Securing Legacy Mobile Medical Devices

Vahab Pournaghshband
Majid Sarrafzadeh
Peter Reiher

Laboratory for Advanced Systems Research

Computer Science Department

University of California, Los Angeles

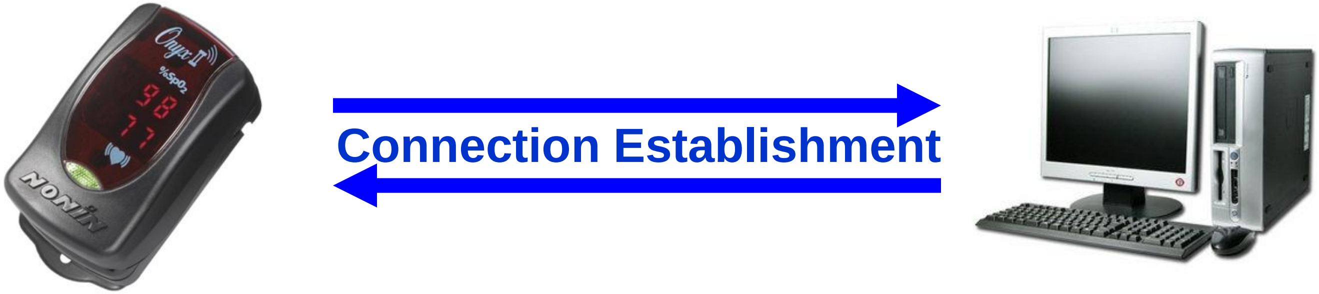
LASR

UCLA

Overview

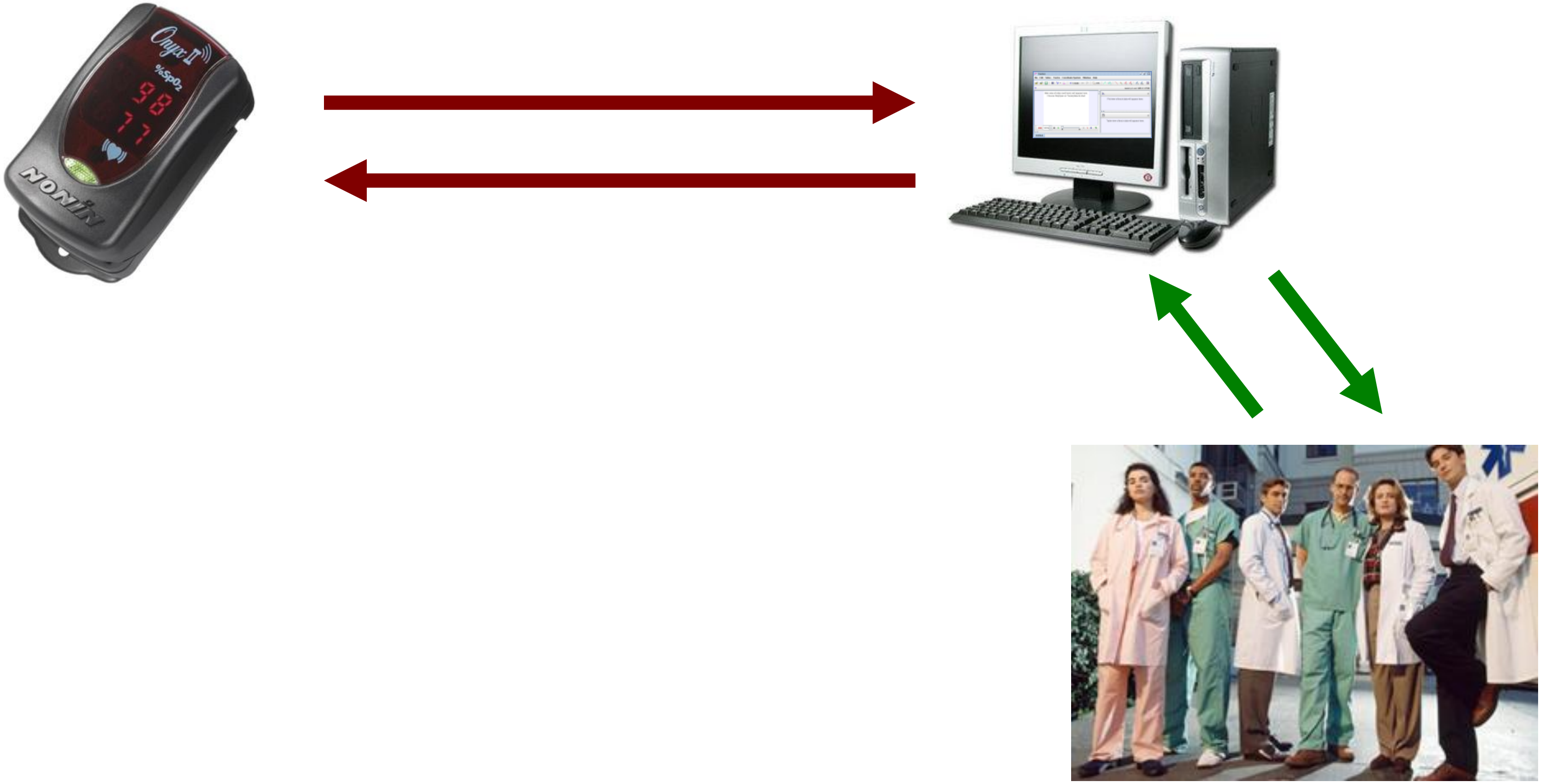
- How Mobile Medical Devices Work?
- MITM Attack
  - Position the Man-in-the-Middle
  - Threat Model
  - Reverse-engineering the Protocol
- Defense
  - Defense Mechanism Characteristics
  - Personal Security Device
  - Discussion
- Summary

How Do They Work?



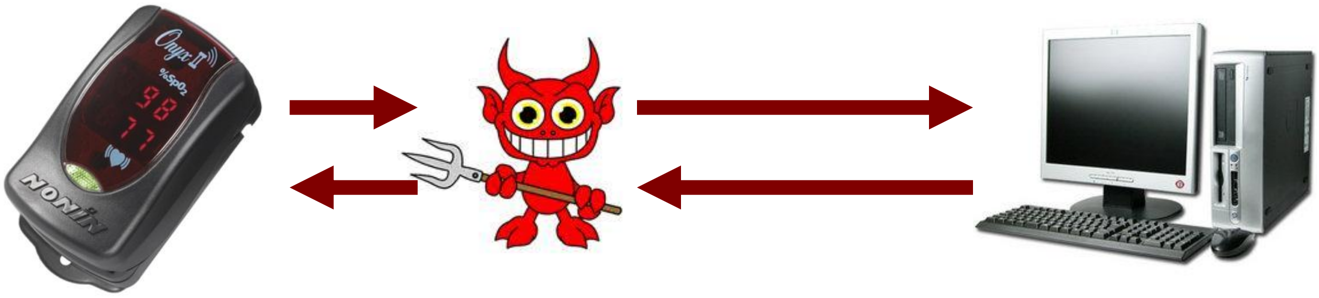
Connection Establishment

How Do They Work?



MITM Attack

Nonin Pulse Oximeter

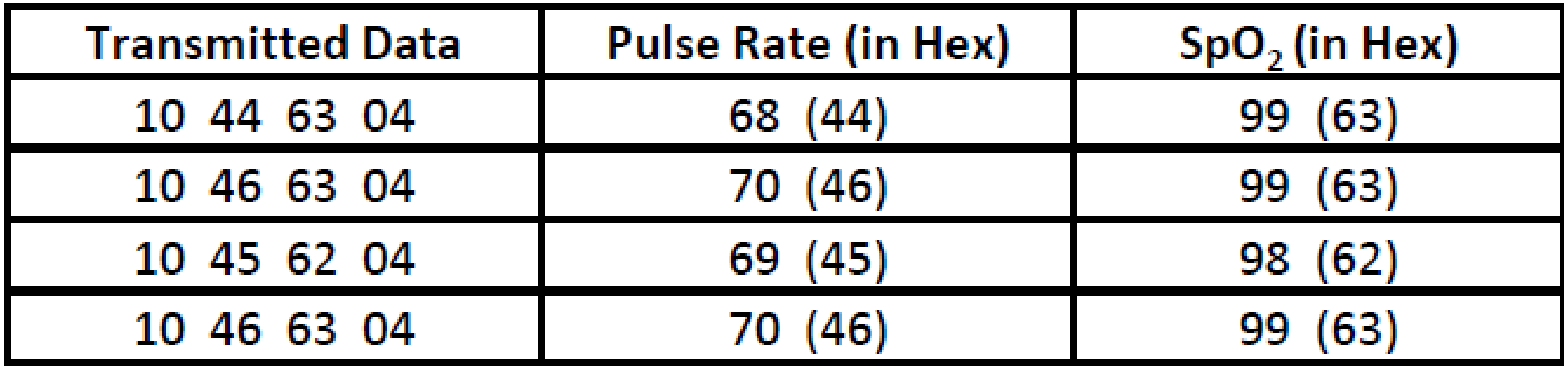


Threat Model

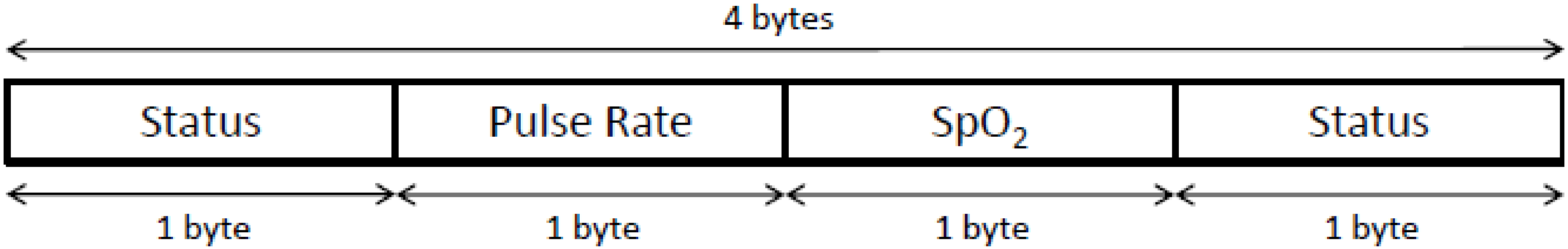
- Confidentiality
  - *Eavesdropping*
  - *Retrieve private information*
- Integrity
  - *Altering data*
  - *Replay attack*
  - *Generating fake data or unauthorized commands*
- Availability

MITM Attack

Reverse-engineering the protocol:



Transmitted Data	Pulse Rate (in Hex)	SpO_2 (in Hex)
10 44 63 04	68 (44)	99 (63)
10 46 63 04	70 (46)	99 (63)
10 45 62 04	69 (45)	98 (62)
10 46 63 04	70 (46)	99 (63)



4 bytes

Status	Pulse Rate	SpO_2	Status
1 byte	1 byte	1 byte	1 byte

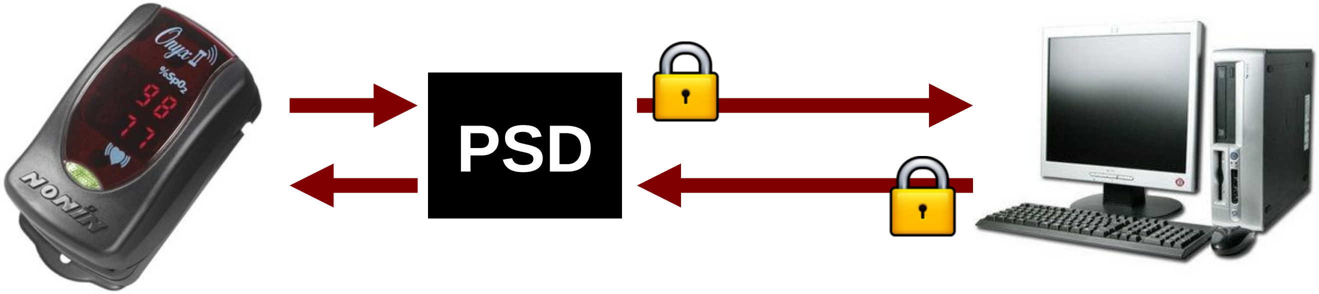
Defense

Desirable Characteristics of a Mechanism:

- Security vs. Responsiveness
- Security vs. Availability
- No Changes to the Medical Device
- No Changes to the Monitoring Software

Defense

Personal Security Device (PSD):



Discussion

- Fail-open property
- Less burden on medical device’s resources
- Little understanding of the protocol
- Any radio technology for PSD-AP link
- Extended to other radio technologies

Summary

- Existing devices are vulnerable to MITM attacks
- MITM attacks threaten safety and privacy of patients
- PSD improves security of the existing systems