Leadership in Embedded Security

Breakout 1 - Medical/Wearable

CCC

Computing Community Consortium

Catalyst

Identify 3 Key Challenges in the Application Area

- Balancing safety, security, and usability in different use cases
  - Different users and situations
  - Security, privacy, and usability are sometimes in conflict
- Long legacy tail
  - Long installed base of hardware
  - Users (e.g., clinicians) have huge training burden, limiting options to change interfaces and add new procedures such as authentication
  - Regular patching over long lifetimes
  - Patching is situation dependent (e.g., patient can't be in the OR)
- Power and energy constraints of wearable, mobile, and implantable devices
- Regulation of safety and privacy does not cover all attack situations
  - e.g., using devices as pivot into clinic network

Identify 3 Key Trends in the Application Area

- Software as a service on the cloud
- Increasing variability of patients/users (elderly, child, soldier) and locations (home/clinic/battlefield)
- Globalization
  - supply chain
  - users
  - mobility of users - how to update implanted device on person in third world area without network?
- More closed loop systems
  - Previous devices often open loop; closing with new sensors and network
  - Previous device, even if closed loop, are independent. New clinical environments are composing control loops between multiple devices
- Wellness apps and devices blurring the space with medical clinical devices
  - Unregulated wellness apps and devices without safety & security properties are growing into regulated space

Identify 3 Potential Novel Solutions in the Application Area

- Leverage physics and locality/distance for authentication
  - Patients, clinicians, and caregivers
- Application of classic control theory to develop and adapt closed loop systems
  - The medical device “physical plant” (the human) is highly variable
- Leveraging the individual variability is a potential solution to solving a task such as authentication, perhaps can be exploited for individualized therapies
- Security by architecture (e.g., fault tolerant) can assure the safety and security of the system despite the failure of any individual component
  - This is different from the typical IT approach of release, test on users, patch, and repeat
- Building things that have appropriate fail back conditions for disruptions
- Education for embedded systems security and safety

Identify 3 Key Challenges in the Application Area

•Reconciling security and safety for medical devices where the two properties collide

The risk equation is different for safety (probability, past predicts future) versus security (adversarial model, vulnerabilities only get worse over time)

•Privacy for health and wellness devices that have access to sensitive personal data and lifestyle information

•Moving paradigm from patching software never to patching monthly or continuously on medical devices

•Low power

- Balancing between safety, security, and useability in different use cases
- Long legacy tail of the devices and components in this space - the need to now go to a regular patch system will both increase the cost and create timing challenges (ex. patient can't be in the OR)
- Power and energy to manage across different types of devices
- Regulation of safety and privacy doesn't cover all attack situations

CCC
Computing Community Consortium
Catalyst

Identify 3 Key Trends in the Application Area

•Increasing variability of patients/users (elderly, child, soldier) and locations (home/clinic/battlefield)

Therefore one security solution is unlikely to fit all patient profiles and locations.

•Asdfadf

- Globalization
- More closed loop systems
- Wellness apps and devices blurring the space with medical clinical devices

CCC
Computing Community Consortium
Catalyst

Identify 3 Potential Novel Solutions in the Application Area

•Control theory hierarchies (Insup)?

•Leveraging physics and locality to authenticate between devices/patients and infrastructure

•Ulparem re simendi gnatiorae doloresti tecta nam qui

•Nam qui officiminis dolorroovit

•Asdfasdf

•Asdfadf

- Leverage physics and locality/distance for authentication
- Application of classic control theory to develop and adapt more closed loop systems with the understanding the physical plant strongly varies
-