PECB

When Recognition Matters.

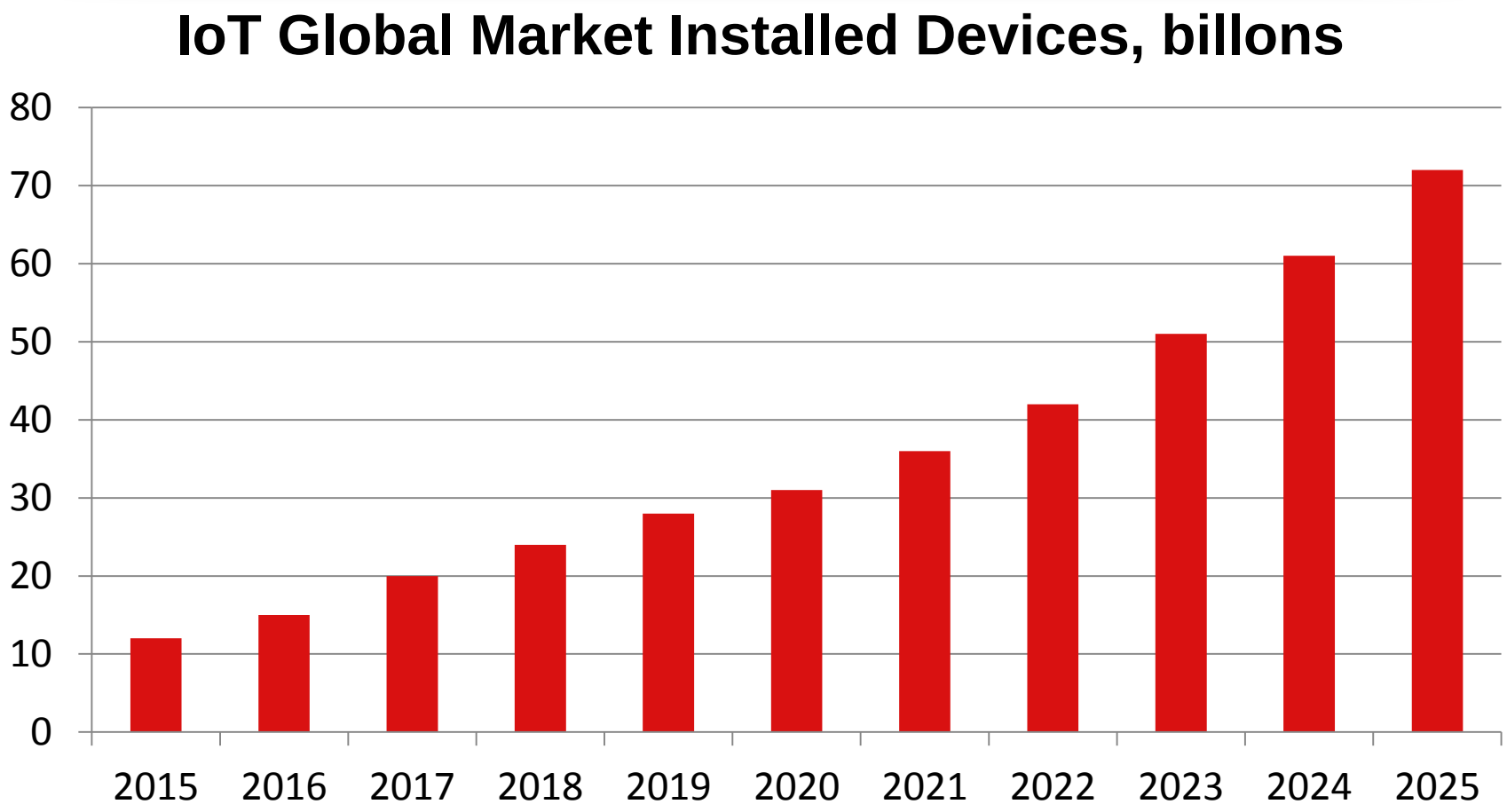
IoT Security: A comprehensive analysis on existing IoT security frameworks

Eric Lachapelle, CEO
www.pecb.com

Agenda

- **IoT Overview**
- **Need for IoT Security Certification**
- **Current IoT Security Frameworks - Principles**
- **Current IoT Security Frameworks - Areas of Review**
- **Conclusion**

IoT Devices Overview



Forbes, 2016-11-27

Expenditure

USD

470

Billion

Expected IoT revenues – 2020

Including: hardware, software & solutions

IoT Security Overview

A recent study by HP found alarming security statistics in the IoT space.
Of 10 popular devices tested:

70%
Contained security exposures

25
Holes or risks of compromising the home network, on average, found for each device

80%
Did not require passwords of sufficient complexity and length

90%
Collected at least one piece of personal information

70%
Allowed an attacker to identify a valid account through account enumeration

IoT Security Overview

Security incidents on IoT increased 152% from 2015 to 2016

More Smart Devices

=

More Sensitive Data

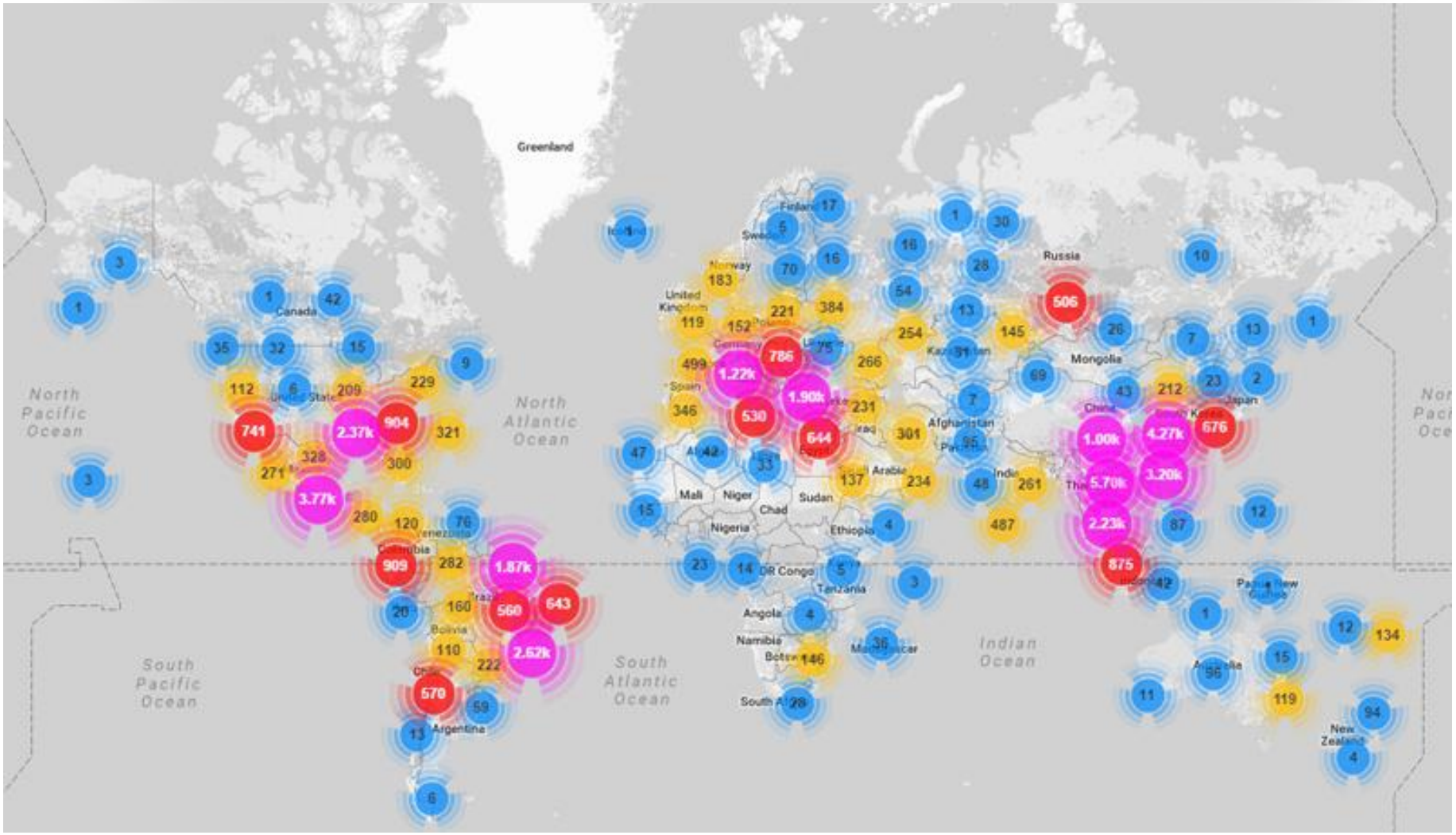
=

Higher Risk

Mirai

- Mirai (Japanese for "the future", 未来)
- Malware that primarily targets online consumer devices such as IP cameras and home routers.
- Mirai scans and identifies vulnerable IoT devices using common factory default usernames and passwords, and logs into them to infect them with the Mirai malware.
- Once infected, the device will monitor a command and control server which indicates the target of an attack.

Geo-locations of all Mirai-infected IoT devices revealed so far



Mirai

- Mirai was used, alongside BASHLITE, in the DDoS attack on 20 September 2016 on the Krebs on Security website.

- At the end of November 2016, approximately 900,000 routers, from Deutsche Telekom and produced by Arcadyan, were crashed due to failed exploitation attempts by a variant of Mirai.

Current Product Security Frameworks/Certifications

- Common Criteria (ISO/IEC 15408)
- FIPS 140-2
- ISO/IEC 27034

Common Criteria (ISO/IEC 15408)

Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner).

Evaluation Assurance Level :

EAL1: Functionally Tested
EAL2: Structurally Tested
EAL3: Methodically Tested and Checked
EAL4: Methodically Designed, Tested and Reviewed
EAL5: Semiformally Designed and Tested
EAL6: Semiformally Verified Design and Tested
EAL7: Formally Verified Design and Tested

FIPS 140-2

- The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.
- FIPS 140-2 defines four levels of security, simply named "Level 1" to "Level 4".
- The Cryptographic Module Validation Program (CMVP) is a joint American and Canadian security accreditation program for cryptographic modules. Accreditations are handled by third-party laboratories that are accredited as Cryptographic Module Testing laboratories.

ISO/IEC 27034

- ISO/IEC 27034 offers guidance on information security to those specifying, designing and programming or procuring, implementing and using application systems. The aim is to ensure that computer applications deliver the desired or necessary level of security in support of the organization's Information Security Management System, adequately addressing many ICT security risks.
- ISO/IEC 27034-4 was intended to describe an application security validation and certification process to assess and compare the 'level of trust' of an application system. It has been canceled, then resurrected, due for publication in 2019.

The Situation

- There is a number of solutions to certify the security of IT products.
- None of them designed specifically for IoT.

- There are however several initiatives to identify specific security issues with IoT, some of them that will lead or contribute to IoT Security Certification.

Current IoT Security Frameworks - Principles

- Strategic Principles for Securing the IoT – U.S. Department of Homeland Security
- IoT Security & Privacy Trust Framework - Online Trust Alliance (OTA)
- Guidance and Principles of IoT Security – OWASP

U.S. Department of Homeland Security

Strategic Principles for Securing the Internet of Things (IoT) – U.S. DHS

This document sets principles that offer stakeholders a way to organize their thinking about how to address IoT security challenges. These principles include:

- Incorporation of Security at the design phase
- Advance Security updates and vulnerability management
- Build on proven security practices
- Prioritize security measures according to potential impact
- Promotion of transparency across IoT
- Careful and deliberate connection

Online Trust Alliance

OTA

Online Trust Alliance

IoT Security & Privacy Trust Framework 2.0 – Online Trust Alliance

- The IoT Trust Framework includes 37 strategic and measurable principles, divided into four key areas, which incorporate earlier listed considerations together with significant learnings from field testing, the growing threat landscape and feedback from industry leaders and associated efforts.
  - Security principles (1-9)
  - User access and credentials (10-14)
  - Privacy disclosure and transparency (15-30)
  - Notifications and related best practices (31-37)

IoT Security & Privacy Trust Framework 2.0 – Online Trust Alliance

The framework consists of 4 key areas which include a mix of essential requirements and recommendations. These include:

- Security principles (1-9)
- User access and credentials (10-14)
- Privacy disclosure and transparency (15-30)
- Notifications and related best practices (31-37)

OWASP

OWASP

Open Web Application Security Project

OWASP – Guidance and Principles of IoT Security

In the document IoT Security Guidance, OWASP provides security guidance for IoT to manufacturers, developers and consumers and categorizes the IoT security in 10 principles. These principles include:

- Insecure Web Interface
- Insufficient Authentication/Authorization
- Insecure Network Services
- Lack of Transport Encryption
- Privacy Concerns
- Insecure Cloud Interface
- Insecure Mobile Interface
- Insufficient Security Configurability
- Insecure Software/Firmware
- Poor Physical Security

Common elements - Principles

- Authorization and Authentication
- Promotion of Transparency
- Vulnerability Management
- Security principles and related best practices

Current IoT Security Frameworks - Areas of Review

- IoT Security Foundation
- NIST SP 800-183 – Networks of ‘Things’
- Industrial Internet of Things Volume G4: Security Framework – Industrial Internet Consortium (IIC)
- Cloud Security Alliance - Security Guidance for Early Adopters of the Internet of Things (IoT)

Common elements – Areas of Review

- Cloud Security
- Encryption
- Physical and hardware based security
- Software updates
- Security by design
- Network Security
- Supply chain security

Conclusion

IoT Security Certification will probably be articulated among two phases:

- Phase 1: an onsite audit of the management system that led to the development of the device, including if best practices were followed, how encryption and updates are managed, how authentication is based…

- Phase 2: a lab-based review of the product, to validate that the product fulfills are series of technical requirements based on a pre-determined set of requirements.

Contact Us

+1-844-426-7322

customer@pecb.com

Help Centre