FEATURE

Building Security Into IoT Devices

How SB 327 Highlights Modern Legislative Challenges

There will be more than 64 billion Internet of Things (IoT) devices by 2025.[1] Many of these devices lack necessary security features and could be discovered using IoT search engines. In a study by the UK government authority Centre for the Protection of National Infrastructure (CPNI), several hundred thousand unprotected devices were found on the Internet.[2] In light of such risk, US State of California Senate Bill 327 Information Privacy: Connected Devices (SB 327) and similar legislative initiatives aim at addressing these practical issues within a judicial capacity.

SB 327 was signed by the governor of the State of California in September 2018 and will go into effect in January 2020.[3] While the bill's title ties it to privacy (as it is a protected fundamental human right), its demanding stipulations address the security of connected devices. The effect of the law is not limited to one US state or just the United States, since it can be difficult for device manufacturers to control where their products are sold. In addition, launching a less secure and less privacy-friendly version of a product anywhere can be a very unpopular decision.

Above all, the law has global impact, as the United States is a large market for Internet of Things (IoT) products. That is why SB 327's effect, like the US California Consumer Privacy Act (CCPA),[4] seems to go beyond the borders of California and the United States. At the same time, it can be expected that other US states may develop their own IoT laws to adjust the scope of their breadth, such as Oregon's House Bill 2395.[5]

SB 327 serves as an illuminating case study in the evolution of privacy through legislation. While it can be attested that privacy is a fundamental right, the same cannot be done for security: In this way, the connected devices law exemplifies a burgeoning domain of legislature that is developed to seek the middle ground among privacy, security and technology.

Farbod H. Foomany, Ph.D., CISSP
Is a technical program manager of security research at SD Elements/Security Compass. His studies are focused on the criminological and security applications of biometrics. Foomany has been involved in academic research and industry projects in the areas of smart card Java application development, Java EE-based enterprise e-banking application development, privacy and security in software development, secure design of enterprise applications, advanced signal processing techniques in speech and sound processing, biomedical engineering, and the evaluation of the social and privacy aspects of biometric identification. Foomany has published and presented his work on signal processing and security in several IEEE conferences and journals, the *ISACA® Journal*, crime science conferences and networks, the International Association of Privacy Professionals (IAPP) conference, and The Open Web Application Security Project (OWASP) Global AppSec Conferences.

Nathanael Mohammed
Is a technical writer at SD Elements/Security Compass. He specializes in communicating about technology, with a focus on security, privacy and compliance. He has been involved with projects concerning EU General Data Protection Regulation requirements and translating compliance policies to executable processes in Agile software development, and he has published articles in the *ISACA Journal* and *IAPP Privacy Tech*.

To Whom Does SB 327 Apply?

SB 327 applies to manufacturers of devices and physical objects sold in California and capable of connecting to the Internet. The law specifies that the object's connection to the Internet can be direct or indirect. Manufacturers of mobile phones, laptops, tablets, e-book readers, Bluetooth headphones (that are indirectly connected to the Internet), smart IoT thermostats, smart TVs and any other device that can connect to the Internet (and are assigned an IP or Bluetooth address) should comply with this law. **Figure 1** depicts the rules of how the law is applicable and what needs to be done to comply with the law. However, when writing a software library or software development kit (SDK) that may be used in an IoT device, the law does not apply. There needs to be a physical object or device in question for SB 327 to apply.

While connected devices can be anything, the following list of consumer IoT devices gives an idea about the range of applications:

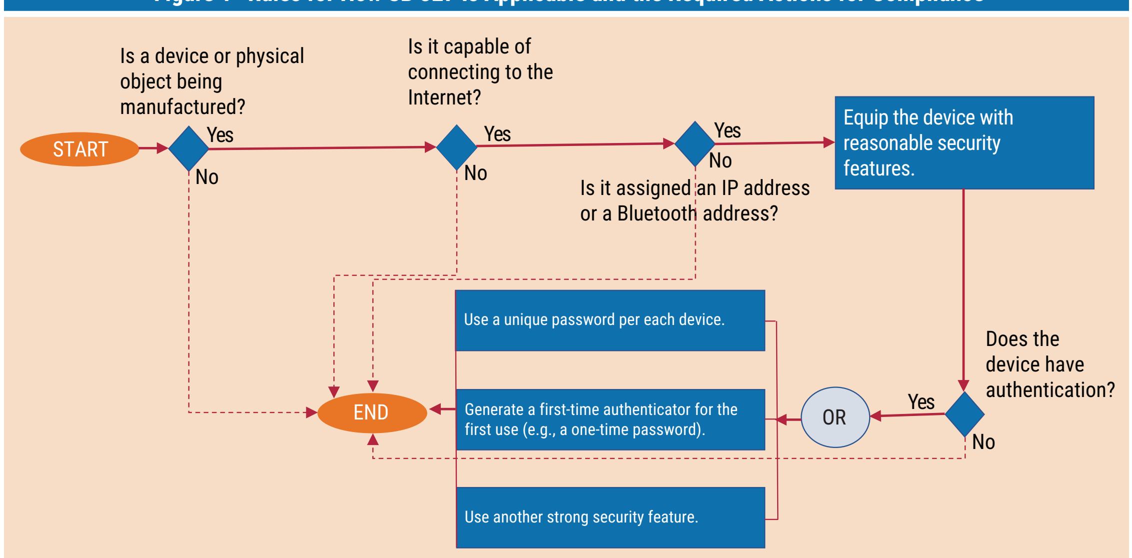
- Connected children's toys and baby monitors
- Connected safety-relevant products such as smoke detectors and door locks
- Smart cameras, TVs and speakers
- Wearable health trackers
- Connected home automation and alarm systems
- Connected appliances (e.g., washing machines, refrigerators)
- Smart home assistants[6]

Understanding the Law: Requirements for Complying With SB 327

The California State Legislature consists of two houses, the Senate and Assembly. SB 327 was initiated in the Senate and was designed to protect the privacy and security of connected devices in the broadest way possible. Through an exchange of amendments, the heart of the law was finalized into two parts.

Subdivision (a) requires equipping devices with reasonable and appropriate security features. Subdivision (b) is slightly harder to decipher, but its core message is illustrated in **figure 1**. The most important point is that while it offers two solutions for secure user authentication, it does not limit what are considered appropriate solutions to only those two. In other words, when the law states "if either of the following requirements are met," it should not be interpreted as "...if and only if..." In fact, password authentication may no longer be necessary in many situations. However, it is easier to resort to one of the two suggestions of subdivision (b) for compliance—that is, either using unique passwords for each device or using a means for first-time user generated authentication (such as tokens and passwords).

Figure 1—Rules for How SB 327 Is Applicable and the Required Actions for Compliance



It is worth noting that SB 327 was not designed to be a "password bill," and subdivision (b) was added to the draft to reconcile it with a similar assembly bill, AB 1906.[7] In fact, the scope of the bill was initially broader and included requirements for the consent and notice of data collection.[8] The initial draft expressed concerns about widespread data breaches and the security and privacy of children and families.[9] Reports of hacked toys, nonconsensual data collection by smart TVs and accounts of a doll that could be programmed to utter obscenities to children demonstrate the motivation behind the bill.[10] The draft also quotes the reports of more than 657 breaches (49 million records) received by the California Attorney General between 2012 to 2015.[11] These facts are crucial in understanding the mission and intended scope of this law and similar initiatives.

Reasonable Security Features

The crux of the law concerns equipping Internet-connected devices with reasonable security features. The law asks for reasonable security features that are appropriate to the nature and function of the device, appropriate to the information it handles, and protect the device. Many have found this wording to be too broad and vague.[12] Some people have even criticized this add-on approach to information security.[13] It will take time to see how subdivision (a) will be interpreted in the future.

Using IoT Security Frameworks to Develop Reasonable Security Features

Several public projects have tried to build frameworks for the development and evaluation of IoT security controls and features necessary for SB 327. It is useful to analyze some of those initiatives because, ultimately, it is unknown what the lawmakers of SB 327 intended by their broad statements until they regulate it through legal ramifications. In the interim, the following frameworks provide a starting point for implementing best practices for addressing SB 327 compliance.

The OWASP IoT Top 10

The Open Web Application Security Project (OWASP) IoT Top 10 and its subproject, IoT Attack Surface Areas Project, attempt to provide guidelines for manufacturers and consumers about IoT security issues.[14] The first vulnerability in the IoT Top 10 is weak, guessable or hard-coded passwords, and number six on the list is insufficient privacy protection. The OWASP IoT Top 10 focuses on simplicity. While these projects aim to create a conceptual structure for understanding, classifying and addressing IoT vulnerabilities, a more comprehensive framework is needed for securing specific aspects of a product. For example, when securing web interfaces, a detailed checklist, such as the Application Security Verification Standard (ASVS),[15] is more suitable. In the latest version of ASVS, a separate appendix C is devoted to IoT verification requirements.

> "THE LAW ASKS FOR REASONABLE SECURITY FEATURES THAT ARE APPROPRIATE TO THE NATURE AND FUNCTION OF THE DEVICE, APPROPRIATE TO THE INFORMATION IT HANDLES, AND PROTECT THE DEVICE."

The OWASP IoT Top 10 and its subprojects provide great raw material for a team of security engineers to examine vulnerabilities and attack surface areas to build a secure development program.

The UK Government's Code of Practice for Consumer IoT

The UK government has developed useful guidance on securing IoT devices to retailers and manufacturers in a series of projects that include best practices in a "Secure by Design" collection,[16] "Code of Practice for Consumer IoT Security"[17] and a mapping between this code of practice against a number of other major IoT security published documents and standards.[18] Completely aligned with SB 327, the first guideline (out of 13) in the code of practice is "No default passwords." Similarly, the documentation includes technical specification by the independent not-for-profit European Telecommunications Standards Institute (ETSI), which produces standards for telecommunications at a global level. ETSI provides 13 provisions for "Cyber Security for Consumer Internet of Things,"[19] and provision 4.1-1 recommends that the passwords of IoT devices be unique and not resettable to any universal factory values, much like SB 327.

> TO ADDRESS THE CHALLENGE OF SECURING DOMAINS SUCH AS IOT DEVICES, VARIOUS ATTEMPTS AT BUILDING A SECURITY TAXONOMY WERE USED TO ARRIVE AT A TAXONOMY OF SECURITY WEAKNESSES AND THEIR RELEVANT SECURITY FEATURES AND MEASURES.

Among the documentation is a simple and well-written guide published by the UK's National Cyber Security Centre (NCSC)[20] on utilizing passwords. The guide contains seven tips for developing a password policy and some analysis about the recommendations.

The second and third recommendations of the code of practice concern implementing a vulnerability disclosure policy and keeping software up to date. In a closely related initiative, the UK government has published a proposal for mandating a few security requirements for consumer smart devices.[21] These requirements are focused on the top three main guidelines in the code of practice: unique passwords, vulnerability disclosure policies and security updates.

The similarities between the UK regulatory proposal and SB 327 show how popular belief and dominant perspectives are structured around the importance of these essential features. It can be helpful for organizations to prioritize the implementation of the UK's 13 guidelines over other IoT guidance. In comparison with OWASP Top 10 (which highlights top 10 vulnerabilities), the UK code of practice has a more prescriptive tone. It provides high-level guidance on addressing the most significant consumer IoT security issues. Implementing those 13 guidelines and considering NCSC's recommendations for passwords can help organizations be compliant with SB 327.

The European Union Agency for Cybersecurity Recommendations

The European Union Agency for Cybersecurity's (ENISA's) IoT Tool[22] and ENISA's "Baseline Security Recommendations for IoT"[23] define security measures and practices for baseline and better security in IoT (and for smart cities and smart cars). Security measures are categorized by security domains and threat groups.

There are more than 80 controls identified by ENISA on the list. The controls are technical measures; policies; or organizational, people and process measures. These controls are mapped to the OWASP IoT Top 10 (and other standards) wherever possible. The descriptions are short and need more interpretation in many cases. For example, a technical control reads: "Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc.,"[24] which is broad enough to require a web application security program.

These recommendations provide a more high-level yet accurate presentation of IoT security requirements and can be used in conjunction with the OWASP IoT top 10 and ASVS to ensure full coverage of required activities. As with the OWASP IoT Top 10 and attack surface, these requirements need to be further broken down and detailed for specific use cases and technology stacks.

Scope and Overview of IoT Security Features

As demonstrated, security and privacy controls can be defined on various levels of granularity on the policy-to-procedure scale. Various initiatives and research groups have attempted to provide classifications for security vulnerabilities and controls at different granularity levels. Some classify security requirements into 12 groups: identification, authentication, authorization, auditing, confidentiality, integrity, availability, nonrepudiation, immunity, survivability, secure maintenance and privacy requirements.[25] Others define seven pernicious kingdoms of security that are widely quoted and cited.[26] Each of these sources serves as a helpful reference for identifying and classifying software security issues in the domain of IoT.

To address the challenge of securing domains such as IoT devices, various attempts at building a security taxonomy were used to arrive at a taxonomy of security weaknesses and their relevant security features and measures. **Figure 2** provides a simplified snapshot of this taxonomy to demonstrate the work's scope. Under each abstract problem, there are several weaknesses and accompanying security measures and controls that can be considered security features. Additionally,

Figure 2—Overview of the Categories of Security Problems (in the IoT Domain)

Security Goal	Weakness Categories	Weakness Variant
Data Confidentiality		Timing leakage
		Error response leakage
		Leakage through logs, media and messages
	Unprotected data in transit	
	Unprotected data at rest	
Access Control	Weak/missing authentication	
		Missing authentication
		Weak authentication
		Weak/lack of authorization
		Weak key/credential protection
		Session management
	Privilege escalation and unnecessary permissions/ privileges	
		Lacking compartmentalization/need to know
Data/System Integrity	Missing or weak input validation	
		Missing target validation
		Cross-site scripting
	Missing or weak encoding	
	(String) injections	
	Data misrepresentation	
		Visual misrepresentations
		Mime confusion
	Jailbreak detection circumvention	
	Trusting client data/operation	
	Lack of obfuscation and anti-debugging	
	Weak/lack of malicious agent detection	
	Cryptographic issues	
		Wrong/weak cryptographic operations
		Weak random variables
Service Availability	Complex or large inputs	
	Lack of priority/emergency design	
	Single point of failure	
	Lacking fault tolerance	
	Faulty exception and error handling	
	Failing unsafe	

Security Goal	Weakness Categories	Weakness Variant
Code Quality		Integer issues
		Buffer and pointer issues
		Type conversions and format strings
	Unclarity of code/error prone practices	
	Using unmanaged code	
	Using dangerous functions	
	Workflow and logic errors	
		Timing and race condition
		Unstable/wrong workflow
Nonrepudiation	Lack of authenticity proof/check	
		Not providing authenticity proof/ feature
		Not checking authenticity/ integrity
Secure System Design	Lacking design for data flow/ boundaries	
	Missing/weak/exploitable backup/restore	
		Lack of information about/ control over third party
		Lack of interface to settings/ parameters
		Missing documentation
	Lacking security control routines	
	Unsecure design features	
		Interface design issues
	Weak/lack of logging and monitoring	
		Lack of log protection
		Insufficient logging
		Lack of monitoring/reduction/ reporting
	Lack of updates	
	Ignoring security warnings and reports	
	Unnecessary features	
		Debuggability
		Remote access/activation
Legal and Privacy Aspects	Lack of profanity blocking	
	Privacy violation	
		Spam emails
		Consent
		Notice

there is a control database that currently has more than 550 weaknesses and more than 1,350 security features and controls in various categories of architecture and design, development, requirements, deployment, and testing.[27] These are filtered based on the applicability criteria for each project. As demonstrated through the study of IoT frameworks, high-level control classes can be decomposed into detailed lists of controls for various technologies. These lists can have hundreds of controls and should be refined based on some applicability rules for those technologies.

For organizations that must meet the challenge of complying with SB 327, determining actionable guidelines for “reasonable security features” is alleviated by these existing taxonomies and control databases. The taxonomy presented previously demonstrates the size of work needed to develop IoT devices with security at the forefront.

Conclusion

SB 327 highlights the frontier of legislating privacy and security. Although the movement toward conceiving of and enforcing the privacy and security of connected devices is gaining traction, as seen in comparable alignment among various other legislative initiatives, there exists few documented examples of how the privacy and security of connected devices should be enforced or how organizations should address compliance.

A good starting point for exploring and developing privacy and security controls for any organization actively seeking to comply with IoT laws is the UK IoT guidelines. In addition to these, developing technology-specific security controls can be completed using technical lists of requirements and vulnerabilities, such as the IoT Top 10, Attack Surface, ASVS App C and ENISA recommendations. These controls can be formed in steps and layers of abstraction but require the expertise of a security engineering team.

While security taxonomies and databases for several programming languages and technologies exist today, it is necessary to define criteria for when they become applicable to the IoT context to best manage and organize these tasks.

This examination of IoT regulations and security controls underscores the paradigm that has become dominant as security, privacy and usability intersect—where the domain was once largely open to interpretation, IoT device security and privacy is increasingly accessible to the communities that not only influence their standards, but that must also abide by them.

Endnotes

1. Newman, P.; “IoT Report: How Internet of Things Technology Growth Is Reaching Mainstream Companies and Consumers,” *Business Insider*, 28 January 2019, *https://www.businessinsider.com/internet-of-things-report*
2. Centre for the Protection of National Infrastructure, “Simplifying Your Approach: Password Guidance,” UK, 2015, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf*
3. California Legislative Information, SB 327 Information Privacy: Connected Devices, USA, 28 September 2018, *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327*
4. Goldman, E.; “A Status Report on the California Consumer Privacy Act,” Technology & Marketing Law Blog, 14 February 2019, *https://blog.ericgoldman.org/archives/2019/02/a-status-report-on-the-california-consumer-privacy-act.htm*
5. Winston & Strawn LLP, “Oregon Becomes Second State to Pass Internet of Things Data Security Law,” Casetext, 21 August 2019, *https://casetext.com/analysis/oregon-becomes-second-state-to-pass-internet-of-things-data-security-law*
6. European Telecommunications Standards Institute, “Cyber Security for Consumer Internet of Things,” 2019, *https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf*
7. California Legislative Information, SB 327 Information Privacy: Connected Devices 06/29/18- Assembly Privacy and Consumer Protection, *https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180SB327*

8 California Legislative Information, SB 327 Information Privacy: Connected Devices 05/17/17- Senate Floor Analyses, *https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180SB327*
9 *Ibid.*
10 *Ibid.*
11 *Ibid.*
12 Marsh, C.; "California's New IoT Security Law Sparks Conversation in Sacramento's Tech Community," LinkedIn, 2 January 2019, *https://www.linkedin.com/pulse/californias-new-iot-security-law-sparks-conversation-tech-marsh/*
13 Errata Security, "California's Bad IoT Law," 10 September 2018, *https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.XRvBHpNKjfZ*
14 The Open Web Application Security Project, "OWASP Internet of Things Project," *https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project*
15 The Open Web Application Security Project, "Category: OWASP Application Security Verification Standard Project," *https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project*
16 Gov.UK, "Secure by Design," 6 June 2019, *https://www.gov.uk/government/publications/secure-by-design*
17 Department for Digital, Culture, Media & Sport, "Code of Practice for Consumer IoT Security," United Kingdom, October 2018, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf*
18 Department for Digital, Culture, Media & Sport, "Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security," United Kingdom, October 2018, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/774438/Mapping_of_IoT__Security_Recommendations_Guidance_and_Standards_to_CoP_Oct_2018.pdf*
19 *Op cit* European Telecommunications Standards Institute
20 Centre for the Protection of National Infrastructure, "Simplifying Your Approach: Password Guidance," United Kingdom, 2015, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf*
21 European Union Agency for Cybersecurity, "ENISA Good Practices for IoT and Smart Infrastructures Tool," *https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool*
22 European Union Agency for Cybersecurity, "ENISA Good Practices for IoT and Smart Infrastructures Tool," *https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool*
23 European Union Agency for Cybersecurity, "Baseline Security Recommendations for IoT," 2017, *https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot*
24 *Ibid.*
25 Merkow, M. S.; L. Raghavan; *Secure and Resilient Software Development*, Auerbach Publications, USA, 2010
26 Tsipenyuk, K.; B. Chess; G. McGraw; "Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors," *IEEE Security & Privacy*, vol. 3, iss. 6, 2005, p. 81-84
27 Security Compass, "SD Elements Product Content," 2019, *https://www.securitycompass.com/sdelements/content/*