www.pipelinepub.com
Volume 20, Issue 9

Protecting IoT Devices and Users through Legislation and Trusted Standards

By: Thorsten Stremlau

Across the globe, Internet-of-Things (IoT) devices continue to underpin operations in most critical industries. The benefits these devices bring to businesses are invaluable, as is reflected in their continued popularity. By 2027, over 29 billion connected devices are expected to be online, a significant increase from the 17.08 billion currently in use.

However, 56 percent of businesses currently they lack the proper awareness and expertise to adequately prepare for an IoT-focused cyberattack. This should be a major cause of concern, not least because between 2022 and 2023 alone, these types of attacks increased by approximately 400 percent. If businesses lack the skills to protect themselves against attacks, then the onus falls on device manufacturers to ensure the necessary levels of cyber protection.

Thankfully, action has been taken worldwide to ensure manufacturers take their responsibilities seriously. A number of key acts and regulations have been rolled out by government institutions and regulators to enhance IoT device security within their respective markets.

Looking After the Consumer

In March 2024, the United States' Federal Communications Commission (FCC) introduced a voluntary labeling program for wireless IoT products. This includes the **U.S Cyber Trust Mark**, which will appear on wireless consumer technologies which have met the FCC's rigorous standards. The approved products will also display a QR code which leads to detailed security information such as whether its software patches are automatic.

Devices ranging from home security cameras and voice-activated shopping devices to internet-connected appliances, fitness trackers, and garage door openers have all been identified as suitable for the Cyber Trust Mark.

You only need to look to the news to see why. In 2023, Ring was accused by the Federal Trade Commission of failing to implement essential security measures in a **$5.6 million USD lawsuit**. As a result, hackers were able to take control of customer accounts, with over 117,000 consumers affected. Before this incident, **over 60 million records** were exposed by an unsecured fitness tracking database. It's these types of incidents the FCC is aiming to thwart through the Cyber Trust Mark.

Securing the Healthcare Sector

For IoT devices deployed in healthcare applications, there is another relevant piece of legislative action: the Protecting and Transforming Cyber Healthcare (PATCH) Act.

Healthcare institutions remain a key target for attackers, with two unfortunate records set in 2023: the most data breaches *and* the most breached records. The U.S Department of Health and Human Services' Office for Civil Rights (OCR) saw **725 reported data breaches and 133 million exposed records** reported to them that year alone, while **79.7 percent of the total data breaches** within the sector directly resulted from hacking attempts.

To better protect patients' sensitive information, the US Congress passed the PATCH Act in March 2023. Designed to provide a better framework for cybersecurity measures, this legislation empowers the U.S Food and Drug Administration (FDA) to take stronger action against manufacturers who lack proactivity when it comes to cybersecurity.

Manufacturers developing new IoT solutions for the healthcare sector must now provide details of their processes to the FDA so any vulnerabilities can be identified and mitigated prior to market launch. They must also disclose a Software Bill of Materials (SBOM), which details of all components found within a device, be it commercial, open-source or anything in between.

SBOMs remain an overlooked element of security. By checking catalogues of known exploits, businesses can see whether any components within their own devices are vulnerable. Yet less than 20 percent of organizations mandated them as part of their engineering practices in 2022. By making SBOMs a mandatory element of the PATCH Act, Congress is essentially dictating that businesses must now become familiar with these inventories and assigning them greater responsibility for protecting end users.

The View from Europe

Recent attacks have also highlighted the need for greater security for IoT devices sold throughout Europe. Attacks have been leveled against everything from **electric vehicle charging ports** and **rail communication equipment** to smart televisions and other consumer equipment.

With hacking attempts growing in both volume and complexity, the European Commission (EC) has introduced **"2014/53/EU"** to establish a regulatory framework for radio equipment. The "Radio Equipment Directive" (RED) outlines essential requirements for device manufacturers that must be fulfilled if they are to sell products within the European Union (EU). Despite a brief postponement, the RED is expected to become mandatory for any device type that transmits or receives radio signals. For example, 4G/LTE/5G cellular and Wi-Fi enabled devices, as well as radio, television, and GPS receivers, all fall under the directive. Cybersecurity is the major focus of RED Article 3.3. Network protection is covered under 3.3(d), with the directive ensuring that manufacturers must implement features that avoid harm to any communication networks. This also means devices cannot affect the functionality of services or websites they are linked to. Article 3.3(e) then looks at the protection of personal data and privacy, insuring measures to prevent unauthorized access to user's information are built into devices.

The main focus of Article 3.3(f) is mitigating fraudulent electronic payments and monetary transfers. To overcome these issues, manufacturers are compelled to add features within devices that deliver enhanced authentication controls to the user.

Cybersecurity: For King and Country

Another highly anticipated piece of legislation came into play in April 2024: the United Kingdom's **Product Security and Telecommunications Infrastructure (PTSI) Act** of 2022. Placing legal duties on electronic and smart home device manufacturers to implement basic security standards within UK-based products, the Act essentially forbids devices from accepting predictable or obviously insecure passwords. It also forces manufacturers to clearly publish contact details so users can report bugs and issues, and to advise consumers of realistic times they can expect software patches and updates.

Built on the back of the previous **IoT Code of Practice** launched in 2018, the PTSI Act applies to any organization looking to import or retail their devices within the region, with a fine up to £10m or 4 percent of a company's global revenue (whichever is highest) if they fail to adhere to its regulations. According to **the National Cyber Security Centre (NCSC)**, the scope covers the same types of devices as U.S Cyber Trust Mark, including specific references to smart domestic appliances such as connected light bulbs, plugs, kettles, ovens, fridges and washing machines.

While the latter may seem innocuous, hackers are now including other people's smart washing machines as part of a large botnet to carry out cryptocurrency mining, which requires an extortionate amount of energy. This type of activity is what the PTSI is aiming to stamp out.

Leveraging a "Trusted Computing" Approach

We are now seeing cybersecurity legislation for IoT devices rolled out at an unprecedented rate. However, if manufacturers want to truly protect device users, then it's important that they also look to adhere to the concept of "trusted computing." At the most basic level, this means adhering to the latest open standards, specifications, and technologies coming from within the computing industry.

For larger devices, the Trusted Platform Module (TPM) is a low-cost, secure crypto-processor which establishes secure operations by protecting a user's identity and sensitive data. TPMs hash sections of device firmware and software before they are executed and send them to the server for validation when the system attempts to connect to a network. If the details do not match, then the boot process will not take place, stopping any access or exploitation of stored data. The signing and verification capabilities offered through a TPM provide the baseline for the essential principles of verification, data protection, identity, and attestation.

Setting the Standards

In situations where the TPM is not suited for the device use case or architecture, the Device Identifier Composition Engine (DICE) can implement key security protocols in a more lightweight solution, providing an attestation architecture perfect for smaller devices. Easily integrated into existing frameworks and protocols, DICE equips manufacturers with the means to both create a cryptographically secure device identity and to verify software in newer devices.

Through DICE, a unique secret is held by the hardware; if an attack is executed against the device, the secret associated with the compromised layer can't be used to breach further layers, limiting the potential damage. In the DICE architecture, the hardware retains a foundational secret known as the Unique Device Secret (UDS). This secret underpins a layered security approach, where each layer independently generates its own unique secret, derived from the UDS. If an attack compromises one layer, then that secret cannot be utilized to compromise the subsequent layers, confining the scope of potential damage, and enhancing overall device security. Should any malicious code be detected, DICE will also facilitate a rapid re-keying process to preserve integrity.

Finally, the Cyber Resilient Module and Building Block Requirements (CyRes) specification can reduce malware persistence while protecting essential code and data. CyRes protects essential code and data within a device, while detecting vulnerabilities and corruption. They are also able to recover a system back to a reliable, trusted state in the event of compromization.

While not directly outlined in any of the recent legislation, these standards and specifications are just as vital to device security and should be the first port of call for manufacturers when it comes to protecting their devices.

•

Looking After the Consumer

In March 2024, the United States' Federal Communications Commission (FCC) introduced a voluntary labeling program for wireless IoT products. This includes the U.S Cyber Trust Mark, which will appear on wireless consumer technologies which have met the FCC's rigorous standards. The approved products will also display a QR code which leads to detailed security information such as whether its software patches are automatic.

Devices ranging from home security cameras and voice-activated shopping devices to internet-connected appliances, fitness trackers, and garage door openers have all been identified as suitable for the Cyber Trust Mark.

You only need to look to the news to see why. In 2023, Ring was accused by the Federal Trade Commission of failing to implement essential security measures in a $5.6 million USD lawsuit. As a result, hackers were able to take control of customer accounts, with over 117,000 consumers affected. Before this incident, over 60 million records were exposed by an unsecured fitness tracking database. It's these types of incidents the FCC is aiming to thwart through the Cyber Trust Mark.

Securing the Healthcare Sector

For IoT devices deployed in healthcare applications, there is another relevant piece of legislative action: the Protecting and Transforming Cyber Healthcare (PATCH) Act.

Healthcare institutions remain a key target for attackers, with two unfortunate records set in 2023: the most data breaches *and* the most breached records. The U.S Department of Health and Human Services' Office for Civil Rights (OCR) saw 725 reported data breaches and 133 million exposed records reported to them that year alone, while 79.7 percent of the total data breaches within the sector directly resulted from hacking attempts.

To better protect patients' sensitive information, the US Congress passed the PATCH Act in March 2023. Designed to provide a better framework for cybersecurity measures, this legislation empowers the U.S Food and Drug Administration (FDA) to take stronger action against manufacturers who lack proactivity when it comes to cybersecurity.

Manufacturers developing new IoT solutions for the healthcare sector must now provide details of their processes to the FDA so any vulnerabilities can be identified and mitigated prior to market launch. They must also disclose a Software Bill of Materials (SBOM), which details of all components found within a device, be it commercial, open-source or anything in between.

SBOMs remain an overlooked element of security. By checking catalogues of known exploits, businesses can see whether any components within their own devices are vulnerable. Yet less than 20 percent of organizations mandated them as part of their engineering practices in 2022. By making SBOMs a mandatory element of the PATCH Act, Congress is essentially dictating that businesses must now become familiar with these inventories and assigning them greater responsibility for protecting end users.

The View from Europe

Recent attacks have also highlighted the need for greater security for IoT devices sold throughout Europe. Attacks have been leveled against everything from electric vehicle charging ports and rail communication equipment to smart televisions and other consumer equipment.

With hacking attempts growing in both volume and complexity, the European Commission (EC) has introduced "2014/53/EU" to establish a regulatory framework for radio equipment. The “Radio Equipment Directive” (RED) outlines essential requirements for device manufacturers that must be fulfilled if they are to sell products within the European Union (EU). Despite a brief postponement, the RED is expected to become mandatory for any device type that transmits or receives radio signals. For example, 4G/LTE/5G cellular and Wi-Fi enabled devices, as well as radio, television, and GPS receivers, all fall under the directive. Cybersecurity is the major focus of RED Article 3.3. Network protection is covered under 3.3(d), with the directive ensuring that manufacturers must implement features that avoid harm to any communication networks. This also means devices cannot affect the functionality of services or websites they are linked to. Article 3.3(e) then looks at the protection of personal data and privacy, insuring measures to prevent unauthorized access to user’s information are built into devices.

The main focus of Article 3.3(f) is mitigating fraudulent electronic payments and monetary transfers. To overcome these issues, manufacturers are compelled to add features within devices that deliver enhanced authentication controls to the user.

Cybersecurity: For King and Country

Another highly anticipated piece of legislation came into play in April 2024: the United Kingdom’s Product Security and Telecommunications Infrastructure (PTSI) Act of 2022. Placing legal duties on electronic and smart home device manufacturers to implement basic security standards within UK-based products, the Act essentially forbids devices from accepting predictable or obviously insecure passwords. It also forces manufacturers to clearly publish contact details so users can report bugs and issues, and to advise consumers of realistic times they can expect software patches and updates.

Built on the back of the previous IoT Code of Practice launched in 2018, the PTSI Act applies to any organization looking to import or retail their devices within the region, with a fine up to £10m or 4 percent of a company’s global revenue (whichever is highest) if they fail to adhere to its regulations. According to the National Cyber Security Centre (NCSC), the scope covers the same types of devices as U.S Cyber Trust Mark, including specific references to smart domestic appliances such as connected light bulbs, plugs, kettles, ovens, fridges and washing machines.

While the latter may seem innocuous, hackers are now including other people’s smart washing machines as part of a large botnet to carry out cryptocurrency mining, which requires an extortionate amount of energy. This type of activity is what the PTSI is aiming to stamp out.

Leveraging a “Trusted Computing” Approach

We are now seeing cybersecurity legislation for IoT devices rolled out at an unprecedented rate. However, if manufacturers want to truly protect device users, then it’s important that they also look to adhere to the concept of “trusted computing.” At the most basic level, this means adhering to the latest open standards, specifications, and technologies coming from within the computing industry.

For larger devices, the Trusted Platform Module (TPM) is a low-cost, secure crypto-processor which establishes secure operations by protecting a user's identity and sensitive data. TPMs hash sections of device firmware and software before they are executed and send them to the server for validation when the system attempts to connect to a network. If the details do not match, then the boot process will not take place, stopping any access or exploitation of stored data. The signing and verification capabilities offered through a TPM provide the baseline for the essential principles of verification, data protection, identity, and attestation.

Setting the Standards

In situations where the TPM is not suited for the device use case or architecture, the Device Identifier Composition Engine (DICE) can implement key security protocols in a more lightweight solution, providing an attestation architecture perfect for smaller devices. Easily integrated into existing frameworks and protocols, DICE equips manufacturers with the means to both create a cryptographically secure device identity and to verify software in newer devices.

Through DICE, a unique secret is held by the hardware; if an attack is executed against the device, the secret associated with the compromised layer can't be used to breach further layers, limiting the potential damage. In the DICE architecture, the hardware retains a foundational secret known as the Unique Device Secret (UDS). This secret underpins a layered security approach, where each layer independently generates its own unique secret, derived from the UDS. If an attack compromises one layer, then that secret cannot be utilized to compromise the subsequent layers, confining the scope of potential damage, and enhancing overall device security. Should any malicious code be detected, DICE will also facilitate a rapid re-keying process to preserve integrity.

Finally, the Cyber Resilient Module and Building Block Requirements (CyRes) specification can reduce malware persistence while protecting essential code and data. CyRes protects essential code and data within a device, while detecting vulnerabilities and corruption. They are also able to recover a system back to a reliable, trusted state in the event of compromization.

While not directly outlined in any of the recent legislation, these standards and specifications are just as vital to device security and should be the first port of call for manufacturers when it comes to protecting their devices.