Vigilant Everyday

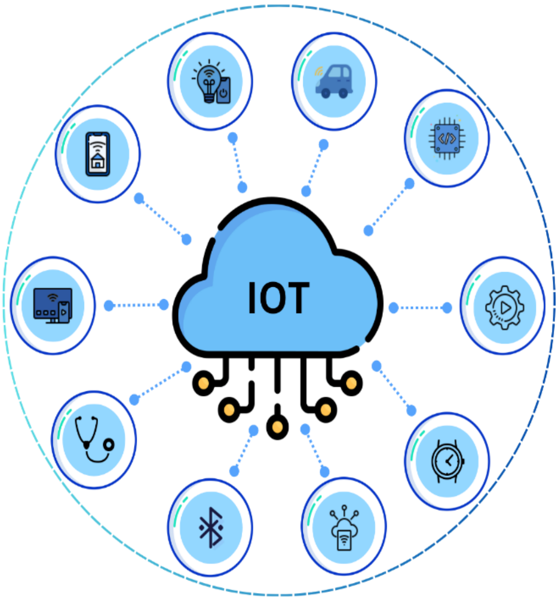
Stay ahead on the security curve, with expertise & experience, …the Jasmin way.

Every morning in Africa, a gazelle wakes up.
It knows it must run faster than the fastest lion or it will be killed.
Every morning a lion wakes up.
It knows it must outrun the slowest gazelle or it will starve to death.

It doesn't matter whether you are a lion or a gazelle:
when the sun comes up, you'd better be running.

quote by Dan Montano, popularized by Friedman in The World is Flat.

Article by Embedded Software Testing Team, Jasmin Silver



Are you chasing or escaping? In a connected world, perhaps you'll never know; except that you ran fast enough to survive; for today.
Security since time immemorial has been a primary concern, not only for animals but mankind too. While the caveman had little to lose, but his life; the modern man has much to lose during his life.
With the sophistication of civilizations - driven by technological advancements - threats have undergone a drastic change, in form, scale, impact & complexity. The good news is that Jasmin can help in matters of non-life.

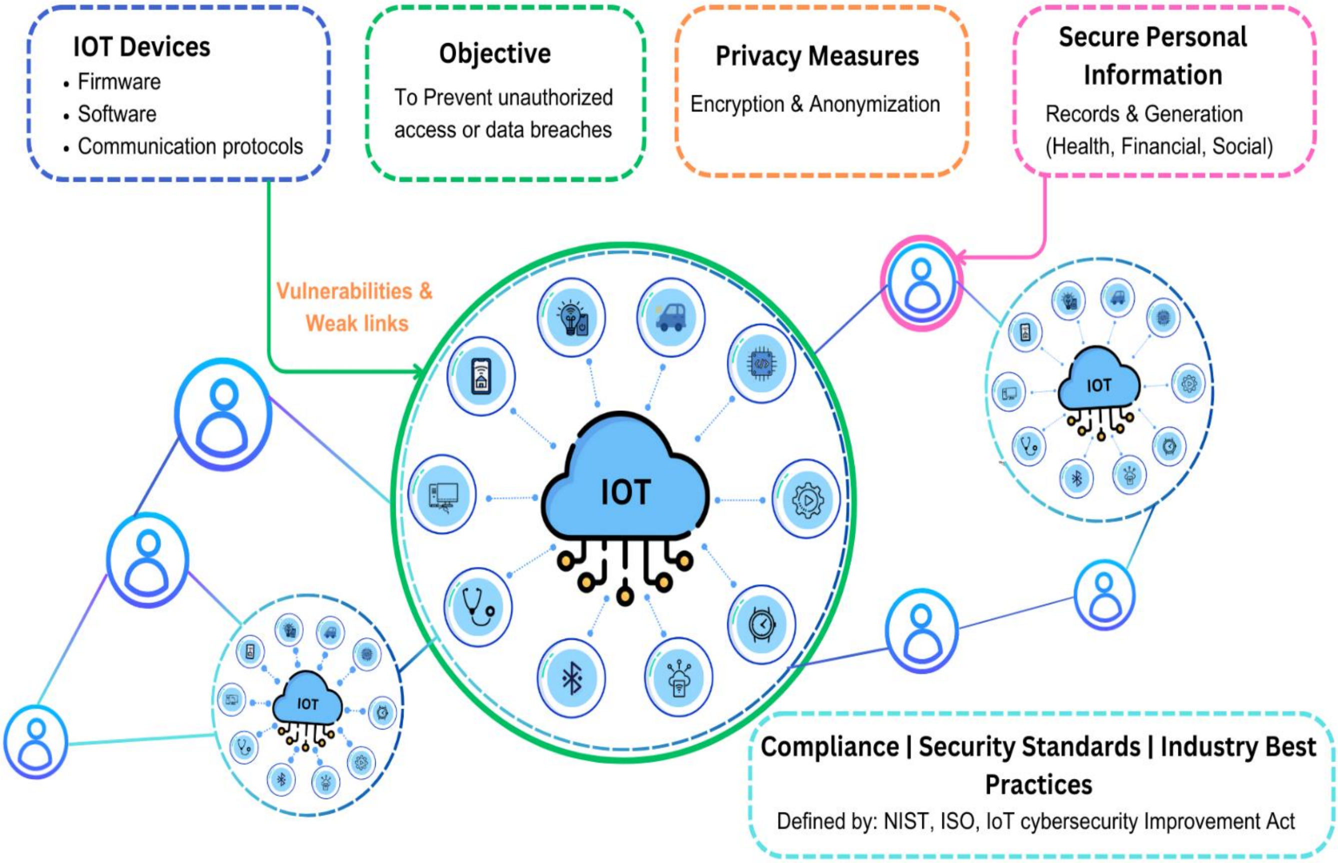
Valuable Connections, Vulnerable Connections

Any relationship, however valuable, comes at the cost of being vulnerable. Communication channels have evolved from simple catcalls to advanced satellite phones, global community exchanges, distributed ledgers, and decentralized storage. However, the hyper-exponential nature of these channels has introduced new challenges, including security.

Threats in the networked era include privacy breaches, trespassing, theft of business information, and intellectual property breaches. Services like impersonation can deliver value to humans but are packaged in vulnerable layers.

Security and reliability are crucial in a higher dimension where machines interconnected across geographies and time zones affect life-and-death matters, highlighting the need for robust security measures.

Smart Safeguarding for the Smarter… a case for IoT


IOT Devices
• Firmware
• Software
• Communication protocols
Objective
To Prevent unauthorized access or data breaches
Privacy Measures
Encryption & Anonymization
Secure Personal Information
Records & Generation (Health, Financial, Social)
Vulnerabilities & Weak links
IOT
IOT
IOT
Compliance | Security Standards | Industry Best Practices
Defined by: NIST, ISO, IoT cybersecurity Improvement Act

Digital security is crucial in the linked world we live in today. Strong security measures are required as a result of the growing use of technology, particularly in the Internet of Things (IoT) space, in order to protect sensitive data, avoid unauthorized access, and reduce hazards.

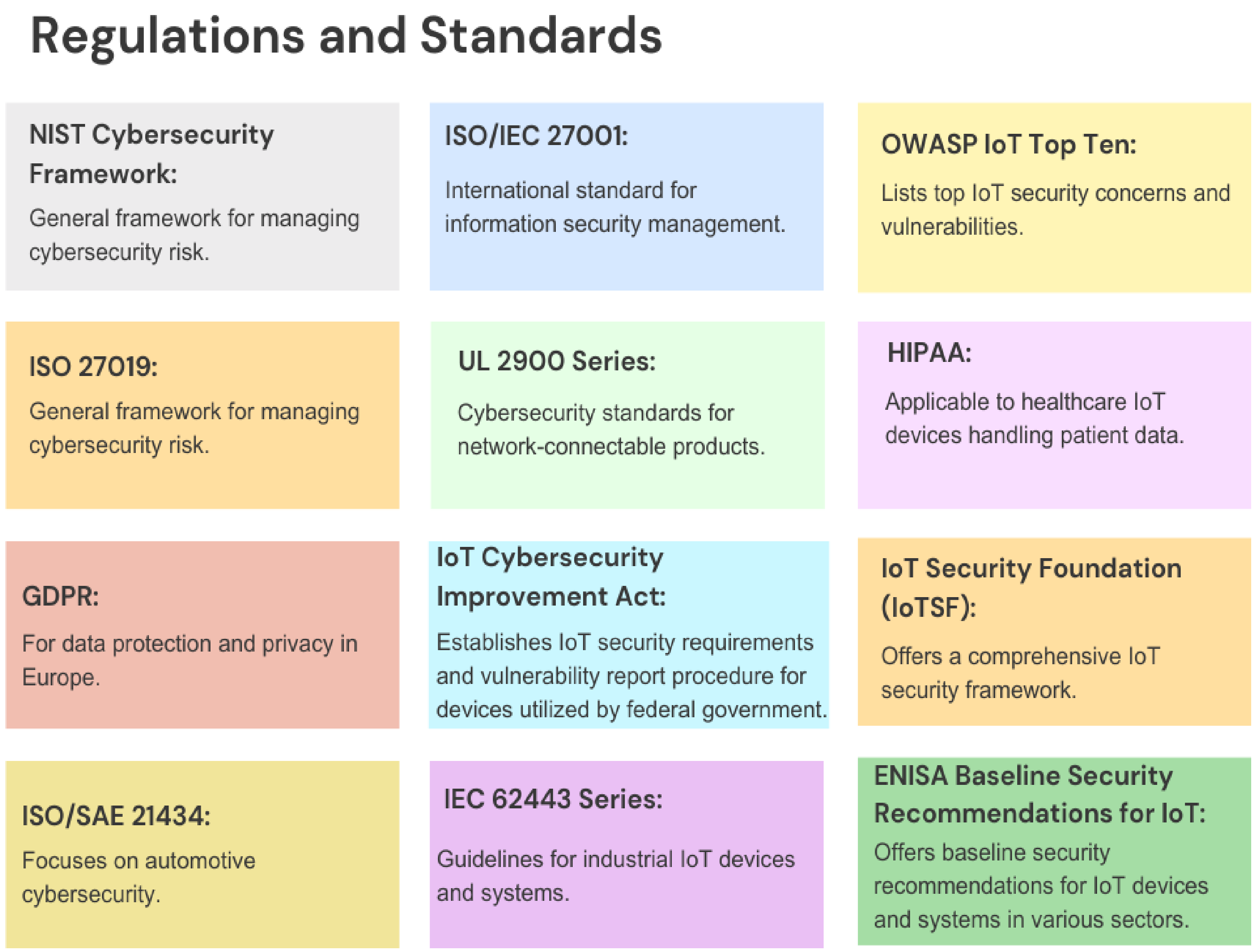
Why is real-time security so critical for IoT devices?

IoT devices are rapidly embedding themselves into our daily lives; as well as industrial scenarios. Ranging from industrial control systems to autonomous vehicles and smart homes to healthcare apps.

The IoT industry is focusing on built-in security mechanisms to manage sensitive data and maintain device integrity. Standards and processes are being established to identify vulnerabilities and weak-links, ensuring user trust and reliability. Robust testing for each layer is essential to protect against unauthorized access and maintain trustworthiness in IoT ecosystems.

Regulations and Standards:

IoT security testing for various sectors like automotive, smart home, healthcare, and industrial requires considering various standards and regulations.



Regulations and Standards

NIST Cybersecurity Framework:

General framework for managing cybersecurity risk.

ISO/IEC 27001:

International standard for information security management.

OWASP IoT Top Ten:

Lists top IoT security concerns and vulnerabilities.

ISO 27019:

General framework for managing cybersecurity risk.

UL 2900 Series:

Cybersecurity standards for network-connectable products.

HIPAA:

Applicable to healthcare IoT devices handling patient data.

GDPR:

For data protection and privacy in Europe.

IoT Cybersecurity Improvement Act:

Establishes IoT security requirements and vulnerability report procedure for devices utilized by federal government.

IoT Security Foundation (IoTSF):

Offers a comprehensive IoT security framework.

ISO/SAE 21434:

Focuses on automotive cybersecurity.

IEC 62443 Series:

Guidelines for industrial IoT devices and systems.

ENISA Baseline Security Recommendations for IoT:

Offers baseline security recommendations for IoT devices and systems in various sectors.

How it Helps Customer

- Customers gain confidence in the security of their IoT deployments through comprehensive testing.
- Identifying security issues during testing is more cost-effective than dealing with the consequences of a security breach. Customers can avoid potential financial losses, regulatory fines, and damage to their reputations.

- By identifying vulnerabilities and weaknesses in IoT devices and systems, customers can proactively address security risks before they can be exploited by malicious actors.

Use Case: Security Testing of Smartwatch Data Synchronization

Objective: The objective of this security testing is to assess the security of the smartwatch's data synchronization feature and identify potential vulnerabilities that could compromise the confidentiality and integrity of synced data.

Step 1: Test Environment and Equipment Selection

- Set up a testing environment that simulates real-world data synchronization conditions.
- Choose appropriate equipment, including a smartwatch, a smartphone for data synchronization, and network monitoring tools.

Step 2: Develop Test Scenario

Develop a testing plan that includes key scenarios:

- Capture and analyze data packets transmitted between the smartwatch and smartphone during synchronization.
- Evaluate the encryption and security of data in transit.
- Check authentication mechanisms between the smartwatch and the smartphone app.

Step 3: Test Execution

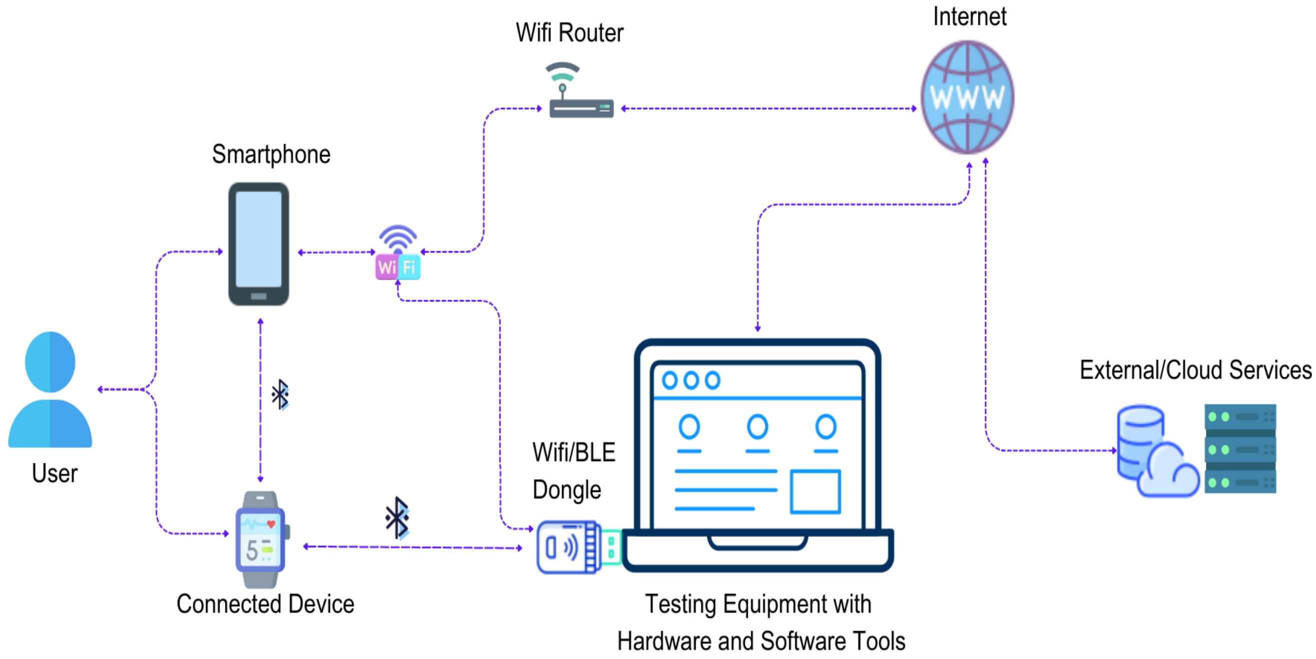
- Execute the test plan, capture relevant data, and assess the security of the data synchronization feature.

Step 4: Compliance Check

- Ensure that the IoT device complies with relevant industry standards and regulatory requirements (e.g., ISO 27001, NIST Cybersecurity Framework)

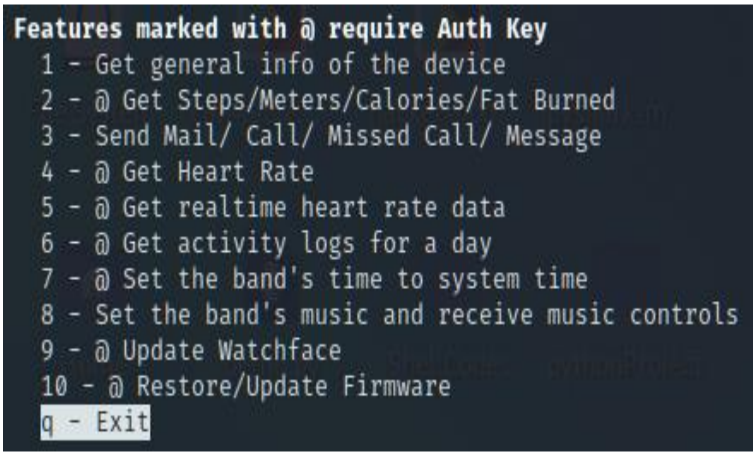
Step 5: Documentation and Recommendations

- Document all test scenarios, including the configurations, and results.
- Analyse the findings, identify vulnerabilities or weaknesses, and provide recommendations for improving security measures to protect user data during synchronization.

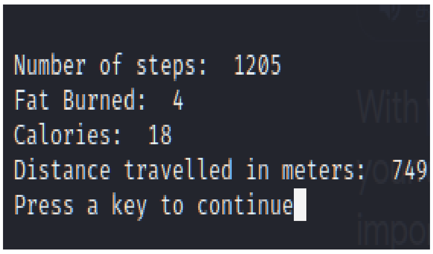


Use Case Result:

We have captured the data from the smartwatch by using the testing equipment based on the use case mentioned above. We have collected the smartwatch information using auth-key as shown in below images.



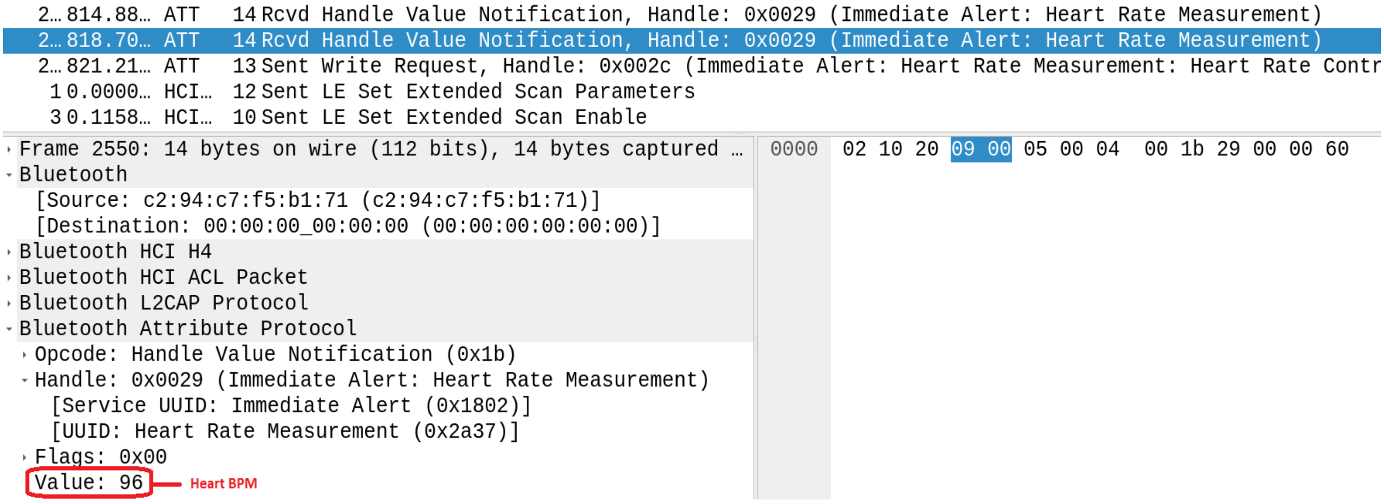
```
Features marked with @ require Auth Key
  1 - Get general info of the device
  2 - @ Get Steps/Meters/Calories/Fat Burned
  3 - Send Mail/ Call/ Missed Call/ Message
  4 - @ Get Heart Rate
  5 - @ Get realtime heart rate data
  6 - @ Get activity logs for a day
  7 - @ Set the band's time to system time
  8 - Set the band's music and receive music controls
  9 - @ Update Watchface
  10 - @ Restore/Update Firmware
  q - Exit
```



```
Number of steps:  1205
Fat Burned:  4
Calories:  18
Distance travelled in meters:  749
Press a key to continue
```

Also, we analysed the data packets using network analysis tool to check the data encryption, but the smartwatch using ATT protocol that does not use data encryption process.

As per GDPR, NIST compliance, data should be in encryption format during transmission.



```
 2… 814.88… ATT   14 Rcvd Handle Value Notification, Handle: 0x0029 (Immediate Alert: Heart Rate Measurement)
 2… 818.70… ATT   14 Rcvd Handle Value Notification, Handle: 0x0029 (Immediate Alert: Heart Rate Measurement)
 2… 821.21… ATT   13 Sent Write Request, Handle: 0x002c (Immediate Alert: Heart Rate Measurement: Heart Rate Contr
  1 0.0000… HCI…  12 Sent LE Set Extended Scan Parameters
  3 0.1158… HCI…  10 Sent LE Set Extended Scan Enable
```

```
› Frame 2550: 14 bytes on wire (112 bits), 14 bytes captured …     0000   02 10 20 09 00 05 00 04  00 1b 29 00 00 60
⌄ Bluetooth
    [Source: c2:94:c7:f5:b1:71 (c2:94:c7:f5:b1:71)]
    [Destination: 00:00:00_00:00:00 (00:00:00:00:00:00)]
› Bluetooth HCI H4
› Bluetooth HCI ACL Packet
› Bluetooth L2CAP Protocol
⌄ Bluetooth Attribute Protocol
  › Opcode: Handle Value Notification (0x1b)
  ⌄ Handle: 0x0029 (Immediate Alert: Heart Rate Measurement)
      [Service UUID: Immediate Alert (0x1802)]
      [UUID: Heart Rate Measurement (0x2a37)]
  › Flags: 0x00
    Value: 96
```

ABOUT JASMIN EMBEDDED SOFTWARE TESTING TEAM

Our services are your shield, identifying vulnerabilities before they are exploited, ensuring the sanctity of your data, and defending against the unpredictable.

- **Tailored Solutions:** We understand that security is not a one-size-fits-all approach. Our solutions are customized to suit your organization's unique needs.
- **Timely Results:** Our efficient testing processes ensure that you receive timely results, allowing you to address vulnerabilities promptly.
- **Service Quality**: We ensure service excellence through thorough testing, risk mitigation, and collaborative client engagement, ensuring high standards and superior service quality.

DISCLAIMER

Protect your digital assets and maintain the trust of your stakeholders. Contact Jasmin today for a consultation and take a proactive step towards securing your digital future.

The upcoming article will delve into the "Shield Jasmin 360" testing framework, offering actionable insights and a glimpse into the next level of security.

Keep an eye out for it – it's heading your way soon! Stay tuned.

Contact Details

Jasmin Infotech Private Limited (HQ)
Plot 119 Velachery Tambaram Road
Pallikaranai, Chennai 600100
India

MS. JEYASUDHA / MR. NARENDRAN OVI

M: +91 89251 09996

narendran.ovi@jasmin-infotech.com