Michael Tang
Due 3/2/19 (Both postponements used, 48h)

Area Summary: Security

Visually Fingerprinting Humans Without Facial Recognition Wang et al. establish the importance of human recognition methodologies for AR and other forward-facing technologies. They propose a methodology that does not require facial recognition, due to the fact that faces are often hard to see in environments with fixed cameras and also due to consumer unease with uploading facial profiles to corporate/public servers. They stress the usefulness this method brings to privacy, such as users being able to upload a custom fingerprint with a "do not save/record" option to keep their identity aspects, such as actual name or device MAC address, private. In their example implementation, InSight, the emphasis is on motion sensing (mainly heading via prediction and accelerometer data of motion) and on color sensing via spatiogram or user custom upload. Wang et al. find promising accuracy in both motion and color detection for InSight.

DolphinAttack: Inaudible Voice Commands Zhang et al. take a first look into the realm of inaudible attacks on voice command systems. These systems must be outside the frequency range of human hearing but depending on the device, voice reception is filtered differently to match that hearing range. They analyze the most popular voice recognition interfaces and find that optimal attack frequency varies between devices but can be easily tuned. Across 16 devices and 7 speech recognition systems Zhang et al. succeeded nearly every time in attacking the systems with inaudible commands after recognition. They also discuss a solution to activating systems that require recognition of a specific user's voice, by stitching together the required intonations after listening to the user for only a short amount of time. Overall, attack efficacy is sufficient for real life attacks on certain devices like the iPhone 4S and Amazon Echo. They establish many scenarios where an attacker may be motivated, such as website-based drive-by phishing or nonconsensual recording. Possible defenses iterated over include classifier detection of non-audible commands and microphone frequency filtering that is even closer to human range.

Acoustic Eavesdropping through Wireless Vibrometry Wei et al. expound on the abilities of wireless vibrometry to detect sound-based activities without the need for a nearby, attacker-placed microphone. The particular setups they use for their implementation, audio-radio transformation (ART), are reflective (broadcasting of wireless signals and measurement of their reflection) as well as emissive (AP capturing sound output's audio waves as Wi-Fi and decoding the packets into sound). Particularly useful to attackers is the high efficacy that Wei et al.'s demonstration of (ART) demonstrates when detecting beyond soundproofing materials. They can capture audio signal via these reflective/emissive techniques and use demodulation as well as prediction of multipath effect to create a very clear recorded audio. Wei et al. also establish that one can combat emissive capture via front-end imposed offset of packets and reflective capture via interfering activity such as human movement.

Speechless: Analyzing the Threat to Speech Privacy Anand and Saxena analyze the potential threat of smartphone accelerometers being able to detect speech via the small vibrations the audio causes. They claim that earlier studies giving promising indication of sound vibration detection were confounded by the smartphones being placed on the audio-emitting surface and capturing vibrations via physical conduction. To that end, they investigate capturing strength further away from these powerful sources as well as with weaker audio sources such as a laptop speaker and the human voice, and find much more limited capturability of audio via accelerometers.

Summary

With the advancement of technology comes many new avenues for one's privacy to be intruded upon, avenues that would not have been possible even a couple years ago and whose consequences have not been fully thought out. It is often the prerogative of security researchers to be able to capture these consequences ahead of their actually becoming mainstream and attacking mass groups, whether or not those factors are actually as dangerous as they seem.