



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



Secure Ranging Technology (IoT)

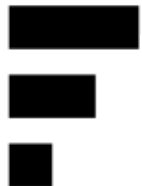


Anapaya Systems
Reinventing the Internet

Secure Networking Solutions

exeon
analytics

Security intelligence
Network Analytics



SOUND PROOF

Usable Authentication Solutions

Other Security-Related Startups in Computer Science @ ETHZ

xorlab

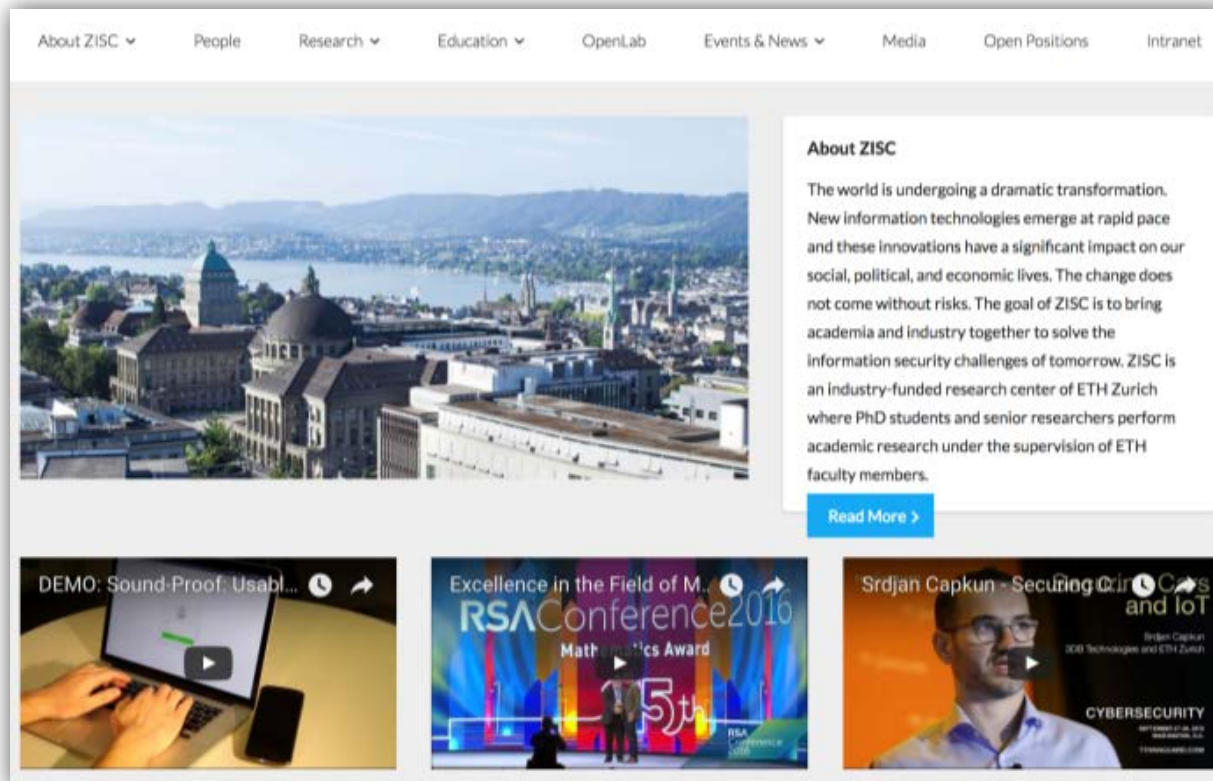
Malware Detection

DEEPCODE

Code Generation / ML

ZISC @ ETH Zurich

<https://www.zisc.ethz.ch>

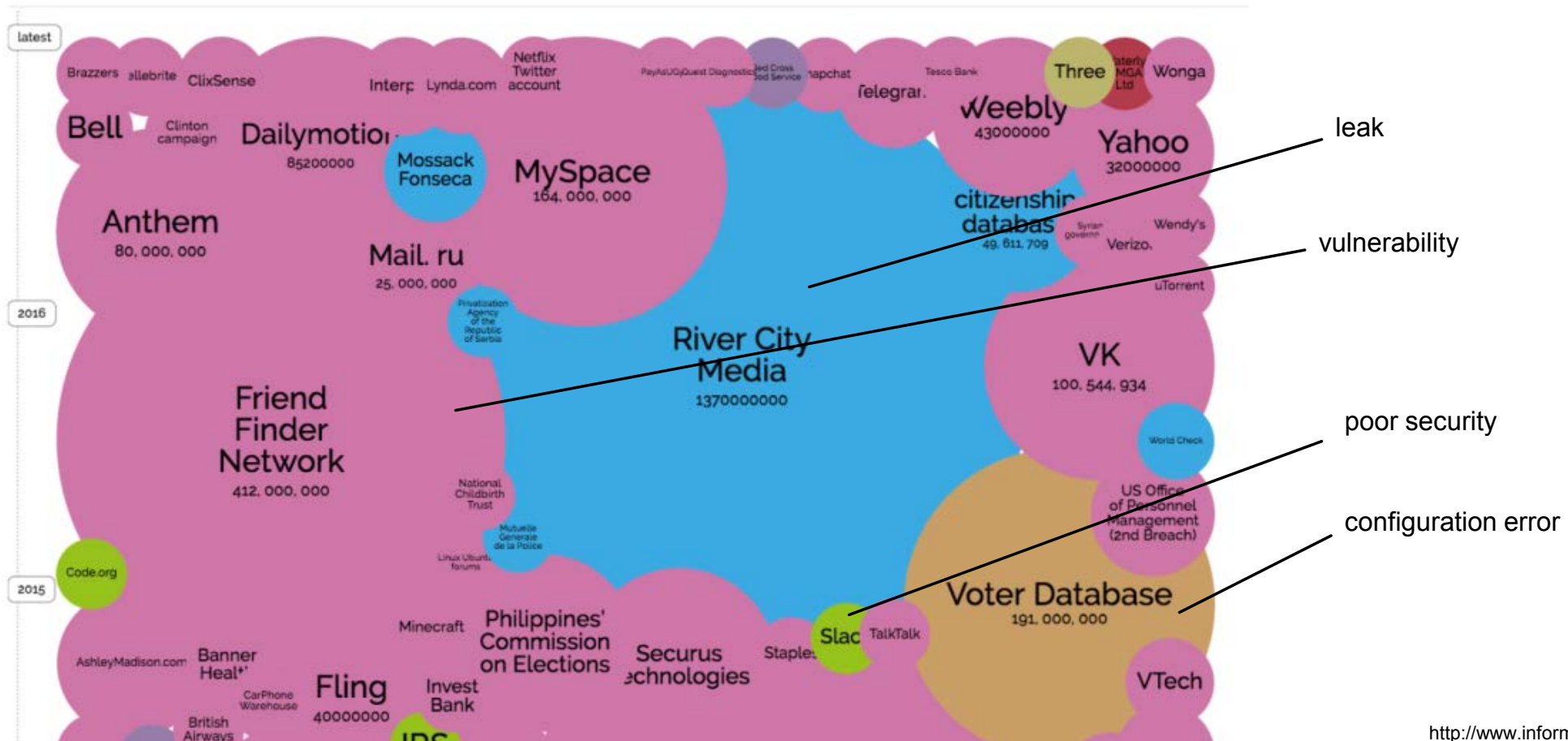




On the (In)security of our Cyber-Physical World

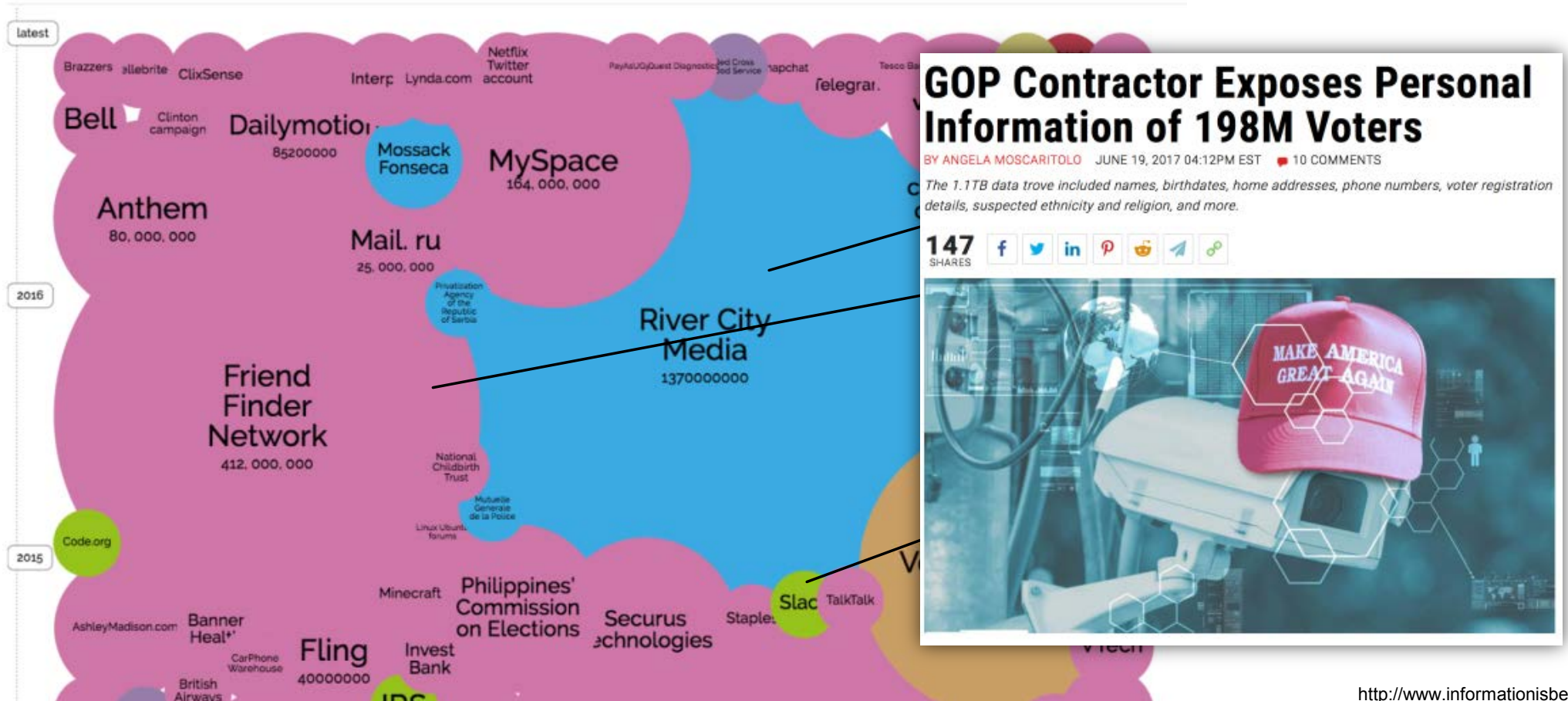
Srdjan Capkun (Srđan Čapkun)
ETH Zürich

Security and Privacy: Data Confidentiality



<http://www.informationisbeautiful.net/>

Security and Privacy: Data Confidentiality



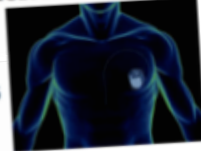
<http://www.informationisbeautiful.net/>

Security and Privacy: **Everything** is Being Hacked

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

By BARNABY J. FEDER
Published: March 12, 2008

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-170 Sentinel drone has been seen on display by Iran's gloating 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

Friday, August 07, 2015 Mohit Kumar

1 Like 1 Retweet 617 297 26 1019



Security researchers have developed a Flying Drone with a custom-made tracking 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.



RollJam — \$30 Device That Unlocks Almost Any Car And Garage Door

Sunday, August 08, 2016 Khyati Jain

340 1 Like 2 Retweets 2954 420 28 4294



We have talked a lot about car hacking. Recently researchers even demonstrated how hackers can remotely hijack Jeep Cherokee to control its steering, brakes and transmission. Now, researchers have discovered another type of car hack that can be used to unlock almost every car or garage door. You [...]

Security and Privacy: We Are Backing Off



Cyber-Physical Systems - **What Are We Afraid Of?**

Cyber-Physical Systems - **What Are We Afraid Of?**

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

ANDY GREENBERG SECURITY 08.04.16 09:00 AM

HACKERS FOOL TESLA S'S AUTOPILOT TO HIDE AND SPOOF OBSTACLES



Security

30

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

SHARE ▼

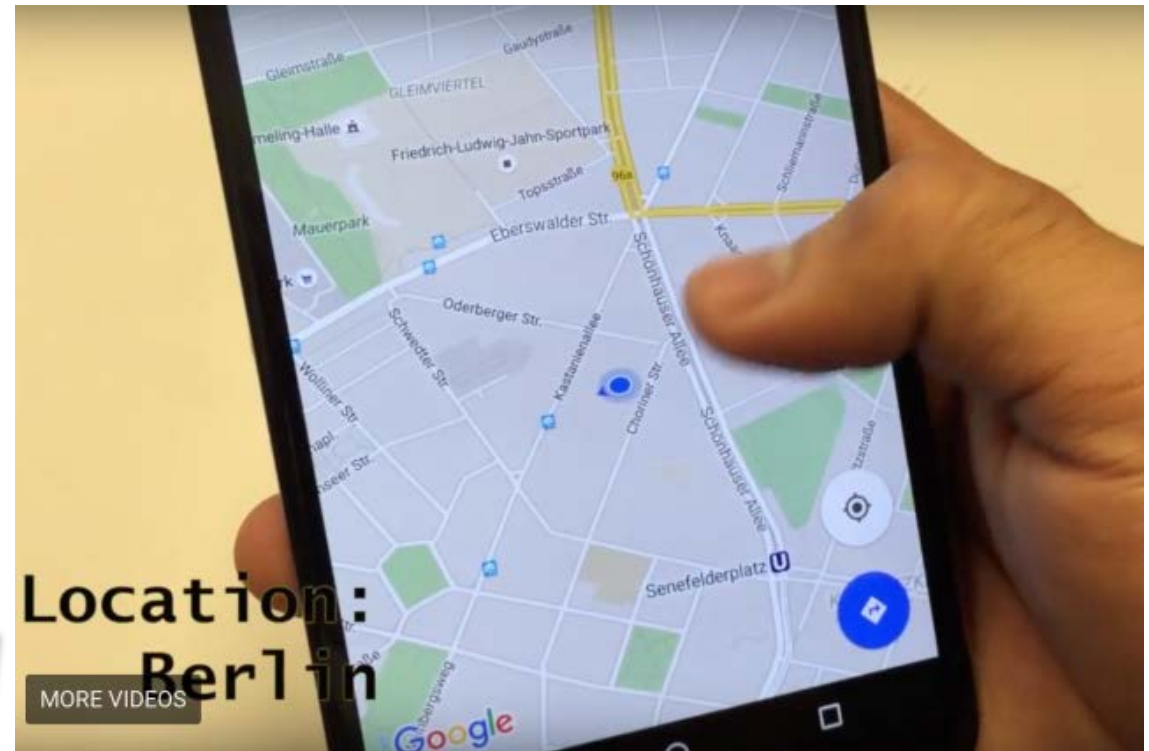


Spoofing of Radar, Ultrasonic Sensors, and Cameras (Tesla)



Spoofing **Position**: GPS Spoofing Attacks and Defenses

- ZISC researchers demonstrated GPS spoofing attacks
- <https://securepositioning.com>
- <https://zisc.ethz.ch>

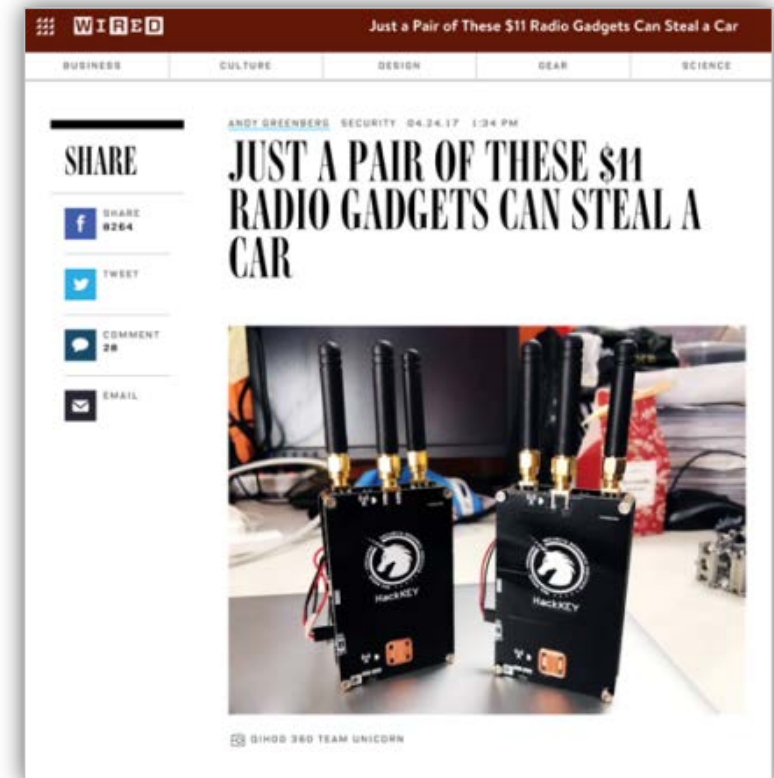


Spoofing Distances: Relay Attacks on Cars

- 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,



NEWS

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

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



CNN tech

BUSINESS

CULTURE

GADGETS

FUTURE

STARTUPS

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

by Selena Larson @selenalarson

🕒 January 9, 2017: 3:53 PM ET

👍 Recommend 1.6K



SW/HW hacking of Legacy and Embedded Systems

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

LILY HAY NEWMAN SECURITY 03.02.17 10:30 AM

MEDICAL DEVICES ARE THE NEXT SECURITY TARGET



“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**”

NEWS

IoT malware behind record DDoS attack is now

creator claims

STARTUPS

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

by Selena Larson @selenalarson

🕒 January 9, 2017: 3:53 PM ET

👍 Recommend 1.6K



Dedicated Programmers, Control Interfaces of Robots, Machinery



Pacemaker
Programmer

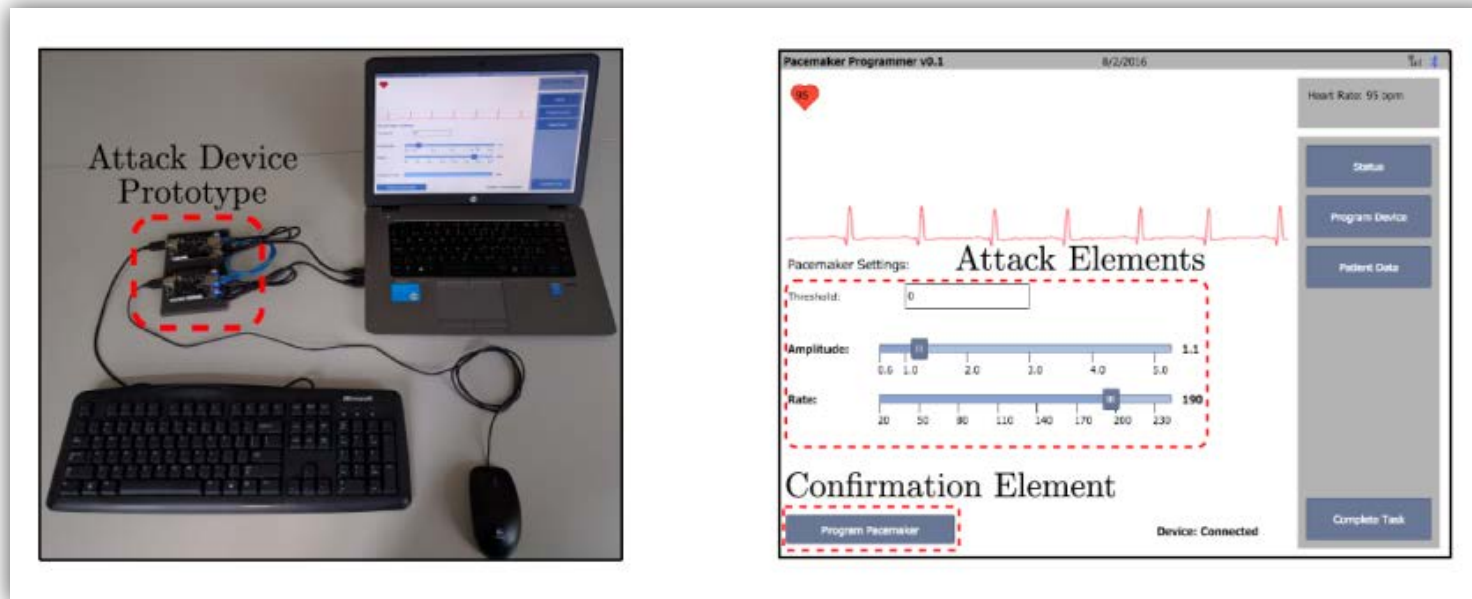


Robot-Assisted
Surgery Console



Touchscreen and Joystick
Operated Robot

- Recent ZISC research: compromise **input so that the operator doesn't notice before physical damage**



Privacy



CNN Regions | U.S. Politics | Money | Entertainment | Tech | Sport | Travel | Style | Health | Video | VR International Edition + 🔍 ☰

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!**

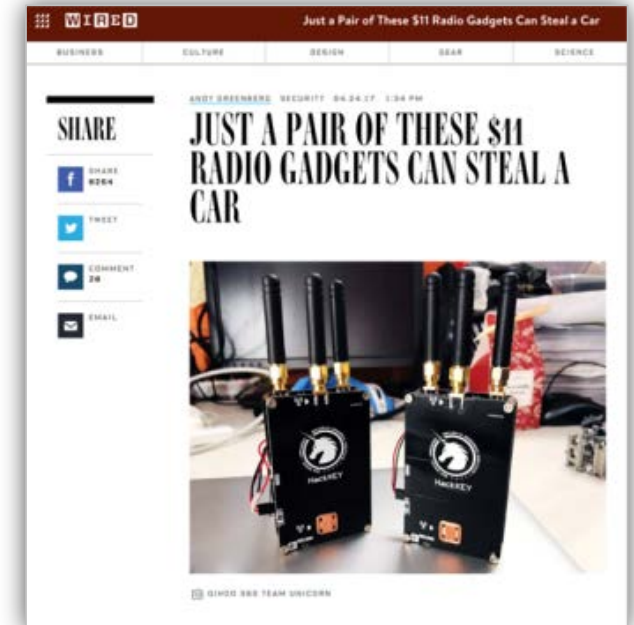


Example: Preventing Distance Spoofing

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

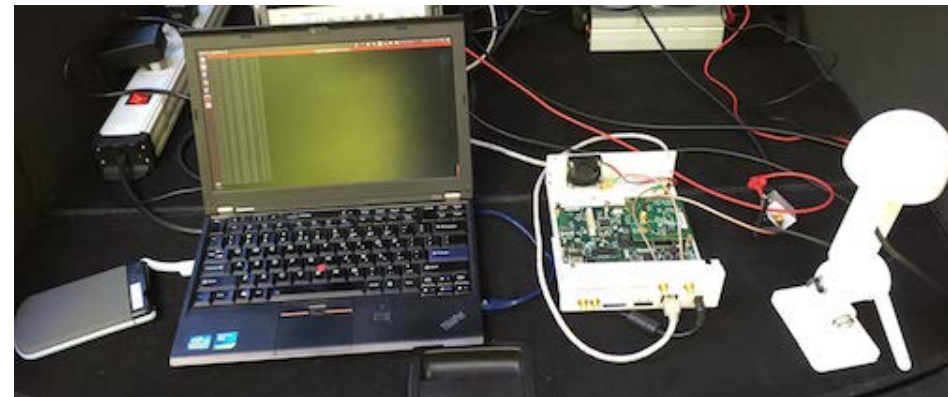


(3dB Access)



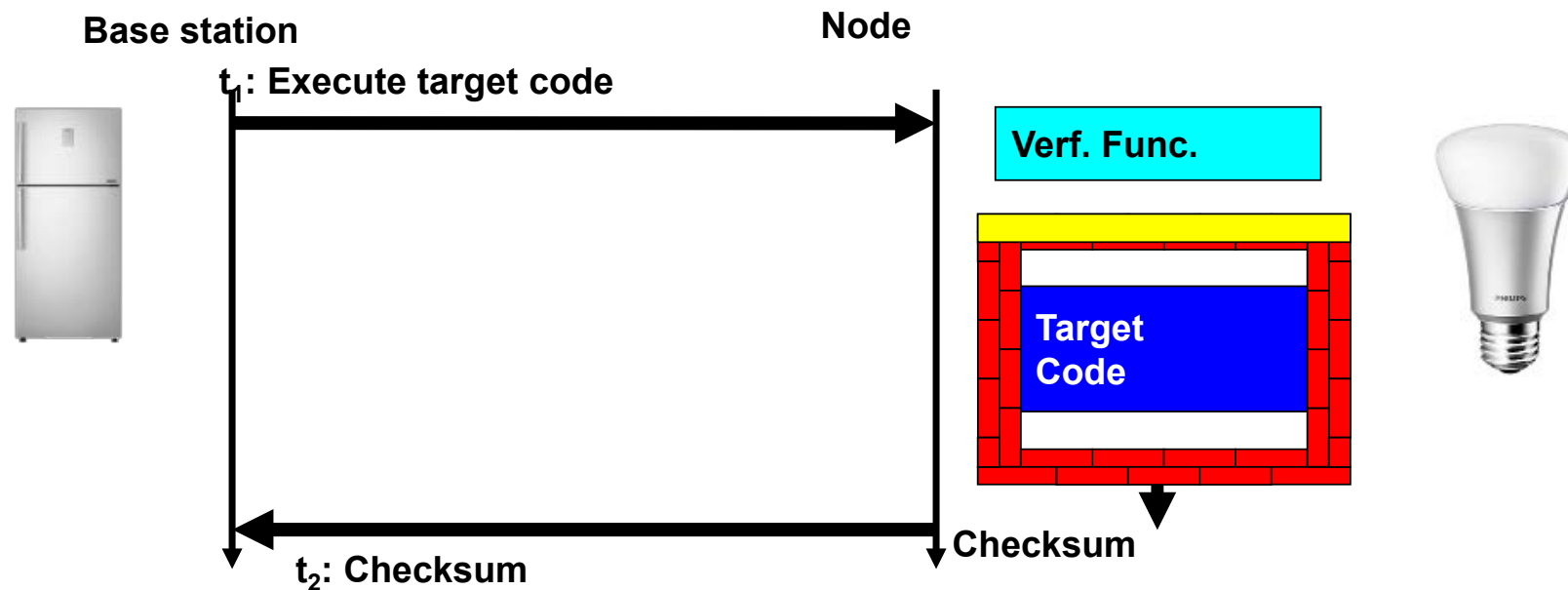
Example: Detecting GPS Spoofing

- Built First Open Source Spoofing-Resistant GPS Receiver
- <https://www.spree-gnss.ch/>



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**

username

srdjan@ethz.ch

password

password1234

Users use easy passwords and reuse the same passwords for various applications

3 billion passwords have been **stolen** in the last 9 years

code

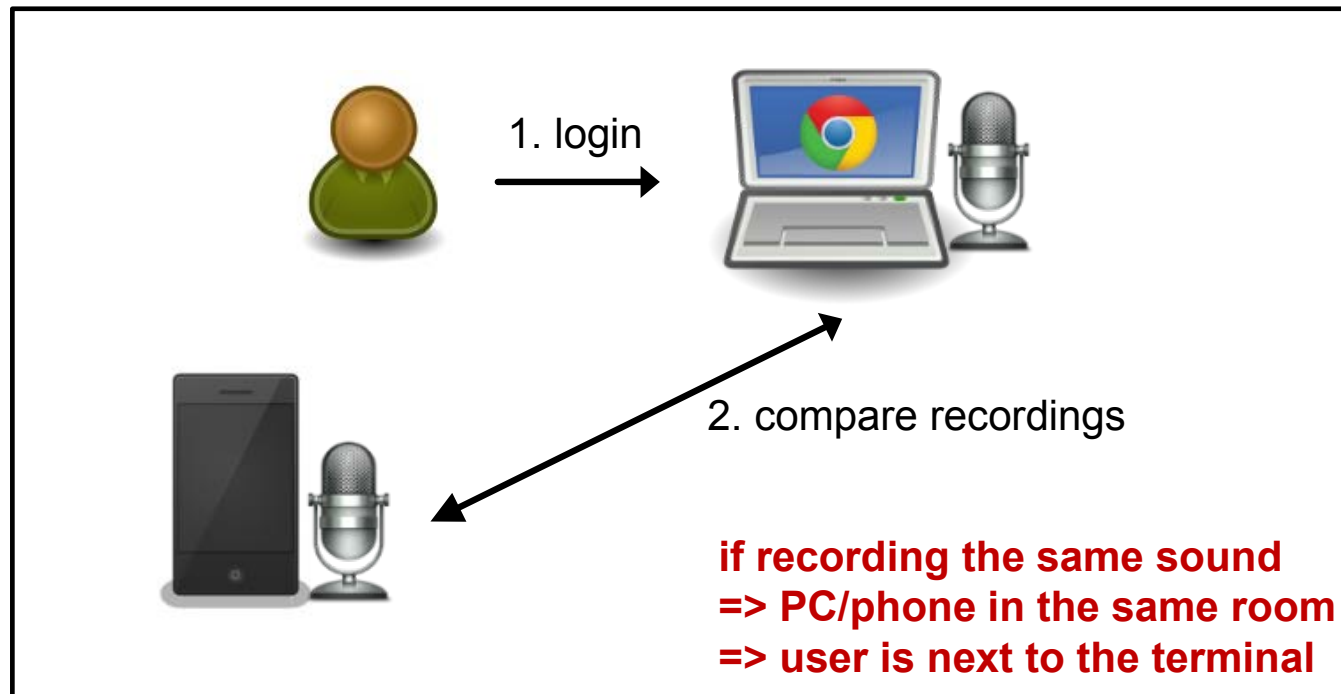
926 358



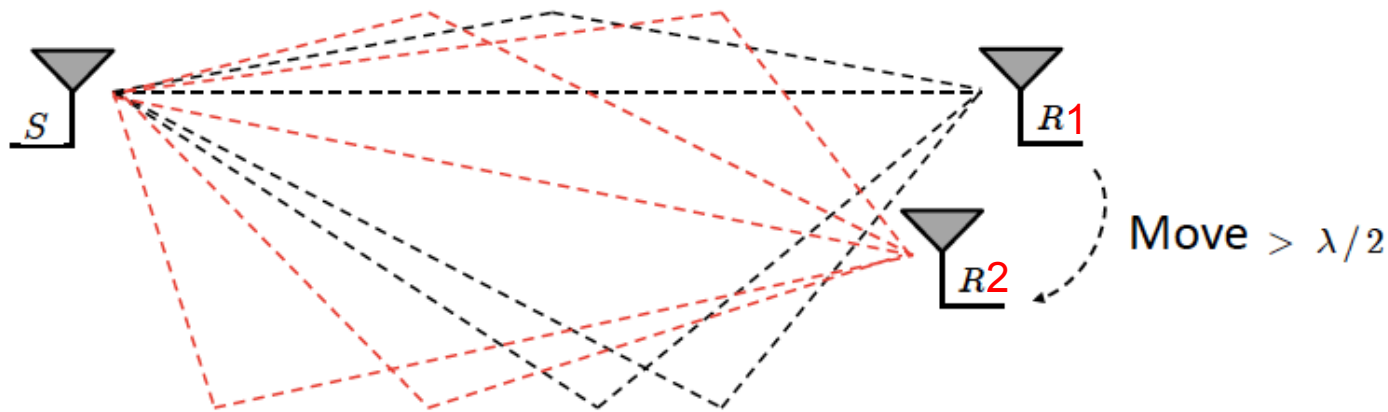
*That's why companies use **strong authentication**.*

Physical World Provides Opportunities: **Online Authentication**

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



Physical World Provides Opportunities: **Wireless Channel**



- In a complex, multipath-rich environment, **channels** exhibit ***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.