Securing the connected world of tomorrow

Jason S. Boswell, CISSP

Sr. Principal Technical BDM

The Future of IoT Security Design:

- Simple
- Predictable
- Enabling

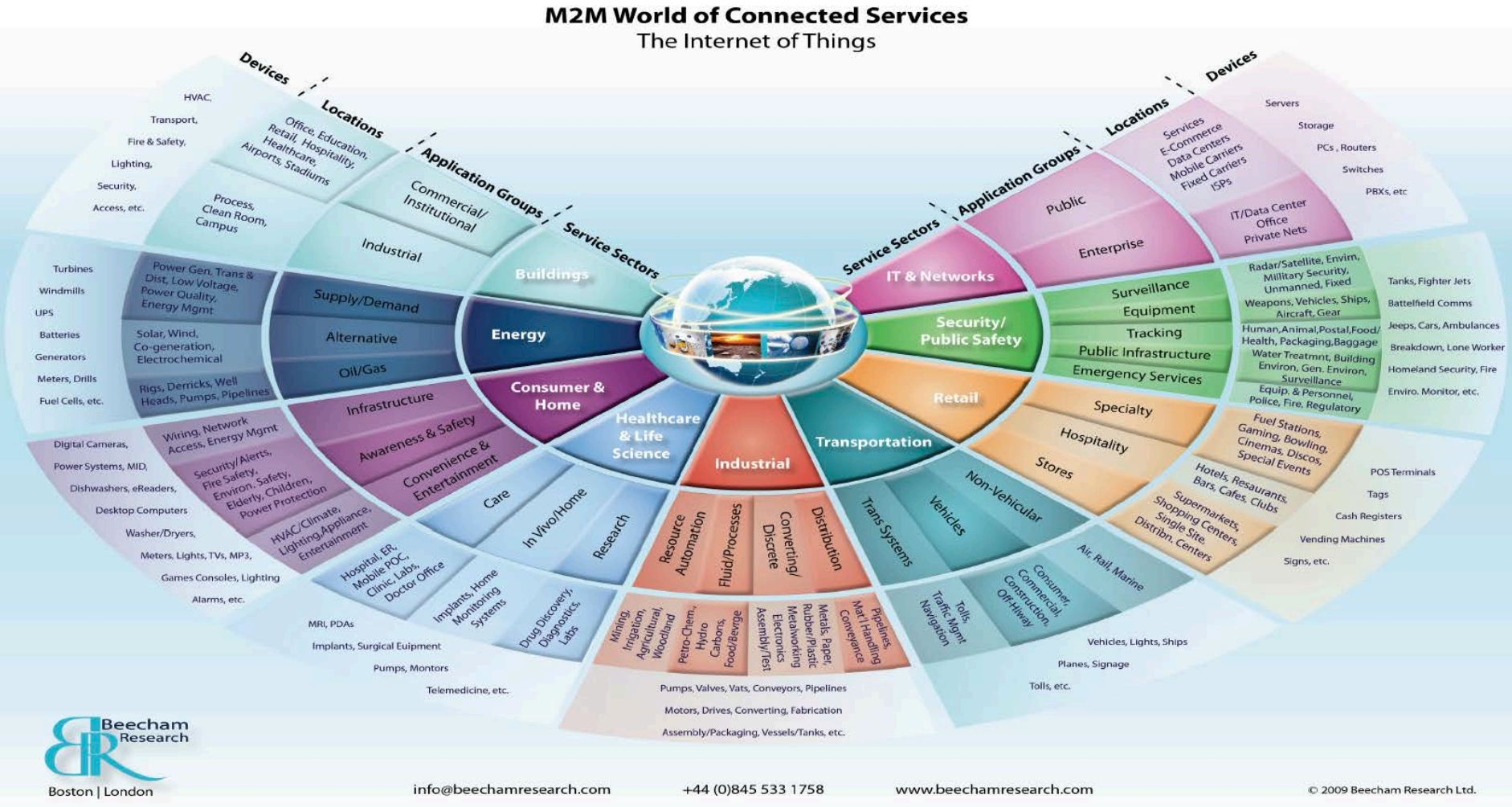
Relationships

- Yes, even machines must establish relationship boundaries. Trust between users, systems & objects requires a verifiable and hierarchical identity structure

Trust

"Roots of trust" for IoT ecosystems - a system of connected gateways & authorities that have visibility and security policy oversight for their segment. This is similar in concept to a traditional domain controller architecture

Is this simplicity?



Simple

- Operational and functional simplicity will be key for IoT adoption by the masses. Most devices will not have the performance or configurability to define and implement complex security policies

- Transparent protection will be required in an ecosystem with limited human interaction

Headlines & headaches

Hacked, Stolen Certificate Used to Spread Malware

By Chloe Albanesius | June 27, 2013 10:55am EST

Bug exposes IP Cameras, baby monitors

Posted Jan 14, 2014

KrebsonSecurity
In-depth security news and investigation

Stolen Digital Certificates Re-Used in Current Watering Hole Attacks on Tibetan and Uyghur Groups

Kurt Baumgartner

Posted April 12, 00:31 GMT

May 15, 2012, 9:51AM

Stolen Certificates Found in Malware Possibly Targeting Tibetan Groups

by Dennis Fisher

July 20th, 2010, 08:10 GMT · By Lucian Constantin

New Stuxnet-Related Malware Signed Using Certificate

IoT worm used to mine cryptocurrency

Symantec

Gaming Company Certificates Stolen and Used to Attack Activists, Others

WIRED BY KIM ZETTER 04.11.13 9:00 AM

[redacted] hacked, stolen digital certificates to sign malware

by paganinip on February 10th, 2013

Flame Malware Uses Stolen Digital Signature

By Paul Wagenseil, SecurityNewsDaily Managing Editor

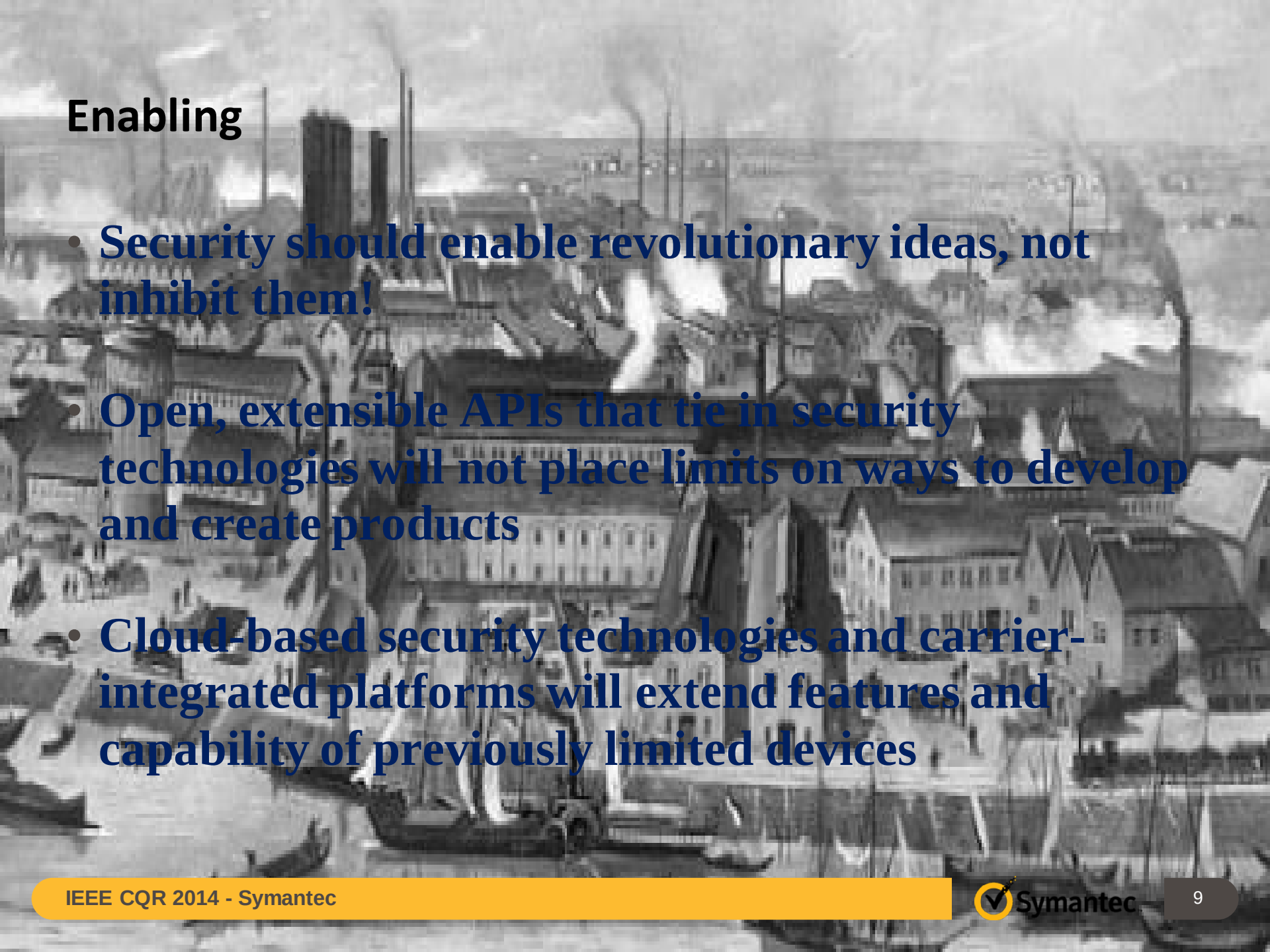
NBCNEWS.com

updated 6/4/2012 2:18:56 PM ET

Predictable

- Code signing and embedded security will make product operations easier and more predictable. Users should not have to guess if their fridge is running the latest firmware or wonder if malware is actually injected in their TV
- Firmware and functionality updates should happen automatically and securely
- Linux.Darlloz: "*Symantec has discovered a new Linux worm that appears to be engineered to target the "Internet of things". The worm is capable of attacking a range of small, Internet-enabled devices in addition to traditional computers. Variants exist for chip architectures usually found in devices such as home routers, set-top boxes, and security cameras.*" [1, 2]
- Chameleon: "*Researchers at the University of Liverpool have shown for the first time that WiFi networks can be infected with a virus that can move through densely populated areas*" [3]
- IP Cameras: "*A bug in the software that powers a broad array of Webcams, IP surveillance cameras and baby monitors made by Chinese camera giant Foscam allows anyone with access to the device's Internet address to view live and recorded video footage*" [4]

Enabling



Enabling

- **Security should enable revolutionary ideas, not inhibit them!**
- **Open, extensible APIs that tie in security technologies will not place limits on ways to develop and create products**
- **Cloud-based security technologies and carrier-integrated platforms will extend features and capability of previously limited devices**

Neighborhood of Things?

Checking the mailbox, going to the corner store - these are routines rooted in safety and security.

Shopping online or touching your phone to a POS terminal; using new wearable technologies; locking down the house from a 1000 miles away – these should all feel as safe and normal as going down to the neighborhood store or sending a letter.

Thank you!

Jason S. Boswell

jason_boswell@symantec.com

Ph: 978-257-5662

References

1. Symantec, *2014 Internet Security Threat Report, Volume 19,* April, 2014, available at http://www.symantec.com/security_response/publications/threatreport.jsp
2. Kaoru Hayashi, *Linux Worm Targeting Hidden Devices,* Symantec Blog, Nov. 27, 2013, available at http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices
3. *Alan Marshall, University of Liverpool, Feb. 25, 2014, available at http://news.liv.ac.uk/2014/02/25/wifi-virus-latest-threat-to-future-it-security/*
4. Brian Krebs, KrebsonSecurity, *Bug Exposes IP Cameras, Baby Monitors,* Jan. 14, 2014, available at http://krebsonsecurity.com/2014/01/bug-exposes-ip-cameras-baby-monitors/