D.J. Anderson dra2zp 11/27/2017

**Gyrophone**

Problem and importance

This paper addresses the problem that audio signals like human speech can be reconstructed and inferred from gyroscope signals such that it could determine what the speaker says and even who the speaker is. This is important because all smartphones as well as some other electronic devices have gyroscopes, and they could potentially be hacked to provide an attacker with this gyroscope data.

Hypothesis

This paper argues that human speech and speaker identification can be inferred from gyroscope signals. They claim that attackers could reconstruct an audio signal if a vulnerable person were to give personal information when the gyroscope is being used maliciously.

Assumptions

* People typically give their credit card information, social security number, or other personal information over the phone.
* People’s personal information will mostly consist of a set of numbers.

Strengths

* The authors showed that the gyroscope readings can map to a much wider frequency range since it’s a sinusoidal wave, which means frequencies outside of the range will still be captured by the gyroscope (although at a weaker signal).
* The authors achieved a 65% success rate for the speaker-dependent case, whereas chance would be 10%.

Weaknesses

* It is very unlikely that someone will give personal information over the phone, especially something like their entire credit card number along with the expiration date and security code or their entire social security number rather than just the last four digits.
* The success rate of 65% is actually quite low. For a social security number, which is only 9 digits, the authors would only get about 6 of them correct.

Compelling evidence

Table 6 is the most compelling because it shows that the highest success rate for the speaker-dependent case, which is 65%.

Presentation Interest Impact Overall Confidence

3 2 1 2 1

D.J. Anderson dra2zp 11/27/2017

**PitchIn**

Problem and importance

This paper addresses the problem that an array of IoT devices could be hacked to obtain non-acoustic sensor data, which could then work together to reconstruct an audio signal.

Hypothesis

This paper argues that intelligible speech can be reconstructed by fusing non-acoustic sensor data collected from a network of nodes.

Assumptions

* There will be multiple sensor nodes in one location, so they can all “pitch in” to help reconstruct an audio signal.
* The timing between sensor nodes will be very tight in order to aggregate data over multiple nodes.

Strengths

* The authors showed that the full human vocal range can be reconstructed if given a sufficient number of sensor nodes’ gyroscopic data.
* The authors showed that the sensor’s accuracy in reconstructing signals reached 79%.

Weaknesses

* The reconstructed speech signals must be manually analyzed to determine if the speaker said anything useful (like their credit card or social security number).
* Other identifying information (like the person’s name and address) must also be known, or else a credit card or social security number will be useless.

Compelling evidence

Figure 11 was the most compelling because it shows the recognition accuracy of four gyroscopes sampled at five different temporal offsets, one representing the best-case and one representing the worst-case scenario.

Presentation Interest Impact Overall Confidence

4 3 3 3 1