Cyber-physical systems

- A system controlled or monitored by computers, tightly integrated with the Internet and its users
- SCADA (Supervisory Control And Data Acquisition) systems
  - Process control systems, $10^3$ – $10^5$ control variables
  - Old design – becoming networked
  - Decisions moved to decentralized nodes
- Energy distribution
  - Smart Grids (production, distribution, meters and appliances)
  - Faces more cyberattacks than any other industry [US Homeland Security]
  - 72% believed they could detect unauthorized software in their network... [Tripwire.com Sept 2017]
- Autonomous cars
Trend: Processing moves to endpoints

IoT reached 15 billion devices Jan 2016

What systems can we trust?
52 Flash Player bugs fixed with Adobe's July Patch Tuesday update

Adobe’s July Patch Tuesday release is once again dominated by vulnerabilities found within the company’s Flash Player product where 52 critical CVEs that could allow an attacker to take control of a system.

The risk that my computer is affected is very low, i.e. patching once a month is ok.

But how about my self-driving car? With a flash player... and third party apps... and 50 million more lines of code 😊

Angry birds on an ATM machine

Security researchers have hacked an automatic teller machine to install a working version of Angry Birds.

The attack also pulled customer Primary Account Numbers (PANs) and expiry dates.

He extracts cash, then long-presses the screen triggering a Windows context menu. From there Internet Explorer appears and he executes via the browser the on-screen keyboard and then opens the command function.

In a post (translated from Russian to English) head of technologies Dmitry Evseev said the company would not yet release more details on the attack “without coordination with system manufacturers” citing principles of responsible disclosure.

European aviation body warns of cyber-attack risk against aircraft

The chief of Europe's top airline safety agencies warned that cyber-criminals could hack into critical systems on an airplane from the ground.

Patrick Ky, director of the European Aviation Safety Agency, told European aviation journalists at a meeting of the Association des Journalistes Professionnels de l'Aviation et de l'Espace (AJPAE) that his organisation had hired a penetration tester to find and exploit vulnerabilities in the ACARS (AirCraft Communications Addressing and Reporting System) used to transmit messages between aircraft and ground stations.

Over the past two years, there has been an increasing number of cyber-security incidents reported in the aviation industry.

Technical problems...

• **Protocols** are insecure
  - IP, TCP, UDP, DNS, ARP, DHCP, etc. were never designed for security
  - Most other protocols rely on their security...

• **Operating systems** are insecure
  - New problems are constantly discovered
  - Incorrect configuration

• **Applications** are insecure
  - Application programmers are not aware of protocols and security issues
    “Look! It works! I can talk to the server!!!”
  - Vendors don want to remove functionality just to enhance security
  - Customers don’t want to pay for better security

• And now we connect millions of such systems...
Can vulnerabilities be removed?

- Critical programs are rigorously tested
  - One bug per 1000 lines of code is extremely good
  - Cost: around $1000 per line of code [old estimate]

- Windows has >50 million lines of code
  - $50,000,000,000 \( \rightarrow \) 50,000 bugs left
  - Too complex to test this well

- Linux has 22 million lines of code
  - Grows with 5,000 lines per day \( \rightarrow \) 5 more bugs per day...

- Design for security testing:
  - Modules small enough to be verified
  - How deal with cooperating, complex clusters of systems?

How well can we test software?

NASA Study on Flight Software Complexity
"Commissioned by the NASA Office of Chief Engineer, Technical Excellence Program, May 2009"
Vehicles begin to communicate and are soon autonomous...

Cooperative Safety Systems

Cooperative Vehicle Safety System or Cooperative Active Safety System
Every vehicle broadcasts its ORS info to its neighbors

Virtual traffic lights
Modern vehicles...

- Contain **50-150 ECUs** (computers)
  - Internal networks: CAN, LIN, Most, FlexRay
  - 2 km cables
  - 40 Antennas
- Communication enhances traffic safety
  - New advanced functionality: ABS, ESP, platooning, awareness, ...
  - v2v and v2i connectivity
- Depend heavily on **software**
  - 10 - 100 million lines of code
  - Mercedes S-Class: **144 ECUs, 65M lines of code**
  - 2 errors per 1,000 lines of code: >100,000 remaining bugs
Hackers crack Tesla CAN Bus, DoT issues policy for securing connected car

For the first time ever, researchers claimed they were able to crack into Tesla’s CAN Bus to achieve remote control of the electric car, meanwhile the U.S. Department of Transportation (DoT) issued new policy concerning automated vehicles.

“The attack involved exploitation of a web browser leading to physical control over the car”

“Ideally these systems should be completely isolated from one another.”

Researchers said they were able to perform the exploits on various models all of which were performed without physically altering the cars.

Sources


Researchers use exploit to disable Audi airbags

Researcher Hacks Self-driving Car Sensors

By Mark Harris
Posted 4 Sep 2015 | 19:00 GMT

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

Hacker Disables More Than 100 Cars Remotely

BY KELLY FALLON | 01/31/16 | 6:12 PM | PERMALINK

Zero-day in Fiat Chrysler feature allows remote control of vehicles

PCWorld
Jan 30, 2015

These are the cars most vulnerable to hacking. Is your car one of these? Sept 2015
What is required?

- Special tools?
- Extreme skill?
- Lots of resources?
- Plenty of time?
- How hard is it to find a security problem?

Typical architecture – Attack surfaces
The Jeep Cherokee Hack 2015

• Researchers has long complained about (lack of) security
• Two researchers, Miller & Valasek, picked one vehicle
• Complete control over the Internet
  ‒ Infotainment system from 3rd party vulnerable
• 1.4 Million cars recalled
• No special skills needed – just the will to investigate

Problems found

• WLAN password is $f(\text{time\_of\_first\_boot})$
  ‒ If month known: 2 minutes to guess
  ‒ But time is not known at first boot, it’s always Jan 1, 2013 00:00:32 GMT

• Nine internal TCP ports open to WLAN
  ‒ Port 6667 used for RPC and inter-process communication
  ‒ Four lines of code enough to send commands from any computer 😎

• Vehicle uses proxy to filter 3G/4G communication
• Telecom operator allowed direct communication
  ‒ Same TCP ports open to the Internet
• Many more ways to attack vehicle found
Summary: Threat or possibility?

• The new technology has lots of potential 😊
  – Energy awareness, green computing, intelligent safer vehicles, ...

• Things not designed for security will never be secure
  – So far, just about every consumer device that’s been desired to be hacked into, has 😎

• Systems will become even more connected, more complex and autonomous...

• And we become more dependent:
  Banks, power systems, water supplies, hospitals, SCADA systems, vehicles, telecommunications, e-commerce, e-cash/Bitcoin, apps, ...

• TVRA?
  Risk = probability of accident * expected loss
  Is this a reasonable approach???