

MED-201: Security in Remote Patient Monitoring Devices

Course Abstract

- Digital healthcare has evolved in the past two years, and this has been accelerated by the broad adoption of technologies in telehealth and remote patient monitoring. Often built using Bluetooth technology, remote patient monitoring enables continuous monitoring of chronic diseases. The RSA conference confirmed end-user data privacy as a fundamental of healthcare but has also clearly illustrated that the medical industry is a key target for criminal cyber organizations through techniques including ransomware.
- This has triggered the absolute need to embed security with wirelessly connected end-products increasing the robustness of complete medical ecosystems against remote and physical attacks.
- This session provides a solid perspective of the most common attacks, and how the EFR32 platform can help defeat them using its latest embedded security hardware and software features.



works with

BY SILICON LABS

VIRTUAL CONFERENCE

SEPTEMBER 14-15, 2021



Security in Remote Patient Monitoring Devices



Medical Products are Becoming Small, Disposable and Connected

MINIATURIZATION



- Greater comfort for patients
- Less invasive techniques
- Faster recovery
- Overall cost reduction

PORTABILITY



- Ensures well-being of active people practicing outdoor sports
- Acceptance of challenging treatments

CONNECTIVITY



- Reporting of the dosage delivery
- Raising alarms to avoid wrong usage
- Big data management
- Sharing the information

The medical market is focusing on chronic care diseases, elderly care-management and transition care from hospital to home

Significant Innovation in Connected Diabetes Devices

Continuous Measurements

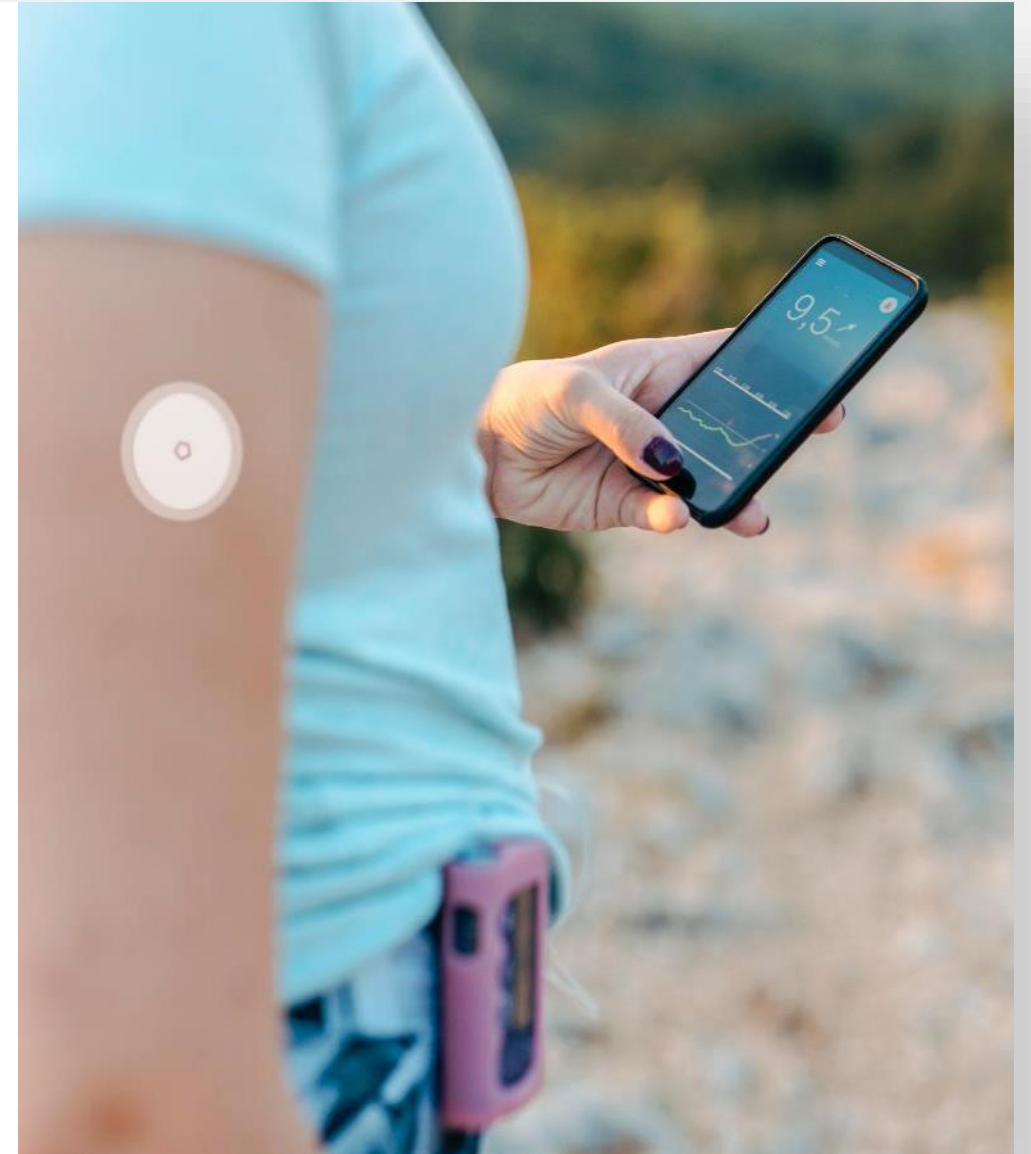
- Strong move towards Continuous Glucose Monitoring (CGM), ensures tighter control of the glucose level
- Direct interface with insulin pumps, to potentially remove costly handheld controllers

Connection to a Smartphone

- Smartphones can replace the handheld controller
- Apps are more sophisticated, offer data logging, reporting and secure identification

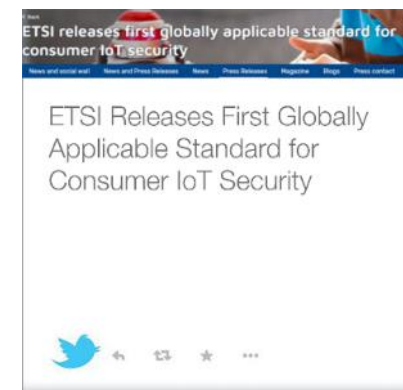
Disposability and Miniaturization

- New CGMs and Insulin Pumps need to be built as disposable electronic products
- Miniaturization is fueling the need for small board layouts and tiny packages

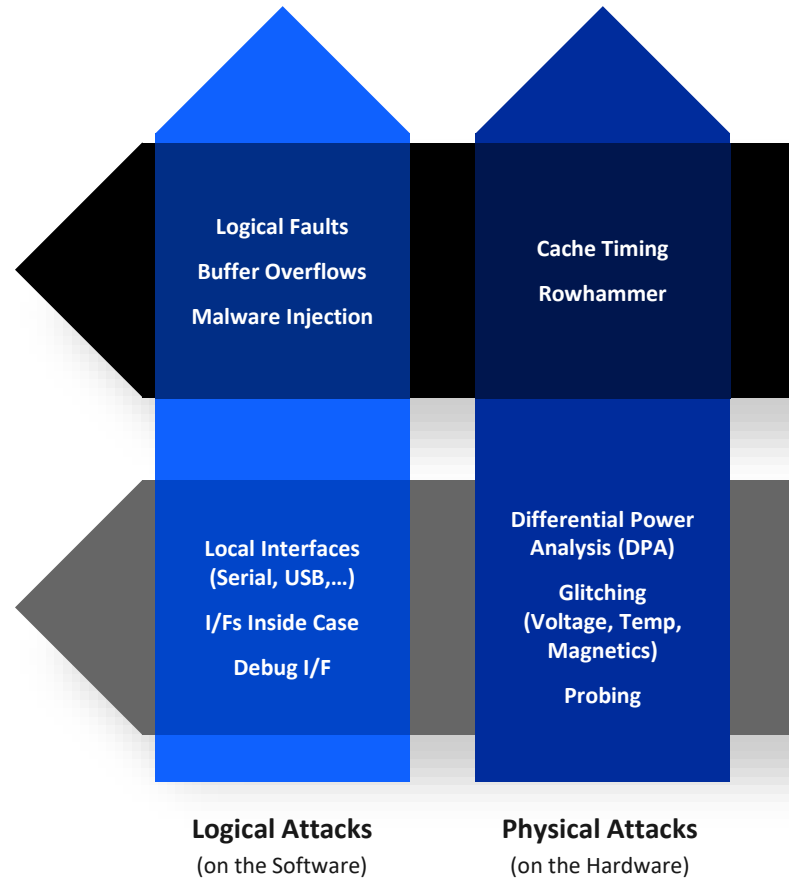
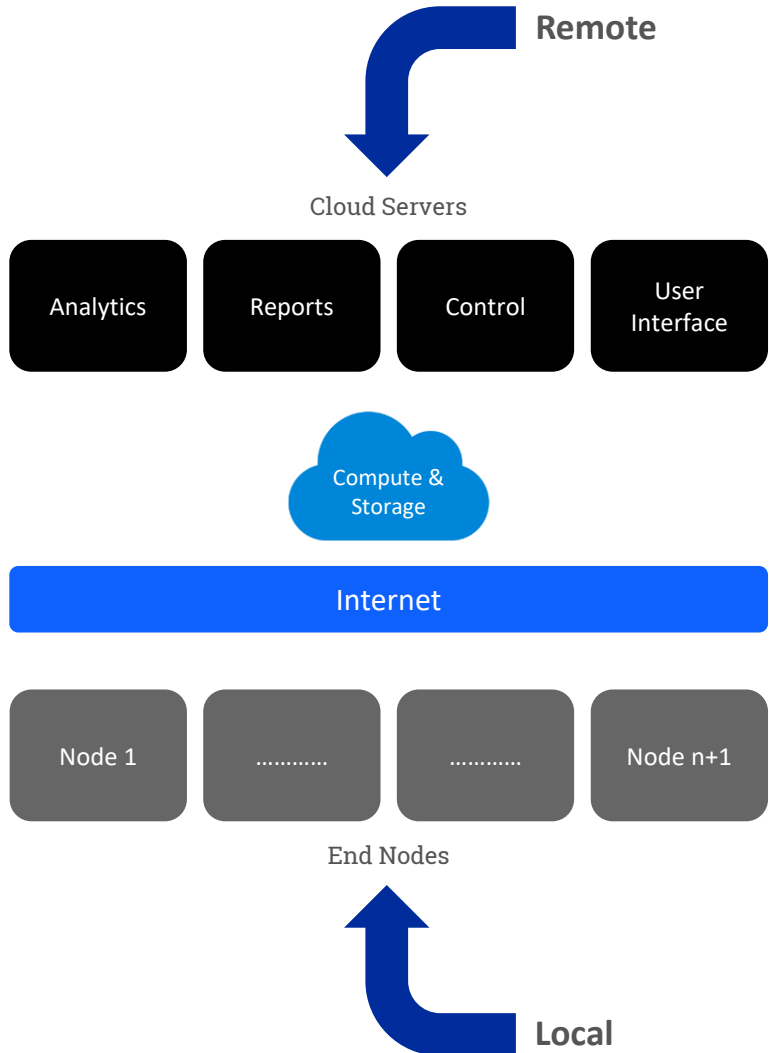


The Security challenge in Healthcare

- Healthcare is a key target for cybercriminals offering Ransomware-as-a-Service. Many examples of attacks in medical (Medtronic insulin pump breach)
- Congress has passed first bill in Dec. 2020 that mandates minimum security to all companies selling IoT products to the US government. <https://www.congress.gov/bill/116th-congress/house-bill/1668/actions>
- It can be expected that the department of Commerce will follow with similar requirements for the general IoT market, defined by NIST 8259A/B/C/D. <https://www.nist.gov/news-events/news/2020/12/nist-releases-draft-guidance-internet-things-device-cybersecurity>



End Node Attack Vectors



Remote Attacks

(through the Internet)

Historically hackers attacked only from the cloud and focused on solely on data servers.

Local Attacks

(Hands-On Access)

'Pivot Attacks' are a growing attack vector against IoT.

End nodes are attacked locally and then used to attack higher level servers for their more valuable data.

Silicon Labs Security Strategy



psacertified™
level three



- **Stay ahead of Security Regulations**
 - IoT US Govt - IoT Cybersecurity Improvement Act of 2020 (Dec 2020) – NISTIR 8259A-D
 - IoT Europe/USA – NISTIR 8259A, IEC 303 645, ISO-27402, ENISA
 - IoT Worldwide - ioXt Alliance w/ Device-type Security Profiles and certs for all the above
- **Certifications that can be inherited for our customers security certifications**
 - first MCU with Arm PSA Level 3
- **The right level of Secure Hardware – Base (Comms), Mid (+Remote), High (+Local)**
 - Secure Vault – securely updateable security sub-system with its own core
 - Secure Boot, Secure Debug
 - Secure Identity Certificates and Secure Key Management/Storage with PUF
 - Tamper Detection and Hardware Glitch Mitigation
- **Secure Software (Communication Stacks, OS, Security Subsystem)**
 - Secure OTA updates
 - Static Code Analysis, Software Glitch Mitigation, Fuzz Testing
- **Security Services**
 - Custom Programming Services – Custom Key, Code, and Certificate Injection
 - HSM Key Generation and Signing Service
 - Long Term SDK Support for Security Patches
- **Continuous Security Process Improvement**
 - Product Security Incident Response Team (PSIRT) -> Security Fixes and Advisories
 - ISO 27001 Information Security Management System Certification

Secure Vault™



psacertified™
level three





- **OTA Updateable Security Sub-system** – Independent Core w/ OTA updateable firmware to future proof your security (i.e., new curves, new algorithms, security patches)
- **Secure Boot** – 4 stages with public signature authentication at each stage with small immutable ROM stage (hardware root of trust)
- **Secure Identity** – First to market with private/public key pair generated by the die and certificate identity chain injected as standard offering of part
- **Secure Attestation/Pairing** – Secure identity can be used to do a secure attestation/pairing at any point in time even after deployment
- **Secure Key Management** – Physically Unclonable Function (PUF) based key wrapping for almost unlimited key storage and protection
- **Secure Debug** – debug lock that has glitch mitigation and can be cryptographically locked and unlocked with a revokable debug token
- **Tamper Protection** – multiple sources of tamper from temp, glitch, external input such as tamper switches programmed to trigger interrupts, resets, or bricking
- **Logical/Physical Attack Protection** - Physical Side Channel Attacks and Glitching
- **Custom Programming Services** – key injection, custom certificates, flashing encrypted images

EFR32 is first DTSec compliant IC on the market

- Developed a DTSec Micro Protection Profile within the framework of Global Platforms SESIP program
- EFR32xG22 was evaluated using this Protection Profile tailored to meeting the MCU level requirements of DTSec at a SESIP Level 3 Assurance level which is the white box testing level where insider info is given to the evaluator
- EFR32xG22 passed the evaluation and is officially recognized on the TrustCB website
- There is a detailed evaluation report that can be shared under NDA

<https://www.silabs.com/security/third-party-accreditation>

TRUSTCB		TRUST AND VERIFY
Certificate ID	SESIP-2000020-02	
<i>TrustCB B.V. declares that</i>		
Product	EFR32MG22 Wireless Gecko SoC Family, Rev C	
<i>of</i>		
Sponsor (and developer)	Silicon Labs in Austin, USA	
<i>complies to the requirements described in the standard and ST</i>		
Standard	GlobalPlatform Technology, Security Evaluation Standard for IoT Platforms (SESIP), GP_FST_070, Public Release v1.0, March 2020 Based on Common Criteria for Information Technology Security Evaluation (CC) Parts 1-3, Version 3.1 Revision 5 (ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3)	
ST Reference	EFR32MG22 Wireless Gecko SoC Family SESIP Security Target, version 0.8	
<i>Summarized:</i>		
Assurance Package	SESIP3 with Limited Physical Attacker Resistance and Software Attacker Resistance; Isolation of Platform and Software Attacker Resistance; Isolation of Platform Parts	
SESIP Profile	SESIP profile for DTSec Connected Diabetes Devices, SESIP-PP-DTSEC, version 1.0 draft, February 2021	
<i>As evaluated by:</i>		
Evaluation Facility	Brightsight B.V. located in Delft, The Netherlands	
<i>Under scheme:</i>		
 TrustCB Scheme Procedures SESIP v2.1		
Validity	Date of 1st issuance: 2021-04-12 Date of expiry: 2023-04-12	
		
Wouter Slegers, CEO		

TrustCB B.V. | www.trustcb.com | trustcb@trustcb.com
Van den Berghlaan 48 | 2132 AT Hoofddorp | The Netherlands

Thank you

EMMANUEL SAMBUIS | SEPTEMBER 2021

May 19th Outline Milestone: Example

▪ Purpose of Outline

- Establish # of slides anticipated to cover course material WITHIN allotted time
- Identify existing slide material that can be repurposed / updated
- Identify missing slide material that must be created
- Complete an initial step that simplifies getting slide content started

▪ Suggestions

- Assume 2 minutes / slide. Given 15 – 30-minute targets, outline should be < 15 slides
- 1st capture an empty slide for each KEY topic that the audience must learn. Topic in Title. “Topic”
- 2nd add empty slides to support those KEY topics. Supporting Detail in Title. “Topic – Detail”
- 3rd add bullets to each slide that captures objective in as few words as possible
- 4th circulate your outline to others to get their feedback
- 5th begin populating slides with existing content that best captures “objectives” listed in step 3.