Vacuum Robot Security

Trong Nguyen
Department of Computer Science
Cal Poly Pomona Cybersecurity and Awareness Fair 2021
Cybersecurity Problem-Solving

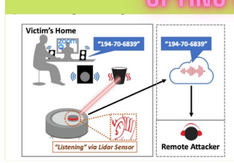
Problem

VACUUM ROBOT SECURITY

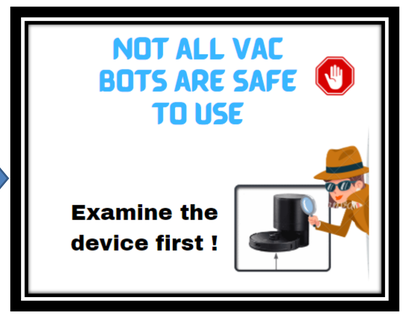
IMPERSONATING VACUUM BOT

- Reverse engineer to find the key to authenticate all Neato robots.
- Control any robot through the server with a known serial number
- Potential attack: Stealing, data leaking, victim's IP address discovering

SPYING WITH VACUUM BOT



- LIDA Sensor can sense sounds from vibrations of nearby objects
-Use machine learning to train and make prediction models based on vibration and sound
-Attacker uses sound captured vibration and uses prediction model to refer to the sound

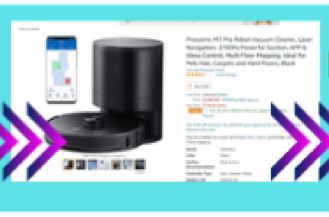


SOPHISTICATED SENSORS + cloud vulnerabilities

PRIVACY VIOLATION

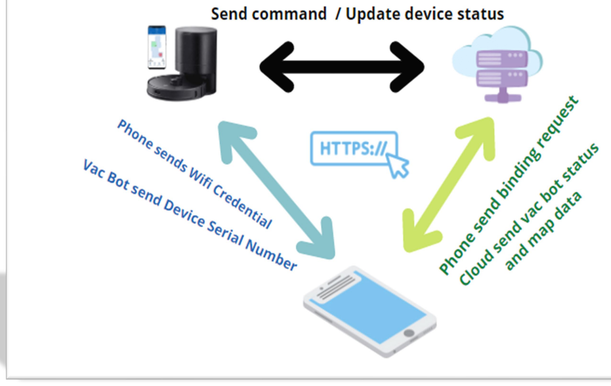
Approach

CHOOSE A POPULAR PRODUCT

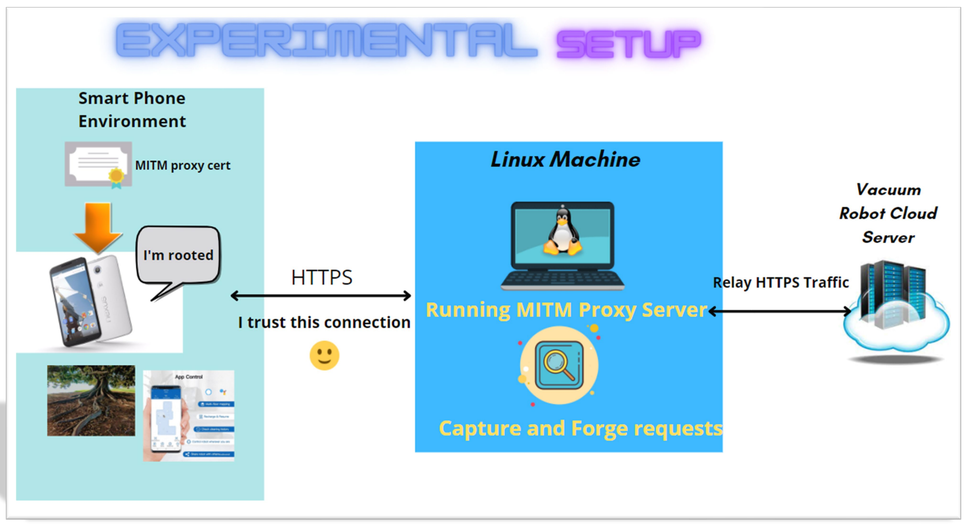


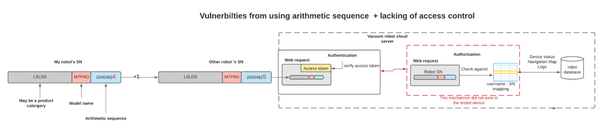
Perform static & dynamic analysis to find vulnerbilities

VACUUM ROBOT ECOSYSTEM



EXPERIMENTAL SETUP

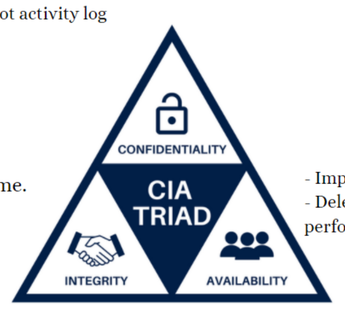




Results

Found VIOLATIONS OF CIA TRIAD

- Retrieve victim's map data without permission.
- Check the online status of the victim's robot
- Retrieve the victim's home wifi SSID and robot's IP address
- Retrieve robot activity log
- Change the victim's robot name.
- Tamper victim's map data.



- Impersonate the victim's robot
- Delete robot's map to alter robot's performance

	Definition	Attack scenario	Mitigation
Spoofing	Gaining access to a system by using a false identity.	Attacker can guess the serial number and control the robot on behalf of the owner	- Use server to generate the serial number randomly and assign to the robot - Check user id - robot mapping before authorizing request
Tampering	Unauthorized modification of data	Attacker can change/ delete victim's map data or change robot name	Same as spoofing mitigation by having stronger access control
Repudiation	Ability of users to deny that they performed specific actions or transactions.	An attacker may deny that they use an account with a tool to forge REST requests to gain unthorized access	Log user activites with user id , IP address, actual data sent
Information Disclosure	Unwanted disclosure of private data	An an attacker can use a known robot serial number to retrieve the victim's robot data such as map, device log, wifi SSID , IP addresses	- Before allowing a request, check if the request comes from an authorized user - Use the server-generated serial number and avoid arithmetic SN
Denial of Service	Flooding the machine with request to overload the system	Robot cloud server does not limit how many request a user can send in each unit of time. An attacker can perform DDOS attack.	Use IDS/Firewall to limit/ drop number of requests from each user in a period of time to prevent flooding attack
Elevation of Privilledge	User with limited privileges assumes the identity of a privileged user to gain higher access	An attacker can perform an injection, buffer overflow attack to execute privileged commands	Protect API endpoints to treat input as strings only by validating the input on both server-side and client-side. Perform security in-depth, least privilege principle

Challenges

- Had to learn IoT ecosystem
- Set up testing environment with MITM Proxy and learn its Python API
- Time constraint due to other classes / projects

Conclusion

- Many IoT devices including vacuum robot are built recklessly that affect user privacy
- The main issues come from lacking proper access control, using hardcoded serial number system and not maintaining IoT device state consistency.
- Manufacturers should not only focus on designing a “beautiful” robot but also need to secure their cloud server
- Users should choose and inspect their IoT devices carefully to prevent the case that their device may be weaponized for bot net attacks

Acknowledgments

-F. Ullrich, J. Classen, J. Eger, and M. Hollick, “Vacuums in the cloud: Analyzing security in a hardened IoT ecosystem,” in *13th {USENIX} Workshop on Offensive Technologies ({WOOT} 19)*, 2019.
- E. Zeng and F. Roesner, “Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study,” in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, 2019, pp. 159–176.
- S. Sami, Y. Dai, S. R. X. Tan, N. Roy, and J. Han, “Spying with your robot vacuum cleaner: Eavesdropping via lidar sensors,” in *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*, 2020.
- “How mitmproxy works,” *Mitmproxy.org*. [Online]. Available: https://docs.mitmproxy.org/stable/concepts-howmitmproxyworks/. [Accessed: 04-May-2021].