

Embedded Systems and Ubiquitous Computing

Connected Systems — Privacy, Security, Safety

CSE 199

Fall 2017

Connecting Embedded Systems

Embedded systems are increasingly connected.

- Communication is getting cheaper
- Wireless uses less power, has more bandwidth
- Market expectations

This magnifies concerns related to privacy, security, and safety.

Connected Sensors

Sensors have become very inexpensive.

Cheap sensors + cheap wireless = connected sensors

Sensors let embedded systems gather data about the world.

As human beings, we do not naturally expect **inanimate objects** to be **collecting data about us** or our activities.

Embedded Systems and Privacy

Connected systems have **privacy implications**.

If a system can communicate, it can probably communicate with **malicious actors**.

Embedded systems are everywhere.

Embedded Systems and Security

Attack surface:

software interfaces exposed to malicious code or users

Connecting systems:

- Increases access to their attack surface
- Often enlarges this surface

Internet connectivity brings particular risk.

Security problems **amplify privacy problems**.

Embedded Systems and Safety

Failure of some embedded systems can cause **harm**.

That harm may be to:

- Human health or life
- Physical infrastructure
- Economic transactions

Privacy Violations

- HVAC information may reveal occupancy
- Smart TVs, Alexa, Siri are always listening
- Car infotainment / navigation systems may reveal location
- Pacemaker data has been used in court

Samsung Smart TV Fiasco

SAMSUNG

Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

Samsung later clarified that this is not continuous surveillance.

However, WikiLeaks documents claimed that Samsung TVs had been used by intelligence services for spying!

Ford Cars Track Location



James Farley, Ford VP
of Marketing and Sales

We know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing. By the way, we don't supply that data to anyone.

He later clarified:

I absolutely left the wrong impression about how Ford operates. We do not track our customers in their cars without their approval or consent.

Pacemaker Data Used in Court



Police obtained a warrant for the pacemaker data of Ross Compton of Middletown, Ohio.

This data was used as evidence that his testimony was inconsistent, and an indictment against him was obtained.

Connected Security


There are two kinds of embedded security concerns:

- The security of the software on embedded systems
 - Quality and resistance to unwanted intrusion
 - Reliability in the face of attacks
- Embedded systems in security roles
 - Physical security: locks, cameras, alarms, ...
 - Data security: firewalls, encryption devices, ...

Physical Security

- Schlage, Kwikset, Yale, *etc.* offer connected locks
- Access controls for prisons, nuclear plants, banks
- Safes, ATMs, deposit boxes

Hacking an ATM

Positive Technologies ATM physical security hack (July 2017) 

This is just a normal computer [...] it's just a safe with a computer on top.

Prison Cells

Lucas Lundgren explored vulnerabilities in MQTT

- MQTT is a protocol used for embedded systems communication
- Reported at Black Hat 2017

He found a **prison** with exposed MQTT **on the Internet**.

He was able to see doors opening and closing ...

...and issue commands to open or close them!

Data Security

- Security keys (Yubico, *etc.*)
- Authentication dongles (*e.g.* RSA SecurID)
- Firewall appliances

But also ...

- Toys
- Appliances
- Assistants

CloudPets hack

Spiral Toys' *CloudPets* teddy bears are controllable via Bluetooth.

Paul Stone of Context reports that they use *no security*.

They can:

- Take recordings
- Upload recordings
- Speak on command
- Download messages to speak

...all over that insecure Bluetooth! 

Safety

Embedded systems can control **dangerous things**.

- Dangerous when operating
- Dangerous **if they fail**

Generator Failure



In 2016, the controller on my standby generator failed.

I don't rely on a generator, but what if I had?

- Oxygen
- Critical refrigeration
- *etc.*

Medical Devices

27 FDA **Class 1 recalls** so far this year (Sep 12 2017).
Eleven are obviously embedded systems problems.

[Class 1 recalls are] ...the most serious type of recall. Use of these devices may cause serious injuries or death.

Abbott-Thoratec has received a total of 70 reports of incidents, including 19 injuries and 26 deaths [...] when patients attempted to exchange [backup system controllers] while away from the hospital. [...] Abbott-Thoratec is providing [...] users with new software and hardware updates[.]

Safety-critical Systems

Safety-critical systems are systems where failure may result in injury or the loss of life, extreme economic damage, or environmental damage.

Example Safety-critical Systems

- Avionics
- Airbag controllers
- Nuclear reactor control systems
- Traffic signals

Mixed-criticality Systems

Mixed-criticality systems contain both safety-critical components and non-critical components.

Some organizations (such as the military) may define other levels of criticality.

- Mission critical
- Low critical
- *etc.*

Criticality Concerns

Safety- and mission-critical systems must account for:

- Failures
- Limited resources
- Service interruptions

Mixed-criticality systems must also manage interplay between criticality levels.

Conclusions

As embedded systems become more connected and more capable, we must work harder to address:

- Privacy
- Security
- Safety

We need **You** to help avert a connected dystopia!