

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

Michael Clifford and Matt Bishop  
UC Davis Computer Security Laboratory  
PETRA 2011

**A Patient in a Pervasive Healthcare Environment**

Many devices monitor the patient

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

Sensors and devices send each other data...

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

...and communicate with doctors and nurses

**Devices May Be Compromised or an Insider May Manipulate Them**

Example: a malicious nurse alters the data from a device

**Devices May Be Compromised or an Insider May Manipulate Them**

Example: a malicious nurse alters the data from a device

**Devices May Be Compromised or an Insider May Manipulate Them**

The altered data is used by a doctor or device, killing the patient!

**Devices May Malfunction For Non-Malicious Reasons**

Devices might provide bad data

...or no data!

**Threat Model**

In a pervasive computing environment, there may be much less control over devices than in a hospital

### Threat Model

This makes the threat model very different!

### 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!

### Healthcare Trust Models

- Other trust models grant or deny access to patient data, allow certain people to add to existing records
- These extend access control mechanisms in Role Based Access Control

### Example of Role Based Access Control

Doctors can read and append data, but not alter it

### Example of Role Based Access Control

Doctors can read and append data, but not alter it

### Example of Role Based Access Control

Doctors can read and append data, but not alter it

### Example of Role Based Access Control

Patients can only read data, not append or alter it

### Example of Role Based Access Control

Patients can only read data, not append or alter it

### Example of Role Based Access Control

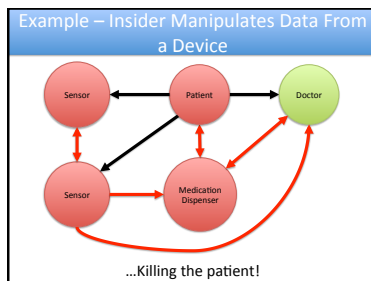
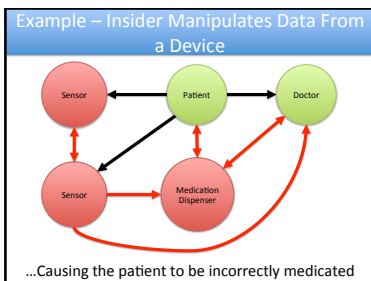
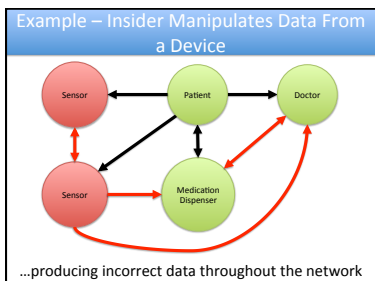
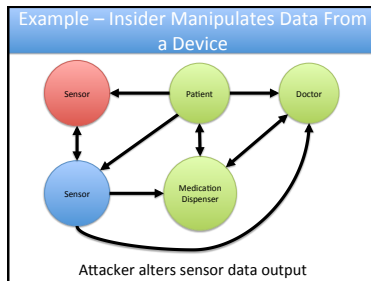
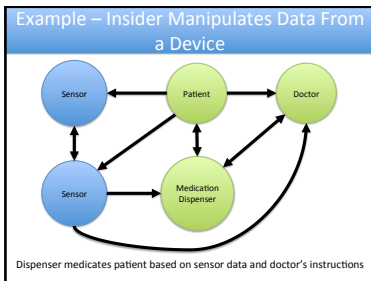
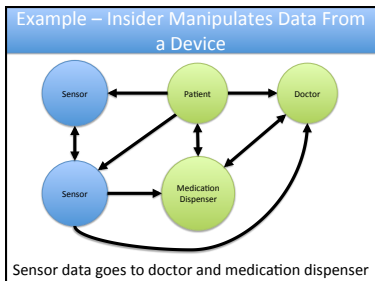
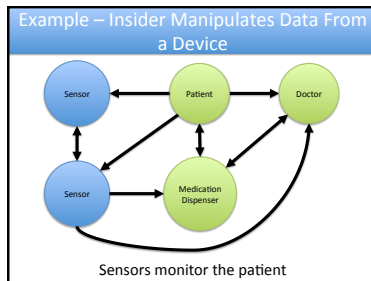
Patients can only read data, not append or alter it

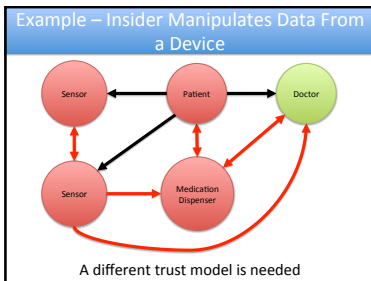
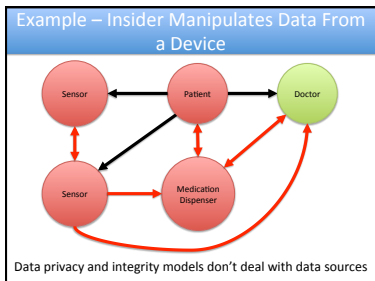
### Healthcare Trust Models

- 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
- Don't examine data **source** trustworthiness!
- These models protect patient privacy, and medical record integrity

### Why This is a Problem

- They don't provide assurance that the 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 patient data **sources** are trustworthy
- Existing healthcare trust models don't let us do that!



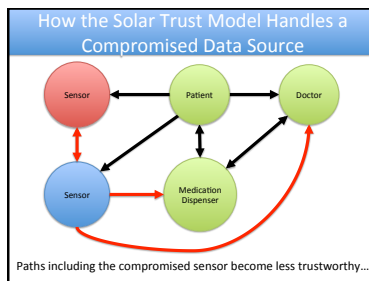
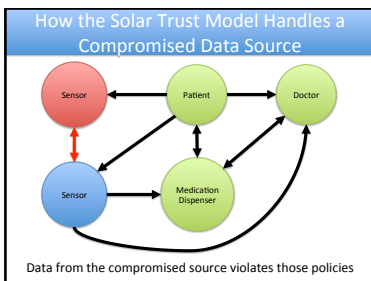
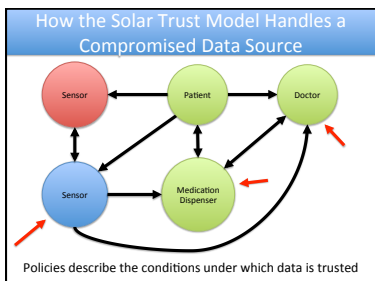
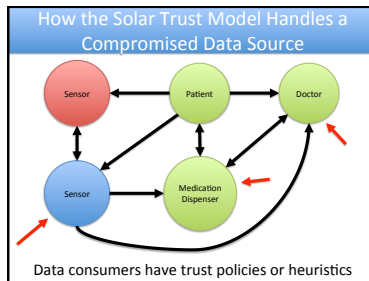
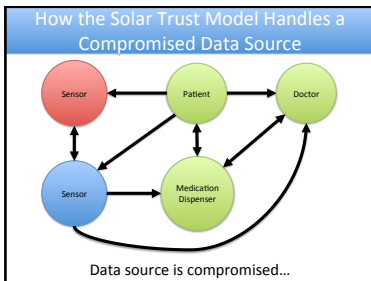


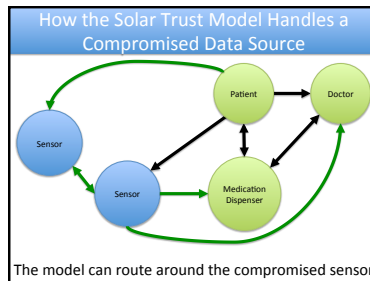
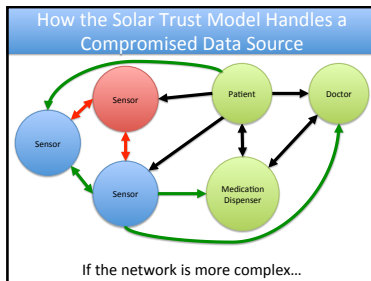
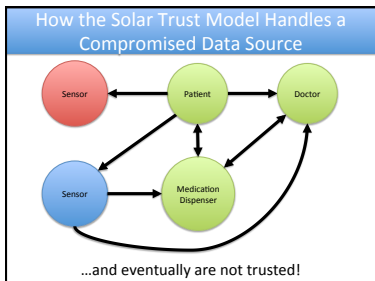
**What we need in a trust model**

- Doctors, patients, and devices should be able to determine how much data from different sources can be trusted relative to each other, or to baselines
- Using that information, we can determine whether to utilize information from each source in different contexts

**The Solar Trust Model**

We can apply the Solar Trust Model to solve this problem





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 STM addresses trust of data sources, providing assurance to patients and doctors that data sources are less open to manipulation, malfunction, and attack

Questions?

?