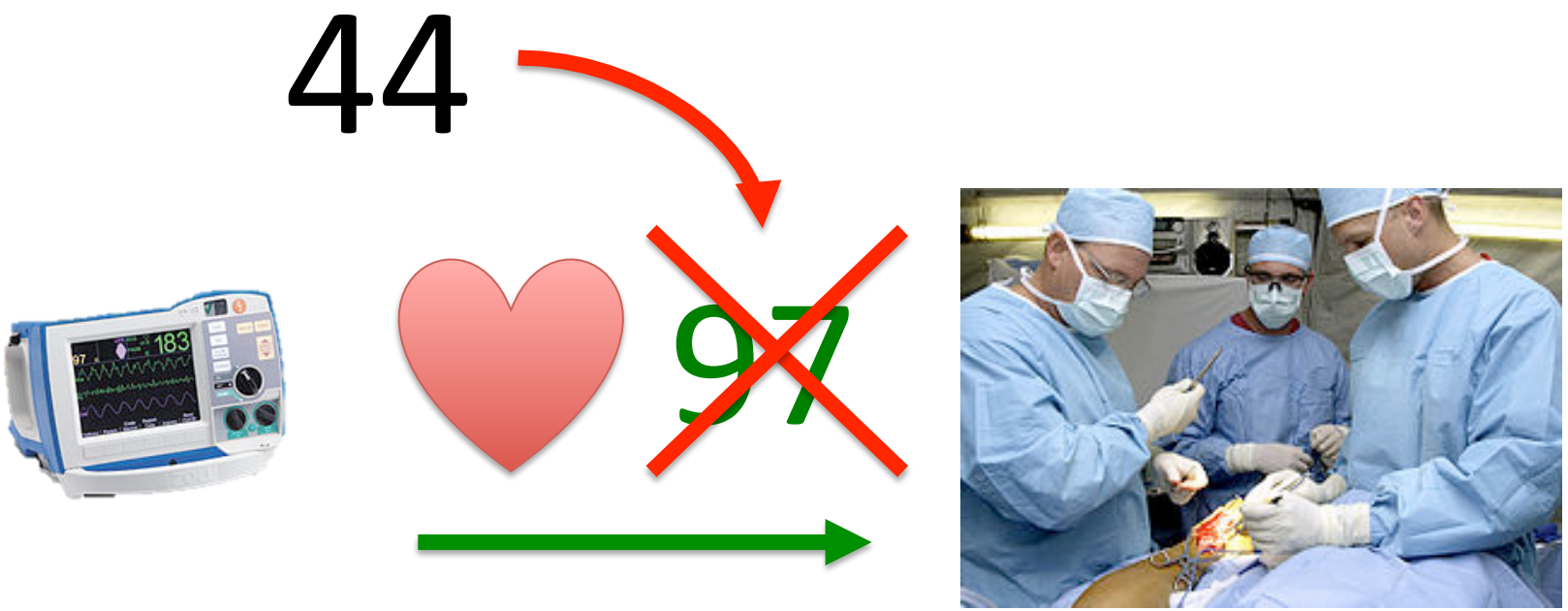
Trust of Medical Devices, Applications, and Users in Pervasive Healthcare

Michael Clifford and Matt Bishop, UC Davis Computer Security Laboratory

Sensors, Devices, Doctors, and the Patient Form a Network

Sensors, devices, patients, and doctors send each other data

Devices May Be Compromised or Manipulated by Attackers or Malfunctions



Example: A malicious nurse alters the data from a device. The altered data is used by a doctor or device, killing the patient!

The Threat Model

- The hospital can not control every data source
- Patients, caregivers, or even strangers may have access to sensors and devices
- Data sources may be networked, and could be attacked from outside!

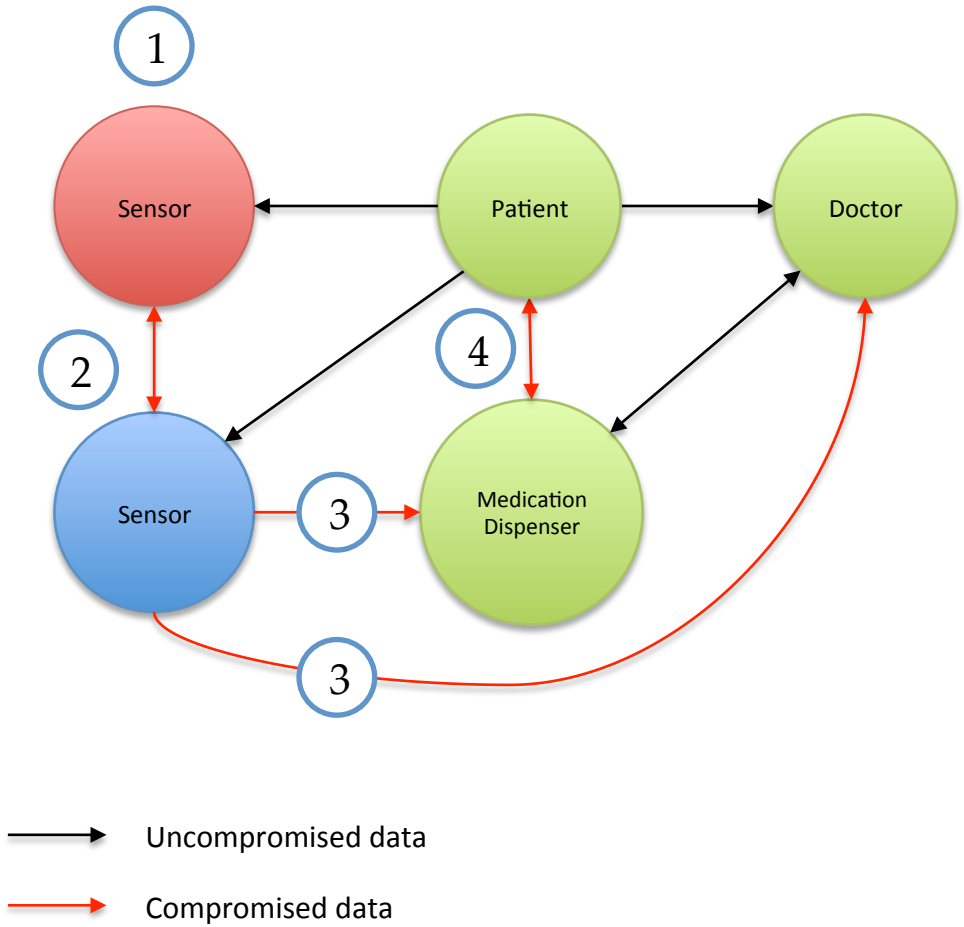
Existing Healthcare Trust Models

- Protect patient privacy and data integrity by restricting access to those who are trusted
- Some address context sensitivity
- Some address the trustworthiness of users to *access* data
- They are designed to protect patient privacy, and medical record integrity
- But…they don't examine data *source* trustworthiness!

Untrustworthy Data Sources May Provide Bad Data

- Existing health care trust models don't provide assurance that data sources are trustworthy
- This leaves data sources such as sensors and devices open to attack and manipulation.
- We'd like to provide assurance that patent data *sources* are trustworthy

Example – Insider Manipulates Data From a Device



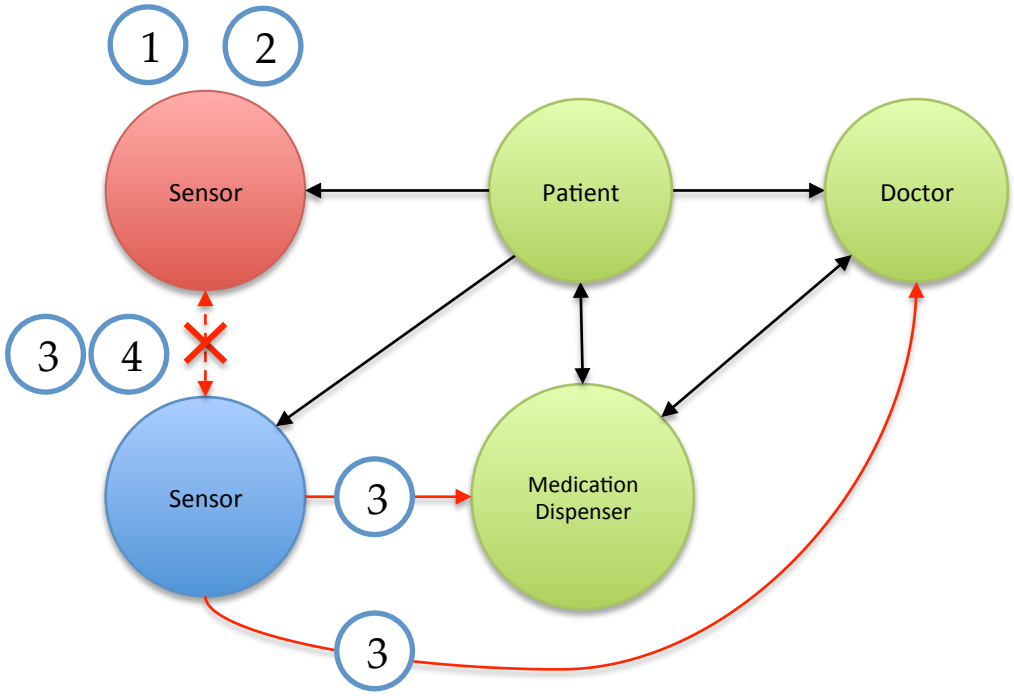
1. An attacker takes control of a sensor used to monitor the patient.
2. The attacker causes the sensor to transmit incorrect data to another sensor.
3. The bad data, and calculations based on it, propagate through the network, corrupting decisions made by devices and doctors that depend on it.
4. The bad data causes the wrong dosage of medicine to be dispensed, killing the patient.

What we need in a trust model

- Doctors, patients, and devices should be able to determine how much data from different sources can be trusted relative to each other, or to known baselines

- Using that information, we can determine whether to utilize information from each source in different contexts

How the Solar Trust Model Handles a Compromised Data Source



Uncompromised data

Compromised data

Insufficiently trustworthy data

Edge removed from network

1. An attacker takes control of a sensor used to monitor the patient.
2. The attacker causes the sensor to transmit incorrect data to another sensor.
3. Policies and heuristics cause the path followed by potentially malicious data to become less trustworthy
4. Data sent along paths incorporating the compromised sensor is no longer trusted. The sensor is isolated from the network.
5. In some cases, it is possible to route around untrusted sources, selecting only sufficiently trustworthy ones.

Conclusion

- Pervasive healthcare has a different threat model than traditional healthcare
- Traditional models address patient privacy and data integrity, but not trust of data sources
- The Solar Trust Model addresses trust of data sources, providing assurance to patients and doctors that data sources are less open to manipulation, malfunction, and attack