# Researchers design system to trace call paths across multiple networks

October 5 2010

(PhysOrg.com) -- Phishing scams are making the leap from email to the world's voice systems, and a team of researchers in the Georgia Tech College of Computing has found a way to tag fraudulent calls with a digital "fingerprint" that will help separate legitimate calls from phone scams.

Voice phishing (or "vishing") has become much more prevalent with the advent of cellular and voice IP (VoIP) networks, which enable criminals both to route calls through multiple networks to avoid detection and to fake caller ID information. However each network through which a call is routed leaves its own telltale imprint on the call itself, and individual phones have their own unique signatures, as well.

Funded in part by the National Science Foundation, the Georgia Tech team created a system called "PinDr0p" that can analyze and assemble those call artifacts to create a fingerprint—the first step in determining "call provenance," a term the researchers coined. The work, described in the paper, "PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance," was presented at the Association for Computing Machinery's Conference on Computers and Communications Security, Oct. 5 in Chicago.

"There's a joke, 'On the Internet, no one knows you're a dog.' Now that's moving to phones," said Mustaque Ahamad, professor in the School of Computer Science and director of the Georgia Tech Information Security Center (GTISC). "The need is obvious to build security into

these voice systems, and this is one of the first contributions to that research area. PinDr0p needs no additional detection infrastructure; all it uses is the sound you hear on the phone. It's a very powerful technique."

PinDr0p exploits artifacts left on call audio by the voice networks themselves. For example, VoIP calls tend to experience packet loss—split-second interruptions in audio that are too small for the human ear to detect. Likewise, cellular and public switched telephone networks (PTSNs) leave a distinctive type of noise on calls that pass through them. Phone calls today often pass through multiple VoIP, cellular and PTSN networks, and call data is either not transferred or transferred without verification across the networks.Using the call audio, PinDr0p employs a series of algorithms to detect and analyze call artifacts, then determines a call's provenance (the path it takes to get to a recipient's phone) with at least 90 percent accuracy and, given enough comparative information, even 100 percent accuracy.

Patrick Traynor, assistant professor of computer science, said that though the technology is modern, vishing is simply classic wire fraud: Someone gets a call which based on caller ID information appears legitimate, and the caller asks the recipient to reveal personal information like credit card and PIN details. During a five-day period in January 2010, bank customers in four U.S. states received fraudulent calls exactly like this, and instances of vishing date back at least to 2006.

PinDr0p is doubly effective for fraud detection, Traynor said, because it relies on call details outside the caller's control. "They're not able to add the kind of noise we're looking for to make them sound like somebody else," he said. "There's no way for a caller to reduce packet loss. There's no way for them to say to the cellular network, 'Make my sound quality better.'"

In testing PinDr0p, the researchers analyzed multiple calls made from 16

locations as far flung as Australia, India, United Arab Emirates, United Kingdom and France. After creating a fingerprint for calls originating from each location, they were able to correctly identify subsequent calls from the same location 90 percent of the time. With two confirmed fingerprints on a call, they could identify subsequent calls 96.25 percent of the time; with three it rose to 97.5 percent accuracy. By the time researchers had five positive IDs for a certain call, they could identify future calls from that source 100 percent of the time.

But PinDr0p does have its limitations—for the moment. "Call provenance doesn't translate into an individual's name or a precise IP address," said Vijay Balasubramaniyan, a Ph.D. student in computer science, who presented the PinDr0p paper in Chicago.

However Balasubramaniyan, Ahamad and Traynor are actively working on the next step: Using PinDr0p not just to trace call provenance, but to geolocate the origin of the call.

"This is the first step in the direction of creating a truly trustworthy caller ID," Traynor said.

Provided by Georgia Institute of Technology