

Welcome to ISSE 2013

Norbert Pohlmann

Chairman: IT security association TeleTrust

Professor: Westphalian University of Applied Sciences

Director: Institute for Internet Security - if(is)

ISSE 2013 Programme



preliminary Conference Programme

Day 1 – Tuesday 22nd October 2013

09.00 – 10.00	Registration open, morning coffee				
10.00 – 11.30	Opening Introduction by Norbert Pohlmann, Chairman, TeleTrust & Director, if(is), Germany Opening plenary keynotes Troels Ørting, Head of European Cybercrime Centre (EC3), Europol, The Netherlands The European cyber-security strategy and the role for the new European Cybercrime Centre Mayank Upadhyay, Principal Engineer, Google, USA Cyber security: human factors and authentication tools John Lyons, Chief Executive, International Cyber Security Protection Alliance, UK Ways to collaborate internationally to fight cyber crime more effectively – and why the EU should lead				
11.30-12.00	Coffee break				
12.00-12.30	Keynote (Main Conference Sponsor Microsoft)				
12.30-13.15	Opening panel: Cybersecurity in Europe – the next steps Chair: Steve Gold, Editor-in-Chief, IT Security Pro, UK Steve Purser, Head of Operations, ENISA, Greece Freddy Dezeure, Head of task force "CERT-EU", European Commission, Belgium Michael Hange, President, German Federal Office for Information Security (BSI), Germany Franky Thrasher, Information Security Manager, Electrabel, Belgium Gerold Hübner, Chief Product Security Officer, SAP, Germany				
13.15 – 14.00	Lunch break and networking				
14.00 – 14.30	EU Regulation on eID and eSignature Roger Dean, Executive Director, EEMA, UK	Trust Services and Cloud Security Erik R. van Zuuren, Director, Deloitte, Belgium	Human Factors, Awareness Achim Klabunde, Head of Sector IT Policy, European Data Protection Supervisor, Belgium	Real Life Deployment	STORK
	Aim and progress of the legislative process Paul Timmermans, Director Sustainable & Secure Society, DG CONNECT, European Commission, Belgium	DRM for HTML5 - combining DRM with document encryption Bruno Quint, Managing Director, Corisecio, Germany	Don't ask what you can do for your security, but ask what your security can do for you Patrick Michaelis, Senior Auditor, AC – The Auditing Company, Germany	Maximising data loss prevention through secure mobile applications and content Dave Renwick, Director of Innovation, EMEA, AirWatch, UK	

Panel: Cyber security in Europe - the next steps. How to come back to a trustworthy Internet?

Human Factors, Awareness

This presentation is featured within your ISSE 2013 proceedings

EU Regulation on eID and eSignature

22nd & 23rd October 2013
MCE, Brussels, Belgium

King new ground in STORK 2.0 updates and business services
 Bert Leitold, Head of Graz, A-SIT, Austria

(continued)
Verification
 Kuipers, Owner, ID Network, Netherlands
 O'Connell, Independent consultant and founder, myFuture.com, UK

Initiatives in international lectures for citizen access to government services, and related identity schemes, using leveraging third party identities and credentials to create an EU, US, UK, NL panel
 Kuipers, Owner, ID Network, Netherlands

User Panel
 Roger Dean, Executive Director, A, UK

Verification
 Belgium
 Kuipers, Owner, ID Network, Netherlands
 O'Connell, Independent consultant and founder, myFuture.com, UK



How has Snowden changed the evaluation of the IT security situation?

Norbert Pohlmann

Chairman: IT security association TeleTrust

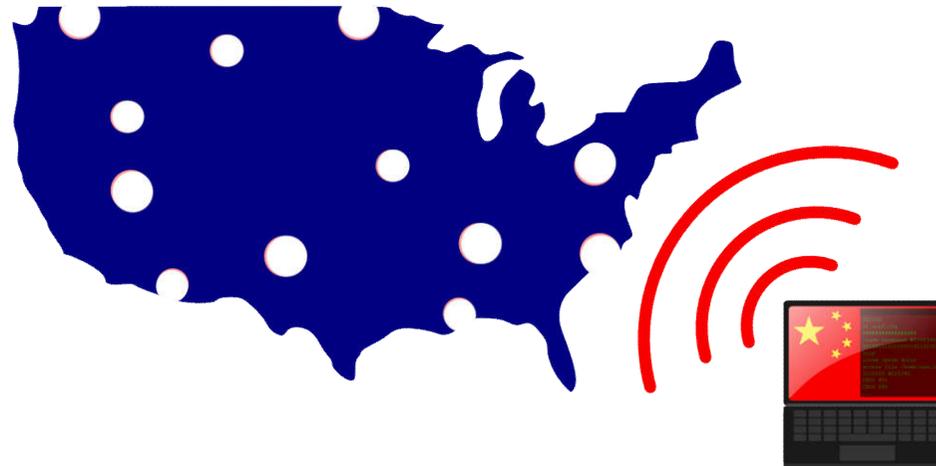
Professor: Westphalian University of Applied Sciences

Director: Institute for Internet Security - if(is)

Findings I

Hackers from “China” hacked everything very successful!

- Google, Microsoft, RSA, ...
- The New York Times, Washington Post, ...
- Every US Government Agency, ...
- ...

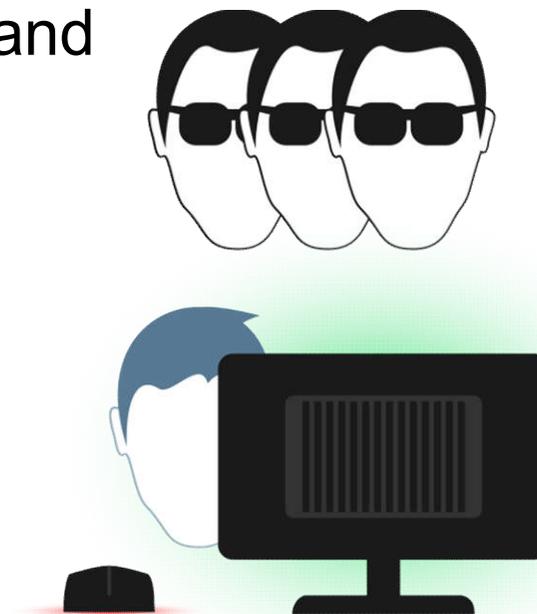


The todays IT and IT security technology cannot stop the attackers.

Findings II

NSA and Co. do everything which is possible

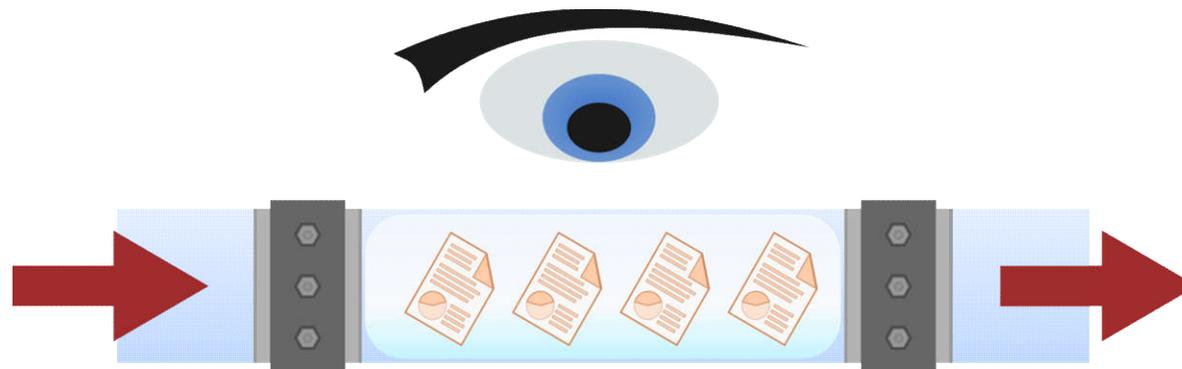
- Of course we all know the theoretical possibilities
- But we are shocked about what is really implemented
- The US IT market leaders are assistants to the NSA
- The laws make everything top secret and therefore it is not discussible
- The NSA is buying the knowledge about new security vulnerability for own attacks, not for publishing
- The end does not justify the means



What is the problem?

Manipulated IT and IT security technologies make our business insecure!

- Implementation errors in IT security technologies (SSL, ...)
- Using insecure Cipher Suite (RC4, DES, ...)
- Bad random generators
- Backdoors in hardware and software (OS, App, ...)
- Using NSA friendly e-mail accounts and cloud services
- ...



No transparency → produces distrust!

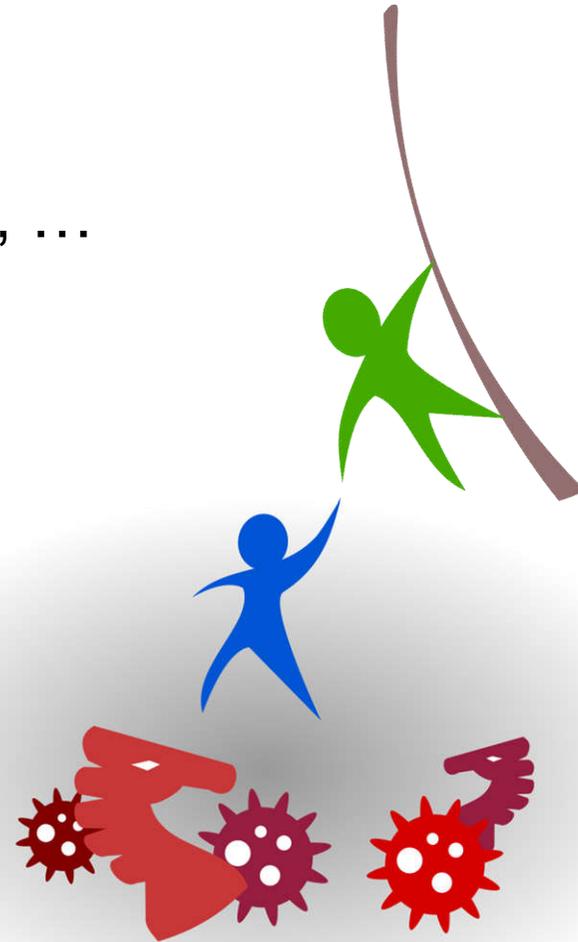
Which IT company can we trust?

- Google, Facebook, Microsoft, Apple, ...

Which government can we trust?

- US, UK, Canada, ..., Germany, ...

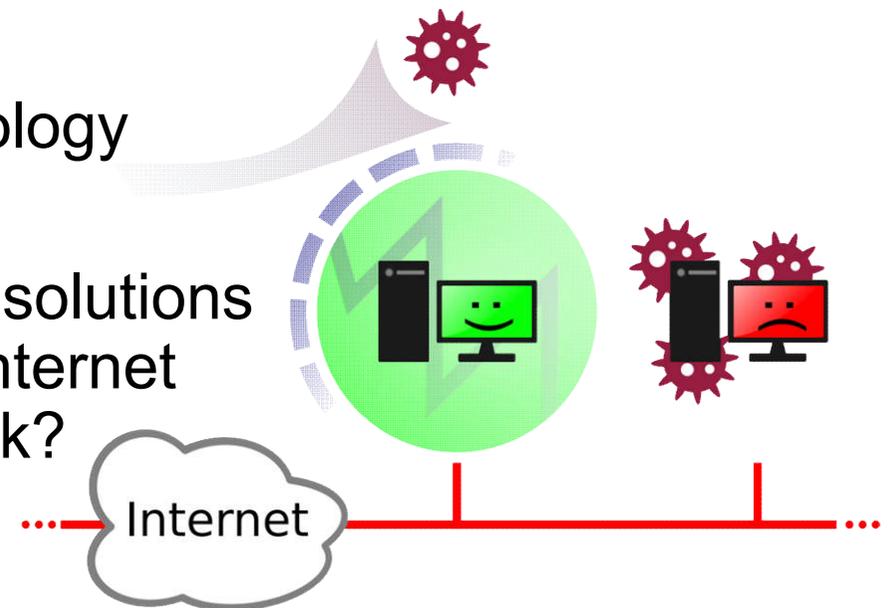
Can we still trust evaluation and certification results?



IT security situation today

How can we improve our IT security situation?

- Can we stop the misuse of IT vulnerabilities?
- Is it possible to detect backdoors in technology and services?
- Can we protect us against the economic espionage and the power of the Intelligence Services and the Cyber soldiers from some countries?
- Which IT and IT security technology can stop the attackers?
- Will we find secure and trusted solutions so that we can use the global Internet with an appropriated level of risk?
- Whom can I trust?
- ...



Thank you very much for your
attention!

I wish everybody a very successful

ISSE 2013

in
Brussels