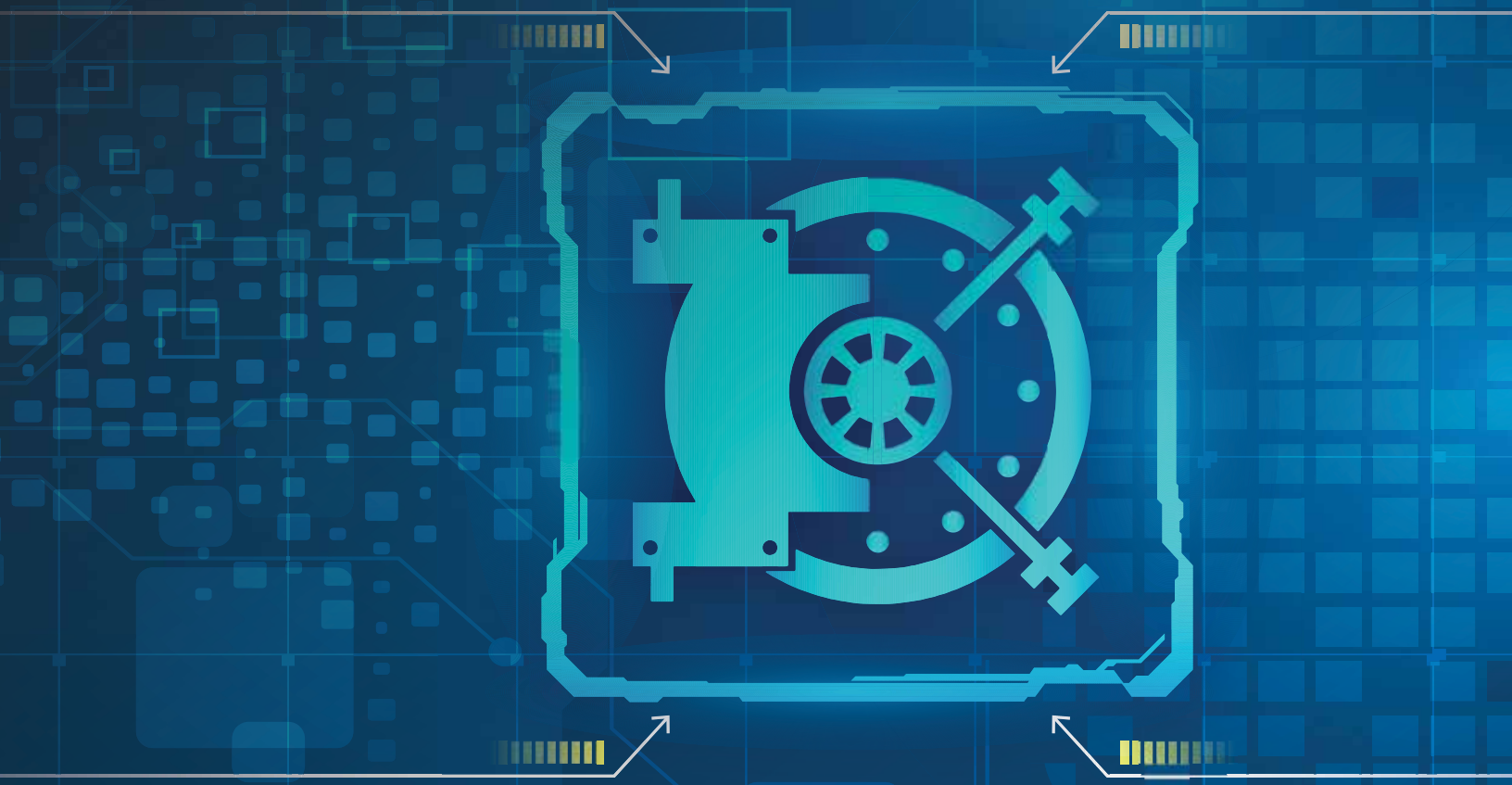
SILICON LABS

Preparing for Next-Generation Cyber Attacks on IoT

By: Mike Dow



Introduction

IoT attacks generally happen in two ways – remote attacks that target a device from a distance, usually over the Internet, and local attacks where the attacker has possession of the device they're targeting. Remote, or logical attacks, target the software while local, or physical attacks, target the silicon inside the device itself. Over the last 20 years, the majority of cyberattacks have been remote attacks from the cloud carried out by individuals with simple goals – to see if they can do it, or to access some protected information. But over the last four or five years, we've seen the rise of much more organized groups focused on extortion via ransomware attacks. This "cyber mafia" are large criminal enterprises with hundreds of employees and coordinated extortion operations. In the past, most ransomware attacks have focused on extorting individuals. But today, the value of the attacks has increased to millions of dollars per attack, and the targets have shifted to larger and larger businesses. Instead of shaking down individuals for a few hundred dollars, they are going after millions from corporate targets.

"Going into 2019, CrowdStrike Intelligence anticipated that big game hunting (BGH) — targeted, criminally motivated, enterprise-wide ransomware attacks — was expected to continue at least at the 2018 pace. However, what was observed was not just a continuation but an escalation. Ransom demands grew larger. Tactics became more cutthroat. Established criminal organizations like WIZARD SPIDER expanded operations, and affiliates of the ransomware-as-a-service (RaaS) malware developers adopted BGH attacks. In short, the greedy got greedier and the rich got richer."

- CROWDSTRIKE – 2020 Global Threat Report

Shifting from Remote to Local Attacks

The attacks themselves have also gotten more deliberate and methodical. Once in these corporate systems, hackers will navigate around using existing tools and time their attacks for specific times when defenses are down, or they know the response will be delayed. Another trend we're seeing is that attacks are moving from remote to local. One reason for this is because those responsible for protecting their corporate networks are doing a good job of defending against cloud-centric attacks. We have sophisticated security countermeasures available, and with those systems in place it's much more difficult to attack the IT infrastructure from the internet. These days the most successful way to breach a system is by hacking human behavior; tricking someone into giving up their username and password through phishing attacks. But even that's getting harder to do as companies are doing a great job educating their employees on how to recognize these scams.

In the 2018 Global Threat Report, CrowdStrike began reporting on "breakout time." This key cybersecurity metric measures the speed from an adversary's initial intrusion into an environment to when they achieve lateral movement across the victim's network toward their ultimate objective.

This forces the attackers to look at other vulnerabilities, including the edge nodes as an access point to larger systems. End nodes historically have not been an especially lucrative target because the reward was just the information contained on that particular device. The biggest exception to this, however, is ransomware. Ransomware of personal computers has become a pretty good income stream for hackers because they can get $200-$300 per hack from as many people as they can infect. But even that is wearing thin as organizations like the FBI and nomoreransom.org have developed tools to unlock encrypted data without paying the ransom.

> "This year, the average breakout time for all observed intrusions rose from an average of 4 hours 37 minutes in 2018 to 9 hours in 2019. This increase reflects the dramatic rise in observed eCrime attacks, which tend to have significantly longer breakout times compared with nation-state adversaries."
>
> CROWDSTRIKE – 2020 Global Threat Report.

Rise of the Pivot Attack

With the good guys winning, what's a criminal to do? Enter the pivot attack. A pivot attack is an attack on an end node for the purpose of using it to attack the higher-level infrastructure. This "bottom-up" approach takes advantage of the assumption that because attacks usually come in from the cloud, the devices at the bottom of the architecture are trustworthy. And since end nodes were never previously considered targets, the security built into them, if there's any at all, is weak. Compounding the innovation of the pivot attack is how the rise of IoT and Industrial IoT is dramatically increasing the number of smart devices at the bottom. These IoT and Industrial IoT devices tend to be very easily accessed in the supply chain. You can get them online or at any electronics store. With the devices easily accessible, opportunistic hackers can spend as much time with them as they need. All these factors make local attacks more attractive. The hacking kits these criminal enterprises can create with sophisticated penetration labs will be ever better conceived, developed, and tested. And now, with the exponential increase of IoT devices, they are more easily deployed on a massive scale.

A Moving Target – Operational Technology

Ransomware is not only becoming much more targeted, but it's focus is moving from IT centric game plan to an operational technology (OT) focus. OT is anything to do with the primary purpose of running a business. At Silicon Labs, we focus heavily on building automation, factory automation, or building control and you can imagine for these types of operations a disruption in business continuity could result in significant financial damage. The attackers know that these operations have a lot to lose are willing to pay. Cyber criminals will seek out the most lucrative targets and it should come as no surprise that extortion in the form of ransomware has emerged as a popular grift.

As we mentioned, ransomware started small but has steadily targeted bigger fish including private companies as well as local and state governments. According to IBM's 2020 X-Force Threat Intelligence Index report, in the fourth quarter of 2019 there was a 67 percent increase in ransomware engagements compared to the same quarter of 2018. Government agencies have been hit especially hard. In 2019, more than 70 government entities were hit with ransomware in first half alone. And the ransoms demanded are getting bigger. For instance, according to that same IBM report, there was a $14 million-dollar ransom demanded from a single hospital in 2019 by a cybercrime group using the Ryuk ransomware.

Profitability is driving the shift to OT being the focus target, but that's not the only factor. Ease of deployment is also at work. Operational equipment which includes manufacturing systems, robots, fire alarm systems, access control systems have been historically proprietary systems with proprietary protocols. This is the same for industrial control systems. Cost has been the primary driver in the past, and security is typically not built into these devices. The IoT and IIoT trend is also introducing devices into the system that weren't there before. And for IIoT specifically, the approach has always been to put inexpensive sensors on the floor and send that data to the cloud. Given the nature and utility of these markets, these devices may be coming from very small companies or start-ups that don't have the resources to focus on best-in-class security features.

Each sensor creates a new attack vector and potentially a way to bring a critical system to its knees. That downtime can be used for extortion of large ransoms for the return of service. Cheap sensors from all corners of the world are easier to intercept in the supply chain and compromise with local attacks in a well-furnished hacking lab. Think about the fire alarm system of a high-rise office tower in New York's financial district being compromised, for example. The alarm system could be tripped, and the entire 300 stories of people evacuated into the street. Now, what if that same building's access control system was also compromised? You now could lock everyone out of that building. Imagine the ransom that could be extracted in that situation. With the amount of money lost every minute, a billion-dollar ransom would not be out of the question.

Another advantage of targeting OT is that a single device could potentially cause much more damage than a single IT device. For instance, a strategically placed electrical distribution breaker can make an entire city go dark. These criminals' have also demonstrated an ability to adapt and learn, and as governments recognize that this threat will only amplify, regulation is coming about to force security on IoT deployments.

Regulation Is Here

The California Consumer Privacy Act came into effect as of January 1, 2020. This act requires "reasonable" security features that are appropriate to the nature and function of the device and to the information it collects, contains, or transmits. Features must be designed to protect the device and any information contained from unauthorized access, destruction, use, modification, or disclosure. Pre-programmed passwords are unique in each device manufactured. In short, the law requires that these devices cannot be hacked. Many additional states have already introduced similar bills making 30% of the US population alone subject to such regulation.

For the US, the National Institute of Standards and Technology will serve as the governing body that decides what is considered "reasonable," and we can expect more legislation and court cases to continue guiding the laws going forward. The NIST has released NISTIR 8259A that establishes a cybersecurity feature baseline for scalable IoT devices.

The US is not alone in its effort to secure IoT devices. The UK and other European countries are currently working within European Telecommunications Standards Institute (ETSI)to enact similar prescriptive security features for Consumer IoT. ETSI is recognized by the European Commission and is chartered with developing standards for the Information and Communication Technology (ICT) within Europe. Many of the same themes of NISTIR 8259A are present, requiring the need for security features such as the updatability of software/firmware and ensuring the integrity of the software which will require a secure boot and secure update of firmware of an embedded device.

Security Should Evolve at the Same Pace as Threats and Regulations

To help customers address the challenges of the evolving security landscape and keep up with regulations, Silicon Labs has introduced Secure Vault, an award-winning platform for securing and future-proofing IoT devices that recently became the first IoT security solution to achieve PSA Certified Level 3 status. One of the key aspects of Secure Vault delivers new security features including Secure Device Identity, Secure Key Management and Storage, and Advanced Tamper Detection. Learn more about Secure Vault at https://www.silabs.com/support/training/secure-vault.

As part of this process, Secure Vault takes advantage of a unique digital fingerprint generated by a physically unclonable function. This can then be used to create an AES symmetric key that physically disappears when the system powers down and so the AES symmetric key doesn't even exist when the chip is off. This is an extremely effective solution to the key management challenge, and the function can scale to support a vast number of keys as required by the developers application. Secure Vault also includes a tamper detection system that makes it so the key cannot be reconstructed once the device is shut down after a tamper event.

Secure Vault is the most advanced suite of hardware and software security protection available today and delivers:

- **Secure Device Identity Certificate**, conceptually, similar to a birth certificate, for each individual silicon die, enabling post-deployment security, authenticity and attestation-based health checks, guaranteeing the authenticity of the chip for its lifetime.
- **Advanced Tamper Detection** that enables developers to set-up appropriate response actions when the device experiences of unexpected behaviors, such as extreme voltage, frequency, and temperature variations, which could indicate a vulnerability
- **Secure Key Management and Storage**, a central component to protect against direct access to an IoT device and its data by encrypting and isolating the keys from the application code and using a master key encryption key (KEK) generated from physically unclonable function (PUF) hardware

Concern	Security Requirement	Technology
Device Identification	The IoT device can be uniquely identified logically and physically.	Secure Attestation
Device Configuration	The IoT device's software and firmware configuration can be changed, and such changes can only be performed by authorized entities.	Secure Upgrade
Software and Firmware Update	The IoT device's software and firmware can be updated by authorized entities using only a secure and configurable mechanism.	
Data Protection	The IoT device can protect the data it stores and transmits from unauthorized access and modification.	Secure Key Management
Logical Access to Interfaces	The IoT device can limit logical access to its local and network interfaces to authorized entities only.	Secure Debug
Software and Firmware Update	The IoT device's software and firmware can be updated by authorized entities using only a secure and configurable mechanism.	Secure Upgrade
Cybersecurity Event Logging	The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.	Anti-Tamper
Software Integrity	Attempts to breach security are logged and developers may select appropriate system counter-measures technologies to protect security.	Secure Boot

For more information on Secure Vault, or to learn about how Silicon Labs can help meet the security demands of your industrial or smart building application, visit www.silabs.com/security

Award-winning Secure Vault

Secure Vault is the world's first IoT security solution to achieve PSA Certified Level 3 Status — the highest level of IoT hardware and software security protection.

PSA Certified — a respected security body for IoT hardware, software and devices co-founded by Arm — awarded PSA Certified Level 3 status to EFR32MG21, a wireless SoC with Secure Vault for greatly reducing the risk of IoT ecosystem security breaches and the compromise of intellectual property or revenue loss from counterfeiting.

Security Requirements Need Consistency and Certification

Once requirements are put into place, there still is the question of how they should be interpreted, measured, and certified. At the end of the day the consumer must be able to pick a product off the shelf and in a quick glance, determine if the device will have the right level of security for that type of device.

At the beginning of the 20th century, when electricity was starting to be delivered to every home, there was a huge increase in the number of electrical home appliances that flooded the market. And with that exponential increase in devices, there was a rash of house fires and deaths caused by appliances that did not have the appropriate fire safety features. To address this problem, there were government safety regulations and entities like UL in the USA and CE in Europe that grew to meet the need for testing and certifying products. These methods have been so effective in reducing the risk to the consumer that I doubt many people in Europe or the USA ever worry or even think about whether an appliance they purchase will burn their house down.

This level of trust with the consumer is where we need to get with Security. But, how do we get to the point where a consumer picks a product off the shelf and knows that he has not just let a hacker into his financial account info stored on his home network. Or a building owner orders a building lighting control system and does not worry about whether they just purchased a back door for hackers to steal their IP, ruin their brand, or poach their market share.

While the ETSI and NIST requirements are a good guideline, the world markets and governments are still struggling how do you consistently apply those requirements to products that vary greatly in the amount of processing power, memory, and raw computing power. For instance, a cable set top box or game console typically has much more shear processing power and memory than a smart thermostat or smart speaker. And a smart speaker has way more processing power and memory than a smart door lock. A smart door lock usually has much more processing power than battery powered leak detector, motion sensor, or contact switch. The good news is that each of these types of devices usually have security needs that are scaled with the level of processing power and memory. For instance, the security requirements for a high-end game console greatly eclipses the security requirements for a motion sensor on a sub-net.

This is where the concept of Protection Profiles become incredibly important. Protection Profiles are part of the Common Criteria ISO standard that has been around for quite some time, but, have largely only been defined for smart cards (secure elements) used in banking cards and passports. There is also a Protection Profile adopted by the GlobalPlatforms.org for defining Trusted Execution Environment or TEEs which have been adopted by smart phones, tablets, and high-end Linux Point of Sale Terminals.

For the IoT and Industrial IoT market we need to accelerate the use of Protection Profiles to define the right level of security of a given type of device. A device specific Protection Profile would weigh the resources of the device, the threat analysis, and the cost of the device to formulate the base level of security required for that device type. You can imagine that the Protection Profile for a set top box would be much more extensive than the Protection Profile for a wireless contact switch.

But, where do these Protection Profiles get defined? They are not getting defined by ETSI or NIST. They are not being defined by the Certification Labs which expect the manufacture to define the Protection Profile. What you don't want is for every company to define their own Protection Profile for their own product line. You can imagine the chaos that would ensue in the consumer world if that happened. What is needed is for the 4-5 biggest makers of a product to sit in a room together and hammer out an agreement on what the base security requirements are for that type of product. Then they would need to agree on standardized way to measure and certify that protection profile.

A place where that can happen is with trade alliances. For instance, the Diabetes Technology Society (DTS), which is a nonprofit organization committed to promoting development and use of technology in the fight against diabetes. DTS created something called the DTSec. DTSec is a cybersecurity Protection Profile for connected diabetes devices. But if we wait for each trade.org to create a Protection Profile we may be waiting for a long time.

Another .org that has recently tackled Protection Profiles is the ioXt Alliance. This is a nonprofit whose promoter members are: Amazon, Comcast, Google, Legrand, Resideo, Silicon Labs, T-Mobile, and the ZigBee Alliance. Other notable members are Somfy, Z-Wave, mobilitie, NXP, Accuity Brands, Cree Lighting, Schneider Electric, MMB Networks, and Logitech. A big part of the ioXt Alliance's mission is to provide a safe and fair place for large manufactures to come together and create protection profiles for their industries.

Once you have a Protection Profile, the next issue is how do you consistently measure and certify the product against that Protection Profile. Of all the issues to getting to that consumer confidence of not worrying about security when they buy an IoT device, consistently measuring and certifying products is the next big issue to overcome behind Protection Profiles. There are standards like ISO 17025 which certify testing labs. But that does not guarantee that lab has any experience testing a particular kind of device and the results could be good or bad, but not likely to be consistent from lab to lab.

In Europe there is Common Criteria, defined by ISO 15408, which gives a testing framework for testing labs to apply for measuring Protection Profiles. But those requirements, like the Protection Profile for Smart Cards, were largely used over the last 10+ years to measure the security of stand-alone secure elements. It is recognized by even the makers of secure elements as too stringent for the dynamic a varied world of IoT. Several European entities have developed a light-weight version of Common Criteria called Security Evaluation Standard for IoT Platforms (SESIP) which has been adopted by GlobalPlatform.org for certifying IoT devices. This standard has promise as it is at least flexible and tailored to the IoT market. But some still argue it is too heavy for a large class of IoT devices and still will not be able to scale to the billions of IoT devices predicted in the near future.

ioXt Alliance is implementing something novel for IoT certification. As it is a new organization and not locked into the ideas of the past, it is not only embracing the idea of every type of device needs its own Protection Profile to define the right level of certification, but also certification can be effectively crowd sourced. The ioXt Alliance believes that self-certification is a perfectly acceptable option to certify a product against a defined profile, but there needs to be a market check and balance for that approach. They do of course offer and encourage ISO 17025 certification labs to certify against ioXt Alliance Protection Profiles, but it is not a hard requirement. Whether or not the product is self-certified, or certified by qualified lab, there is bug-bounty program that each company must sign up to abide by. This bug-bounty program is controlled, and claims are vetted before a company must pay the bounty.

The great thing about the bug-bounty is that it keeps everyone honest and the certification system self regulates. And because it is a controlled process, it is a much better system for vendors than the free-for-all of the way things happen today where a university can do a tiny bit of security testing and make broad claims about and exploit that have no basis in reality or fact which can damage a company's reputation and market share with very little repercussions.

The other major benefit of the self-certification is that it is very scalable for large ecosystems that rely on many hundreds of vendors to abide by the same security principles on the same network. A company that provides an IoT Cloud Service is a good example of this kind of ecosystem. These companies typically do not manufacture the devices that connect to their cloud, and likely, not even the gateways that aggregate those devices. How does an IoT Cloud Service provider police the security of the devices that connect to its network. One way would be to develop the appropriate security profiles within the ioXt Alliance and then require all the companies that attach devices to their service to show that they have at least self-certified against the Protection Profile. ioXt bug-bounties will work out the bad actors over time.

Summary

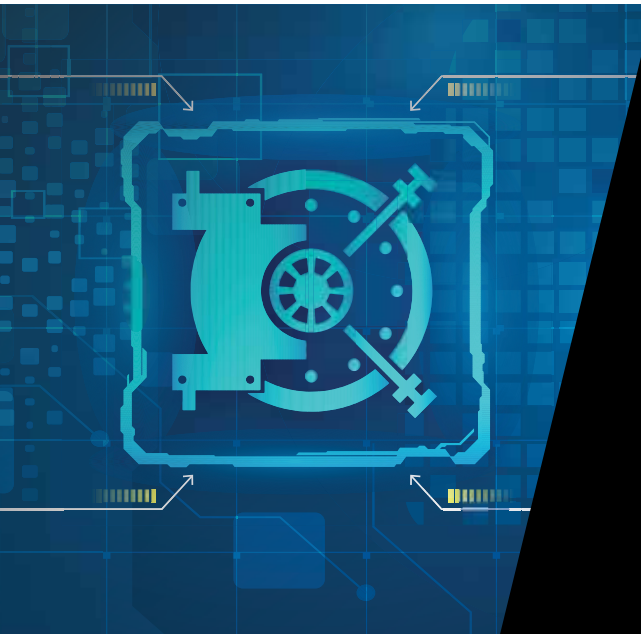
IoT products are working their way into every aspect of our lives whether consumers and businesses proactively embrace them immediately or the pace of life brings them in naturally over time. In either case they offer those with malicious intent, a vector on which to prey and security should not be considered an optional feature. Implementing security protects the consumer and the manufacturer, the data, the privacy, and the brand. Regulation is here and governments around the world are taking it very seriously.

Implementing security however isn't the complex and daunting experience developers may expect it to be, because semiconductor vendors such as Silicon Labs are actively adding the capability to their hardware and software portfolios and are simplifying implementation While there may be some differences in specific security requirements for final IoT devices as specified by NIST, ETSI, and ioXt, the underlying security requirements for the MCU/MPU are looking very much the same which is good news for developers. The big question to answer still remains "what is the right level of security for this type of device". This is why the work that the ioXt Alliance is doing around Protection Profiles is so critical to the advancement of security in IoT. The best way to certify against those Protection Profiles will be up for debate for quite some time. Will that certification come via the more traditional certification labs, or, will it be more of the crowd-sourcing approach offered by ioXt Alliance that can easily scale? Time will tell, but, likely it will be a mix of the two.

Even with some of this ambiguity in requirements, Protection Profiles, and certifications, it is clear that IoT Security is no longer a "nice to have". Developers must start embracing the need for security in their products … it's the law.

SILICON LABS

Mike Dow has worked in the semiconductor industry for Motorola, Freescale, NXP, and now Silicon Labs for the past 25 years. He has a Professional Engineering License in the state of Texas. He has extensive experience driving and participating in wireless standards organizations such as IEEE and ISA and helped form the Wireless Industrial Technology Consortium (WiTECK) where he filled the position of Chair and President from 2007-2009. He has worked for the last 11 years in the roles of Business Development, New Product Development, and Marketing where he specializes in Security, Connectivity, IoT, Industrial IoT, Point of Sale, and Smart Energy verticals.



For more information on Secure Vault, or to learn how Silicon Labs can help you meet the security demands of your smart home or industrial products, visit www.silabs.com/security.

Explore the first products with Secure Vault enabled: EFR32BG21 Series 2 Bluetooth® Wireless SoC and EFR32MG21 Series 2 Multiprotocol Wireless SoC