Addressing the Wicked Challenges of IoT Security

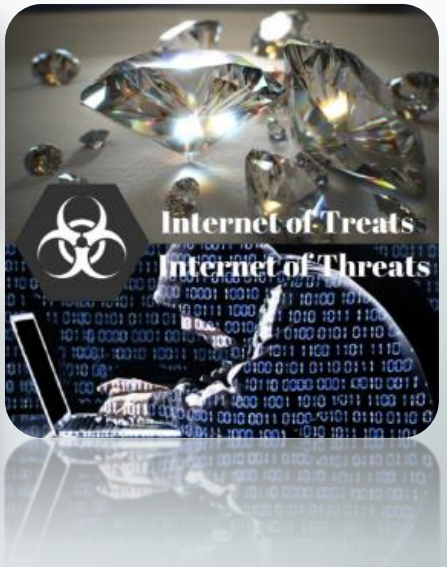
John Moor

Caveat Emptor

The IoT Security Journey: observation, insight and action

IoT: What more can be said?

- **$:** The economic impact of the Internet of Things will be measured in $trillions.
- **∑:** The number of connected devices will be measured in billions.
- **∞:** The resultant benefits of a connected society are significant, transformational and disruptive.



Bletchley Summit: we can't carry on like this

IoT Security Foundation

Fiat Chrysler recalls 8,000 more Jeeps over wireless hacking

Latest recall designed to protect connected vehicles from remote manipulation, says automobile company

News > World > Americas

Hacker takes control of Ohio couple's baby monitor and screams 'bad things'

NEWS

Anonymous hacker claims he broke into wind turbine systems

Cyber criminals hack a REFRIGERATOR: Will the 'Internet of Things' create a new bot army for the spammers?

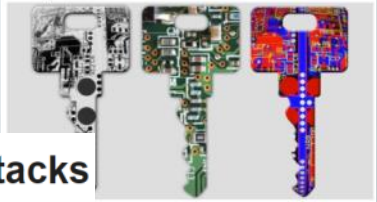
HOME › EXTREME › OUR INSECURE INTERNET OF THINGS IS BECOMING TERRIFYING

Our insecure Internet of Things is becoming terrifying

By Graham Templeton on September 8, 2015 at 8:37 am | 19 Comments

Lazy IoT, router makers reuse skeleton keys over and over in thousands of devices – new study

SSH logins, server-side HTTPS certs baked in firmware



Multiple Backdoors found in D-Link DWR-932 B LTE Router

Wednesday, September 28, 2016 Swati Khandelwal

Army of webcams used in net attacks

29 September 2016 | Technology

Hacking traffic lights with a laptop is easy

TECHNOLOGY NEWS | Tue Oct 4, 2016 | 8:58pm BST

J&J warns diabetic patients: Insulin pump vulnerable to hacking

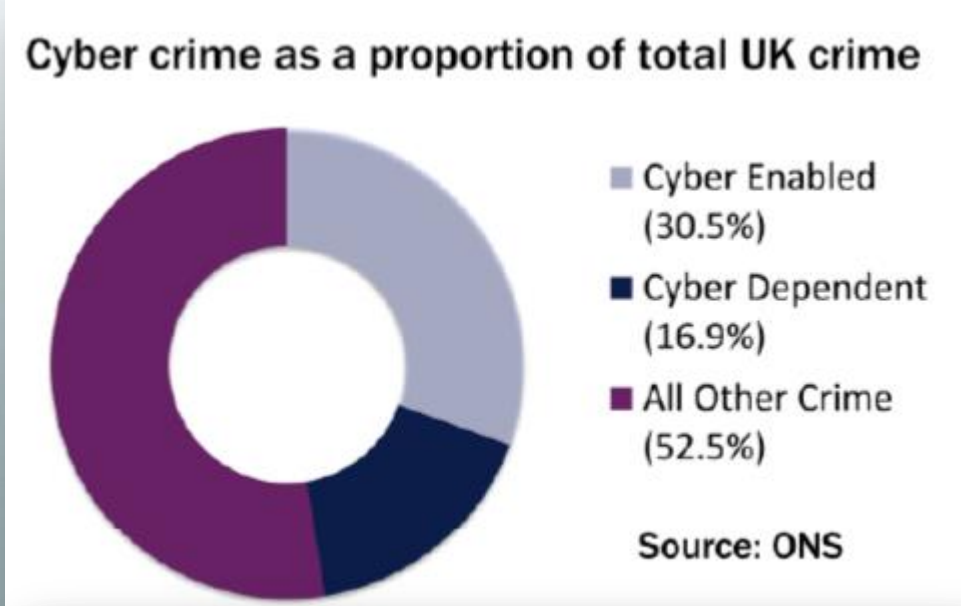
RISK ASSESSMENT —

New, more-powerful IoT botnet infects 3,500 devices in 5 days

Discovery of Linux/IRCTelnet suggests troubling new DDoS menace could get worse.

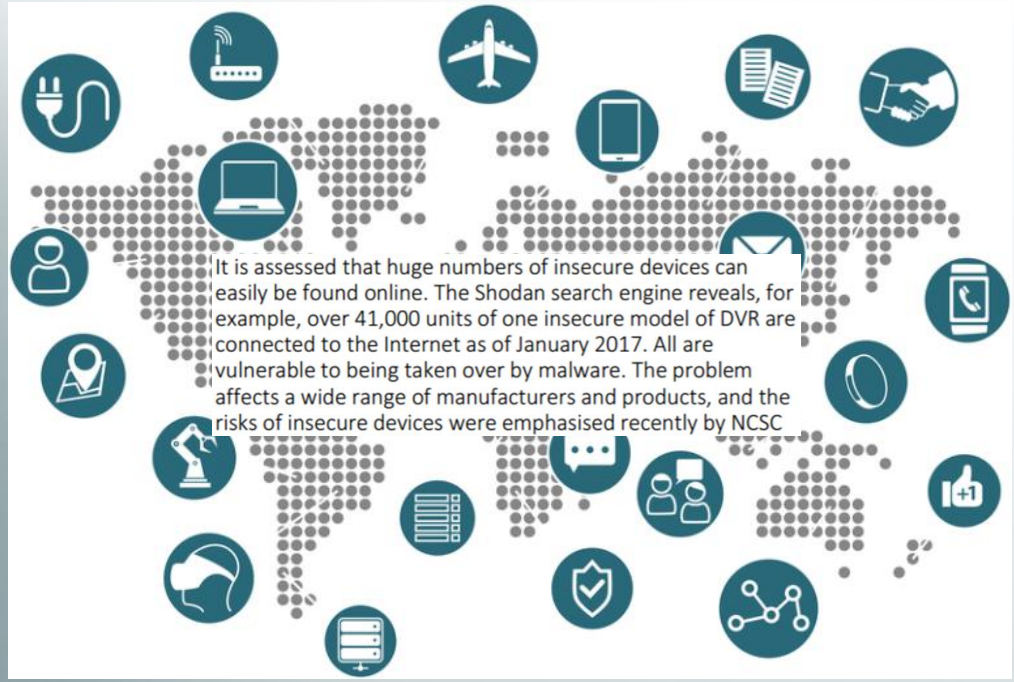
DAN GOODIN - 11/1/2016, 9:15 PM

The Realty of the Digital Trend



The rise of internet connected devices gives attackers more opportunity. Consumer goods and industrial systems combined with the ever increasing commercial footprint online provides threat actors with more attack vectors than ever before.

What's The Big Idea?



IoT security is a ***"Highly Distributed Moral Responsibility"***

- We must all accept accountability
- In the global interest

SUPPLY CHAIN OF TRUST
DUTY OF CARE

- Producers
- Integrators
- Procurers
- Retailers / Users
- Governments and Citizens

What's new with the IoT security challenge?

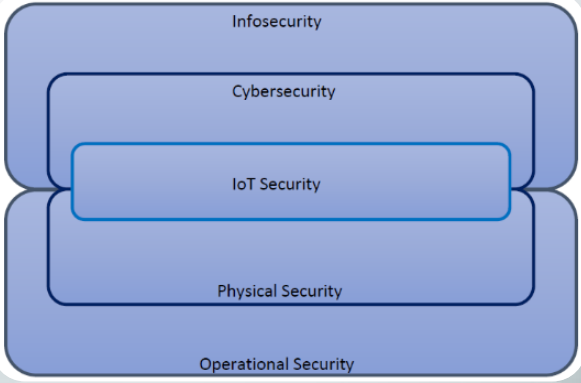
- It's all the same…
  - apart from the players (supply chains) and the markets and the scale, and the scope (operating / regulatory environments), potential for physical harm, headless, constrained, coordinated patching, and, and, and…
- IoT concept at odds with security
  - Complexity/provenance ~ Long and porous borders
- The ugly truth about being cyber-secure
  - *You cannot win – you can only 'not lose'*

Security, at its most basic, means "the state of being free from danger or threat." In cybersecurity, well, good luck with that. Companies will never be free of cyberthreats as long as they operate in an interconnected world.

What's new with the IoT security challenge II?

- Dynamic context: Convergence IT/OT/Emb
  - Differences in knowledge, reporting structures, cultures, demographics, skills, technologies etc.
- Reasonable Expectations
  - Should we expect all developers to be security experts?
  - Should we expect users to be infallible?
- Assertion: Best practice security needs to be consumable for developers and convenient for users
  - Cost and Complexity are our enemies

Finally, many organizations focus on securing their systems when what they really want to do is secure their *data*. This is a critical distinction. A system compromise isn't a cybersecurity concern; after all, systems go down all the time for non-nefarious reasons. What organizations care about is what happens to their data.



Machina Research,
IoTSF 2016 Annual Conference

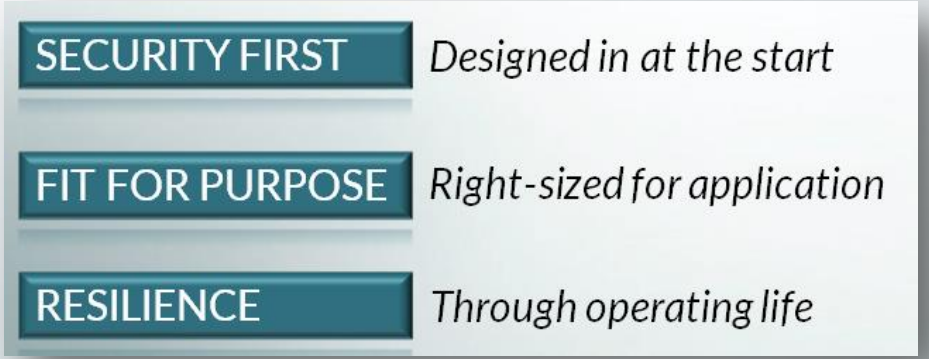
Introducing the Internet of Things Security Foundation

Beyond the horror stories: the IoT Security Foundation was launched on Sept 23rd 2015 in response to wide-ranging security concerns from IoT stakeholder groups

Simplified mission statement:

"Drive the quality and pervasiveness… of IoT security"

"Make it safer to connect in the era of IoT"



How we are (currently) organized

Executive Steering Board

Plenary Group

Working Groups

Members

Priority Working Groups	Chaired by:
Working Group 1: Self-Certification	
Working Group 2: Connected Consumer / Home	
Working Group 3: Patching Constrained devices	
Working Group 4: Vulnerability Disclosure	
Working Group 5: IoT Security Landscape	
Working Group Formed: Trustmark / Regulatory	

Executive Steering Board

Prof. Paul Dorey, **CSO Confidential**

Prof. John Haine, **University of Bristol**

Prof. David Rogers, **Copper Horse Solutions**

Ken Munro, **PenTest Partners**

Prof. Ben Azvine, **BT plc.**

Majid Bemanian, **Imagination Technologies**

Dr. Stephen Pattison, **ARM**

Haydn Povey, **Secure Thingz**

Prof. Kenny Paterson, **Royal Holloway, University of London**

Dr. Steve Babbage, **Vodafone Group**

Richard Marshall, **Xitex Ltd.**

John Moor, **IoT Security Foundation**

Members

88 members, large and small, and growing…

Doubled in 2016

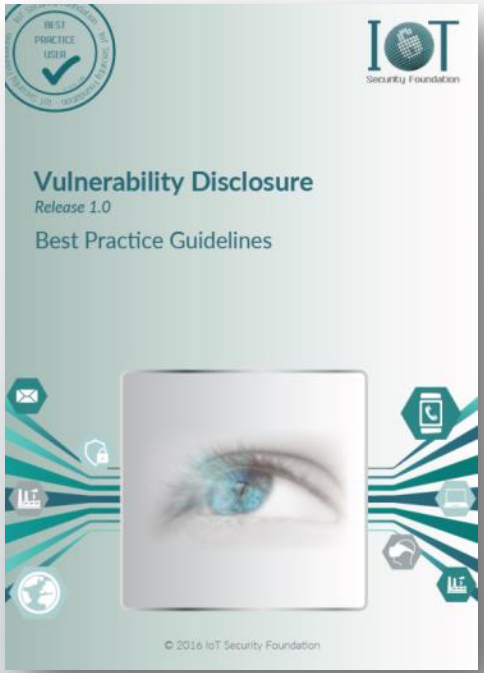
Low Cost Membership / High Value Activity

IoT Security Foundation Member

EST. 2015 Member

See https://iotsecurityfoundation.org/our-members

Best Practice Guides



Free to download and use
More to come…

See https://iotsecurityfoundation.org/best-practice-guidelines/

IoT Security Compliance Framework

RELEASE 1.0

What's ahead for IoTSF?

Expansion

Home

Situation Now and for 2017…

- Moveable feast
- Know your enemy
  - Attribution blurring
  - Crime-as-a-service
- 2017 attacks
  - Weaponisation
    - More DDoS
  - Ransomware
    - Consumers and Citizens
- Legacy systems challenge
  - IIoT / Vulnerability shields

THREAT ACTORS WILL COME UP WITH NEW TARGETED ATTACK TACTICS THAT CIRCUMVENT CURRENT ANTI-EVASION SOLUTIONS.

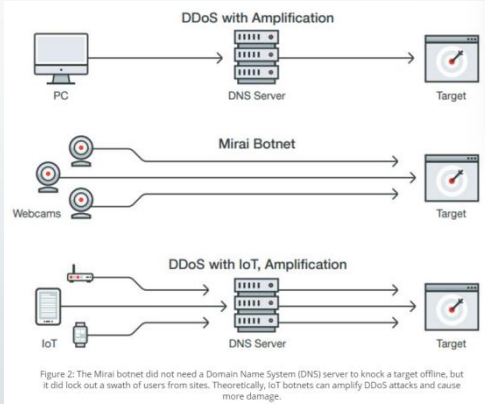


Figure 2: The Mirai botnet did not need a Domain Name System (DNS) server to knock a target offline, but it did lock out a swath of users from sites. Theoretically, IoT botnets can amplify DDoS attacks and cause more damage.

IOT DEVICES WILL PLAY A BIGGER ROLE IN DDOS ATTACKS; IIOT SYSTEMS IN TARGETED ATTACKS.

Nation states

Nation states may seek to exploit UK businesses to further their own n agenda and prosperity.

Campaigns by nation states are persistent, focusing on (but not espionage and intellectual prope taking place over many years an significant technical capability.

Hacktivists

Hacktivists aim to raise awareness for their cause. They focus on propaganda, defacement and DoS attacks. Few hacktivists can carry out a successful DoS attack against organisations with mitigations in place. This includes

Weeping Angel (*noun*):

1. A terrifying monster from the popular UK sci-fi series "Doctor Who," which resembles a harmless winged statue -- until you blink or look away.

2. An alleged spying tool, co-developed by the CIA and the UK's MI5 security agency, which lets a Samsung Smart TV (specifically, the F8000 Smart TV) *pretend* to turn itself off -- and record your conversations -- when you're not using the screen.

Anyone can be (or hire) a cyber criminal

Easy access to offensive cyber capabilities, such as ransomware or DDoS, has allowed individuals and groups to have an impact disproportionate to their technical skill. This

Like any good entrepreneurs, the authors of ransomware have not just profited from running their own operations, they've also begun selling their services for a cut of the action. This business model is commonly referred to "ransomware as a service" (RaaS). One of the first RaaS kits was called Tox.

A recent search of malware forums revealed RaaS kits for sale ranging in price from $15 to $95.

References:
1. Security predictions: The Next Tier, Trend Micro
2. The Cyber Threat to UK business, NCSC NSA
3. The Black Report, Nuix

Footnotes – *a few words on…*

- S/W integrity / agility
- Patching constrained X
- PKI too heavy for IoT?
- Authentication methods
  - Passwords, MFA
  - Immutable ID
- ML
- Blockchain, Quantum
- Regulation / Certification
- GDPR? DSO + $$

The National Institute of Standards and Technology (NIST) reports that 64% of software vulnerabilities stem from programming errors and not a lack of security features.
(industry average 15-50 bugs for every 1000 lines)

PKI: System to manage digital certificates and public key encryption

Final word

In this hyper-connected, increasingly software defined, digital world, ***security is a right****, not a nice to have*

…make it safe to connect

john.moor@iotsecurityfoundation.org
https://iotsecurityfoundation.org

@IoT_SF