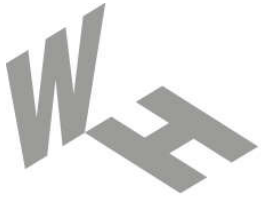


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Changing the defense paradigms to protect the Cyber

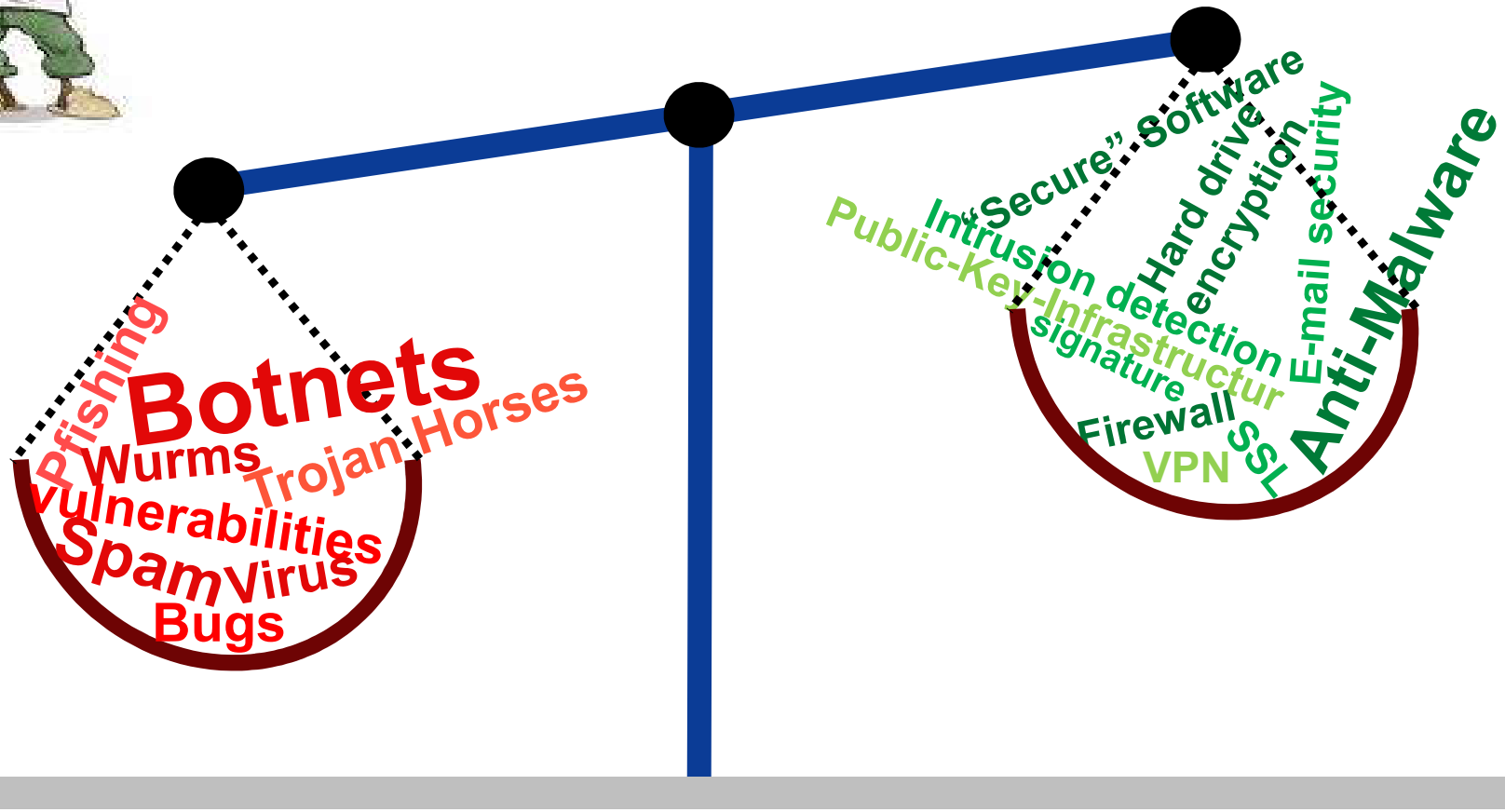
Prof. Dr. (TU NN)
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.

Assessment of the situation
→ Attracts <-> Security Mechanisms

The Hare and the Hedgehog



- Attacks -

- Security Mechanisms -

IT Security Situation Today
→ Threat Potential (1/2)

- Too many vulnerabilities in our Software

- Unsecure websites in the field

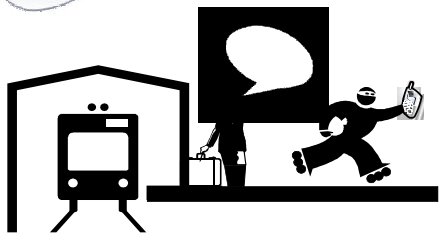
- Insufficient anti malware protection

- No international identity management

IT Security Situation Today
→ Threat Potential (2/2)

- Too high risk in e-mail communication

- SmartPhones become a challenge



- Cloud Computing becomes a challenge

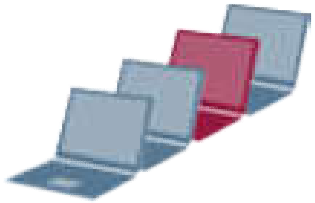
- Smart everything open new door (attack vectors)

© http://www.sevensheaven.nl, via futureclick.net © http://4.bp.blogspot.com

IT Security Situation Today
→ Imbalance of power

Imbalance of power in cyberspace between attackers and defenders

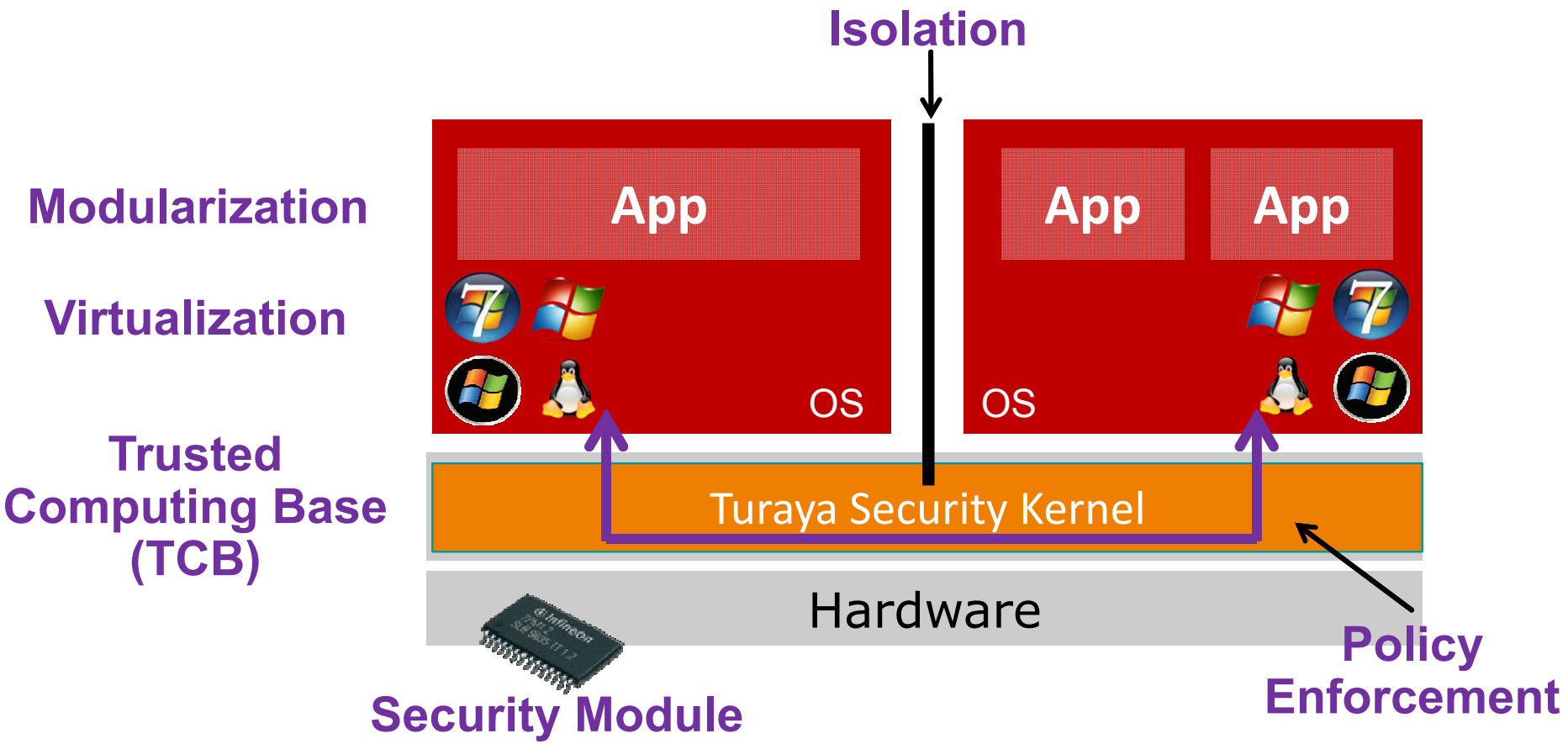
- Highly motivated and skilled attackers
- **Operating in secrecy from almost anywhere in the world,**
- Use a lot of computers (Malware, botnets) with unlimited power



- **Very good, professional and international organized**
- Successful business concepts
  (Underground economy)

Changing the defense paradigms
→ Proactive versus reactive IT security

- **Robust and trusted IT systems**
  - security kernel
  - with separation and isolation technology
  - combined with intelligent cryptographic security mechanisms

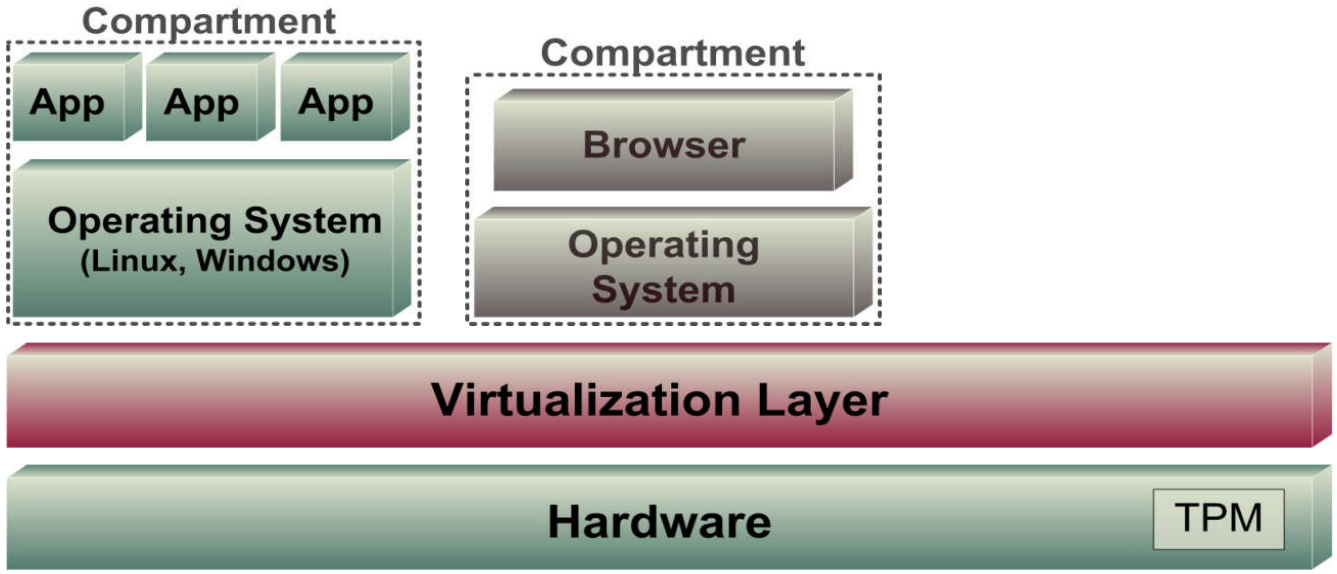


Security Platform - Turaya
→ Architecture and Technology 1/3

- ***Conventional hardware***
  - CPU / hardware devices
- ***TPM***
  - Highest level of protection through hardware-based security
- ***Use the advantages of Trusted Computing technology***

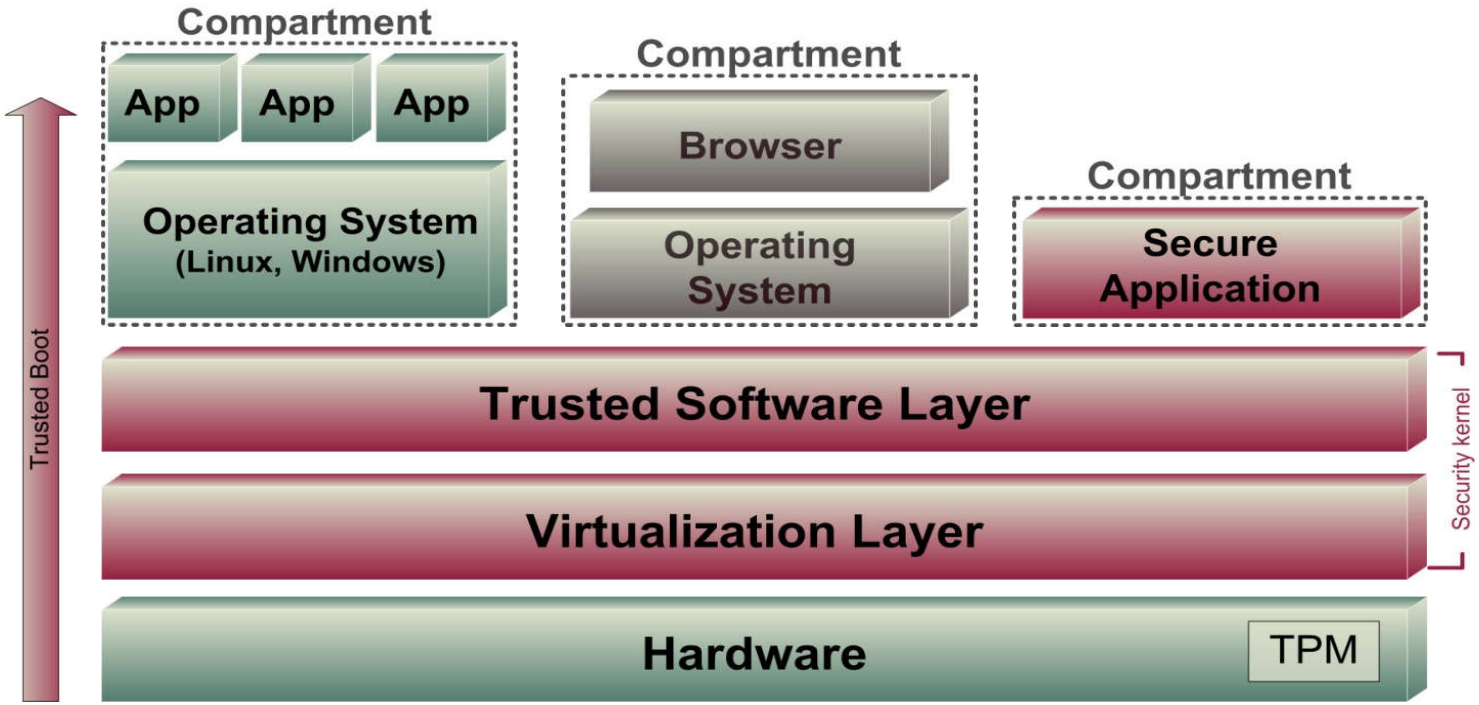
Security Platform - Turaya
→ Architecture and Technology 2/3

- ***Virtualization layer for the purposes of isolation...***
  - Protect applications
  - Protect user data
  - Protect against the manipulation of an application (e.g. browser)
- ***... through modern virtualization technologies***
  - Micro-kernel architecture
  - Use of existing components in compartments



Security Platform - Turaya
→ Architecture and Technology 3/3

- ***Security Platform (Trusted Software Layer)***
  - **Binding of data** to individual compartments
  - **Remotes attestation** (remote integrity check)
  - **Trusted Path (**Between user & application / application & smartcard)
  - **Secure policy enforcement , Secure GUI,** and so on



Changing the defense paradigms
→ Collaboration between the defenders

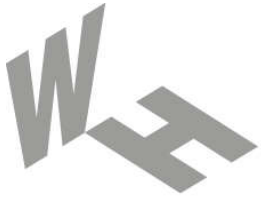
- **Using every Computer as a sensor**
  - All computers send information to build up a common situation awareness
- **Collective counteractive measures**
  - Initiate efficient collective reactions on incidents preferably in an automated fashion
- **Business model of the defenders` collaboration**
  - Less money for security mechanism, lower risk-level, …

Changing the defense paradigms
→ Build up an interna. ITsec infrastructure

- **E-Mail**
  - Common PKI infrastructure
  - Bridge CA, trust model, ….
- **ID Management**
  - Common unique identifier
  - Federation, …
- **Trusted IT system**
  - Common TPM infrastructure
  - Configuration, …
- **…**

Changing the defense paradigms
→ Summary

- The security situation today **is not good enough**
- **There is an imbalance between attackers and defenders**
- We have to change our **defense paradigms**!
- **Proactive security mechanisms help a lot to protect our IT systems and data**
- **Collaboration** between the defenders **are a must!**
- **Let us start today to change the defense paradigms …**



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Changing the defense paradigms to protect the Cyber

Thank you for your attention!
Questions?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institute for Internet Security - if(is)
University of Applied Sciences Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet security.