DRAFT

New Challenges for IT-Security Research

Udo Helmbrecht, Rainer Plaga

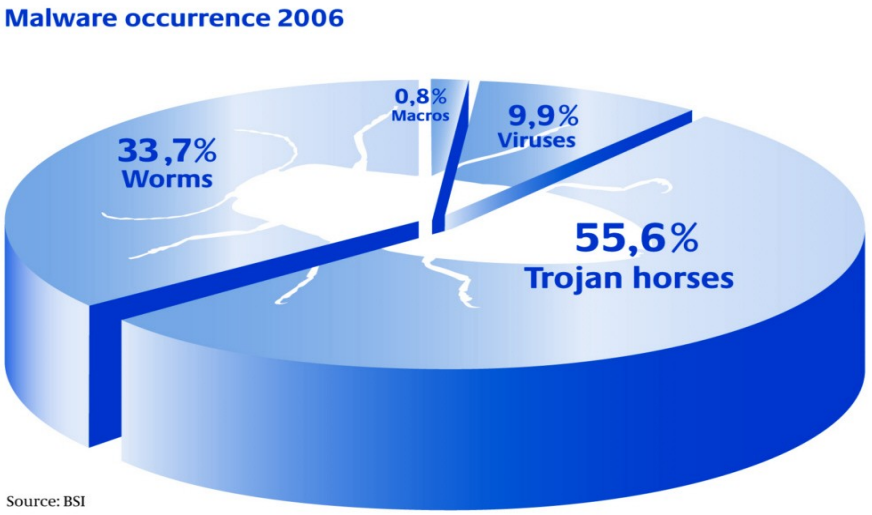
Federal Office for Information Security, BSI

Erice, August 20th, 2008

Threat Situation – Today

DRAFT

- attacks today
  - spam-mails
  - security vulnerabilities
  - malware (viruses, worms, trojan horses)
  - phishing and identity theft
  - denial-of-service
  - botnets
- increasing quality of attacks
  - organized crime
  - terrorist organizations



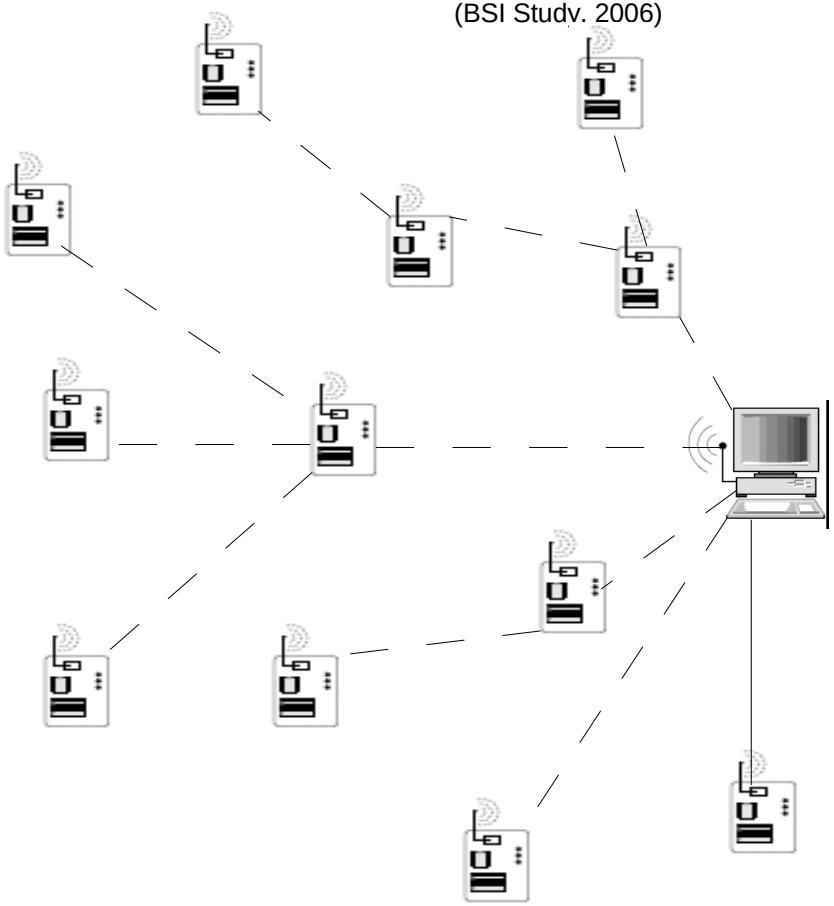
Threat Situation – Tomorrow

DRAFT

- new attack possibilities
  - data encrypted with classical cryptography and stored for long periods attacked with quantum computers
  - new mathematical possibilities to crack classical cryptography
  - New technological possibilities to eavesdrop using stray radiation
- increasing quality of attacks
  - over long periods of time
  - technological possibilities of single individuals tomorrow will vastly exceed the one of governments today

Technological Challenge: Pervasive Computing

DRAFT



Security Attacks concerning

- Network infrastructure (sensor nodes, routing information, ...)
- Data communication

Attacks

- Cloning / Replication of Wireless Sensor Nets (WSNs)
- Sybill-Attacks

  („Simulation of WSNs“)
- Routing-Attacks (Black-Hole)
- Denial of ServiceSpecific

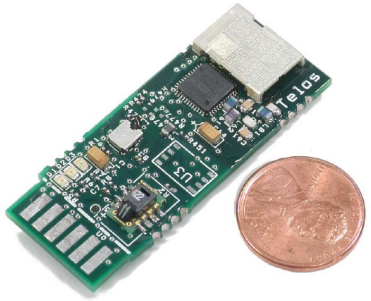
=> Specific Security Mechanisms are needed

WSN = Wireless Sensor Net

Technological Trends: Wireless Sensor Nets

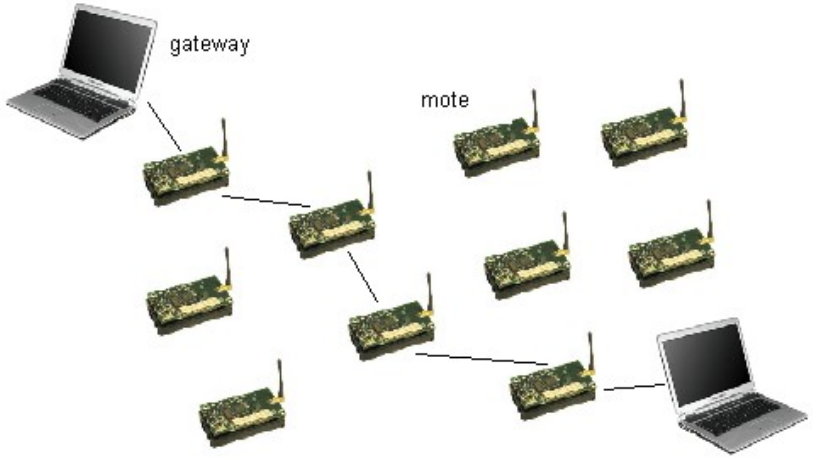
DRAFT

Sensor Chips



Sensor Nodes (Motes)

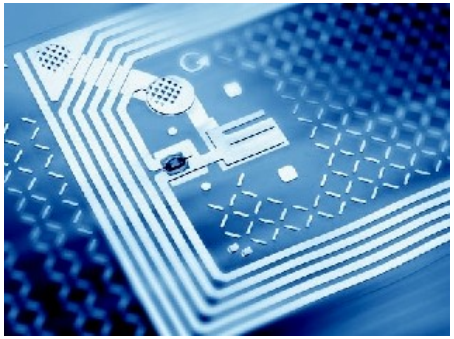
Wireless Sensor Net



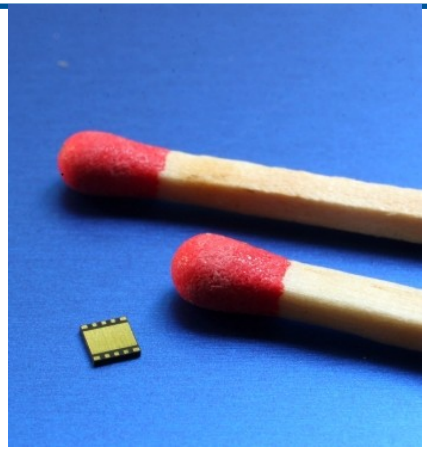
- Flexible, mobile detection of persons and objects
  - Power consumption is critical – new challenge
  - Novel sensor combinations
  - New security mechanisms with very low power consumption

Technological Trends: Mobile Cryptographic RFID Chips

DRAFT



SIEMENS



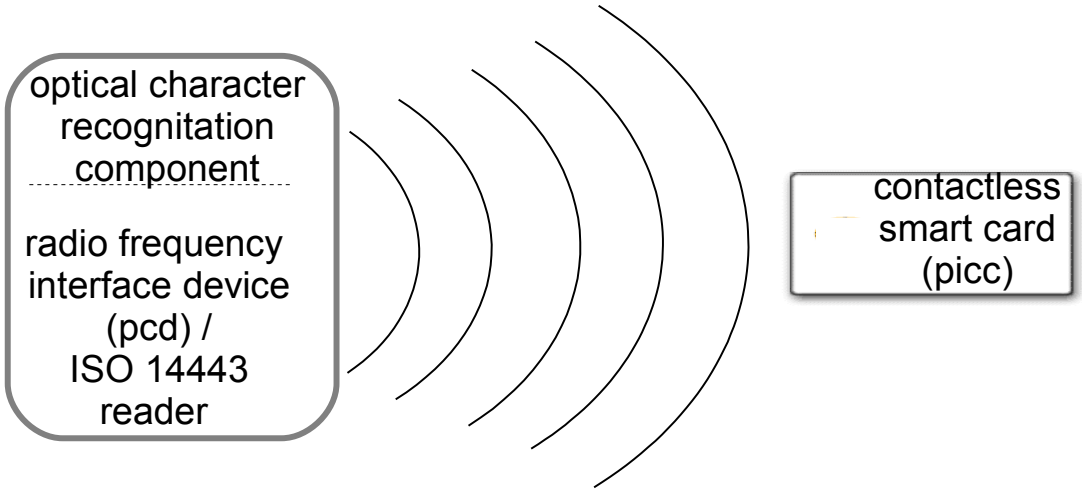
- RFID tags usually send out their serial number in plaintext
  - Attackers can clone tags at will
  - Attackers can track and monitor
  - Threat to authenticity and privacy
- Security mechanism: elliptic curve asymmetric cryptography
  - Total power consumption for one id: 9.1 µW
  - True random number generator based on Galois Ring Oscillators

Federal Office
for Information Security

Technological Trends: Mobile Cryptographic Smartcard-Reader

DRAFT

Bundesamt
für Sicherheit in der
Informationstechnik

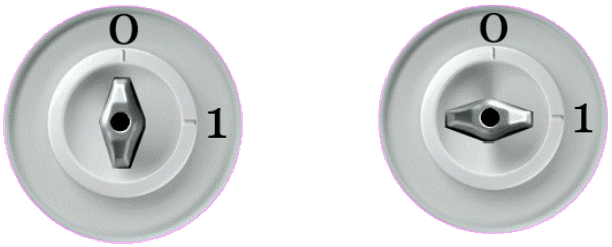


- Presentation of two password based protocols for secure connection establishment between contactless smart card and terminal
  - Forward secrecy of the session keys
  - Security against off-line disctionary attacks

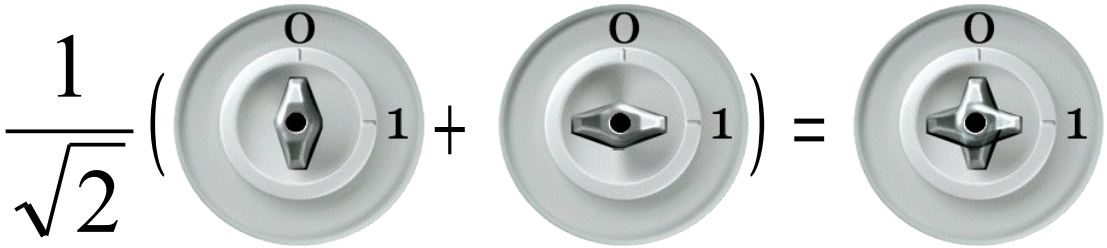
Technological Trends: Quantum Information Technology

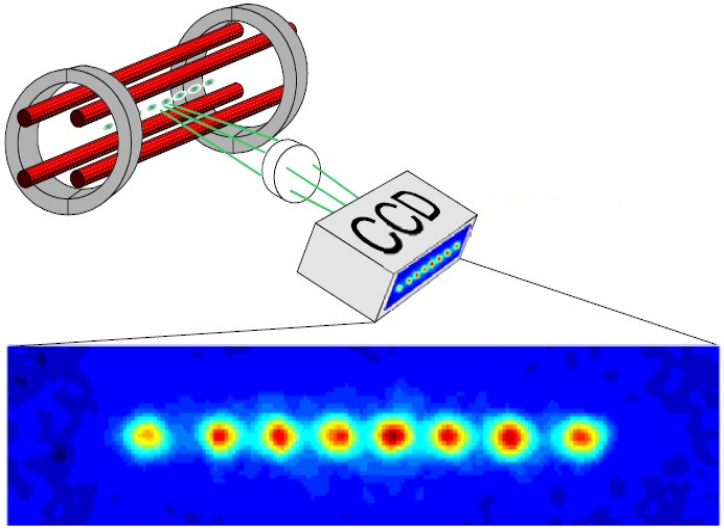
DRAFT

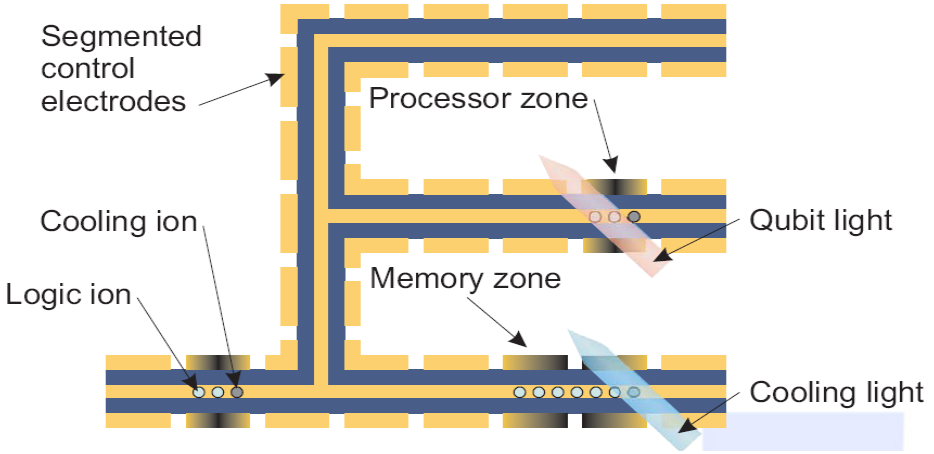
Classical Bits



Quantum Qubits







Quantum Computing

Security Measures

DRAFT

- today: mostly acting reactive
  - security vulnerabilities -> updates / patches
  - new viruses -> update virus scanner
  - new trojan horses -> new patches
- tomorrow: increased prevention by

sustainable IT-Security Research

Security Measures – New Technologies

- Sustainable measures
  - long term security -> quantum cryptography, fading channels
  - Classical cryptography -> research into crypto-analysis algorithms on adiabatic quantum computers
  - Perimeter security -> wireless sensor nets for mobile perimeter security, systematic research of “side channels” (even a general definition is lacking presently)

BSI IT-Security-Research

DRAFT

1. Internet Early Warning Systems
   - prevention strategies to protect against new attacks
   - early warning via new sensor data collection and analysis
   - extension of the BSI IT Early Warning System
     - implementation and evaluation of new types of sensors and components
     - investigation of technical, organisational and legal implications
2. Trusted Computing
   - self-protecting IT systems
   - highly secure embedded processor platforms

DRAFT

3. Biometrics and ID-Cards
   - livefinger detection
   - innovative security token platform
   - security architecture for micro sensor networks
4. Quantum computer resistant cryptographic mechanisms and security technologies
   - selection and investigation of quantum computer resistant cryptographic algorithms, including security implementations and prototypical applications
   - quantum cryptography: practical realisation and system security aspects
     - resistance against side-channel and fault attacks
   - (medium-term) security of / security with classical cryptographic mechanisms
   - application areas: encryption, electronic signatures, authentication, data integrity

Federal Office
for Information Security

„Culture of Cyber Security“ in the Scientific Community

DRAFT

Security community	Academic research community
1. The attacker will tend to exploit the simplest vulnerability	... not the academically most interesting or challenging topics
2. Completeness must be achieved...	... special cases suffice most of the time.
3. All ideas / terms / facts must be explicitely, rigorously stated...	... facts “known in the community” can be assumed.
4. Parts of a model not reliably describable must be excluded...	... such parts must be ignored for now.

attacking security problems with a purely „academic research“ approach results in systems

1. easy to break
2. in various ways
3. with design errors due to misunderstandings
4. and lack of knowledge

„Culture of Research“: applied, „pseudoapplied“ and fundamental

DRAFT

- „Practical problems“ are useful
  - interesting science is often done as a response to a practical challenges. The ivory tower is not necessarily the most productive work place (Peter Galison).
  - proposal: build a physical system that withstands real attackers

- „Pseudopractical problems“ are practical problems
  - that must not / cannot be solved within the “foreseeable” (say, within 5-10 years) future.
  - proposal: build a physical system that is “provably secure“
    build a large scale quantum computer.
  - Usefulness if pseudoapplied problems is questionable because it is difficult to find common criteria for success.

„Culture of Research“: applied, „pseudoapplied“ and fundamental

DRAFT

- Fundamental question

  typically addressing the „axioms“ of a research field.

  - No-cloning theorem – *doubting unitary evolution*
    - Is the Schrödinger equation *strictly* correct? Nonlinear additions (S.Weinberg 1989, and many others)
    - Might gravity remain classical and introduce non-linearities? (D. Page 1982, in context of quantum cryptography, Plaga 2006)
    - If yes: cloning becomes possible – quantum cryptography dead bur mind boggling consequences

  - Quantum computer – spontaneous wave-function collapse
    - If components of total state vanish above certain scale / mass
    - --> Loss of coherence in large structures unavoidable
    - Large scale quantum computers could not be built

„Culture of quantum information“: field is current strongly driven by „pseudoapplied“ problems...

DRAFT

- For „large quantum computers“ this can hardly be replaced by „practical“ problems
- Proposal: introduce fundamental questions as a stronger driver
- E.g.: Build a system that tests validity of superposition principle on as „large“ scales as possible.
- Need for further research: introduce abstract model to concisely define „large“ (might include mass and size in nontriviral ways).
- Test could have two results: an explicit collapse of the wavefunction (=trip to Stockholm, increased security of classical cryptography) or continued large scale quantum coherence (concrete step toward quantum computer)

Federal Office
for Information Security

Contact

DRAFT

Dr. Udo Helmbrecht
udo.helmbrecht@bsi.bund.de

Dr. Rainer Plaga
rainer.plaga @bsi.bund.de

Godesberger Allee 185-189
D-53175 Bonn
www.bsi.bund.de