

# Trust in IT: Upcoming research issues

Mag. Markus Klemen  
Managing Director, Secure Business Austria  
CISSP, CISA, CSSLP

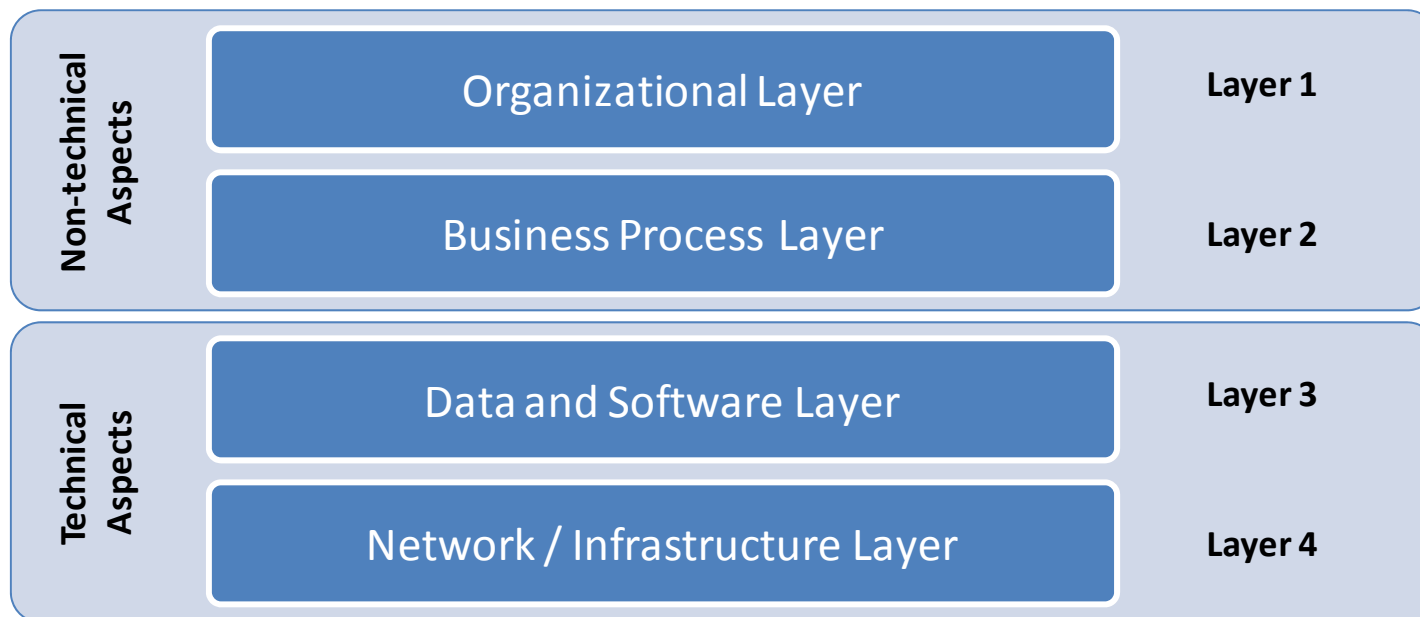
# Secure Business Austria / SBA Research

- Secure Business Austria Research is the first Austrian competence center focusing on organizational and technical IT-Security research aspects
- About 20 companies dedicated to Information Security Research
- Staff: 40 researchers
- Active in European Security initiatives
- Currently: Application for second phase from 2010 to 2017
- Hearing on October 1st 2009

# About this presentation

- Most important issues identified reflect our research agenda
- Hammer / nail situation
- Research agenda constitutes the most important trends as we see them
- In this presentation, I will focus on the most significant research trends in the next 5 years (as I see them)
- Security issues usually lag behind IT developments
  - „Technology before security“ (example: WLAN)
- Increasing awareness in SMEs for IT security concerns

# IT-Security: Holistic view



# Main Areas of Research – Phase 2: 2010 - 2017

**Area 1 (GRC):**  
Governance, Risk and  
Compliance

P1.1: Risk Management and Analysis  
P1.2: Secure Business Process Modeling, Simulation and Verification  
P1.3: Computer Security Incident Response Team  
P1.4: Awareness and E-Learning

**Area 2 (DSP):**  
Data Security and Privacy

P2.1: Privacy Enhancing Technologies  
P2.2: Enterprise Rights Management  
P2.3: Digital Preservation

**Area 3 (SCA):**  
Secure Coding and  
Code Analysis

P3.1: Malware Detection and Botnet Economics  
P3.2: Systems and Software Security  
P3.3: Digital Forensics

**Area 4 (HNS):**  
Hardware and  
Network Security

P4.1: Hardware Security and Differential Fault Analysis  
P4.2: Pervasive Computing  
P4.3: Network Security of the Future Internet

# IT Trends

1. Virtualization
2. Cloud Computing
3. SOA
4. Mobile Computing
5. New software development methodologies

# IT Trends - 2

6. Value of data – document protection
7. IPv6
8. Forensics / Anti-Forensics
9. Combining organizational and technical issues
10. (Green IT)

# 1 . Virtualization

- Base technology is very stable and mature
- Additional aspects are now coming into focus
- Has a major impact on all aspects of IT infrastructure administration
- Inventory, Session Management, automatic VM generation are current issues
- Can increase efficiency significantly
- Cost reduction is not the major driver
- Security aspects will be a major issue in the future (Bluepill)



## 2. Cloud Computing

- May be an important future technological aspect
- Still in a early development phase (E.g. Microsoft Azure)
- Has major security research issues
- Has interesting unresolved legal implications

# 3. Service Oriented Architecture (SOA)

---

- Important technology for B2B
- Enables inter-company communication on a new level
- Introduces inter-company security issues (e.g. access control)
- Security aspects are becoming more and more important

# 4. Mobile Computing

- Wireless broadband enables remote work and smart device applications
- Security on embedded systems
- Security on smartphones (device security)
- Wireless security
  - NFC has great potential (everybody has a cellphone)
  - New payment solutions will develop
  - Authorization/payment schemes will come under scrutiny and will require security research

# 5. Software Development Frameworks

---

- Agile Frameworks
- E.g. Scrum
- Security aspects as part of design phase (architecture)
- Secure development is nothing new, but still not sufficiently established

# 6. Value of Data – Document Protection

- Data Loss Prevention (DLP)
  - Products are in an early stage
  - Technology still in development
  - Major organizational issues
    - Document Classification
    - Rules Setup
- Enterprise Rights Management
  - Different than DRM
  - Company documents are in the main focus
  - Technology still in development (usability)

# 7. IPv6

- Seems to be a never-starting story
- NAT led to a significant delay
- IPv4 address shortage will make IPv6 necessary (soon)
- Some overlapping technologies (IPSEC)
- In the IPv6 protocol family security research will be a major issue in the coming years

# 8. Forensics / Anti-Forensics

- Forensics will become important for judicial disputes
- Research in sub-branches is progressing quickly
  - e.g. database forensics
  - Forensics countermeasures
  - Partly related to malware research
- Establishing systems which support Non-Repudiation is a major goal
- Digital signatures: Usability issue

# 9. Combining organizational and technical aspects

---

- Security economics
- Risk management
- Compliance
- Business process integration
- Business continuity planning
- "Benefits" of security for business in terms of enablement

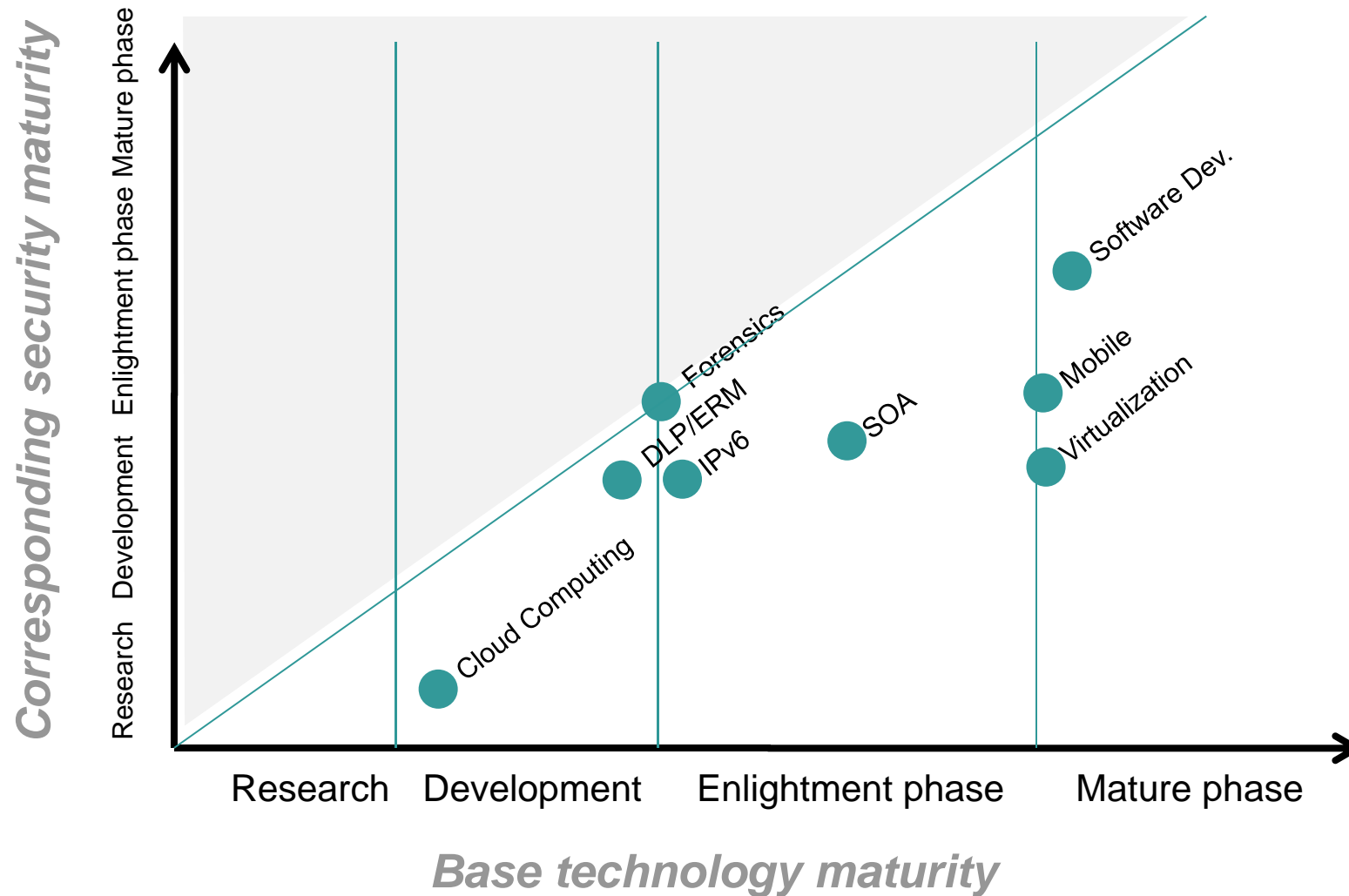


# Long term trends

- Consolidation of communication technologies to IP will continue
- Resulting in single point of failure problems
- Dependency will increase
- "Internet of things" – Intelligent devices will require more security (e.g. pacemakers)
- "Commitment" for transactions will be required → Digital signatures will (have to) become more dominant

# Maturity matrix

www.sba-research.org



# Contact

*Markus Klemen*

*mklemen@sba-research.org*

*mklemen@securityresearch.at*

*Edgar Weippl*

*eweippl@sba-research.org*

*eweippl@securityresearch.at*