Total Information Governance

Trading Old Risks for New Ones?

Andreas U. Schmidt
Fraunhofer Institute for Secure Information Technology SIT, Darmstadt, Germany
A lot of work on conceptual levels has been done and supporting technology is there.

**Thesis of this talk:** Some fundamental issues of information security, i.e., Confidentiality, Integrity and Availability, are either overlooked or tacitly assumed. Though these are problems in the small, they pose considerable risk, as the weakest link determines overall security.

A few inventions, designing IC&T (security) keeping the information value of data in mind, can resolve many of these issues in a cost-efficient way.
Some (anecdotic) ‘evidence’

- Jan 2008: Incident at Société Générale
  - Broker J. Kervier manipulated DAX futures and sunk 7.2bn US$
  - Direct cause was insufficient separation of duties, perhaps due to lack of human resources, and
  - Password-based AC
  - More governance, finer granularity of access control?
  - ITSec: The issue is rather the lack of personal identification in authentication

- Mid 2007: A B2C contract was disputed in a German court
  - VoIP recording was used successfully as evidence
  - Call recorded by the call-centre using proprietary systems (Cisco)
  - The call was leaked on the Web afterwards – making the customer look stupid

- 2007: In a patent litigation, e-mail was excluded as evidence
  - Bcc to legal counsel triggers CP rule of professional secrecy
  - As the e-mail was archived by the stakeholder – is that Bcc authentic?

Maybe not universally valid examples, but the general problem is probative force and integrity of information kept in self-interest
The Commonplace Panacea: Electronic Signatures

- **Fundamental issues**
  - **Long-term probative force** of signed information
    - Signatures ‘wear out’ – algorithm strength, key length, ... Practical solutions by re-signing, time-stamps and hash-trees
  - Data formats become obsolete, migration breaks signatures – Means for legally secure transformations are needed
  - What You See Is What You Sign (?)
  - Trust in signing systems

- **Application-level issues**
  - Enable **scaled application of digital signatures**
    - According to varying IG & security requirements apply anything from digest values over simple digital signatures with or w/o PKI, up to qualified electronic signatures
  - Enable **convergence**
    - Find analogues for electronic signatures for other media than documents (VoIP, multi-media)
    - Integrate signature-based information security (document-centric) with communication security
Document „Transformations“ in Workflows
TransiDoc – Establishing ‘Seals’ for Transformations

A transformation seal guarantees the properties of a ,legally secure‘ transformation. It enables

- Ex-post assessment of the transformation process
- That contents remain the same resp. Are changed just as desired
- Assignment to a responsible (transforming) entity, e.g. a scanner or a notary by digital/electronic signature
- Usage of the target document as evidence in place of, and without, the original one

TransiDoc is ultimately a collection of structured XML schemata, which allow profiling for any application domain

The seal refers to

- Converted content
- Transformation report
- Transformation notice, e.g. notarisation
TransiDoc Application – Patient Records

Transformierte Erst-Dokumentation-Brustkrebs

Das konvertierte Dokument

AOK Rheinland/SVA

Meier
Katarina

Ottostr. 4
50859 Köln

4212505 12345678 1334 1

2780123 12.07 05.12.06

Le Medicina
Dr. med. Paul
Am Plützberg 1
69019 Heidelberg
TransiDoc Application – Authorised Translations

- Source & target bound by seal & staple
- Description of handwritten signatures
- Translator’s notice
- Translator’s signature and seal
Edisons “Voice Recording Machine”, patented 1905-1911 suggests the subject has a long history
VoIP Security

- Basic issues are tackled
  - Protocols like SRTP can provide end-to-end security to phone calls, making them independent from the security of the transport medium. SPIT and DoS are future threats
  - Spam over Internet Telephony (SPIT) considered a major threat – approaches are Gatekeepers, CAPTCHAs, IDS, …
  - ITU Recommendations for Secure Telecommunications

- „Application-level security?“
  - Verbal communication is traditionally bestowed with a high level of trustworthiness
  - Is the integrity of VoIP communication as high as the inter-personal character of conversations suggests?
  - Recent court cases suggest there might be a problem

- Goal: Non-repudiation of conversations by caller and callee, for speech over packet-oriented, digital channels, and in particular for VoIP conversations
  - Providing tenable evidence of
  - Contents of a call
  - Identity of caller and callee
  - Ancillary information (forensic), time & date, …

- For electronic documents, this is usually done by electronic signatures
VoIPS Core Technology

- Electronic signatures over packet-oriented, time-based data streams

- Methods
  - Separation into intervals consisting of an adjustable number of packets
  - Chaining by hash values
  - Securing by digital signatures
  - Accommodating for packet loss by specific protocols
  - Temporal context by time stamps

- Properties
  - Signature is formed during call
  - bi-directional, time-based nature of communication is taken into account
  - time-sequence is secured
  - “What is Heard is What is Signed”

VoIPS is patented
Application: Self-signed VoIP Archive

Separation of duties between long-term archive and security module that secures and signs archived calls.

Trusted time source or time-stamping authority to securely pinpoint exact start of call.

Time-stamping service for long-term security.

VSec can be a passive listener or have an active role and enforce policies.

Only one point in channel A ↔ B needs to be digital and packet-based.

Main Benefit: high accountability by separation of duties and resulting administrator security.

Complete audit trail for digital voice communication.

Plan: show a prototype of integrated e-mail and VoIP archive with partners.
Trust is chained (more often than not)

- How do partners put trust in each other in application scenarios?
- Through technical systems!

- Those need to be trusted as well
- Chains of trust become increasingly long and complex

Transitive trust:
Attest a systems trustworthiness to a third party over multiple hops

Attestation:
Provide authentic information about a system’s state to a verifier
Attestation and Trust

- American Heritage Dictionary says:
  - **Attestation**: “To affirm to be true, correct or genuine”

- For trusted platforms:
  - Cryptographic proof of information regarding the platform

- Information that could be attested to includes:
  - HW on platform
  - BIOS
  - Configuration options
  - And much more

- Trusted Computing provides a **hardware trust anchor**

- and surrounding technology and infrastructure standards

**Trust**

- An entity can be trusted if it always behaves in the expected manner for the intended purpose

**Trusted Computing**

- Basically a reporting technology to testify the state of a certain system to and optionally its identity to an external verifier
Many components are involved in trust chains in complex, open systems.
TC – IG related Use Cases

- Securing data storage and archives to comply with data protection
- Attesting to systems’ states while handling information in workflows, e.g.
- Attested transformations, scanners, printers
- Secure communication
- Securing signature terminals
- ...

...
Some commonplace prejudice

- Scientists are whining about reporting duties
- Management is ignorant toward their ideas, and shows this by ever more detailed approval processes
- Reaffirming what management always knew: these guys are too lazy to do real work

This might be just due to

- Learning curve, awareness
- Improper or incomplete IG system deployment
- Or other euphemisms for “getting used to it”

But anecdotic evidence* suggests

- Systematic reasons for conflict between IG/CG and innovation
- Introducing friction in innovation processes
- Simple alignment of innovation processes with IG might not work
- Undermining the claim of CG to manage risk – in contrast to avoiding it

* Partner unable to get LoI approved in time for project proposal, since he could not obtain all required information
Innovation and Information Economy

- Pfizer’s Incubator project
  - Innovation park, funded with $50M over 5 years
  - Investment in start-ups
  - Looks like outsourcing, but
  - Projects without a concrete drug in the pipeline
  - Basic research with high risk which fails to attract conventional venture capital
  - Streamlined approval process – no business plans
  - Incubator is run independently from mother company

- What Incubator does, phrased differently in terms of
  - **Industrial Organisation**: Vertical disintegration externalises innovation process and associated risk
  - **IG**: Reduces internal requirements
  - **Information Security**: implements a minimal need to know principle by separation of duties
  - **Information Economy**: Removes information asymmetry, by simplifying contractual situation
    - Mitigates moral hazard

- **Information Economy** should provide more insight into the impact of IG
Copyright notice and disclaimer

The material contained is for educational purpose only. All cited trademarks, images, and texts are property of their respective holders.

This on-line material is being provided in the interest of rapid dissemination of information of research work. Some or all of the material here may be covered by copyright owned by the respective authors. You may browse the material at your convenience as you would in a public library. Permission is also granted to make a hard copy for personal use without fee provided that the copied material clearly indicates the author and source of the material and any original copyright notations are unaltered on every portion of the referenced material. Retrieval, copy, or distribution of any material herein for profit or any commercial advantage may violate the copyright protection law of Germany and other countries and may require prior written permission of the copyright owners.

Specific sources for images and texts in this presentation are

- Bristol Primary Care Trust, Education Training Department: EDUCATION & TRAINING BULLETIN. JANUARY – JUNE 2008
- www.pfizer.com/
- gwydir.demon.co.uk/diaries/
- State of Texas, Department of Information Resources. Guidelines for the Management of Electronic Transactions and Signed Records
- Infineon
Backup slides
The TCG

- Formed 2003, now ~200 organisations, among them Fraunhofer SIT as academic liaison member
- Not-for-profit organization,
  - formed to develop, define and promote open, vendor-independent specifications for trusted computing and security technologies, including hardware building blocks and software interfaces, across multiple platforms, peripherals and devices
  - Efforts to ensure compliance and conformance of TPMs and trusted hardware
- [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org)
- And by the way: DRM is not on the agenda!
Working Groups

- **Mobile**
  - provides trust for mobile devices including mobile phones and PDAs

- **PC Client**
  - provides common functionality, interfaces and a set of security and privacy requirements for PC clients that use TCG components to establish their root of trust

- **Trusted Platform Module**
  - created the Trusted Platform Module (TPM) specification version 1.1b and 1.2. The TPM is the root of trust that is the basis of the work of the other TCG work groups.

- **Infrastructure**
  - defines architectural framework, interfaces and metadata necessary to bridge infrastructure gaps
Working Groups

- Hard Copy
  - defining open, vendor-neutral specifications for hardcopy devices that will use TCG components to establish their root of trust.

- Software Stack
  - provides a standard set of APIs for application vendors who wish to make use of the TPM.

- Server
  - provides definitions, specifications, guidelines and technical requirements as they pertain to the implementation of TCG technology in servers.

- Storage
  - is building upon existing TCG technologies and focusing on standards for security services on dedicated storage systems.

- Trusted Network Connect
  - focuses on ensuring endpoint compliance with integrity policies at and after network connection.