Hamburg Aerospace Lecture Series

Cybersecurity – The Downside of Digitalization

23 May 2019

Dieter Gollmann
TUHH & Nanyang University of Technology, Singapore

http://doi.org/10.5281/zenodo.5596591

TUHH
Hamburg University of Technology

Deutsche Gesellschaft für Luft- und Raumfahrt Lilienthal-Oberth e.V. Bezirksgruppe Hamburg

ROYAL AERONAUTICAL SOCIETY HAMBURG BRANCH e.V.

ZAL

Verein Deutscher Ingenieure Hamburger Bezirksverein e.V. Arbeitskreis Luft- und Raumfahrt

Hamburg Aerospace Lecture Series
Hamburger Luft- und Raumfahrtvorträge

HAW HAMBURG

RAeS Hamburg in cooperation with the DGLR, VDI, ZAL & HAW invites you to a lecture

Cyber Security – the Downside of Digitisation

Prof. **Dieter Gollmann,** Professor for Security in Distributed Applications, Hamburg University of Technology

Date: Thursday 23 May 2019, 18:00
Location: HAW Hamburg Berliner Tor 5, (Neubau), Hörsaal 01.13

Lecture followed by discussion
No registration required !
Entry free !

Some may see digitisation as the next industrial revolution, bringing new opportunities, but also new dangers. However, digitisation is already with us. Programmable connected devices with interfaces to the physical world provide a basis for a more flexible and efficient control of processes in many application domains. Programmable connected devices can have remote effects and can be remotely adjusted and updated. By the same means, remote adversaries may send specially crafted inputs to programmable connected devices to control processes according to their own objectives.

Cyber security, another fashionable term that may be little more than a new name for established concepts, deals with the flipside of digitisation. How can one defend against attacks facilitated by digitisation? This talk will look at the armouries of attackers and defenders and discuss what needs to be done to stay in control of digitised processes.

Prof. Dieter Gollmann received his Dipl.-Ing. in Engineering Mathematics (1979) and Dr.tech. (1984) from the University of Linz, Austria.
He was a Lecturer in Computer Science at Royal Holloway, University of London, and later a scientific assistant at the University of Karlsruhe, Germany. He rejoined Royal Holloway in 1990, where he was the first Course Director of the MSc in Information Security. He moved to Microsoft Research in Cambridge in 1998. In 2003, he took the chair for Security in Distributed Applications at Hamburg University of Technology. He is currently Visiting Professor at Nanyang Technological University, Singapore, and member of the Advisory Board of the Centre for Doctoral Training in Cyber-Security at Royal Holloway, University of London.
Dieter Gollmann is an editor-in-chief of the International Journal of Information Security and an editor of the IEEE Security & Privacy Magazine. His textbook on 'Computer Security' has appeared in its third edition.

DGLR / HAW	Prof. Dr.-Ing. Dieter Scholz	Tel.: (040) 42875 8825	info@ProfScholz.de
DGLR	Dr.-Ing. Martin Spiek	Tel.: (040) 9479 2855	martin.spiek@thelsys.de
RAeS	Richard Sanderson	Tel.: (04167) 92012	events@raes-hamburg.de

DGLR Bezirksgruppe Hamburg http://hamburg.dglr.de
RAeS Hamburg Branch http://www.raes-hamburg.de
VDI, Arbeitskreis L&R Hamburg http://www.vdi.de/
ZAL TechCenter http://www.zal.aero/veranstaltungen

Hamburg Aerospace Lecture Series DGLR HAW Hamburg RAeS VDI ZAL

Hamburg Aerospace Lecture Series von DGLR, RAeS, ZAL, VDI und HAW Hamburg (PSL)
http://hav-connect.aero/Group/Lectures

Security is a Fashion Industry

IT Security

Information Security

Information Assurance

Cybersecurity

FUD

Fear – Uncertainty – Dread

FUD

- One easy test for cyber security is to ask yourself the following question: Could Godzilla do it?
- If the answer's yes, it's probably not a very realistic scenario
- So when you get into these things where a big green monster is going to shut down the whole electrical system or the water system, it's not very likely

James A. Lewis, Center for Strategic and International Studies

Digitalization – Think Big

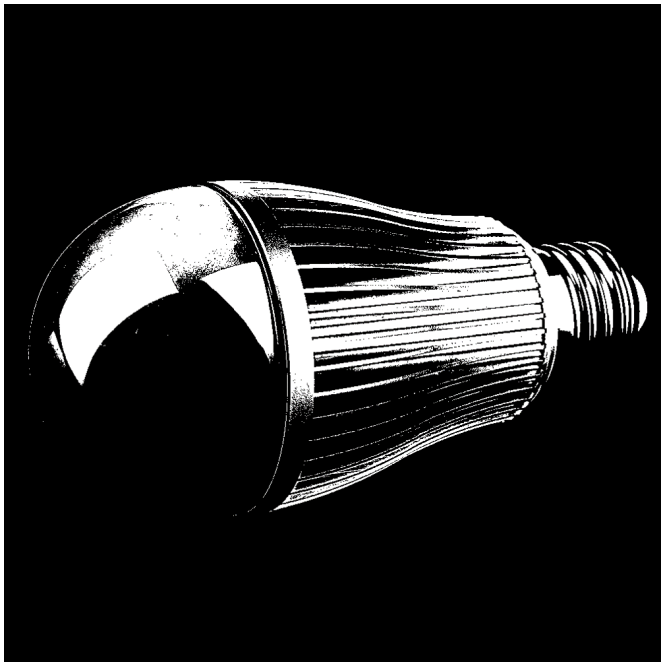
computer tomography for trees

mathematics + computer science + sensors make possible
what was impossible before

`sinews.siam.org/Details-Page/a-reconstruction-algorithm-is-a-key-enabling-technology-for-a-new-ultrafast-ct-scanner`

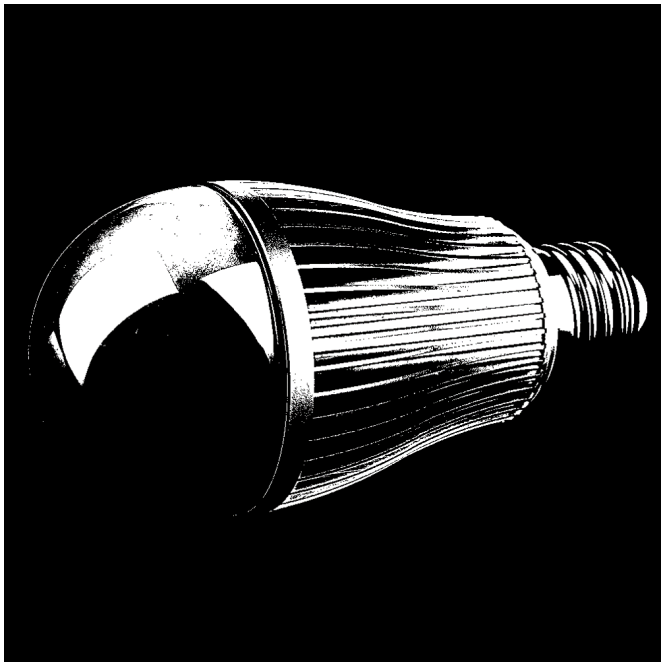
Digitalization – At Home

What is this?



Digitalization – At Home

What is this?

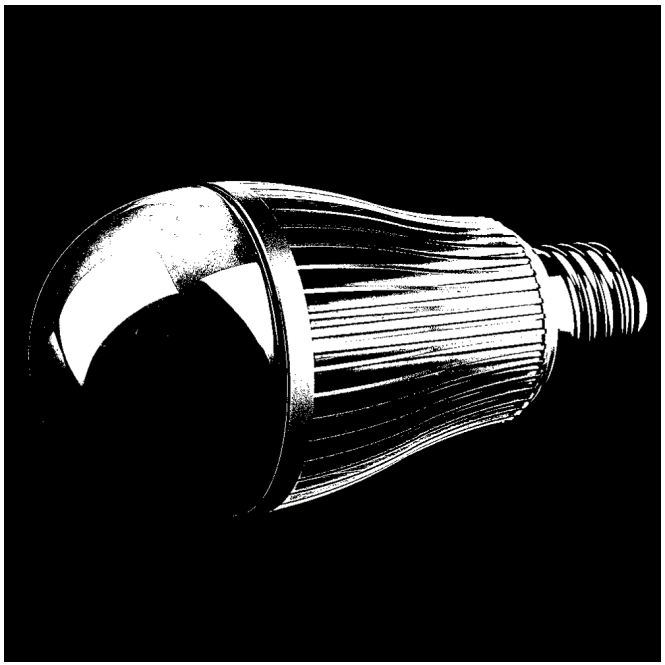


this is a webserver

www.aliexpress.com/store/product/New-Arrival-E27-9W-LED-Bulb-2-4G-Wireless-RGBW-Light-WiFi-Controller-iOS-Android-MiLight/106303_32233209687.html

Webserver

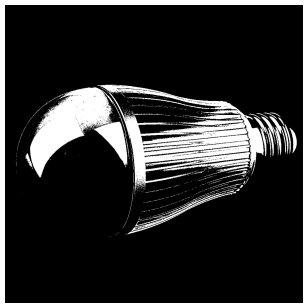
What is this?



software handling and responding to requests
sent via the HTTP protocol

#1: Software

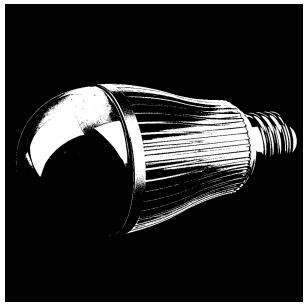
- Software facilitates intelligent control
- How does it react to unforeseen inputs?
- Tetris in IFE, 2005: enter difficulty level 5 numerically, then keep pressing the $\oplus$ button



> *Suddenly, the display now flashes -128 just for an instant and then poof . . . screen goes black.*
>
> *Poof . . . screen of the person next to me goes black.*
>
> *Screens in front of me and behind me go black.*
>
> *The entire plane entertainment system goes down.*

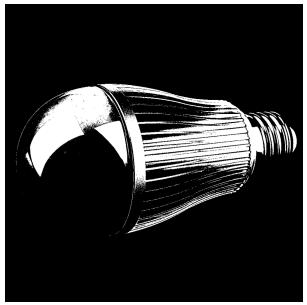
`https://www.csoonline.com/article/2136265/data-protection/how-to-crash-an-in-flight-entertainment-system.html`

#1: Software



- The big software vendors had faced this problem 20 years ago, and they have reacted
  - *My friends who used to earn their money writing exploits have given up; the hurdles have become too high*
  - What about the manufacturers of light bulbs, home routers, and the creators of websites?

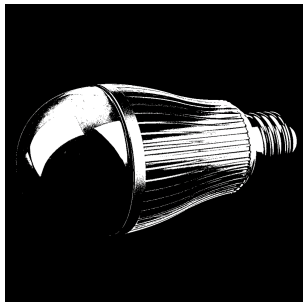
#1: Software



- The big software vendors had faced this problem 20 years ago, and they have reacted
  - *My friends who used to earn their money writing exploits have given up; the hurdles have become too high*
  - What about the manufacturers of light bulbs, home routers, and the creators of websites?

- . . . a webserver could give access to more than a light bulb, e.g. to a database

#1: Software



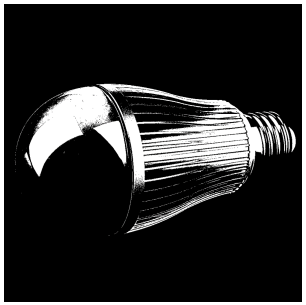
- The big software vendors had faced this problem 20 years ago, and they have reacted
  - *My friends who used to earn their money writing exploits have given up; the hurdles have become too high*
  - What about the manufacturers of light bulbs, home routers, and the creators of websites?

- . . . a webserver could give access to more than a light bulb, e.g. to a database

- SQL injection attack on Panasonic Avionics IFE, 2016, `https://ioactive.com/in-flight-hacking-system/`

#2: Who is authorized to control the bulb?

- Passwords for light bulbs?
  - One password to rule them all?
    Not particularly secure
  - Each bulb has its own password?
    Needs proper password management

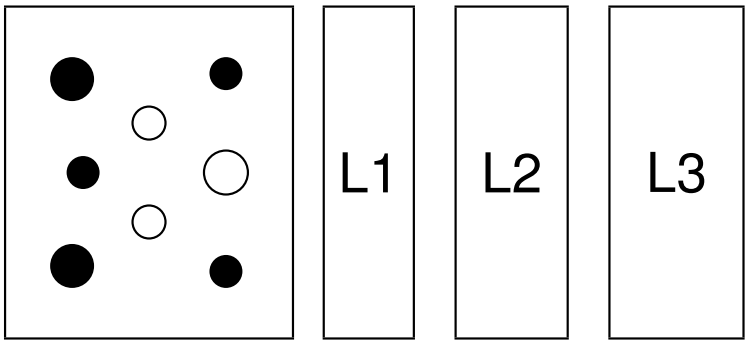


- Who is authorized to repair software (install updates)?
- How do you know that the correct software is running?
- Who fixes errors in software?

#3: Palaces Built on Sand – A Mirage?

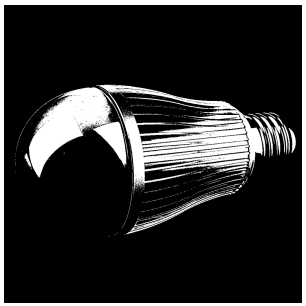
#3: Palaces Built on Sand

- Assume your software is provably secure
- Is its execution provably secure?
- Differences between model and actual behaviour?



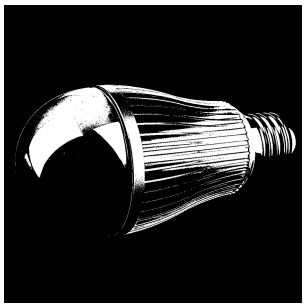
- Machine instructions split into μ-operations, optimistic execution, rollback to a consistent state if necessary
- Consistency w.r.t. the CPU state, but not for the cache
- Spectre and Meltdown, January 2018

#4: Recursion



- You have a secure connection from the browser in your smartphone to your devices
- US Department of Homeland Security
  - *We are not worried if you walk out on your factory site and use your smartphone to query the state of devices*
  - *We would be worried, if you use your smartphone to control the devices*

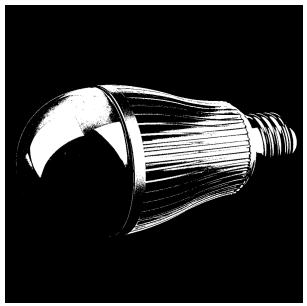
#4: Recursion



- You have a secure connection from the browser in your smartphone to your devices
- US Department of Homeland Security
  - *We are not worried if you walk out on your factory site and use your smartphone to query the state of devices*
  - *We would be worried, if you use your smartphone to control the devices*

- Whose software is running on your smartphone?

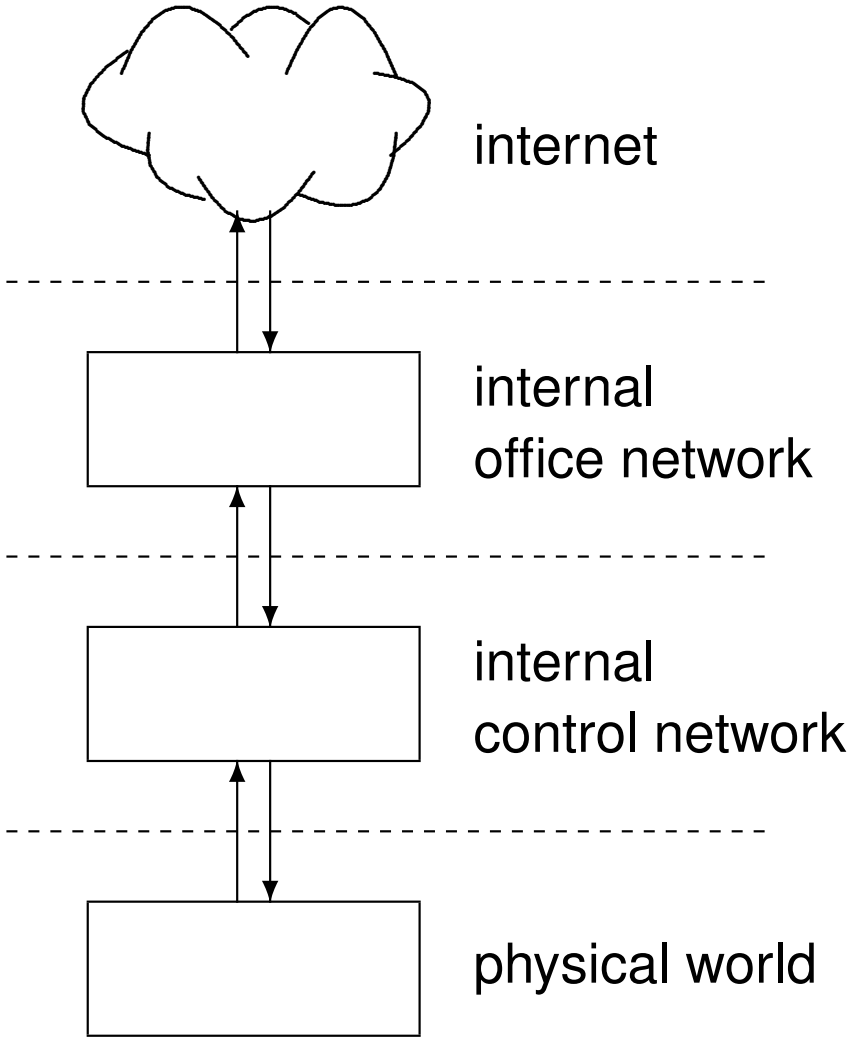
#4: Recursion



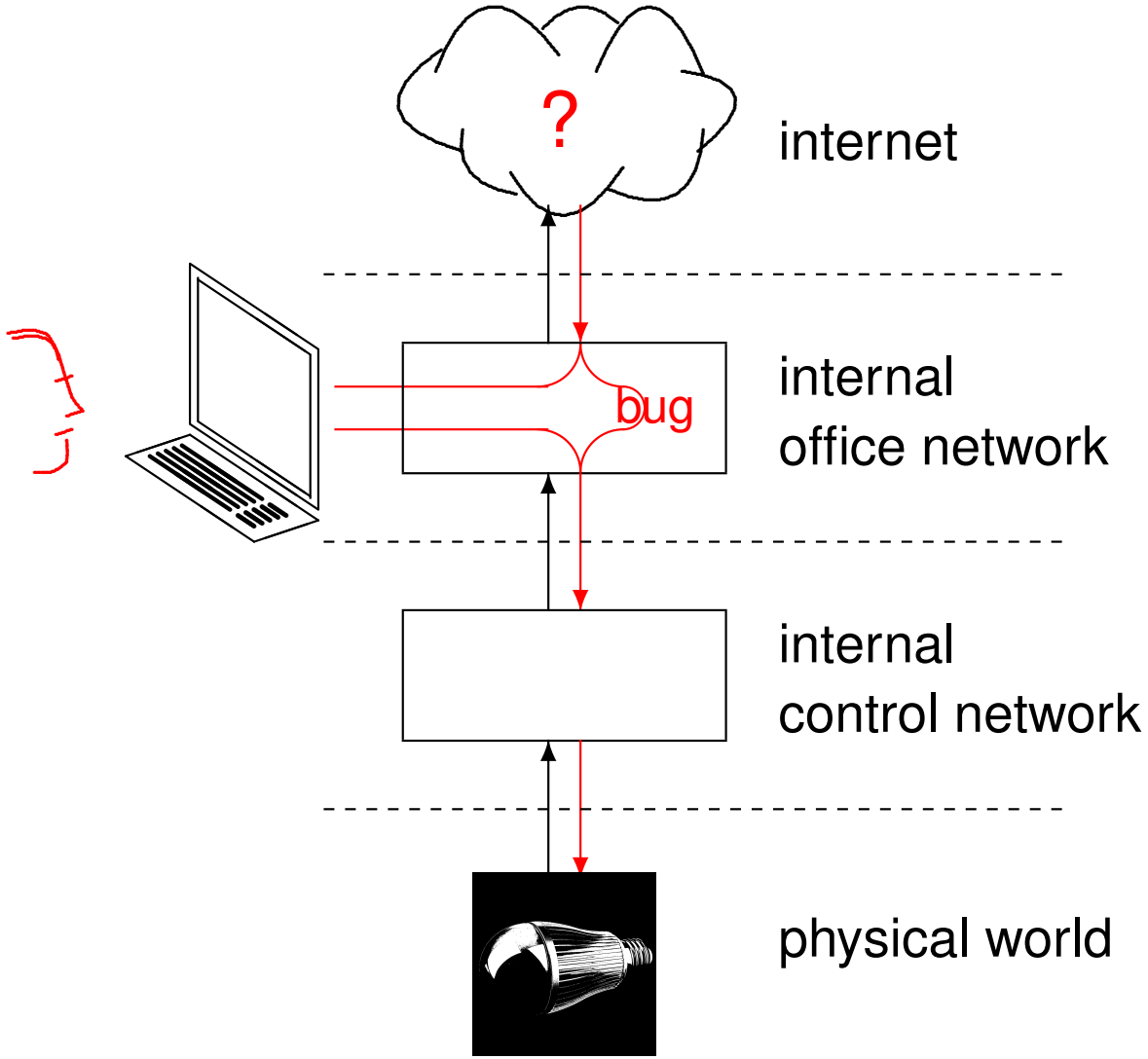
- You have a secure connection from the browser in your smartphone to your devices
- US Department of Homeland Security
  - *We are not worried if you walk out on your factory site and use your smartphone to query the state of devices*
  - *We would be worried, if you use your smartphone to control the devices*

- Whose software is running on your smartphone?
- Back to Square One

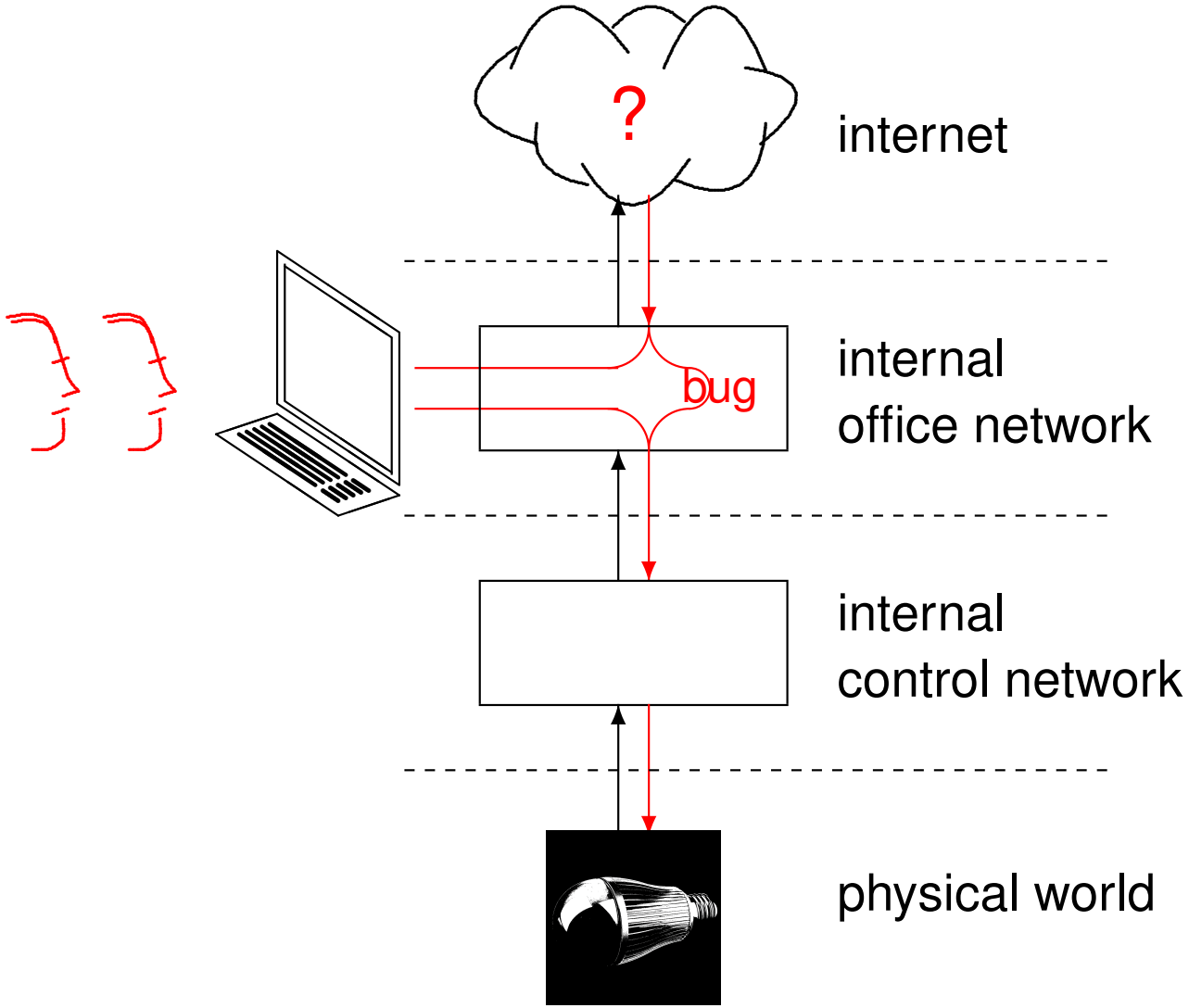
IT-Landscape



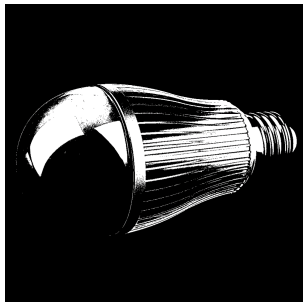
Hostile Remote Control?



Hostile Remote Control?



#5: Who is reading your traffic?



- Whoever has eavesdropped on a password can control the device remotely
- Defence: encrypt communication (cryptography)
- Déjà vu: keys for bulbs?
  - Where do the keys come from?
  - Security chip in every light bulb?
- Distribution chains similar to those for chips in bank cards?

#6: Dependency

- DDoS-Attack (Mirai) on building management system; heating system controller reboots if the management system doesn't respond; boiler switches off if it doesn't hear from controller – fail safe behaviour (in winter?)

`metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter`

Defences

- Secure Software
  - that cannot be deceived by intentionally malformed inputs
- Access control
- Firewalls
  - access control between networks
- Attack detection – Intrusion Detection
- Cryptography – encryption
- User training

Intrusion Detection

- May detect known attack patterns
- Can artificial intelligence tell Good from Evil?

Intrusion Detection

- May detect known attack patterns
- Can artificial intelligence tell Good from Evil?

- Anti-virus software since the early 1990s
- Machine Learning used in Intrusion Detection for 20 years
  - Criterion for practitioners: keep false alarm rate low

- *Whether ML can be applied in a concrete application depends more on the data than on the learning algorithm*

Intrusion Detection

- May detect known attack patterns
- Can artificial intelligence tell Good from Evil?

- Anti-virus software since the early 1990s
- Machine Learning used in Intrusion Detection for 20 years
  - Criterion for practitioners: keep false alarm rate low

- *Whether ML can be applied in a concrete application depends more on the data than on the learning algorithm*

- Can ML be lured to learn a falsehood?

Cryptography – Encryption

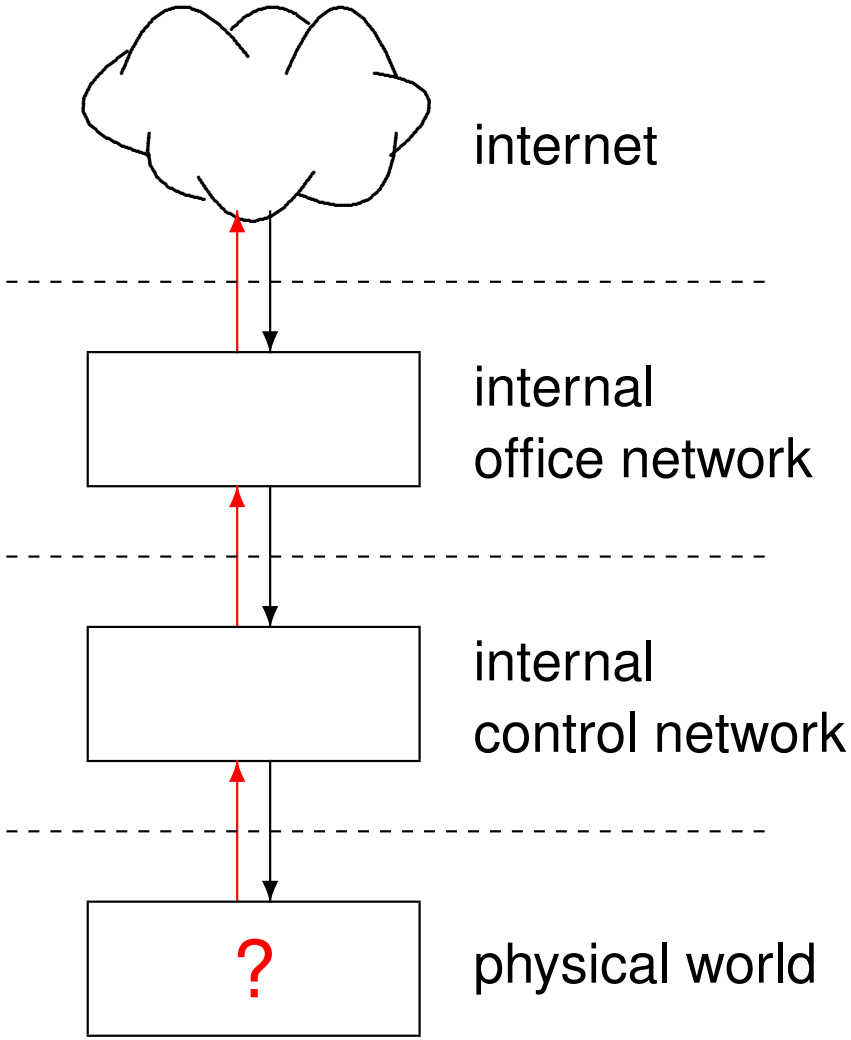
- Protects against attacks on data in transmission
- Protects against attacks on data in storage
- Does not defend against bugs in software
- Can get in the way of Intrusion Detection

Cryptography – Encryption

- Protects against attacks on data in transmission
- Protects against attacks on data in storage
- Does not defend against bugs in software
- Can get in the way of Intrusion Detection

- Cryptography rarely solves security problems; cryptography transforms security problems into key management problems

Manipulation of Inputs



Security of Cyber-physical Systems

- Inputs manipulated before they are transmitted ‘securely’
  - False manual data input
  - Manipulating the environment: temperature, smoke, . . .
  - Manipulation of sensors, e.g. use ultra sound to destabilize quadrocopters
- Challenge for manufacturers: manipulation resistant devices
- Influence on false data on process control?
- Being able to manipulate inputs does not necessarily imply that you now know how to control the system
- *Programming Weird Machines* in the physical world?

My Summary

- Digitalization $\approx$ Remote Control and Reconfigurability
- The Promise: better control, how and whither?
- The Downside: inferior control, who and whither?
- “Solutions” exist for all the points mentioned
- Must be considered early enough in the planning stages
- Planning must be aware of the security challenges

My Summary

- Digitalization $\approx$ Remote Control and Reconfigurability
- The Promise: better control, how and whither?
- The Downside: inferior control, who and whither?
- “Solutions” exist for all the points mentioned
- Must be considered early enough in the planning stages
- Planning must be aware of the security challenges

- Will the problems disappear with the next user generation?

My Summary

- Digitalization $\approx$ Remote Control and Reconfigurability
- The Promise: better control, how and whither?
- The Downside: inferior control, who and whither?
- “Solutions” exist for all the points mentioned
- Must be considered early enough in the planning stages
- Planning must be aware of the security challenges

- Will the problems disappear with the next user generation?

Thank you very much for your attention