Dolphin Attack: Inaudible Voice Commands

## 1. Target system & service (Contributed by Taehwa Lee and TA)

- VCS: Voice Controllabe System

- An approach to inject inaudible voice commands at VCS

- The ultrasound channel (i.e., f > 20 kHz) and the vulnerability of the underlying audio hardware.

## 2. Vulnerability (Contributed by Taehwa Lee and TA)

- High frequency sound like dolphins, so it is inaudible for human, but it is accepted by the machine

- In reality, some sensors have non-linear parts and that non-linear parts can make the inaudible sound pass the low pass filter.

## 3. Exploitation (attacks) (Contributed by Taehwa Lee)

- If attackers inject a modulated signal, then people cannot hear it. When it passes the microphone, a non-linear part appears, be amplified, and it can pass the low pass filter and manipulate the VCS

- The system knows who the owner is, so brute force attacks with TTS system. Recording the owner's sentence first, and then synthesize the activation command by concatenating the recorded sentences.

## 4. Evaluation and experimental method (Contributed by Taehwa Lee and TA)

- They made their custom inaudible sound generator and portable transmitter for the feasible attack. And they experimented with many products such as Samsung and Apple.

- Also, they measured various attack vectors such as sound pressure level, attack distance, and so on.

- Even the attacker uses the portable device, the attacker has to go at least 1m for the attack. It is hard to use in the reality.

**5. Defense (potential solutions for the attacks) (Contributed by Junho Ahn)**

- In hardware-based defense, 1) Enhance and design the microphone to suppress any acoustic signal and 2) Add a module that detects modulated voice commands and cancels it before LPF.

- In software-based defense, looks into unique features of modulated voice commands that are distinctive from original ones since recovered attack signal show difference from both the original signal and recorded signal in the high frequency range.