Concealed Threats… Reining in the Trojan's Horse

Staying vigilant on IoT platforms isn't an option, but a necessity.

Deception is a time-tested tactic. In the mythical tale of Trojan's horse, the Greek army - after a fruitless 10-year siege of the city of Troy - constructed a huge wooden horse, to conceal a select force of men. They left it at the city gates, while pretending to sail away. The defending army, assuming it to be a "gift", pulled it in within city limits to display the victory trophy.

The rest as we know is history.

Men deceptively planted inside, opened the gates in the dark of the night. The Greeks returned to vanquish the enemy.

Thus through deception came to end the decade old war.

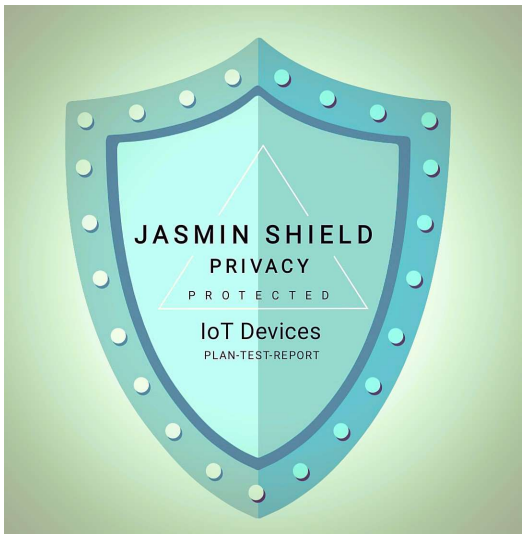
The Trojan's Horse, although mythical, is an apt lesson on the consequences of misjudgment & letting one's guards down. However strong the defence, a momentary lapse can be catastrophic.

In the networked world today - of everything & everyone, always connected - at our citadel gates a clutch of Trojan horses await their chance of breaking in.

Internet-of-Things (IoT) in particular makes the world vulnerable. Owing to limited resources at the edge (thin clients) and the sheer magnitude of deployment, these last mile devices are an open field for the Internet of Trojan horses (IoT-horses)

Reining in the Internet of Trojan's Horses

Jasmin Infotech offers cutting-edge customizable security testing services for IoT products & systems.

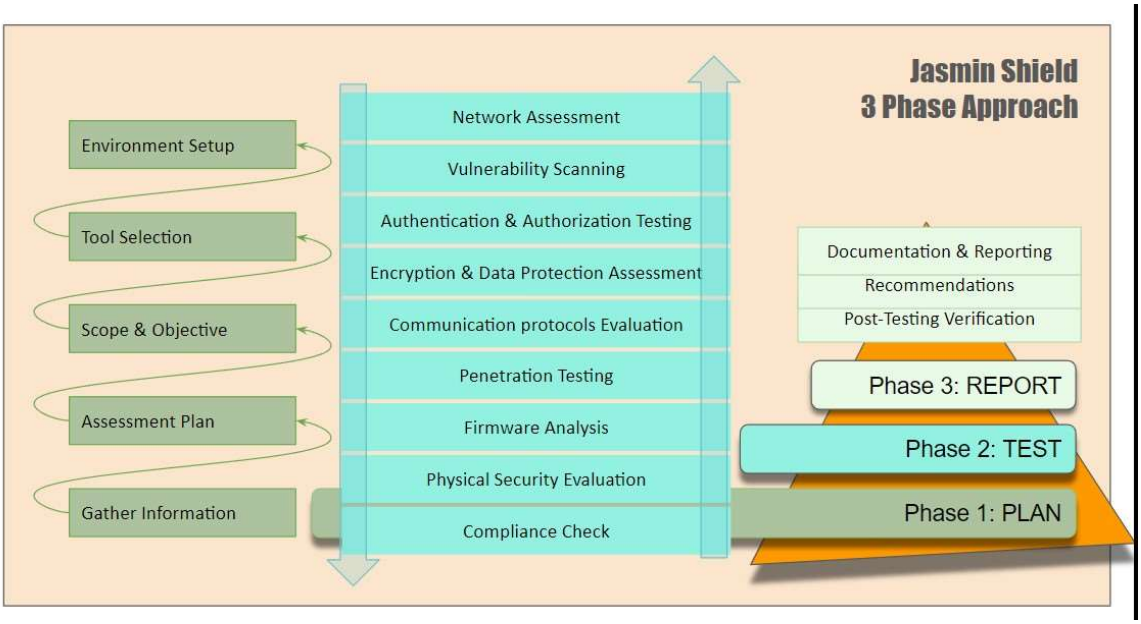


Protection of digital infrastructure from cyber threats require sophisticated tools, deep understanding of software, system & network architectures.
Processes that provide 24 x 7 x 365 vigilance for early detection, quick analysis & swift response stand out as the most robust & reliable.
Platforms tailored to align seamlessly with each customer's unique security needs.
Predictive Models to predict deviations or anomalies that might indicate a security breach based on historical data and known attack patterns.

Jasmin Shield

Jasmin Shield effectively uses manual and automated *"Predictive Modeling"* techniques to identify anomalous behaviour in IoT devices and networks. It can consider factors like device behaviour, network traffic, and vulnerability databases to dynamically prioritize security efforts.

We address the IoT device vulnerabilities and enhance overall security by considering the security measures with below three phases that cover efficient IoT security testing techniques.

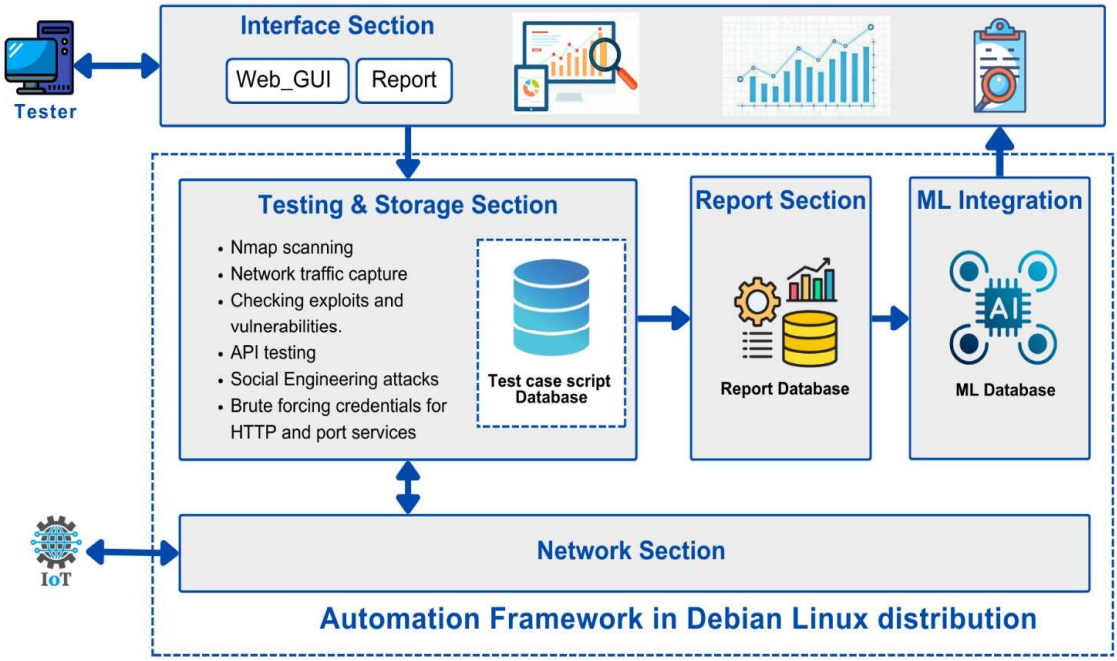


Test Automation Framework:

"Testing Phase" will utilize the Jasmin Shield test automation tool, which includes pre-loaded utilities from the Debian Linux distribution. This tool provides a comprehensive security analysis solution, including vulnerability scanning, penetration testing, threat intelligence, and compliance checks.

Machine Learning (ML) can enhance IoT security testing by identifying and preventing abnormalities and intrusions, detecting malware and malicious software on devices, and analyzing report and device behaviour to detect and respond to malware infections.

It enhances efficiency and accuracy, reduces manual effort, and offers real-time reporting for security analysis results. Reports can be exported in PDF, CSV, and HTML formats, and the database includes authentication, authorization, encryption features, and auditing for data protection regulations compliance.



- **Interface section:** This module acts as an I/O interface. It consists of two units: a Graphical User Interface (GUI) unit and a Report unit.

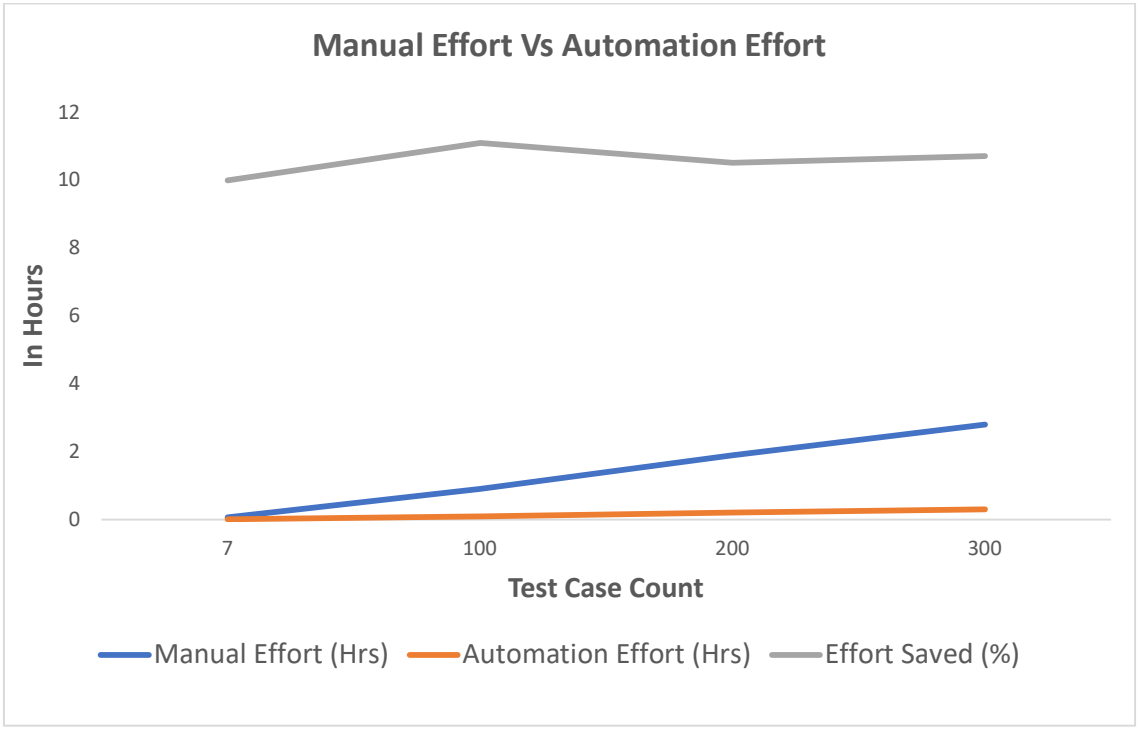
- **Testing and Storage section:** The testing section manages the test cases, and it calls up general scripts from the storage section database to examine the general network characteristics of the IoT devices.

- **Network section:** This section controls network activities and communication with IoT devices. Using the Network section, Kali Linux audits all network traffic and examines packets in the network.

- **Report section:** Once the assessment is complete, a summarized report is saved in the report section.

- **ML Integration:** The report section's summary is input into the ML database, and appropriate algorithms are used to evaluate the model's performance and deploy it for predictions.

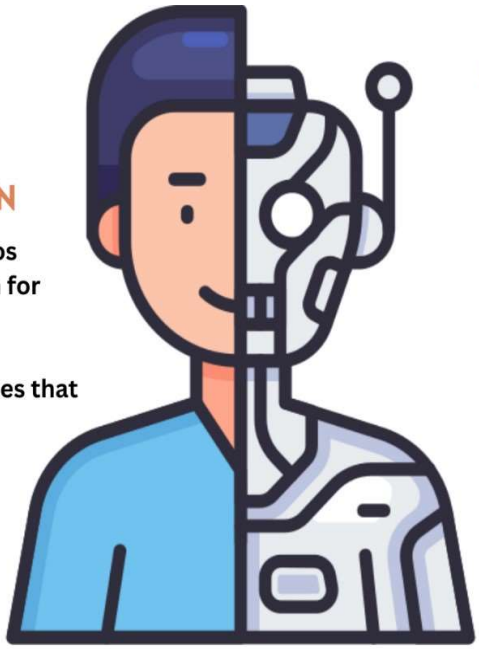
A comprehensive security testing strategy for IoT should ***incorporate both manual and automated methods***. Manual testing should focus on complex attack vectors, real-world scenarios, while automated testing handles routine checks, known vulnerabilities, and scalability, providing a robust defense against diverse threats.



JASMIN SHIELD KEY FEATURES

MANUAL EVALUATION

- Customizable Test Scenarios
- Critical Thinking & Intuition for penetration testing
- Evaluate user experience.
- Reveal critical security issues that automation cannot find.
- False Positive Reduction



AUTOMATION EVALUATION

- Dynamic Vulnerability Tracking
- Cloud Integration and robust database Support
- Advanced Reporting & Analytics
- Reduce Manual effort & Time
- Repeatability and Continuous Monitoring Solutions

ML EVALUATION

- Predictive Analysis
- Pattern Recognition and anomaly Detection
- Reduced Human Error

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.

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