CERIAS

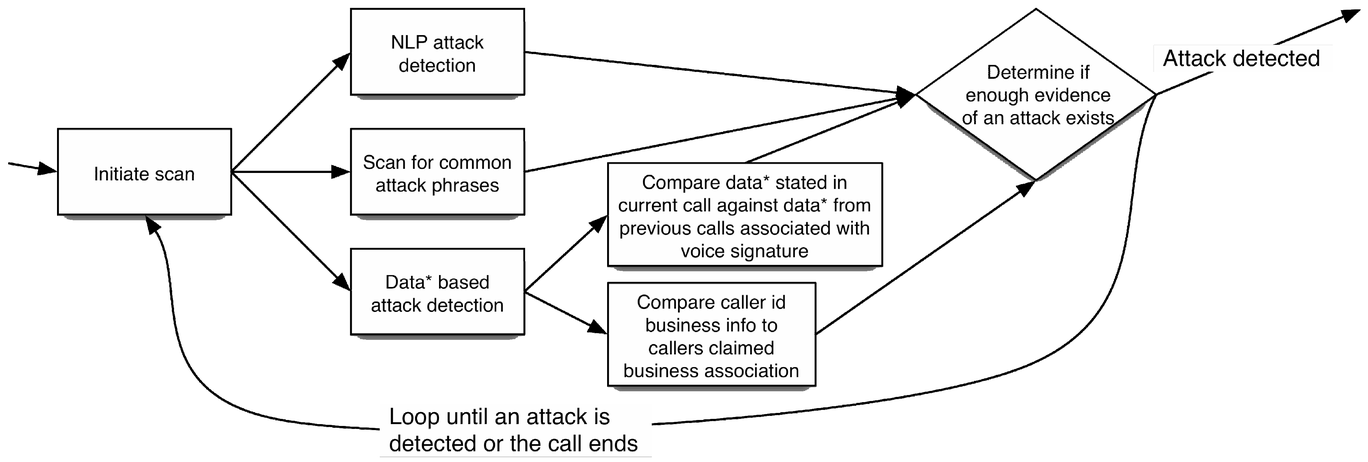
Social Engineering Defense Architecture

Michael D. Hoeschele & Marcus K. Rogers

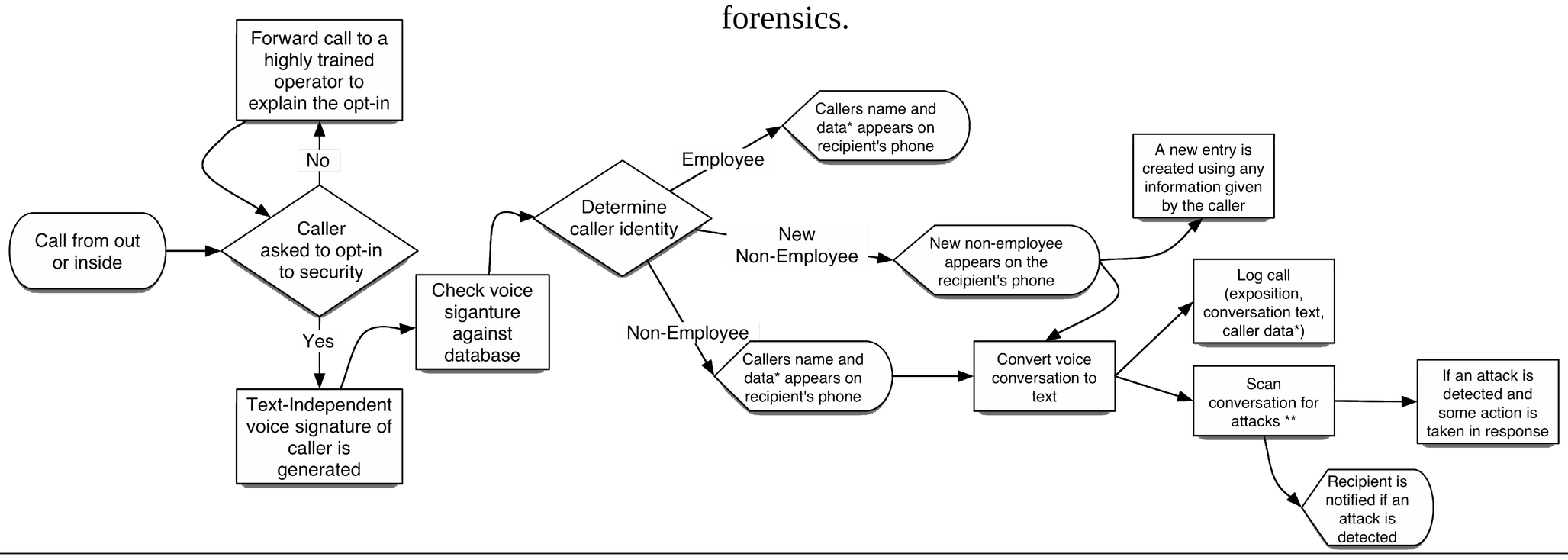
Abstract

This project proposes a theoretical solution to the problem of Social Engineering (SE) attacks perpetrated over the phone lines. As a byproduct real time attack signatures are generated, which can be used in a cyber forensic analysis of such attacks. Current methods of SE attack detection and prevention rely on policy and personnel training, which fails because the root of the problem, people, are still involved. The proposed solution relies on computer systems to analyze phone conversations in real time and determine if the caller is deceiving the receiver. This Social Engineering Defense Architecture (SEDA) is completely theoretical as the technologies employed are only in the proof of concept phase, but they are all proven to be tractable problems.

Attack Detection Diagram



SEDA Decision Tree Diagram



Future Research

Handling internal calls

- The proposed solution treats all calls equally regardless of the location of the caller.
- Streamlining of internal calls could decrease amount of processing power.

Response to detected attacks

- Attack response guidelines need to be formulated help create countermeasures.

SE forensics

- Forensics tools need to be created to parse SEDA log files and find clues.
- Policy on how to conduct a SE cyber forensic investigation using the logs needs to be created.
- All current research on cyber forensics has to be done in Social Engineering forensics.

PURDUE UNIVERSITY

CERIAS®

Discovery Park e-Enterprise Center