Threats to Voice Control Systems and their mitigations

Presented by Patrick Crowe

Motivation

VCS is relatively new and vulnerable and needs its defense protocol reviewed. Privacy (and eventually lives) are

Threats

- Replay attack
- Hidden Command att
- Inaudible attack
  - DolphinAttack
- Audio Hotspot attack
  - Long-range DolphinAttack
- LipRead

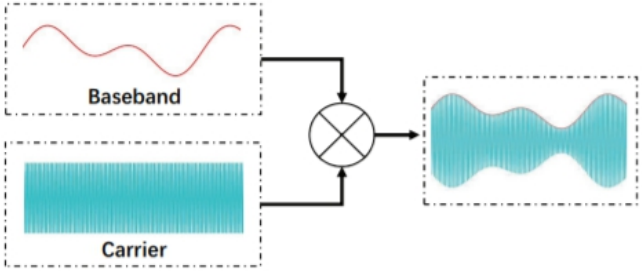


Figure 9: An illustration of modulating a voice command onto an ultrasonic carrier using AM modulation.

Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. 2017. DolphinAttack: Inaudible Voice Commands. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17). Association for Computing Machinery, New York, NY, USA, 103–117. DOI:https://doi.org/10.1145/3133956.3134052

Threats

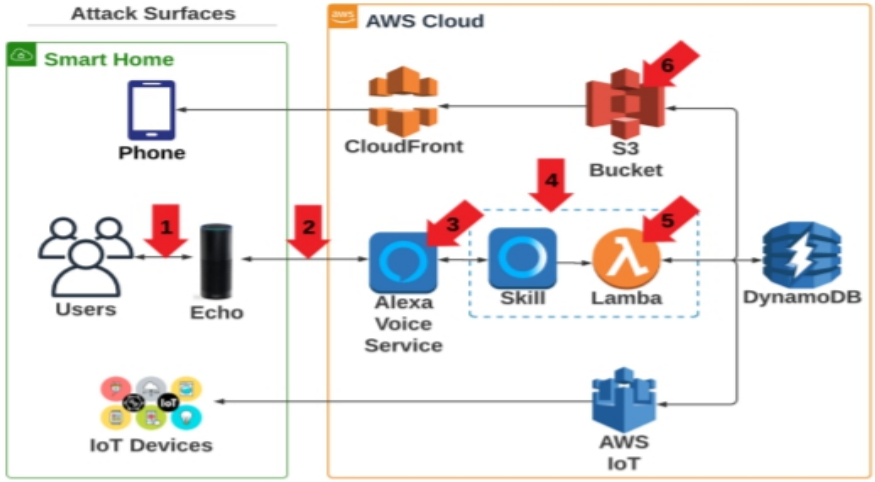


Fig. 2: Attacks surfaces of Alexa ecosystem

Li, Yanyan & Kim, Sara & Sy, Eric. (2021). A Survey on Amazon Alexa Attack Surfaces.

- Surfaces:
  - Voice Captu
  - Traffic b/w speaker and cloud server
  - Overriding service (skill) calls through dialect misinterpretation
    - Target server storing media associated with service (skill)
  - SQL Injection

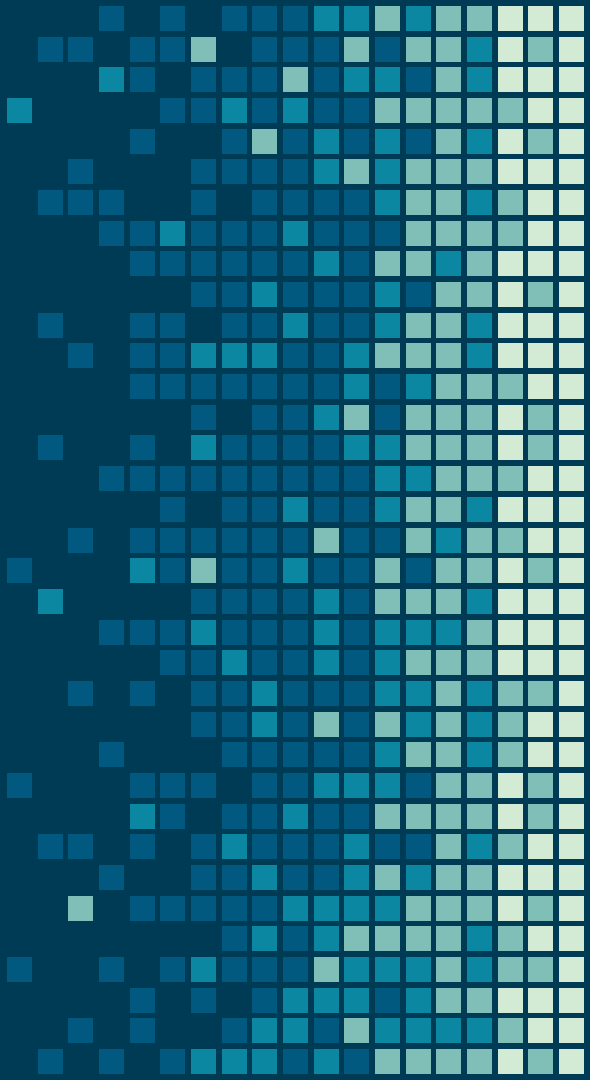
Defenses

- 2MA (Two Microphone Authentication)
  - Can localize a source to within a narrow physical cone ($< 30°$) with zero false positives, eliminate replay attacks and prevent the injection of inaudible/hidden commands
- Pop authentication

Defenses

- WSVA checks the consistency between the voice signal and its corresponding mouth motions, which can be captured by wireless signals (CSI)
- Independent device that deploys a two-step lightweight detecting algorithm to identify the attack signals

By gathering current knowledge about our VCS vulnerabilities, we can make them more secure and start trusting them to do more important things, like drive cars.



Discussion and Questions