The Importance of Detecting Social Engineering

Tishauna Wilson, Ian G. Harris, PhD

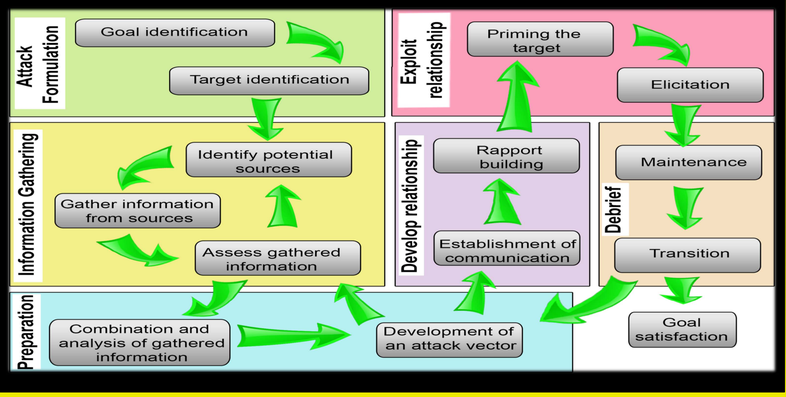
Department of Computer Science, University of California, Irvine

ABSTRACT

- This current research project “Fraudster” intends to detect vishing/social engineering attacks as they are occurring using a hardware engine.
- Vishing is the criminal practice of using social engineering and Voice over IP(VoIP) to gain access to private personal and financial information from the public for financial reward.
- Social engineering is the use of deception to manipulate individuals into giving out confidential information through any source of communication, which may be used for dishonest purposes.
- For this project, we decided to take the speech of the attacker, convert it, then, analyze it.
- We are programming the Raspberry Pi 3 (RP3) to detect vishing through audio with the help of IBM Watson’s Speech to Text Application Programming Interface (API).

INTRODUCTION

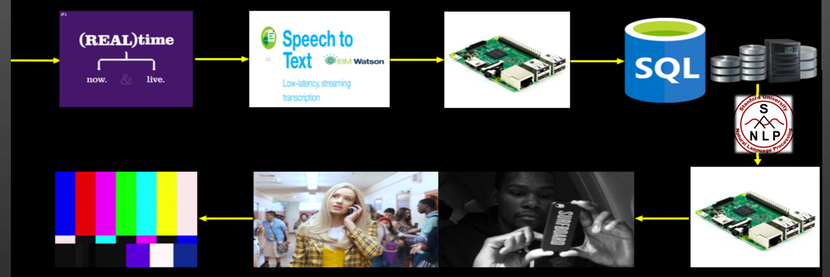
- “As computer security approaches improve, social engineering attacks have become more prevalent because they exploit human vulnerabilities which are hard to automatically protect” [1].
- “Individuals make themselves even more vulnerable to social engineering attacks by not expecting to ever be a victim of such an attack, and many will never know that they were a victim of such an attack” [2].
- Social engineering is extremely common, costly and detrimental in a variety of ways. This problem has caused a high level of distrust among technology users, and companies; individuals are wary of using technology for financial and personal purposes.
- According to “The Social Engineering Framework”, vishing led to a global loss of about $46.3 billion per year [3].



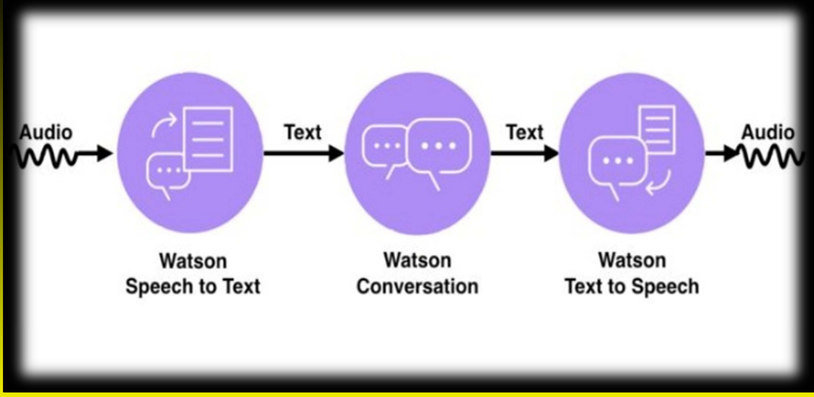
METHODOLOGY

(1) Methods

(1) Methods Cont.



FINAL DESIGN



RESULTS/CONCLUSION

- Fraudster will be a device that will accept audio and transcribe it into text and detect fraud in several seconds
- Fraudster will be the first device to detect social engineering attacks in audio streams.

```
# converting response content to JSON format
data = json.loads(resp.content)

# get text from data
text = data['_text']
```

WIT CODE

```
if text == text:
    print("Attacker Said: " + (text))
    turnonFraud(text);
```

IBM WATSON

FUTURE WORKS

- Mobile users should be able to access Fraudster through a mobile application.
- Fraudster will be able to reverse the attacker’s phone number if needed and forward the information to law enforcement using White Pages API and Twilio.

ACKNOWLEDGEMENTS

- Dr. Ian Harris for his mentorship
- University of California, Irvine, and Donald Bren Hall for their help, support and lab space
- Funding Sources: National Science Foundation (NSF)

REFERENCES

[1] Harris, I. G., Ph.D, Sawa, Y., Bhakta, R., & Hadnagy, C. (2016, March 24). Detection of Social Engineering Attacks Through Natural Language Processing of Conversations. Retrieved August 09, 2017, from http://ieeexplore.ieee.org/document/7439345/

[2] Heartfield, R., Loukas, G., Ph.D, & Gan, D., Ph.D. (2017, July 03). An eye for deception: A case study in utilizing the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks. Retrieved August 09, 2017, from http://ieeexplore.ieee.org/document/7965754/

[3] Vishing. (n.d.). Retrieved August 09, 2017, from https://www.social engineer.org/framework/attack-vectors/vishing/