Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

The next step in IT security after Snowden

Prof. Dr. (TU NN)
Norbert Pohlmann

Institute for Internet Security - if(is)
Westphalian University of Applied Sciences
Gelsenkirchen, Germany
www.internet-sicherheit.de

if(is) internet security.

Content

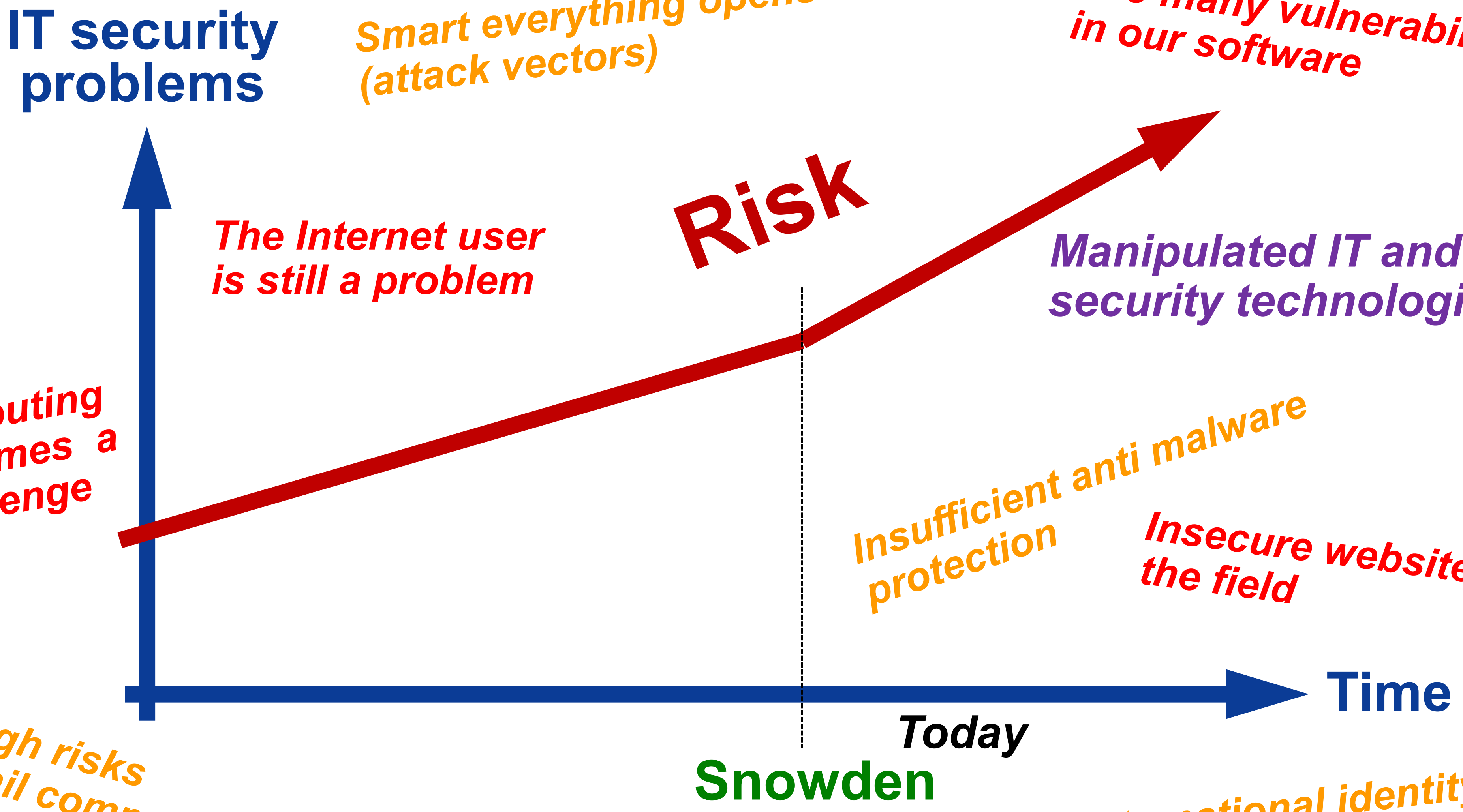
internet security.

- Evaluation of IT Security
- Much more encryption is needed
- Paradigm Shifts in IT and IT Security
- Summary

Evaluation of IT Security
→ Overview of the biggest problems

Smart everything opens new doors (attack vectors)

Too many vulnerabilities in our software



The Internet user is still a problem

Manipulated IT and IT security technologies

Cloud Computing becomes a challenge

Insufficient anti malware protection

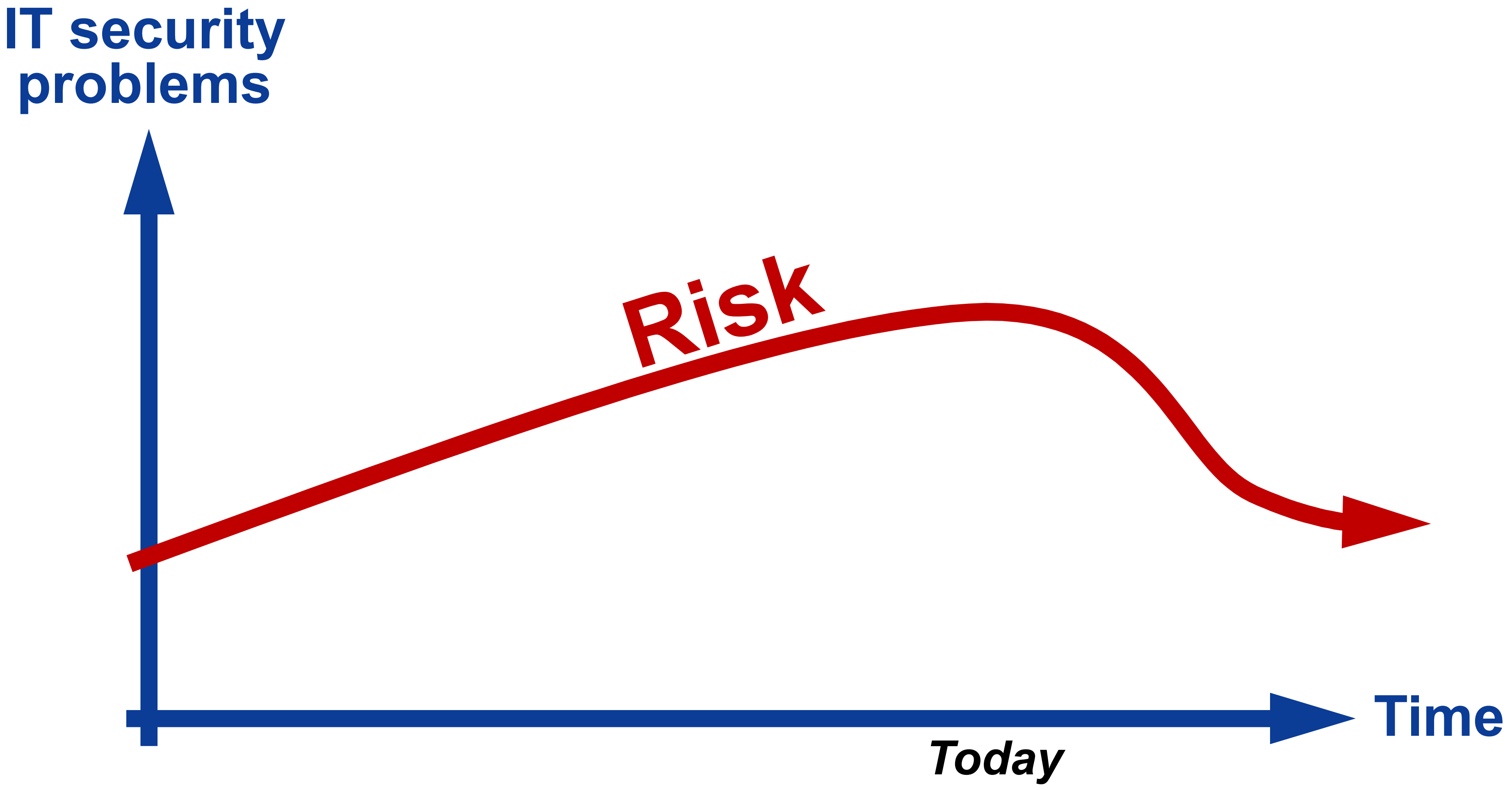
Insecure websites in the field

Too high risks in e-mail communication

Smartphones offer new attack vectors

No international identity management

Evaluation of IT Security
→ Our challenge



Active Encryption → Much more is needed

- Encryption for a sustainable protection of our data
  - IPSec (every 125th IP packet), SSL (every 7th IP packet), …
  - E-Mail-Encryption (~ every 20th E-Mail), ...
  - Disc-, File Encryption, …
- **Requirements:**
  - **Trustworthy encryption technology**
    (No backdoors, strong random numbers, correct implementation, ...)
    → *Very powerful IT security industry in DE*
    → *IT Security made in Germany*
  - **Trustworthy IT security infrastructure**
    (PKI with RA und CA; Root certificates, …)

Paradigm Shift – (1)
→ More responsibility less indifference

- **Producer responsibility**
  - Software and hardware will better matched and problems would be better identified and solved.

- **Validation / Certification**
  - Independent and qualified organizations prove (improve) the quality of IT (security) products and solution

Paradigm Shift – (2)
→ More proactive less reactive IT security

Reactive IT Security Systems

- Today we use a lot of reactive IT security solutions and that means we are always **running behind the attacker**.
- The idea of reactive IT security is, if we **detect an attack**, we try to protect us as fast as possible to **reduce the damage**.
- For example “reactive IT security systems” are
  - *Intrusion Detection Solutions*
  - *Anti-Malware products*
  - *Anti-Spam /-Phishing*
  - *…*

„Airbag approach“:
If it happens, it should hurt less.

Paradigm Shift – (2)
→ More proactive less reactive IT security

Proactive IT Security Systems

- Proactive IT security offers more **robust** and much more **trustworthy** protection.
- Here we use for example a security kernel with separation and isolation technology combined with intelligent cryptographic security mechanisms.

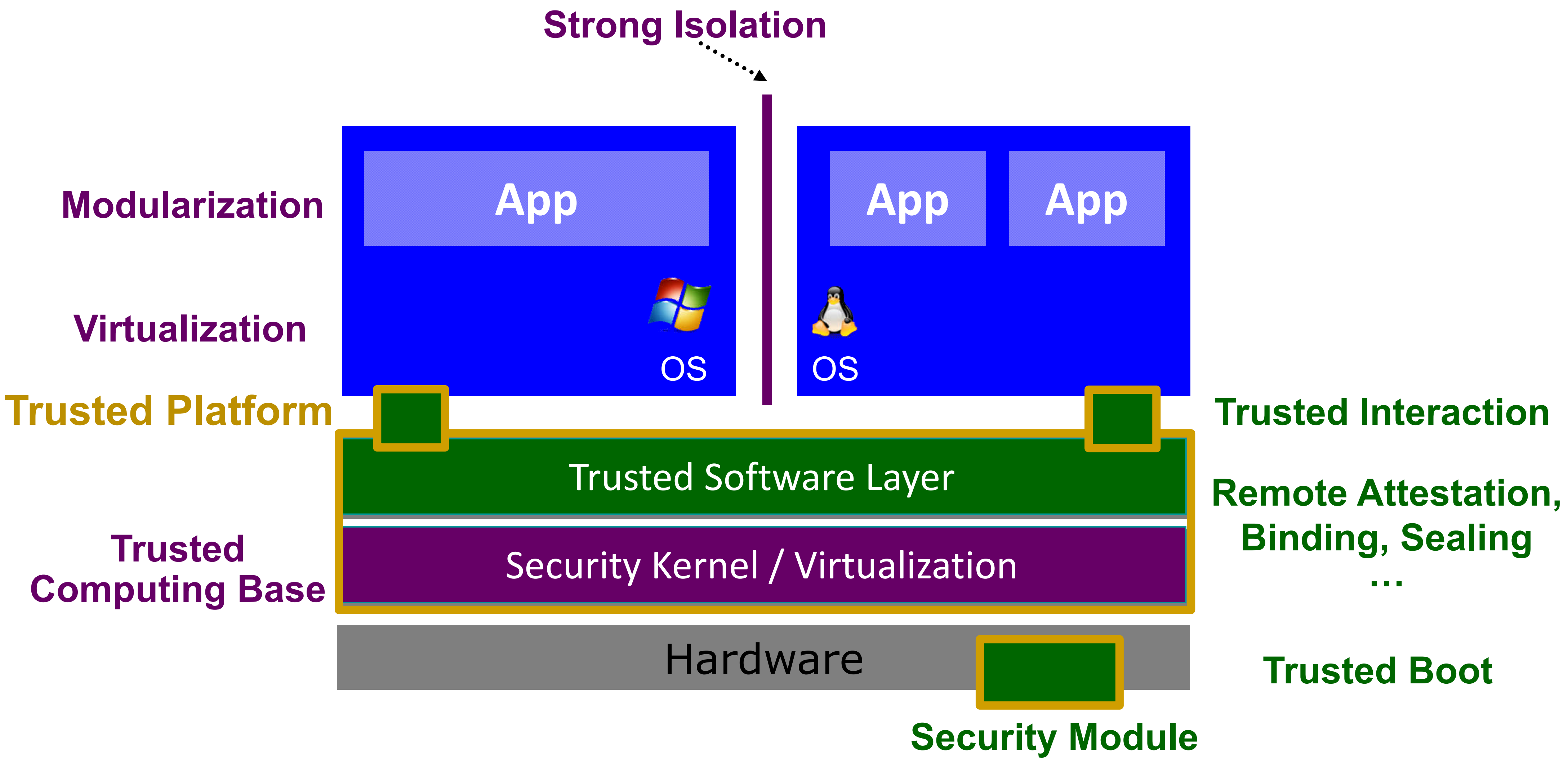
(Trusted Platform)

„ESP strategy“:
Avoid skidding, before it happens.

Paradigm Shift – (2)
→ Trusted Platform

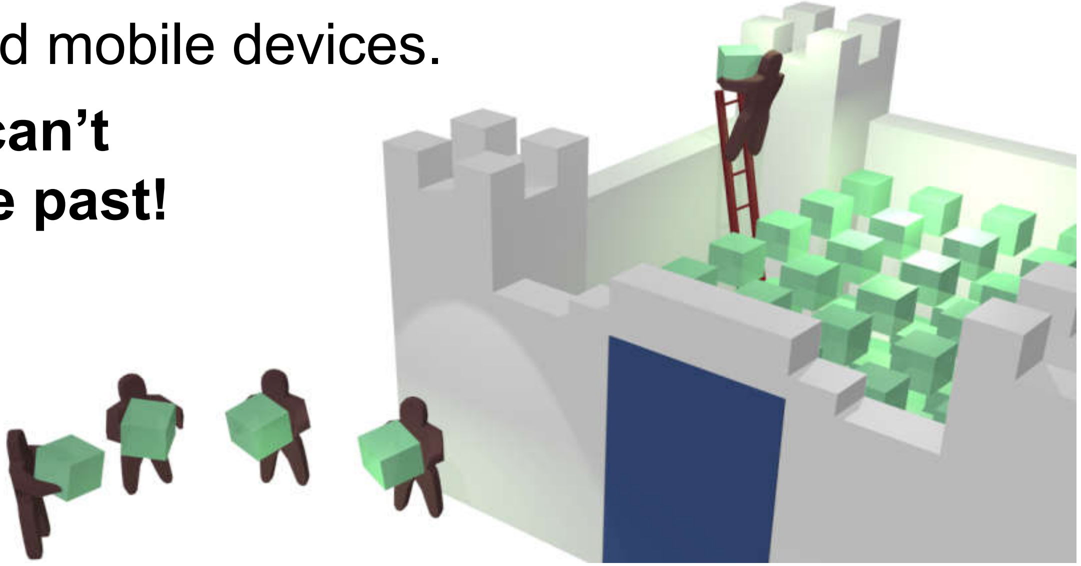
Robustness/Modularity

Integrity Control



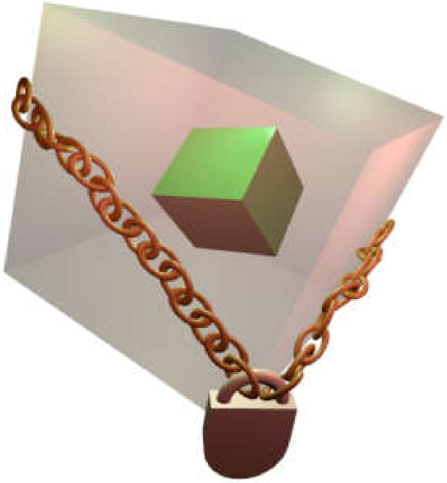
Paradigm Shift – (3)
→ More object less perimeter security

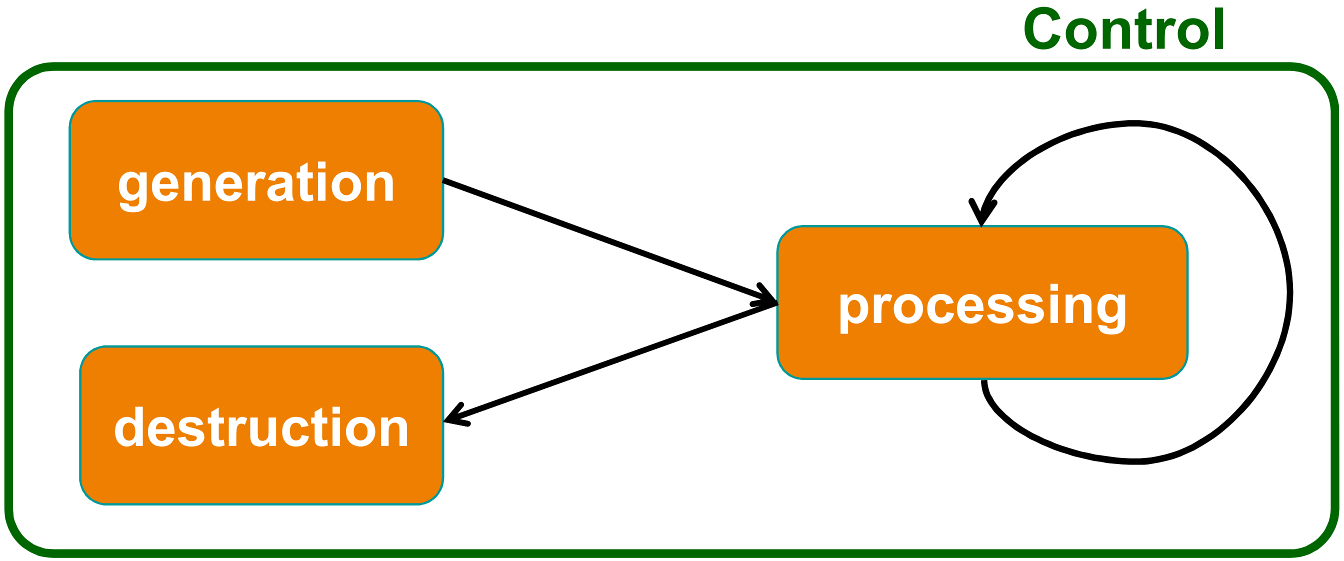
- **Perimeter security**
  - **Defense Model:**
    - Protect a set of computer systems and networks with the help of Firewalls, VPNs, Intrusion detection and so on.
    - Assumption: The computers and the networks are fixed installed.
  - **Evaluation:**
    - Modern world uses flexible and distributed mobile devices.
    - **Perimeter security can’t protect us like in the past!**



Paradigm Shift – (3)
→ More object less perimeter security

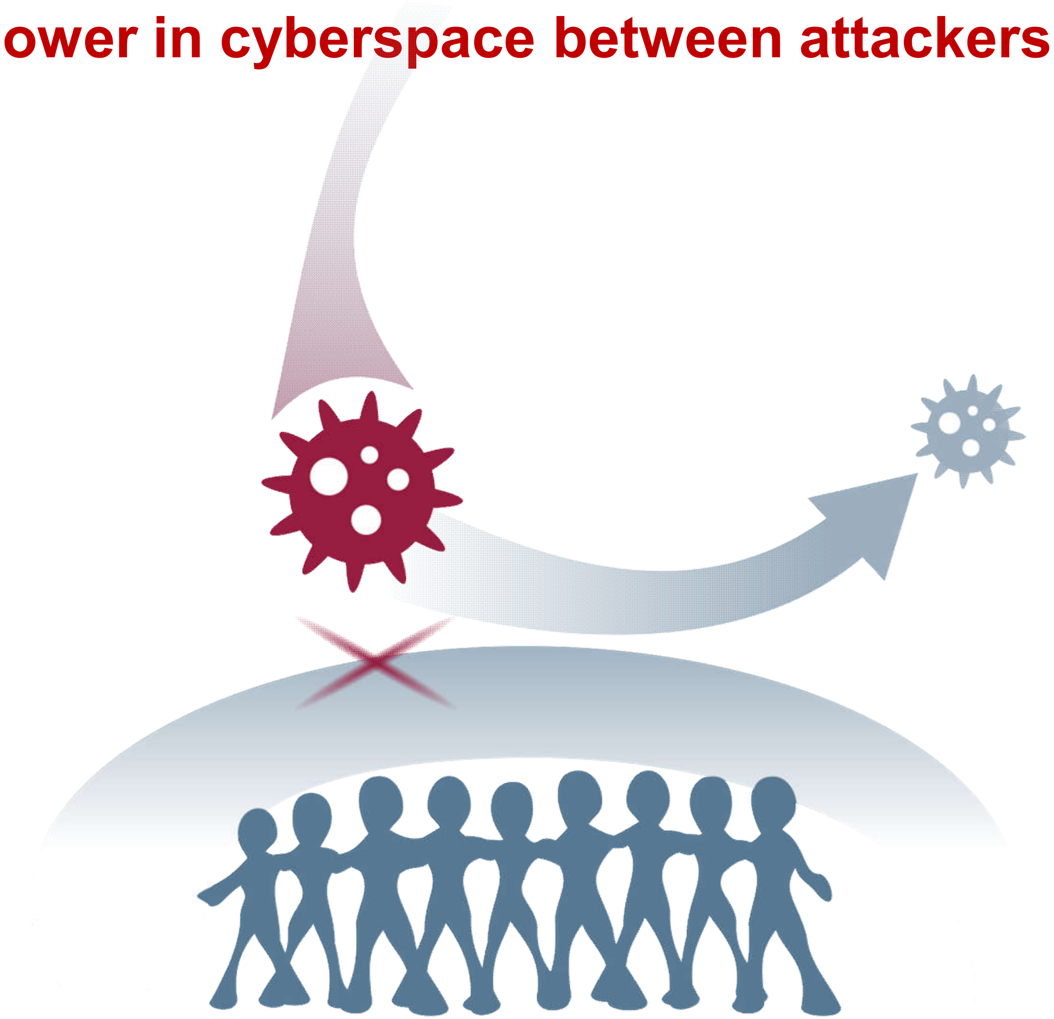
- Object Security (Information Flow Control)
  - Idea:
    - Domain **object-oriented security**, in which the objects are provided with **rights**.
    - The rights define **who can** use the object with **which action** in **which IT environment**
  - *Object Lifecycle Protection*
  - *Distributed Policy Enforcement (even on foreign systems)*





Paradigm Shift – (4)
→ More collaboration less separation

Imbalance of power in cyberspace between attackers and defenders.



Collaboration helps to overcome the imbalanced situation

The next step in IT security
→ Summary

- **Over the time our IT security problems have become bigger and bigger!**

- ***It is very important that we use much more encryption***

- **We need paradigm shifts in IT and IT security, so that we can build trust in using the Internet in the future**
  - **More responsibility less indifference**
  - **More proactive less reactive IT security**
  - **More object less perimeter security**
  - **More collaboration less separation**
  - **…**

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

The next step in IT security after Snowden

Thank you for your attention!
Questions?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institute for Internet Security - if(is)
Westphalian University of Applied Sciences
Gelsenkirchen, Germany
www.internet-sicherheit.de

if(is)
internet security.