A Security Assessment of a Voice-Based Virtual Assistant

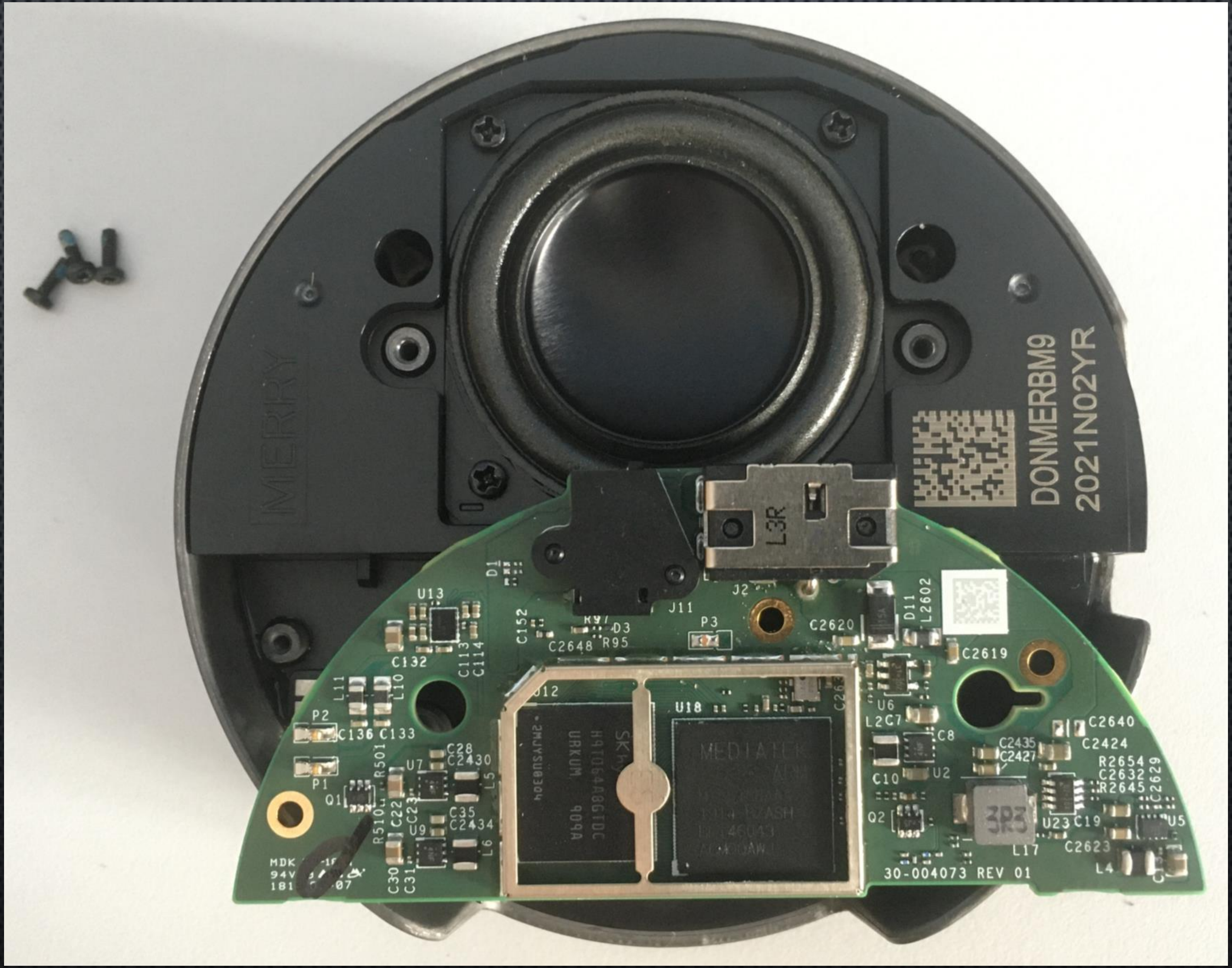
Ronak Kapadia (1722325)

THE PROJECT ITSELF

- Project main aim
  - Arrive at an informed assessment/evaluation of the security measures adopted by a certain voice assistant, this also included an analysis and evaluation of the privacy implications of the assistant.
  - Does this assistant employ adequate security and privacy measures to protect its consumers?

Voice Assistant & Device

- Assistant
  - Amazon Alexa
- Device
  - Amazon Echo Dot (3rd generation)


MERRY
DONMERBM9
2021N02YR
L3R
J2
J11
P3
U13
U18
U6
MEDIATEK
3R3
L17
30-004073 REV 01

Security Assessment Process

- Generally, security assessments are formed through the results of extensive testing of a system.
- Attack/Test → Results/Response → analysis → Evaluation

Overview of Attacks

- Skill-Based attacks
    - Skill squatting
    - Skill privacy
- General attacks
    - SYN flood
    - ARP Spoof
- Smart speaker/assistant attacks
    - Previous vulnerabilities

ARP SPOOF ATTACK

SYN FLOOD ATTACK

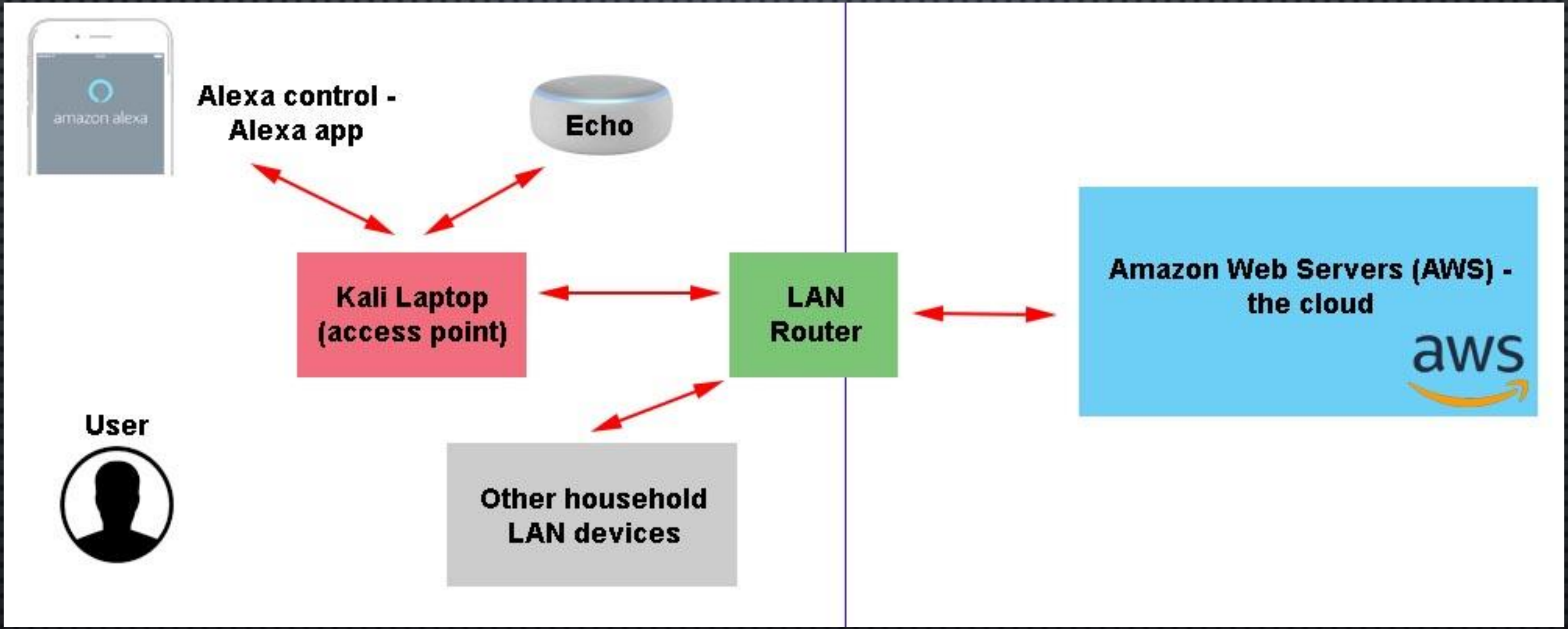
- Was also performed similar to the previous (DoS), but longer recovery.

WHAT IS INTERESTING ABOUT YOUR PROJECT?

- Security testing
  - Efficiency, effectiveness, resourcefulness, portability
  - Breaking and fixing systems
- Emerging technology (smart speakers)
  - New verbal UI

What was the hardest part?

1. Steep learning curve
   - Weeks of research and practise
2. Amazon skill development (frustration and time concern)
   - Netted no final results
3. Local testing network



Alexa control - Alexa app

Echo

Kali Laptop (access point)

LAN Router

Amazon Web Servers (AWS) - the cloud

User

Other household LAN devices

How could you extend your project?

1. Future knowledge
   - New techniques, tools and approaches.
2. Revisit skill development
   - Drop trail & error string testing, look for another way to squat
3. Testing security of third-party smart home devices
   - Third-party device compromise echo/Alexa?

THAT’S ALL FOLKS!

- I hope it has answered more questions than it has created!
- Email me if you need the slide set or demo video
- Thanks for listening to my project demo ☺