"About ICT Security and Safety in the Banking Industry"

Dr. Klaus Brunnstein
Professor emeritus for Applications of Informatics
Department of Informatics, University of Hamburg

24th IFIP International Information Security Conference (IFIP SEC-2009), Pafos/Cyprus

Part I: Appreciation of Kristian Beckman Award

Part II: A Holistic Security and Safety Risk Analysis with special View at the Banking Industry

II.1 Security Risk Analysis of Banking Industry IT

II.2 The Financial Crisis: Safety Risk Analysis of Financial Processes

Part III: Outlook: Towards sustainable IT Applications

Part I: Appreciation of TC-11s
Kristian Beckman Award

I.0 Thanking for Kristian Beckman Award

I.1 Working with TC-11

I.2 Hamburg IT Security curriculum

I.3 Security AND Safety: a holistic approach

I.1.1 Working with TC-11

- First IFIP Technical Committee to deal with Data Protection was IFIP TC-9 „Social Implications“ (1980), with WG 9.2 „Social Responsibility“ being established by Louise Yngström, Richard Sizer, Jacques Berleur and KB (founding chair). Special focus: privacy, ethics. IFIP TC-11 „Security“ founded in 1983.

  - Background #1: Informatics at Hamburg university combined, from its start in 1972, technical methods and social implications of IT. Consequently, Data Protection were regarded both from their technical and legal sides.
  - Background #2: starting in 1987, the number of Computer Viruses and consequently the threat to professional IT rapidly increased. In parallel to the start of several IT Security companies, a curriculum on IT Security (2 years/4 semesters) started in Hamburg university, with „Virus Test Center“ as student and research project.

I.1.2 Working with TC-11

- IFIP TC-11 established1983. Founding chair: Kristian Beckman.
- IFIP General Assembly 1989 in San Francisco: TC-11 chair Bill Caelli and TC-9 chair (KB) submit a resolution that implementing and distributing Computer Viruses should be (legally) banned (IFIP Ban of Computer Viruses).

  Regrettably, nobody took notice that developping malicious code is a real danger for information processing, whether in enterprises, public organisations or in private use. Even (at least) one university (Calgary) openly offered a „course on virus writing“.

I.1.3 Contributions to TC-11 SEC Conferences

- 6th SEC-1990, Helsinki, May 1990:

  Klaus Brunnstein, Simone Fischer-Hübner:

  "Risk Analysis of 'Trusted' Computer Sytems„

  Session chaired by Harold Highland

  Remark: close cooperation with HAROLD on Malware!

  Content: critical analysis of the concept of Trust,

  and analysis of IT Security Criteria from Spectral Series (Orange/Red books) to European ITSec.

- 7th SEC-1991, Brighton, May 1991:

  Klaus Brunnstein, Simone Fischer-Hübner,

  Morton Swimmer, "Concepts of an Expert System for Virus Detection"

I.1.4 Contributions to TC-11 SEC Conferences

- 13th SEC-1997, Copenhagen, May 1997:
  - Klaus Brunnstein (Keynote): „Towards a holistic view of security and safety of enterprise information and communication technologies: adapting to a changing paradigm.“
  - Klaus Brunnstein: Analysis of Java security and hostile applets.
- TC-11 workshop at IFIP World Computer Congress 2006 in Santiago de Chile: „The Vulnerability of the Information Society“
- Finally: this presentation at 24th SEC-2009 in Pafos.

I.2.1 Hamburg IT Security Curriculum

4-semester/2 year course „Introduction to IT Security“

- Definitions and Concepts of IT Security
- Legal Aspects: Data Protection,Computer Crime Laws,
- Intellectual Property
- Theoretical Models, Security Criteria
- Cryptography
- System and Network Security,
- Database Security,
- Attacks on Computers and Networks,
- Computer Incident Analysis
- Digital Forensics

Student and Research Labs: Virus Test Center (VTC): est.1987,
Biometry Lab, Network Test Center

Support of (cooperation) in EU/Erasmus project on „IT Security Curriculum“, lead by Sokratis Katsikas + Dimitris Gritzalis (Athens).

I.2.2 ITSecurity work in Hamburg university:

Total: between 1987 and 2004 (when, after official retirement, a new professor took over, until 2007)

- 1000 students, over 100 diplom and bachelor theses
- doctor theses on Privacy (Simone Fischer-Hübner), Incident Response Organisation (Klaus-P. Kossakowski, establishment of DFN CERT, blueprint for several CERTs in Germany)

More themes: Electronic Commerce Security, Methodology of Computer Viruses Detection, Methodology of Computer Emergency Handling, ATM Firewalls, Paradigms of Informatics, Methodology of Flight Incident Analysis, et al.

I.3.1Security+Safety:a holistic approach

In an „Information“ (aka „Knowledge“) society, generation of values depends

a) on the safety (e.g. quality) of processes which generate values, and

b) on the security (e.g. resistance against attacks) of the systems, in which value-generating processes operate.

Reference: Contribution to SEC-1997.

I.3.1 Reference #1:

Towards a Holistic View of Security and Safety of Enterprise Information & Communication Technologies:

Adapting to Changing Paradigmata

Klaus Brunnstein

SEC 97: Copenhagen, May 16, 1997

I.3.1 Reference #2:

Towards a Holistic View of Security and Safety ...

2.1: Status of "Information Processing Quality"

* **Thesis #1**:
  - Present trends in development of Information Communication Technologies will yield **less reliable, less secure and and less controlable systems**.
  - Following traditional patterns, the methodological basis of related fields is divided into **non-interacting subfields, both** in education and scientific organisation:
    - Security (e.g. IFIP TC-11)
    - Safety and Dependability (e.g. IFIP TC-7)
    - User-Machine Interaction (e.g. IFIP TC-13)
    - Legal Aspects, Implications (e.g. IFIP TC-9)
  - A **unified (="holistic") view** is needed to overcome the division of methods.

I.3.1 Reference #3:

Towards a Holistic View of Security and Safety ...

3.1 The Traditional Paradigm: “Security”

---

* **"Traditional" Security Requirements:**
  - **Confidentiality**: I&A, Audit, Covert channels; encryption etc (TCSEC/ITSEC)
  - **Trustworthiness**: partially proven correctness (TCSEC); trusted path, trusted partnership (signature)
  - **Integrity**: Label integrity (TCSEC), avoidance of integrity attacks (virii, worms etc)
  - Communication/Network Confidentiality (TNI)
  - Data Base Confidentality (TDBI)
  - Communication/Network Integrity (ITSEC)

I.3.1 Reference #4:

Towards a Holistic View of Security and Safety ...

4.1 New Dimensions of Protection: "Safety"

* **Foundation of "Safety"**
* **Highly Sensitive Systems requiring High Degree of Guaranteed Functionality:**
  - **Examples**: Real-Time Control in Traffic (e.g. EFCS), Energy Production/Distribution (Nuclear Power), Chemical Production, Industry Robots, etc
  - **High Awareness of Risks**
  - **Professional** (less Research oriented) **Methods of Specification, Implementation and Quality Assurance**, often semi/formal, improved documentation

I.3.1 Reference #5:

Towards a Holistic View of Security and Safety ...

4.2 New Dimensions of Protection: “Safety”

* **"Holistic" Security/Safety Requirements for IT/Networking dependent Enterprises:**
  - Traditional Security
  + **Availability** of System and Network Services
  + **Reliability** of System and Network Services
  + **Maintainability** of Systems and Networks
  + **Functional Behaviour** of Systems and Networks: "Services provably behave as specified or required"
  + **Integrity** of Programs, Data and Structure (ITSEC)
  + **Correctness** of Objects + Structures (time, content)
  + **Consistency and Persistency** of Objects

I.3.1 Reference #6:

Towards a Holistic View of Security and Safety ...

4.4 New Dimensions of Protection: “Safety”

* **Why Safety is NOT enough:**
  - Safety is **Technical Feature**, derived from Specification, Design, Implementation of a Product
  - **User Aspects** (if regarded in Design) are **not always foreseeable**, esp. in changing environments
  - **Adaptations** to changes in enterprise organisation requires **custom-tailored concepts**
  - In life-cyclces of IT products, many **adaptations** (e.g. during installation, updating or emergency handling) **depend upon Human Minds**
  - Successful ICT usage requires **User Awareness**!

I.3.1 Reference #7:

Towards a Holistic View of Security and Safety ...

4.5 Another Dimension of Protection: “Sikerhet”

* **More Holistic Requirements for IT/Networking dependent Enterprises:**
  - – Traditional Security (see 3.1)
  - – Safety (see 4.1-4.4)
  - + **ITN Security and Safety Policy Development**
    - Development of an ITN Security+Safety (S+S) Policy
    - Implementation and Enforcement of an ITN S+S Policy
    - Analysis of Failures, and Update of ITN S+S Policy
  - + **Assessement of Residual Risk**
  - + **Recovery Methods if Residual Risk Materializes**
  - + **User/Usee Awareness**

I.3.1 Reference #8:

Towards a Holistic View of Security and Safety ...

4.6 Another Dimension of Protection: "Sikerhet"

Sikerhet = Security + Safety + Adaptation

Webster (1997): "security"/"safety overlap

- "**safety**: 1: the state of being safe: security ..."
- "**safe:** 1: free from harm or risk: unhurt ..."
- "**security**: 1 the quality or state of being secure..."
- "**secure**: 1:easy in mind: confident ... 2b free from risk or loss ..."

– Scandinavian + German: 1 term/holistic meaning:

- Sikkerhed (Dansk/Denish, Norsk/Norwegian)
- Saekerhet (Svensk)
- Zekerheid (Dutch, Flemish), Veiligheid (Dutch)
- Sicherheit (Tysk/German/Swedish)

II.0 A Holistic Security+Safety Risk Analysis with special View at the Banking Industry

II.0 Holistic Requirements applied

II.1 Security Risk Analysis of Banking Industry IT

- .1 Customer IT Security
- .2 Bank (InHouse/Outsourced) IT Security
- .3 Bank-Customer Communication Channels
- .4 Case study: A Criminal/Professional e-Bank Attack

II.2 The Financial Crisis: Safety Risk Analysis of Financial Processes

II.0.1 Holistic Requirements applied

The Security Dimension:

Confidentiality, Integrity, Trustworthiness

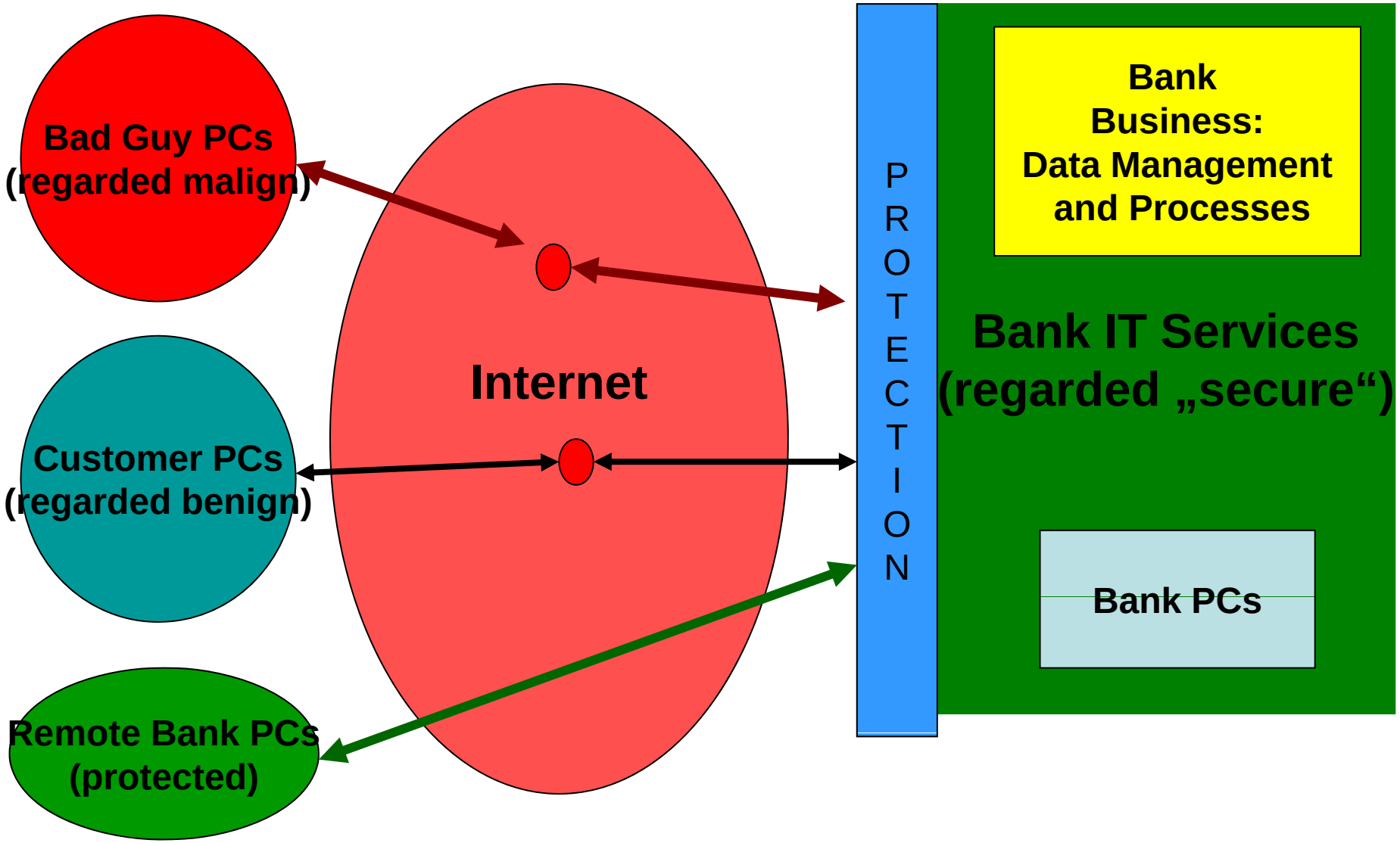
The Safety Dimension:

Availability, Reliability and Maintainability Services
Functional Behaviour of Systems and Networks
Integrity of Programs, Data and Structure
Correctness of Objects + Structures (time, content)
Consistency and Persistency of Objects

The Policy and Usability Dimension:

Security and Safety Policy Development and Enforcement
Assessement of Residual Risk
Recovery Methods if Residual Risk Materializes
User/Usee Awareness

II.0.2 A Holistic Model of Bank Operations: Communication Channels



II.1.1 Banking Industry: Customer IT Security

.1 Customer IT Security:

- Banks assume (enforce) that customers are responsible
- BUT: banks decide about IT services/no choice of c.

- Indeed: customer PCs are major risk:

  Weak Systems/Software (BO), Trojan Horses,

  Phishing/Pharming, Botnets (capturing customer PCs)

  - Good news: „viruses“ and „worms“ no longer a threat
  - BUT viruses/worms are risks on mobile devices, esp. under Symbian: presently „SymbOS/HatiHati worm“

- Attemps of banks to improve customer security by offering „secure communication devices“ (e.g. HBCI) failed!

II.1.2 Banking Industry: Bank IT Security

.2 Bank (InHouse/Outsourced) IT Security:

- **InHouse IT services (main servers):**
  - **Bank IT Security Policy can be enforced DIRECTLY**
  - **Main servers: good availability, backup plans**
  - **Risks: DoS/DDoS, cross-site scripting, code injection**
  - **Servers for special tasks: administration-intense**

- **Distributed PCs: high risks of „creative“ users endangering proper operation**
  - **No solution: user surveillance (Data Protection)**
  - **Solution: system operations (incl. update) not permitted, limitation of user privileges.**

- **Outsourced IT Services:**
  - **Security depends upon partner, contract and possibility to enforce in case of an incident**
  - **Often, problems upon updating systems & software**

- **esp. „Cloud“ Services:**

  Outsourcing without knowing the location → no solid legal basis

II.1.3 Banking Industry: Bank Security

.3 Security of Customer-Bank Channels:

Content reliably encrypted → Secure transmission

BUT: users then regard messages (that is: CONTENT) as „secure“, and they hardly understand that an encrypted message from a trojanised system is INSECURE, as a PHISHING or PHARMING message also opens an INSECURE CHANNEL to another site.

.4 Case study: A Criminal/Professional Attack on an e-Bank:

This (ongoing) attack on a large, globally operating bank via an extensive botnet was presented in a conference for IT executives. The following short description is deliberately anonymized and simplified to demonstrate the principle; from the excellent presentation, I just copy one (the next) picture ☺

II.1.4a Picture/Courtesy from an IT Executive of „BANK“

II.1.4b Banking Industry: Case of BANK Attack

At Login to e-banking (online attack)

- Local Trojan notifies remote attacker with client contract number
- Attacker provides Trojan with 'input number' requested from BANK
- Trojan visualizes 'input number' to client in a perfectly manipulated login page
- Trojan collects and forwards 'secure client code' to attacker
- Attacker misuses 'secure client code' to correctly open 'secure session' with BANK
- Attacker misuses session to place money transfer order to selected intermediary

II.1.4c Banking Industry: Case of BANK Attack

What then happens:

- Access to login page is intercepted and routed to the hacker via the drop zone
- The hacker presents authentic looking login pages to the client
- Fake challenge and response pages are provided via the drop zone and admin page, letting the hacker login directly to the real bank
- After a successful login, the hacker gives the client a "System Down" page

After Logout:

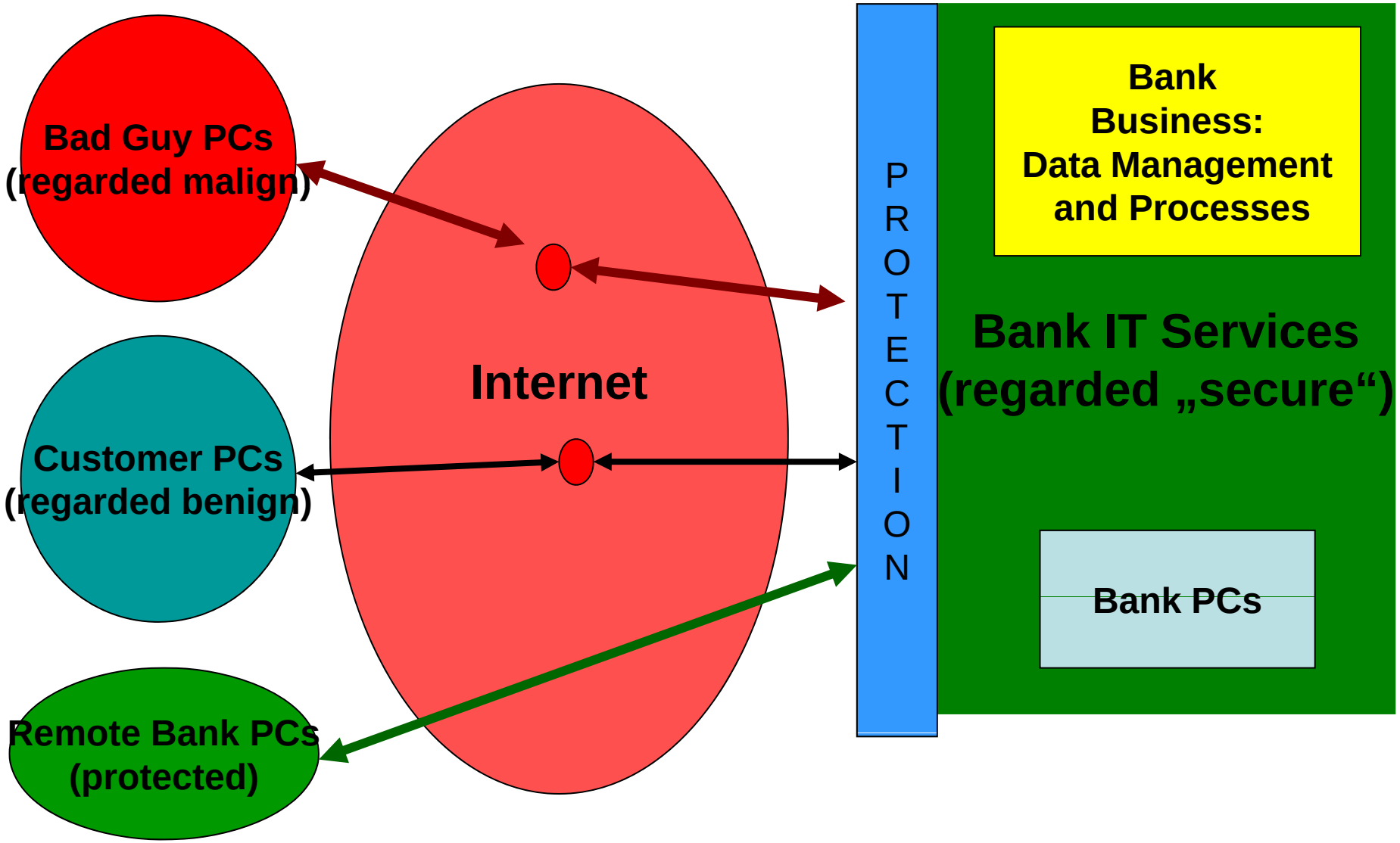
- Attacker notifies intermediary to urgently forward cash via money transfer service

II.1.4d Banking Industry: Case of a Bank Attack

Lesson learnt:

- **Even improved online authentication of the users with token based schemes and encryption do not prevent from being successfully hacked.**
- **Botnets cannot be efficiently stopped at this point in time and even not mid-term (seems to become a fact of life)**
- **Client PCs remain inherently insecure what ever accurate virus protection might be installed => think of boot record infections!**
- **Only a minority of servers could have been shut-down with the support of the ISPs and/or local Law Enforcement Agencies**
- **For certain jurisdiction, it is deemed impossible to get the attackers arrested even though their identity might be revealed**
- **Strong authentication of users is not strong enough to prevent highly sophisticated hacking attacks**
- **Banks are set to go beyond encryption and strong authentication**

II.2 The Financial Crisis: Safety Risk Analysis of Financial (=Bank Business) Processes



II.2.1 Safety Requirements for Bank Processes

Safety of Bank Business Processes and Databases:

- ✓ **Customer Account Mgt, Credit Mgt, Values and Investment Mgt: reliability, integrity, consistency, persistency, trustworthiness, AND Residual Risk Assessment: OK!**

- **Packaging different assets and values to complex products:**
  - **Gigantic Losses (order of 5 billion Euros)**
  - **No Knowledge/Data-Base where/what/how much**
  - **No Risk Analysis, No Survey of Assets,**
  - **No Consistency,**
  - **No Residual Risk Analysis→No Trustworthiness**

III.1 Towards sustainable IT Applications

First, (Bank) IT Applications must reside in a secure environment, where criminal attacks can be contained: → Built-in Security required!

Second, (Bank) IT Applications must assure safety criteria, esp. availability, reliability, maintainability of System and Network Services, Functional Behaviour of Systems and Networks, "Services provably behave as specified or Correctness, Consistency and Persistency of Objects

Finally, an adequate Security and Safety Policy, Residual Risk Assessment, Contingency Plans and awareness of Users and Usees are required.

I.3.1 Reference 10:
III.2 Towards a Holistic View of Security and Safety

---

* **Thesis #2: Developping ICT "Sikerhet"**
- 2.1 Assessing "Sikerhet" is the User`s task!
- 2.2 In a **mature Information Society**, product quality shall match user requirements:
  - 2.1 Users specify details of Sikerhet they require
  - 2.2 Manufacturers specify product features
  - 2.3 If user requirements match product specifications, manufacturers (legally) guarantee

PS: Final comment (relating to historical analogy with Industrial Society)

When will **"Virtual Nader"** appear?

Pessimistic Answer: 1939 (Zuse Z1) +80 years = 2019