Cybersecurity Workshop

The Security Innovations Network

www.securityinnovationnetwork.com
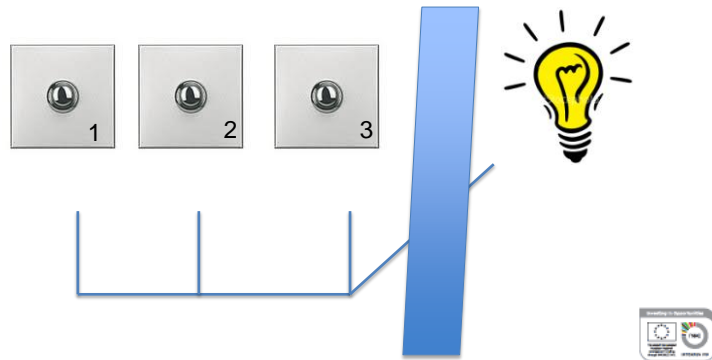
BRUcon, September 25th 2010,

Agenda

- Start Thinking
- Some Examples
- Some Solutions?
- Other Solutions :
- About
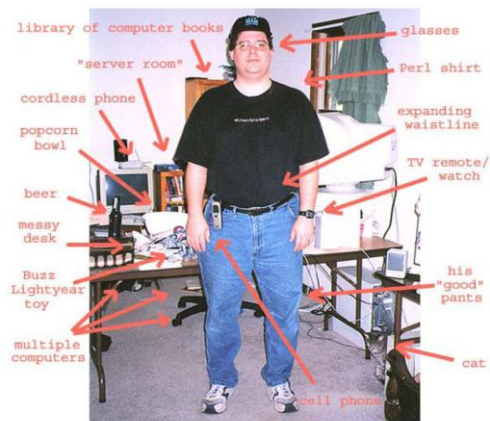
* Sources : iDefense, Websense, McAfee, LSEC and others,

Which Switch turns on the light?

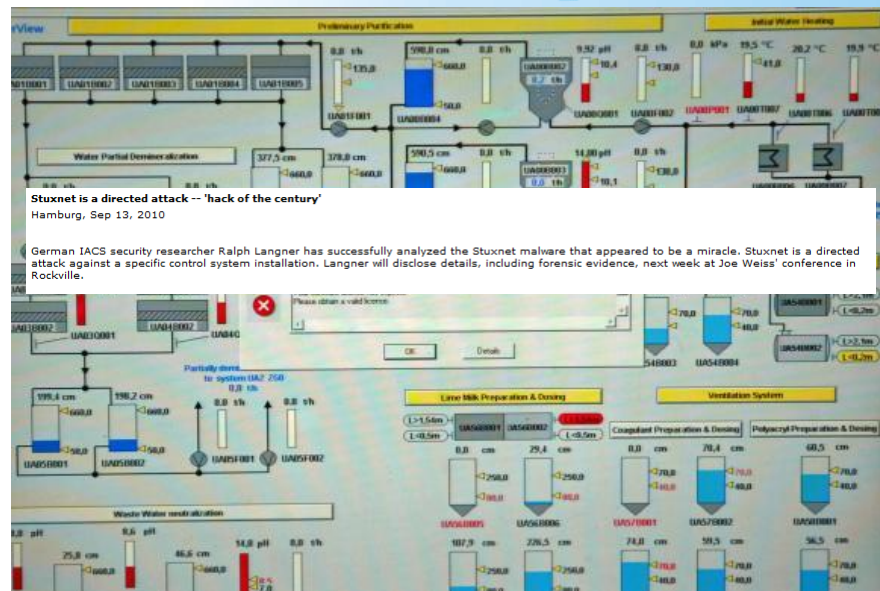Which switch turns on the light?

Anatomy of a Hacker

Anatomy of a Hacker

Cybersecurity ?

Stuxnet is a directed attack -- 'hack of the century'
Hamburg, Sep 13, 2010

German IACS security researcher Ralph Langner has successfully analyzed the Stuxnet malware that appeared to be a miracle. Stuxnet is a directed attack against a specific control system installation. Langner will disclose details, including forensic evidence, next week at Joe Weiss' conference in Rockville.

Cybersecurity ?

Rich Internet Applications drives multimedia, interactive applications, and dynamic content on all platforms.

Cloud Computing drives SaaS and PaaS, moves application and data to outside the network.

Social Web drives communication, interaction, and sharing of data.

Source : LSEC Future Internet Security Seminar, Websense Patrik Runald, 2010

Reaction times?

2009 Trends

iDEFENSE

Microsoft — Monthly, 2d Tuesday

ORACLE — Quarterly, 2d Tuesday

CISCO — Bi-Annually: Mar / Sep 4th Wednesday

Quarterly, 2d Tuesday

Reaction times?

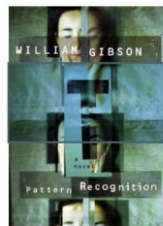Vulnerability Fixes   34 **Microsoft**

ORACLE Postponement

October 2009   29 Adobe

63 Total

Methods : Vulnerabiliities

Pattern Recognition"
By William Gibson

Pattern

Targeted Attacks

↓

Report to Authorities

↓

Public Disclosure

↓

Proof of Concept Code
in the public

↓

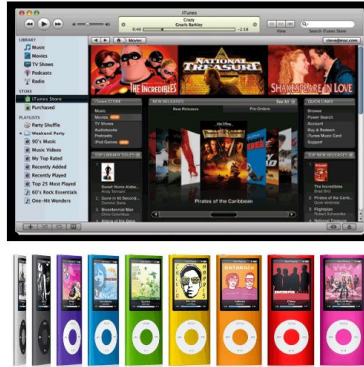Low-level Trojan Kits
(Chinese Gaming)

VM Obfuscation

Value of PIM

Date of Birth:	$10.00
Credit Card Balance:	$0.30
Mother's Maiden Name:	$10.00
Social Security Number:	$4.00
Driver's License	$10.00

Business Disruptors

Disruptors

Robert Morris

WarGames

TRON

HACKERS

CYBER CRIME

CYBER ESPIONAGE

CYBER WARFARE

Vladimir Levin

Titan Rain

Estonia

Disruptors

🇺🇸 New Cyber Command; New Cyber Security Czar

🇰🇷 Cyber forces expand by 3,000; New Command Opened In Jan

🇯🇵 Increases funding to Self-Defense Forces

🇧🇷 Government partnering with private-sector hackers

🇨🇳 Expands Net Militia system; forbids foreign contracting to the PLA

🇮🇳 Extensive planning; new organizations to launch soon
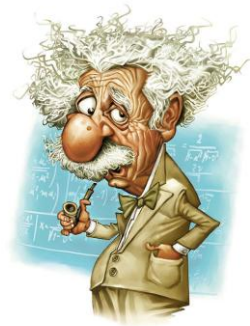

Disruptors

Innovation

When you always do what
you've always done,

You will always get what
you've always got !!

An innovator, A. Einstein

Innovative Solutions ?

- Sandboxing
- Mirroring
- Deep packet inspection
- Multi-layered security
- WARPS
- Certifications
- Trusted Computing
- ....

About

About

Ulrich Seldeslachts
ulrich at securityinnovationnetwork.com

ulrich at lsec.be
+32 16 32 8541