# Can You Trust Your Smart Building?

## Whitepaper

### Understanding the security issues and why they are important to you

**June 2019**

IoT Security Foundation

# Preface

This Whitepaper from the Internet of Things Security Foundation (IoTSF) [ref 1] aims to: raise awareness of the security issues associated with Internet connected 'smart' building systems and devices; show why these issues are important and how they are relevant to a broad range of different building stakeholders, including but not limited to:

- Owners
- Contractors
- Facility Managers
- Engineers
- Architects
- Consultants
- Designers
- Integrators
- Installers
- OEMs

The IoTSF was established to make it safe to connect in the smart and hyper-connected era of Internet of Things (IoT). Right now, we are witnessing the steady invasion of IoT devices into buildings and their networks, and we can see a growing need to support this area.

We seek to encourage people from stakeholder groups to engage with IoTSF's Smart Buildings Working Group and provide input as we develop best practice security guidance.

*We seek to encourage people from stakeholder groups to engage with IoTSF's Smart Buildings Working Group and provide input as we develop best practice security guidance*

# Contents



 

# Introduction

Buildings are becoming increasingly connected and 'Smart' with the deployment of sensors, IoT networks, analytics and their integration with building management systems (BMS), building automation systems (BAS) and other systems (e.g. security, fire detection and alarms, occupancy, environmental, parking).

*"The IoT for intelligent buildings global market is expected to grow from $6.3 billion in 2017 to $22.2 billion in 2026"*

*Source: Navigant Research, ref 2*

Instead of operating as a set of vertical integrated 'stove pipe' systems, a Smart Building System is a 'System of Systems" as illustrated in the figure below.

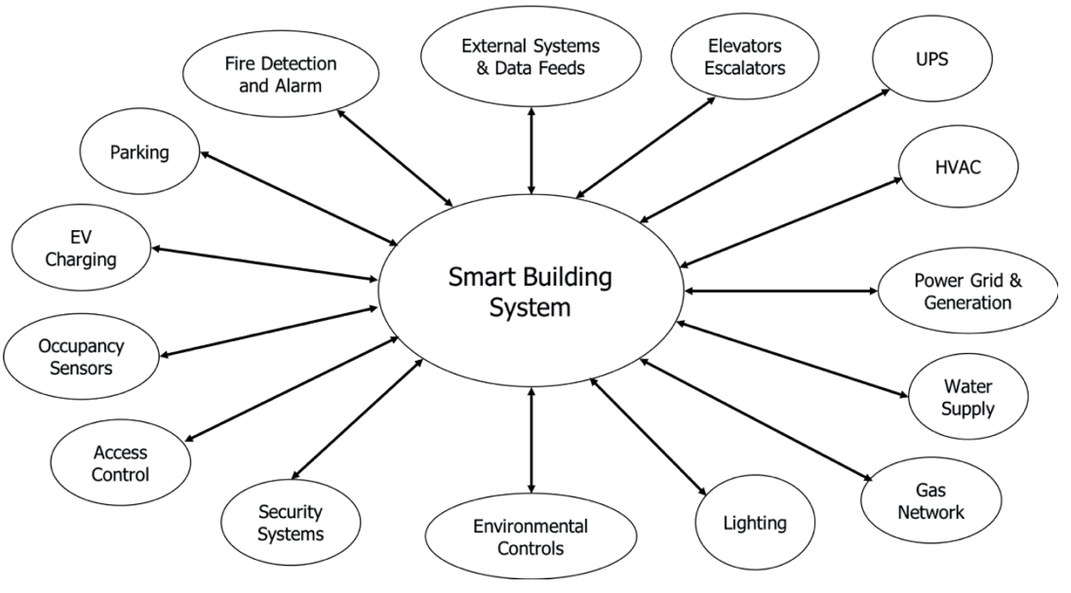


**Figure 1: System of Systems**

*"A Smart Building System provides a unified view and control of all the building sub-system domains"*

The smart building system provides a unified view and control of all the building sub-system domains (which in themselves are likely to be 'smart'), sharing data (historical & real-time) and making use of analytics. This allows smart buildings to be managed and optimised 'holistically' and provides 'situation awareness' to help managers understand the impact to their customers and aid their decision-making across a broad range of situations.

Smart Buildings can generate a deluge of data. Predictive analytics, machine learning and other branches of artificial intelligence (AI) allow managers and Smart Buildings to 'intelligently' optimise the use of assets, operations and the consumption of resources. Industries such as hospitality, medical, retail and manufacturing are all being transformed through the use of Smart Building and IoT technology.

Smart Buildings offer potential benefits to users, owners and managers of buildings such as:

- Savings in energy and water usage and the resulting reduction in costs and carbon footprint
- Improved working conditions, safety and security for occupants
- Improved customer service levels
- Visibility and management of occupancy levels
- Optimisation of resources (physical, space and human)
- Reduced maintenance costs

As well as the benefits, it is important to consider the risks of introducing new technology and devices. IT Cyber Security risks are not new, however, the proliferation of connected IoT devices introduces new system elements and components that can be exposed to possible attacks (attack surfaces) and mechanisms by which the attack can take place (attack vectors).

The risk to an organisation or individual through poor security practice could impact:

- Reputation
- Share price
- Costs - operational, replacement, sales, legal, fines etc.
- Health & Safety

## Threats to Smart Buildings

Threats to Smart Buildings can come from a number of difference sources or 'actors' including financially motivated cyber criminals, states and state-sponsored groups, hacktivists and malicious insiders (employees).

*Too cold to work?*
*Are you sure your BMS has not been hacked?*
Source: Pen Test Partners, ref 3

Security research company, Pen Test Partners, have demonstrated how poor installation by electricians and HVAC engineers who don't understand security can lead to BMS controllers being exposed on the public internet and vulnerable to attacks that, for instance, could sabotage HVAC devices to close offices [ref 3] or cause life threatening issues at healthcare facilities. A simple search on Shodan [ref 4], the search engine for Internet-connected devices can reveal thousands of insecure BMS systems across the globe.

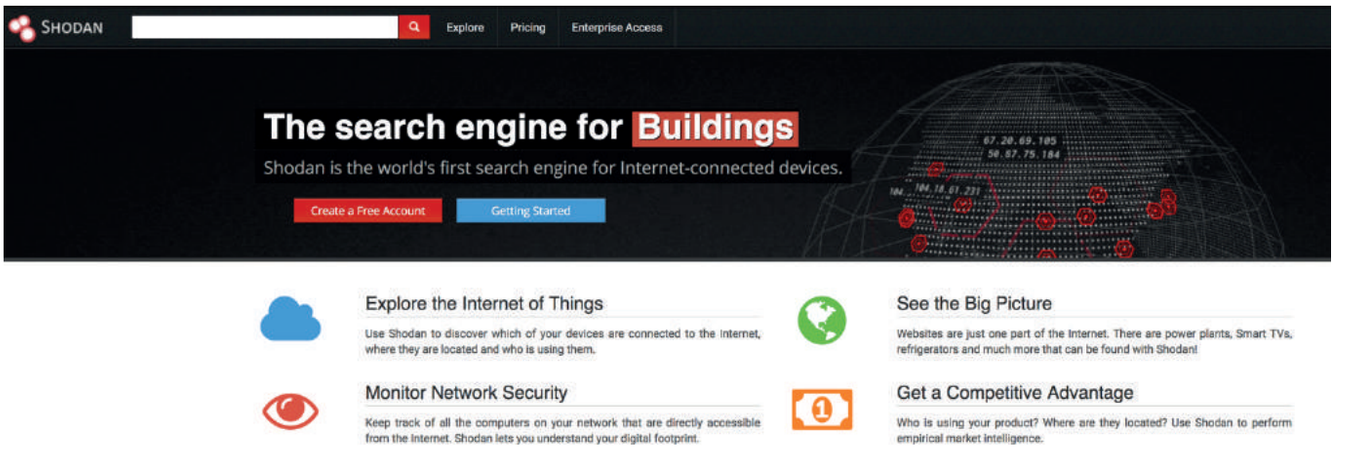


**Figure 2: Shodan, the search engine for Internet-connected devices**

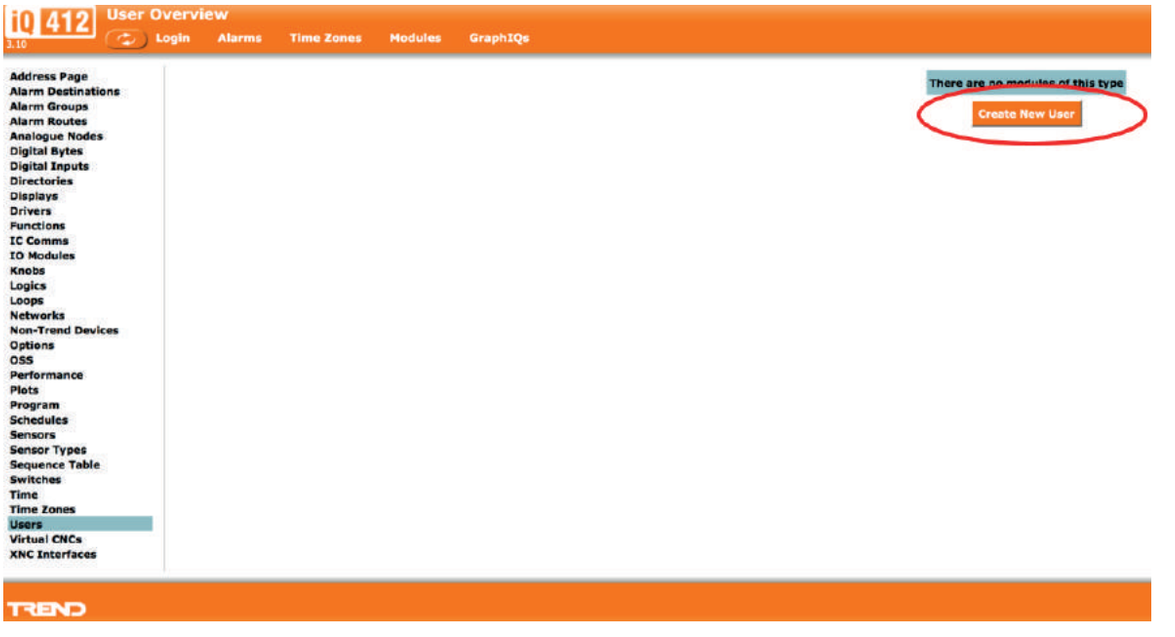


**Figure 3: An example of a school's boiler room BMS controller that is connected to the Internet (found using Shodan) that allows anyone to set themselves up as a user**

*Malicious actors could potentially take advantage, launching attacks that could, for instance, sabotage HVAC devices to overheat data centres or compromise physical access control systems in order to gain unauthorised entry to sensitive locations*

*Source: SC Media, Ref 5*

Researchers at ForeScout have developed a proof-of-concept malware capable of compromising Building Automation Systems (BAS) after discovering two critical bugs in a BAS programmable logic controller (PLC) [ref 5]. The malware exploits both vulnerabilities in combination with several older flaws that were previously known to the public, according to ForeScout.

*Thousands of freezers and chillers in hospitals and supermarket chains could be accessible online*

*To defrost a machine, all you would need to do is click a button then enter the default username and password*

Researchers from Safety Detective Lab uncovered a major security breach in temperature control systems [ref 6] which meant that they could be accessed online through any browser. These control systems are used by hospitals and supermarket chains all over the world. A basic scan using Shodan revealed hundreds of insecure installations in the UK, Australia, Israel, Germany, the Netherlands, Malaysia, Iceland, and many other countries around the world. These systems used the insecure HTTP protocol, a default username and “1234” as the default password, which is rarely changed by system administrators.

*Criminals Hacked a Fish Tank to Steal Data from a Casino*

*Source: Forbes, Ref 7*

In 2017, it was revealed that criminals had managed to steal 10GB of data from a North American casino high-roller database via an internet connected thermometer in a lobby aquarium [ref 7]. The internet connected fish tank allowed it to be remotely monitored, automatically adjust temperature and salinity, and automate feedings.

*Mirai – hacked CCTV video cameras and digital video recorders caused a massive Internet outage affecting Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix*

*Source: Krebs On Security, Ref 8*

The assets/computing resources of buildings can also be hijacked to perform distributed denial of service attacks on other organisations as in the case of the 2016 attack on Dyn [ref 8], an Internet infrastructure company, which caused outages and network congestion to the online services in North America of Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix. This attack was attributed to Mirai malware on mainly compromised, CCTV video cameras and digital video recorders. Mirai scours the Web for IoT devices protected by little more than factory-default usernames and passwords, and then enlists the devices in attacks that hurl junk traffic at an online target until it can no longer accommodate legitimate visitors or users.

*"No-one would be interested in hacking us, we're not a bank; we have nothing a hacker would want"*

You may think 'no-one would be interested in hacking us, we're not a bank' however, you may become the unintended victim of collateral damage as in the case of the WannaCry ransomware attack [ref 9] and NotPetya [ref 10]:

*WannaCry - infected over 200,000 devices infected in more than 150 Nations*

WannaCry - infected over 200,000 devices in more than 150 Nations. This attack impacted FedEx, Spanish telecoms and gas companies, Renault French car production factories, the Russian interior ministry, and the U.K. National Health Service infecting tens of thousands of the NHS's hospitals' devices, including computers, Magnet Resonance Imaging (MRI) scanners, blood-storage refrigerators and theatre equipment.

***$10 Billion***

*Total damages from NotPetya, as estimated by the White House*

NotPetya – in a report published by Wired, a White House assessment estimated the total damages brought about by NotPetya to more than $10 billion [ref 11]. Those affected included British advertising company WPP, American pharmaceutical company Merck & Co and Maersk, the world's largest container ship and supply vessel operator. These companies are estimated to have lost between $200 and $300m in revenues.

# Protecting People, Assets and Your Investments

In this digital age, what risks are posed to your tenants, staff, visitors and assets from vulnerabilities in Internet connected building systems and devices? It is not feasible to eliminate all risks from Smart Buildings. Security investments should be balanced against the effect of undesirable outcomes. Balancing should be grounded in a realistic assessment of the threats, the risks they pose and how they might prevent the system from fulfilling its intended functions. Costs should be evaluated, and a rational selection of implementation choices made to deliver an acceptable return on investment.

*What risks are posed to your tenants, staff, visitors and assets from vulnerabilities in Internet connected building systems and devices?*

In preparing for your risk assessment you might like to consider:

- Have you identified your critical digital assets? Not all systems and data are created equal.
- Have you identified which systems are critical for health and safety reasons and therefore must be fail-safe?
- Do you have and maintain lists of all your assets (devices, software, and any sensitive information/data)? If so, do you know who has access to them and where the data resides?
- Are you able to detect unusual behaviour/activity on your network? Do you use real time monitoring solutions?
- Would you know if a rogue device came on to the system?
- If the building systems are attacked do you have processes and policies in place to deal with this and are your staff familiar with these?
- If the power and UPS fails as a result of an attack, will you be able to recover quickly and be operational as needed?
- Do your key system suppliers (e.g. BMS, CCTV, access control and fire) have cyber security policies and understand their responsibilities?
- Do your suppliers have data protection policies and are you satisfied they comply with the EU GDPR?
- Do you and your suppliers have written policies on vulnerability disclosure, system patching and updates?
- Have you considered asking the physical and information/cyber security teams to work together to understand the risks to your building systems?
- Do your fire-drill preparations include turning off key systems to determine how the building and personnel respond to broken systems?

These and other questions are important for a Smart Building's stakeholders to carefully weigh up throughout its lifecycle from design to decommissioning especially given the legal and health and safety requirements which relate to data protection and duty of care. The problems of systems failures resulting in serious harm can be significant and hence the value of conducting risk assessments.

# Connected Buildings

The design of a smart building incorporates layered technologies that collectively enable building management, monitoring and control functions that optimally support the people and processes inside it.

At the edge of the smart building network, physical sensors and actuators interact with their environments. Components are connected to their sub-system domain software/platforms through building management gateways and controllers such as Programmable Logic Controllers (PLCs) via wired or wireless connections.

Numerous communication protocols exist, and a smart building will often implement many of these in support of individual sub-systems domains.

*Traditional building automation communications protocols and standards have moved to support the Internet Protocol (IP) suite and thus become Internet connected*

Traditional building automation communications protocols and standards have moved to Internet Protocol (IP) suite and thus become Internet connected. For instance, BACnet has evolved to BACnet/IP and BACnet/IPv6, LON to LON/IP and KNX to KNX IP. System designers, integrators and installers need to understand the unique cyber security considerations associated with each protocol [see Appendix A] as many of these do not offer encryption, authentication and non-repudiation in their original form.

Smart building systems have also seen a move away from on-site hosted BMS platforms to Software as a Service (SaaS) running in the 'Cloud'.

# Vulnerabilities

Smart building systems are complex and likely to suffer from a range of weaknesses that must be resolved to keep them available, safe and secure.  Potential weaknesses include:

- Common vulnerabilities and exposures (CVE) in the software or firmware of the devices, gateways and web services that make up the smart building
- Lack of or inconsistent processes for updating the software and firmware of products or applying patches on a routine basis
- Vulnerabilities caused by the procurement and integration of insecure devices (e.g. surveillance CCTV equipment with default usernames and passwords) and use of insecure protocols
- Lack of or inconsistent security best practice training
- Lack of visibility of the cyber security state of connected products and systems
- Limited or no physical protection to restrict access to device internals or tap wired networks
- Poor cryptographic key management policies and procedures
- Insufficient security for device discovery features allowing adversaries to perform reconnaissance activities (e.g. identify devices of a certain type and their location)

- Poor security processes and misconfigurations (e.g. use of default passwords, repeating passwords across systems, devices exposed on the internet through UPnP, misconfigured remote access etc.)

## Security Best Practice

Organisations can mitigate potential vulnerabilities with a mixture of technical and non-technical means. Non-technical factors include, but are not limited to policy, procedure, training, and reporting as well as even broader factors such as organisational culture. Data classification has now become a necessary component to protect the building occupants' personal or sensitive data and help you maintain regulatory compliance.

*Protecting your investments in Smart Buildings requires a structured approach to implementing and maintaining security best practice, policies and procedures*

This is well illustrated and documented by the US National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity" [ref 12] which:

*"provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations, or it can be focused on the delivery of critical services within an organization."*

The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. The main Core Functions are **Identify, Protect, Detect, Respond,** and **Recover.**


**Figure 4: NIST Core Functions**

The Functions should be performed concurrently and continuously to form an operational culture that addresses dynamic cybersecurity risk. Core activities include:

- Management Governance
- Risk Assessment
- Threat Modelling
- Security by Design (throughout the enterprise and system of systems) and leveraging Defence in Depth [ref 13 & 14]
- Procurement (specifying security requirements for products)
- Supply Chain Processes (ensuring security is maintained throughout and at source)
- Secure Implementation Processes
- Testing and Validation
- Secure Maintenance and Lifecycle Management (including security software updates)
- Training for system administrators and an enterprise monitoring plan to watch for suspicious events within the building network
- Detection of Anomalies and Events
- Continuous Security Monitoring
- Incident response plan to effectively respond to cyber security incidents as they occur
- Vulnerability Disclosure
- Recovery and Resilience processes and plans to restore services in the event of a security event
- Physical access controls (PACS) to provide wider visibility across the physical and electronic space

The insecure configuration of smart building technologies opens opportunities to inadvertently expose weaknesses in a smart building's defences. Proper implementation of confidentiality, integrity and availability controls requires an understanding of not only individual component security weaknesses but also weaknesses at points of interconnection across the smart building. Threat modelling can assist in identifying those weaknesses and identifying the mitigating controls, for example:

- Deployment of hardened gateway platforms
- Logging and auditing of security events
- Encryption, authentication and integrity protection for communications
- Tamper alarms
- Patching processes
- Configuration management
- Network segmentation
- Zero-trust configurations
- Access controls
- Service level agreements

# Stakeholder Responsibilities

To help open the dialogue on cyber security needs and hand-offs between stakeholders we have created a table to illustrate how responsibilities might possibly be allocated:

| Cyber Security Role | Stakeholder/ Actor |
|---|---|
| **Vision, Purpose and Objectives –** how will the building be used and what cyber security threat landscape might it experience? How will cyber security be managed and maintained in the life of the building? | **Occupier and/or developer in conjunction with the architect** |
| **Building Design –** what cyber security goals and standards should be met? What cyber security functions will be delivered, and by which systems? Ensuring that security requirements are specified for procurement. | **Architect, Engineers** |
| **Systems Design –** ensuring that cyber security foundations and key functions are built into individual systems and components (e.g. HVAC, fire and security, lifts etc.) and that individual systems can operate securely with others. | **Systems and Device Manufacturers** |
| **Build and Integration –** ensuring that security requirements are correctly procured and integrated and set up to correct security configurations. | **Building Contractor, Engineers** |
| **Facilities Operation/Maintenance –** managing and maintaining secure system operation, configurations and secure access for maintenance. | **Facilities Management, Engineers, Systems Manufacturing** |
| **Systems Maintenance –** keeping security up to date (e.g. patches) and supporting facilities management in having patches applied. | **Systems and Device Manufacturers** |
| **Building Occupation -** Integration of security status reporting and management with enterprise cyber security – e.g. identity management, vulnerability status & alert detection. | **Building Occupier, Facilities Management** |

# Conclusion

Ensuring that people and assets are safe from cyber hackers requires:

*Support from the Board and Executive Directors*

*A model of governance that empowers the central team and involves the business owners*

*Cybersecurity best practices that are part of the requirements and budget for the design, build and operations of the facility*

*Implementation of governance and security best practice across your organisation and supply chain with the cooperation of your customers, business partners and suppliers*

*Collaboration and adoption of cyber security responsibilities by a whole range of stakeholders*

# IoT Security Foundation's Smart Buildings Working Group

The Smart Buildings Working Group aims to:

- Build upon established best practice (e.g. NIST Cybersecurity Framework), its Compliance Framework [ref 15] and Secure Design Best Practice [ref 16]
- Encourage people from a broad range of stakeholders to engage with the group and collaborate to create, develop, adopt and implement best practice security for Smart Buildings

We believe that, only with participation from of people with responsibility or involvement with building systems can we be confident that the guidance is relevant, up-to-date and useful.

**To find out how you can be involved with the Smart Buildings Working Group, please contact: smartbuildings@iotsecurityfoundation.org**

# Appendix A - Communication Protocol Cyber Security Considerations

The following are examples of cyber security considerations that need to be taken into account for common communication protocols used by building management and automation systems:

- BACnet/MSTP is a master/slave token passing bus protocol used in a variety of building automation processes. If not secured properly, BACnet can expose device information such as location, status or software version and can allow unauthorised modification of device configurations. Many implementations also implement a 56-bit DES session key encryption which is a known vulnerability [ref 17]

- BACnet/Ethernet is a modern version of the BACnet protocol. It is potentially susceptible to spoofing and denial of service attacks but includes a cyber security specification [ref 18]

- Modbus/RTU is a legacy serial protocol used in a master/slave configuration. Modbus/RTU provides no encryption nor authentication and uses simple CRC32 checks for integrity protection

- Modbus/TCP is a modern version of Modbus that incorporates cyber security protections that include the use of Transport Layer Security (TLS) Version 1.2 for encryption and message authentication/integrity protection [ref 19]

- M-Bus enables the remote collection of meter values. Insecure M-bus configurations can open a smart building up to disclosure of consumption values and orchestrated remote disconnects [ref 20]

- LonTalk is used in lighting and HVAC systems. The LonTalk protocol includes no data encryption. Sender authentication is based on a 48-bit device authentication key [ref 21]

- DALI is the digital addressable lighting interface that enables the control, configuration and query of lighting devices

- EnOcean is a wireless energy harvesting protocol for building automation. EnOcean communications can be protected using an optional 32-bit message authentication code and AES 128-bit encryption

- OPC-Unified Architecture (UA) enables building automation by networking diverse devices together including HVAC, lighting, elevator and security systems. OPC-UA includes a security model that incorporates authentication, authorisation, auditability and availability protections

- KNX can be used as a backbone to connect multiple networks together. The protocol incorporates authentication and 128-bit encryption features

# References

The following organisations, publications and/or standards have been used for the source of references in this document:

- CEN (European Committee for Standardization)
- INCIBE (Spanish National Cybersecurity Institute)
- IoTSF (Internet of Things Security Foundation)
- ISO (International Organization for Standardization)
- OWASP (Open Web Application Security Project Foundation)
- Modbus Organization
- NIST (US National Institute of Standards and Technology)

The following references are used in this document:

1. Internet of Things Security Foundation
https://www.iotsecurityfoundation.org

2. Navigant Research, 2017, “IoT for Intelligent Buildings”
https://www.navigantresearch.com/reports/iot-for-intelligent-buildings

3. Pen Test Partners, “Too cold to work? School closed? Sure your BMS hasn’t been hacked?”
https://www.pentestpartners.com/security-blog/too-cold-to-work-school-closed-sure-your-bms-hasnt-been-hacked

4. Shodan, “search engine for Internet-connected devices”
https://www.shodan.io

5. SC Media, Bradley Barth, Jan. 2019, “Researchers develop proof-of-concept malware for attacking Building Automation Systems”
https://www.scmagazineuk.com/researchers-develop-proof-of-concept-malware-attacking-building-automation-systems/article/1523116

6. Safety Detective, “Major Security Breach Found in Hospital and Supermarket Refrigeration Systems”
https://www.safetydetective.com/blog/rdm-report

7. Forbes, July, 2017, " Criminals Hacked A Fish Tank To Steal Data From A Casino
https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino

8. Krebs on Security, October 2016 “Hacked cameras, DVRs Powered Todays Massive Internet Outage:
https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage

 

9. Wikipedia, “WannaCry ransomware attack”
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

10. PenTest Partners, “Maersk wasn’t hacked”
https://www.pentestpartners.com/security-blog/maersk-wasnt-hacked

11. Wired, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History”
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world

12. National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity”
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

13. OWASP, “Defense in depth”
https://www.owasp.org/index.php/Defense_in_depth

14. US Department of Homeland Security, “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies”
https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

15. IoT Security Foundation, “IoT Security Compliance Framework”
https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/IoTSF-IoT-Security-Compliance-Framework-Release-2.0-December-2018.pdf

16. IoT Security Foundation, “Secure Design Best Practice Guides”
https://www.iotsecurityfoundation.org/wp-content/uploads/2018/12/Best-Practice-Guides-Release-1.2.1-December-2018_final.pdf

17. NIST, NISTIR 7009, “BACnet Wide Area Network Security Threat Assessment”
https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=860911

18. Echelon, “LonTalk Protocol Specification, version 3.0”
http://www.enerlon.com/JobAids/Lontalk%20Protocol%20Spec.pdf

19. Schneider Electric, “MODBUS/TCP Security”
http://www.modbus.org/docs/MB-TCP-Security-v21_2018-07-24.pdf

20. Compass Security, Black Hat USA 2013, “Wireless M-Bus Security Whitepaper”
https://www.compass-security.com/fileadmin/Datein/Research/Praesentationen/blackhat_2013_wmbus_security_whitepaper.pdf

 

# Acknowledgements

We wish to acknowledge significant contributions from IoTSF members to this Whitepaper:

Brian Russell, VDOO connected Trust Ltd

Duncan Purves, Connect2 Systems Ltd

Emma Boakes, University of Portsmouth

Eric Salveggio, Micro Systems Automation Group

James Willison, Unified Security Ltd

John Moor, IoT Security Foundation

Michael Richardson, Sandelman Software Works Corporation

Nikdokht Ghadiminia, Birmingham City University

Pamela Gupta, Outsecure Inc

Pascal Mary, Hager Group

Paul Dorey, CSO Confidential

Paul Kearney, Birmingham City University

Salil Shukla, Cybersecurity Consultant

Sarb Sembhi, Virtually Informed Ltd

Peer Reviewers

Fabio Vignoli, Signify Ltd

Mark Zwolinski, University of Southampton

Trevor Hall, DisplayLink Ltd

IoT

Security Foundation