Automated Validation of IoT Security Design Patterns for Smart Lamps

NAME: Automated Validation of IoT Security Design Patterns for Smart Lamps

TICT

DATE: July 4, 2025 6:34 PM

DESCRIPTION OF TECHNOLOGY
The project focuses on automating the validation of IoT security design patterns, specifically for smart lamps like Philips Hue and low-cost models. Using tools such as Node-RED, Nmap, and Wireshark, the system identifies vulnerabilities like weak encryption and insecure communication. It validates security patterns, including encrypted communication and authentication mechanisms....

HUMAN VALUES

The technology does not directly affect user identity, but it indirectly impacts it by securing devices tied to personal data. By protecting user data, it empowers individuals to feel safer using IoT devices. However, if not transparent, it may create a trust gap, leading users to question its motives or effectiveness.

TRANSPARENCY

Yes, stakeholders are informed through detailed documentation and transparent reporting. The goals of the technology are explicitly tied to improving IoT security by automating validation processes. However, additional efforts are needed to simplify technical explanations for less technical stakeholders.

IMPACT ON SOCIETY

The main problem is the lack of robust security in IoT devices like smart lamps, which are vulnerable to attacks such as unauthorized access, data breaches, and denial-of-service (DoS) attacks. These vulnerabilities can compromise user privacy, network integrity, and device functionality. This is a real problem for both manufacturers and end-users, as it directly impacts trust, usability, and safety in IoT ecosystems.

STAKEHOLDERS

- Casper Schellekens

SUSTAINABILITY

The technology minimizes energy use by optimizing automated testing scripts and using lightweight tools like Node-RED. However, indirect energy use, such as testing environments and server uptime, requires further evaluation. Future iterations may include energy-efficiency metrics as part of the testing framework.

HATEFUL AND CRIMINAL ACTORS

If misused, the technology could identify vulnerabilities and exploit them instead of securing devices. This could include unauthorized access to IoT devices, data breaches, or denial-of-service attacks. Additionally, the technology could be used to bypass security mechanisms of competing products if ethical guidelines are ignored.

DATA

Yes, the technology addresses issues like incomplete datasets and biases by relying on standardized security frameworks (e.g., OWASP). It avoids correlation/causation errors by focusing on repeatable and validated test cases. However, user-defined device data introduces subjectivity, and mitigation involves anonymization and strict data handling protocols.

FUTURE

If widely adopted, the technology could standardize IoT security validation, making secure devices the norm. However, misuse or unethical applications (e.g., by malicious actors) could undermine trust in IoT ecosystems. It could also lead to an arms race between attackers and defenders, requiring continuous updates to stay effective.

PRIVACY

Yes, the technology may indirectly collect data such as device IP addresses, MAC addresses, and user-defined device configurations during testing. While not directly personal data, this information can be linked to individuals if combined with other data sources.

INCLUSIVITY

Potential biases may arise from the datasets used for testing (e.g., focusing more on high-end devices like Philips Hue and less on low-cost alternatives). To reduce this bias, the technology incorporates multiple device types and encourages diverse testing scenarios. However, assumptions about core vulnerabilities could limit its applicability to other IoT devices.

FIND US ON WWW.TICT.IO

NAME: Automated Validation of IoT Security Design Patterns for Smart Lamps

TICT

DATE: July 4, 2025 6:34 PM

DESCRIPTION OF TECHNOLOGY

The project focuses on automating the validation of IoT security design patterns, specifically for smart lamps like Philips Hue and low-cost models. Using tools such as Node-RED, Nmap, and Wireshark, the system identifies vulnerabilities like weak encryption and insecure communication. It validates security patterns, including encrypted communication and authentication mechanisms.…

HUMAN VALUES

How is the identity of the (intended) users affected by the technology?

To help you answer this question think about sub questions like:

- If two friends use your product, how could it enhance or detract from their relationship?
- Does your product create new ways for people to interact?…

TRANSPARENCY

Is it explained to the users/stakeholders how the technology works and how the business model works?

- Is it easy for users to find out how the technology works?
- Can a user understand or find out why your technology behaves in a certain way?
- Are the goals explained?
- Is the idea of the technology explained?
- Is the technology company transparent about the way their…

IMPACT ON SOCIETY

What is exactly the problem? Is it really a problem? Are you sure?

Can you exactly define what the challenge is? What problem (what 'pain') does this technology want to solve? Can you make a clear definition of the problem? What 'pain' does this technology want to ease? Whose pain? Is it really a problem? For who? Will solving the problem make the world better? Are you sure? The problem definition will help you to determine…

STAKEHOLDERS

Who are the main users/targetgroups/stakeholders for this technology? Think about the intended context by…

When thinking about the stakeholders, the most obvious one are of course the intended users, so start there. Next, list the stakeholders that are directly affected. Listing the users and directly affected stakeholders also gives an impression of the intended context of the technology.
…

SUSTAINABILITY

In what way is the direct and indirect energy use of this technology taken into account?

One of the most prominent impacts on sustainability is energy efficiency. Consider what service you want this technology to provide and how this could be achieved with a minimal use of energy. Are improvements possible?

HATEFUL AND CRIMINAL ACTORS

In which way can the technology be used to break the law or avoid the consequences of breaking the law?

Can you imagine ways that the technology can or will be used to break the law? Think about invading someone's privacy. Spying. Hurting people. Harassment. Steal things. Fraud/ identity theft and so on. Or will people use the technology to avoid facing the consequences of breaking the law (using trackers to evade speed radars or using bitcoins to launder…

DATA

Are you familiar with the fundamental shortcomings and pitfalls of data and do you take this sufficiently into…

There are fundamental issues with data. For example:

- Data is always subjective;
- Data collections are never complete;
- Correlation and causation are tricky concepts;
- Data collections are often biased;…

FUTURE

What could possibly happen with this technology in the future?

Discuss this quickly and note your first thoughts here. Think about what happens when 100 million people use your product. How could communities, habits and norms change?

PRIVACY

Does the technology register personal data? If yes, what personal data?

If this technology registers personal data you have to be aware of privacy legislation and the concept of privacy. Think hard about this question. Remember: personal data can be interpreted in a broad way. Maybe this technology does not collect personal data, but can be used to assemble personal data. If the technology collects special personal data (like…

INCLUSIVITY

Does this technology have a built-in bias?

Do a brainstorm. Can you find a built-in bias in this technology? Maybe because of the way the data was collected, either by personal bias, historical bias, political bias or a lack of diversity in the people responsible for the design of the technology? How do you know this is not the case? Be critical. Be aware of your own biases.…

FIND US ON WWW.TICT.IO