readiness
Application Identity
Application Information
Application Layer Gateway Service
Application Management
AppX Deployment Service (AppXSVC)
Auto Time Zone Updater
Background Intelligent Transfer Service
Background Tasks Infrastructure Service
Base Filtering Engine
BitLocker Drive Encryption Service
Block Level Backup Engine Service
Bluetooth Handsfree Service
Bluetooth Support Service
BranchCache
CDPUserSvc_[illegible]
Certificate Propagation
Client License Service (ClipSVC)
CNG Key Isolation
COM+ Event System
COM+ System Application
Computer Browser
Connected Devices Platform Service
Connected User Experiences and Telemetry
Contact Data_[illegible]
CoreMessaging
Credential Manager
Cryptographic Services
Data Sharing Service
DataCollectionPublishingService
DCOM Server Process Launcher
Delivery Optimization
Device Association Service
Device Install Service
Device Management Enrollment Service
Device Setup Manager
DevQuery Background Discovery Broker
DHCP Client
Diagnostic Policy Service
Diagnostic Service Host
Diagnostic System Host
Distributed Link Tracking Client
Distributed Transaction Coordinator
dmwappushsvc
DNS Client
Downloaded Maps Manager
Embedded Mode
Encrypting File System (EFS)
Enterprise App Management Service
Extensible Authentication Protocol
Fax
File History Service
Function Discovery Provider Host
Function Discovery Resource Publication
Geolocation Service
Google Update Service (gupdate)
Google Update Service (gupdatem)
Group Policy Client
HomeGroup Listener
HomeGroup Provider
Human Interface Device Service
HV Host Service
Hyper-V Data Exchange Service
Hyper-V Guest Service Interface
Hyper-V Guest Shutdown Service
Hyper-V Heartbeat Service
Hyper-V PowerShell Direct Service
Hyper-V Remote Desktop Virtualization Service
Hyper-V Time Synchronization Service
Hyper-V Volume Shadow Copy Requestor
IKE and AuthIP IPsec Keying Modules
Infrared monitor service
Intel(R) Integrated Clock Controller Service - Intel(R) ICCS
Interactive Services Detection
Internet Connection Sharing (ICS)
IP Helper
IPsec Policy Agent
KtmRm for Distributed Transaction Coordinator
Link-Layer Topology Discovery Mapper
Local Session Manager
MessagingService_[illegible]
Microsoft (R) Diagnostics Hub Standard Collector Service
Microsoft Account Sign-in Assistant
Microsoft App-V Client
Microsoft iSCSI Initiator Service
Microsoft Passport
Microsoft Passport Container
Microsoft Software Shadow Copy Provider
Microsoft Storage Spaces SMP
Microsoft Windows SMS Router Service.
MSI Command Center Clock Service
MSI Command Center Comm Service
MSI Command Center control Service
MSI Command Center CPU Service
MSI Command Center DDR Service
MSI Command Center SMBus Service
MSI Command Center SuperIO Service
Net.Tcp Port Sharing Service
Netlogon
Network Connected Devices Auto-Setup
Network Connection Broker
Network Connections
Network Connectivity Assistant
Network List Service
Network Location Awareness
Network Setup Service
Network Store Interface Service
NVIDIA Display Container LS
Offline Files
Optimize drives
Peer Name Resolution Protocol
Peer Networking Grouping
Peer Networking Identity Manager
Performance Counter DLL Host
Performance Logs & Alerts
Phone Service
Plug and Play
PNRP Machine Name Publication Service
Portable Device Enumerator Service
Power
Print Spooler
Printer Extensions and Notifications
Problem Reports and Solutions Control Panel Support
Program Compatibility Assistant Service
Quality Windows Audio Video Experience
Radio Management Service
Remote Access Auto Connection Manager
Remote Access Connection Manager
Remote Desktop Configuration
Remote Desktop Services
Remote Desktop Services UserMode Port Redirector
Remote Procedure Call (RPC)
Remote Procedure Call (RPC) Locator
Remote Registry
Retail Demo Service
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Accounts Manager
Security Center
Sensor Data Service
Sensor Monitoring Service
Sensor Service
Server
Shared PC Account Manager
Shell Hardware Detection
Smart Card
Smart Card Device Enumeration Service
Smart Card Removal Policy
SNMP Trap
Software Protection
Spot Verifier
SSDP Discovery
State Repository Service
Still Image Acquisition Events
Storage Service
Storage Tiers Management
Superfetch
Sync Host_[illegible]
System Event Notification Service
System Events Broker
Task Scheduler
TCP/IP NetBIOS Helper
Telephony
Themes
Tile Data model server
Time Broker
Touch Keyboard and Handwriting Panel Service
Update Orchestrator Service for Windows Update
UPnP Device Host
User Data Access_[illegible]
User Data Storage_[illegible]
User Experience Virtualization Service
User Manager
User Profile Service
Virtual Disk
Volume Shadow Copy
WalletService
WebClient
Windows Audio
Windows Audio Endpoint Builder
Windows Backup
Windows Biometric Service
Windows Camera Frame Server
Windows Connect Now - Config Registrar
Windows Connection Manager
Windows Defender Advanced Threat Protection Service
Windows Defender Network Inspection Service
Windows Defender Service
Windows Driver Foundation - User-mode Driver Framework
Windows Encryption Provider Host Service
Windows Error Reporting Service
Windows Event Collector
Windows Event Log
Windows Firewall
Windows Font Cache Service
Windows Image Acquisition (WIA)
Windows Insider Service
Windows Installer
Windows License Manager Service
Windows Management Instrumentation
Windows Media Player Network Sharing Service
Windows Mobile Hotspot Service
Windows Modules Installer
Windows Push Notifications System Service
Windows Push Notifications User Service_[illegible]
Windows Remote Management (WS-Management)
Windows Search
Windows Time
Windows Update
WinHTTP Web Proxy Auto-Discovery Service
Wired AutoConfig
WLAN AutoConfig
WMI Performance Adapter
Work Folders
Workstation
WWAN AutoConfig
Xbox Live Auth Manager
Xbox Live Game Save
Xbox Live Networking Service

Access Control

## Configure Users, Groups, and Authentication

- Not all users with access to a system will have the same access to all data and resources on that system
- <u>**Elevated privileges**</u> should be restricted to only those users that require them, and then only when they are needed to perform a task

- **System planning process should consider:**
  - Categories of users on the system
  - Privileges they have
  - Types of information they can access
  - How and where they are defined and authenticated
- **Default accounts included as part of the system installation should be secured**
  - Those that are not required should be either removed or disabled
  - Policies that apply to authentication credentials configured

## Configure Resource Controls

- Once the users and groups are defined, appropriate **<u>permissions can be set on data and resources</u>**
- Many of the security hardening guides provide lists of recommended changes to the default access configuration

## Install Additional Security Controls

- Further security possible by installing and configuring additional security tools:
  - Anti-virus software
  - Host-based firewalls
  - IDS or IPS software
  - Application white-listing

# Test the System Security

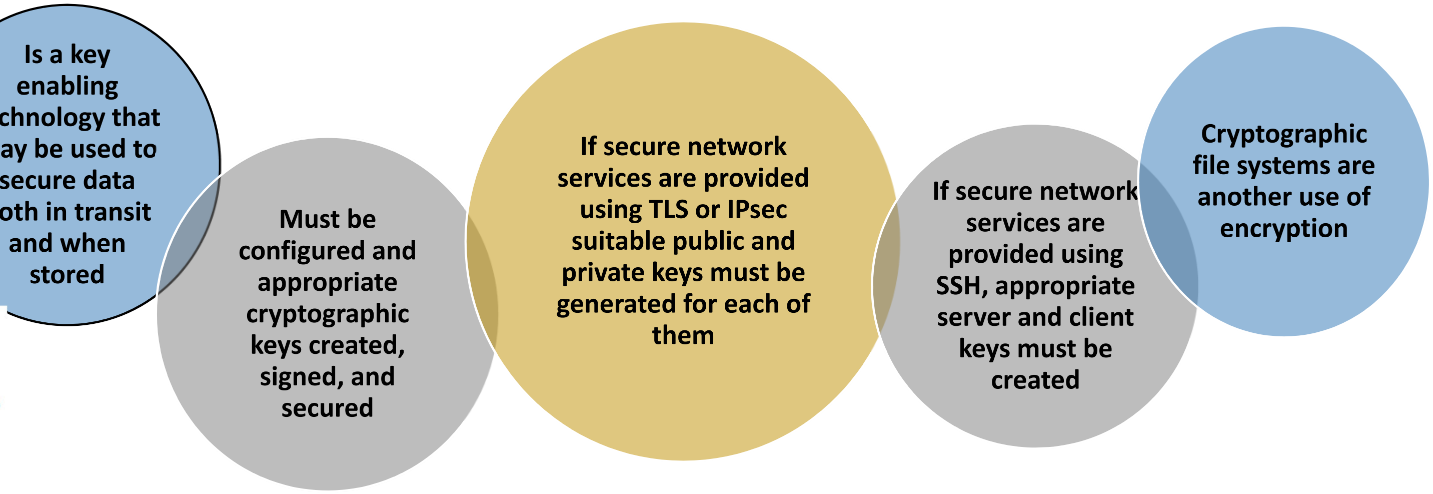
- Final step in the process of initially securing the base operating system is security testing
- Goal:
  - Ensure the previous security configuration steps are correctly implemented
  - Identify any possible vulnerabilities

- Checklists are included in security hardening guides
- There are programs specifically designed to:
  - Review a system to ensure that a system meets the basic security requirements
  - Scan for known vulnerabilities and poor configuration practices
- Should be done following the initial hardening of the system
- Repeated periodically as part of the security maintenance process

# Application Configuration

- Security policy can control app execution
  - Whitelisting and blacklisting
  - Whitelisting nothing run unless it’s approved (very restrictive)
  - Blacklisting everything run except those in the blacklist
  - This can be achieved using app hash of certificates (trusted publishers)
- Of particular concern with remotely accessed services such as Web and file transfer services
  - Risk from this form of attack is reduced by ensuring that most of the files can only be read, but not written, by the server

# Encryption Technology



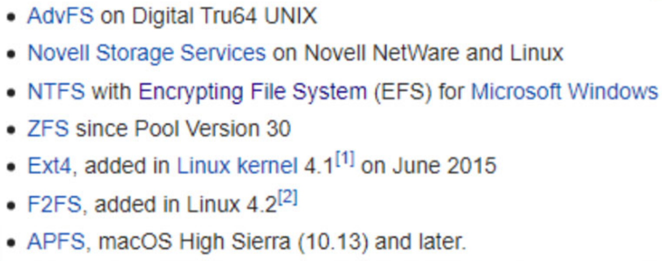
Is a key enabling technology that may be used to secure data both in transit and when stored

Must be configured and appropriate cryptographic keys created, signed, and secured

If secure network services are provided using TLS or IPsec suitable public and private keys must be generated for each of them

If secure network services are provided using SSH, appropriate server and client keys must be created

Cryptographic file systems are another use of encryption



- AdvFS on Digital Tru64 UNIX
- Novell Storage Services on Novell NetWare and Linux
- NTFS with Encrypting File System (EFS) for Microsoft Windows
- ZFS since Pool Version 30
- Ext4, added in Linux kernel 4.1[1] on June 2015
- F2FS, added in Linux 4.2[2]
- APFS, macOS High Sierra (10.13) and later.

# Security Maintenance

- Process of maintaining security is continuous
- Security maintenance includes:
  - Monitoring and analyzing logging information
  - Performing regular backups
  - Recovering from security compromises
  - Regularly testing system security
  - Using appropriate software maintenance processes to patch and update all critical software, and to monitor and revise configuration as needed

# Security Maintenance

- Process of maintaining security is continuous
- Example secure configuration policies:
  - Stay updated with the latest patches
  - Compromised systems are re-imaged (not cleaned)

# Logging

Can only inform you about bad things that have already happened

In the event of a system breach or failure, system administrators can more quickly identify what happened

Key is to ensure you capture the correct data and then appropriately monitor and analyze this data

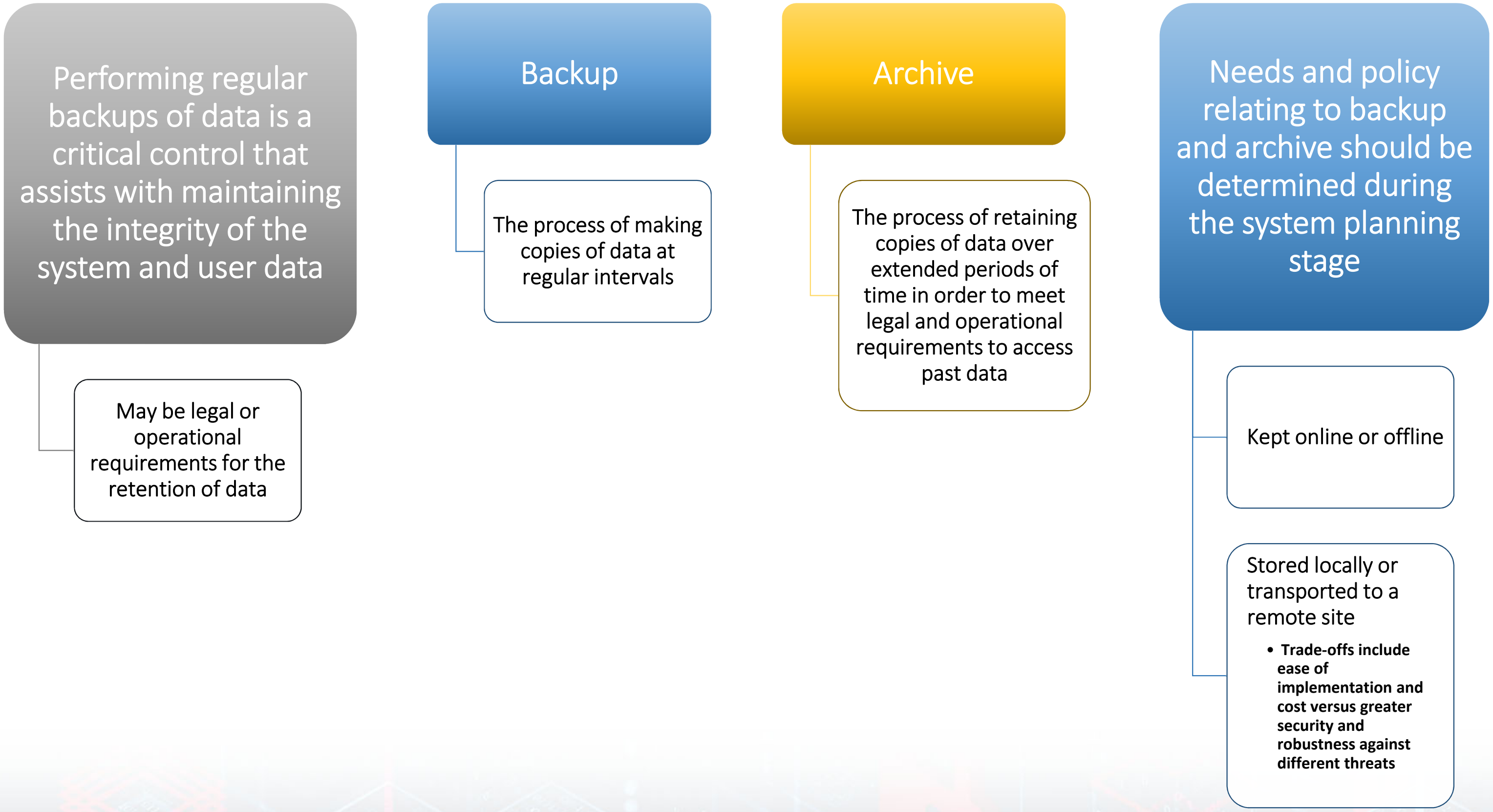
Information can be generated by the system, network and applications

Range of data acquired should be determined during the system planning stage

Generates significant volumes of information and it is important that sufficient space is allocated for them

Automated analysis is preferred

# Data Backup and Archive



Performing regular backups of data is a critical control that assists with maintaining the integrity of the system and user data

- May be legal or operational requirements for the retention of data

Backup

- The process of making copies of data at regular intervals

Archive

- The process of retaining copies of data over extended periods of time in order to meet legal and operational requirements to access past data

Needs and policy relating to backup and archive should be determined during the system planning stage

- Kept online or offline
- Stored locally or transported to a remote site
  - **Trade-offs include ease of implementation and cost versus greater security and robustness against different threats**

# Video Summary

- OS Initial Setup and Patching
- OS Application Configuration
- Encryption Technology
- Security Maintenance
- Logging and Backup