Tackling the Insecurity of Things

July 2018 | UL

Empowering Trust™

UL operates in more than **143 COUNTRIES**

and across more than **20 INDUSTRIES**

UL MARKS appear on more than **22 BILLION**

UL has helped to set **MORE THAN 1,600** standards defining safety, security, quality and sustainability

Who we are

Empowering Trust™

UL software is used by **10,000+** ORGANIZATIONS *in* **OVER 10 INDUSTRIES**

IDENTITY management *and* **SECURITY**

250+ laboratories, testing and certification facilities ***across the world***

Identity management and security

Enable businesses across a myriad of industries to:

- Innovate securely
- Guarantee compliance
- Build consumer trust
- Increase market access

Markets

Telecom

- Mobile ecosystem gap analysis
- Global/regional implementations
- Payment infrastructure support

Payments

- Full ecosystem expertise
- Strategy & rollout plans
- Testing & certification

Automotive

- IoT secure access solutions
- Supply chain security analysis
- Vulnerability risk assessment

Transit

- Ticketing infrastructure modernization
- Security evaluation & reporting
- Supply chain assessment

Retail

- Secure CX strategy & rollout plans
- Omni-channel security validation
- Web-based self-testing

Government

- Secure digitization planning
- Standards development guidance
- Citizen identity secure solutions

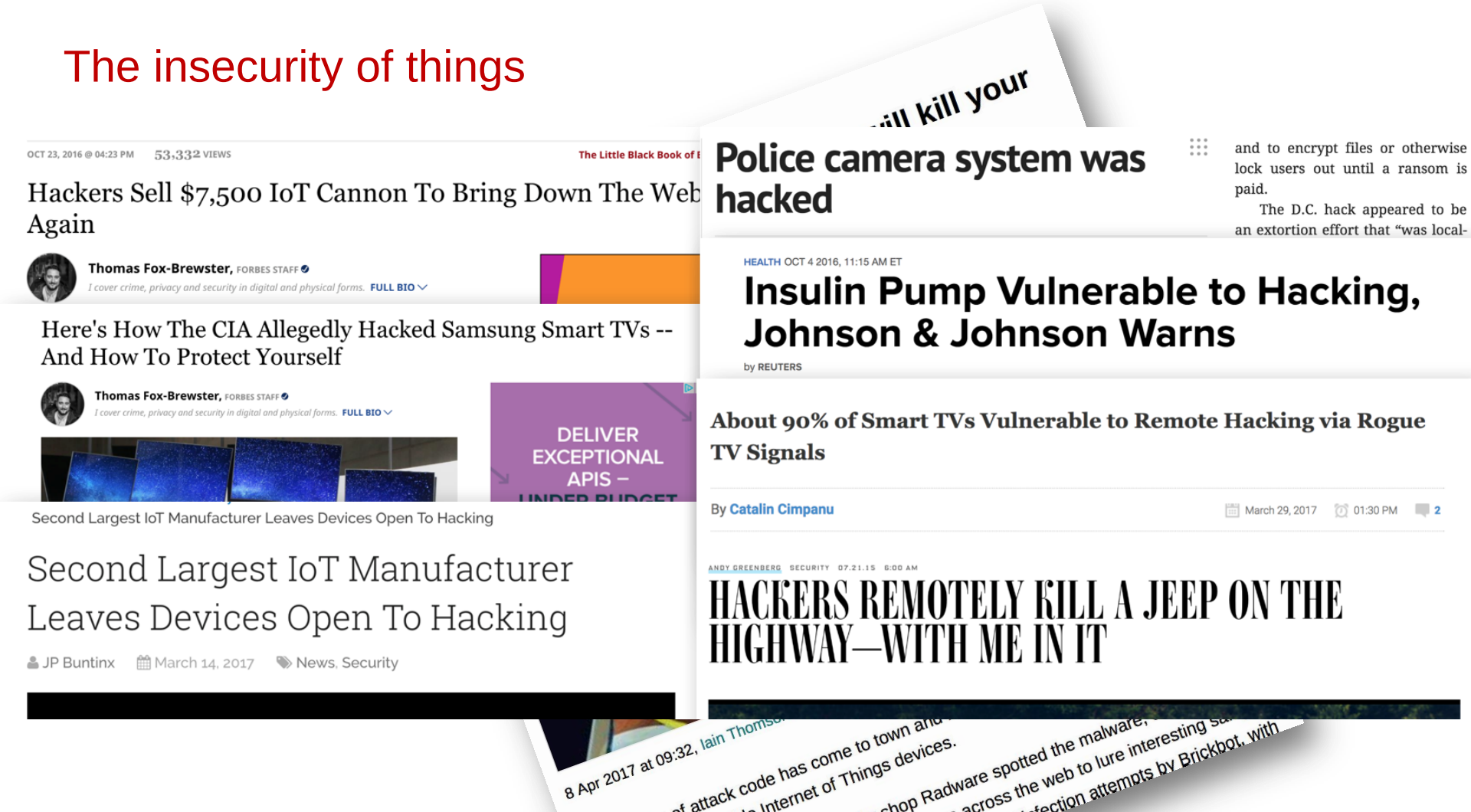
The world is growing more connected

27 BILLION
connected IoT devices were in use
in 2017 and will reach
125 BILLION
in 2030

In 2017 there were
5.2 BILLION
connected CONSUMER DEVICES growing with 13.8% CAGR 2013-30

Source: IHS Markit

The insecurity of things



ill kill your

OCT 23, 2016 @ 04:23 PM 53,332 VIEWS The Little Black Book of E

Hackers Sell $7,500 IoT Cannon To Bring Down The Web Again

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

Here's How The CIA Allegedly Hacked Samsung Smart TVs -- And How To Protect Yourself

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

DELIVER EXCEPTIONAL APIS –

Second Largest IoT Manufacturer Leaves Devices Open To Hacking

Second Largest IoT Manufacturer Leaves Devices Open To Hacking

JP Buntinx March 14, 2017 News, Security

Police camera system was hacked

and to encrypt files or otherwise lock users out until a ransom is paid.

The D.C. hack appeared to be an extortion effort that "was local-

HEALTH OCT 4 2016, 11:15 AM ET

Insulin Pump Vulnerable to Hacking, Johnson & Johnson Warns

by REUTERS

About 90% of Smart TVs Vulnerable to Remote Hacking via Rogue TV Signals

By Catalin Cimpanu March 29, 2017 01:30 PM 2

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

8 Apr 2017 at 09:32, Iain Thomso

of attack code has come to town and

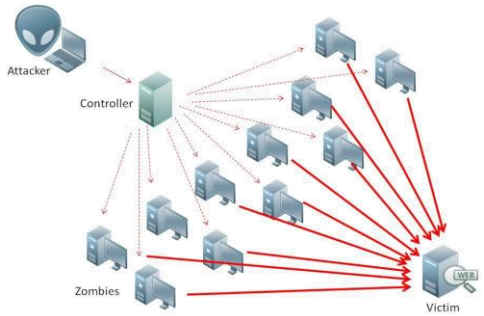
the Internet of Things devices.

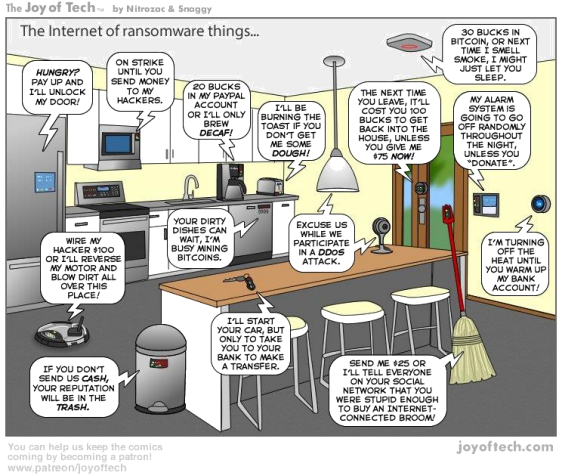
shop Radware spotted the malware,

across the web to lure interesting sa

fection attempts by Brickbot, with

Botnets and DDOS





A Report to the President

on

Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats

Transmitted by
The Secretary of Commerce
and
The Secretary of Homeland Security

May 22, 2018

The problem with IoT Security

- **Products are built to a functional / cost / time-to-market target**
  - **Security is not considered, or an after-thought**
- **Security is opaque to customers**
  - **Why build security in, if it's not part of the purchase decision?**
- **Security is a point-in-time concept, not an absolute**
  - **Therefore different to traditional functional / safety problems**

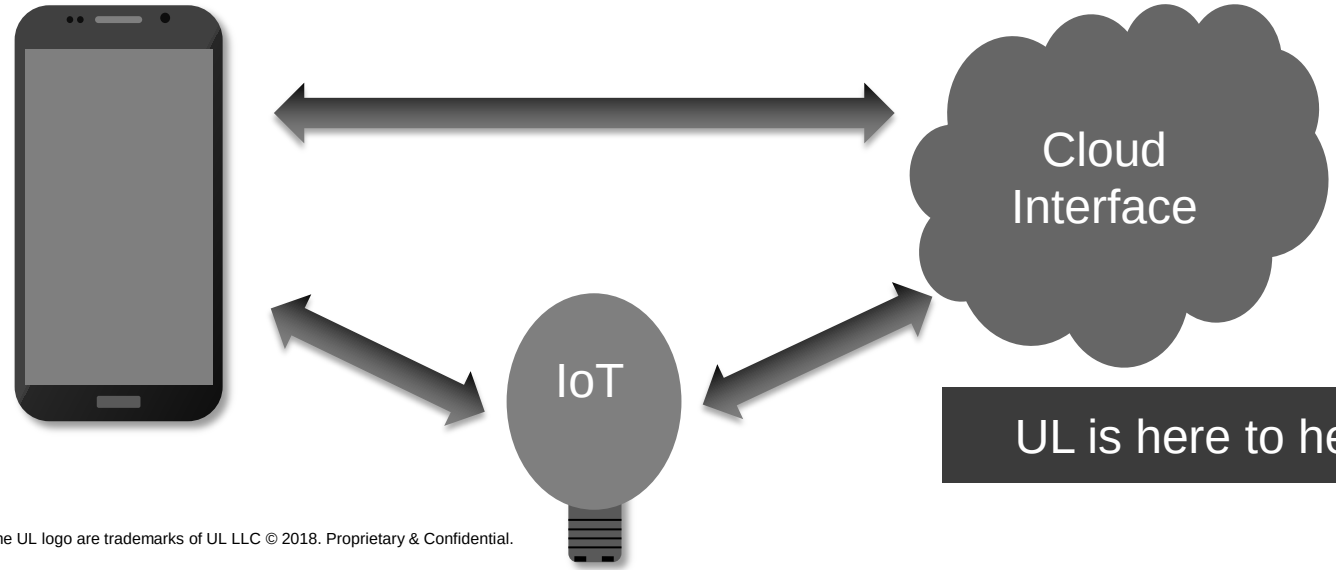
IoT security is a commercial problem

It’s about more than the things

Increasingly, product functionality is distributed

The ‘end point’ device often requires functionality and control provided by remote systems – such as gateways, cloud systems, or mobile apps

Security issues at any one end can affect the entire solution



UL is here to help!

IOT SECURITY TOP 20

DESIGN PRINCIPLES

THE WILD WEST OF MOBILE SECURITY

95% OF BANKING APPLICATIONS LACK THE SECURITY REQUIRED

FEBRUARY 21, 2018

A joint research between Inside Secure and UL

63%

of Gen X and Millenials are using mobile banking applications

95%

of the banking industry **does not reach the security benchmark** laid down by the payment schemes

20%

of Europe's mobile banking applications are all that achieve appropriate levels of security

Compared to mobile payment app security, **mobile banking app security is severely lagging behind***

*Source: Inside Secure & UL Mobile Banking App Research 2017

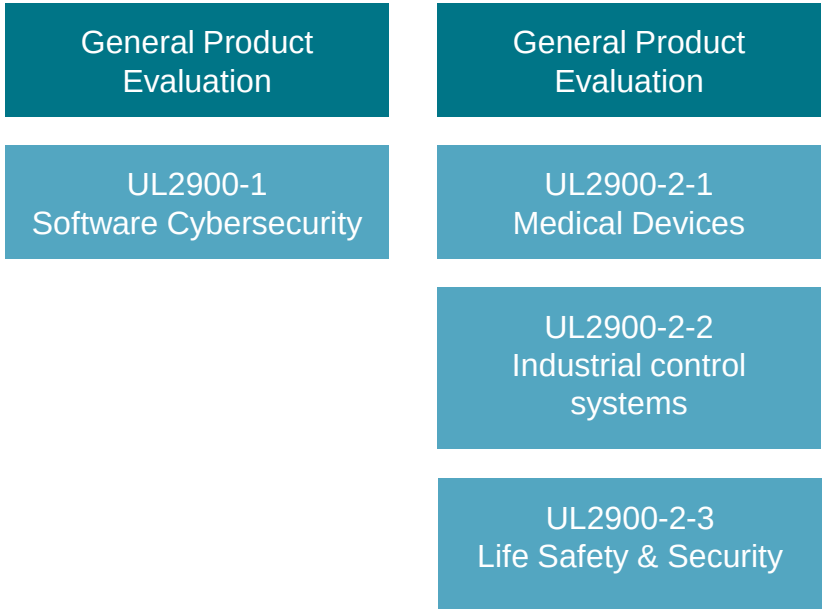
Cybersecurity Assurance Program: UL 2900 series of standards

Testable cybersecurity requirements for networked systems, to:

- assess software vulnerabilities and weaknesses
- address known malware
- review security controls

Based on existing industry best practices and guidance

UL 2900-1 and 2900-2-1 are accredited ANSI standards



Amazon Voice Service Evaluations

Speakers integrating Amazon Alexa must:

- Use secure software update mechanisms
- Be implemented with a patch management strategy
- Implement a security response plan
- Provide a security disclosure and response method
- Implement industry best practice hardening
- Use secure TLS sessions for sensitive data

And, be tested by an independent security lab ….

UL Recommended Minimum Security Requirements

Allow for software updates, and ensure that these updates are cryptographically authenticated prior to installation and execution. Implement ‘anti-roll-back’ features to prevent the installation of previous, vulnerable versions of firmware

Ensure that parameters for which the disclosure could lead to the compromise of the system, such as secret/private cryptographic keys, passwords, etc, are unique per device

Use industry standard security protocols, with ‘best practice’ defaults for any remote or wireless connections and authentication of connections to management services

Protect passwords and security / authentication related secrets

Test the system to be sure that it is free of known, exploitable vulnerabilities prior to release

Authenticate remote access and interfaces to system management functions, with session and time-out limits

Provide a manual override for any safety critical operations

Protect customer privacy and allow for opt-in and opt-out

COMPLEXITY IS THE PROBLEM.

TRUST

IS THE SOLUTION.

- Powers smarter decisions
- Makes brands easier to choose
- Makes supply chains simpler to manage
- Makes differentiation quicker to achieve

Thank you

Gonda Lamberink
Senior Business Development Manager
UL – Consumer Technology (CTECH) division
E: Gonda.Lamberink@ul.com
M: +1 4153508169