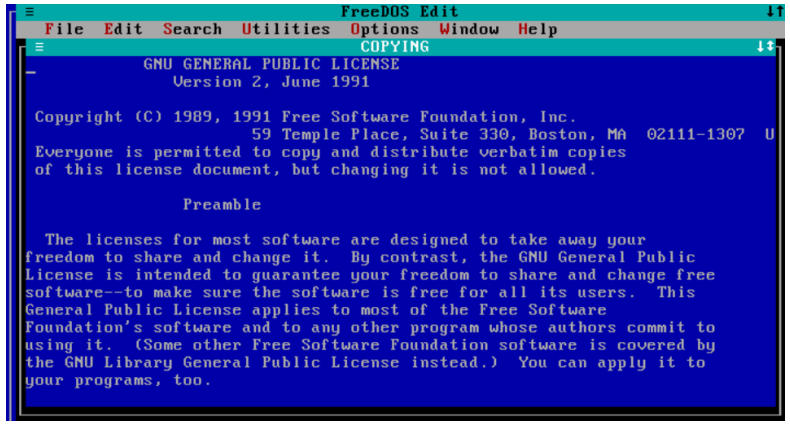
Voice-based Security Operation with Smart Speaker, SDN, AI

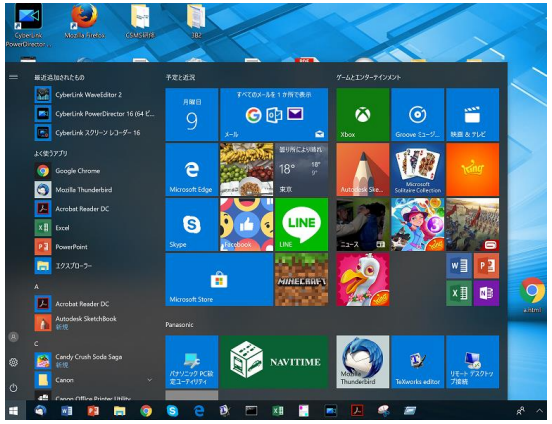
Takuho Mitsunaga, University of Tokyo
Yoshinori Matsumoto, Capy Inc.

Background

- With the advancing information technology, richer computer interfaces have been invented and applied into various devices. It started from classic CUI input into black and white screens, and then shifted to GUI to click on an icon with a mouse, and lately Voice User Interface (VOI), which operates by voice, has been developed.



CUI(character user interface)



GUI (graphical user interface)

Examples of VUI (voice user interface)

cite:https://store.google.com/us/product/google_home
https://www.amazon.com/dp/B06XCM9LJ4/

Background

- This can be a one step towards what we used to think “futuristic” as in “Knight Rider” or “Star Trek”. In the near future, cars and spaceships can be operated just by voice commands using AI and VUI. Such automation technology has the following three advantages:

1. Automated operation
2. Efficient operation
3. Simplified operation

Security Operation

- Our research aims to apply the voice command technology to accomplish automation, efficiency and simplification in cyber security operations.

- Our system proposes a combined use of AI and Software Defined Network (SDN) for automatic blocking of communication and threat analysis by interacting with machines by voice.

Building Blocks

Alert
- Notification is sent from Log Analyzer when suspicious communication is detected.

AI Speaker
- A speaker as an interface (communicates with the cloud)

External Organization
- Partner organizations who share indicators

FW
- Firewall

SDN Switch
- Dynamically change network configurations based on commands from SDN Controller

Log Analyzer
- Collects network logs in an organization
- Stores indicators that were received in the past or shared publicly

Smart Speaker API
- Cloud server communication with AI speakers
- Provided by Google, Amazon
- Sends our API based on the information collected by the speaker

SDN Controller
- Conveys information from Speaker API to SDN Switch
- In this research, Smart Speaker API and SDN Controller on the DMS are only allowed to communicate through secure protocols (e.g. VPN)

Proxy Server
- Collects network logs in an organization
- Stores indicators that were received in the past or shared publicly

Sample scenario