Zurich Information Security and Privacy Center (ZISC)

Srdjan Čapkun
ZISC Director
ZISC is a Security and Privacy Research Center of ETH Zurich

- Enables collaborations between ETH, industry and public institutions
- **Open Lab:** a collaborative space for ETH-industry collaboration
- 60 researchers
  - From cryptography to wireless security
  - Blockchains, E-voting, Secure Internet, Secure Positioning, Formal Verification, Policy Monitoring
Security Startups (recently) Created by ZISC Students/Faculty

- **3db**: Secure Ranging Technology (IoT)
- **Anapaya Systems**: Secure Networking Solutions
- **exeon analytics**: Security intelligence Network Analytics
- **SOUND PROOF**: Usable Authentication Solutions
- **xorlab**: Malware Detection
- **DEEP CODE**: Code Generation / ML
On the (In)security of our Cyber-Physical World

Srdjan Capkun (Srđan Čapkun)
ETH Zürich
Security and Privacy: Data Confidentiality

configuration error

leak

vulnerability

poor security

configuration error

http://www.informationisbeautiful.net/
Security and Privacy: Data Confidentiality

http://www.informationisbeautiful.net/
Security and Privacy: **Everything** is Being Hacked

**The New York Times**
A Heart Device Is Found Vulnerable to Hacker Attacks

Doctors disabled wireless in Dick Cheney’s pacemaker to thwart hacking

We hacked U.S. drone: Iran claims it electronically hijacked spy aircraft’s GPS and tricked aircraft into landing on its soil

- RQ-179 Sentinel drone has been seen on display by Iran’s growing military
- Engineer claims Iran downed drone by using fake signals to confuse it
- Claimed GPS signals are easy to hack without cracking U.S. control codes
- Alleges aircraft’s GPS weakness was long known to U.S. military officials

How Drones Can Find and Hack Internet-of-Things Devices From the Sky

Mapping Security researchers have developed a Flying Drone with a custom-made tool capable of sniffing out data from the devices connected to the Internet - better known as the Internet-of-Things. Under its Internet of Things Map Project a team of security researchers at the Texas-based firm [...]

**The New York Times**
Keeping Your Car Safe From Electronic Thieves

Last week, I started keeping my car keys in the freezer, and I may be at the forefront of a new digital safety trend.
Security and Privacy: We Are Backing Off

France drops electronic voting for citizens abroad over cybersecurity fears

WORLD NEWS | Mon Mar 6, 2017 | 12:19pm EST

Doctors disabled wireless in Dickson pacemaker to thwart hacking

How Drones Can Find and Hack Devices From the Sky

The New York Times
A Heart Device Is Found Vulnerable

Srdjan Čapkun
June 26, 2017
Cyber-Physical Systems - What Are We Afraid Of?
Cyber-Physical Systems - What Are We Afraid Of?

Srdjan Čapkun

June 26, 2017

Copyright ETH Zurich
Afraid of Attacks that can do **Physical** Harm

- Cyber-Physical Systems have real physical impact on our environment
- Sense the environment **[spoofed?]**
- Controlled by computers **[hacked?]**
- Act on the environment **[ouch?]**
Afraid of Attacks that can do **Physical Harm**

**Security**

*Move over, Stuxnet: Industroyer malware linked to Kiev blackouts*

Modular nasty can seize direct control of substation switches and circuit breakers

*By John Leyden 12 Jun 2017 at 15:36*
Spoofing of Radar, Ultrasonic Sensors, and Cameras (Tesla)
Spoofing Position: GPS Spoofing Attacks and Defenses

- ZISC researchers demonstrated GPS spoofing attacks
- https://securepositioning.com
- https://zisc.ethz.ch
Spoofing **Distances**: Relay Attacks on Cars

- In 2011 We Published First Attack Against PKES Systems

- **Attack Allows to Open and Start All Modern Cars**

- **Cost went down from 1000$ (2011) to 22$ (2017)**
Hack into Cars & Protect Cars
SW/HW hacking of Legacy and Embedded Systems

- Fridges, lightbulbs, insulin pumps, energy substations, PLCs,

---

*Medical devices are the next security nightmare*

IoT malware behind record DDoS attack is now available to all hackers

The Mirai trojan enslaved over 380,000 IoT devices, its creator claims

---

FDA confirms that St. Jude's cardiac devices can be hacked

by Selena Larson   @selenalarson

January 9, 2017: 3:50 PM ET
SW/HW hacking of Legacy and Embedded Systems

- Fridges, lightbulbs, insulin pumps, energy substations, PLCs,

“"The FDA confirmed that St. Jude Medical's implantable cardiac devices have vulnerabilities that could allow a hacker to access a device. Once in, they could deplete the battery or administer incorrect pacing or shocks.""

FDA confirms that St. Jude's cardiac devices can be hacked

by Selena Larson  @selenalarson

January 9, 2017: 3:50 PM ET
Recent ZISC research: compromise input so that the operator doesn’t notice before physical damage
Privacy

Alexa, what other devices are listening to me?

By Elliott C. McLaughlin, CNN

Updated 2245 GMT (0645 HKT) January 12, 2017

Killing car privacy by federal mandate

JUNE 21, 2017 BY LEONID REYZIN 3 COMMENTS

The US National Highway Traffic Safety Administration (NHTSA) is proposing a requirement that every car should broadcast a cleartext message specifying its exact position, speed, and heading ten times per second. In comments filed
Why is This Happening

- Why is this happening?
  - High Complexity and Interconnectivity of Systems
  - Wide-Spread Knowledge and Available Tools
  - Traditional Industries Still Playing Catch-Up
  - Underestimation of cost / attacker’s knowledge
  - ‘Post-Snowden’ World

- Unless not addressed
  - Will Prevent the Deployment of Many Technologies / Stall Progress
  - Will Negatively Impact the Development of our Societies
No ‘Silver Bullet’
No ‘Silver Bullet’: We Just Need to Solve Many Challenges

- Software/Hardware Attestation
- Spoofing Detection Techniques
- Robust ML/AI
- Formal Protocol and Software Verification

- Better Practices and Awareness (Education)
- Not equate Compliance with Security

- & we need new enabling technologies!
Example: Preventing Distance Spoofing

- Developed new **Secure Distance Measurement** Techniques
- >200m range, 15cm LoS precision

(3DB Access)
Example: Detecting GPS Spoofing

- Built First Open Source Spoofing-Resistant GPS Receiver
- [https://www.spree-gnss.ch/](https://www.spree-gnss.ch/)

---

Srdjan Čapkun | June 26, 2017 | 26
Example: Remote (Software) Attestation

- Remotely Attest the state (i.e., code) of a device
Physical World Provides Opportunities: Secure Distance Meas.

- If key fob close (1m) to the car/door => unlock the car/door
- If laptop close (1m) to the access point => allow network access
- If phone in the building/room => allow access to data
- If phone/card close (20cm) to the terminal => execute payment
- If bracelet close (10cm) to the gun => allow the gun to be fired
- If two devices close (10cm) => establish keys

- Secure Distance Measurement => Usable Security (in these contexts).
Physical World Provides Opportunities: Online Authentication

Users use easy passwords and reuse the same passwords for various applications. 3 billion passwords have been stolen in the last 9 years.

That’s why companies use strong authentication.
Physical World Provides Opportunities: **Online Authentication**

- **Soundproof: Usable, Continuous Authentication by Ambient Sound**

  1. login
  2. compare recordings

  if recording the same sound
  => PC/phone in the same room
  => user is next to the terminal

[www.futurae.com](http://www.futurae.com)
In a complex, multipath-rich environment, channels exhibit \textit{time-varying, stochastic and reciprocal} fading.

For receivers that are $> \lambda/2$ away, channels are not correlated.
Conclusion

- **Cyber Physical Systems present both Challenges and Opportunities**

- They act on our environment and thus present danger.

- They exist in our environment and can therefore help us build more usable and secure systems.