Introduction to the IoT Security Foundation

Build Secure, Buy Secure, Be Secure





The Questions



- Why does the IoT Security Foundation exist?
- Who are we?
- What do we aim to do?
- How do we do it?
- How can you participate?

IoT

IoT stands for

'Internet of Threats'

if you forget the

'S' for security



IoT security status 'egregious'

Army of webcams used in net attacks

O 29 September 2016 | Technology

News > World > Americas

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

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

🛗 Wednesday, September 28, 2016 🛛 🌡 Swati Khandelwal

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

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

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

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

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

Anonymous hacker claims he broke into wind turbine systems

Fiat Chrysler recalls 8,000 more Jeeps over wireless hacking

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



IoT vulnerabilities and exploits dominate the news headlines

'we cannot carry on like this' Something needs to be done to protect users

Manufacturers must do better

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







Beyond the horror stories: the IoT Security Foundation was launched on

<u>Sept 23rd 2015</u> in response to wide-ranging security concerns from IoT stakeholder groups







SECURITY FIRST

RESILIENCE

Designed in at the start

FIT FOR PURPOSE Right-sized for application

Through operating life

www.iotsecurityfoundation.org

or simply IoTSF.org

Purpose

IoT is Socially and Economically Important

- 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, disruptive and transformative.



Security Foundation

Yet the growth of IoT also represents a growing attack surface – a real threat.

The IoTSF mission is to help secure the Internet of Things and 'make it safe to connect'.



Our mission: Make it safe to connect



Organisation and Operation



Executive Steering Board **Plenary Group** *Central Working Groups International Chapters Members

Impactful Benefits

- Promote awareness and a security mindset
- Produce best practice materials and tools for vendors and users of IoT technologies.
- Bilateral links to international standards efforts
- Influence / consult on cyber security regulations
- Conferencing, Meetings and Networking Events
- Collaborative Projects

*See https://www.iotsecurityfoundation.org/working-groups/

How do we do it?

- Published IoT Security
 Assurance Framework
- Secure Design Essentials
- Helping members meet regulations
- Monthly Webinars









Assurance Applicability - Business Secur 2.4.3 2.4.4 Assurance Applicability - Device Hardw Assurance Applicability - Device Softwa 2.4.5 2.4.6 Assurance Applicability – Device Opera Assurance Applicability - Device Wired 2.4.7 Assurance Applicability - Authentication 2.4.8 2.4.9 Assurance Applicability - Encryption a 2.4.10 Assurance Applicability - Web User Ir 2.4.11 Assurance Applicability - Mobile App Assurance Applicability - Data Prote 2.4.12 2.4.13 Assurance Applicability - Cloud and 2.4.14 Assurance Applicability - Secure Su 2.4.15 Assurance Applicability - Configur 2.4.16 Assurance Applicability - Device

Release

IOT WEBINAR SERIES

0

6 308 MI Sourty Incodes

THURSDAY, 27th APRIL 2023

EUROPEAN CYBER RESILIENCE ACT

FLORIAN LUKAVSKY CTO & FOUNDER ONEKEY

MATT TETT ADVISOR IOT SECURITY MARK

Membership: Security is a Team Sport



Security Foundation

An ecosystem of professional and corporate stakeholders



Invitation

Join the home of IoT Security

 \checkmark Be part of an expert international community

✓ Help champion and drive the IoT cybersecurity agenda

✓ Network and raise your profile with customers, associates and stakeholders.

Join: https://www.iotsecurityfoundation.org/join/



Member Benefits Better Informed, Better Connected, Better Protected



 \Rightarrow Access to

Knowledge networks and resources

Security professionals and world class academics

Members only community platform

Papers: guidance and best practice

Market and trend briefings (as available)

owledge networks

Members have access to the outputs from working groups & projects

Members can participate and lead working groups

 \Rightarrow Working

Groups &

Projects

Contributions publicly acknowledged in IoTSF's globally recognised and referenced security

publications Members can also propose joint projects aligned to the mission and, when authorized, become part of the official program.

and promotional

Sponsorship &

opportunities at

opportunities at

Opportunity to

Ambassador

Produce opinion

represent IoTSF at

events as a Member

pieces, blog writing &

article contributions for the IoTSF website

member rates

materials

exhibition

Speaking

events

⇒ Marketing and ⇒ Events brand benefits including

Logo on IoTSF website Free attendance at physical and virtual member meetings &

summits

Free attendance at working group meetings

IoTSF Annual Conference – discounted member rates on conference tickets, exhibitor and sponsorship packages

Discounted member rates for training courses and workshops ⇒ Access to Education and Training Activities



 \Rightarrow Newsletter

⇒ Voice and Representation

 \Rightarrow Use IoTSF

member only

resources and

guidelines





IoTSF Bangalore Chapter Meetup Q3 2024

Topic Future Proofing Industrial IoT Security







OT vs IT



Security Foundation



OT carries out tasks, controls, and monitors processes, while IT safeguards, stores, and manipulates data.



For OT, **safety** is the top priority; in IT, **security** is paramount.



OT systems are predominantly **isolated** compared to IT's higher **internet connectivity**.

OT is often not initially **designed with security in mind**, whereas IT is **built to be secure** from the start.

OT vs IT (Cyber Security)



Encryption: In OT, it's used sparingly or not at all to avoid operational delays, whereas IT regularly uses advanced encryption for data protection.



Patch Management: OT updates are infrequent, requiring vendor input and offline testing, unlike IT where updates are routine.



Penetration Testing: Conducting these tests on OT systems can be risky when live, but it's a common practice by ethical hackers in the IT field.

Security Foundation



Upgrade: OT tends to have many legacy systems, while IT systems are upgraded more regularly.



Cyber Security Awareness: Generally lower in OT, and ranging from medium to high in IT.



Data Loss: In OT, this might mean production and process loss; IT relies on backups restoration.



Availability: Design of OT systems often focuses on resilience, and for IT, it's always critical.



Performance: In OT, performance is crucial, whereas in IT, it takes on varying levels of importance.





Security Foundation

Real Examples of Industrial IoT Threats: The Stuxnet Attack

- First known cyberattack to cause physical damage to an industrial system
- Occurred in 2010

Real Examples of Industrial IoT Threats: The Triton Attack

- First known cyberattack on safety instrumented system
 - Targeted petrochemical plant in Saudi Arabia
 - Occurred in 2017







Security Foundation

Real Examples of Industrial IoT Threats: The SolarWinds Attack

- The SolarWinds attack was one of the largest and most sophisticated cyber espionage campaigns ever.
 - It compromised the software supply chain of many IIoT vendors and customers.
 - It affected multiple government agencies and private companies.

Future Proofing Industrial IoT (IIoT) Security





- Securing the Edge: Fortifying Connectivity at the Frontier
- Ensuring Resilience: Safeguarding Supply Chains
- Future-Proofing Security: Embracing Crypto Agility and Post-Quantum Cryptography
- Advancing IoT Security: Exploring the IIC IoT Security Maturity Model
- Panel discussion: Adapting to Modern Threats Resilient Security Strategies for Manufacturing