SEC – 101: Security Regulation and How it will Drive Innovation in IoT
Silicon Labs Announces New Security Services

- Custom Part Programming Service (CPMS) for security provisioning
- Long Term SDK Support Service (LTSSS)
- Be sure to attend SEC-102: Enforced Security Regulations will Demand a Security Warranty in IoT Devices for more details
Regulation at the US National Level is Accelerating

IoT Cybersecurity Act of 2020

The Senate yesterday by unanimous consent passed legislation to mandate certain security requirements for internet of things devices purchased by the federal government, moving forward legislation that had been stalled on Capitol Hill since 2017.

Cyber Shield Act

Sen. Ed Markey (D-MA) and Rep. Ted Lieu (D-CA-33) reintroduced the Cyber Shield Act on March 24, 2021. The proposed legislation is not new to Congress; Sen. Markey and Rep. Lieu previously introduced the Cyber Shield Act in both 2017 and 2019. However, the bill never made it to a vote in either the House or the Senate.

As written, the Cyber Shield Act calls for the creation of a voluntary cybersecurity certification program for Internet of Things (IoT) devices. IoT devices span a wide
Executive Order on Improving the Nation’s Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the

(i) Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the Federal Trade Commission (FTC) and representatives of other agencies as the Director of NIST deems appropriate, shall identify IoT cybersecurity criteria for a consumer labeling program, and shall consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law. The criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products. The Director of NIST shall examine all relevant information, labeling, and incentive programs and employ best practices. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation.
IoT Security Legislation... States are the first movers

Multiple states have already introduced bills that resemble California’s CCPA example:

- Virginia (HB 2793)
- Oregon (HB 2395)
- Hawaii (SB 418)
- Maryland (SB 0613)
- Massachusetts (SD 341)
- New Mexico (SB 176)
- New York (S00224)
- Rhode Island (SB 234)
- Washington (SB 5376)

- **California Consumer Privacy Act (§ SB-327)**
  - Introduced: Feb 13, 2017
  - Approved: Sept 28, 2018
  - Effective: Jan 1, 2020 (<3yrs)

- Requires ‘reasonable security features’
  - Appropriate to the nature and function of the device
  - Appropriate to the information it may collect, contain, or transmit
  - Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure
  - Pre-programmed passwords are unique in each device manufactured

Already accounts for ~30% US population
Governmental Regulatory Landscape – United States

Australia

Congress
Department Commerce

Vulnerability Disclosure
Firmware Updates
Software Transparency

Cyber Shield Act
IoT Improvement Act

NISTIR 8259A
NISTIR 8259D

ISO 27402

Legend

Concern

Federal Requirement

Device Identification (Secure Identity)
The IoT device can be uniquely identified logically and physically.

Device Configuration (Secure Boot)
The IoT device’s software and firmware configuration can be changed, and such changes can be performed by authorized entities only.

Data Protection
The IoT device can protect the data it stores and transmits from unauthorized access and modification.

Logical Access to Interfaces (Secure Debug)
The IoT device can limit logical access to its local and network interfaces to authorized entities only.

Software and Firmware Update (Secure OTA Updates)
The IoT device’s software and firmware can be updated by authorized entities only using a secure and configurable mechanism.

Cybersecurity Event Logging
The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.
IoT Code of Practice

TS 103 645 / EN 303 645
Cyber Security for Consumer Internet of Things
- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store credentials and security-sensitive data
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is protected
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data

Legend
- Published
- Pending
Challenging Landscape for Our Customers

**LAWs**
What is required legally?

**STANDARDS**
What is required functionally per market?

**DEVICE PROFILES**
What is required functionally per device type?

**CERTIFICATION SCHEMES**
How do you standardize labs and testing of devices?

**GOVERNMENTS**

**GOVERNMENTS**

**COMPANIES**

**GOVERNMENTS**
ioXt Alliance is Tackling Device Security Profiles and

450+ MEMBER COMPANIES
35+ COUNTRIES
Example of an ioXt Base Device Security Profile

- **No Universal Passwords**
- **Must have user authentication**
- **Interfaces secured against remote attack**
- **Interfaces secured against physical attack**
- **Interfaces secured against proximity attack**

**Selected Security Components**

- **Sw images and apps are signed and verified**
- **Software is maintained and updated**
- **Software updates supported**
- **Security Updates Automatically Applied**

**PSA/SESIP IC Level Certification**

- **Anti-rollback**
- **Secure boot based on hardware**
- **Software image verified at boot**
- **Limit Downgrade attack**
- **Proven Cryptography**
- **SW images and apps are signed and verified**

**Secure OTA Bootloader**

- **Public bug bounty program**
- **Responsible disclosure**
- **Monitoring security relevant components**
- **Vulnerability Disclosure Program in place**
- **Expiration Date or EOL policy**

**Related Certifications**

- **ZigBee Platform Certifications**
- **Thread Platform Certifications**
- **PSA/SESIP IC Level Certification**
- **NIST CAVP**
- **Secure Debug & Debug Glitch Mitigation**
- **With Module Certification and Custom Provisioning Services**
- **Two factor authentication**
- **Independently reviewed protocol**
- **Standard Cryptography**
Smart Speaker Profile

With Silicon, Modules, and Custom Provisioning Services

- Side channel protection
- Microphone hardware mute switch
- No unencrypted data between processor and network interfaces
- Data at rest is secured
- Microphone is optically shielded
- Local debug is disabled
- De-register device when config is changed
- Interfaces are secured against proximity attack
- Interfaces are secured against remote attack
- Independently reviewed protocol
- Standard Cryptography
- Options for gating command on voice commands
- Factory data reset removes account credentials and other PII
- Factory data reset removes network credentials
- Mfg has a update patch policy
- Anti-rollback
- Secure boot based on hardware
- Software image verified at boot
- Proven Cryptography
- SW images including plug-ins and apps are signed and verified
- Mfg has a update patch policy
- Security Updates Automatically Applied
- SW images including plug-ins and apps are signed and verified
- Public bug bounty program
- Responsible disclosure
- Monitoring security relevant components
- Software updates supported
- Vulnerability Disclosure Program in place
- Security updates are made available
- Software is maintained and updated
- Software updates supported
- Vulnerability Disclosure Program in place

No Universal Passwords
Secured Interfaces
Proven Cryptography
Security By Default
Verified Software
Automatic Software Updates
Vulnerability Reporting Program

Level 1
Level 2
Level 3
Level 4
Level 5
Level 6

Required

#workswith
QR Code – Picture of Device Appears with Certification

ioxt

Pixel 4a
Google

QD4A.200805.003

ioxt CERTIFIED

Meet Pixel 4a, the helpful Google phone at a helpful price. It comes packed with the things you want most in a phone. You can take great photos, even if the lighting isn’t right. It can even capture the Milky Way. (Yes, that Milky Way.) It has an Adaptive Battery that lasts up to 24 hours. And with the new Google Assistant, you get the help you need, fast. Pixel 4a comes with all this and more, for a lot less than you’d expect.

Visit Pixel 4a web page

Dispute Certification
Report Vulnerability
Scalable Crowd Sourced Certification Policed by Certification Bounties

Method 1 - Self Assessment
Manufacturer Submits Security Information

Method 2 - Lab Assessment
Manufacturer Chooses Lab for Security Analysis

Researchers
Independent researchers submit security issues for any certified product (either self- or lab-certified) on the ioXt site and are rewarded for all verified flaws.

Manufacturer Certifies Device
Inheritance through
Silicon Labs ioXt Certified Components

1. Customer Selects Silicon Labs
2. Silicon Labs Certified Modules Presented
3. A mouse hover over the module gives a module description and link to Silicon Labs Website
4. Select a module
   • Auto-completes security survey
Insert Video here

- Play video of certified platform demo from Brad Ree at ioXt Alliance
Silicon Labs Makes It Easy to Protect the IoT Ecosystem

Works With Device
3rd Party Device Manufacturer only needs to do a delta certification against the specific Ecosystem Security Profile

Silicon Labs ioXt Certifications can be inherited by 3rd Party Device Manufacturer

Silicon Labs Security Certifications Inherited by 3rd Party Ecosystem Device Manufacturers
A Paradigm Shift in the Security Philosophy to “Zero Trust”

**Yesterday**
- Everything behind the gateway is trusted
- And assume devices are trusted perpetually

**Today**
- Nothing on the subnet can be trusted
- Authenticate device identity before allowing it to join and continuously re-authenticate
Keeping a Secure Identity Secret in the End Node is now in Scope

Comms MCU
  • Secure Stack
  • Secure Boot
  • Secure Debug
  • Network Crypto
  • Identity
    • Crypto
    • Micro Operation
    • Secure the
      Micro Operation,
      Secure Keys,
      & Crypto

Secure the Comms Pipe with Crypto

$3800 USD

ChipWhisperer-Pro Kit

$3300 USD

ChipSHOUTER®

Electromagnetic fault injection allows attacks and testing done in situ, without the need to use special development boards or to modify the target board. It is a powerful attack method that requires careful consideration of how it might apply to your product.
Securing Ecosystems with Secure Identity Provisioning from Silicon Labs

- Certificate Authority
- Certificate Signing Request (CSR)
- Approved by Ecosystem
- Pre-register Devices in bulk
- Secure Identity
- ODM/OEM/CM
- IoT Devices
- Ecosystem Cloud Provider
## Secure Vault™ Right Level of Security to Protect Identities

<table>
<thead>
<tr>
<th>Feature</th>
<th>Base</th>
<th>Mid</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>True Random Number Generator</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Crypto Engine</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure Application Boot</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure Engine</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure Boot with RTSL</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure Debug with Lock/Unlock</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DPA Countermeasures</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Anti-Tamper</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure Attestation</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure Key Management</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Advanced Crypto</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- **Base**
  - ✓: Available
  - —: Not Available

- **Mid**
  - ✓: Available
  - Optional: Not Available

- **High**
  - ✓: Available
Related Security Focused Works With Sessions

- **Works With Sessions**
  - SEC-102: Enforced Security Regulations will Demand a Security Warranty in IoT Devices
  - SEC-201: Applying Security to Verify Deployed Products are Authentic
  - SEC-301: Hands on Security
  - SEC-PNL: Smart Home Security and the User Experience

- Join ioXt Alliance and get ahead of the regulations [www.iuxtalliance.org](http://www.iuxtalliance.org)