

Research Challenges in IT Security

Wolfgang Schneider (wolfgang.schneider@sit.fraunhofer.de)



Fraunhofer Institut
Sichere Informations-
Technologie

Trends

- **Ubiquitous networking**
Various types of networks with different bandwidths
LAN, WLAN, GSM, GPRS, UMTS, bluetooth, infrared
- **Ubiquitous computing**
Large computers, laptops, PDAs, mobile phones, devices, RFID
- **Mobility**
Mobility of persons, mobility of content

Challenges in IT Security

- The notion of „inside“ and „outside“ disappears
- Application context becomes important rather than network assignment or location
- Infrastructures merge through business processes which span over organisations
- Service roaming – Single Sign On
- Secure accounting and billing
- Quality of service

Challenges in IT Security

- We need to manage a growing number of digital identities, roles, capabilities
- Growing machine-to-machine communication which needs to be trustworthy
- Integration of security in very small devices with very limited capabilities or in networks with very limited bandwidth

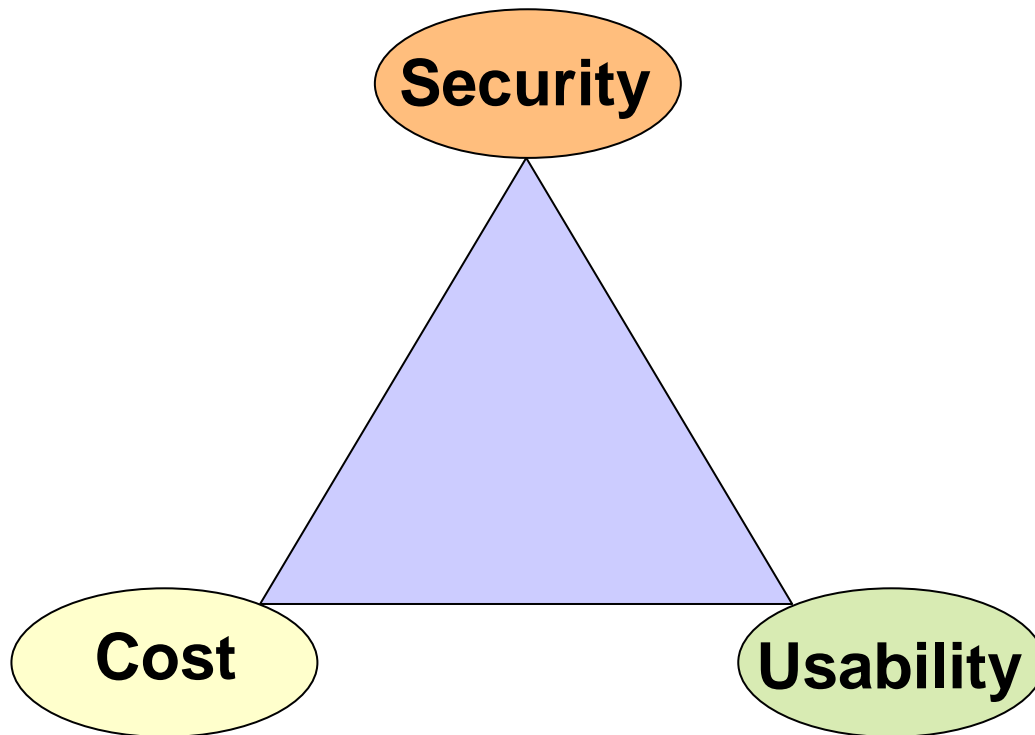
Research issues

- Analysis tools for the control of systems
- Analysis tools for the control of software
- Source code analysis
- Security-aware software development process
- Compiler-supported security
- Tools for the recognition and assessment of attacks
- New concepts for the isolation of incidents

Research issues

- Trustworthy decentralised access and use control systems
- Holistic security management
- Security concepts for mobile content, protection of digital documents and assets
- Combination of hardware and software means for security (Trusted Computing)
- RFID security

Trade-offs in IT Security



Cryptography

- Political control apparently vanished
- Cryptography appears to be solved
- We are using basically cryptography which is 30 years old
- Research in cryptography mainly cryptanalysis

Cryptography

- NIST proposed to withdraw DES (July 24th 2004)
- AES: two years after AES announcement no attack which poses a serious threat to the algorithm
- Hashfunctions:
MD4 and MD4 with serious flaws (collisions can be computed within 15 mins)
- Sha-0, SHA-1, RIPEMD with serious problems
- Current best choice: SHA-256 or SHA 512

Cryptography

- New challenges through quantum computers?
- Shor 1994 (perfect factoring)
- If a quantum computer can be built,
 - all algorithms based on the factoring problems (like RSA) will be insecure
 - All algorithms based on the discrete logarithm problem and elliptic curves will be insecure
- New research topic: quantum computer resistant public-key cryptography (so far not practical)

Most Important Security Areas

according to a survey from TeleTrusT in 2004

- Digital Rights Management
- Secure Web Services
- Trusted Computing
- RFID Security
- Identity Management

Thank you for your attention

Contact: Wolfgang Schneider
Tel. +49 6151 869 700
wolfgang.schneider@sit.fraunhofer.de