



 POLITECNICO DI MILANO



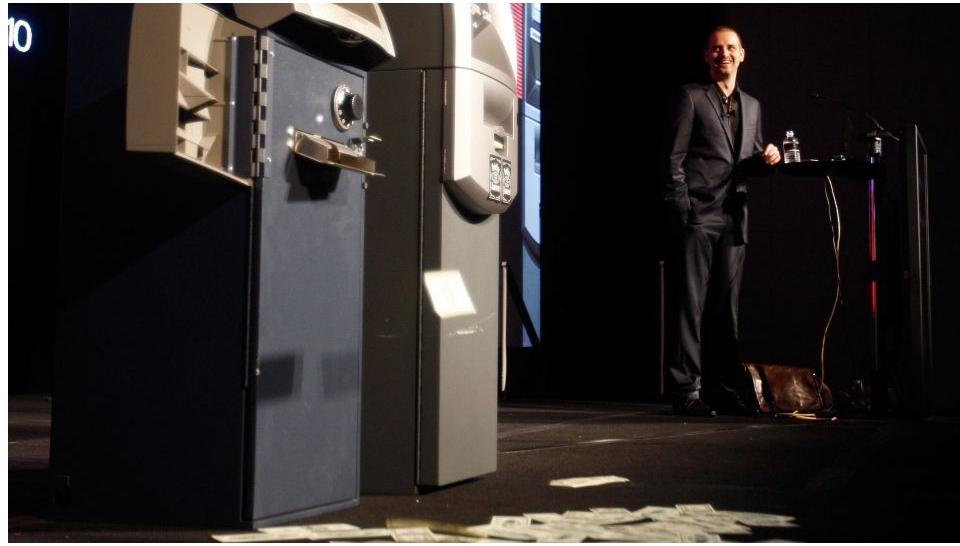
Securing Cyber-Physical Systems: moving beyond fear

Stefano Zanero, PhD
Associate Professor, Politecnico di Milano

Welcome to the security circus!

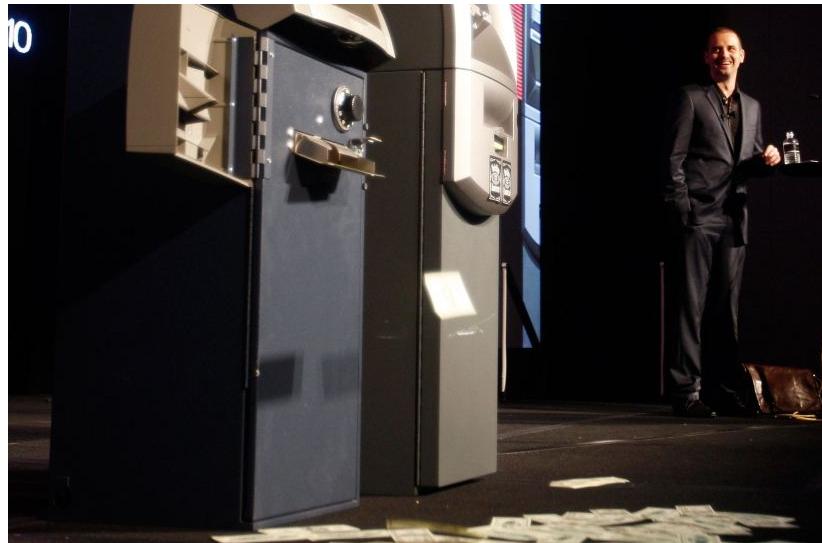


We all like to see the attractions



10

We all like to see the attractions



We all like to see the attractions

10





And who are the attractions, really?

- Our conferences reward **attack research**
- Because we are hackers at heart and we enjoy the **beauty** of many of these hacks, their skill and their ingenuity
- But you may have realized by now that we are not on IRC in our hacker crews anymore
- We are on the top frontpage news
- Our findings **impact the public perception**



This is what we showed in the circus

- Costin: “Ghosts in air traffic”
 - Discussed ADS-B security
 - https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_Slides.pdf
 - Peer-to-peer value > (perceived) vulnerability
 - Humans in the loop = low possibility of this leading to lack of safety
- Still, on the media...

Forbes

New Posts

+18 posts this hour

Most Popular

Fastest Cars Under \$50K

Lists

2000 Biggest Companies

LAST CHANCE: Get Forbes for \$8!



Andy Greenberg, Forbes Staff

Covering the worlds of data security, privacy and hacker culture.

[+ Follow](#) (779)

SECURITY | 7/25/2012 @ 1:54PM | 15.906 views

Next-Gen Air Traffic Control Vulnerable To Hackers Spoofing Planes Out Of Thin Air



4 comments, 3 called-out

[+ Comment Now](#) [+ Follow Comments](#)

A hacker attack that leads to planes dropping from the sky is the stuff of every cyberwar doomsday prophesy. But some security researchers imagine a less sensational, if equally troubling possibility: Hundreds or thousands of aircraft radioing their approach to an air traffic control tower, and no way to sort through which are real and which are ghost plane signals crafted by a malicious hacker.



- Hugo Teso: “Aircraft hacking”
 - Used ADS-B (just as a first step to “target a plane”)
 - Showed how to exploit a FMS unit bought on eBay (this was the actual core contribution)
 - Showed how this could affect a plane (on a simulator)
 - <http://conference.hitb.org/hitbseccconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf>
 - Response by FAA and expert pilots:
http://www.theregister.co.uk/2013/04/13/faa_debunks_android_hijack_claim/
- Still, on the media...

The screenshot shows the Computerworld website. At the top, there is a navigation bar with links for "Topics", "News", "In Depth", "Reviews", "Blogs", "Opinion", and "Search". Below the navigation bar is a large image of a woman with long brown hair, smiling, identified as Darlene Storm. Her name is displayed in large bold letters, and below it is the subtitle "Security Is Sexy". There are links to "Read Bio" and "See Posts". To the right of the bio are social media icons for "Subscribe" (RSS) and "Follow @SecurityIsSexy" (Twitter). The main headline of the news article is "Hacker uses an Android to remotely attack and hijack an airplane". Below the headline, it says "By Darlene Storm" and "April 10, 2013 4:28 PM EDT". It also indicates "230 Comments". Below the article are sharing options for LinkedIn, Twitter, Google+, StumbleUpon, Facebook, and Email, with counts of 276 shares and 7.8k likes.

The Hack in the Box (#HITB2013AMS) security conference in Amsterdam has a very interesting lineup of talks [pdf]. One that jumped out was the Aircraft Hacking: Practical Aero Series presented by Hugo Teso, a security consultant at n.runs in Germany. According to the abstract, "This presentation will be a practical demonstration on how to remotely attack and take full control of an aircraft, exposing some of the results of my three years research on the aviation security field. The attack performed will follow the classical methodology, divided in discovery, information gathering, exploitation and post-exploitation phases. The complete attack will be accomplished remotely, without needing physical access to the target aircraft at any time, and a testing laboratory will be used to attack virtual airplanes systems."

ALTRI ARTICOLI DI
Tecnologia



Cybercrimine finanziario e spionaggio: il 2012 è stato messo alla prova così



Twitter prova a blindarsi dopo gli attacchi, lavora a doppia chiave di autenticazione

Musica e film in streaming illegali, la polizia chiude 2 internet

Sei in: [Repubblica](#) > [Tecnologia](#) > L'hacker che voleva dirottare un aereo ...



6



16



133

L'hacker che voleva dirottare un aereo con lo smartphone e una piccola app

Hugo Teso ha stupito la platea in una conferenza svoltasi nei giorni scorsi ad Amsterdam: è riuscito a cambiare la traiettoria e la velocità di un aereo virtuale cliccando su una mappa sul suo smartphone Android o facendo oscillare il telefono. Ma gli esperti rassicurano: lo ha fatto su un simulatore, software che non ha certo le protezioni di un vero velivolo

di MATTEO CAMPOFIORITO

[Lo leggo dopo](#)

FMS 101

- Flight Management System typically consists of two units:
 - A computer unit
 - A control display unit
- Control Display Unit (CDU or MCDU) provides the primary human/machine interface for data entry and information display.
- FMS provides:

"UNO SMARTPHONE Android e il programma giusto. Tanto basta per dirottare un aereo". A parlare è l'hacker Hugo Teso che alla conferenza Hack In The Box, nei giorni scorsi ad Amsterdam, ha stupito la platea con una presentazione che descrive come sia possibile prendere il controllo di un velivolo sfruttando delle vulnerabilità nei sistemi di controllo degli aerei di linea. Ma dall'European Aviation Safety Agency, l'ente che si occupa della

And the list goes on and on...



42...
@Sidragon1

Find myself on a 737/800, lets see Box-IFE-ICE-SATCOM, ? Shall we start playing with EICAS messages? "PASS OXYGEN ON" Anyone ? :)

10:08 PM · Apr 15, 2015 · Twitter Web Client

192 Retweets 237 Likes

A Teller of Tales?

All of this appears to add up to the conclusion that there's no way Roberts could have hacked the thrust controls of a plane and manipulated the aircraft, either through the IEF, the SATCOM or anything else. But then how to explain the FBI affidavit?

KIM ZETTER SECURITY 05.15.15 10:14 PM

FEDS SAY THAT BANNED RESEARCHER COMMANDEERED A PLANE



See: <https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/>

And the list goes on and on...

ANDY GREENBERG SECURITY 08.07.19 03:29 PM

A BOEING CODE LEAK EXPOSES SECURITY FLAWS DEEP IN A 787'S GUTS



Santamarta claims that leaked code has led him to something unprecedented: security flaws in one of the 787 Dreamliner's components, deep in the plane's multi-tiered network. He suggests that for a hacker, exploiting those bugs could represent one step in a multistage attack that starts in the plane's in-flight entertainment system and extends to highly protected, safety-critical systems like flight controls and sensors.

Boeing flatly denies that such an attack is possible, and it rejects his claim of having discovered a potential path to pull it off. **Santamarta himself admits that he doesn't have a full enough picture of the aircraft—or access to a \$250 million jet—to confirm his claims.**



Why is this the case with cyber-physical systems in particular?

- They are systems that people **see** and can immediately perceive as **relevant**

The great cyberfear is spreading

“... potential (cyber)attacks against network infrastructures may have widespread and devastating consequences on our daily life: *no more electricity or water at home, rail and plane accidents, hospitals out of service*”

Viviane Reding
VP of European Commission (at time of delivering these remarks)

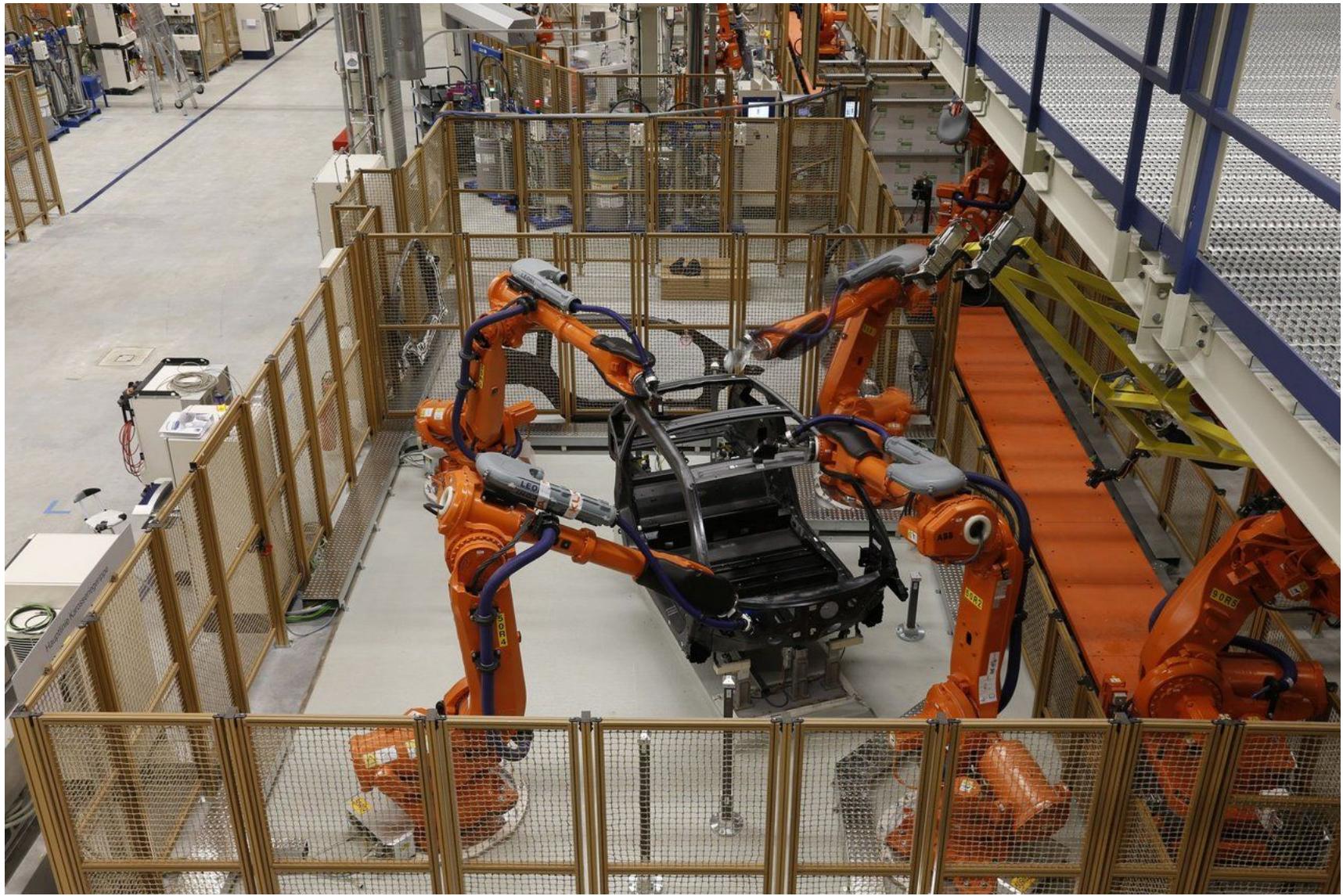




Why is this the case with cyber-physical systems in particular?

- They are systems that people **see** and can immediately perceive as **relevant**
- They are systems with **safety** constraints which may involve danger for **human life**

For instance, industrial robots...



... are getting out of their cages





Why is this the case with cyber-physical systems in particular?

- They are systems that people **see** and can immediately perceive as **relevant**
- They are systems with **safety** constraints which may involve danger for **human life**
- They are systems that are becoming more and more reliant on **automation**

Automation...



... has always evoked fear



BRIDGE
CHECKERS
CHESS
POKER
FIGHTER COMBAT
GUERRILLA ENGAGEMENT
DESERT WARFARE
AIR-TO-GROUND ACTIONS
THEATERWIDE TACTICAL WARFARE
THEATERWIDE BIOTOXIC AND CHEMICAL WARFARE
GLOBAL THERMONUCLEAR WAR





We can't just keep the circus going!

- “Stunt hacks” have been important in **raising awareness** and in opening up discussions in the industry
- However, they focus on specific **vulnerabilities**

“Are vulnerabilities in software dense or sparse? If they are sparse, then every vulnerability you find and fix meaningfully lowers the number of vulnerabilities that are extant. If they are dense, then **finding and fixing one more is essentially irrelevant to security and a waste of the resources spent finding it.**”

Dan Geer





We can't just keep the circus going!

- “Stunt hacks” have been important in **raising awareness** and in opening up discussions in the industry
- However, they focus on specific **vulnerabilities**
- **We are not going to solve anything by just squashing one vulnerability at a time!**



Words of wisdom

A flaw that Brad Spengler [...] has been incessantly pointing out for years [is] that **bugs don't matter**. Bugs are irrelevant. Yet our industry is fatally focused on what is essentially vulnerability masturbation. [...]

And it's all bullshit. If you care about security that is. [...]

"But to stop exploitation you have to understand it!". Sure. But here's an inconvenient truth. **You are not going to stop exploitation. Ever.**

So if you truly, deeply, honestly care about security. Step away from exploit development. All you're doing is ducking punches that you knew were coming. It is moot. It is not going to stop anyone from getting into anything, it's just closing off a singular route.

But if you care about systemic security [...] **don't chase and fix vulnerabilities, [...] design a system around fundamentally stopping routes of impact.**

Containment is the name of the game. Not prevention. The compromise is inevitable and the routes are legion. It is going to happen.

Bas Alberts



We can't just keep the circus going!

- “Stunt hacks” have been important in **raising awareness** and in opening up discussions in the industry
- However, they focus on specific **vulnerabilities**
- **We are not going to solve anything by just squashing one vulnerability at a time!**
- Often, vulnerability research lacks systemic context, leading to uncertain results

ANDY GREENBERG SECURITY 08.07.19 03:29 PM

A BOEING CODE LEAK EXPOSES SECURITY FLAWS DEEP IN A 787'S GUTS



Santamarta claims that leaked code has led him to something unprecedented: security flaws in one of the 787 Dreamliner's components, deep in the plane's multi-tiered network. He suggests that for a hacker, exploiting those bugs could represent one step in a multistage attack that starts in the plane's in-flight entertainment system and extends to highly protected, safety-critical systems like flight controls and sensors.

Boeing flatly denies that such an attack is possible, and it rejects his claim of having discovered a potential path to pull it off. **Santamarta himself admits that he doesn't have a full enough picture of the aircraft—or access to a \$250 million jet—to confirm his claims.**



How do we fix this?

- I'm sorry, I don't believe I have a **solution**, but I definitely have two **suggestions**
- First, we need to think systemically, and not of the specific vuln, let me bash my own research as an example



POLITECNICO
MILANO 1863

DIPARTIMENTO DI ELETTRONICA
INFORMAZIONE E BIOINGEGNERIA

Breaking the Laws of Robotics Attacking Industrial Robots

Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi,
Andrea M. Zanchettin, Stefano Zanero

 #BHUSA / @BLACKHATEVENTS

What the circus cheered for:



Update problems



FlexPendant

Axis Computer

Microcontrollers

How? FTP at boot

```
FTP      116 Request: SIZE /hd0a/ROBOTWARE_5.13.1037/TPS//SxTPU/2.0/TpsStart.exe
FTP      66 Response: 213 415744
FTP      116 Request: RETR /hd0a/ROBOTWARE_5.13.1037/TPS//SxTPU/2.0/TpsStart.exe
FTP      95 Response: 150 Opening BINARY mode data connection
```

.... plus, no code signing, nothing

#BHUSA / @BLACKHATEVENTS

What the circus cheered for:



Update problems



FlexPendant

How? FTP at boot

FTP	116 Request
FTP	66 Response
FTP	116 Request
FTP	95 Response

.... plus, no code signing, r

```
FTP      117 Response: 220 ABB Robotics FTP server (VxWorks5.5.1) ready.  
FTP      84 Request: USER _SerB0xFtp_  
FTP      89 Response: 331 Password required  
FTP      81 Request: PASS [REDACTED]  
FTP      86 Response: 230 User logged in  
FTP      72 Request: PASV  
FTP      114 Response: 227 Entering Passive Mode (192,168,125,1,4,25)  
FTP      93 Request: RETR /command/startupInfo  
FTP      107 Response: 150 Opening BINARY mode data connection  
FTP      89 Response: 226 Transfer complete  
FTP      72 Request: QUIT  
FTP      91 Response: 221 Bye...see you later
```



ABBVU-DMRO-124642

#BHUSA / @BLACKHATEVENTS

What the circus cheered for:



Update problems



FlexPendant

Autoconfiguration is magic!



Enter / command

Let's look at **cmddev_execute_command**:

```
shell → sprintf(buf, "%s", param)  
other commands → sprintf(buf, "cmddev_%s",  
arg)
```

overflow **buf** (on the stack) → **remote code execution**

.1) ready.
L,4,25)



#BHUSA / @BLACKHATEVENTS

ABBVU-DMRO-128238

#BHUSA / @BLACKHATEVENTS

What the press impact was:

Catastrophe Warning: Watch An Industrial Robot Get Hacked



EDITOR'S PICK

Thomas Fox-Brewster Forbes Staff

May 3, 2017, 08:00am • 3,154 views • #CyberSecurity



ABB has fixed vulnerabilities in its robots that allowed hackers to remotely change its configuration, opening the door for catastrophic results, researchers warned Wednesday. (Photo credit: SAM YEH/AFP/Getty Images)

What the press impact was:

Catastrophe Warning: Watch An Industrial Robot Get Hacked



EDITOR'S PICK

Thomas Fox-Brewster Forbes Staff

May 3, 2017, 08:00am • 3,154 views • #CyberSecurity



ABB has fixed vulnerabilities in its robots that allowed hackers to remotely change its configuration, opening the door for catastrophic results, researchers warned Wednesday. (Photo credit: SAM YEH/AFP/Getty Images)

ANDY GREENBERG SECURITY 05.03.17 08:00 AM

WATCH HACKERS SABOTAGE AN INDUSTRIAL ROBOT ARM



What the press impact was:

Catastrophe Warning: Watch An Industrial Robot Get Hacked



EDITOR'S PICK

Thomas Fox-Brewster Forbes Staff

May 3, 2017, 08:00am • 3,154 views • #CyberSecurity



ABB has fixed vulnerability
catastrophic results, rese

MOTHERBOARD

INTERNET INSECURITY | By Lorenzo Franceschi-Bicchieri | May 3 2017, 2:01pm

Hackers Are Remotely Controlling Industrial Robots Now

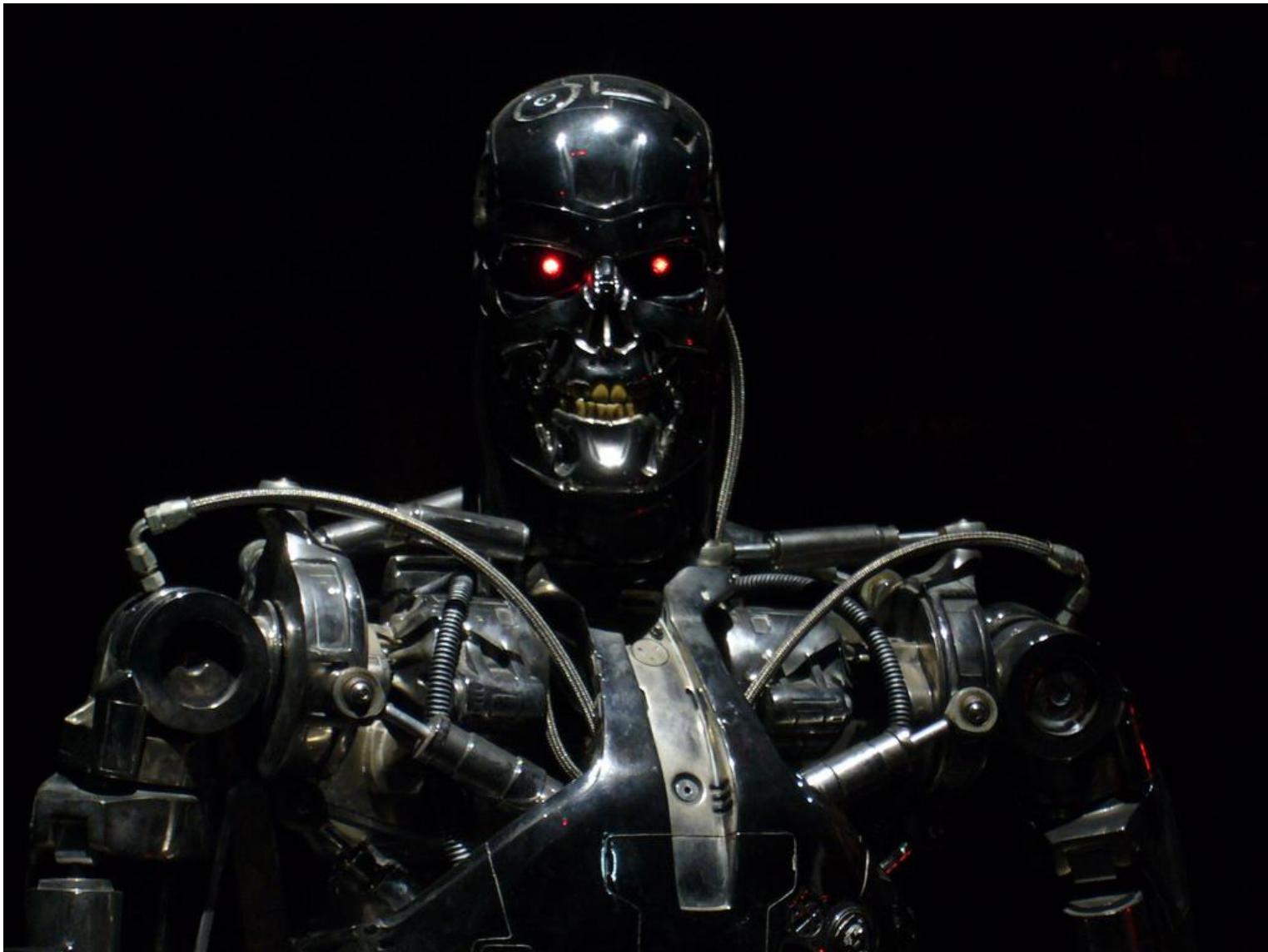
Security researchers have found multiple vulnerabilities into a specific model of robot arm used in factories.

ANDY GREENBERG SECURITY 05.03.17 08:00 AM

WATCH HACKERS SABOTAGE AN INDUSTRIAL ROBOT ARM



What the public perception was:





What was actually important in the paper:

- We explored the domain-specific **post-exploitation strategies** (which leads to intuitive ways to close them off)
- We explored the **threat landscape** to identify ways to minimize **impact**
- We explored **architectural changes** that would improve **resilience** (e.g. firmware signatures)
- We proposed **research directions** to further improve security of industrial robots (e.g. static analysis of domain specific languages)
- We identified **industrial routers** as an appealing target for further investigation



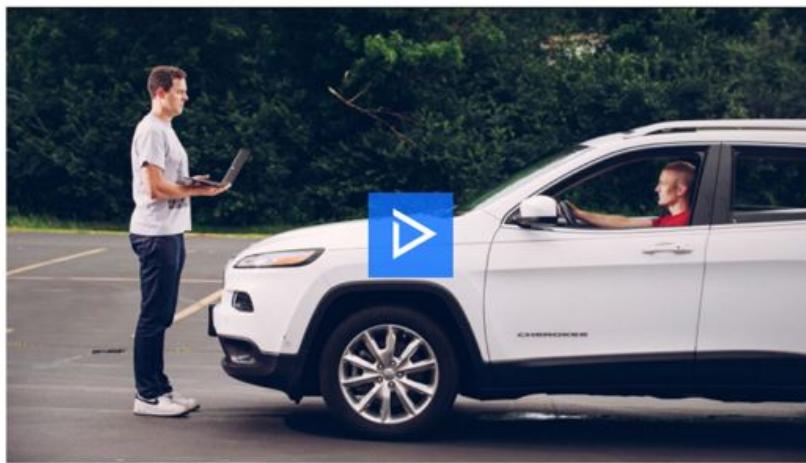
How do we fix this? (2)

- I definitely have two **suggestions**
- First, we need to think systemically, and not of the specific vulnerability, but rather of its **impact**, of **resilience strategies**, of **architectural changes**...
- Second, we need to embed security in the **design process**, and to make security decisions **risk-driven**. Let me use the automotive industry as an example.

Multiple attacks and hacks (local and remote)

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY –WITH ME IN IT



I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Hackers can easily drain the battery on the world's most popular electric car



Paul Szoldra

© Feb. 24, 2016, 3:42 PM

4,836



FACEBOOK



LINKEDIN



TWITTER



The [popular Nissan Leaf](#) electric car can be drained of its battery life using little more than its vehicle identification number (VIN).

The major security hole was [found by researcher Troy Hunt](#), who figured out that the Leaf's smartphone app interface (API) uses [only the VIN to control car features](#) remotely without passwords. These features include seeing the car's current battery life, times and distances the car has traveled, and

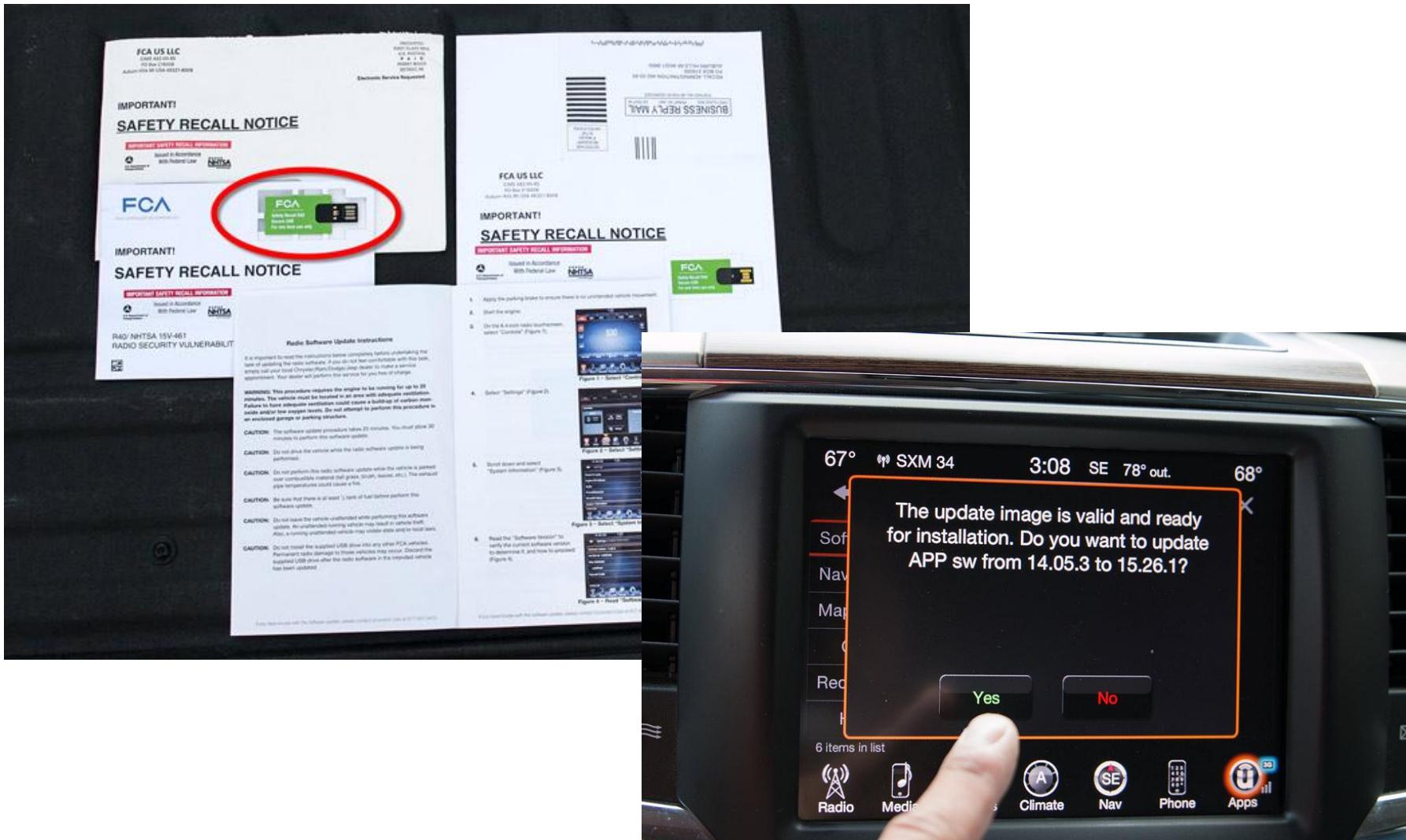




But in reality they are all the same attack

1. Attacker finds exploit in physical or wireless systems
 - Most of these systems not designed to be secure gateways
 - Changed assumptions, e.g. “if inside the vehicle, authorized”
2. Exploit is used to gain access to the in-vehicle network
 - Which was not designed to host non-trusted entities, so
3. Message forgery or diagnostics actions can be leveraged
 - Vehicle theft
 - Temporary influence on vehicle operation
 - Permanent modification of vehicle
 - Extraction of personal information, tracking, etc.

The defense circus is sometimes better than the offense circus!





What is the systemic way out?

- The issue is that CAN is a trusted network
- Lots of research tries to address this, but reality is, changing this is **impractical**
- Lots of research tries to come up with magic IDSs, but we and others showed you can design attacks that simply **cannot be detected**
- Obviously, squashing bugs in **thousands** of combinations of ECUs and firmwares is pointless
- We can only approach this through **secure design** of networks based on **risk approaches**

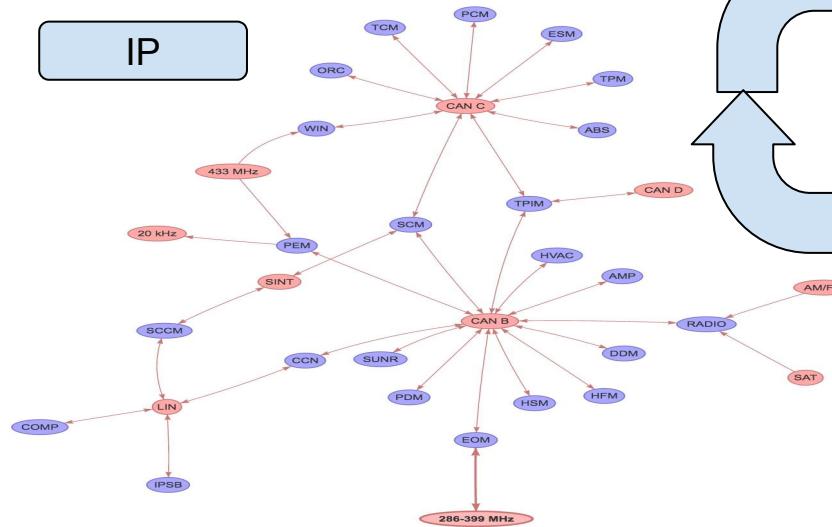
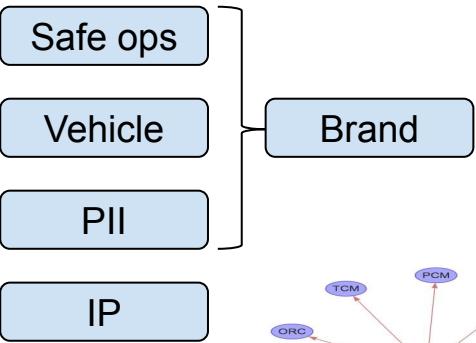


What is the systemic way out?

- The issue is that CAN is a trusted network
- Lots of research tries to address this, but reality is, changing this is **impractical**
- Lots of research tries to come up with magic IDSs, but we and others showed you can design attacks that simply **cannot be detected**
- Obviously, squashing bugs in **thousands** of combinations of ECUs and firmwares is pointless
- We can only approach this through **secure design** of networks based on **risk approaches**

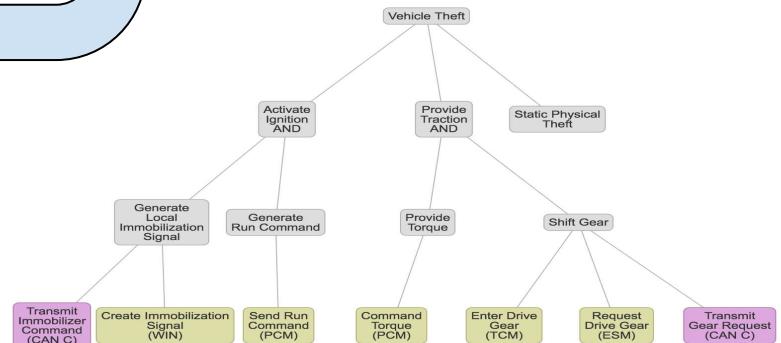
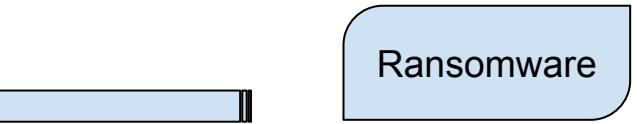
An approach: risk-based design of networks (for automotive and more)

Asset definition and value analysis



Vehicle network topology mapping

Threat assessment and evaluation



Attack tree definition and analysis

- We focus way too much on attack research, vulnerability discovery and exploitation
- Vulnerabilities, in the grand scheme of things, do not really matter
- Stunt hacking distracts the industry and the public from actual sensible risk-based security
- We need more focus on:
 - Structural resilience
 - Architectural changes
 - Impact reduction

Questions?

- Thank you for your attention!
- You can reach me at stefano.zanero@polimi.it
- Or just tweet @raistolo

Disclaimer: none of these materials, if posted without a video of the talk, should be construed to be a criticism of the specific research I used as examples.

