Hospital Network Security

Danielle McGeary
November 6, 2014
NECSE 2014 Symposium
SECURITY— What is It?

se·cu·ri·ty  \si-ˈkyur-ə-tē\  
noun

1. The quality or state of being secure
2. Freedom from danger
3. Freedom from fear or anxiety
4. Measures taken to guard against espionage or sabotage, crime, attack, or escape
Information Security

Protecting information and information systems (including computers, medical devices and networks) from:

- Unauthorized access
- Unauthorized use
- Unauthorized alterations
- Unauthorized interruptions
- Devastation
Why does this Effect Clinical Engineering??

Medical devices and systems represent a growing risk with respect to the security of the medical data they contain. Hospitals and similar healthcare organizations typically have 300% to 400% more medical equipment than IT devices and two trends are contributing to the increasing significance of this security risk:

1. Medical devices and systems are being designed and operated as special purpose computers … more features are being automated, increasing amounts of medical data are being collected, analyzed and stored in these devices.

2. There has been a rapidly growing integration and interconnection of disparate medical (and information) technology devices and systems where medical data is being increasingly exchanged.
Information Security Includes:

Confidentiality

– Ensuring only authorized individuals have access to information.
– Making sure that individuals with access keep the information private and do not share with others.

Integrity

– Data in a system is the same as the data from the original source.
– Data has not been altered or destroyed, intentionally or unintentionally.
Information Security Includes:

**Availability**
- System/data is available when needed
- Fault-tolerance infrastructures so if one part of the system fails, the entire system doesn’t go down (RAIDs, etc)

**Accountability**
- System must identify users and maintain an audit trail of actions.
- No generic sign ons
The Health Insurance Portability and Accountability Act (HIPAA)

• Addresses the security and privacy of health data.

• Encourages the widespread use of electronic data interchange (EDI) in the U.S. health care system.

• Protects health insurance coverage for workers and their families when they change or lose their jobs.

• Requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.
Encryption

Hi Tevin,
Our meeting today will start at 2 pm. Don’t forget to bring the UNC file so we can go over it.

Thanks,
Michele

Plaintext + Cipher = Ciphertext
How Does Encryption Work?

Cipher = Shift characters X amount to the Y

Example:
Let’s encrypt the word: Hospital (Plaintext)

Cipher: X = 3, Y = right
Ciphertext = KRVSLWDO

Cipher: X = 4, Y = left
Ciphertext = DKOLEPWH
Types of Encryption

**Symmetric**
- Same key used in encrypt and decrypt
- Shared Key

**Asymmetric**
- One key use to encrypt and another used to decrypt
- Public key encryption
Access Control

• Who or what is allowed access to a particular resource and what level of access they are allowed
• Only allow people who really need access

Terminology
  – Identification (User Name)
  – Authentication (Password)
  – Authorization (Permissions)
Access Control Best Practices

• Separation of Duties
  – Doctor should not be the primary user of the application and the manager of the server
  – No one person should have access to perform an action that could lead to fraudulent activity.

• Least Privilege
  – Only give users the access they need to perform their jobs
  – Users will do things they shouldn’t -- either intentionally or unintentionally, so only give them access to do the things they should be doing.
Access Control Types

Logical
- Access to data files, programs, and networks
  - Access Control Lists (ACLs)
  - Account Restrictions
  - Passwords

Physical
- Access to Physical Locations
  - Locks
  - Badges
  - Mantraps
Access Control List (ACL)

An ACL is a list that is associated with file, directory or object that lists who has access to it and what access they have.
Access Control List (ACL)

- Access lists filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces.
- Provide security for your network
- Decide which types of traffic are forwarded or blocked at the router interfaces. Example: permit e-mail traffic to be routed, but Telnet traffic
Access Control Lists (ACLs)

• Can apply up to two access lists to an interface: one inbound access list and one outbound access list

• If the access list is inbound, when the router receives a packet, the software checks the access list's criteria statements for a match. If the packet is permitted, the software continues to process the packet. If the packet is denied, the software discards the packet.

• If the access list is outbound, after receiving and routing a packet to the outbound interface, the software checks the access list's criteria statements for a match. If the packet is permitted, the software transmits the packet. If the packet is denied, the software discards the packet.
Password

• Combination of letters, numbers and special characters
• Recommend upper and lower case characters
• The more characters the better
• Should be changed frequently
• Should not be the default password set by the vendor
• Should not be used for more than one account
• Should not be written down
Physical Access Control

- **Location**
  - Servers and connectivity devices like routers, switches, and firewalls should be in a place that is not easily accessed

- **Doors**
  - Can be secured with a key-in-knob lock, or a deadbolt
  - Cipher lock requires a user to know the code.
    - Codes should be changed frequently and especially after an employee leaves
  - RFID, radio frequency ID cards, or badges
    - These cards have an RFID that transmits a radio signal to a receiver. A database is checked to make sure the user can have access to the location.

- **Video surveillance**

- **Access log**
  - Locations that have access logs that require a person to sign in and out
  - RFID and card readers keep a log of everyone who enters
Authentication Practices

• Layering
  – Requires users to have multiple authentications to have access
  – Authentications should be of different types

• Multi-factor

• Single Sign-On (SSO)
  – Require a user to login once and then they are able to access other resources
  – Authentication credentials are passed between systems
Virtual Private Networks (VPNs)

- Internet technology to transmit data between sites (Vendor to Server)
- Data is encrypted
- Data is kept separate from other data traveling on the internet
Manufacturer Disclosure Statement for Medical Device Security (MDS\textsuperscript{2})

- HIMSS/NEMA Standard HN 1-2013

- Be useful to healthcare provider organizations worldwide. The information presented, should be useful for any healthcare delivery organization that aspires to have an effective, information security risk management program.

- Include device-specific information addressing the technical security-related attributes of the individual device model.

- Provide a simple, flexible way of collecting the technical, device-specific elements of the common/typical information needed by provider organizations (device users/operators) to begin medical device information security (i.e., confidentiality, integrity, availability) risk assessments.
Manufacturer Disclosure Statement for Medical Device Security (MDS\textsuperscript{2})

• In 2010, standard IEC 80001-1, Application of risk management for IT-networks incorporating medical devices, was published.
  – Deals with the application of risk management to IT-networks incorporating medical devices and provides the roles, responsibilities and activities necessary for risk management.

• In 2012, a Technical Report (TR) supplement to IEC 80001 was published, IEC/TR 80001-2-2.
  – Guidance for the communication of medical device security needs, risks and controls.

• HIMSS and NEMA recommend that the information in the MDS\textsuperscript{2} form be used as part of each organization’s security compliance and risk assessment efforts.
Manufacturer Disclosure Statement for Medical Device Security (MDS²)

The Role of Healthcare Providers in the Security Management Process

The provider organization has the ultimate responsibility for providing effective security management. Device manufacturers can assist providers in their security management programs by offering information describing:

• the type of data maintained/transmitted by the manufacturer’s device;
• how data is maintained/transmitted by the manufacturer’s device;
• any security-related features incorporated in the manufacturer’s device.

In order to effectively manage medical information security and comply with relevant regulations, healthcare providers must employ administrative, physical, and technical safeguards—most of which are extrinsic to the actual device.
Keep Your Devices Organized
Keep Your Devices Organized

• Have list of IPs associated with Asset Numbers
  – Enter to asset software

• Have an accurate list of Servers
  – Computer names
  – IP address
  – Location

• Servers
  – Manage your ACLs
  – Know what user accounts are available
QUESTIONS?