CSF 432: Intro to Network and System Security

Week 11 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes

Physical Security

Physical Security

Video surveillance

- CCTV (Closed circuit television)
  - Can replace physical guards
- Camera properties are important
  - Focal length - Shorter is wider angle
  - Depth of field - How much is in focus
  - Illumination requirements - See in the dark
- Often many different cameras
  - Networked together and recorded over time
- Can provide notification of activity
  - Motion detection

Physical Security

Asset tracking tags

- A record of every asset
  - Routers, switches, cables, fiber modules, CSU/DSUs, etc.
- Financial records, audits, depreciation
  - Make/model, configuration, purchase date, location, etc.
- Tag the asset
  - Barcode, RFID, visible tracking number

Physical Security

Tamper detection

- You can't watch all of your equipment all of the time
  - Have your systems monitor themselves
- Hardware tampering
  - Case sensors, identify case removal
  - Alarm sent from BIOS
  - Firewalls, routers, etc.
- Foil asset tags
  - Identify the tampering

Physical Security

Identification badges

- ID badge
  - Picture, name, other details
  - Must be worn at all times
- May be integrated with door access or a smart card
  - It's more than just a visual identification
- Standardized format
  - Train all employees to look for ID and ask questions if they don't see one

Physical Security

Biometrics

- Biometric authentication
  - Fingerprint, iris, voiceprint
- Usually stores a mathematical representation of your biometrics
  - Your actual fingerprint isn't usually saved
- Difficult to change
  - You can change your password
  - You can't change your fingerprint
- Used in very specific situations
  - Not foolproof

Physical Security

Tokens and cards

- Smart card
  - Integrates with devices
  - May require a PIN
- USB token
  - Certificate is on the USB device
- Hardware or software tokens / key fobs
  - Generates pseudo-random authentication codes
- Your phone
  - SMS a code to your phone

Physical Security

Door access controls

- Conventional
  - Lock and key
- Deadbolt
  - Physical bolt
- Electronic
  - Keyless
- Token-based
  - Magnetic swipe card or proximity reader
- Multi-factor
  - Smart card and PIN

Authorization, Authentication, and Accounting

Authorization, Authentication, and Accounting

AAA framework

- Identification - This is who you claim to be
  - Usually your username
- Authentication
  - Prove you are who you say you are
  - Password and other authentication factors
- Authorization
  - Based on your identification and authentication, what access do you have?
- Accounting
  - Resources used: Login time, data sent and received, logout time

Authorization, Authentication, and Accounting

RADIUS (Remote Authentication Dial-in User Service)

- One of the more common AAA protocols
  - Supported on a wide variety of platforms and devices
  - Not just for dial-in
- Centralize authentication for users
  - Routers, switches, firewalls
  - Server authentication
  - Remote VPN access
  - 802.1X network access
- RADIUS services available on almost any server operating system

Authorization, Authentication, and Accounting

TACACS

- Terminal Access Controller Access-Control System
  - Remote authentication protocol
  - Created to control access to dial-up lines to ARPANET
- XTACACS (Extended TACACS)
  - A Cisco-created (proprietary) version of TACACS
  - Additional support for accounting and auditing
- TACACS+
  - The latest version of TACACS, not backwards compatible
  - More authentication requests and response codes
  - Released as an open standard in 1993

Authorization, Authentication, and Accounting

Kerberos

- Network authentication protocol
  - Authenticate once, trusted by the system
- No need to re-authenticate to everything
  - Mutual authentication - the client and the server
  - Protect against man-in-the-middle or replay attacks
- Standard since the 1980s
  - Developed by the Massachusetts Institute of Technology (MIT)
  - RFC 4120
- Microsoft starting using Kerberos in Windows 2000
  - Based on Kerberos 5.0 open standard
  - Compatible with other operating systems and devices

Authorization, Authentication, and Accounting

SSO with Kerberos

- Authenticate one time
  - Lots of backend ticketing, uses cryptographic tickets
- No constant username and password input! - Save time
- Only works with Kerberos
  - Not everything is Kerberos-friendly

Authorization, Authentication, and Accounting

LDAP (Lightweight Directory Access Protocol)

- Protocol for reading and writing directories over an IP network
  - An organized set of records, like a phone directory
- X.500 specification was written by the International Telecommunications Union (ITU)
  - They know directories!
- DAP ran on the OSI protocol stack
  - LDAP is lightweight, and uses TCP/IP (tcp/389 and udp/389)
- LDAP is the protocol used to query and update an X.500 directory
  - Used in Windows Active Directory, Apple OpenDirectory, OpenLDAP, etc.

Authorization, Authentication, and Accounting

Local authentication

- Credentials are stored on the local device
  - Does not use a centralized database
- Most devices include an initial local account
  - Good devices will force a password change
- Difficult to scale local accounts
  - No centralized administration
  - Must be added or changed on all devices
- Sometimes useful as a backup
  - The AAA server might not be available

Authorization, Authentication, and Accounting

Certificate-based authentication

- Smart card - Private key is on the card
- PIV (Personal Identity Verification) card
  - US Federal Government smart card
  - Picture and identification information
- CAC (Common Access Card)
  - US Department of Defense smart card
  - Picture and identification
- IEEE 802.1X
  - Gain access to the network using a certificate
  - On device storage or separate physical device

Authorization, Authentication, and Accounting

Auditing

- Log all access details
  - Automate the log parsing
  - OS logins, VPN, device access
- Usage auditing
  - How are your resources used?
  - Are your systems and applications secure?
- Time-of-day restrictions
  - Nobody needs to access the lab at 3 AM

Multi-factor Authentication

Multi-factor Authentication

Multi-factor Authentication

- More than one factor
  - Something you are
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do
- Can be expensive
  - Separate hardware tokens
  - Specialized scanning equipment
- Can be inexpensive
  - Free smartphone applications

Multi-factor Authentication

Something you know

- Password
  - Secret word/phrase, string of characters
  - Very common authentication factor
- PIN
  - Personal identification number
  - Not typically contained anywhere on a smart card or ATM card
- Pattern
  - Complete a series of patterns
  - Only you know the right format

Multi-factor Authentication

Something you have

- Smart card
  - Integrates with devices
  - May require a PIN
- USB token - Certificate is on the USB device
- Hardware or software tokens
  - Generates pseudo-random authentication codes
- Your phone - SMS a code to your phone

Multi-factor Authentication

Something you are

- Biometric authentication
  - Fingerprint, iris scan, voiceprint
- Usually stores a mathematical representation of your biometrics
  - Your actual fingerprint isn't usually saved
- Difficult to change
  - You can change your password
  - You can't change your fingerprint
- Used in very specific situations
  - Not foolproof

Multi-factor Authentication

Somewhere you are

- Provide a factor based on your location
  - The transaction only completes if you are in a particular geography
- IP address
  - Not perfect, but can help provide more info
  - Works with IPv4, not so much with IPv6
- Mobile device location services
  - Geolocation to a very specific area
  - Must be in a location that can receive GPS information or near an identified mobile or 802.11 network
- Still not a perfect identifier of location

Multi-factor Authentication

Something you do

- A personal way of doing things - You're special
- Handwriting analysis
  - Signature comparison or writing technique
- Typing technique - Delays between keystrokes
- Very similar to biometrics - Close to something you are

Access Control

Access Control

Network Access Control (NAC)

- IEEE 802.1X - Port-based
  - Network Access Control (NAC)
  - You don't get access until you authenticate
- Makes extensive use of EAP and RADIUS
  - Extensible Authentication Protocol / Remote Authentication Dial In User Service
- We're talking about physical interfaces
  - Not TCP or UDP ports
- Administrative enable/disable
  - Disable your unused ports
- Duplicate MAC address checking - Stop the spoofers

Access Control

Port security

- Prevent unauthorized users from connecting to a switch interface
  - Alert or disable the port
- Based on the source MAC address
  - Even if forwarded from elsewhere
- Each port has its own config
  - Unique rules for every interface

Access Control

Port security operation

- Configure a maximum number of source MAC addresses on an interface
  - You decide how many is too many
  - You can also configure specific MAC addresses
- The switch monitors the number of unique MAC addresses
  - Maintains a list of every source MAC address
- Once you exceed the maximum, port security activates
  - Default is to disable the interface

Access Control

MAC filtering

- Media Access Control - The “hardware” address
- Limit access through the physical hardware address
  - Keeps the neighbors out
  - Additional administration with visitors
- Easy to find working MAC addresses through wireless LAN analysis
  - MAC addresses can be spoofed
  - Free open-source software
- Security through obscurity

Access Control

Captive portal

- Authentication to a network
  - Common on wireless networks
- Access table recognizes a lack of authentication
  - Redirects your web access to a captive portal page
- Username / password
  - And additional authentication factors
- Once proper authentication is provided, the web session continues
  - Until the captive portal removes your access

Access Control

Access Control Lists (ACLs)

- Used to allow or deny traffic
  - Also used for NAT, QoS, etc.
- Defined on the ingress or egress of an interface
  - Incoming or outgoing
- ACLs evaluate on certain criteria
  - Source IP, Destination IP, TCP port numbers, UDP port numbers, ICMP
- Deny or permit
  - What happens when an ACL matches the traffic?

Wireless Encryption

Wireless Encryption

Wireless encryption

- All wireless computers are radio transmitters and receivers - anyone can listen in
- Solution: Encrypt the data
  - Everyone gets the password
  - Or their own password
- Only people with the password can transmit and listen
  - WPA and WPA2

Wireless Encryption

WPA (Wi-Fi Protected Access)

- 2002: WPA was the replacement for serious cryptographic weaknesses in WEP (Wired Equivalent Privacy)
  - Don't use WEP
- Needed a short-term bridge between WEP and whatever would be the successor
  - Run on existing hardware
- WPA: RC4 with TKIP (Temporal Key Integrity Protocol)
  - Initialization Vector (IV) is larger and an encrypted hash
  - Every packet gets a unique 128-bit encryption key

Wireless Encryption

Temporal Key Integrity Protocol

- Mixed the keys
  - Combines the secret root key with the IV
- Adds sequence counter - prevents replay attacks
- Implements a 64-bit Message Integrity Check
  - Protects against tampering
- TKIP has it's own set of vulnerabilities
  - Deprecated in the 802.11-2012 standard

Wireless Encryption

WPA2 and CCMP

- WPA2 certification began in 2004
  - AES (Advanced Encryption Standard) replaced RC4
  - CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) replaced TKIP
- CCMP block cipher mode
  - Uses AES for data confidentiality
  - 128-bit key and a 128-bit block size
  - Requires additional computing resources
- CCMP security services
  - Data confidentiality (AES), authentication, and access control

Wireless Authentication and Security

Wireless Authentication and Security

EAP

- EAP - Extensible Authentication Protocol
- An authentication framework
- Many different ways to authenticate based on RFC standards
- WPA and WPA2 use five EAP types as authentication mechanisms

EAP types

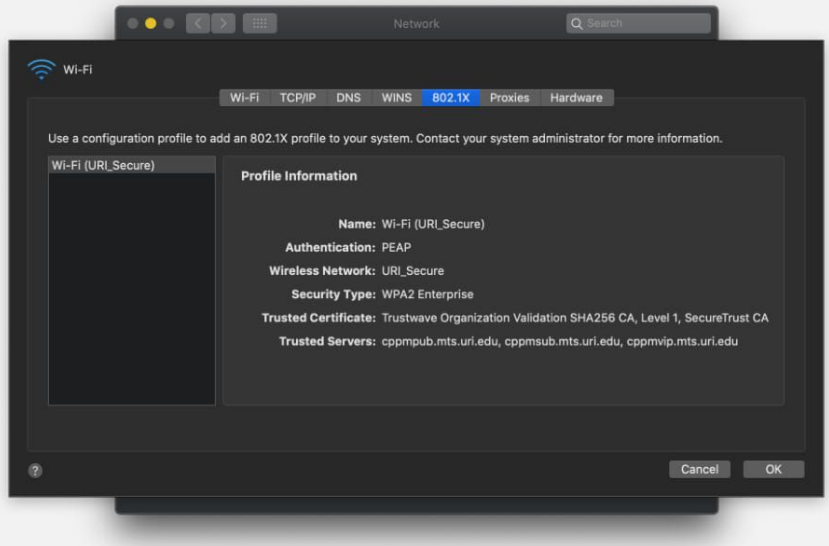
- EAP-FAST
  - EAP Flexible Authentication via Secure Tunneling
  - Cisco's proposal to replace LEAP (Lightweight EAP - previously used with WEP)
  - Lightweight and secure
- EAP-TLS (EAP Transport Layer Security)
  - Strong security, wide adoption
  - Support from most of the industry
- EAP-TTLS (EAP Tunneled Transport Layer Security)
  - Support other authentication protocols in a TLS tunnel
  - Use any authentication you can support, maintain security with TLS

PEAP

- Protected Extensible Authentication Protocol
  - Protected EAP
- Created by Cisco, Microsoft, and RSA Security
- Encapsulates EAP in a TLS tunnel, one certificate on the server
  - Combined a secure channel and EAP
- Commonly implemented as PEAPv0/EAP-MSCHAPv2
  - Authenticates to Microsoft's MS-CHAPv2 databases

Wireless security modes

- Configure the authentication on your wireless access point / wireless router
- Open System - No authentication password is required
- WPA-Personal / WPA-PSK
  - WPA2 with a pre-shared key
  - Everyone uses the same 256-bit key
- WPA-Enterprise / WPA-802.1X
  - Authenticates users individually with an authentication server (i.e., RADIUS)



Wireless Authentication and Security

MAC filtering

- Media Access Control - The “hardware” address
- Limit access through the physical hardware address
  - Keeps the neighbors out
  - Additional administration with visitors
- Easy to find working MAC addresses through wireless LAN analysis
  - MAC addresses can be spoofed
  - Free open-source software
- Security through obscurity (not actual security)

Wireless Authentication and Security

Geofencing

- Some MDMs allow for geofencing
  - Restrict or allow features when the device is in a particular area
- Cameras
  - The camera might only work when outside the office
- Authentication
  - Only allow logins when the device is located in a particular area

CSF 432: Intro to Network and System Security

Week 11 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes