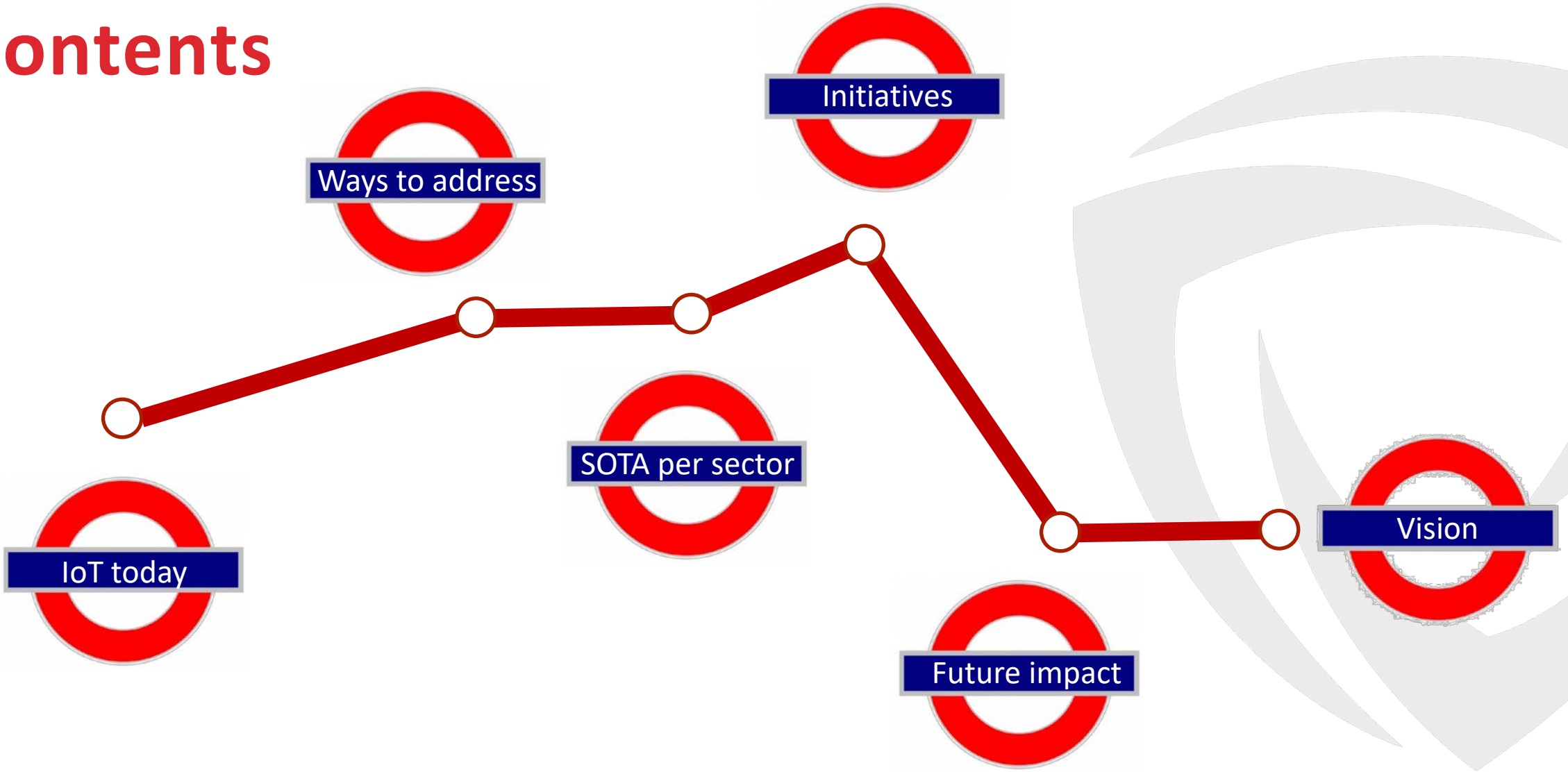
Towards a base security level in IoT

a deployment and regulatory perspective

Erwin Jansen, Secura

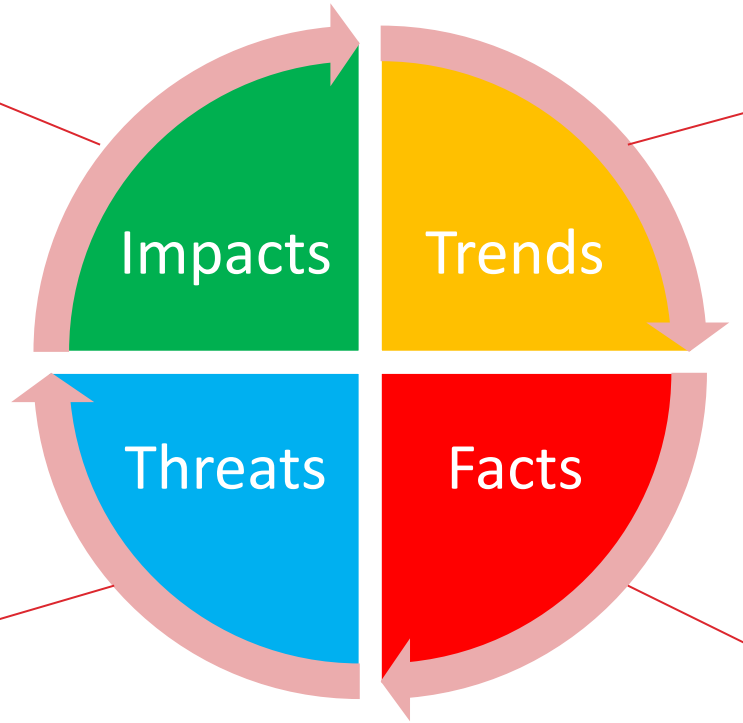
Secura

Contents


Initiatives
Ways to address
SOTA per sector
IoT today
Vision
Future impact

IoT evolution cycle

Successful attacks are a reality

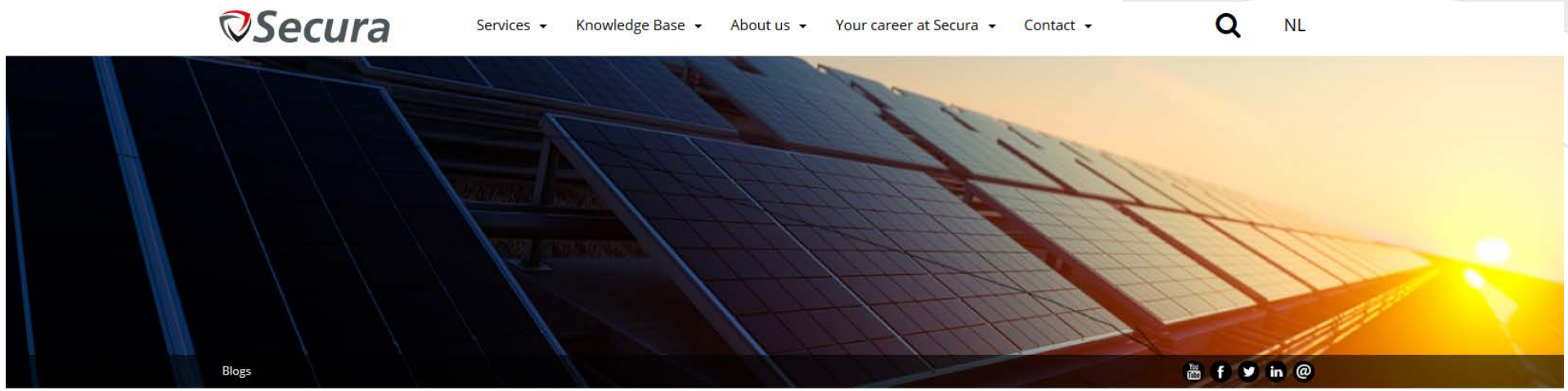


IoT is everywhere

Yes, so many attack paths

The increase rate of IoT is impressive, across all sectors

Still hot and happening…



IoT Solar Inverters & Trickle-Down Vulnerabilities

Blog post 3 September 2019, by Jos Wetzels, Principal Security Consultant at Secura

In this blog post we'll delve into the insecure configuration and OTA firmware update protocols of a popular Chinese manufacturer of Wi-Fi modules and explore how IoT vulnerabilities trickle down a (very opaque) supply chain by starting with the 'junk hacking' of a single vendor's solar inverter Wi-Fi kit and following the thread upstream to see how these same vulnerabilities end up in very different products from very different OEMs with very different, and potentially dangerous, impacts.

This story started when a friend of mine was driving around the middle of nowhere and saw a lot of open wireless access points pop up, all with similar SSIDs starting with a prefix string of 'AP_' followed by 10 digits. Given that open access points have become far more rare than they were a decade ago, this understandably piqued his interest. While visiting a friend's place he happened to spot a similar SSID and noticed a small device with an antenna hooked up to an Omnik solar inverter. After connecting to the open AP, it turned out to indeed belong to the Wi-Fi kit and allowed anyone connected to it and logged in (using default admin:admin credentials) access to inverter configuration and any other networks the kit was hooked up to. At this point, he contacted me in order to figure out what exactly was going on and whether dozens or hundreds of solar inverters across the country were potentially similarly exposed.

Secura

Addressing security

No process in place

Claim

Compliance

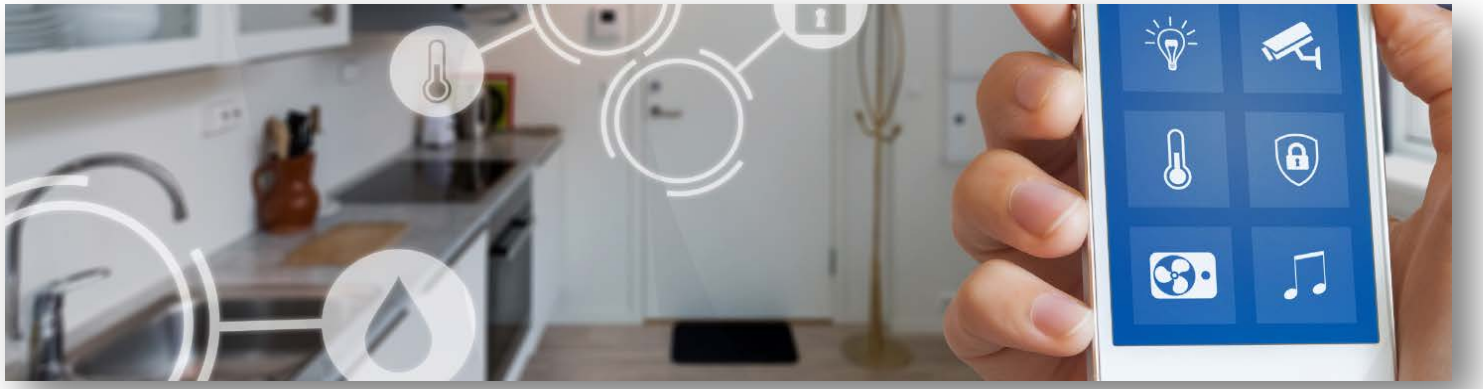
Certification

Harmonization

What is State-Of-The-Art?

Standardization - *Consumer IoT*

Consumer IoT	Current state
Regulations	Currently none
Certification schemes	Common Criteria (general IT products), no dedicated IoT scheme in place
Domain specific standards and publications	• ETSI TS 103 645 • IEC 62443 • UL 2900 • IoT Security Foundation • GSMA



Standardization - *Automotive*

Automotive	Current state	
Regulations	Currently in preparation (UNECE)	
Certification schemes	Common Criteria (general IT products), no dedicated automotive scheme in place	
Domain specific standards and publications	International: ISO 21434	
	US: • SAE J3061 • Department of Transportation Best Practices	EU: • ENISA “Cybersecurity and resilience of smart cars”

Standardization - *ICS*

Industrial Control Systems	Current state
Regulations	Currently none
Certification schemes	IECEE, ISASecure, Common Criteria (general IT products)
Domain specific standards and publications	• IEC 62443 • UL 2900

Standardization - *Medical devices*

Medical devices	Current State
Regulations	• USA: FDA • EU: Medical Devices Regulation
Certification schemes	IECEE, UL CAP
Domain specific standards and publications	• IEC 62443 • UL 2900

Standardization - *Network and Telecom eq*

Network and Telecom equipment	Current state
Regulations	Currently not in place
Certification schemes	Common Criteria (general IT products), no dedicated network products scheme in place
Domain specific standards and publications	• IEC 62443 • Common Criteria Network Devices Protection Profile

Conclusion – SOTA standardization

- **Great deal of fragmentation** in available standards and publications
- **Regulations lacking** or just in development
- **Lack of domain-specific certification** schemes
- All of these are **real issues** in the adoption of standards

Which initiatives are taken?

EU Cybersecurity act

EUROPEAN UNION AGENCY FOR CYBERSECURITY

- Main current EU driver for cybersecurity
- Voted and adopted in June 2019
- EU-wide certification schemes, with mutual recognition among EU states
- Covering products, processes, organizations
- Basic, Substantial and High assurance levels

EU Cybersecurity act

What concrete initiatives can we expect?

EU Cybersecurity act

- First harmonized schemes are being currently drafted
- **Common Criteria (SOG-IS)**, **Cloud**, **ICS components** in first round
- 5G, **Consumer IoT** in second round
- First round schemes expected to be live in 2020

EU Cybersecurity act

What will happen after the schemes are live?

EU Cybersecurity act

1. Other (overlapping) national schemes will not be introduced
2. A single certification, resulting in EU recognition
3. Aim for maximum re-use of existing schemes and standards
4. Certification voluntary, however could become mandatory per sector (Ex. for Smart Meters)

Other emerging initiatives

- UNECE regulations for automotive
  - Cybersecurity and Software Updates
  - Harmonized vehicle type approval across UN countries
- Smart meters Protection Profile
- FDA approval program for medical devices

Remember the current fragmentation and issues of the SOTA…

Will the new certification initiatives change this?

Harmonizing certification across sectors

- Once in place, the new initiatives will address many high-focus sectors
- The established schemes will become the “default” option

What do we expect?

Certification vision for coming years

- ICS components EU -> EU ICS components scheme
- ICS components international -> IECEE certification

- Network devices EU-> EU SOG-IS scheme
- Network devices international -> Common Criteria

- Smart Meters EU -> EU SOG-IS scheme (see initiative for specific PP)
- Smart Meters international -> Common Criteria

Certification vision for coming years

- Consumer IoT EU -> EU IoT scheme
- Consumer IoT international -> UL CAP/ IoTSF?

- Automotive -> UNECE regulations

- Medical devices USA -> FDA approval program
- Medical devices international -> UL CAP/ IECEE certification

Questions?

Erwin.Jansen@secura.com

Secura