

Privacy Issues in Application Development

Gerald Quirchmayr

Professor, Head of Department, and Vice Dean
@
University of Vienna
Faculty of Computer Science
Department of Distributed and Multimedia Systems
Liebiggasse 4/3-4, 1010 Wien
Tel. +43-1-4277-39631 Fax +43-1-4277-39649
Gerald.Quirchmayr@univie.ac.at

Adjunct Professor
@
University of South Australia
Division of IT, Engineering and the Environment
School of Computer and Information Science
Mawson Lakes SA 5095
Tel. +61 8 8302 5114 Fax. +61 8 8302 3988
Gerald.Quirchmayr@unisa.edu.au

Institute of Distributed and Multimedia Systems







The screenshot shows the homepage of the University of Vienna. At the top, there is a navigation bar with links for UNIVERSITY, STUDIES, RESEARCH, ORGANISATION, and SERVICES. Below this is a large banner with the text "Welcome to the University of Vienna" and three images: a cityscape, a group of students in a lecture hall, and a modern building. To the right of the banner is a search bar and a language selector set to "Deutsch". Below the banner is a "Quicklinks" section with various links such as "Faculties and staff", "Library catalogue", and "Event calendar". A "News" section is also visible, featuring three articles: "Lecture by linguist and philosopher John R. Searle", "UB provides access to Elsevier Freedom Collection", and "Neurobiology Summer School Vienna in September". At the bottom right, there is a logo for "EURO 2008" and a large blue button with the text "www.univie.ac.at".



Welcome at the Faculty of Computer Science!

The website offers [news and information](#) about the faculty, its [institutes](#), [research labs](#), and [didactic centers](#), as well as [administrative information](#) and information about the [staff](#), [projects](#), [publications](#), and [courses](#).
The website is under permanent development to improve, and extend its features.

faculty

-  Projects
-  Teaching
-  People
-  Publications

3 Departments:

- Distributed and Multimedia Systems
- Knowledge and Business Engineering
- Scientific Computing

2 Specialized Research Labs

- Computational Technologies and Applications
- Educational Technologies

1 Didactic Center for Computer Science

www.cs.univie.ac.at

Personal research focus

- *Information Security Management*
 - *Secure processes.*
 - *Management of security risk.*
 - *Business continuity management.*
- *Legal Aspect of Information Security and technological solutions*
 - *(Privacy) Legislation.*
 - *Law enforcement (forensics) and court procedures.*
 - *Mobile equipment security and privacy.*



The continuously moving target

- **Traditional IT Security**

1. Threat Analysis
2. Organizational Policies
3. Intrusion Prevention



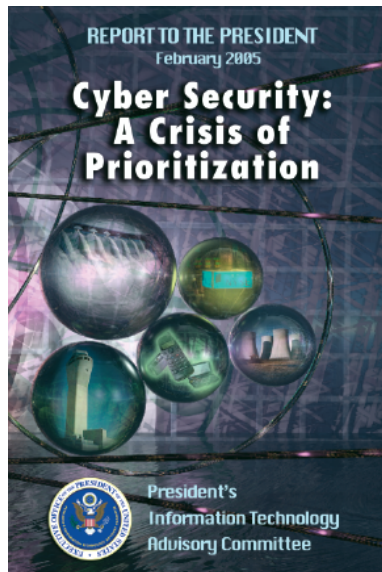
- **Changed situation**

1. Information Asset Centric Threat + Risk Analysis
2. Organizational Policies
3. Intrusion Prevention, Intrusion Detection, Survivability under Attack



The screenshot shows a Mozilla Firefox browser window displaying the website for the United Nations Office on Drugs and Crime (UNODC). The browser's address bar shows the URL <http://www.unodc.org/unodc/uncjin.html>. The website header includes the UNODC logo and navigation links such as Home, Site Map, Links, Contact Us, and Regional Websites. A search bar is visible, and the main content area is titled "United Nations Crime and Justice Information Network". The page contains a welcome message, a search bar, and a sidebar with various menu items like "News and Publications", "Drug Abuse & Demand Reduction", "Terrorism, Corruption & Human Trafficking", and "Treaty & Legal Affairs". There are also logos for "Britannica Internet Guide Award" and "Seal of Web Feet".

One of the Latest Cyber Security Reports ...



<http://www.nitrd.gov>

Fundamentally New Security Models, Methods Needed

The weakness of the perimeter defense strategy has become painfully clear.

An expanded portfolio of Federal cyber security R&D efforts is required because today we simply do not know how to model, design, and build systems incorporating integral security attributes.

Ubiquitous interconnectivity is the primary conduit for exploiting vulnerabilities on a widespread basis.

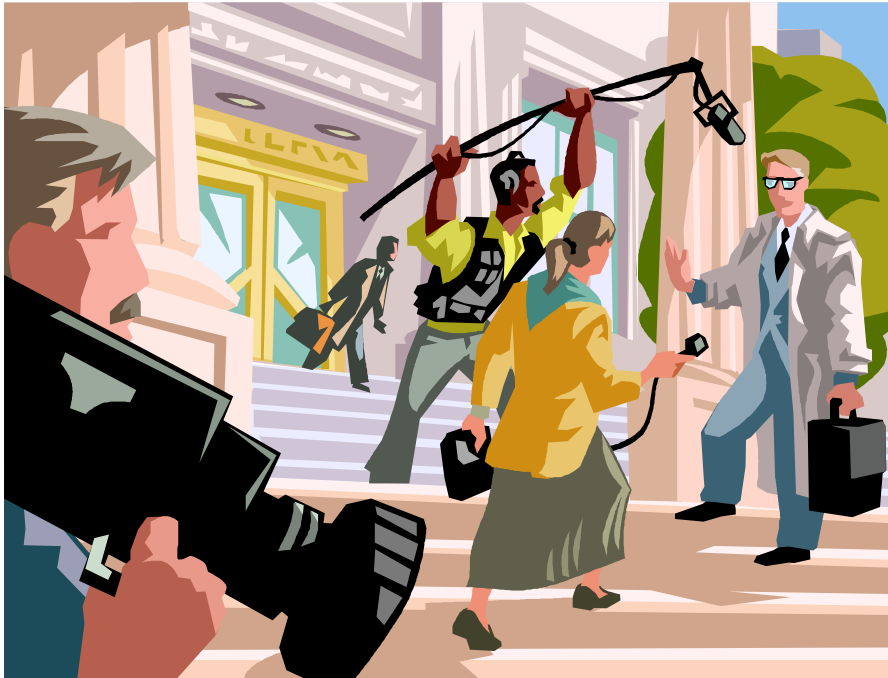
Classified cyber security research largely cannot be applied to the civilian cyber security marketplace.

Rule of law ?

- Where do we deal with relevant legal issues?
- Have we developed a culture in which it is normal to first do things and then investigate legal implications, i.e. When the damage has been done?
- How much risk are we as society prepared to take?
- Business first, technology second, ...
- **And what about legislation?**
- **The role of law enforcement?**
- **Law courts?**
- **International agreements?**



Waiting until a case hits the media (again)?



9 Oct-29-09

Gerald Quirchmayr, Institute of Distributed and Multimedia Systems



We are in deep trouble already ...

http://www.dswshoe.com/credit_card_faq.jsp

A screenshot of a Mozilla Firefox browser window displaying a DSW press release. The browser's address bar shows the URL 'http://www.dswshoe.com/credit_card_faq.jsp'. The page content includes the DSW logo and several sections of text. The first section is titled 'What information was stolen from DSW?' and describes the theft of approximately 1.4 million credit and debit cards. The second section is titled 'How long has DSW known about this problem?' and states that DSW was made aware of the problem just days before its initial March 8, 2005 press release. The third section is titled 'Why did it take until April 18 to announce the results of DSW's fraud investigation and provide a list of the stores?' and explains that DSW did not want to report further facts until a forensic investigation by Ubizen was concluded. The fourth section is titled 'If I provided information to DSW on its web site, was that stolen?' and states that information provided via the DSW web site was not involved in the theft. The fifth section is titled 'How can I find out if my information was stolen?' and states that DSW cannot advise customers who contact them as to whether their specific information was stolen. The browser's status bar at the bottom indicates 'Transferring data from www.dswshoe.com...'.

DSW - Press Releases - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

DSW

What information was stolen from DSW?

The numbers and the names associated with approximately 1.4 million credit and debit cards used at 108 of our stores primarily during a 90 day period between mid-November 2004 and mid-February 2005 were stolen from DSW. This involved debit cards used as credit cards only. No PIN numbers were in the stolen data. Also, no addresses or other information relating to the credit card or debit card customers were stolen.

In addition, checking account information was stolen for around 96,000 checks used to make purchases at these same stores. This included the bank account numbers located on checks that were provided to DSW (the "Magnetic Ink Character Recognition" or "MICR" numbers) and the drivers' license numbers provided when paying by check. However, the stolen MICR and driver's license numbers did NOT include the name, address or social security number of the customer.

How long has DSW known about this problem?

DSW was made aware of a possible problem just days before it issued its initial March 8, 2005 press release. Since that time DSW has been investigating and verifying basic facts about the data theft.

Why did it take until April 18 to announce the results of DSW's fraud investigation and provide a list of the stores?

DSW did not want to report any further facts until the forensic investigation by Ubizen, one of the nation's leading computer security firms, was concluded. Key facts about this data theft, including the number of stores affected, were not known and verified until Ubizen finished its investigation.

If I provided information to DSW on its web site, was that stolen?

Information provided via the DSW web site was not involved in the theft.

How can I find out if my information was stolen?

Due to the sensitivity of the information and the amount of information stolen, DSW cannot advise customers who contact us as to whether their specific information was stolen. However, if you shopped in one of the following stores between mid-November 2004 and mid-February 2005, and you used a credit card, debit card or check to pay

Transferring data from www.dswshoe.com...

10 Oct-29-09

Gerald Quirchmayr, Institute of Distributed and Multimedia Systems



- What information was stolen from DSW?
- The numbers and the names associated with approximately 1.4 million credit and debit cards used at 108 of our stores primarily during a 90 day period between mid-November 2004 and mid-February 2005 were stolen from DSW.
- In addition, checking account information was stolen for around 96,000 checks used to make purchases at these same stores. This included the bank account numbers located on checks that were provided to DSW (the "Magnetic Ink Character Recognition" or "MICR" numbers) and the drivers' license numbers provided when paying by check.

Possible legal implications

- Privacy violation.
- Liability issues.
 - System administration.
 - Technology supplier.
 - Management (-> SOX?).
- Financial damage.
 - DSW.
 - Credit card companies.
 - Individual credit card users.
- Reputation of the company.



More general implications

- Reputation of the whole retail sector.
- Public confidence ...
 - in the technology,
 - in credit cards and checks,
 - in the financial sector,
 - in ...
- Institutional responses.
 - Law enforcement.
 - Legislation.
 - Justice system.



And that against the background of diminishing trust ...

<http://www.boycottbenetton.com/>

A screenshot of a Mozilla Firefox browser window displaying the Boycott Benetton website. The browser title is "Boycott Benetton - No RFID tracking chips in clothing! - Mozilla Firefox". The website content includes a large "BOYCOTT BENETTON" header, a "SEND BENETTON A MESSAGE: DON'T BUY CLOTHING WITH TRACKING DEVICES!" section, and buttons for "press releases", "news articles", and "links". A central image shows a man's profile on the left and a woman sitting on the right with the text "I'd rather go naked." Below this is a "Benetton Meets CASPIAN Halfway!" section with a "Click here for details" link. The URL "http://www.boycottbenetton.com/" is visible in the address bar.

Event-driven, purely reactive legislation cannot be the only solution we are able to come up with ...

- RFID-specific legislation discussed in California.
- A purely reactive mode is not good enough.
- Once the damage is done, we can at best clean up.
- Shift in focus from reaction, investigation and punishment to a proactive approach.



Bad Allies: Ignorance, Panic, Nationalistic Pride

- *Ignorance*: Let's give it a try (Bentton et al.) without first thinking about the possible consequences, i.e. overreactions from the public and legislators.
- *Panic Mode*: Immature, sometimes grossly exaggerated approaches accompanied by patchy legislation and threats, often resulting in the waste of huge amounts of money and occasionally also in unnecessary conflict (exchange of airline passenger data) straining and damaging relationships with core partners.
- *Nationalistic Pride*: This of course cannot happen to us; even trying to deny it after it happened (first trying to blame the Madrid train attacks on ETA).

Loss of Trust

- “Enemy of the state syndrom“.
 - Fear of abuse of collected data.
- “Businesses spying on their customers“.
 - Increasing reluctance of consumers to provide any information.
- “Permanent monitoring“.
 - “Always on technology“ is already earning a bad name.
 - Tracking systems are increasingly rejected.
 - Workplace relations are being severely strained.
- Not knowing the law, not being aware of what existing legislation can prevent and how strict it sometimes is.

Theorem: Existing legislation can cope

- The core problem is not the existing legislation it is the enforcement of law.
- Perceived inappropriateness of legislation vs. the often very tough reality.
- Law can bite and when it does, it usually hurts a lot!
- Temporary proof through failed falsification attempts: DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995.

Article 2 - Definition of “Data“

- (a) 'personal data 'shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

This covers all personal data,
independent of the technology used!

Article 2 - Definition of “Processing of Personal Data “

- (b)'processing of personal data'('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

This covers all processing,
independent of the technology used!

So where is the problem with RFID tags?

- Are we sure that companies will stick to the legislation? Haven't we in the past seen too many incidents of the law being broken?
- Will they get away with it?
- Are crimes being prosecuted?
- Do the penalties hurt?

- Law is being enforced.
- The penalties are not negligible anymore.
- Negative publicity hurts even more than the possible penalties do.

There must be room for handling exceptional situations.

Article 13

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:
 - (a) national security;
 - (b) defence;
 - (c) public security;
 - (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
 - (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
 - (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
 - (g) the protection of the data subject or of the rights and freedoms of others.

Necessary changes in attitude.

- Privacy protection has to be taken seriously.
- Increasing the awareness of system designers, builders and operators.
- Giving the public back the confidence that legislation is sufficient and that it is being enforced.
- “Workarounds“ to undermine the legislation just don't work anymore.

Making the law sting like a ...



*"Many thanks to you all for the timely help. **Who said a WASP couldn't sting twice?**"*
(PM Winston Churchill, May 11th, 1942 on the successful delivery of 60 Spitfires to Malta)

Article 16 - Confidentiality of processing

- Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.



DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995

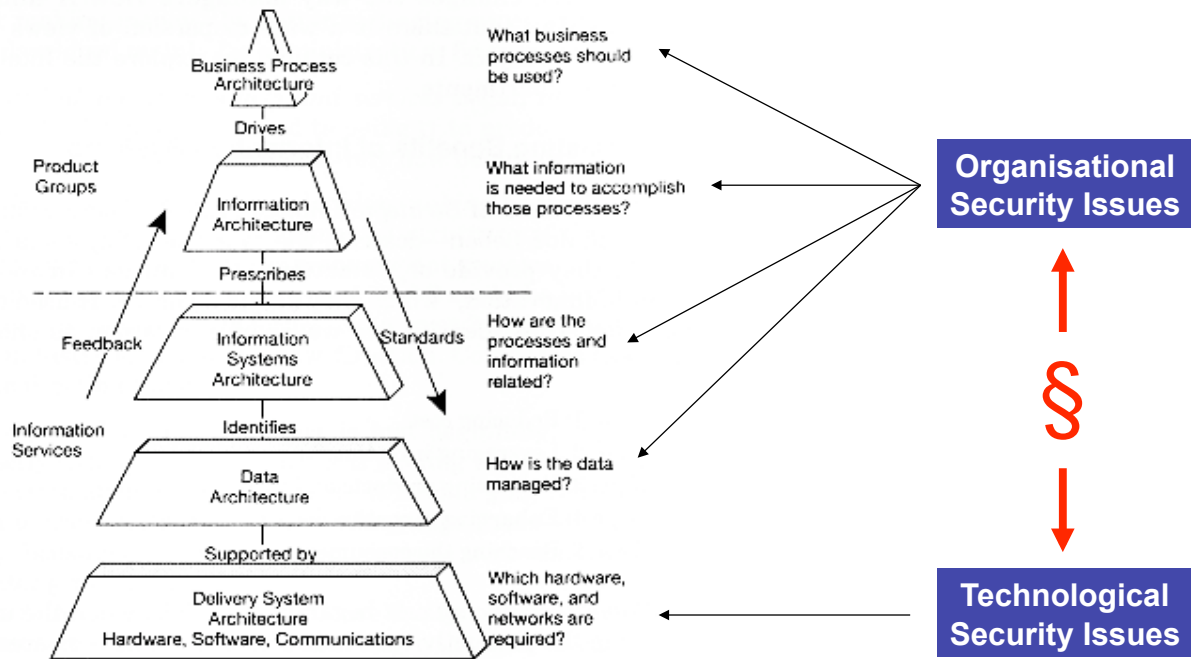
Article 17 - Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.



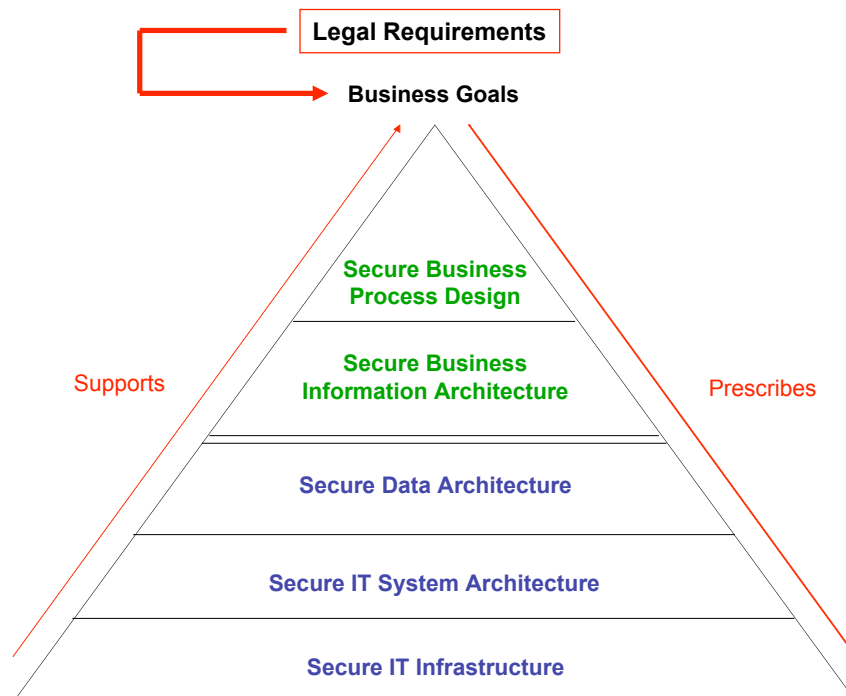
DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995

Where do we start to implement the legislation?



Barbara C. McNurlin (Editor), Ralph H. Sprague (Editor): Information Systems Management, 5th edition, Prentice Hall, Pearson Education 2002, ISBN 0-13-034073-1.

Making it work



Conclusion

- Technology, organisational concepts and legislation need to mutually support each other.
- Think about law and public opinion first before causing unnecessary and hardly repairable damage.
- At least as far as Europe is concerned, the legislative situation is not too bad.



Thank you very much