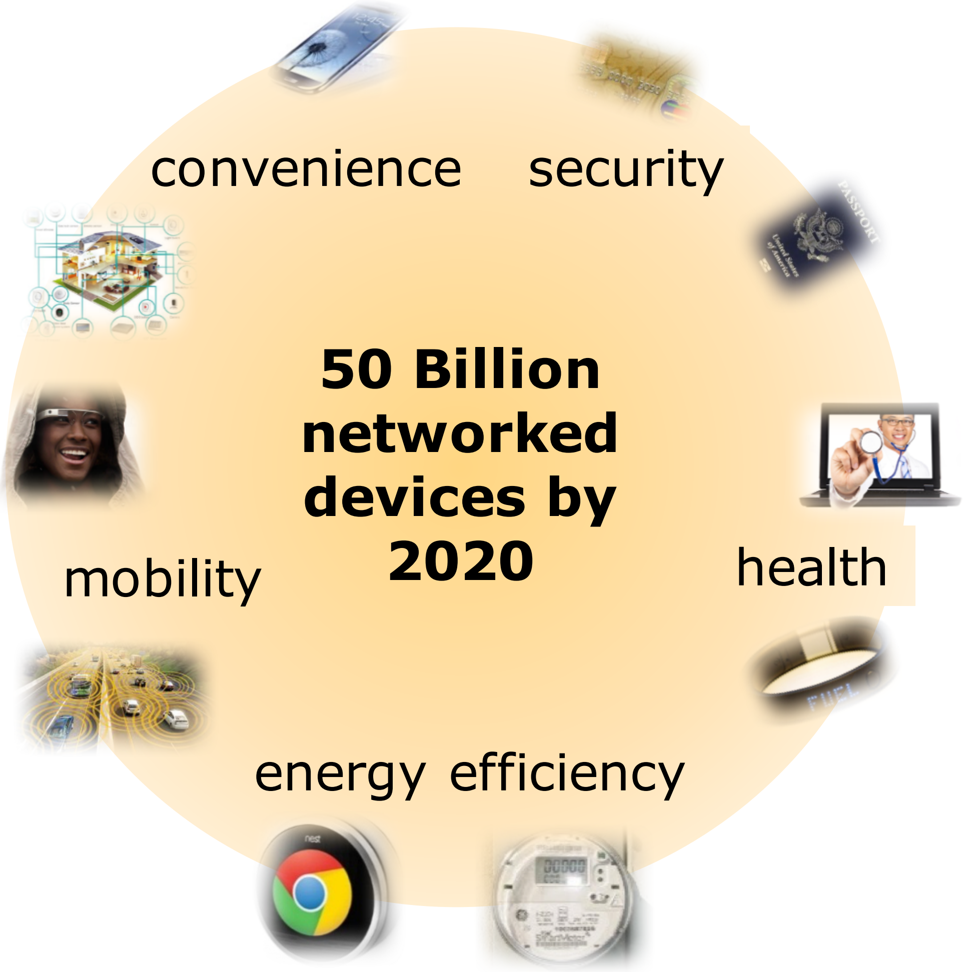
Hyper connectivity is changing our world forever



convenience

security

50 Billion networked devices by 2020

mobility

health

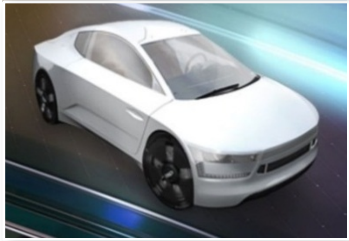
energy efficiency

Internet of Things

Cyber Security

Portable & Wearable

Connected Car

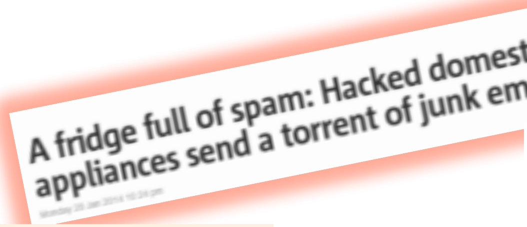


Beckstrom's* Laws of Cyber Security

1. Everything that is connected to the Internet can be hacked
2. Everything will be connected to the Internet
3. Everything else follows from the first two laws

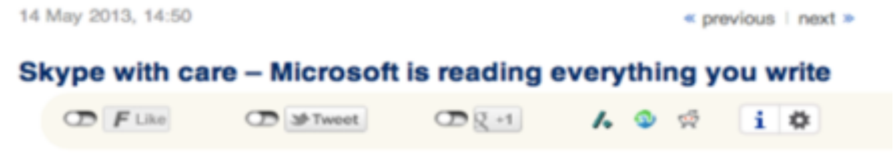
*Rod Beckstrom, CEO and President of ICANN, former Director of the National Cyber Security Center.

Beckstrom’s* Laws of Cyber Security



A fridge full of spam: Hacked domestic appliances send a torrent of junk email

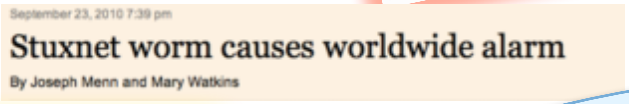
Monday 20 Jan 2014 10.24 pm



14 May 2013, 14:50

« previous | next »

Skype with care – Microsoft is reading everything you write

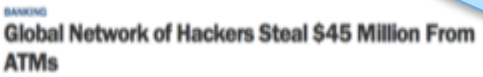


September 23, 2010 7:39 pm

Stuxnet worm causes worldwide alarm

By Joseph Menn and Mary Watkins

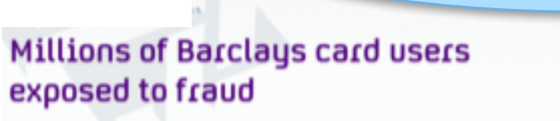
1. Everything that is connected to the Internet can be hacked
2. Everything will be connected to the Internet
3. Everything else follows from the first two laws



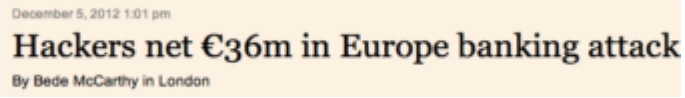
BANKING

Global Network of Hackers Steal $45 Million From ATMs

By AP / Colleen Long | May 09, 2013 | 3 Comments



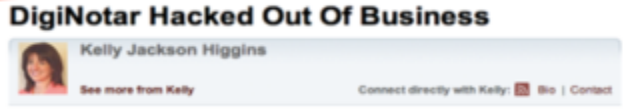
Millions of Barclays card users exposed to fraud



December 5, 2012 1:01 pm

Hackers net €36m in Europe banking attack

By Bede McCarthy in London



DigiNotar Hacked Out Of Business

Kelly Jackson Higgins

See more from Kelly

Connect directly with Kelly: Bio | Contact

*Rod Beckstrom, CEO and President of ICANN, former Director of the National Cyber Security Center.

Secure Hardware and Trusted Software

- Secure Hardware supports Trusted software
- Signed boot image (using a Root of Trust of Verification)
- Provides controlled access to resources
  - MMU/IOMMU
  - Encrypted data
  - Secure Memory
- Root of Trust of Storage
  - Chip unique encryption key
- Immutable chip configuration

- Trusted software has a signature
  - Not necessarily Trustworthy
- Trustworthy software works as advertised
  - Properly implements APIs
  - Does nothing unexpected (i.e., malicious)
- Supports separation of tasks
  - TrustZone
  - Trusted Execution Environments
  - Hypervisor
  - Sandboxes

Invasive and Information Leakage attacks

- Invasive attacks
- Open up the processor package
  - Reverse engineering
  - Probing the die
  - Modifying the die with FIB
  - Fault injection attacks

- Information Leakage attacks
  - Side-channel attacks
  - Timing attacks
  - Simple Power Analysis
  - Differential Power Analysis
  - EM Analysis
  - Audio (listening to hard drives)

Information Leakage Attacks (SPA, DPA, EMA)

- Washington Domino Pizza Index (early ’90)
- Pentagon, at any normal evening about 12 - 15 pizzas…

- But every once in a while 36 - 45 pizzas…

Panama, Gulf War, …

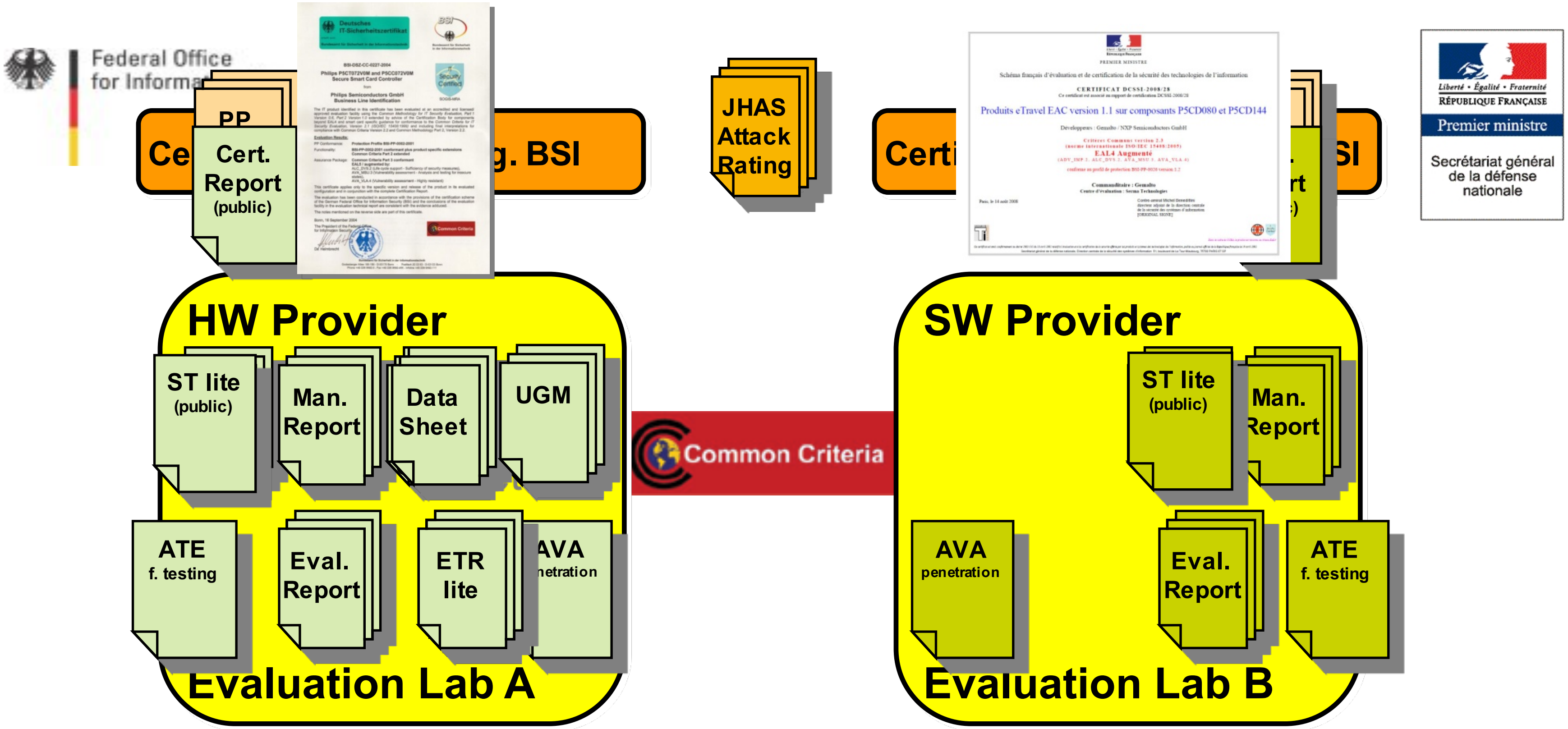
- Information leakage without any official press announcement!

SPA: Simple ~~Pizza~~ Power Analysis

DPA: Differential ~~Pizza~~ Power Analysis

A Helicopter View on a CC Evaluation

- **Provides assurance that the Secure HW and SW are Trustworthy**
  - HW provider gets the HW platform evaluated
  - SW provider gets the final product with OS evaluated



Federal Office for Informa

PP

Cert. Report (public)

Ce… g. BSI

Deutsches IT-Sicherheitszertifikat

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0227-2004

Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller

from

Philips Semiconductors GmbH Business Line Identification

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0 extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999) and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

PP Conformance: Protection Profile BSI-PP-0002-2001

Functionality: BSI-PP-0002-2001 conformant plus product specific extensions Common Criteria Part 2 extended

Assurance Package: Common Criteria Part 3 conformant EAL5 augmented by: ALC_DVS.2 (Life cycle support - Sufficiency of security measures), AVA_MSU.3 (Vulnerability assessment - Analysis and testing for insecure states), AVA_VLA.4 (Vulnerability assessment - Highly resistant)

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 16 September 2004

The President of the Federal Office for Information Security

Dr. Helmbrecht

Common Criteria

IT Security Certified SOGIS-MRA

JHAS Attack Rating

Certi… …SI

Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

CERTIFICAT DCSSI-2008/28

Ce certificat est associé au rapport de certification DCSSI-2008/28

Produits eTravel EAC version 1.1 sur composants P5CD080 et P5CD144

Développeurs : Gemalto / NXP Semiconductors GmbH

Critères Communs version 2.3 (norme internationale ISO/IEC 15408:2005)

EAL4 Augmenté

(ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4)

conforme au profil de protection BSI-PP-0026 version 1.2

Commanditaire : Gemalto

Centre d'évaluation : Serma Technologies

Paris, le 14 août 2008

Contre-amiral Michel Benedittini directeur adjoint de la direction centrale de la sécurité des systèmes d'information [ORIGINAL SIGNE]

…rt …)

Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

Premier ministre

Secrétariat général de la défense nationale

HW Provider

ST lite (public)

Man. Report

Data Sheet

UGM

ATE f. testing

Eval. Report

ETR lite

AVA …netration

Evaluation Lab A

Common Criteria

SW Provider

ST lite (public)

Man. Report

AVA penetration

Eval. Report

ATE f. testing

Evaluation Lab B

Platform Evaluation

Composite Evaluation

SECURE CONNECTIONS
FOR A SMARTER WORLD