

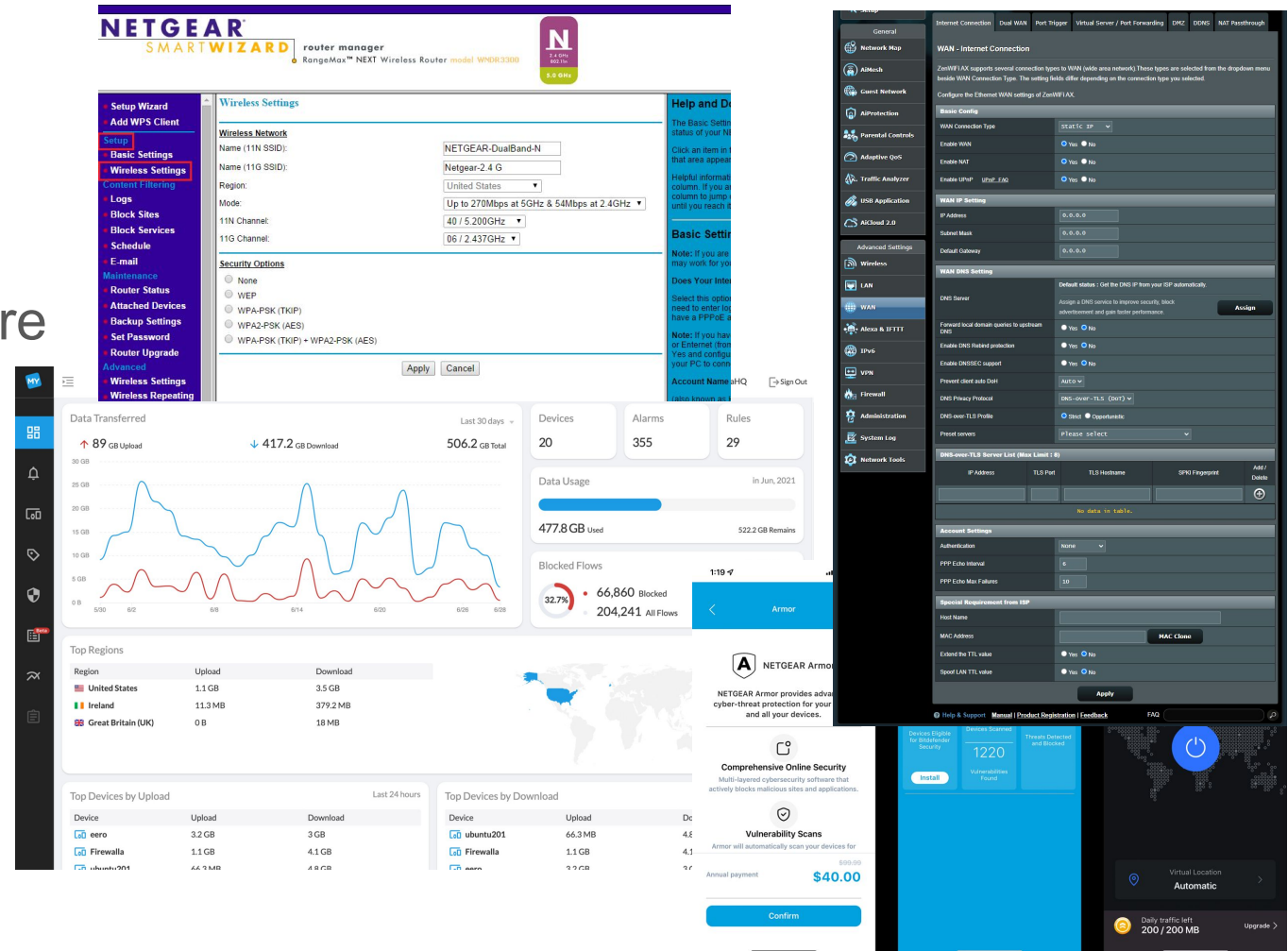
FINAL PRESENTATION

TEAM S.LAB

Leroy Chee
Ben Leonard
Anton Soloshenko
Sudip Kar

Increasingly Connected, Increasingly Vulnerable?

- Over 17 *billion* IoT devices
- 400% Increase in IoT malware attacks, year-over-year
- Subjective Simplicity

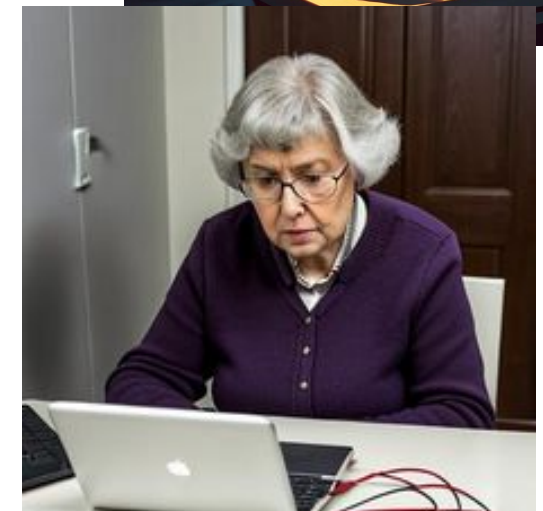
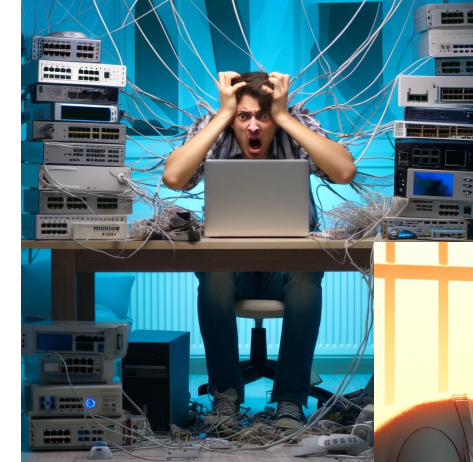


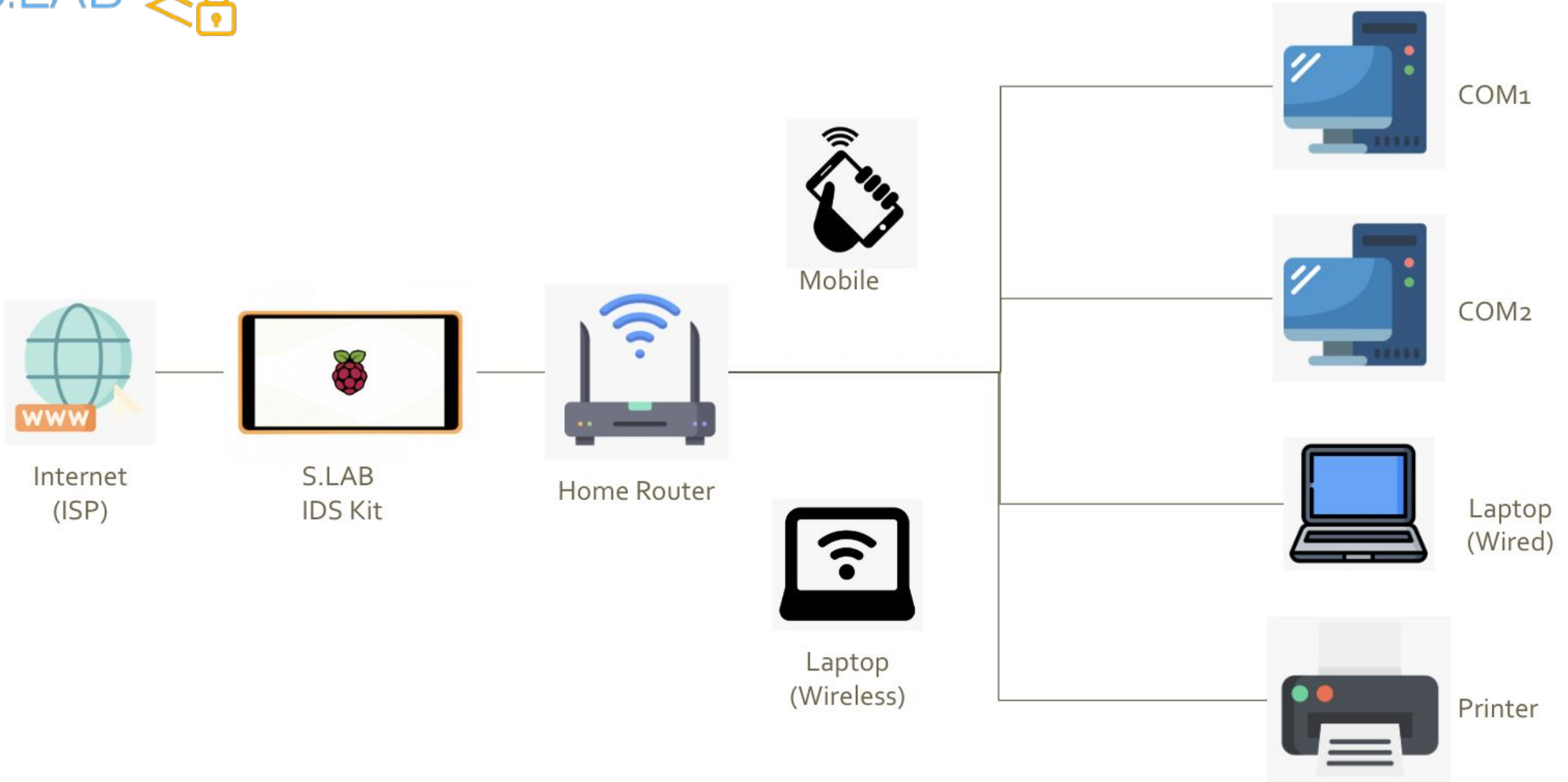
The image displays a collage of screenshots from a Netgear router's web interface, illustrating various settings and monitoring tools. Key elements include:

- Wireless Settings:** A configuration page for the wireless network, showing fields for Name (11N SSID), Name (11G SSID), Region, Mode, 11N Channel, and 11G Channel. Security options include None, WEP, WPA-PSK (TKIP), WPA2-PSK (AES), and WPA-PSK (TKIP) + WPA2-PSK (AES).
- Dashboard:** A central overview showing data transfer statistics (89 GB Upload, 417.2 GB Download, 506.2 GB Total), device counts (20 Devices, 355 Alarms, 29 Rules), and a world map highlighting top regions like the United States, Ireland, and Great Britain (UK).
- Comprehensive Online Security:** A prominent overlay for Netgear Armor, offering vulnerability scans for \$40.00. It includes a 'Vulnerability Scans' button and a 'Confirm' button.
- WAN - Internet Connection:** A settings page for the WAN connection, including options for WAN Connection Type, IP Address, Subnet Mask, Default Gateway, and DNS Server.

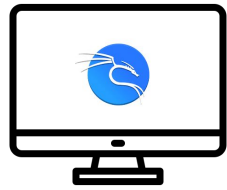
Non-technical Users, Technical Attackers

- Time, money, peace of mind; empowering the end user
- Reducing the barrier to action, instilling confidence
- Intentionally uncomplicated



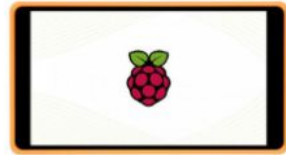


Demo Setup



Adversary

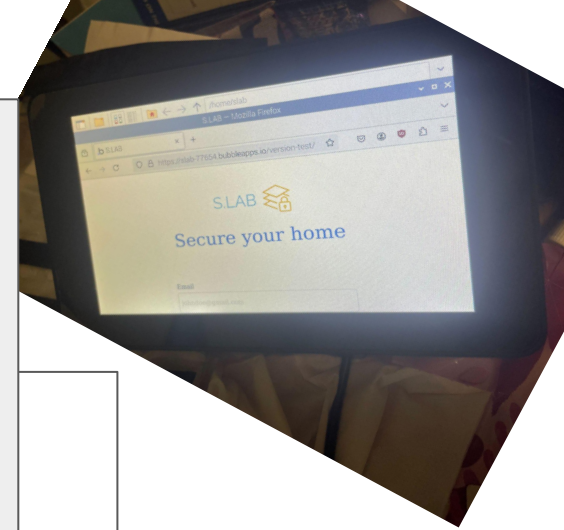
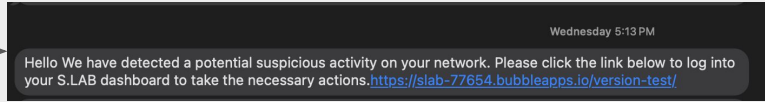
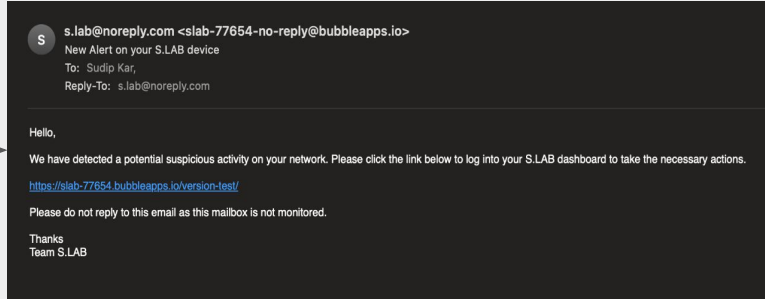
Nmap scan used for typical reconnaissance



1. DETECT

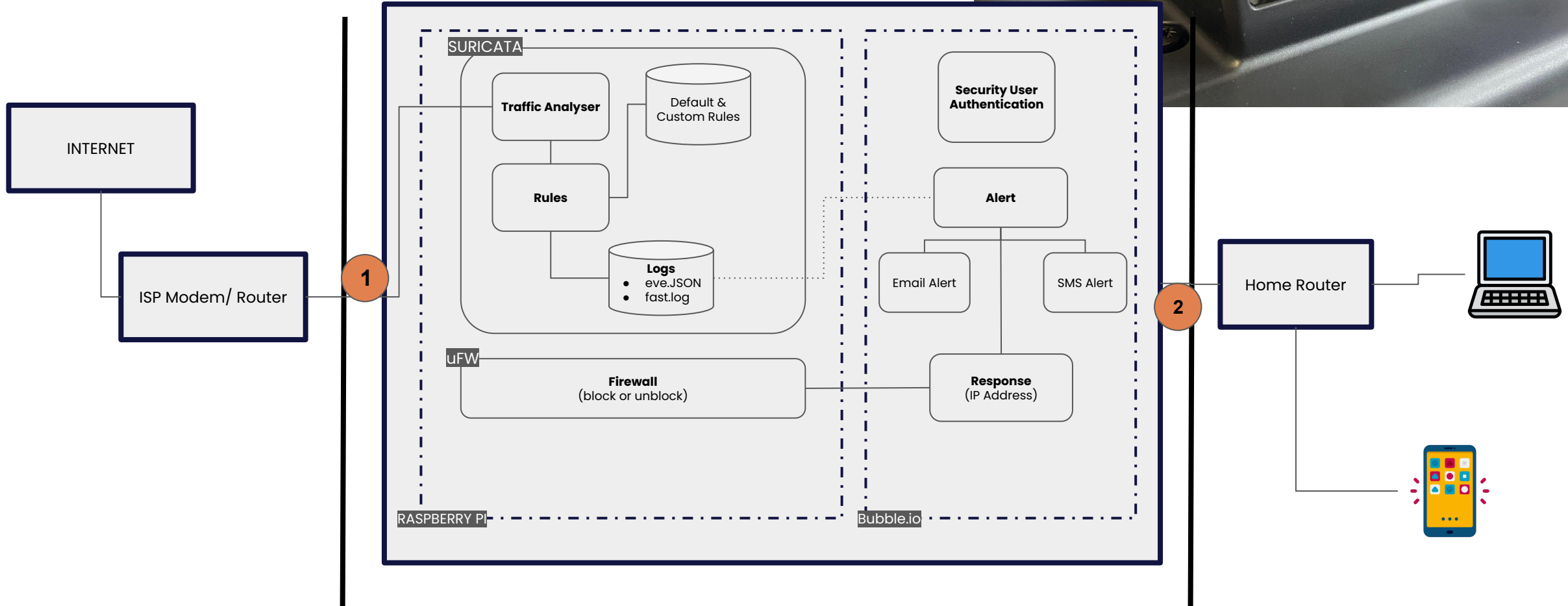
2. ALERT

Away from Home



3. RESPONSE

Solution Architecture



S.LAB Security Considerations

STRIDE Threat Model

Potential Risks

Mitigations

S : Spoofing of User Identity

- Unauthorized access
- Unauthorized actions
- User Privacy

- Privacy by design (Log retention)
- Enforce strict password requirements
- Enforce periodic password change

T : Tampering

R : Repudiation

I : Information Disclosure

- Loss of data
- Unauthorized access to data
- User access compromised

- Proper input sanitization
- Timely DB upgrades

D : Denial of Service (DOS)

E : Elevation of Privilege

- Spy on devices
- Addition of malicious device
- Malicious redirection
- Execute MITM
- Allow malicious connections
- Add/modify rules in IDS

- Robust firewall rules
- Update router software & hardware
- Avoid using old routers
- Periodic updates to latest software
- Avoid using old IDS

What's Next?



Step
01



Machine Learning
(AI-Powered Threat Detection)

Improve Firewall
(Application and Identity-Based Inspection)



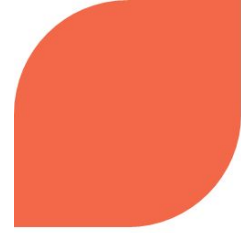
Step
02



Step
03



Expand Customization
(Better Network Segmentation)



THANK YOU

<https://www.ischool.berkeley.edu/projects/2024/slab-home-ids>

<https://www.slab-ids.net>

