A Vulnerability Assessment of Smart Vacuums

Abigail Baker, Dakota State University
Mentor: Laura Ann Anderson, Geospatial Science and Human Security, Oak Ridge National Laboratory

INTRODUCTION

Smart vacuums are in many homes throughout America. These devices, while helpful in keeping a home clean, are part of the Internet of Things (IoT). IoT devices often have lax security measures, if any security exists. They are vulnerable to many exploits other devices such as phones and computers are protected against. In addition, IoT devices have not been thoroughly researched yet, creating a need for more research and funding in this area. This poster explores potential areas of lax security in iRobot Roomba Vacuums and Eufy Robot Vacuums.

Eufy Clean G30 SES, nicknamed King Pin

EQUIPMENT

Vacuums:

- iRobot Roomba Combo i5+ (Annie)
- iRobot Roomba Vac Essential (Destroyer)
- Eufy Clean G30 SES (King Pin)

Tools:

- Kali Linux Machine
- Windows HP Machine
- Samsung Galaxy A12 Phone
- Wireshark
- Nmap
- Deauthentication Script

ACKNOWLEDGEMENTS

[1] Austin Albright provided the base for the Deauthentication script.
[2] This work was supported in part by the U.S. Department of Energy, Office of Science, Office of Workforce Development for Teachers and Scientists (WDTS) under the Science Undergraduate Laboratory Internships program.

RESULTS

Nmap Scan:

Annie has port 8883 open, which is not associated with any exploits. King Pin has port 6668 open. This port is associated with several exploits and could be used to remotely communicate with the device. Destroyer has ports 8883, 5678, and 58362 open. Port 5678 is associated with several exploits and 58362 is unknown.

Wireshark Capture:

The robots all communicated with multiple IP addresses, with Destroyer sending the most packets, followed by Annie and then King Pin.

	Annie	Destroyer	King Pin
Total Packets Sent	2,913	5,853	13,522
Total Packets Received	2,013	3,822	4,034
Unique Conversations	27	58	10

Summary of the conversations each robot had over a 15-hour period

Deauthentication Attack:

Deauthentication packets were sent at various speeds to each robot, performing ten attacks per speed and recording each robot's recovery time. King Pin recovered quickest while Destroyer recovered second quickest, and Annie recovered slowest. Only Annie had a complete failure due to the attack, requiring a reboot to return to functionality.

	Annie		Destroyer		King Pin	
Packets Per Second	Mean	Std. Deviation	Mean	Std. Deviation	Mean	Std. Deviation
1	40.9	17.9	67.2	122.0	17.6	13.8
2	46.7	64.6	31.5	17.9	23.6	20.8
4	83.4	110.5	26.5	5.1	15.1	3.0
8	50.6	69.8	26.6	2.5	16.4	4.8
16	33.1	31.2	25.7	1.1	29.5	35.6
32	91.0	66.2	59.3	102.8	15.4	4.2
64	58.2	14.4	25.0	3.2	32.5	41.3
128	68.9	24.5	24.3	4.0	23.0	25.4
256	57.7	16.7	24.9	0.7	29.5	23.1
512	38.3	9.6	23.4	2.3	27.1	22.3
Overall	57.0	53.8	33.4	50.8	23.0	22.9

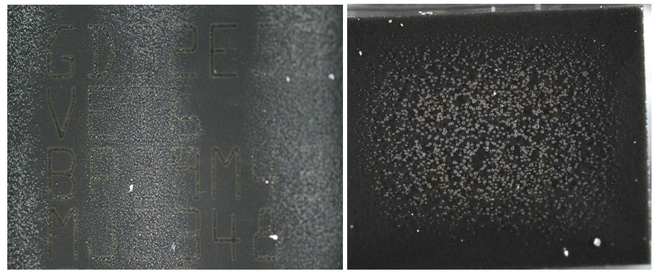
The average recovery time for each attack speed and the overall attack

Other Things of Note:

- Destroyer's chipset is made by a Chinese company and is designed for an AI voice emulator
- The devices only work on the 2.4 GHz network and do not work with WPA3 encryption

CHALLENGES

- The Eufy Clean app requires iOS 10.0 and newer or Android OS 5.0 and newer
- The iRobot Home app requires iOS 15.0 and newer or Android OS 9.0 and newer
- Overnight Wireshark captures resulted in 10+ million packets to sift through and often caused the computer to lag or crash
- Conformal Coating on the printed circuit board prevents chip labels from being easily read
- During setup, the router's 5 GHz network must be off to ensure both phone and vacuum are on 2.4 GHz
- When a vacuum crashed, it often took 5+ minutes and several reboots to become functional again



Examples of Conformal Coating on Destroyer

NEXT STEPS

Further research should explore the open ports in more detail as some, such as 6668 on King Pin, may be used for remote communication. Additionally, research into the robots' chipsets and potential capabilities should occur. The chipsets likely have additional features that are unavailable in the current configuration but may still be present in the programming.

CONCLUSION

Of the vacuums tested, Eufy's Clean G30 SES (King Pin) appears to be the most secure, with the fewest ports open and smallest amount of outside communication. iRobot's Combo i5+ (Annie) is the next most secure, and iRobot's Vac Essential (Destroyer) is the least secure due to its many open ports and outside conversations.