Lesson 12

Implementing Host Security Solutions

Topic 12A

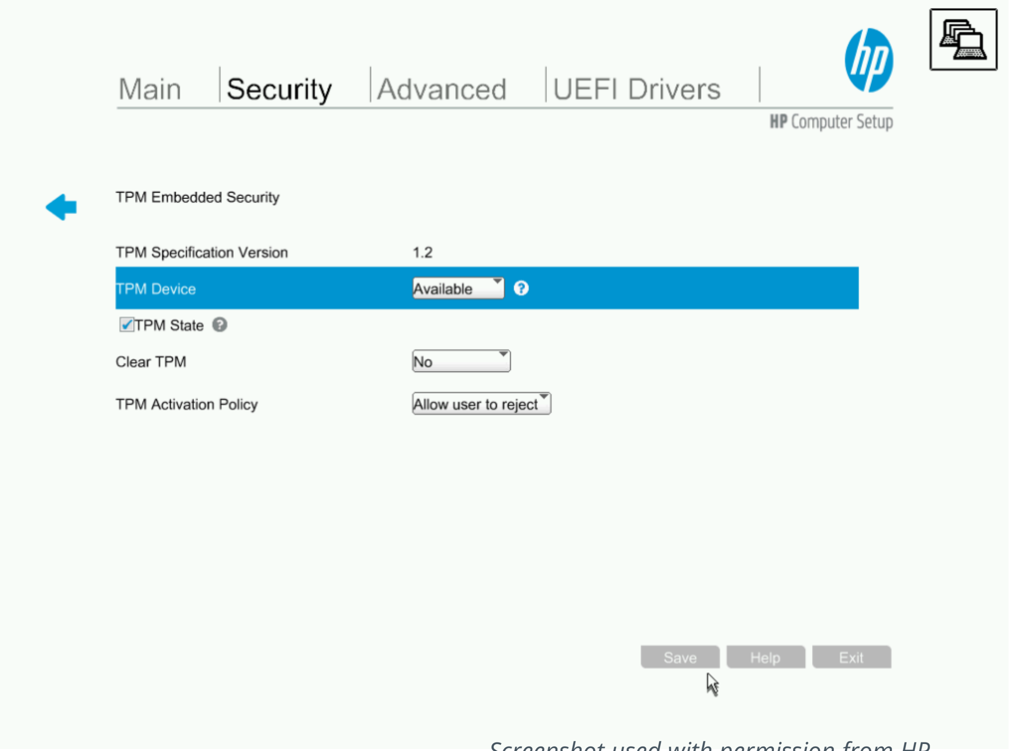
Implement Secure Firmware

Syllabus Objectives Covered

- 1.2 Given a scenario, analyze potential indicators to determine the type of attack
- 3.2 Given a scenario, implement host or application security solutions
- 5.3 Explain the importance of policies to organizational security

Hardware Root of Trust

- Hardware root of trust/trust anchor
- Attestation
- Trusted Platform Module (TPM)
  - Hardware-based storage of cryptographic data
  - Endorsement key
  - Subkeys used in key storage, signature, and encryption operations
  - Ownership secured via password



TPM Embedded Security

TPM Specification Version 1.2

TPM Device Available

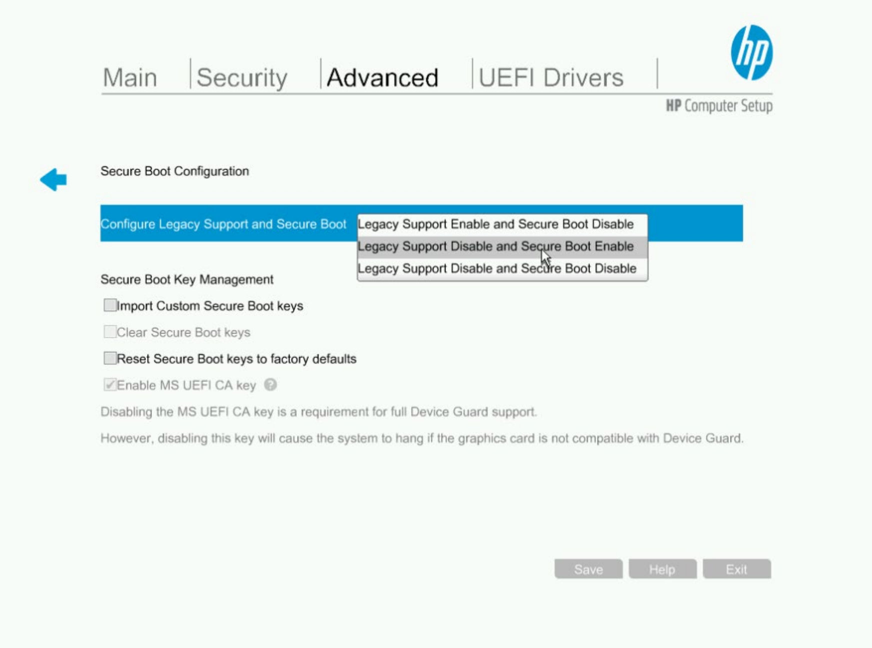
☑ TPM State

Clear TPM No

TPM Activation Policy Allow user to reject

Screenshot used with permission from HP.

Boot Integrity



Secure Boot Configuration

Configure Legacy Support and Secure Boot
- Legacy Support Enable and Secure Boot Disable
- Legacy Support Disable and Secure Boot Enable
- Legacy Support Disable and Secure Boot Disable

Secure Boot Key Management

☐ Import Custom Secure Boot keys

☐ Clear Secure Boot keys

☐ Reset Secure Boot keys to factory defaults

☑ Enable MS UEFI CA key

Disabling the MS UEFI CA key is a requirement for full Device Guard support.

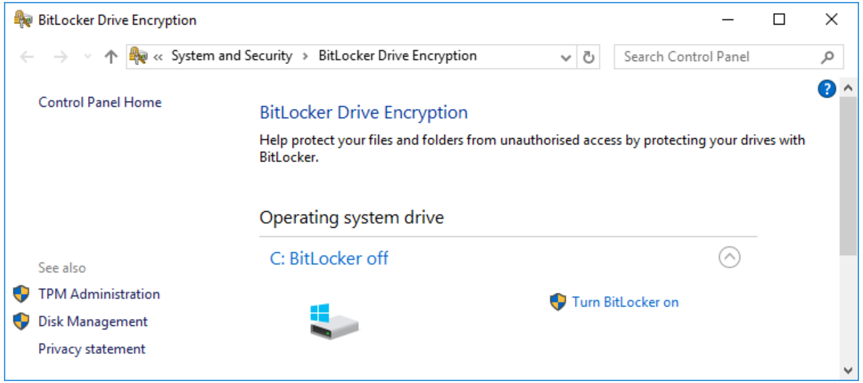
However, disabling this key will cause the system to hang if the graphics card is not compatible with Device Guard.

Screenshot used with permission from HP.

- Unified extensible firmware interface (UEFI)
- Secure boot
  - Validate digital signatures before running boot loader or OS kernel
- Measured boot
  - Use TPM to measure hashes of boot files at each stage
- Attestation
  - Report boot metrics and signatures to remote server

Drive Encryption

- Full disk encryption (FDE)
  - Encryption key secured with user password
  - Secure storage for key in TPM or USB thumb drive
- Self-encrypting drives (SED)
  - Data/media encryption key (DEK/MEK)
  - Authentication key (AK) or key encrypting key (KEK)
  - Opal specification compliant



BitLocker Drive Encryption

Help protect your files and folders from unauthorised access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Screenshot used with permission from Microsoft.

USB and Flash Drive Security

- BadUSB
    - Exposes potential of malicious firmware
    - Malicious USB cable
    - Malicious flash drive
- Sheep dip
    - Sandbox system for testing new/suspect devices
    - Isolated from production network/data

Third-party Risk Management

- Supply chain and vendors
  - End-to-end process of supplying, manufacturing, distributing, and finally releasing goods and services to a customer
  - Could malicious actors within supply chain introduce backdoor access via hardware/firmware components?
  - Most companies must depend on governments/security services to ensure trustworthiness of market suppliers
  - Consider implications of using second-hand equipment
- Vendors versus business partners

End of Life Systems and Lack of Vendor Support

- Support lifecycles
- End of life (EOL)
  - Product is no longer sold to new customers
  - Availability of spares and updates is reduced
- End of service life (EOSL)
  - Product is no longer supported
- Lack of vendor support
  - Abandonware
  - Software and peripherals/devices

Organizational Security Agreements

- Memorandum of understanding (MOU)
  - Intent to work together
- Business partnership agreement (BPA)
  - Establish a formal partner relationship
- Non-disclosure agreement (NDA)
  - Govern use and storage of shared confidential and private information
- Service level agreement (SLA)
  - Establish metrics for service delivery and performance
- Measurement systems analysis (MSA)
  - Evaluate data collection and statistical methods used for quality management

Topic 12B

Implement Endpoint Security

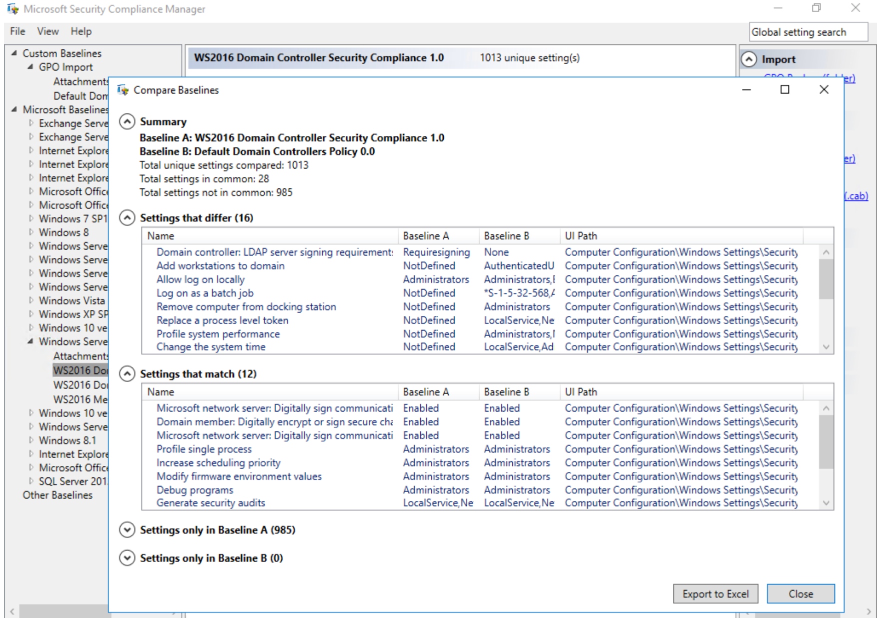
Syllabus Objectives Covered

- 3.2 Given a scenario, implement host or application security solutions

Host Hardening

- Reducing attack surface
- Interfaces
  - Network and peripheral connections and hardware ports
- Services
  - Software that allows client connections
- Application service ports
  - TCP and UDP ports
  - Disable application service or use firewall to control access
  - Detect non-standard usage
- Encryption for persistent storage

Baseline Configuration and Registry Settings



WS2016 Domain Controller Security Compliance 1.0 1013 unique setting(s)

Compare Baselines

Summary

Baseline A: WS2016 Domain Controller Security Compliance 1.0
Baseline B: Default Domain Controllers Policy 0.0
Total unique settings compared: 1013
Total settings in common: 28
Total settings not in common: 985

Settings that differ (16)

Name	Baseline A	Baseline B	UI Path
Domain controller: LDAP server signing requirement:	Requiresigning	None	Computer Configuration\Windows Settings\Security
Add workstations to domain	NotDefined	AuthenticatedU	Computer Configuration\Windows Settings\Security
Allow log on locally	Administrators	Administrators,I	Computer Configuration\Windows Settings\Security
Log on as a batch job	NotDefined	*S-1-5-32-568,A	Computer Configuration\Windows Settings\Security
Remove computer from docking station	NotDefined	Administrators	Computer Configuration\Windows Settings\Security
Replace a process level token	NotDefined	LocalService,Ne	Computer Configuration\Windows Settings\Security
Profile system performance	NotDefined	Administrators,I	Computer Configuration\Windows Settings\Security
Change the system time	NotDefined	LocalService,Ad	Computer Configuration\Windows Settings\Security

Settings that match (12)

Name	Baseline A	Baseline B	UI Path
Microsoft network server: Digitally sign communicati	Enabled	Enabled	Computer Configuration\Windows Settings\Security
Domain member: Digitally encrypt or sign secure cha	Enabled	Enabled	Computer Configuration\Windows Settings\Security
Microsoft network server: Digitally sign communicati	Enabled	Enabled	Computer Configuration\Windows Settings\Security
Profile single process	Administrators	Administrators	Computer Configuration\Windows Settings\Security
Increase scheduling priority	Administrators	Administrators	Computer Configuration\Windows Settings\Security
Modify firmware environment values	Administrators	Administrators	Computer Configuration\Windows Settings\Security
Debug programs	Administrators	Administrators	Computer Configuration\Windows Settings\Security
Generate security audits	LocalService,Ne	LocalService,Ne	Computer Configuration\Windows Settings\Security

Settings only in Baseline A (985)

Settings only in Baseline B (0)

Screenshot used with permission from Microsoft.

- OS/host role
  - Network appliance, server, client, …
- Configuration baseline template
- Registry settings and group policy objects (GPOs)
- Malicious registry changes
- Baseline deviation reporting

Patch Management

- All types of OS, application, and firmware code potentially contains vulnerabilities
- Patch management essential for mitigating these vulnerabilities as they are discovered
- Update policies and schedule
  - Apply all latest – auto-update
  - Only apply specific patches
  - Third-party patches
- Scheduling updates
- Managing unpatchable systems

Endpoint Protection

- Antivirus (A-V)/anti-malware
  - Signature-based detection of all malware/PUP types
- Host-based intrusion detection/prevention (HIDS/HIPS)
  - File integrity monitoring and log/network traffic scanning
  - Prevention products can block processes or network connections
- Endpoint Protection Platform (EPP)
  - Consolidate agents for multiple functions
  - Combine A-V, HIDS, host firewall, content filtering, encryption, ...
- Data loss prevention (DLP)
  - Block copy or transfer of confidential data
- Endpoint protection deployment

Next-Generation Endpoint Protection

- Endpoint detection and response (EDR)
  - Visibility and containment rather than preventing malware execution
  - User and entity behavior analytics driven by cloud-hosted machine learning
- Next-generation firewall integration
  - Use endpoint detection to alter network firewall policies
  - Block fileless threats and covert channels
  - Prevent lateral movement

Antivirus Response

- Signature-based detection and heuristics
- Malware identification and classification
  - Common Malware Enumeration (CME)
- Manual remediation advice
- Advanced malware tools
  - Manually identify file system changes and network activity
- Sandboxing
  - Execute malware for analysis in a protected environment

Topic 12C

Explain Embedded System Security Implications

Syllabus Objectives Covered

- 2.6 Explain the security implications of embedded and specialized systems

Embedded Systems

- Computer system with dedicated function
- Static environment
- Cost, power, and compute constraints
  - Single-purpose devices with no overhead for additional security computing
- Crypto, authentication, and implied trust constraints
  - Limited resource for cryptographic implementation
  - No root of trust
  - Perimeter security
- Network and range constraints
  - Power constrains range
  - Emphasize low data rates, but minimize latency

Logic Controllers for Embedded Systems

- Programmable logic controller (PLC)
- System on chip (SoC)
  - Processors, controllers, and devices all provided on single package
  - Raspberry Pi
  - Arduino
- Field programmable gate array (FPGA)
  - End customer can configure programming logic
- Real-time operating system (RTOS)
  - Designed to be ultra-stable
  - Prioritizes real-time scheduling

Embedded Systems Communications Considerations

- Operational Technology (OT) networks
  - Serial data and Industrial Ethernet
- Cellular networks/baseband radio
  - Narrowband-IoT (NB-IoT)
  - LTE Machine Type Communication (LTE-M)
  - 4G versus 5G
  - Subscriber identity module (SIM) cards
  - Encryption and backhaul
- Z-Wave and Zigbee
  - Low-power wireless over ~900 MHz and 2.4 GHz
  - Encryption and pairing

Industrial Control Systems (1)

- Availability, integrity, confidentiality (AIC triad)
- Workflow and process automation
  - Industrial control systems (ICSs)
  - Plant devices and embedded PLCs
  - OT network
  - Electromechanical components and sensors
  - Human machine interface (HMI)
  - Data historian
- Supervisory Control and Data Acquisition (SCADA)
  - Runs on PCs to gather data and perform monitoring
  - Manage large-scale, multiple site installations over WAN communications

Industrial Control Systems (2)

- Energy
  - Power generation and distribution
- Industrial
  - Mining and refining raw materials
- Fabrication and manufacturing
  - Creating components and assembling them into products
- Logistics
  - Moving things
- Facilities
  - Site and building management systems
  - Heating, ventilation, and air conditioning (HVAC)

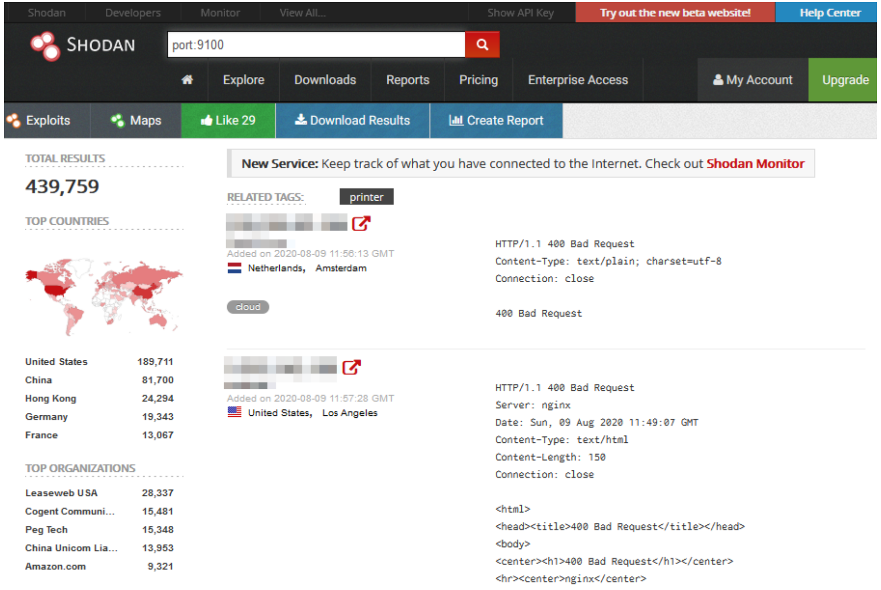
Internet of Things

- Machine to Machine (M2M) communication
- Hub/control system
  - Communications hub
  - Control system for headless devices
  - Smart hubs and PC/smartphone controller apps
- Smart devices
  - IoT endpoints
  - Compute, storage, and network functions and vulnerabilities
- Wearables
- Sensors
- Vendor security management
  - Weak defaults
  - Patching and updates

Specialized Systems for Facility Automation

- Building automation system (BAS)
  - Smart buildings
  - Process and memory vulnerabilities
  - Credentials embedded in application code
  - Code injection
- Smart meters
- Surveillance systems
  - Physical access control system (PACS)
  - Risks from third-party provision
  - Abuse of cameras

Specialized Systems in IT



TOTAL RESULTS

439,759

TOP COUNTRIES

United States	189,711
China	81,700
Hong Kong	24,294
Germany	19,343
France	13,067

TOP ORGANIZATIONS

Leaseweb USA	28,337
Cogent Communi...	15,481
Peg Tech	15,348
China Unicom Lia...	13,953
Amazon.com	9,321

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

RELATED TAGS: printer

[redacted]

Added on 2020-08-09 11:56:13 GMT

Netherlands, Amsterdam

cloud

```
HTTP/1.1 400 Bad Request
Content-Type: text/plain; charset=utf-8
Connection: close

400 Bad Request
```

[redacted]

Added on 2020-08-09 11:57:28 GMT

United States, Los Angeles

```
HTTP/1.1 400 Bad Request
Server: nginx
Date: Sun, 09 Aug 2020 11:49:07 GMT
Content-Type: text/html
Content-Length: 150
Connection: close

<html>
<head><title>400 Bad Request</title></head>
<body>
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx</center>
```

Screenshot used with permission from shodan.io.

- Multifunction printer (MFP)
  - Hard drives and firmware represent potential vulnerabilities
  - Recovery of confidential information from cached print files
  - Log data might assist attacks
  - Pivot to compromise other network devices
- Voice over IP
- Shodan

Specialized Systems for Vehicles and Drones

- Unmanned Aerial Vehicles (UAV)/drones
- Computer-controlled or assisted engine, steering, and brakes
- In-vehicle entertainment and navigation
- Controller area network (CAN) serial communications buses
    - Onboard Diagnostics (OBD-II) module
    - Access via cellular or Wi-Fi

Specialized Systems for Medical Devices

- Used in hospitals and clinics but also at home by patients
- Potentially unsecure protocols and control systems
- Use compromised devices to pivot to networks
  - Stealing Protected Health Information (PHI)
- Ransom by threatening to disrupt services
- Kill or injure patients

Security for Embedded Systems

- Network segmentation
    - Strictly restrict access to OT networks
    - Increased monitoring for SCADA hosts
- Wrappers
    - Use IPSec for authentication and integrity and confidentiality
- Firmware code control
    - Supply chain risks
- Inability to patch
    - Inadequate vendor support
    - Time-consuming patch procedures
    - Inability to schedule downtime

Lesson 12

Summary