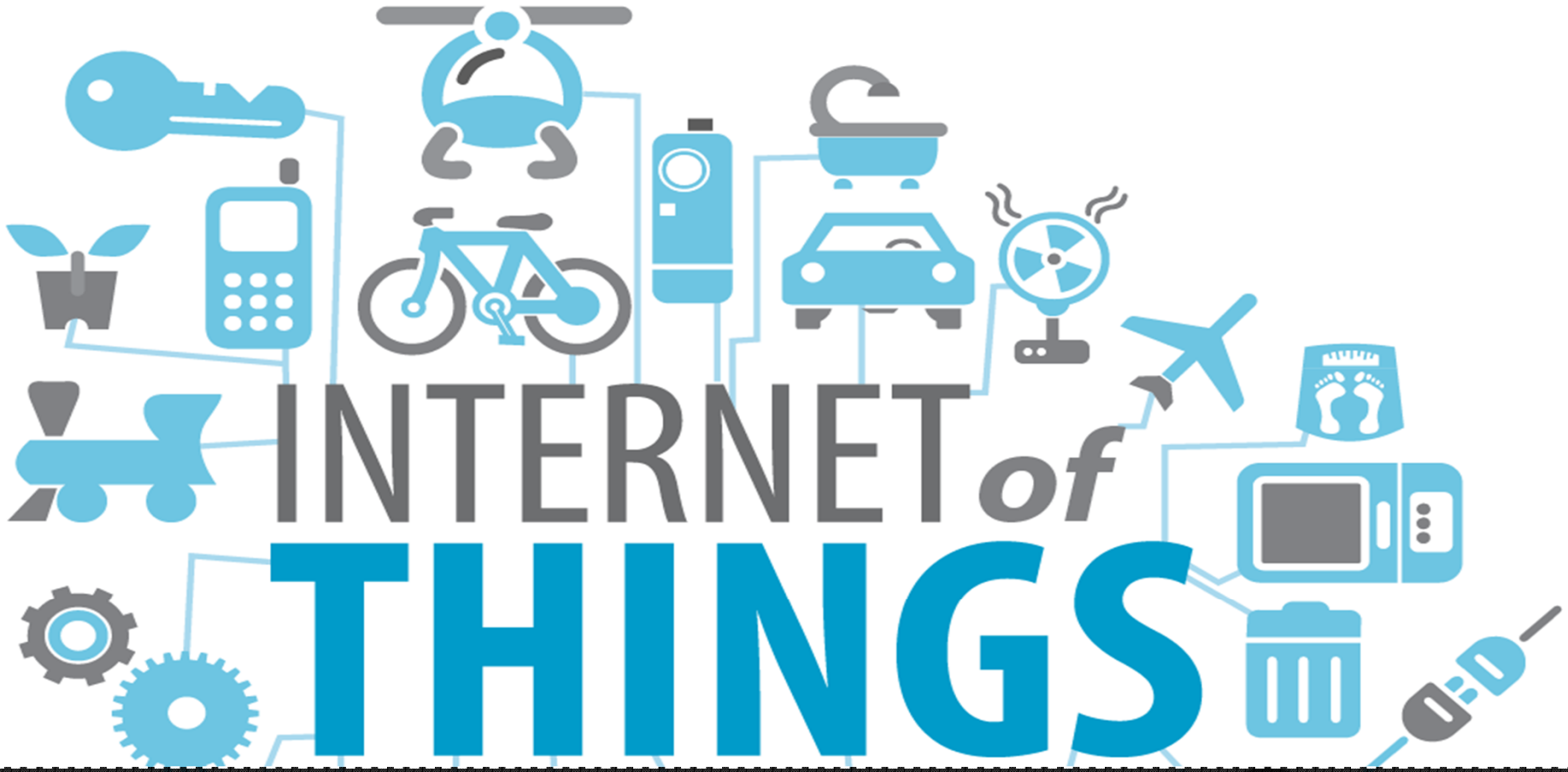


Internet delle cose

ISACA Roma & OWASP Italia
Oltre l'IT Governance Conference

Pierluigi PAGANINI

Roma
12 Dicembre 2014

AGENDA

- The Internet of Things 
- Internet of Things risks 
- Cyber Threats and Security Challenges 
- Under attack 
- Privacy Issues 
- Evolution 
- Conclusions 

The Internet of Things

Source: https://www.youtube.com/watch?v=Qs4OcQNOM34&list=PL18A5A2C4BD2BBB11

The Internet of Things

Let's talk about

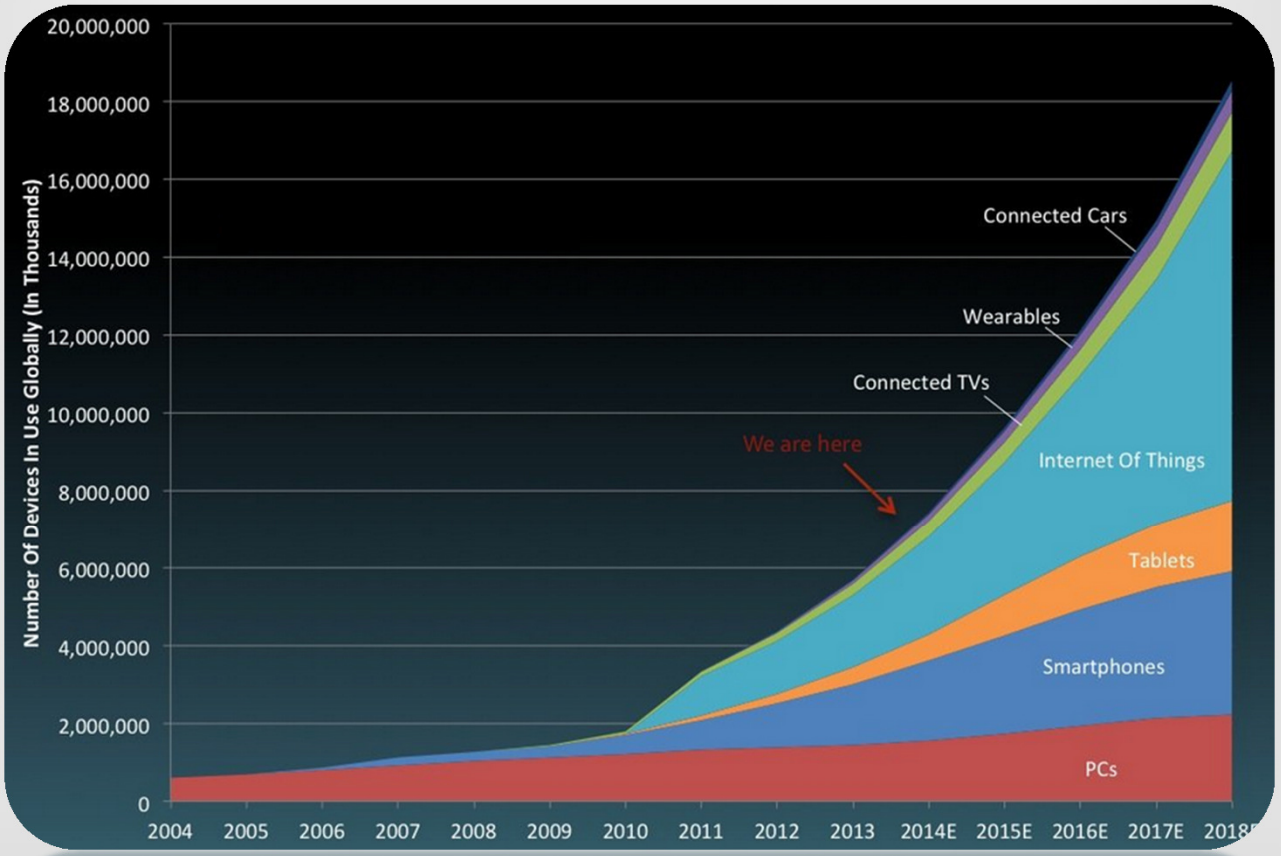
"The Internet of Things (IoT) is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. Things, in the IoT, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, automobiles with built-in sensors, or field operation devices that assist fire-fighters in search and rescue." Wikipedia

- *IoT network resilience to cyber attacks*
- *Individual as a Data cluster*
- *Privacy*
- *Concrete cyber threats*
- *Influencing human behavior*

We are already nodes of a global network

The Internet of Things

IoT today scenario

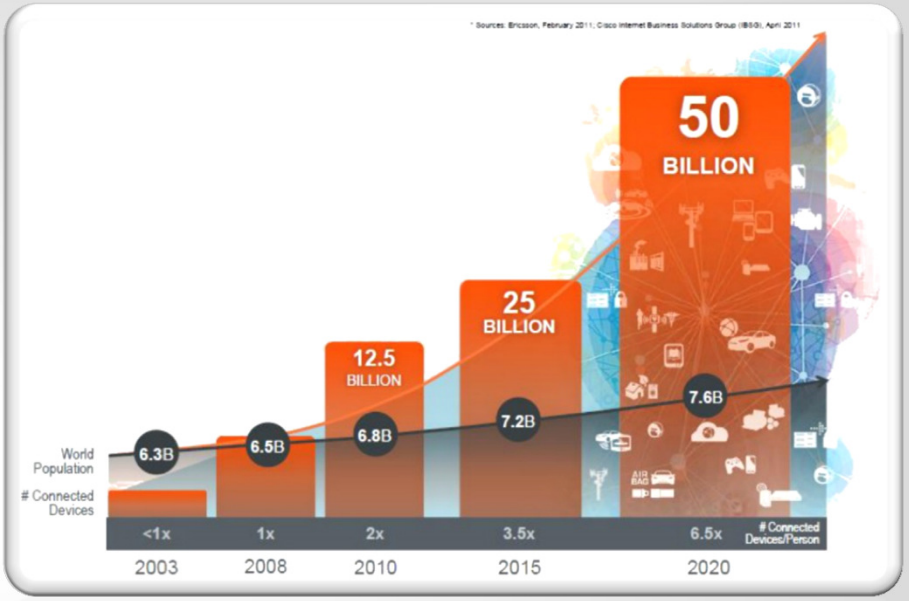


More than 7 billions, exceeding the earth's population

Source: BI Intelligence Estimates

The Internet of Things

IoT diffusion: Forecast

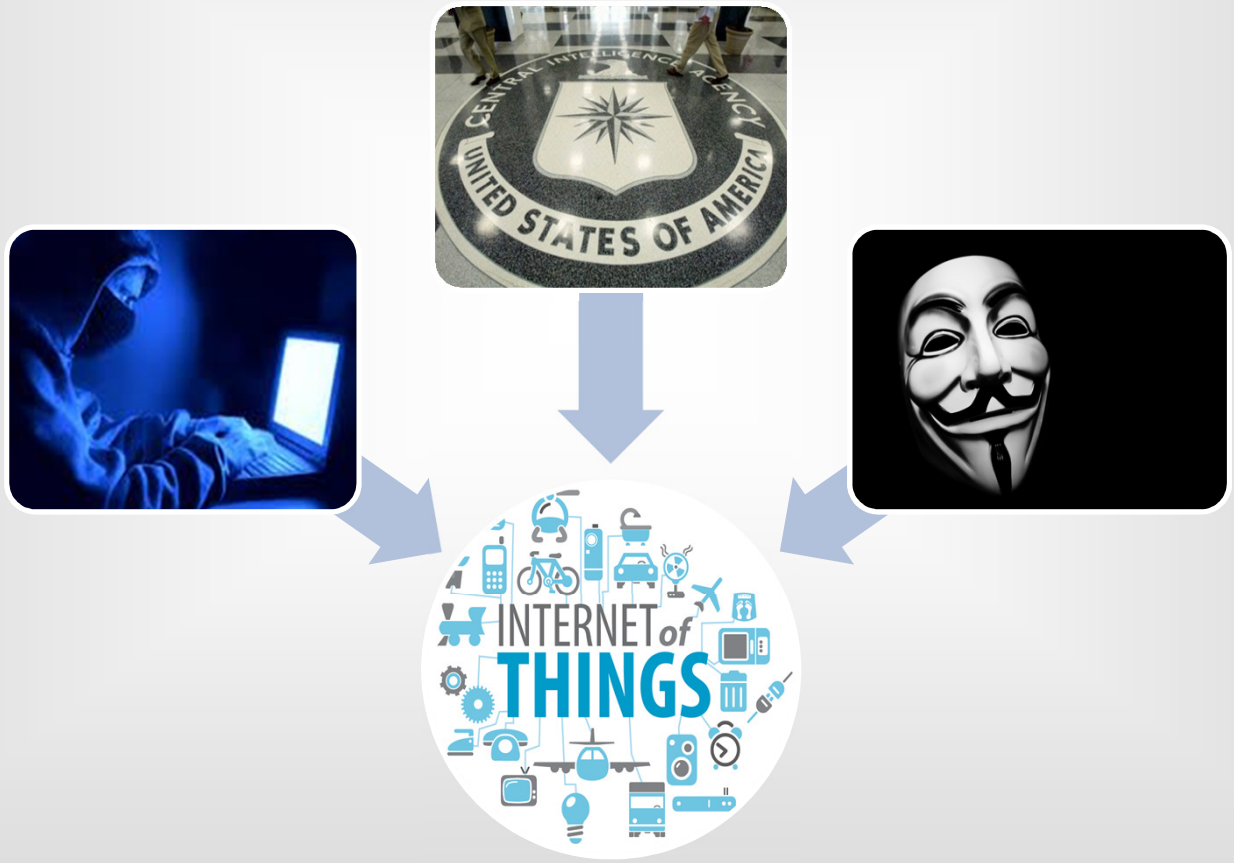


- *50 billion connected devices by 2020*
- *More than 6 connected devices per Person*
- *$1.7 trillion in value added to the global economy in 2019*
- *By 2020 IoT will be more than double the size of the smartphone, PC, tablet, connected car, and the wearable market combined.*
- *Technologies and services generated global revenues of $4.8 trillion in 2012 and will reach $8.9 trillion by 2020, growing at a compound annual rate (CAGR) of 7.9%.*

Connected devices grow up

Internet of Things risks

Threat actors



Threat actors adopt even more sophisticated TTPs

Internet of Things risks

How to exploit a IoT device?

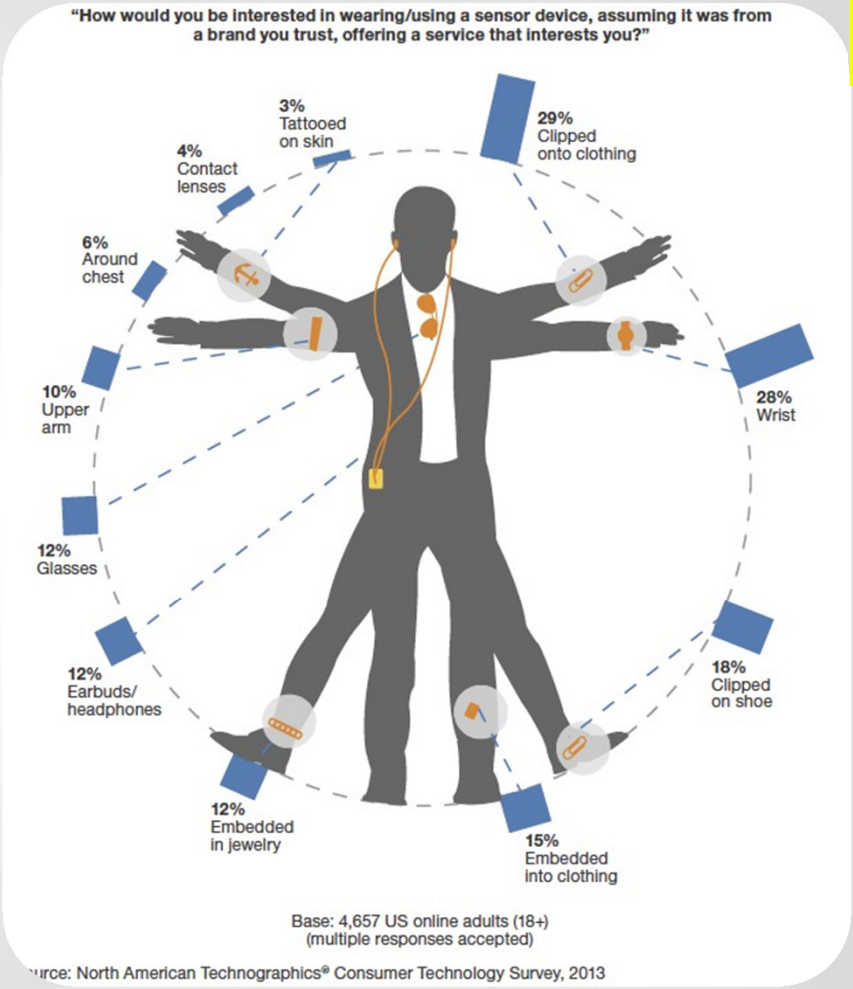
- *DDoS attacks*
- *Botnets and malware based attacks*
- *Weakening perimeters (Objects not designed to be internet-connected)*
- *Data Breaches*
- *Inadvertent breaches*

IoT is dramatically enlarging our attack surface

Internet of Things risks

Individuals as data cluser

- *Wearable devices collect a huge amount of personal data as well as surrounding environment information.*
- *Significant impact on privacy rights of these technologies will require a careful review.*
- *Great concern for Health-related sensitive data (i.e. Medical devices and fitness apps).*
- *Confidential information and easily disclose it to third parties.*
- *A Threat for enterprise perimeter.*



We are a node of a global network

Internet of Things risks

The OWASP Internet of Things Top 10 - 2014

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

The project walks through the top ten security problems that are seen with IoT

Under attack

Botnets are already a major threats …

- *A ThingBot is a botnet consisting of devices within the Internet of things.*
- *Vulnerable or infected appliances that are connected to the Internet can potentially pose a risk to corporate networks (Kaspersky).*
- *Number of attacks against Routers, SmartTV, network-attached storage devices, gaming consoles and various types of set-top boxes is increasing.*
- *Many set-top boxes runs on embedded linux or apache operating systems of ARM-like microcomputers.*

Oops … my refrigerator is sending spam messages

Under attack

Principal abuses of IoT devices

Computational capabilities, increasing capabilities of microcomputers and Internet connection makes IoT devices a privileged attack tool for hackers.

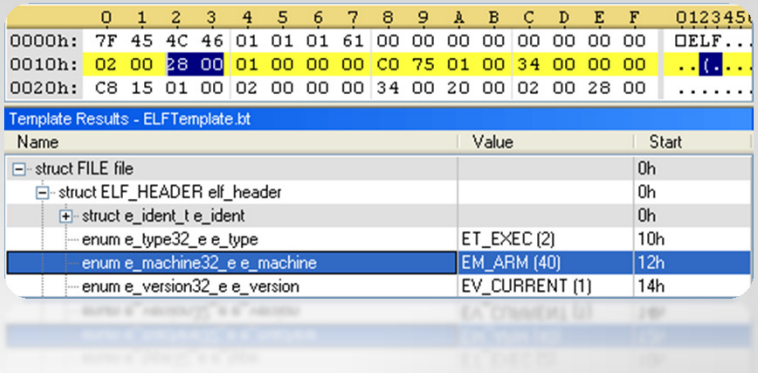
IoT devices could be used to:

- *Send Spam.*
- *Coordinate an attack against a critical infrastructure.*
- *Serve a malware.*
- *Work as entry point within a corporate network.*

Potentiality of IoT devices is unlimited, like their abuses

Under attack

A Linux worm designed to target IoT devices



- *In November 2013 Symantec detected the worm Linux.Darlloz exploiting the PHP vulnerability CVE-2012-1823 to propagate itself.*
- *The Linux.Darlloz infected Home internet kits with x86 chips (i.e.routers) and were discovered variant for ARM, PPC, MIPS and MIPSEL architectures.*
- *The worm:*
  - *generates random IP addresses and attempts to use commonly used credentials to log into the target machine.*
  - *It sends HTTP POST requests specifically crafted, once compromised the target it downloads the worm from a C&C server and starts searching for other targets.*
  - *Once the worm has compromised a device, it kills off access to any Telnet services running.*
- *Change default settings, adopt strong password, keep updated the software and firmware.*

Security firms detect first sample of IoT malware … a new business opportunity

Under attack

One of the first cases observed

- *Proofpoint discovered more Than 750,000 Phishing and SPAM Emails Launched From "Thingbots" thingBotscould be used in an attack against a critical infrastructure from anywhere in the globe*
- *Cyber criminals sent in bursts of 100,000, three times per day, targeting Enterprises and individuals worldwide*
- *More than 100,000 Refrigerators, Smart TVs and other smart household appliances have been hacked.*
- *No more than 10 emails were initiated from any single IP address.*

The strength of large numbers

Under attack

Spike botnet runs DDoS from IoT devices

- *Akamai spotted a Spike malware which is used to run DDoS attacks through desktops and IoT devices.*
- *Spike toolkit is able to to generate an ARM-based payload*
- *The spike botnet was composed by routers, smart thermostats, smart dryers, freezers, Raspberry Pi and other IoT devices.*
- *Spike botnet composed by 12,000 - 15,000 devices (sept 2014).*
- *One of the attack clocked 215 Gbps and 150 million packets per second (Mpps).*
- *SNORT signature analysis suggested to mitigate application-layer GET flood attacks.*

Oops … my refrigerator is sending spam messages

Under attack

Hacking smartwatch

- *Data sent between the Smartwatch and an Android mobile phone could be intercepted.*
- *An attacker that could be able to decode users' data, including text messages to Google Hangout chats and Facebook conversations.*
- *Bluetooth communication between most Smart watches and Android devices relies on a six digits PIN.*
- *Easy to crack with a brute-force attack.*
- *Mitigate the attack with NFC pairing procedure in pin code exchange or the use of passphrases.*
- *PoC with Samsung Gear Live smartwatch and Google Nexus 4*

Hacking wearable devices

Under attack

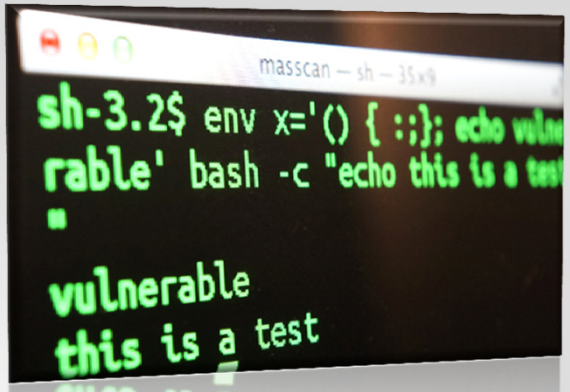
Hacking Smart meters

- *Smart meters can be hacked to hit the National power network*
- *In Spain, millions of Smart meters, are susceptible to cyberattack due to lack of proper security controls. (researchers, Javier Vazquez Vidal and Alberto Garcia Illera).*
- *8 million smart meters are deployed in Spain (30 percent of households).*
- *Attackers could cause a blackout or conduct fraudulent activities (i.e. billing frauds).*
- *Poorly protected credentials stored in the smart meters.*
- *Attackers could modify device unique ID to impersonate other customer or use the smart meter for launching attacks against the power network.*

Smart meters can be hacked to hit the National power network

Under attack

The Bashbug (Shellshock) Bug



- *Bash Bug (CVE-2014-6271) is a critical flaw in the widely used Unix Bash shell disclosed on 24 September 2014. Many IoT devices have Linux embedded and could not be easily patched.*
- *Many Internet-facing services use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands.*
- *Attackers could gain unauthorized access to a computer system and execute arbitrary code remotely.*
- *The impact is incredibly high because there are a lot of embedded devices that use CGI scripts (i.e. home appliances and wireless access points). It's asy to exploit.*
- *With the number of Internet-facing devices vulnerable to this, it would be very easy for an attacker to turn this into a worm*

This is potentially worse than Heartbleed

Cyber Threats and Security Challenges

Securing the IoT world

- *Demand of connectivity for the Internet of Things (IoT) exploding.*
- *The global network must be able to securely and efficiently handle all these connections.*
- *Lack of standardization in the IoT market.*
- *Every single connection could make networks vulnerable.*
- *Every connected device has a network address. Internet Protocol (IPv6) extends the addressing space*
- *DNS will play an even more central role with the diffusion of M2M connections.*
- *Organizations will need to improve security and prevent DDoS and cache poisoning attacks.*

Cyber Threats and Security Challenges

RFC 7123 – Security Implications of IPv6 on IPv4 Networks

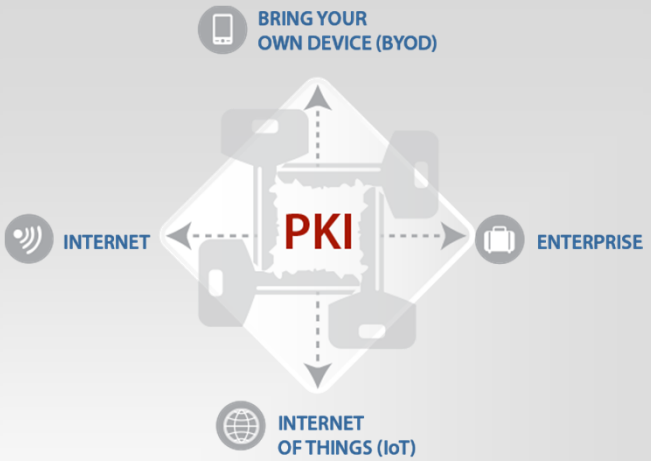
- *Security exposure in enterprise networks resulting from unplanned use of IPv6 on such networks.*
- *Native IPv6 support and/or IPv6 transition/coexistence technologies could be leveraged by local or remote attackers for a number of (illegitimate) purposes.*
- *Attack/incident scenarios include:*
  - A Network Intrusion Detection System (NIDS) might be prepared to detect attack patterns for IPv4 traffic, but might be unable to detect the same attack patterns when a transition/coexistence technology is leveraged for that purpose.
  - An IPv4 firewall might enforce a specific security policy in IPv4, but might be unable to enforce the same policy in IPv6
  - Some transition/coexistence mechanisms could cause an internal host with otherwise limited IPv4 connectivity to become globally reachable over IPv6, therefore resulting in increased (and possibly unexpected) host exposure
  - IPv6 support could, either inadvertently or as a result of a deliberate attack, result in Virtual Private Network (VPN) traffic leaks if IPv6-unaware VPN software is employed by dual-stacked hosts.

Mitigation by enforcing security controls on native IPv6 traffic and on IPv4-tunneled IPv6 traffic

Source http://www.internetsociety.org/deploy360/resources/rfc-7123-security-implications-of-ipv6-on-ipv4-networks/

Cyber Threats and Security Challenges

IoT and PKI



- *IoT devices communicate among themselves with little human interaction, mutual authentication is a crucial aspect of the paradigm.*
- *Prevent leakage of personal information and harmful actuating tasks by means of peer authentication and secure data transmission.*
- *Recent attacks like the "smart" light bulb password leaks, hacks of Foscam baby monitors, Belkin home automation systems, and hacks of smart cars systems are just the beginning.*
- *PKI-based solutions could help to secure exchanging information across the Internet and mutual authenticate the actors.*
- *PKI is already being used to address problems similar to the ones the Internet.*

PKI could help to improve security of the Internet of Things

Privacy Issues

Mapping Top 10 Privacy Risks on the IoT paradigm

P1 Web Application Vulnerabilities
P2 Operator-sided Data Leakage
P3 Insufficient Data Breach Response
P4 Insufficient Deletion of personal data
P5 Non-transparent Policies, Terms and Conditions
P6 Collection of data not required for the primary purpose
P7 Sharing of data with third party
P8 Outdated personal data
P9 Missing or Insufficient Session Expiration
P10 Insecure Data Transfer

Improving privacy by design, privacy impact assessments, and privacy enhancing technologies to promote trust in IoT paradigm.

Privacy Issues

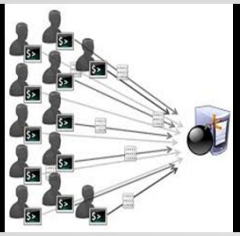
Mapping Top 10 Privacy Risks on the IoT paradigm

- *The company managing the App used through the wearable technology will be subject to the privacy law of the country where the device/user is located even in the case of non-European entities and it will not be sufficient to merely ask for a privacy consent.*

- *Countries like Italy that require a written privacy consent for the processing of sensitive data and allow the data processing only within the limits of a so called "general authorization" issued by the Data Protection Authority*

- *Biometric data includes any data obtained from physical or behavioral features of a person. The Italian Data Protection Authority issued in relation to biometric data very stringent requirements as to the modalities of collection, the security measures to be implemented for their storage and the maximum term of storage.*

Improving privacy by design, privacy impact assessments, and privacy enhancing technologies to promote trust in IoT paradigm.



Privacy Issues

Unintended Consequences of the IoT

- *Loss of privacy*
- *Amplification of surface of attack.*
- *Unforeseen spill-over effects (i.e. Network congestions, power blackout).*
- *Social changes, such as growing new professionals or amplifying the digital divide.*
- *Loss of ability to maintain understanding and control.*
- *Developing of new capability of Pre-crime forecasting.*

Causes and effects are not always predictable

Evolution

Today, Tomorrow

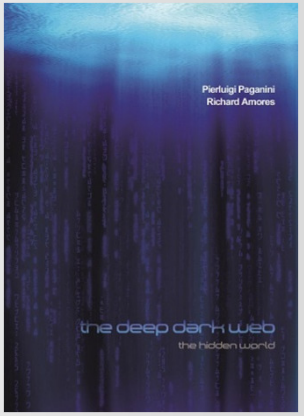
- The IoT is propelled by an exceptional convergence of trends (mobile phone ubiquity, open hardware, big data, the resurrection of AI, cloud computing, 3D printing and crowdfunding). [Techcrunch]
- We're rapidly evolving toward a world where just about everything will be connected.
- Privacy and security must be addressed.
- Growing Business opportunity for startup and big companies.
- Number of cyber attacks will rapidly increase.
- IoT devices are a privileged target as highlighted recently by the Europol, the European agency citing a December 2013 report by US security firm IID, warned of the first murder via "hacked internet-connected device" by the end of 2014."


Thank you

Conclusions

Pierluigi Paganini

About Pierluigi Paganini:
Chief Information Security Officer, Security Evangelist, Security Analyst and Freelance Writer.
Security expert with over 20 years experience in the field. Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led me to found the security blog "Security Affairs". Today I am CISO for Bit4id company, firm leader in identity management, and I work as a writer with some major publications in the security field such as Cyber War Zone, Infosec Island, The Hacker News, Hakin9, PenTesting Magazine, Audit & Standard Mag. and Independent of Malta Journal. Author of the incoming book «The Deep Dark Web»



Ing. Pierluigi Paganini

Chief Information Security Officer Bit4id

ppa@bit4id.com

www.bit4id.com

Founder Security Affairs

http://securityaffairs.co/wordpress

pierluigi.paganini@securityaffairs.co