IT Maturity Models

- Successful organizations are based on effective and efficient IT processes
- Assess the IT environment using and IT maturity model
  - Where are we now?
  - Where do we want to be?

IT Maturity Models

- People
- Processes
- Technology

Capability Maturity Model Integration (CMMI)

CMMI capability and performance levels

1. Initial state: lack of process efficiency
2. Managed: configuration management, controlled service delivery
3. Defined: policies – incident response, security, disaster recovery, user training, and risk management
4. Quantitative management: baselines, performance metrics, alignment to business objectives
5. Optimization: continuous process improvement

IT Maturity Assessment

- Identify gaps between current and desired state
- Determine direction to take to reach desired state
- Example
  - IT hardware and software procurement and management takes too long and costs too much
  - Consider outsourcing to a public cloud provider

Organizational Security Policies

- Driven by
  - Laws, regulations, and contractual obligations
  - Alignment with business objectives
- User awareness and training
  - Scams and other threats
  - Acceptable use policies

Organizational Security Policies

Issues addressed

- Allowable use of technology
- Definition of conflict of interest
- Auditing of system and data access
- Reduced legal liability
- Counters reputation loss
- Where responsibility falls

Organizational Security Policies Types

Data privacy	VPN
E-mail	Web browsing
Social media use	Equipment disposal
Malware scanning	Building access
Incident response	Data classification
Web server configuration	Database server configuration
Mobile device user onboarding	User station reimaging

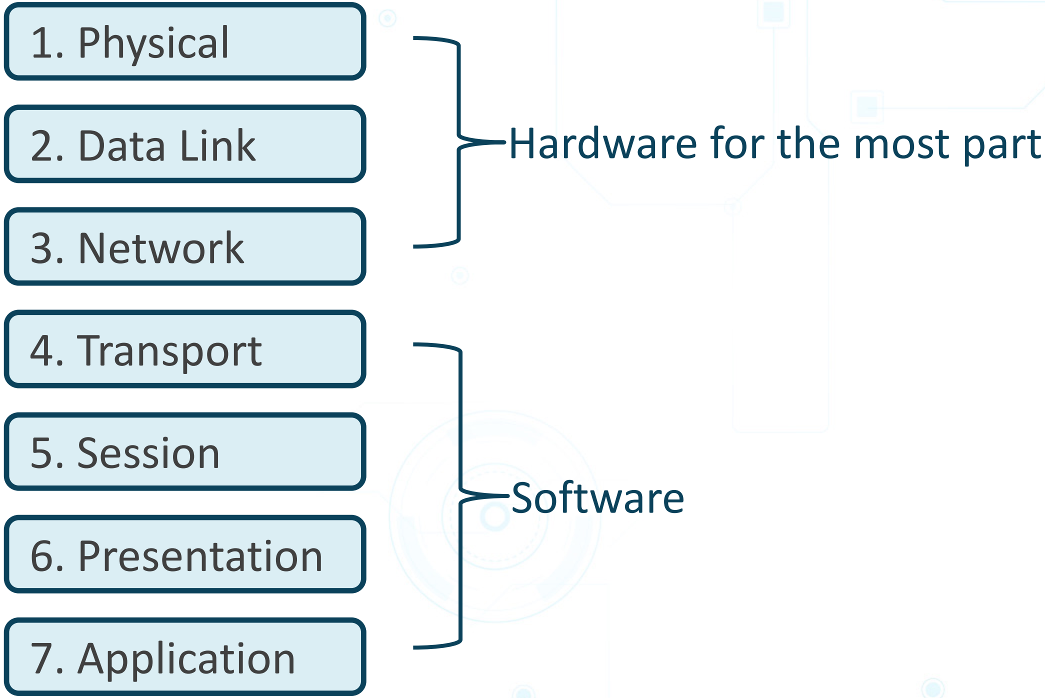
Policies should be reviewed for effectiveness semi-annually

The OSI Model

Seven layer conceptual model

- Internationally accepted
- Map communication hardware and software to the model
- Not all technology maps neatly to specific layers

The OSI Model

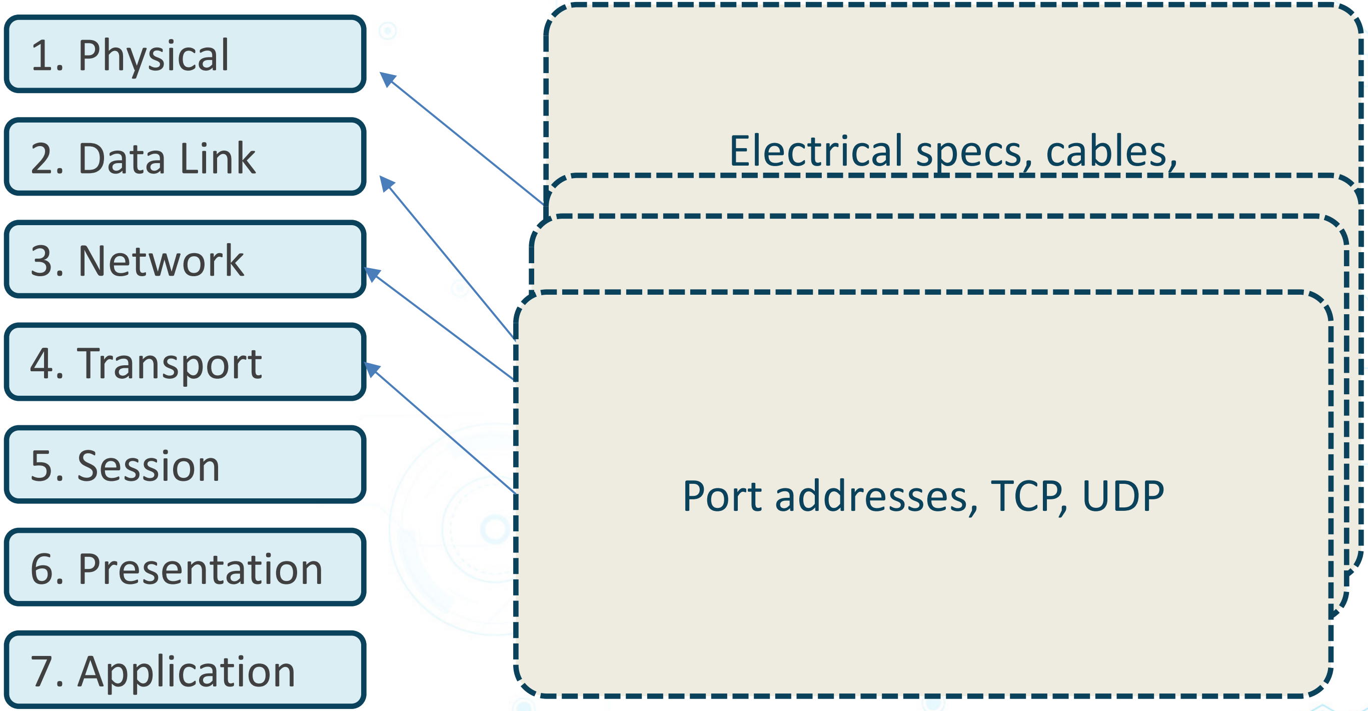


1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

Hardware for the most part

Software

The OSI Model

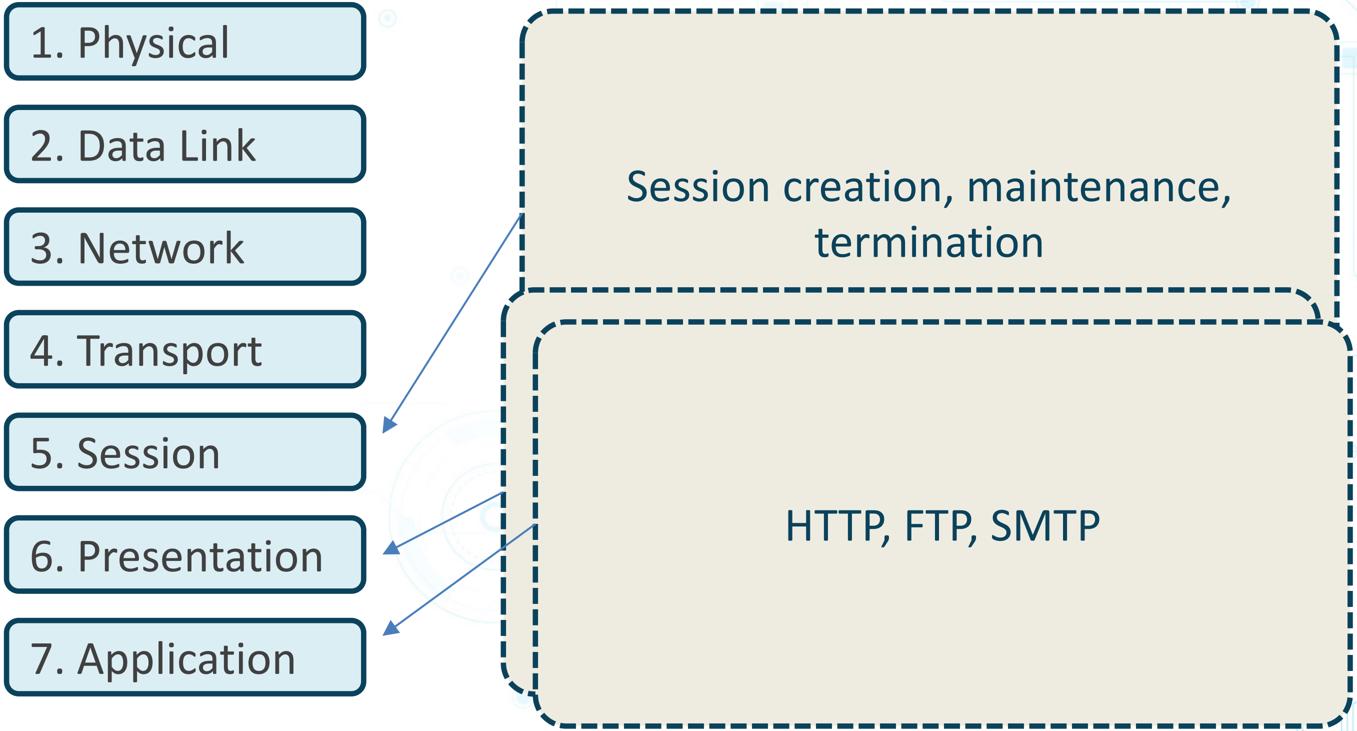


1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

Electrical specs, cables,

Port addresses, TCP, UDP

The OSI Model



1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

Session creation, maintenance, termination

HTTP, FTP, SMTP

The OSI Model and Security

- Compliance with laws, regulations, and contractual obligations could reference OSI model layers
- Remember that network traffic is easily forged with freely available tools

OSI Model layer	Security solution
2	MAC address filtering
3, 4	Packet filtering firewalls
7	Content-filtering firewalls

Password Policies

Something you "know"

Critical in protecting user accounts

User Account Management

- Unique user accounts
  - Provides accountability when auditing usage
- Intruder lockout
- Principle of least privilege
  - Grant only those permissions required to perform a task

User Account Management

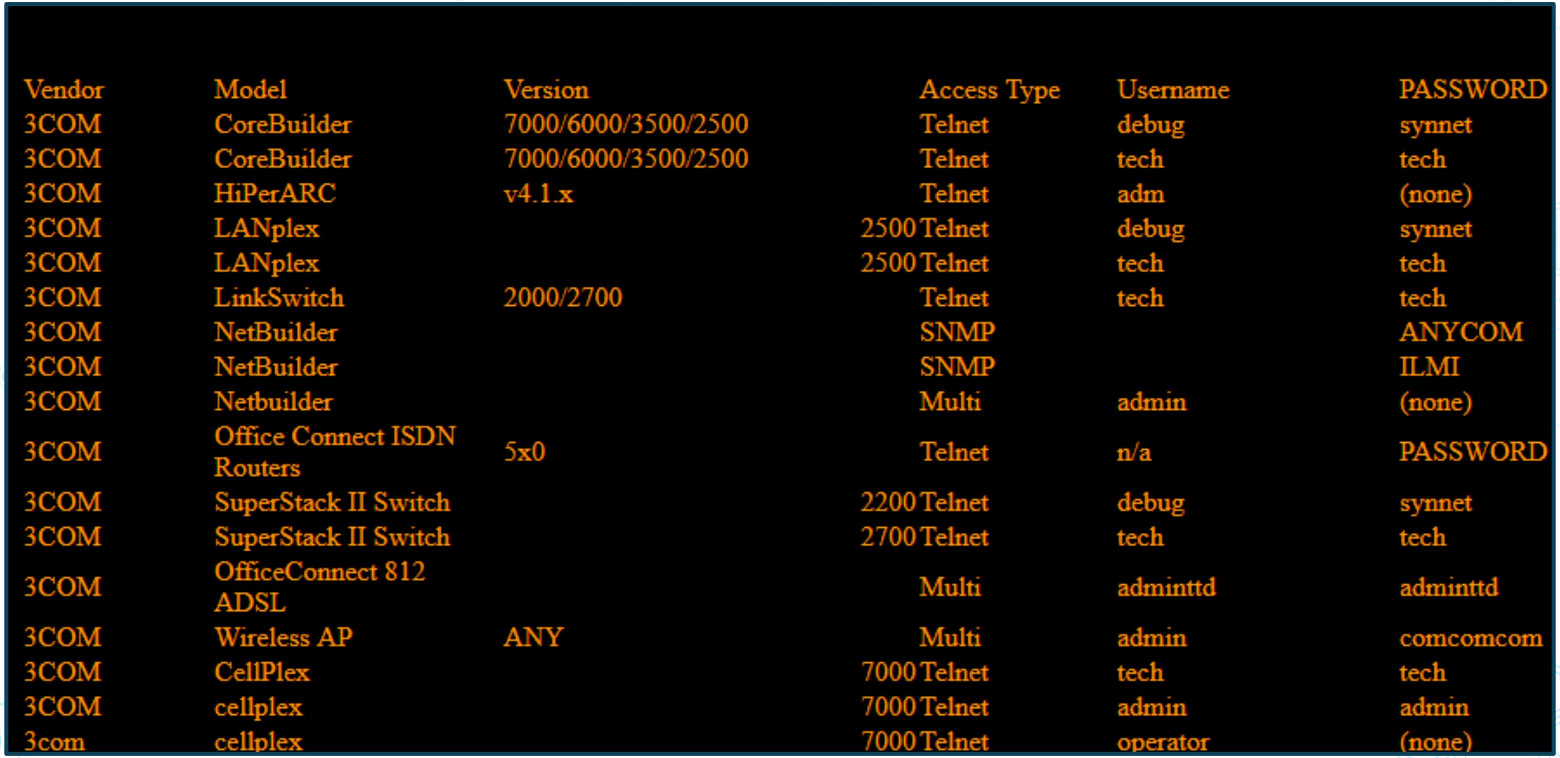
Password settings

- Password length
- Password expiration
- Password reuse

Multifactor authentication

- Username + password + smartcard
- Username + password + SMS text message PIN

Default Password Lists

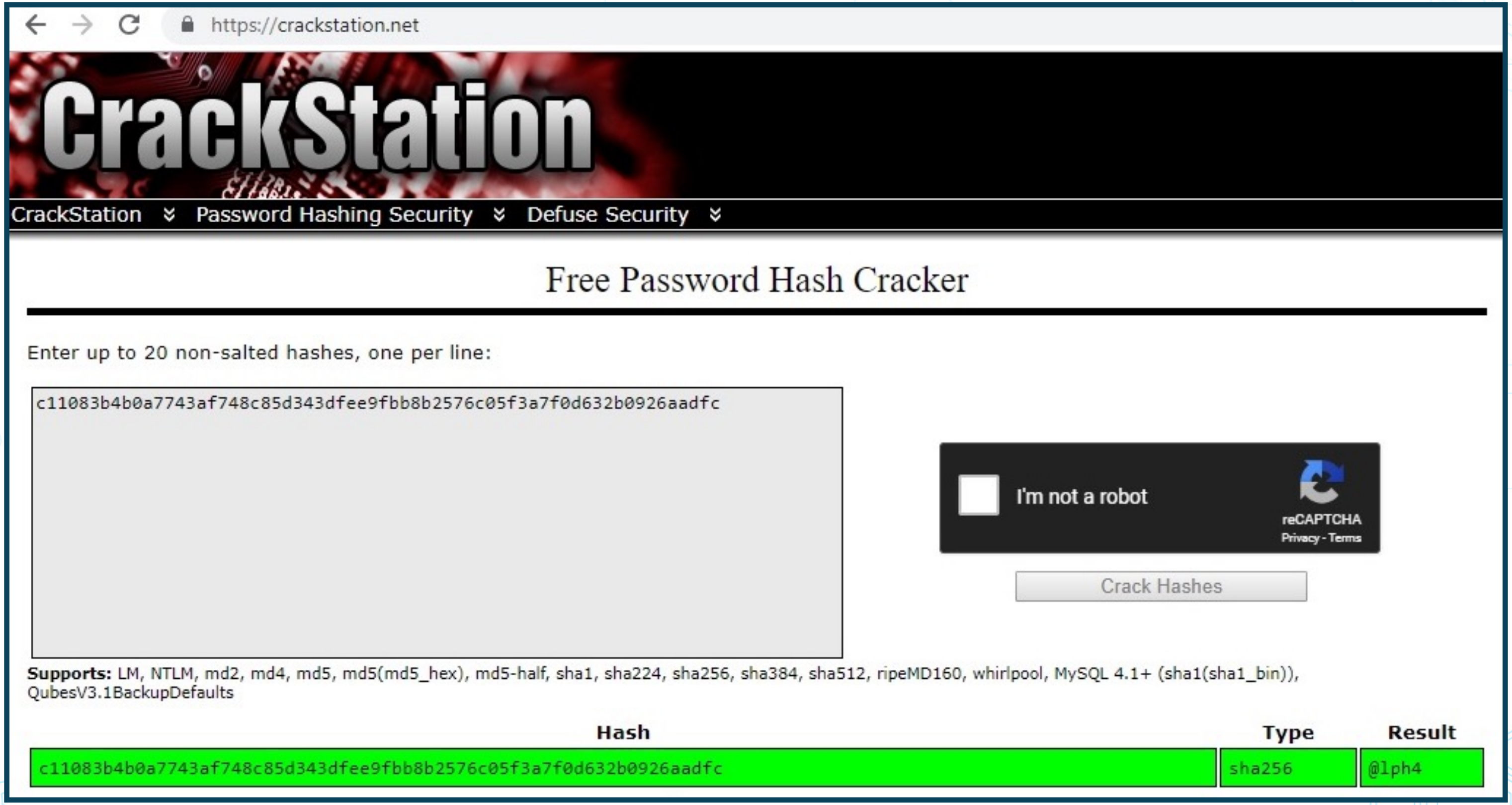


Vendor	Model	Version	Access Type	Username	PASSWORD
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)
3COM	LANplex	2500	Telnet	debug	synnet
3COM	LANplex	2500	Telnet	tech	tech
3COM	LinkSwitch	2000/2700	Telnet	tech	tech
3COM	NetBuilder		SNMP		ANYCOM
3COM	NetBuilder		SNMP		ILMI
3COM	Netbuilder		Multi	admin	(none)
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD
3COM	SuperStack II Switch	2200	Telnet	debug	synnet
3COM	SuperStack II Switch	2700	Telnet	tech	tech
3COM	OfficeConnect 812 ADSL		Multi	adminttd	adminttd
3COM	Wireless AP	ANY	Multi	admin	comcomcom
3COM	CellPlex	7000	Telnet	tech	tech
3COM	cellplex	7000	Telnet	admin	admin
3com	cellplex	7000	Telnet	operator	(none)

Lookup Tables

- Passwords are fed from a password dictionary
- Hashes for each password are generated
- The hashes are stored with the passwords

Lookup Tables - Password Hashes



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
c11083b4b0a7743af748c85d343dfee9fbb8b2576c05f3a7f0d632b0926aadfc
```

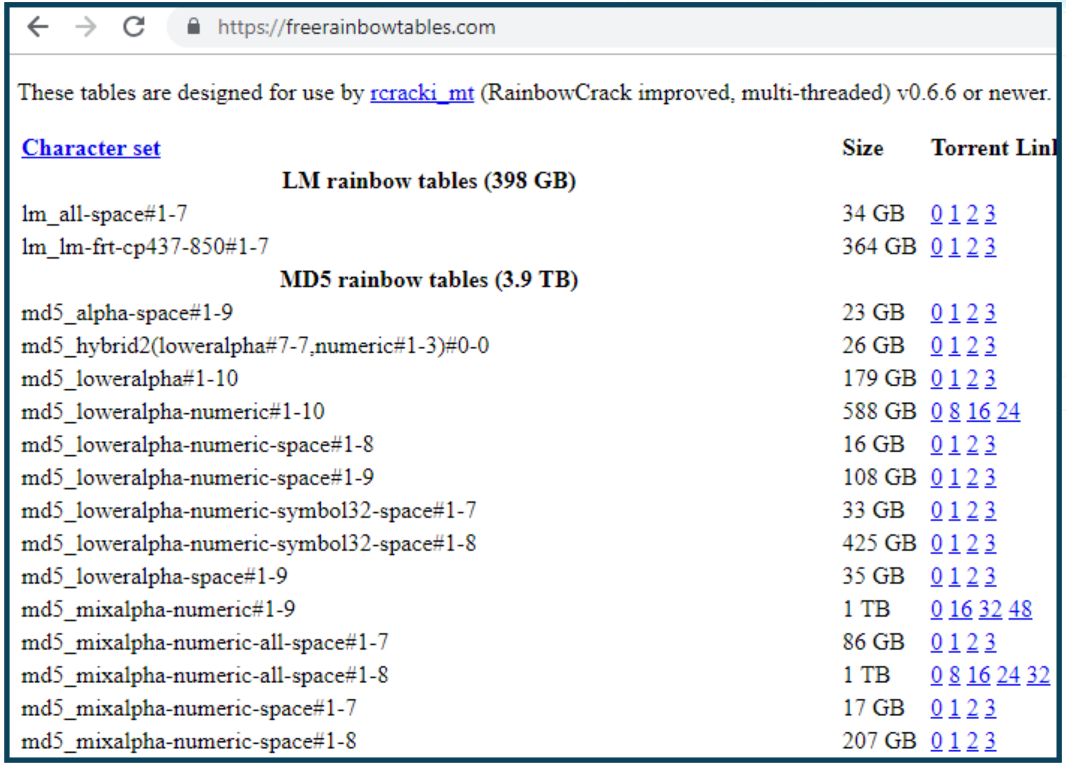
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
c11083b4b0a7743af748c85d343dfee9fbb8b2576c05f3a7f0d632b0926aadfc	sha256	@lph4

Rainbow Tables

- MD5 hashes of passwords up to eight characters are proven to be easily cracked
- Like lookup tables, precomputed hashes are stored, but use less space than lookup tables
  - If many precomputed hashes start with "f3aa5600b", this prefix is stored only once
- Rainbow table lookups are slower than lookup tables

Rainbow Tables - Free Downloads



https://freerainbowtables.com

These tables are designed for use by rcracki_mt (RainbowCrack improved, multi-threaded) v0.6.6 or newer.

Character set	Size	Torrent Link
LM rainbow tables (398 GB)		
lm_all-space#1-7	34 GB	0 1 2 3
lm_lm-frt-cp437-850#1-7	364 GB	0 1 2 3
MD5 rainbow tables (3.9 TB)		
md5_alpha-space#1-9	23 GB	0 1 2 3
md5_hybrid2(loweralpha#7-7,numeric#1-3)#0-0	26 GB	0 1 2 3
md5_loweralpha#1-10	179 GB	0 1 2 3
md5_loweralpha-numeric#1-10	588 GB	0 8 16 24
md5_loweralpha-numeric-space#1-8	16 GB	0 1 2 3
md5_loweralpha-numeric-space#1-9	108 GB	0 1 2 3
md5_loweralpha-numeric-symbol32-space#1-7	33 GB	0 1 2 3
md5_loweralpha-numeric-symbol32-space#1-8	425 GB	0 1 2 3
md5_loweralpha-space#1-9	35 GB	0 1 2 3
md5_mixalpha-numeric#1-9	1 TB	0 16 32 48
md5_mixalpha-numeric-all-space#1-7	86 GB	0 1 2 3
md5_mixalpha-numeric-all-space#1-8	1 TB	0 8 16 24 32
md5_mixalpha-numeric-space#1-7	17 GB	0 1 2 3
md5_mixalpha-numeric-space#1-8	207 GB	0 1 2 3

Data Loss Prevention (DLP)

- "…intentional or unintentional release of secure or private/confidential information to an untrusted environment."

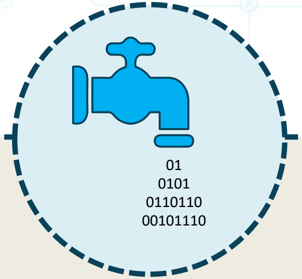
-Wikipedia

Data Loss Prevention

01
0101
0110110
00101110

- User awareness and training
  - Social engineering
- New employee on-boarding
- Periodic training updates
  - Latest scams and organizational security policies

Data Loss Prevention

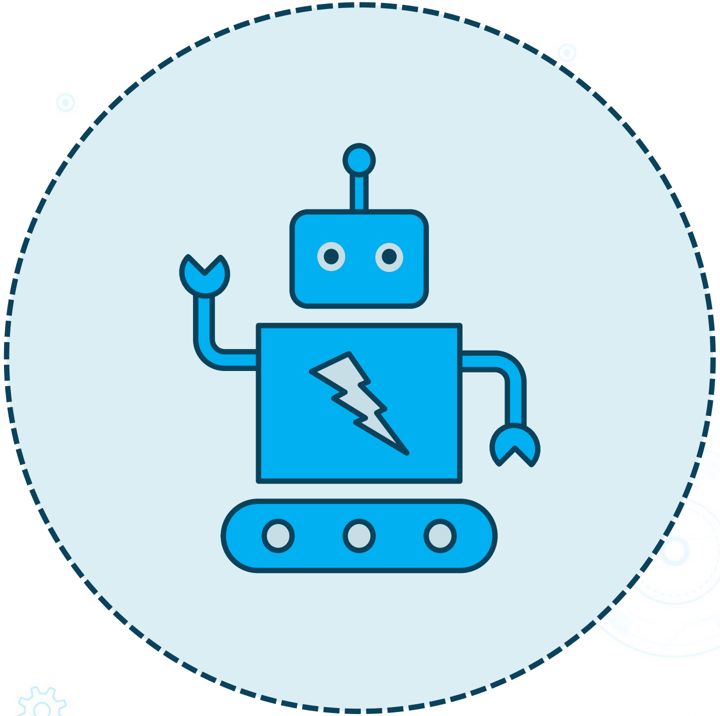


- Policies
  - Conditions
  - Actions
- Example
  - Prevent sensitive file attachments from being sent outside of the organization via e-mail

Data Loss Prevention - Malware

- Definition updates
- Malware scanning engine updates
- Behavioural analysis
- Limited external media use
- Network isolation

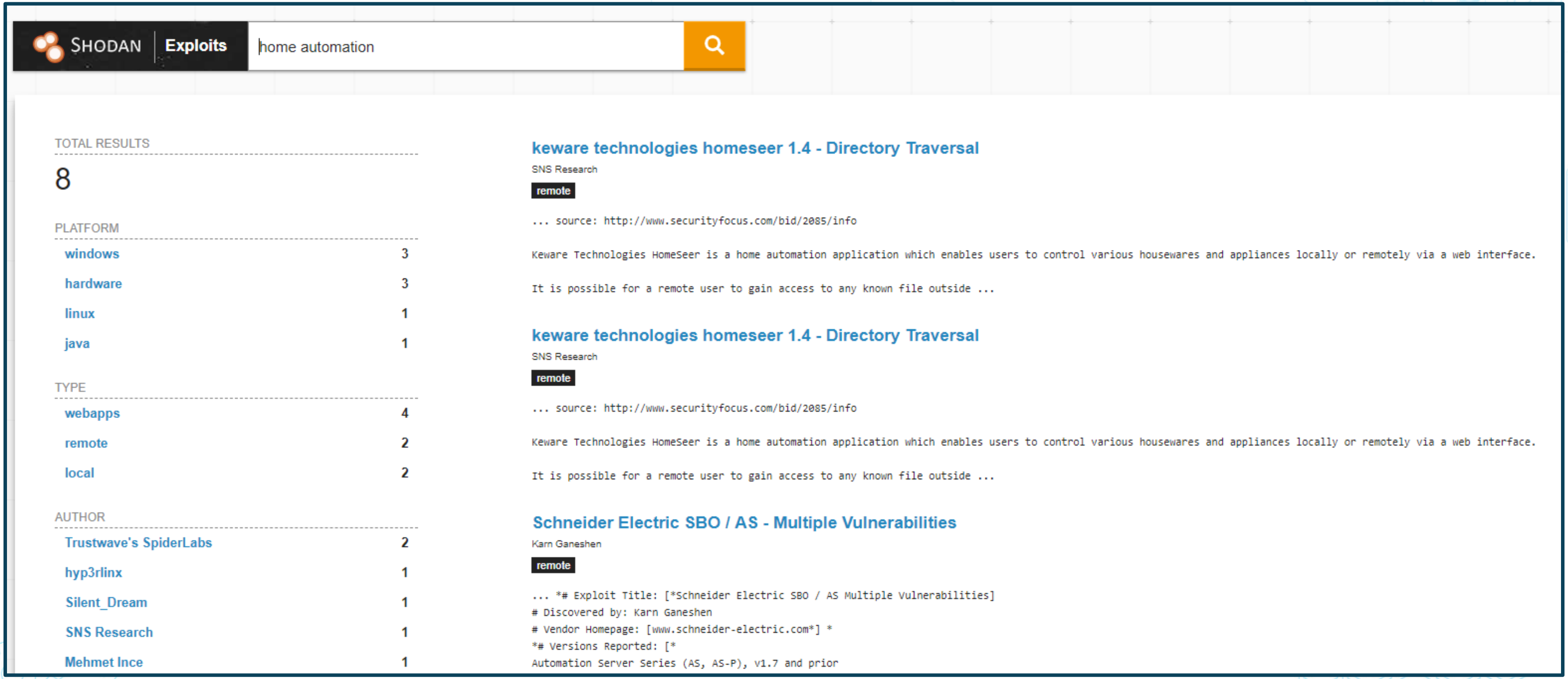
Internet of Things (IoT)



- Physical device with embedded software
- Wide variety of devices that communicate over the Internet
- Cloud data processing such as using Azure IoT Hub

IoT Device Examples

IoT Search Engine



home automation

TOTAL RESULTS

8

PLATFORM	
windows	3
hardware	3
linux	1
java	1

TYPE	
webapps	4
remote	2
local	2

AUTHOR	
Trustwave's SpiderLabs	2
hyp3rlinx	1
Silent_Dream	1
SNS Research	1
Mehmet Ince	1

keware technologies homeseer 1.4 - Directory Traversal

SNS Research

remote

```
... source: http://www.securityfocus.com/bid/2085/info

Keware Technologies HomeSeer is a home automation application which enables users to control various housewares and appliances locally or remotely via a web interface.

It is possible for a remote user to gain access to any known file outside ...
```

keware technologies homeseer 1.4 - Directory Traversal

SNS Research

remote

```
... source: http://www.securityfocus.com/bid/2085/info

Keware Technologies HomeSeer is a home automation application which enables users to control various housewares and appliances locally or remotely via a web interface.

It is possible for a remote user to gain access to any known file outside ...
```

Schneider Electric SBO / AS - Multiple Vulnerabilities

Karn Ganeshen

remote

```
... *# Exploit Title: [*Schneider Electric SBO / AS Multiple Vulnerabilities]
# Discovered by: Karn Ganeshen
# Vendor Homepage: [www.schneider-electric.com*] *
*# Versions Reported: [*
Automation Server Series (AS, AS-P), v1.7 and prior
```

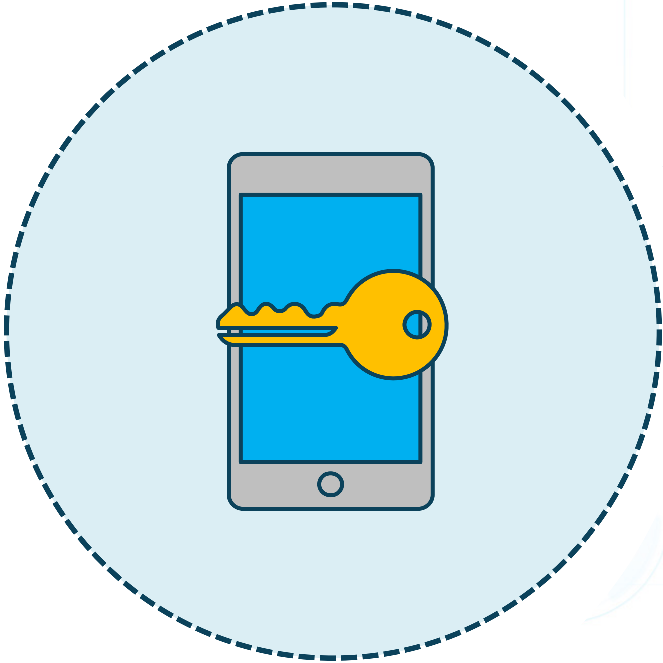
IoT and Security

- Consumer grade IoT devices
  - Security is not a priority
  - Firmware is not updatable
- Change default settings
- Place on isolated and secured network

Mobile Device Access Control

- Introduces organizational security risks (BYOD)
- Mobile Device Management (MDM)
  - Centralized mobile device management
- Microsoft
  - System Center Configuration Manager (SCCM)
  - Intune

Mobile Device Access Control



- Captive portal
- PKI certificates
- Network isolation

Mobile Device Access Control

- MAC address whitelisting for network access
  - MAC addresses are easily spoofed
  - Not scalable for anonymous guest networks
- Configure mobile device settings
  - Turn off microphone and camera
  - Disable GPS
  - Enable device encryption and remote wipe

Mobile Device Access Control

- Scheduled malware engine and definition updates
- Schedule malware scanning
- Restricted ability to install mobile device apps
- Password/authentication settings
- Inventory
  - Hardware
  - Software

Mobile Device Partitioning

Supports selective wipe for lost or stolen devices

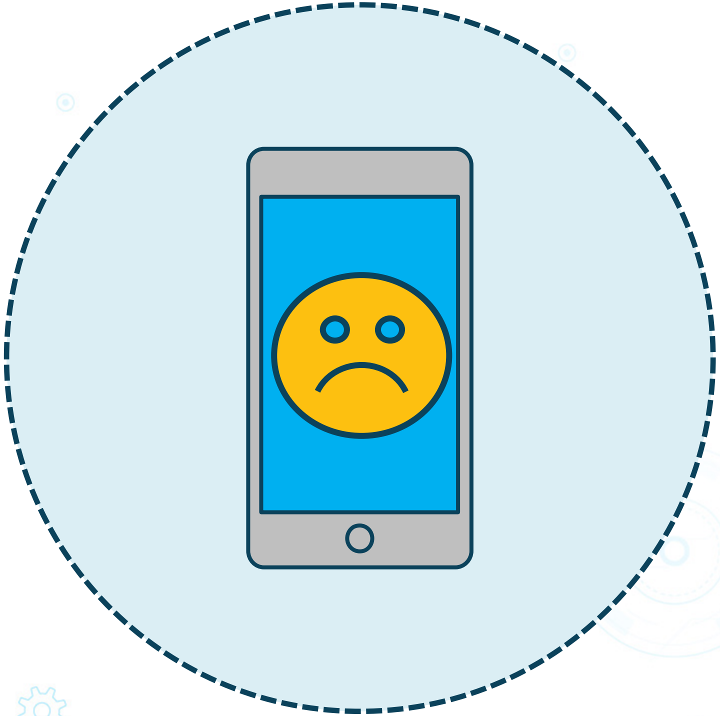
- Corporate partition
  - Apps
  - Settings
  - Data

✗

- Personal partition
  - Apps
  - Settings
  - Data

✓

Malicious Mobile Apps in App Stores



- Malicious apps have been known to exist in public app stores
  - PII leakage and banking malware
- Mitigation
  - Tools such as Google Play Protect
  - Code signing certificate
  - Bug bounties

Malicious Mobile Apps in App Stores

- Vendor app stores
  - Google Play Store, Apple App Store, and Microsoft Store
- Enterprise
  - Contains only corporate-approved apps
  - Can require admin approval to allow app installation
  - Users can have the option to request apps

Auditing Mobile Apps

- App store usage and signed apps
- Turn of Bluetooth, GPS location, NFC, and camera
- Limited device app permissions
- Antimalware, firewall, patches, and remote wipe
- Encryption of data at rest and in transit

In this exercise, you will

- Explain why OSI Layer 7 security solutions provide more options than Layer 3 security solutions
- Provide mitigation recommendations against Linux rainbow attacks
- List five examples of common IoT devices
- Describe how mobile devices can be hardened

OSI

- Layer 3 - Network
  - Limited to MAC and IP addresses
- Layer 7 - Application
  - Ability to parse all packet data including payload

Rainbow Attack Mitigations

- Ensure SHA 256 hashes are used, not MD5
- Use a complex password for the *root* account
- Apply standard host and network hardening techniques

Common IoT Devices

- Wireless video surveillance cameras
- Baby monitors
- Home and business environmental control
- Blood pressure monitor
- Smart car

Mobile Device Hardening

- Disable Bluetooth
- Limit Wi-Fi network connectivity
- Disable public app store access
- Antimalware and firewall app
- Apply updates
- Network isolation