Cyber-Physical Systems in the Smart Grid - potential and challenges

Stamatis Karnouskos
SAP Research

EU-US JOINT OPEN WORKSHOP ON CYBER SECURITY OF ICS AND SMART GRIDS
15 October 2012, Amsterdam, The Netherlands

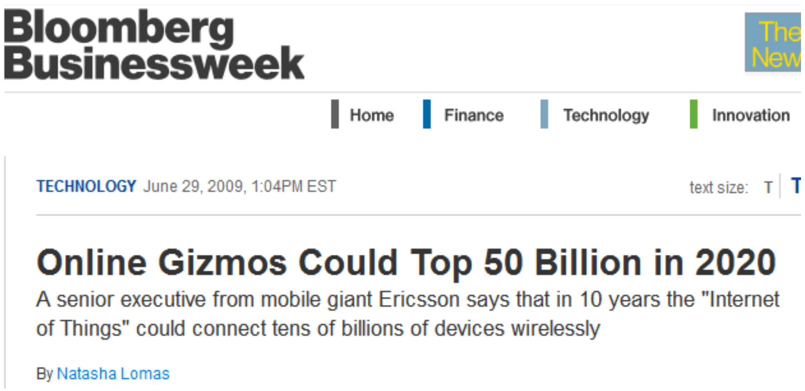
ICT Trends for device growth → Towards Trillion Node Net (cum grano salis)

□"[In 10 years' time], everything has connectivity. We're talking **about 50 billion connections, all devices will have connectivity**...” Håkan Djuphammar, VP of systems architecture, Ericsson (2009)

□“...at least **20 billion connected devices by 2020** and a 300-fold increase in traffic...” John Woodget, global director, telecoms sector, Intel (2009)

□... the smart grid network will be “**100 or 1,000 times larger than the Internet**” Marie Hattar, vice president of marketing, Cisco Network Systems Solutions

□“**The next billion SAP users will be smart meters**” Vishal Sikka, CTO of SAP (2009)

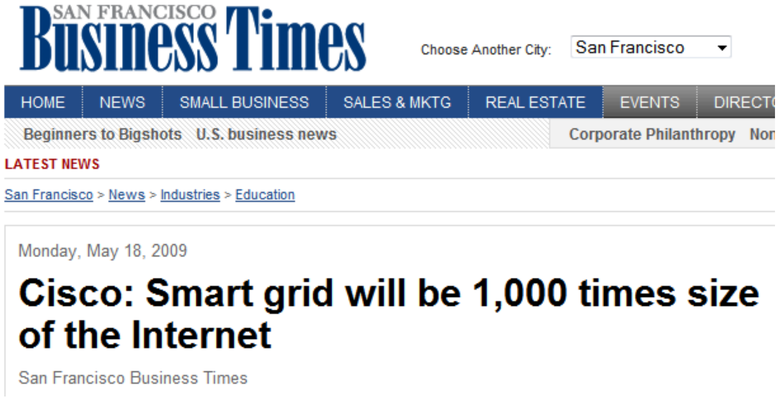


TECHNOLOGY June 29, 2009, 1:04PM EST

Online Gizmos Could Top 50 Billion in 2020

A senior executive from mobile giant Ericsson says that in 10 years the "Internet of Things" could connect tens of billions of devices wirelessly

By Natasha Lomas

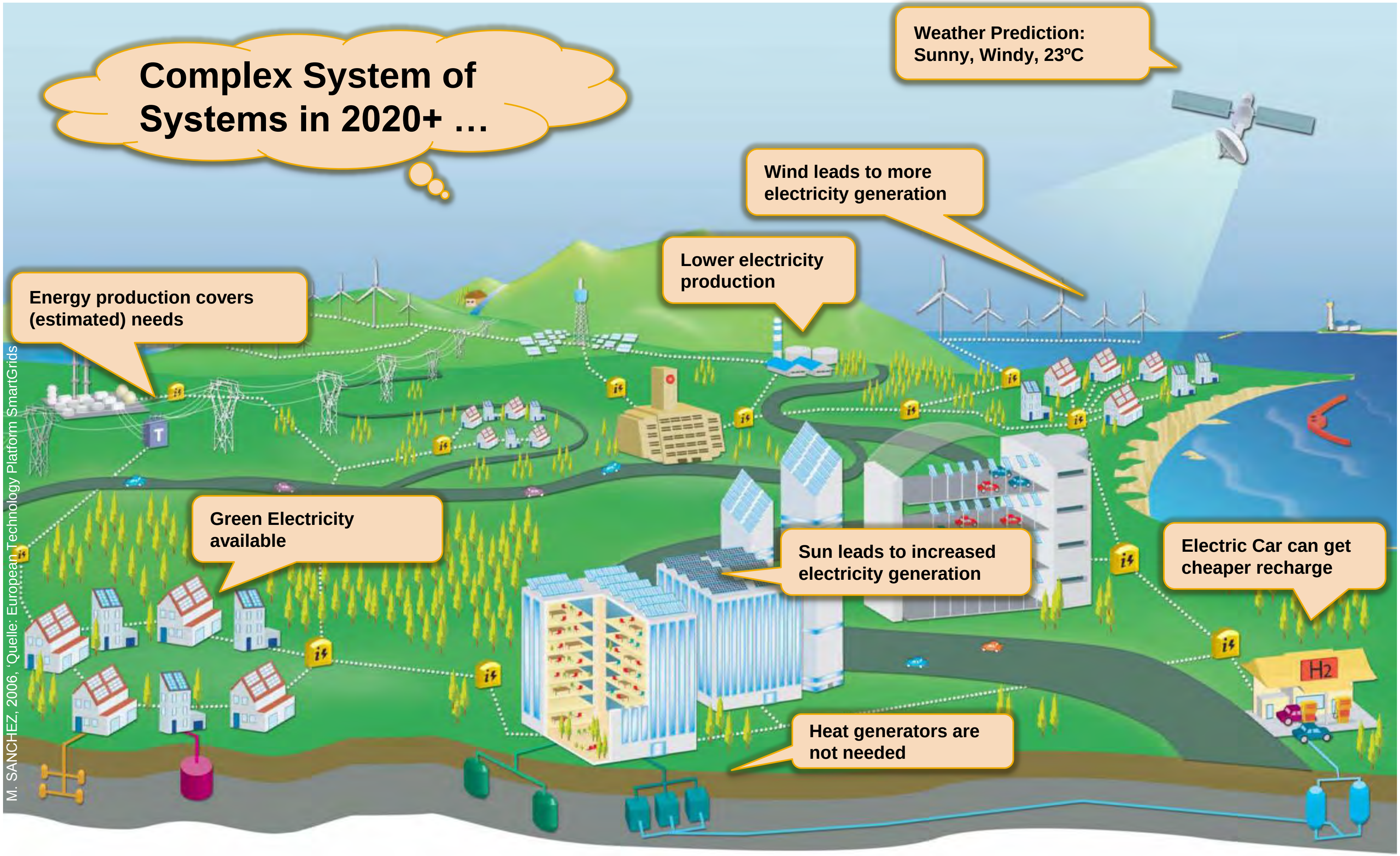


Monday, May 18, 2009

Cisco: Smart grid will be 1,000 times size of the Internet

San Francisco Business Times

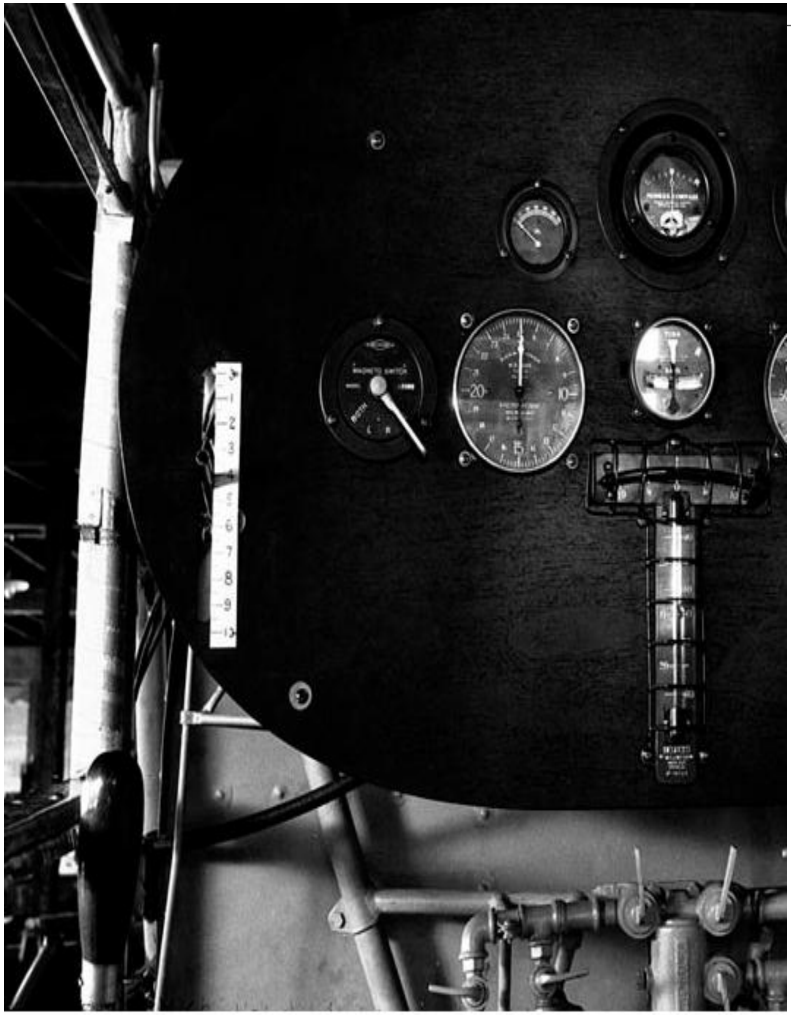
The SmartGrid City– a collaborative System of Systems



Complex System of Systems in 2020+ …
Weather Prediction: Sunny, Windy, 23ºC
Wind leads to more electricity generation
Lower electricity production
Energy production covers (estimated) needs
Green Electricity available
Sun leads to increased electricity generation
Electric Car can get cheaper recharge
Heat generators are not needed
T
H2

M. SANCHEZ, 2006, 'Quelle: European Technology Platform SmartGrids

Smart City: Growing Complexity Management Challenges



The Spirit of St. Louis (1927)

Source: www.charleslindbergh.com

Airbus A380 (2005)

Trillion Node Era - A Security Nightmare?

❑ Trillions of Devices available! Are they going to be “secure”?

❑ What does “secure” mean ? How do we assess it system-wide?

❑ Who manages the devices and their lifecycle (e.g. updates)?

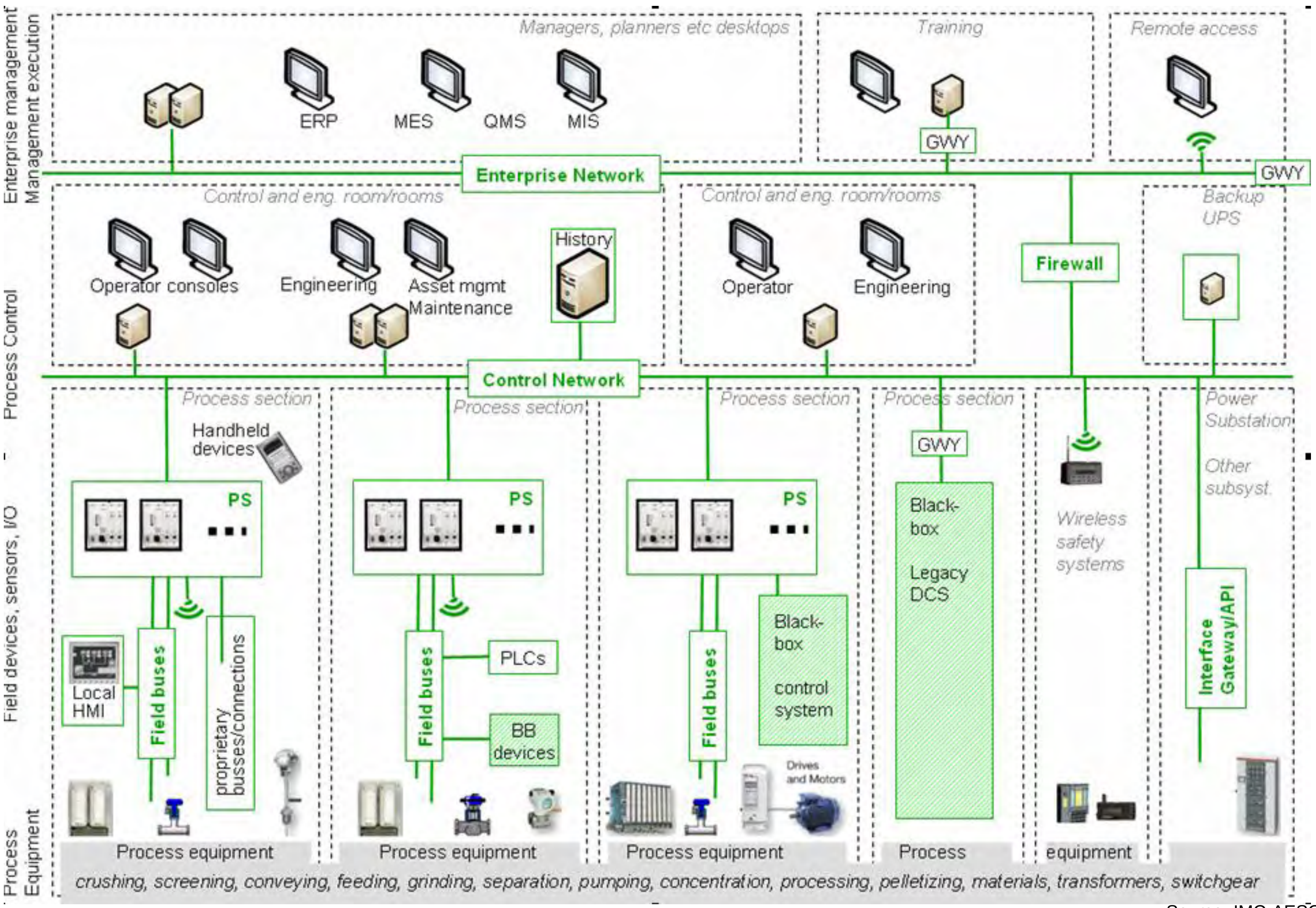
❑ What about the info they emit? What is the benefit vs. misuse ratio?

❑ What about privacy issues in a fully-interconnected Future Internet?

❑ What is the impact on the real-world?

❑ What about critical infrastructures?

Towards highly interconnected complex systems

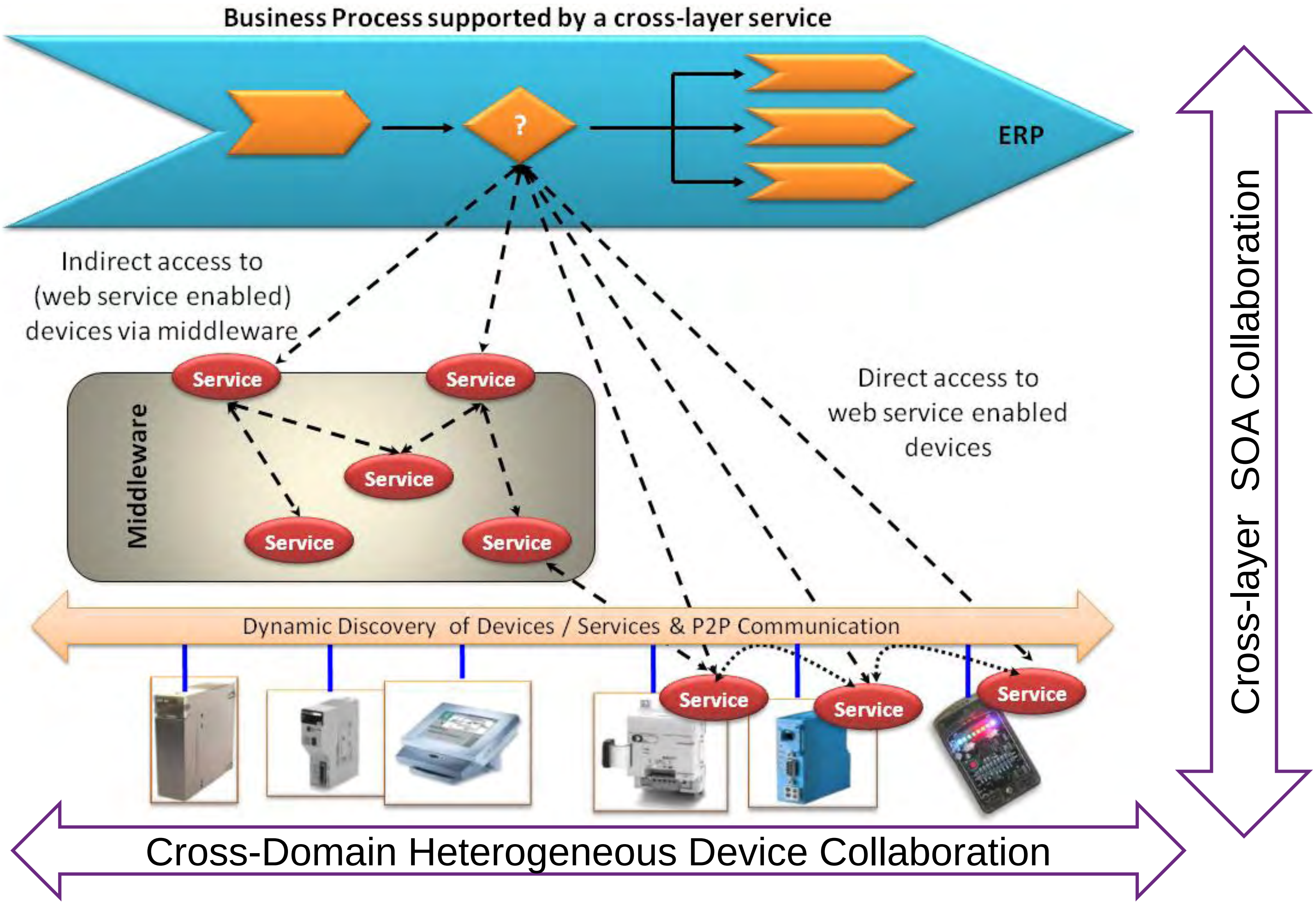


Source: IMC-AESOP Project

Trends

- Increasing usage of Internet Technologies e.g. TCP/IP, web services etc.
- Information Driven Interaction vs. Communication focus
- Distributed Business Processes
- Virtualization and Cloud Computing
- Multi-core Networked Embedded systems and GPU computing
- SOA-ready devices and systems
- Commercial DBs and tools for vizualisation & management
- Integration with business systems e.g. ERP, GIS etc.
- High performance analytics, asset management, reporting, etc.
- Drivers: minimize cost + optimize performance

Machine-to-Business (M2B) Interactions


Business Process supported by a cross-layer service
?
ERP
Indirect access to (web service enabled) devices via middleware
Middleware
Service
Service
Service
Service
Service
Direct access to web service enabled devices
Dynamic Discovery of Devices / Services & P2P Communication
Service
Service
Service
Cross-layer SOA Collaboration
Cross-Domain Heterogeneous Device Collaboration

Stuxnet capabilities

- Utilized zero-day exploits i.e. security holes that the software developers were unaware of.
- Its code was obfuscated and difficult to reveal its functionality. Even today we do not understand it in its hole.
- A custom encryption algorithm was used for its configuration data.
- It took advantage of the private network (not connected in the Internet) to automatically update itself once a new copy of it was discovered. Hence an infected machine with newer Stuxnet version in the network would result in all existing Stuxnet installations to be upgraded to that version.
- It utilized peer-to-peer networks to dynamically discover and communicate (update) with all Stuxnet installations. All of the actions were done in memory and therefore no disk evidence (files) exists.
- It kept an infection counter

Stuxnet capabilities

- Had a highly modular architecture.
- Was masking under legal programs.
- Deployed anti-virus detection mechanisms.
- Could detect Internet connectivity and only then would attempt to connect to its Internet hosted Command & Control center.
- Elevated privileges (via specific exploits) in an unpatched machine in order to have the necessary execution rights
- Would infect in a very specific way only targeted systems (highly target-customizable).
- Had strict self-scalability control i.e. it would contain safeguards to prevent infected computers spreading the worm to more than three others.

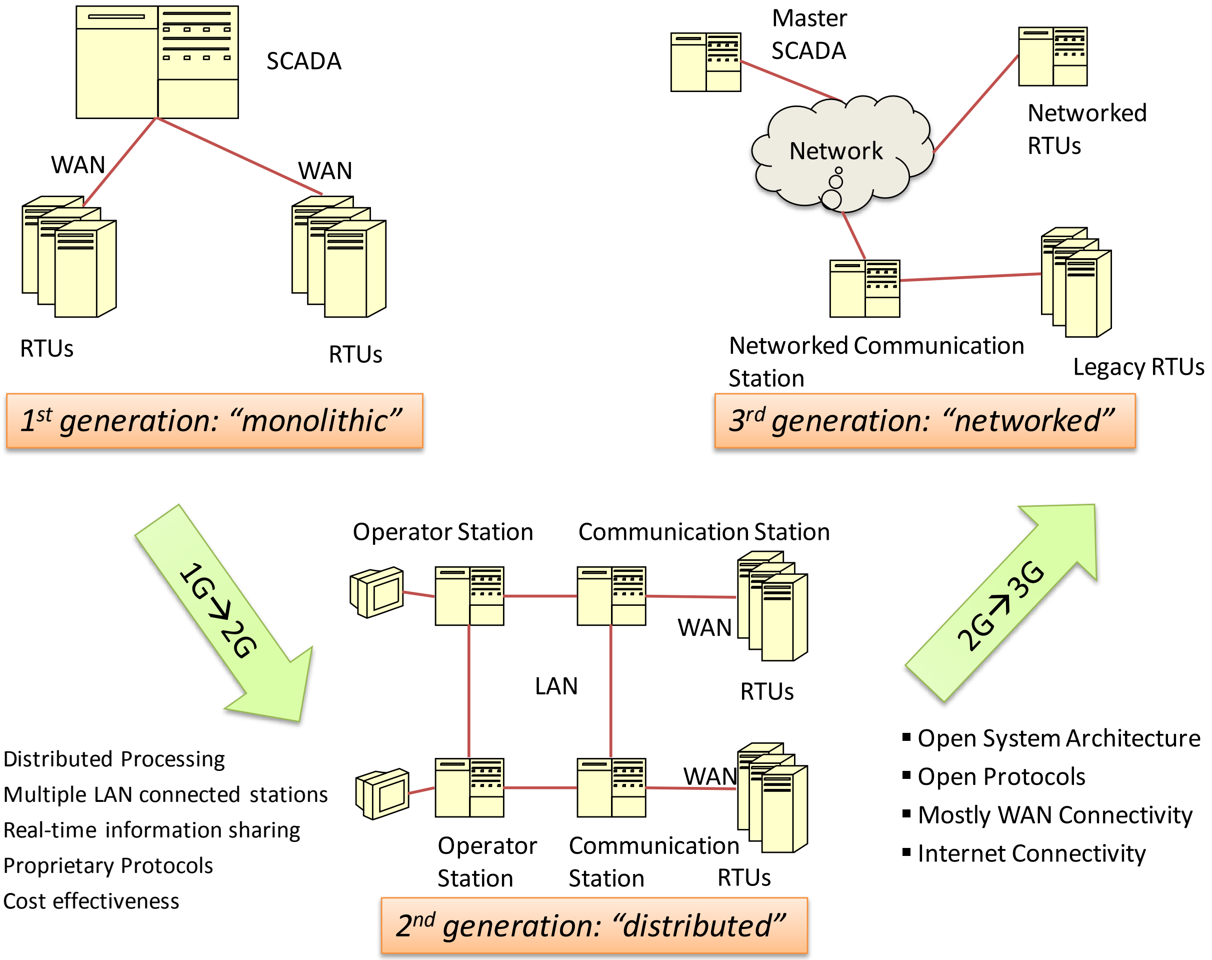
Stuxnet capabilities

- Had an un-install mechanism which removed itself (self-lifecycle management). It was programmed to erase itself on 24-June-2012 (stop spreading only -- the malfunction continues).
- Contains, among other things, code for a man-in-the-middle attack that fakes industrial process control sensor signals; hence processes and tools relying on the data it generates would falsely depict further ``normal'' values and functionality that did not mirror the actual real world.
- Deployed legitimate digitally signed device drivers (with stolen private keys of two certificates that were stolen from separate companies)
- Had external websites configured as command and control (C&C) servers. This would enable various monitoring and control activities (if Internet was available) including industrial espionage by uploading information (originating internal connections to external servers are usually ``acceptable'' flows by firewalls)

Stuxnet: Lessons Learned

- Security awareness low and risk assessment is faulty.
- Many live on the “don’t touch a running system” / “I am not on the Internet” motto
- Security problems of 2+ years old were not addressed
- Lifecycle management of assets and processes has to include security and be adjusted/revised on-demand for critical systems
- Do NOT trust single sources of data / verify independently (multiple information paths / checks).
- Security 101: ask/verify/check security/safety/quality requirements on supplier
- Prepare for the known threats, and plan for the unknown (e.g. via heuristics)

SCADA Evolution



1st generation: "monolithic"

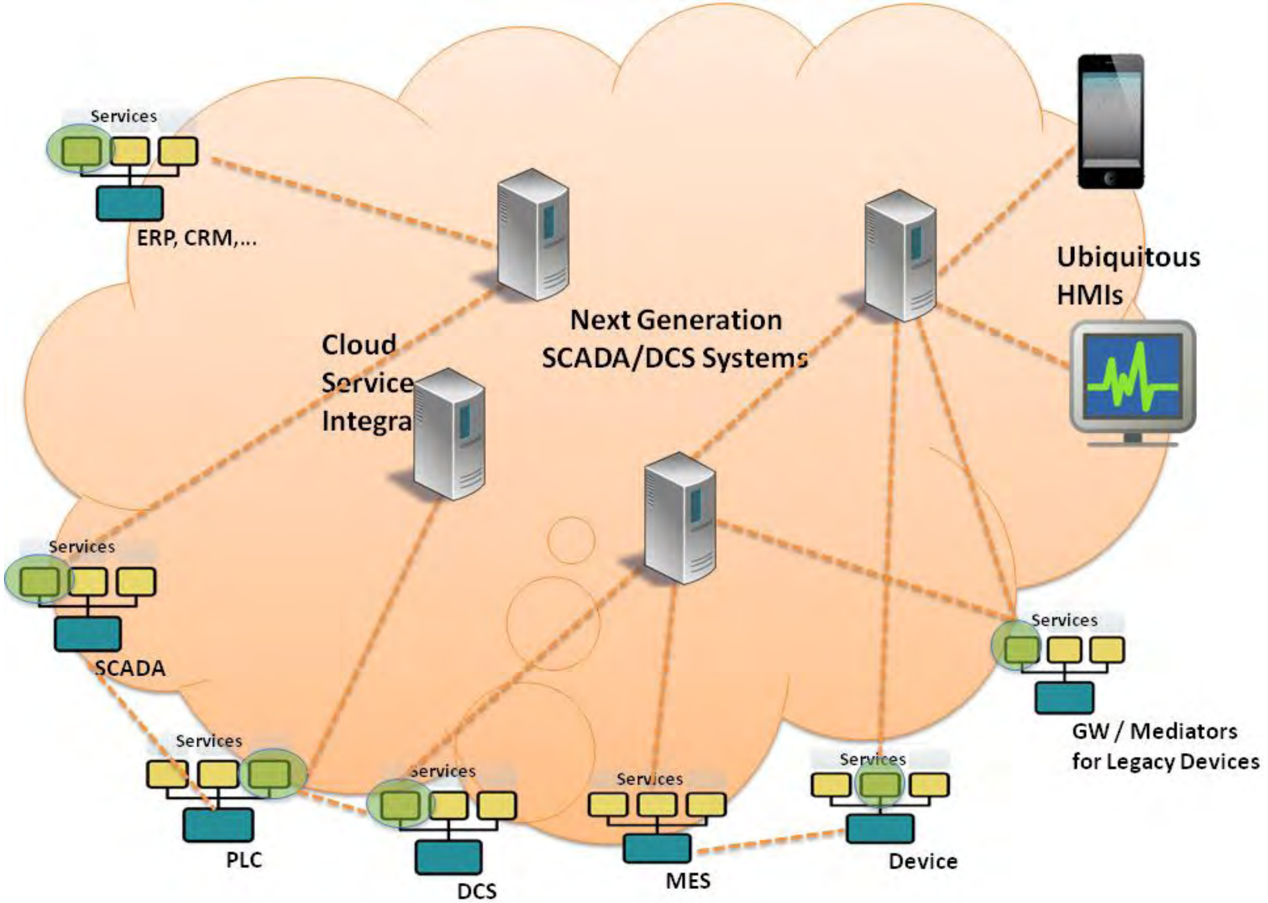
3rd generation: "networked"

2nd generation: "distributed"

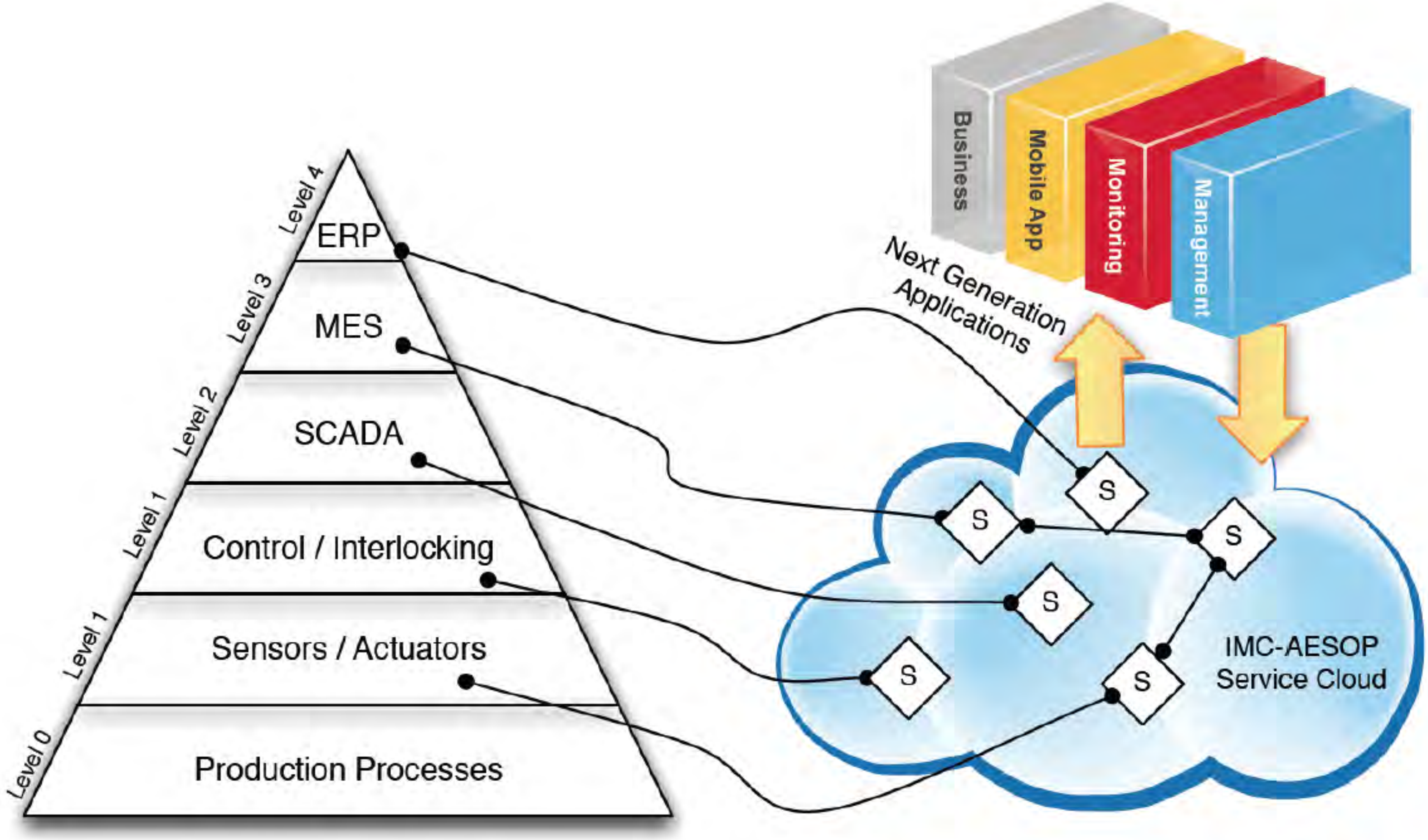
- Distributed Processing
- Multiple LAN connected stations
- Real-time information sharing
- Proprietary Protocols
- Cost effectiveness

- Open System Architecture
- Open Protocols
- Mostly WAN Connectivity
- Internet Connectivity

Next generation of SCADA/DCS … towards cloud-based CPS systems

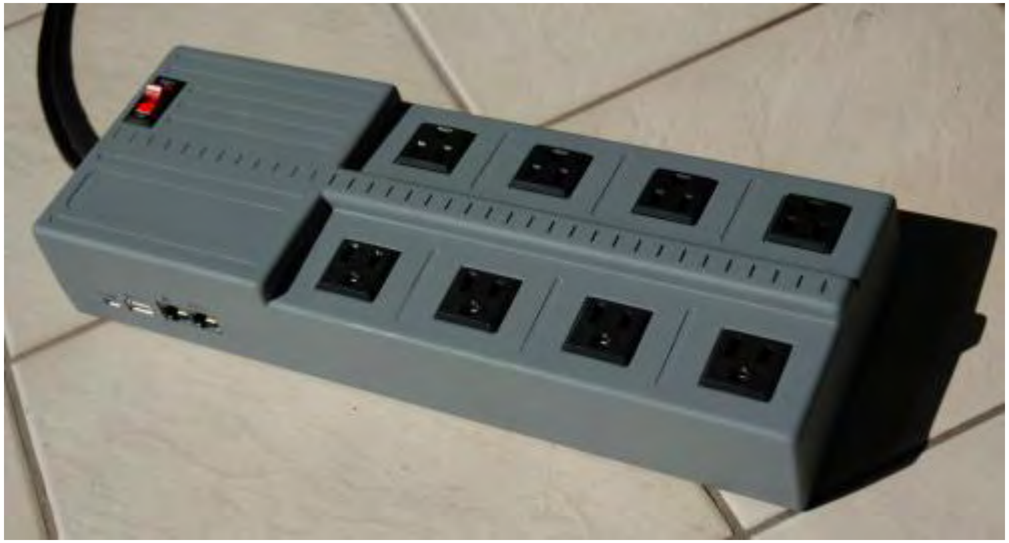


A new cloud-based approach for industrial automation



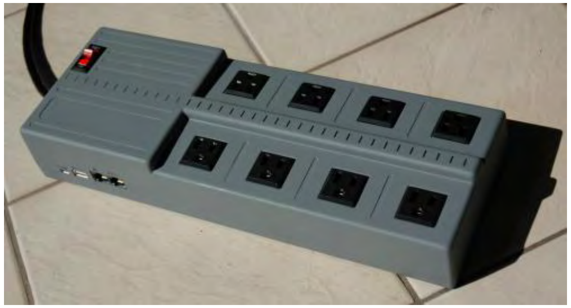
www.imc-asesop.eu

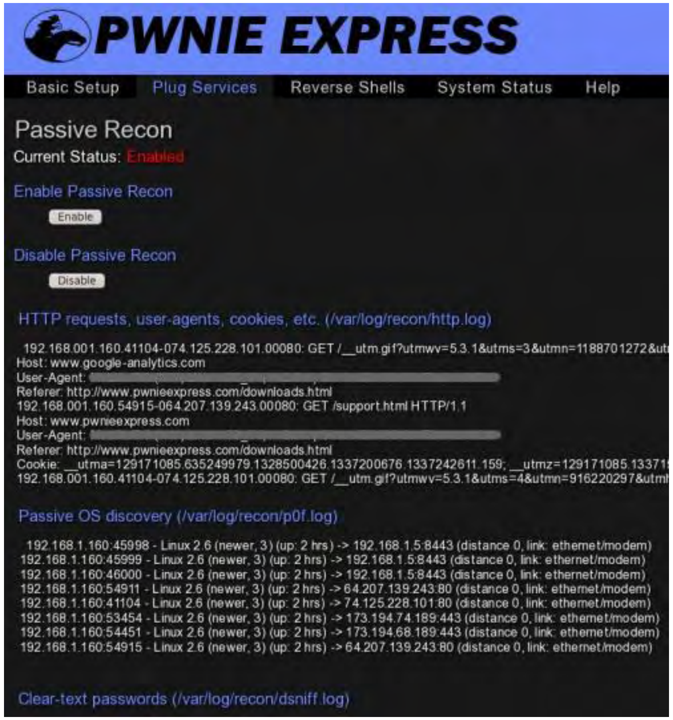
What is this?



Should you worry about it?

“known” physical world camouflage in an office near you





Passive Recon

Current Status: Enabled

Enable Passive Recon

Disable Passive Recon

HTTP requests, user-agents, cookies, etc. (/var/log/recon/http.log)

```
 192.168.001.160.41104-074.125.228.101.00080: GET /__utm.gif?utmwv=5.3.1&utms=3&utmn=1188701272&ut
Host: www.google-analytics.com
User-Agent: [redacted]
Referer: http://www.pwnieexpress.com/downloads.html
192.168.001.160.54915-064.207.139.243.00080: GET /support.html HTTP/1.1
Host: www.pwnieexpress.com
User-Agent: [redacted]
Referer: http://www.pwnieexpress.com/downloads.html
Cookie: __utma=129171085.635249979.1328500426.1337200676.1337242611.159; __utmz=129171085.13371
192.168.001.160.41104-074.125.228.101.00080: GET /__utm.gif?utmwv=5.3.1&utms=4&utmn=916220297&utm
```

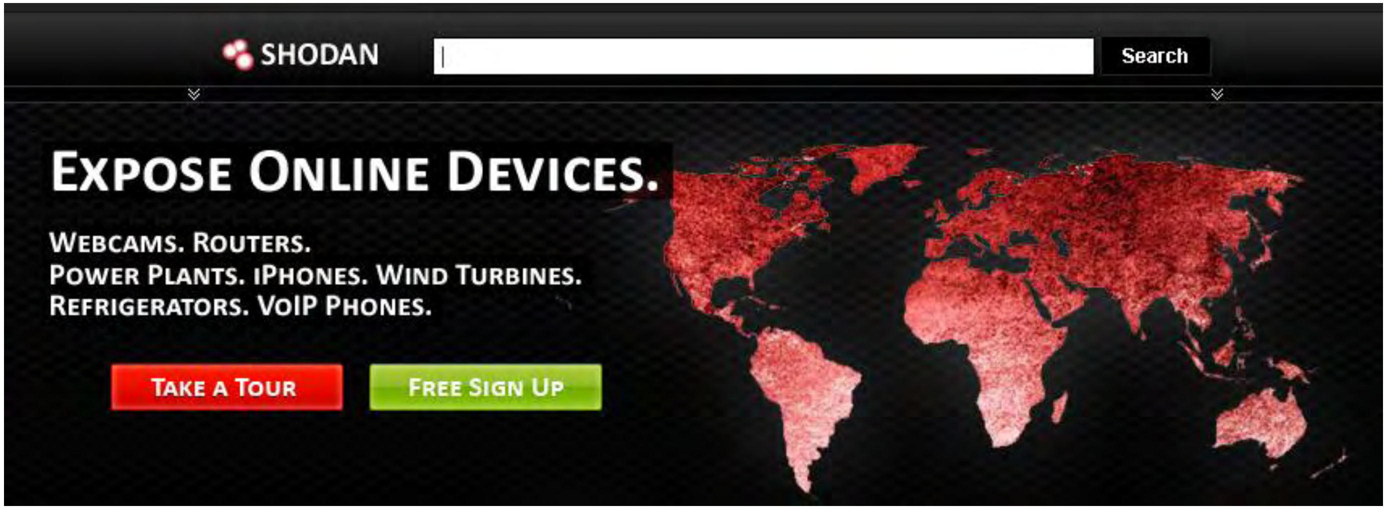
Passive OS discovery (/var/log/recon/p0f.log)

```
 192.168.1.160:45998 - Linux 2.6 (newer, 3) (up: 2 hrs) -> 192.168.1.5:8443 (distance 0, link: ethernet/modem)
192.168.1.160:45999 - Linux 2.6 (newer, 3) (up: 2 hrs) -> 192.168.1.5:8443 (distance 0, link: ethernet/modem)
192.168.1.160:46000 - Linux 2.6 (newer, 3) (up: 2 hrs) -> 192.168.1.5:8443 (distance 0, link: ethernet/modem)
192.168.1.160:54911 - Linux 2.6 (newer, 3) (up: 2 hrs) -> 64.207.139.243:80 (distance 0, link: ethernet/modem)
192.168.1.160:41104 - Linux 2.6 (newer, 3) (up: 2 hrs) -> 74.125.228.101:80 (distance 0, link: ethernet/modem)
192.168.1.160:53454 - Linux 2.6 (newer, 3) (up: 2 hrs) -> 173.194.74.189:443 (distance 0, link: ethernet/modem)
192.168.1.160:54451 - Linux 2.6 (newer, 3) (up: 2 hrs) -> 173.194.68.189:443 (distance 0, link: ethernet/modem)
192.168.1.160:54915 - Linux 2.6 (newer, 3) (up: 2 hrs) -> 64.207.139.243:80 (distance 0, link: ethernet/modem)
```

Clear-text passwords (/var/log/recon/dsniff.log)

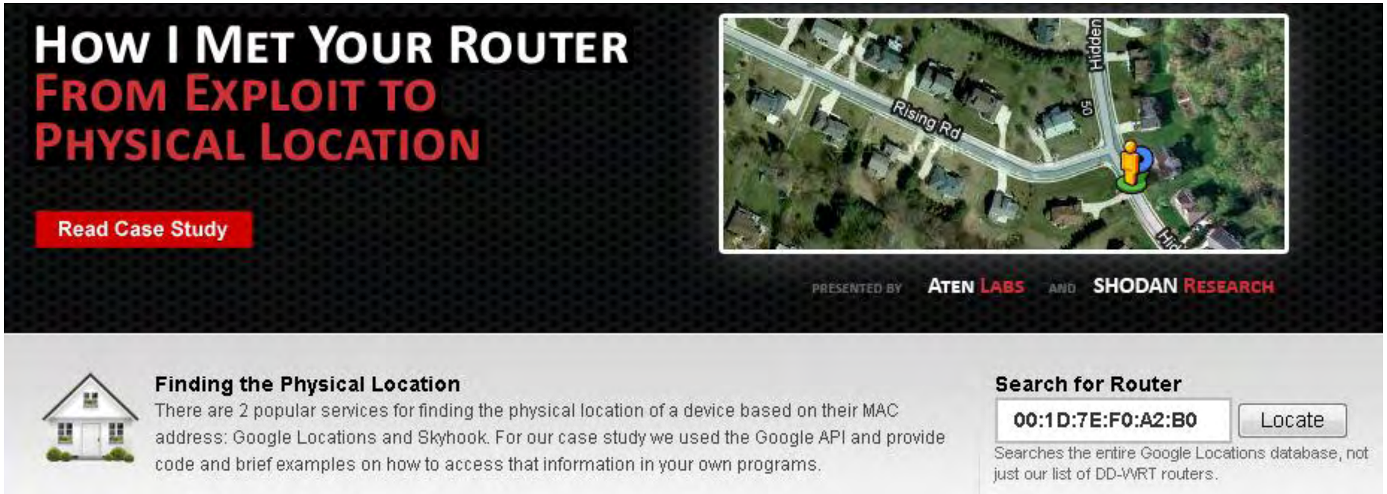
- Onboard high-gain 802.11b/g/n wireless.
- Onboard high-gain Bluetooth (up to 1000').
- Onboard dual-Ethernet.
- Fully functional 120/240v AC outlets!.
- Includes 16GB internal disk storage.
- Includes external 3G/GSM adapter.
- Includes all release 1.1 features.
- Fully-automated NAC/802.1x/RADIUS bypass.
- Out-of-band SSH access over 3G/GSM cell networks!.
- Text-to-Bash: text in bash commands via SMS! .
- Simple web-based administration with "Plug UI".
- One-click Evil AP, stealth mode, & passive recon.
- Maintains persistent, covert, encrypted SSH access to your target network [Details].
- Tunnels through application-aware firewalls & IPS.
- Supports HTTP proxies, SSH-VPN, & OpenVPN.
- Sends email/SMS alerts when SSH tunnels are activated.
- Preloaded with Debian 6, Metasploit, SET, Fast-Track, w3af, Kismet, Aircrack, SSLstrip, nmap, Hydra, dsniff, Scapy, Ettercap, Bluetooth/VoIP/IPv6 tools, & more.
- Unpingable and no listening ports in stealth mode.

Searching for Devices online



EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.


HOW I MET YOUR ROUTER
FROM EXPLOIT TO
PHYSICAL LOCATION

Finding the Physical Location

There are 2 popular services for finding the physical location of a device based on their MAC address: Google Locations and Skyhook. For our case study we used the Google API and provide code and brief examples on how to access that information in your own programs.

Search for Router

00:1D:7E:F0:A2:B0 Locate

Searches the entire Google Locations database, not just our list of DD-WRT routers.

www.shodanhq.com

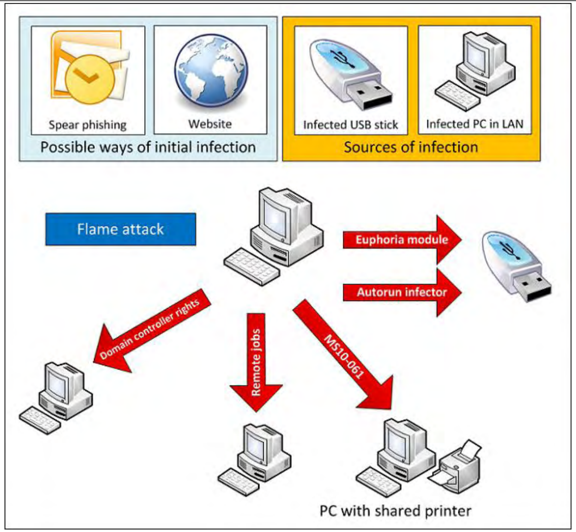
Duqu, Flame, Operation Shady RAT, Gauss …

Flame can spread to other systems over a local network (LAN) or via USB stick. It can record audio, screenshots, keyboard activity and network traffic.[6] The program also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth-enabled devices. This data, along with locally stored documents, is sent on to one of several **command and control servers** that are scattered around the world. The program then awaits further instructions from these servers.

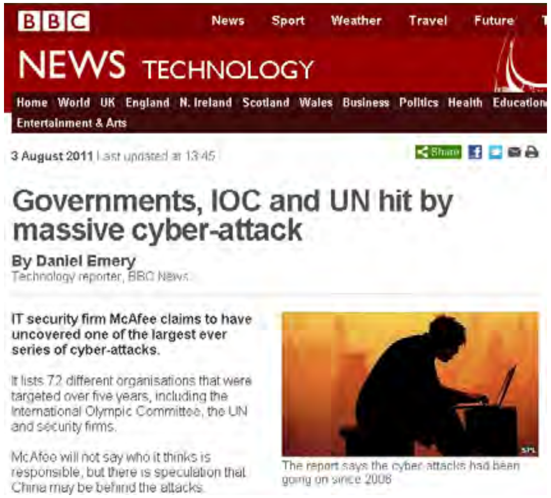
Duqu looks for information that could be useful in attacking industrial control systems. Its purpose is not to be destructive, the known components are trying to **gather information.** However, based on the modular structure of Duqu, special payload could be used to attack any type of computer systems by any means and thus **cyber-physical attacks based on Duqu might be possible**.

Gauss: another example of a cyber-espionage toolkit based on the Flame platform

Source: wikipedia



https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers



3 August 2011 Last updated at 13:45

Governments, IOC and UN hit by massive cyber-attack

By Daniel Emery
Technology reporter, BBC News

IT security firm McAfee claims to have uncovered one of the largest ever series of cyber-attacks.

It lists 72 different organisations that were targeted over five years, including the International Olympic Committee, the UN and security firms.

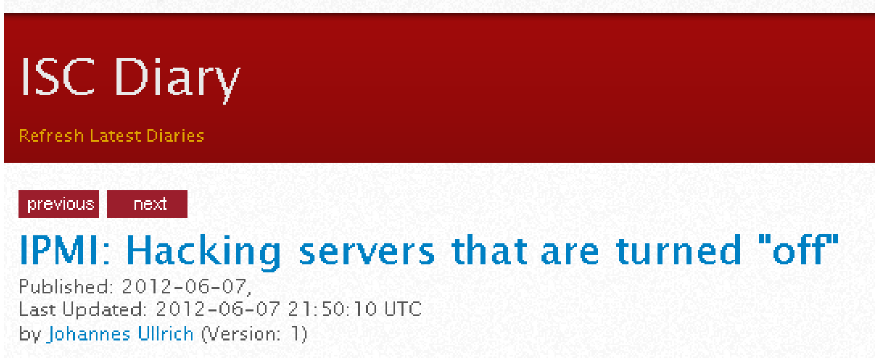
McAfee will not say who it thinks is responsible, but there is speculation that China may be behind the attacks.

The report says the cyber attacks had been going on since 2006

Only always-on devices are under continuous threat…

Let’s turn off the computers / devices … to be secure!

Quiz: Would that work out?



ISC Diary

Refresh Latest Diaries

IPMI: Hacking servers that are turned "off"

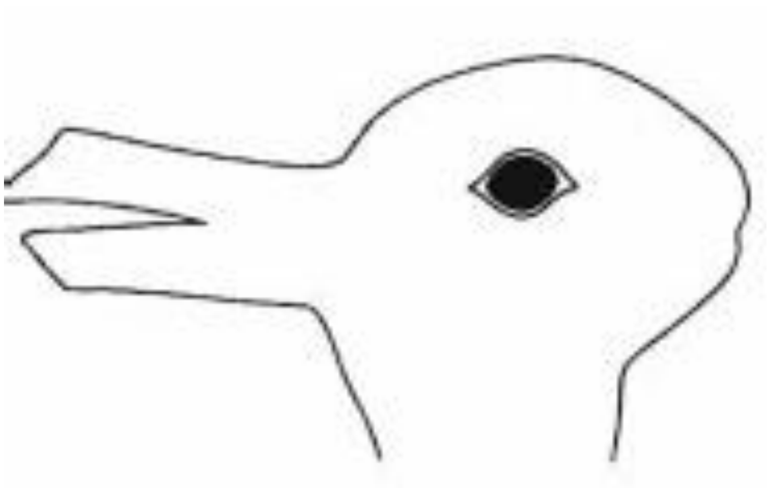
Published: 2012-06-07,
Last Updated: 2012-06-07 21:50:10 UTC
by Johannes Ullrich (Version: 1)

Intelligent Platform Management Interface

- IPMI is active once the server is connected to power. It does not depend on the server to be actually "switched on".
- IPMI is implemented as a specific circuit on the motherboard. Sometimes, you may find it on an optional plugin board. But it does not require CPU, RAM or other components
- It may use an existing network card, and doesn't necessarily need a dedicated network card
- Aimed at remote admin monitoring

Source: https://isc.sans.edu/diary.html?storyid=13399

How do we capture reality when perceptions vary ?



Remember that …

Up to now most security problems in Internet resulted in disturbing services and/or image/money loss …

… but in Cyber-Physical System (CPS) dependent Infrastructures …

the impact might be more real than ever… especially on the physical part!

Most of the CPS driven Industrial Infrastructures (and critical ones) rely on Europe, Japan and US.

Targeted attacks may have devastating effects.

SAP®

www.imc-aesop.eu

ICT4E2B Forum

www.ict4e2b.eu

NOBEL
Neighbourhood Oriented
Brokerage Electricity
and Monitoring System

www.ict-nobel.eu

SAP RESEARCH

Contact:

Stamatis Karnouskos
SAP Research

SAP AG
Vincenz-Priessnitz-Strasse 1
D-76131 Karlsruhe,
Germany

Email: stamatis.karnouskos@sap.com