

Biomedical Devices and Systems

David Arney
Insup Lee
University of Pennsylvania



CPS Security Workshop



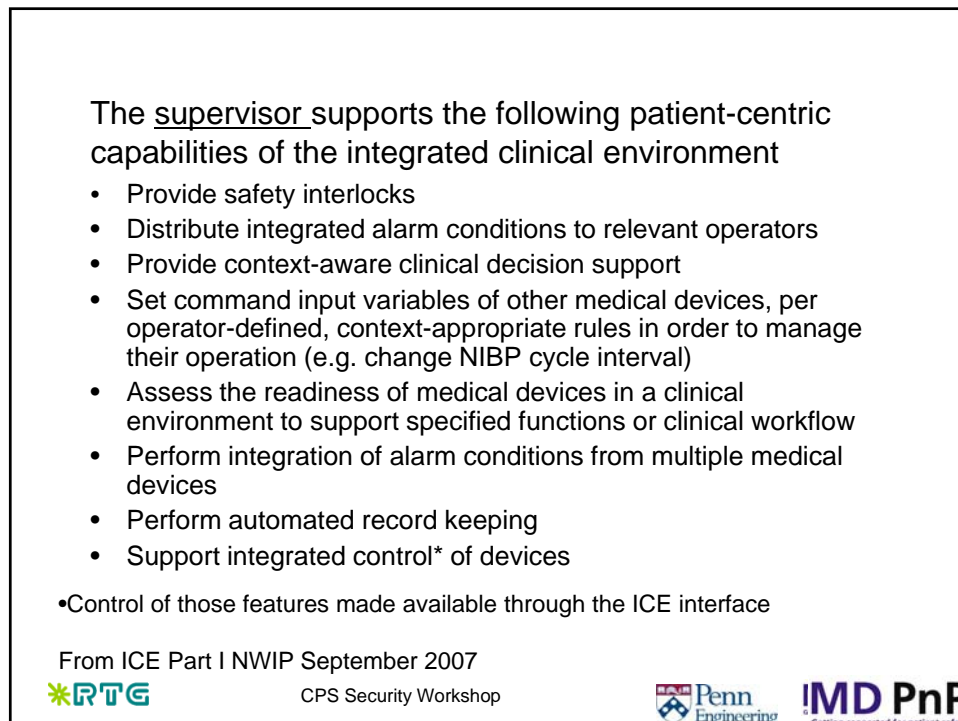
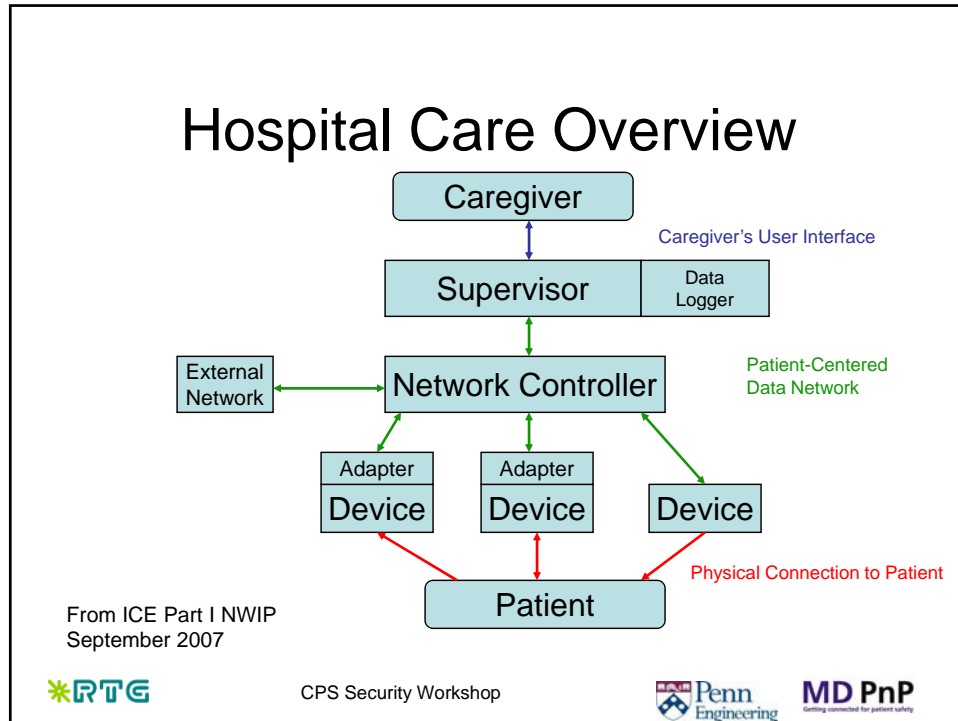
The Biomedical Domain

- The domain of biomedical devices includes:
 - Hospital Care
 - Home Care
 - Electronic Health Records Systems
 - Ambulatory and Implanted Devices



CPS Security Workshop





The network controller supports the following patient-centric capabilities of the integrated clinical environment

- Provide “Plug and Play” (PnP) connectivity with medical devices and other devices
- Interface with (compatible) equipment
- Provide data logs for forensic analysis (flight recorder)
- Perform network control functions independently of the underlying data communication mechanization
- Provide relevant information to support a healthcare equipment management system
- Also provides a common time base and binding of data to patient identity
- Also can provide and retrieve relevant clinical data to a healthcare information system/electronic medical record/electronic health record (HIS/EMR/EHR)

From ICE Part I NWIP September 2007



CPS Security Workshop



Forensic Data Logging

- Patient and device data are logged to a flight-recorder style data logger.
- Logs assist in uncovering causes of adverse events.
- Logs can help to distinguish use error, equipment failure, or abnormal use.
- Logs also open new hazards.
 - Log is itself a desirable target
 - Transmissions of data to log may be intercepted. Encryption before transmission may help.
- The data logging of the “state-of-the-clinical environment” shall include:
 - a) Ice equipment interface-connected equipment technical variables and technical alarm conditions available to the ice network controller;
 - b) Patient physiological variables and alarm conditions from ice equipment interface-connected medical devices available to the ice network controller;
 - c) Ice network controller commands to ice equipment interface-connected equipment;
 - d) Ice network controller status;
 - e) Any other significant events and errors.



CPS Security Workshop



Extended Use Case: X-Ray / Ventilator

Ventilation stopped
during intraoperative
cholangiography



Anesthesia
Machine



Portable x-ray machine



Surgeons



CPS Security Workshop



“With the advent of sophisticated anesthesia machines incorporating comprehensive monitoring, it is easy to forget that serious anesthesia mishaps still can and do occur.” APSF Newsletter Winter 2005

A 32-year-old woman had a laparoscopic cholecystectomy performed under general anesthesia. At the surgeon's request, a plane film x-ray was shot during a cholangiogram. The anesthesiologist stopped the ventilator for the film. The x-ray technician was unable to remove the film because of its position beneath the table. The anesthesiologist attempted to help her, but found it difficult because the gears on the table had jammed. Finally, the x-ray was removed, and the surgical procedure recommenced. At some point, the anesthesiologist glanced at the EKG and noticed severe bradycardia. He realized he had never restarted the ventilator. This patient ultimately expired.



CPS Security Workshop



What is the “root cause”?

- Inadequate alarms?
- Inadequate vigilance/need more coffee?
- *At its root, this is a system problem*



CPS Security Workshop



Synchronization or gating of shutter and flash (x-ray) is not a new concept ...



... but cannot be performed with current devices which do not interoperate



CPS Security Workshop



Intraoperative Cholangiography Use Case

- **CURRENT HAZARD**
- Clinician forgets to manually turn ventilator back on, or it is turned off for an excessive amount of time, possibly leading to patient physiological instability, hypoxemia, and death.
- **DESIRED STATE**
- Synchronization (gating) or triggering of x-ray machine with ventilator.
- System may assess x-ray exposure requirements and ventilatory parameters, and inform the clinician that synchronization is or is not possible.
- System will advise the clinician when to inject contrast agent.
- System may briefly pause ventilation (to prolong expiration of 1 breath by 3-5 s) if supported by ventilator



CPS Security Workshop



Intraoperative Cholangiography Use Case

- **POTENTIAL FUTURE HAZARDS**
- Too-tight coupling of control between devices, e.g. x-ray machine pauses too long or malfunctions, results in ventilator pausing too long to wait for ventilator, possibly causing adverse physiological changes.
- System determines that there is no period sufficiently long for an x-ray, and prevents a necessary - although potentially blurred, x-ray from being taken.



CPS Security Workshop



Extended case: X-Ray synchronization during spontaneous respiration

- **Synchronize portable x-ray with spontaneous ventilation**
- Appearance of chest x-ray is a function of the phase of respiration.
- Most x-rays are taken at full inspiration.
- Sequential x-rays (e.g. taken every morning) may not be comparable if taken during different phases of respiration.
- Neonates cannot hold their breath for manual synchronization of the x-ray with the phase of respiration.
- An impedance respirometer or other sensor may be used to synchronize the x-ray with the respiratory phase.



CPS Security Workshop



Extended case: Chest X-Ray X-Ray synchronization with ventilator at full inspiration

- **Goal: Synchronize portable x-ray with ventilator to obtain image at full inspiration.**
- **Most Chest radiographs are taken at full inspiration to image lungs**
- **Timing of x-ray is usually performed by radiology technician watching the ventilator and/or chest to “catch” the lungs at full inspiration. But, newer anesthesia machine designs block the technician’s view of the ventilator bellows or piston.**
- **For a number of reasons, it is not practical to manually deliver a breath and hold the lungs at full inspiration during x-ray exposure.**
- **Conclusion: Synchronizing the x-ray and ventilator could improve image quality and repeatability, thereby enhancing diagnostic value.**



CPS Security Workshop



Security Hazards for Single Devices

Stand-alone medical devices are (by far) the most common.

- Subject to tampering, reprogramming by unauthorized persons, and device-specific hazards.
- Device firmware may be upgraded over a network or manually, opening additional hazards.



CPS Security Workshop



Security Hazards for Networked Devices

- Network interface provides another avenue for attack
 - Enables remote attacks
 - The more devices there are on the HIS, the more attractive it is as a target
- Unexpected interactions between devices and systems



CPS Security Workshop



Unexpected Interaction: RFID

- Electromagnetic interference by two RFID systems (active and passive) was assessed in the proximity of 41 medical devices (in 17 categories, 22 different manufacturers). The devices included items such as external pacemakers, mechanical ventilators, infusion/syringe pumps, dialysis devices, defibrillators, monitors and anesthesia devices.
- A total of 34 EMI incidents were found.
- The passive signal induced a higher number of incidents (26 in 41 EMI tests; 63 percent), and hazardous incidents (17), compared with the active signal.
- Hazardous incidents included: total switch-off and change in set ventilation rate of mechanical ventilators; complete stoppage of syringe pumps; malfunction of external pacemakers; complete stoppage of renal replacement devices, and interference in the atrial and ventricular electrogram curve read by the pacemaker programmer.

Electromagnetic Interference From Radio Frequency Identification Inducing Potentially Hazardous Incidents in Critical Care Medical Equipment

Remko van der Togt, MSc; Erik Jan van Lieshout, MD; Reinout Hensbroek, MSc; E. Beinat, PhD; J. M. Binnekade, PhD; P. J. M. Bakker, MD, PhD
 JAMA. 2008;299[24]:2884-2890



CPS Security Workshop



Targets of Security Attacks

- Patient's Physical Security
 - Attacks which target the patient
- Patient's Data Security / Privacy
 - Attacks seeking to expose patient's personal information
- Device Physical Security
 - Attacks which target medical devices, including network components
- Institutional Data Security / Privacy
 - Attacks aimed at an institution's private information



CPS Security Workshop



Patient's Physical Security

- Attacks which target the patient's health
- Sample attacks include:
 - Triggering a device to give an additional dose of medication
 - Altering programming of a radiation therapy device, either by corrupting its program directly or by feeding it bad data.
 - Interfering with an implanted device
 - Falsifying printed labels on medication between the pharmacy and the patient
 - Tampering with a patient's EHR to make it appear that they have- or do not have- a medical condition



CPS Security Workshop



Patient's Data Security

- Attacks which seek to expose a patient's personal information
 - HIPAA
- Some examples:
 - An infusion pump is programmed with a patient's age, weight, and the drug they're receiving. Afterwards, the pump is not cleared and the data can be read. Next generation pumps will know the patient's ID and stream data to the EHR.
 - A patient's records are read by curious hospital staff.
 - Medical records are stolen and used to file fake Medicare claims.



CPS Security Workshop



HIPAA

Privacy

The privacy provisions of the federal law, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), apply to **health information created or maintained by health care providers who engage in certain electronic transactions, health plans, and health care clearinghouses**. The Department of Health and Human Services (HHS) has issued the regulation, "Standards for Privacy of Individually Identifiable Health Information," applicable to entities covered by HIPAA.

Security Standard

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for the security of electronic health care information. The final rule adopting HIPAA standards for security was published in the Federal Register on February 20, 2003. **This final rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information.**



CPS Security Workshop



Pacemaker Hacking Example

QuickTime™ and a TIFF (LZW) decompressor are needed to see this picture.

Researchers working with an implantable cardiac defibrillator were able to remotely read telemetry data and reprogram the device.

These devices currently have no safeguards beyond an unpublished, proprietary interface.

Besides the obvious physical hazards, there are also privacy implications.

Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel
IEEE Symposium on Security and Privacy, May 2008

- "To our knowledge there has not been a single reported incident of such an event in more than 30 years of device telemetry use, which includes millions of implants worldwide," a Medtronic spokesman, Robert Clark, said.
- St. Jude Medical, the third major defibrillator company, said it used "proprietary techniques" to protect the security of its implants and had not heard of any unauthorized or illegal manipulation of them.
<http://www.nytimes.com/2008/03/12/business/12heart-web.html?ref=business>



CPS Security Workshop



Medical Device Physical Security

- Attacks which target medical devices, including network components
- Examples:
 - Theft of devices or medication
 - New firmware is uploaded to infusion pumps using their online update feature. This firmware changes pressure limits causing the pumps to burn out their motors.



CPS Security Workshop



Institutional Data Security / Privacy

- Attacks which expose the institution's private information or target network functionality
- Examples:
 - Traffic analysis of the hospital network reveals that patients have a high rate of adverse events.
 - Sniffing the wireless network shows that one brand of device is prone to problems
 - DOS attack makes the hospital network unusable
 - Changes to the hospital's Dose Error Reduction System result in alarms triggering incorrectly or incorrect dosages.



CPS Security Workshop



Developing Secure Medical Devices

- Device manufacturers have a process for safety properties
 - FMEA: Failure Modes and Effects Analysis
 - Safety Cases / Assurance cases
 - Manufacturers must convince the FDA that they have accounted for and mitigated all safety hazards
- An FMEA and assurance case process for security properties, along with formal methods techniques for verifying implementations, gives a pathway for developing secure medical devices.



CPS Security Workshop



Responses

- Tough operating environment:
 - limited resources
 - long lifetime
 - minimally-trained, unsupervised operators
- Taking the human out of the loop:
 - When do we let the FMS override the pilot / operator?
 - "free flight"- limit possible solutions to reduce complexity so humans can follow what's going on
- Importance of supporting legacy systems
- High risk activities based on limited number of tests. Difficulty of obtaining good data to analyze.



CPS Security Workshop



Relevant Standards

- ICE
- ISO 14971:2007, *Medical devices— Application of risk management to medical devices *
- IEC 62304:2006, *Medical device software—Software life cycle processes*.
- HIPAA Privacy Regulations
- HIPAA Security Educational Paper Series
 - There are seven papers in the HIPAA Security Educational Paper Series. The papers currently available include: "Security 101 for Covered Entities", "Security Standards Administrative Safeguards", "Security Standards Physical Safeguards", "Security Standards Technical Safeguards", "Security Standards Organizational, Policies and Procedures and Documentation Requirements" and "Basic of Risk Analysis and Risk Management".
<http://www.cms.hhs.gov/SecurityStandard/>
- New ISO 80002 Standard on Medical Device Security under development
- FDA Guidance Documents



CPS Security Workshop

