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].

REFERENCES


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)

WIT CODE

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.

REFERENCES