Security
INTERNET of THINGS

Health & Automotive

Outline

1. Introduction
2. Regulatory & Industry Frameworks
3. Case Study: Apple Health App Security
    a. HealthKit
    b. Data Storage and Transfer
4. Broader Health IoT Security Practices
5. Security challenges in Automotive IoT
6. Example: Security Technologies in Automotive IoT
7. Discussion
8. Conclusion

Security Health IoT Introduction

What is Health IoT?

- Network of connected devices that collect, share, and monitor health-related data
- Includes wearables, smartphones, medical sensors, and health apps like Apple Health
- Enables remote diagnostics, patient monitoring, and personal wellness tracking

Importance of Security in Health IoT

- Health data is highly sensitive and personal—vulnerable to misuse or breaches
- Compromised devices or apps can endanger user safety (e.g. false readings or device tampering)
- Legal frameworks require strict safeguards to protect personal health data

Security Health IoT
Regulatory and Industry Frameworks

HIPAA (US) - 1996

- Ensures safeguards for Health Information of all kinds in all electronic systems
- Still applies to “modern” technology, specifically health apps that share data with healthcare providers or insurers

GDPR (EU) - 2018

- Enforced since 2018 by the European Union
- Requires explicit user consent and strict control over personal health data
- Grants users the unrestricted right to access, correct, and delete their data

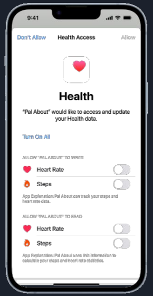
ISO/IEC 27001 - most recent revision 2022

- Global standard for Information Security Management Systems (ISMS)
- Encourages risk assessment, encryption, and access control for all devices handling health data

Security Health IoT
Case Study: Apple Health App

HealthKit

- Dedicated software framework for managing health and fitness data
- Acts as a central repository: collecting, storing, and sharing data
- HealthKit is tied to the secure enclave, physically isolating encryption keys from the rest of the system
- 3rd party apps can access health data only with explicit, user-granted permission



Security Health IoT
Case Study: Apple Health App

cloud encryption

- Data is stored end-to-end encrypted
- Device/Private keys generated on phone encrypt the health data
- Apple or the iCloud itself holds no master decryption key, cannot access them

in-transit protection

- Data is transmitted via HTTPS
- Encryption keys are dynamically created per data transfer and expire after use

at-rest encryption

- Access requires the user’s passcode, Face ID, or Touch ID
- No access => no key => no decryption possible, not even locally

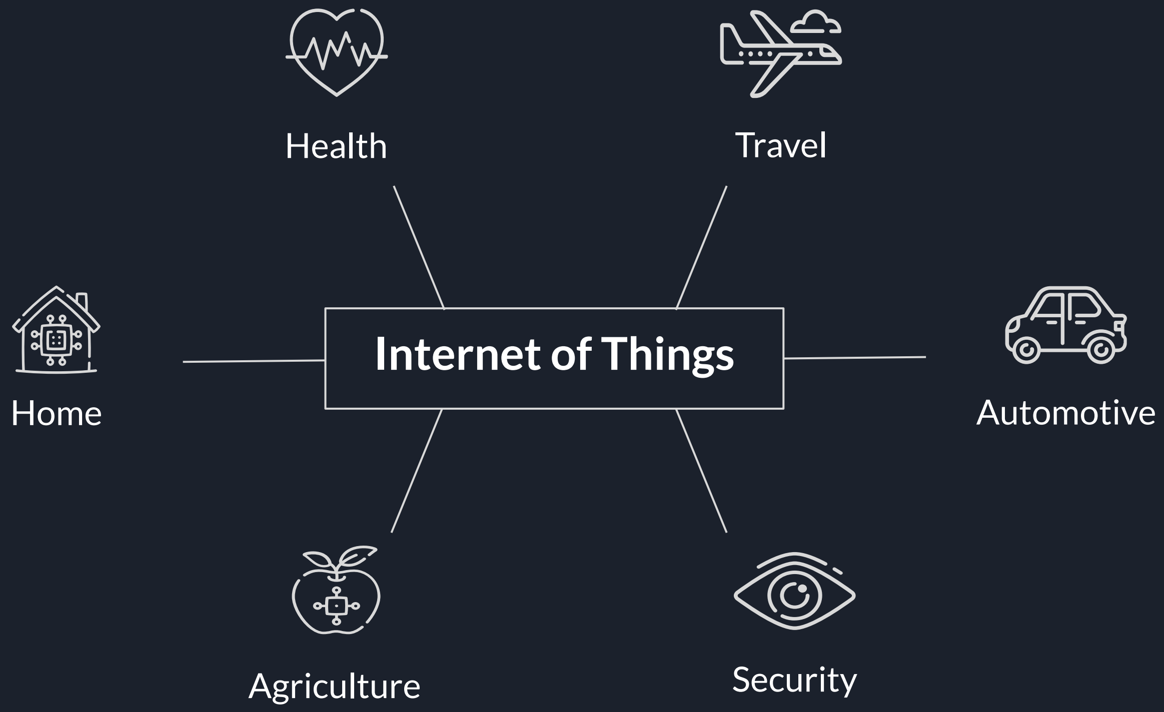
Security Health IoT
Broader Health IoT Security Practices

- **Pseudonymization**: a process in which directly identifying information is separated from medical research data
    - Usage of UUIDs: unique 128-bit label
- **Data minimization**: Only the minimum amount of data is actually collected
    - Enforced fine grained permission request
- **Audit trails**: All data access attempts are logged for future review
    - Append-only file systems and immutable logs or even blockchains
- **Regular Security Updates**: Frequent patches against newly discovered vulnerabilities prevent security gaps

Security Health IoT
Common Medical Devices and Security Issues

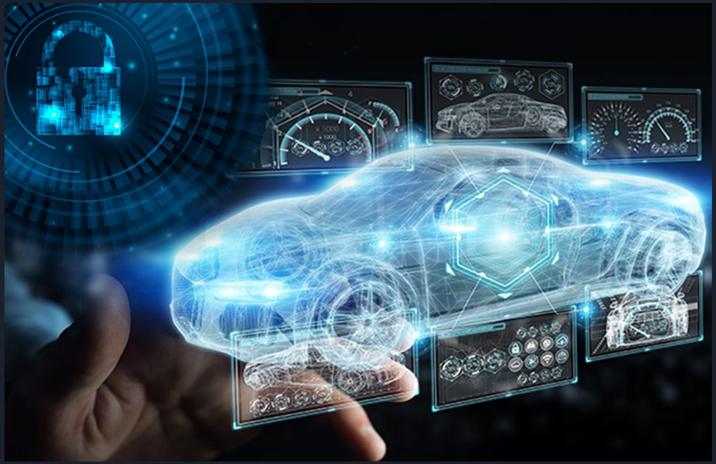
Device Type	Typical Protocol	Security Issues
Blood Pressure Cuff	Bluetooth/Wi-Fi	Data interception, weak encryption
Glucometer	Bluetooth	Unauthorized access, data leaks
Pulse Oximeter	Bluetooth Low Energy/ Wi-Fi	Outdated software, lack of updates
Wearables (Watches, Heart Rate Monitor, …)	Bluetooth Low Energy/ Near Field Communication	Eavesdropping, relay attacks
Hospital Monitors	Wi-Fi/Zigbee (Low Powered Wi-Fi Alt.)	Network attacks, device spoofing

Security in other spaces of the IoT



Security in other spaces of the IoT
Security challenges in Automotive IoT

- **Safety-Critical Operations**
  - danger of physical harm or life-threatening situations -> safety above all else
- **Complex Supply Chain**
  - multiple tiers of suppliers that contribute various components that must work together securely
  - GSMA IoT Security Assessment framework
- **Extended Lifecycle**
  - vehicles in operation for 10-15 years
  - long-term updatability and resilience against evolving threats over extended periods needed



Security in other spaces of the IoT
Example: Security Technologies in Automotive IoT

Secure Onboard Communication (SecOC)

- adds authentication and freshness checks to ECU communications
- Technologies: Message Authentication Codes and Freshness Values to prevent spoofing and replay attacks

Impact from SecOC on Automotive IoT Challenges:

- Safety-Critical Systems: Protects steering/braking ECUs from malicious commands
- Supply Chain Risks: Provides standardized security layer across OEM/Tier 1-2 components

Conclusion & Discussion

- Is it ethically and morally justifiable if hospitals, health institutions or doctors directly sacrifice a little bit of security (Authentication on ER workstations, skipping data transfer protocols, …) in order to be able to respond as fast as possible in emergency situations?

- What role should AI play in detecting or preventing intrusions in connected cars, and how can this be secured itself?

- What responsibility do car manufacturers have for securing the entire IoT supply chain—including partners and vendors?

Sources

[1] Learn how the Health app and HealthKit protect your privacy
[2] Healthcare IoT Security 101
[3] Abu Attieh, H., Müller, A., Wirth, F. *et al.* Pseudonymization tools for medical research: a systematic review. *BMC Med Inform Decis Mak* **25**, 128 (2025). https://doi.org/10.1186/s12911-025-02958-0
[4] https://www.gsma.com/solutions-and-impact/technologies/internet-of-things/wp-content/uploads/2018/03/Automotive-IoT-Security-digital-Mar-18.pdf
[5] Securing the Future of Connected Cars: Tackling Automotive IoT Cybersecurity Threats in 2024
[6] CANAttack: Assessing Vulnerabilities within Controller Area Network - PMC
[7] Specification of Secure Onboard Communication Protocol
[8] Specification of Secure Onboard Communication Protocol AUTOSAR FO R24-11
[9] https://autosec.se/wp-content/uploads/2019/03/4.-Bashar-Dawood.pdf
[10] Security Challenges and SecOC Solutions for Automotive Internal Communication - Shanghai Tongxing Intelligent Technology Co.
[11] Master's Thesis: Vehicle Control Unit Security using Open Source AUTOSAR
[12] Purificato, Erasmo & Wehnert, Sabine & De Luca, Ernesto. (2021). Dynamic Privacy-Preserving Recommendations on Academic Graph Data. Computers. 10. 107. 10.3390/computers10090107.
[13] https://www.ncbi.nlm.nih.gov/books/NBK210047/
[14] https://www.pedistat.com/blog/types-of-medical-equipment-are-necessary-for-home-care
[15] https://www.ibm.com/think/insights/cybersecurity-in-healthcare-onging-crisis
[16] https://healthtechmagazine.net/article/2023/09/what-health-systems-need-consider-about-home-acute-care-security
[17] https://www.healthrecoverysolutions.com/blog/7-common-remote-patient-monitoring-devices