St. Pölten University of Applied Sciences
Department Information Security

IT-SECX
IT-Security Community Xchange
2013

Six Ways to Kill by Hacking

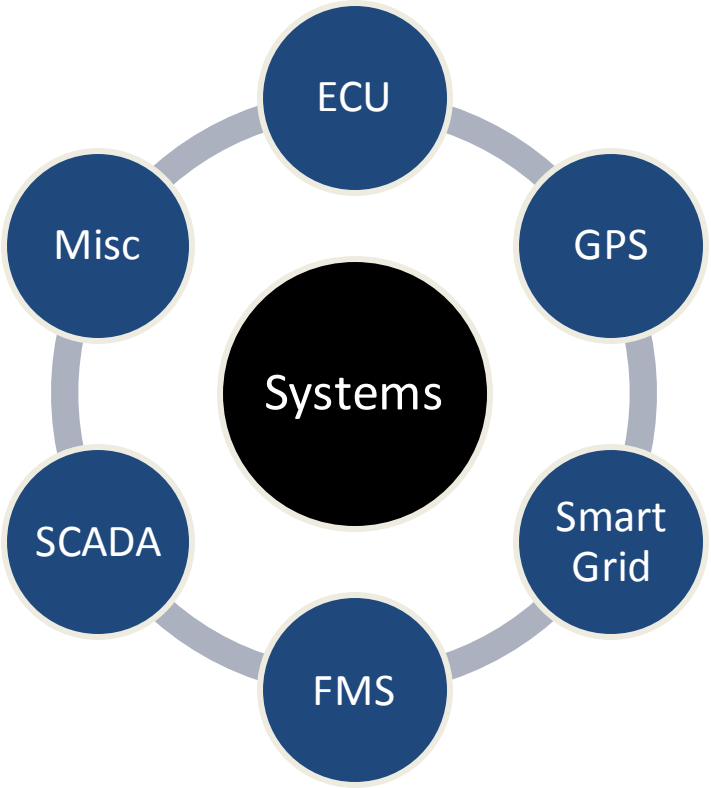
Critical Systems · Infrastructure

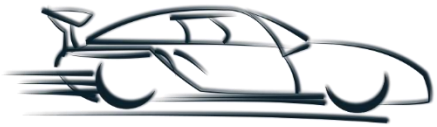
A murderous journey through Systems Security

Robert Luh
Institute of IT Security Research, St. Pölten University of Applied Sciences

Introduction

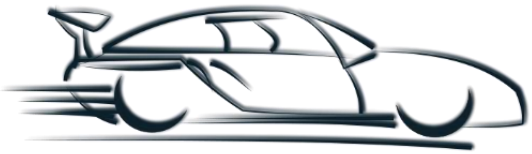
- Topic: Systems and Critical Infrastructure
  - Overview: Functionality, Security, Threats
- Potential for causing physical harm

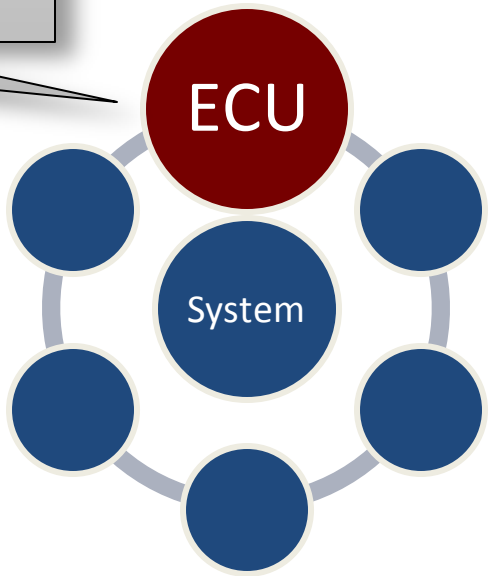




Case #1

- Car Computers
  - Electronic Control Unit (ECU)
  - 50-70 ECUs in a modern car
  - Responsible for almost all car functions
  - Communication via internal bus
  - Physical access via OBD-II
  - Wireless access via TPMS sensors, 3G, 802.11p,…)





ECU: Controller Area Network (CAN)

High-Speed Network

- Motor control (EMC)
- Brake control (EBCM)
- Transmission (TCM)

Low-Speed Network

- Heating and AC (HVAC)
- Door control (RCDLR)
- Airbag and seat belts (SDM)
- Dashboard (IPC)
- Radio
- Theft protection

Networks are connectioned via:
Diagnostics system (BCM), Telematics

ECU: Security

Flaws:

- Direct bus access
  - Manipulated (USB) device
  - On-Board Diagnostics Port (OBD-II) + Laptop
  - Wireless (via sensors, Telematics, GSM/UMTS,…)
- CAN Packets
  - Broadcast to all CAN nodes (ECUs)
  - Susceptible to DoS (disabled all ECU functions)
  - No authentication
  - Lacking access control
    - Diagnostics mode can be triggered
    - Weak key material (16 bit)

ECU Attacks (exemplary attack sequence)

Attack Status: CONFIRMED

Increase of motor RPM

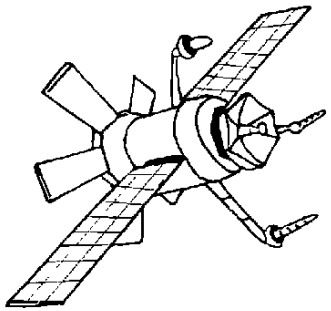
Locking doors

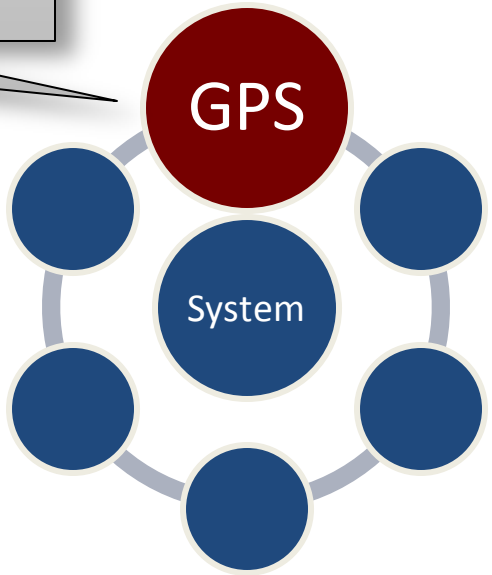
Falsification of dashboard

Disabling brakes

Case #2

- GPS
  - Global Positioning System (GPS)
  - Navigation und time provider
  - Operates with triangulation (measures distance to 4+ satellites using signal transit time)
  - Internal atomic clock provides accurate time





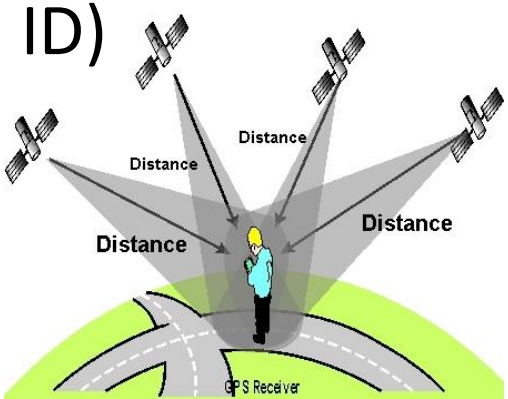
GPS: Use und Functionality

Applications (e.g.):

- Civilian and military navigation
- Frequency regulation in electricity and communication grids
- Time provider (also for Internet/NTP servers)
- Tracking systems
- Freight handling

Data transmission

- C/A Code (time, week, nav data, satellite ID)
- Signal strength approx. -160dBW (weak)



GPS: Security

Weaknesses/Threats:

- Signal encryption
  - Not implemented (civilian GPS)
- Jamming
  - Overriding the signal with a stronger one
- Spoofing
  - Falsification and retransmission of the signal
  - Pretends to be genuine (manipulated C/A code)
  - Denial of Service attack on receivers possible
- Receivers
  - Often conventional computers with lacking sec.
  - Missing integrity and plausability check

GPS Attacks

Attack Status: CONFIRMED/EXPERIMENTAL

Route manipulation

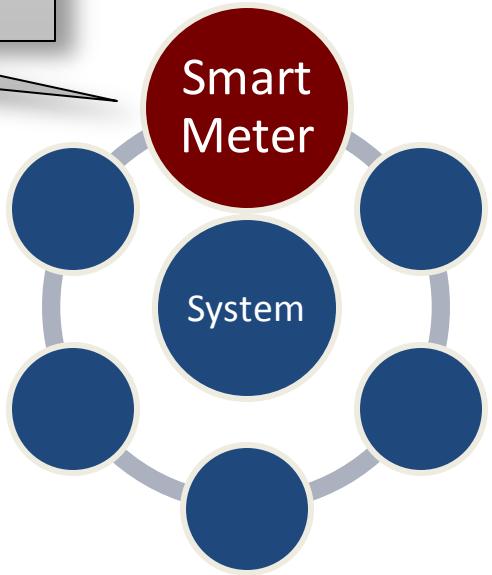
Disrupting traffic lights

Middle-of-Earth attack

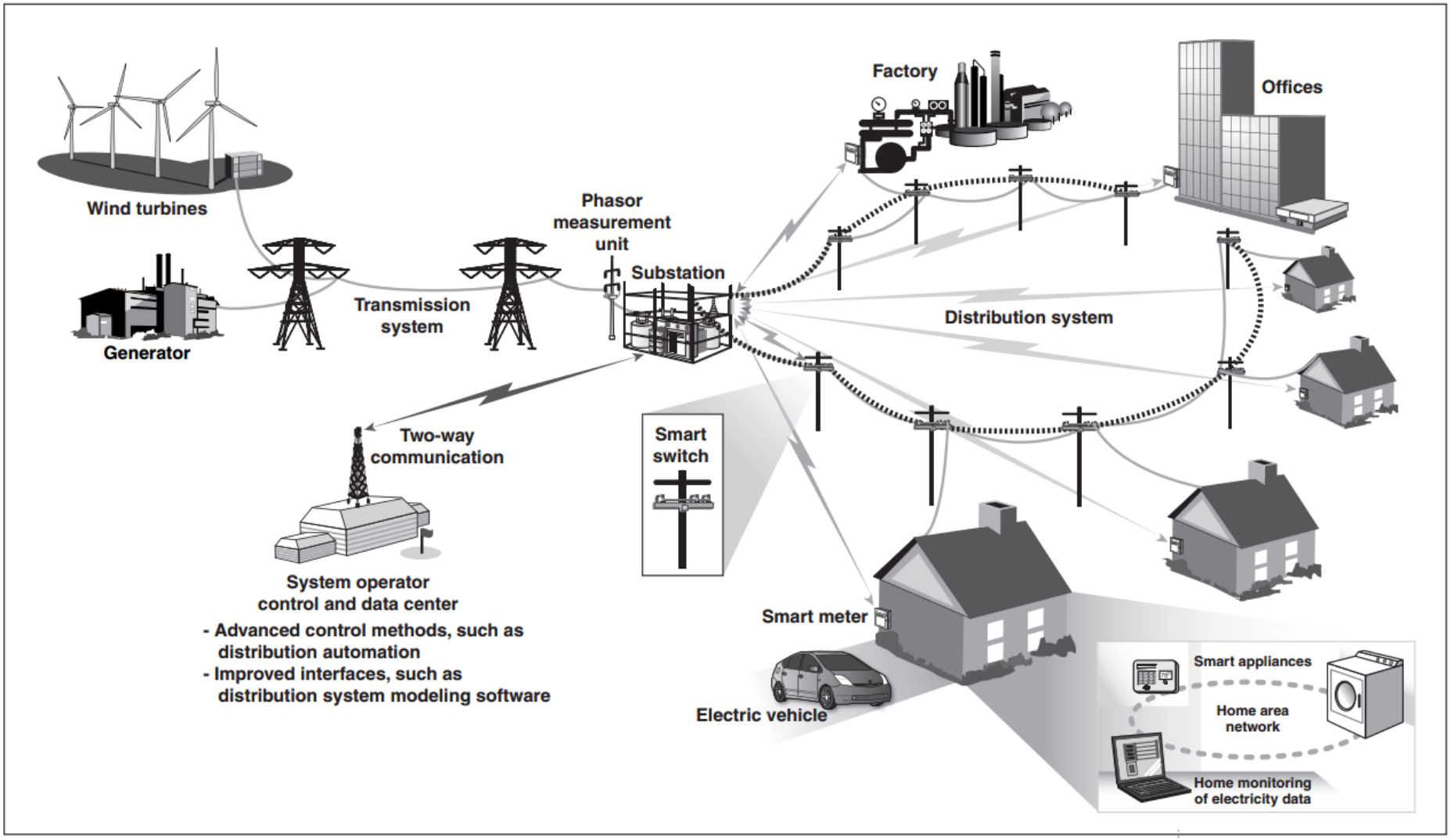
De-Sync of power grid

Case #3

- Smart Meter
  - Commodity metering and control device
  - Usually for metering of power, gas
  - Connects to the smart grid
  - Communicates with HAN/LAN, WAN
  - Wired (PLC) or wireless (RF mesh)
  - EU: Implementation until 2020



Smart Grid



Quelle: United States Government Accountability Office

Smart Grid: Security

Weaknesses/Threats:

- Weaknesses
  - Device IDs are not secret (printed on the face)
  - Password reuse
- Attack vectors
  - Memory: e.g.: Extracting admin passwords
  - RF signal: Interception, disruption, malware spread.
  - WAN: MITM attacks and more…
- Scenarios
  - Remote reading of consumption data
  - Service interruption
  - Energy theft

Smart Meter Attacks

Attack Status: EXPERIMENTAL

Activation of intelligent device

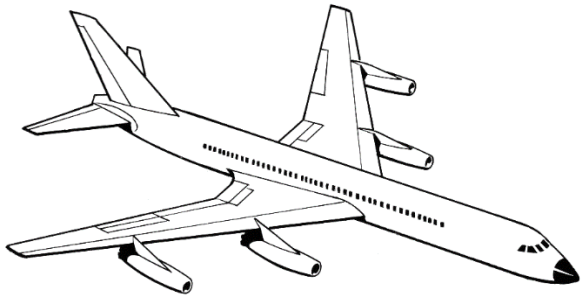
Regional power outage

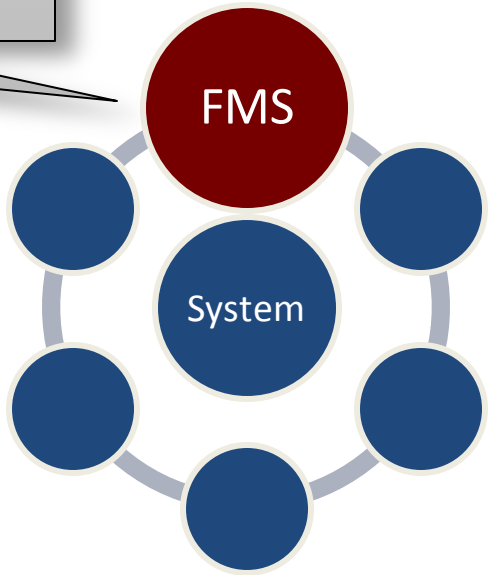
Chain reaction (see U.S., 2003)

Chaos

Case #4

- ADS-B/ACARS
  - Automatic Dependent Surveillance Broadcast (ADS-B)
    - Airplane tracking via radio
  - Aircraft Communications Addressing and Reporting (ACARS)
    - Ground <> Airplane communication
  - Flight Management System (FMS)





Airplane Communication: Functionality

ADS-B (Tracking)

- Radio transmission to and from the airplane
- U.S. commercial planes: Implementation until 2020

ACARS (Data exchange)

- Radio or satellite connection
- Arrival and departure information
- Weather data
- Engine information

FMS (On-board computer)

- Navigation database, flight plan
- Autopilot

Airplane Communication: Security

Weaknesses/Threats:

- ADS-B
  - No encryption
  - No authentication
- ACARS
  - Easy to eavesdrop; enables reverse engineering
- FMS
  - Computer system with weaknesses (like any other computer/OS)

FMS Attacks

Attack Status: EXPERIMENTAL/THEORETICAL

Setting a new waypoint

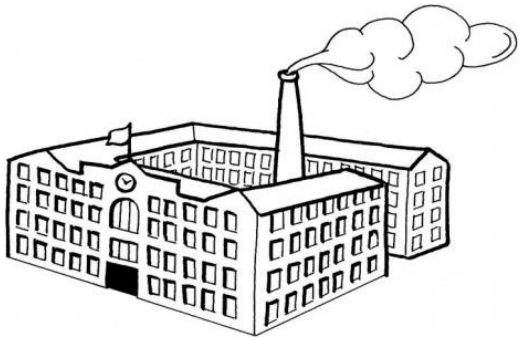
Changing positional data

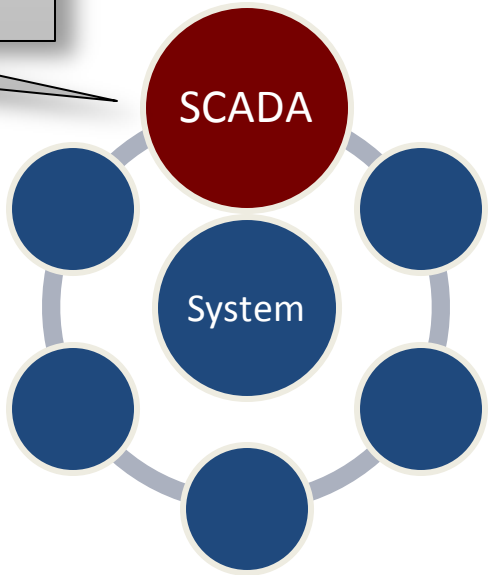
Disrupting internal systems

Forcing plane to “land”

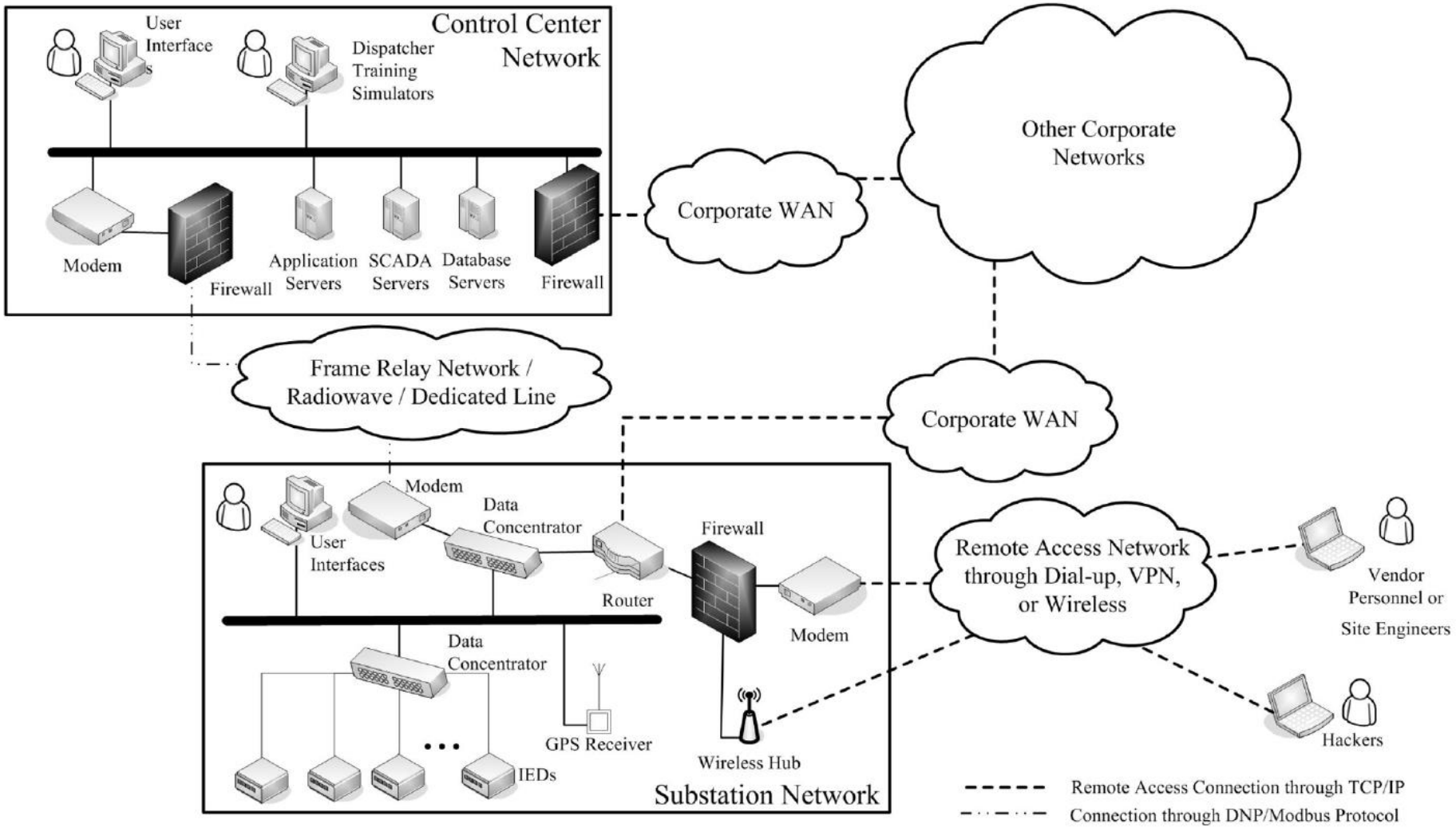
Case #5

- Industrial Control Systems
  - Supervisory control and data acquisition (SCADA) systems
  - Manufacturing, process control, automation, supply, transportation,…
  - Separate network
  - Remote access for service technicians
  - Logic is coded on Windows machines





SCADA System



SCADA: Security

Weaknesses/Threats:

- Security in industrial computers not a priority until recently
- Outdated technologies; low performance and small memory (although real-time capable)
- Attack vector: programming machine (conventional PC)
- Web server on-chip (e.g. current SIMATIC generation)
- Maintenance “backdoor”
- Internet connectivity; switch to IP-based systems
  - Links: Dial-up, VPN, wireless, satellite,…

Tatmittel SCADA

Attack Status: CONFIRMED/EXPERIMENTAL

Building:
Disable heating

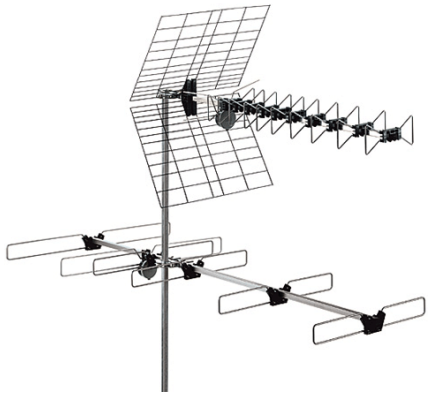
Sewers
overflow

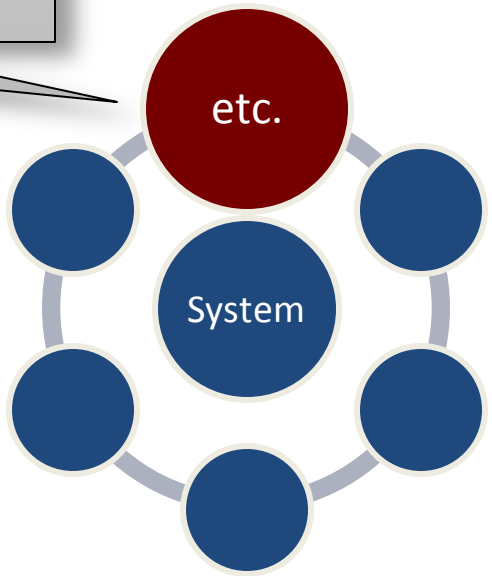
Pipeline burst

Hollywood
Scenario X

Case #6+

- Deadly jolt via pacemaker (remote hack, 10m range)
- Manipulation of medical devices (increasingly connected to the LAN)
- Many more radio hacks: Spoofing/Jamming using a 1500$ software radio and open source SW
- …





Conclusion

„Why make it simple, when you can use a computer?“

- Hi-Tech murder requires a lot of know-how
- Security flaws are often ancient…
- …or brand-new and barely researched

- Cybercrime is on the rise
- Internet penetration is increasing (IoT, etc.)
- Infrastructure attacks threaten national stability; constantly increase

Computer are more than just PCs and laptops!
Exotic systems will not always be exotic!
Security needs to keep pace!

It has begun…

Attack Status: PENDING

References

ECU

K. Koscher et al., “Experimental Security Analysis of a Modern Automobile”, IEEE Symposium on Security and Privacy, 2010.

D.K. Nilsson and U.E. Larson, “A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure”, Journal of Networks, Vol. 4, No.7, 2009.

C. Miller and C. Valasek, “Adventures in Automotive Networks and Control Units”, 2013.

I. Rouf et al., “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study”, University of South Carolina, 2010.

University of Innsbruck, “Vehicular Networks (C2X)”, Computer and Communications Systems, Lehrstuhl für Technische Informatik, University of Innsbruck, 2012.

R. Havelt and B. Oliviera, “Hacking the Fast Lane: Security Issues with 802.11p, DSRC, and WAVE”, Trustwave Spider Labs, 2011.

A. Bellissimo et al., “Secure Software Updates: Disappointments and New Challenges”, 1st USENIX Workshop on Hot Topics in Security, HotSec, 2006.

Security Week/AFP, “Car-hacking Researchers Hope to Wake up Auto Industry”, Security Week, https://www.securityweek.com/car-hacking-researchers-hope-wake-auto-industry (accessed 2013/07/30), 2013.

GPS

J.A. Volpe, “Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System”, National Transportation Systems Center, 2001.

J.S. Warner and R.G. Johnston, “GPS Spoofing Countermeasures”, Los Alamos National Laboratory, 2003.

T. Nighswander et al, “GPS Software Attacks”, CCS’12, Raleigh, North Carolina, USA, 2012.

Smart Grid

G. Rasche, “Intrusion Detection System for Advanced Metering Infrastructure”, Electric Power Research Institute, University of Illinois at Urbana-Champaign, 2012.

P. McDaniel and S. McLaughlin, “Identifying (and Addressing) Security and Privacy Issues in Smart Electric Meters”, http://cnls.lanl.gov/~chertkov/SmarterGrids/Talks/McDaniel.pdf, Network and Security Research Center, Pennsylvania State University, 2011.

C. S. King, “The Economics of Real-Time and Time-of-Use Pricing for Residential Consumers”, Technical report, American Energy Institute, 2001.

S. McLaughlin et al., “Multi-vendor Penetration Testing in the Advanced Metering Infrastructure”, Network and Security Research Center, Pennsylvania State University, 2010.

E. Naone, “Meters for the Smart Grid”, MIT Technology Review Magazine, September/October, 2009.

United States Government Accountability Office, “ELECTRICITY GRID MODERNIZATION - Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed”, http://www.gao.gov/new.items/d11117.pdf (accessed 2013/11/04), 2011.

U.S.-Canada Power System Outage Task Force, “Interim Report: Causes of the August 14th blackout in the United States and Canada“, 2003.

Organization for Security and Co-operation in Europe (OSCE), “Good Practices on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace”, OSCE Study, 2013.

Ausschuss für Bildung, Forschung und Technikfolgenabschätzung, “Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung“, Drucksache 17/5672 des Deutschen Bundestages, 2011.

ADS-B/ACARS/FMS

L. Constantin, “Researcher: Vulnerabilities in aircraft systems allow remote airplane hijacking”, http://www.pcworld.com/article/2033807/vulnerabilities-in-aircraft-systems-allow-remote-airplane-hijacking-researcher-says.html (accessed 2013/04/23), IDG News Service, 2013.

A. Greenberg, “Researcher Says He's Found Hackable Flaws In Airplanes' Navigation Systems (Update: The FAA Disagrees)”, http://www.forbes.com/sites/andygreenberg/2013/04/10/researcher-says-hes-found-hackable-flaws-in-airplanes-navigation-systems/ (accessed 2013/07/06), Forbes, 2013.

SCADA

B. Galloway and G.P. Hancke, “Introduction to Industrial Control Networks”, University of Pretoria, revised version, 2012.

C. Ten et al., Vulnerability Assessment of Cybersecurity for SCADA Systems”, IEEE Transactions on Power Systems, Vol.23, No.4, 2008.

N. Subramanian, “Improving Security of Oil Pipeline SCADA Systems Using Service-Oriented Architectures”, OTM 2008 Workshops, LNCS 5333, pp. 344–353, 2008.

G.G. Brown et al., “Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses”, Operations Research Department, Naval Postgraduate School, 2005.

N. Falliere et al., “W32.Stuxnet Dossier“, Symantec Security Response, Version 1.4, 2011.

D.E. Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran”, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (accessed 2013/07/06), The New Your Times, 2012.

Industrial Control Systems Computer Emergency Response Team, “Incident Response Activity: Brute Force Attacks on Internet-Facing Control Systems”, ICS-CERT Monitor, April/May/June, 2013.

Misc

United Nations Office on Drugs and Crime, “Comprehensive Study on Cybercrime”, Draft, 2013.

International Telecommunications Union, “Internet users per 100 inhabitants 2006-2013”, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2012/ITU_Key_2006-2013_ICT_data.xls (accessed 2013/06/29), ITU Geneva, 2013.

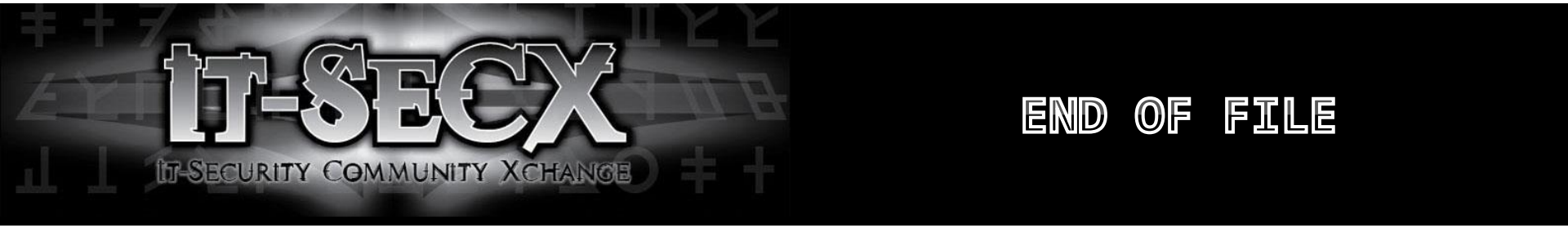
D. Evans, “The Internet of Things - How the Next Evolution of the Internet Is Changing Everything”, Cisco Internet Business Solutions Group, 2011.

T. Heer et al., “Security Challenges in the IP-based Internet of Things”, RWTH Aachen University, 2011.

Department of Homeland Security, “National Strategy for Homeland Security”, www.hsdl.org/?view&did=479633 (accessed 2013/06/27), DHS, 2007.

J. Kirk, “Pacemaker hack can deliver deadly 830-volt jolt”, http://www.computerworld.com/s/article/9232477/Pacemaker_hack_can_deliver_deadly_830_volt_jolt (accessed 2013/11/04), Computer World, 2012.

Wikipedia, “Software-defined Radio”, http://en.wikipedia.org/wiki/Software-defined_radio (accessed 2013/11/04), 2013.



Thanks for your attention!
See you next time!

Questions?

robert.luh@fhstp.ac.at