Efficient Identification and Content Authentication for Phone Calls

*Cryptographically Authenticates Phone Calls for Secure Personal and Professional Communications*

This application cryptographically verifies the identity of callers to ensure that phone calls are authentic, assuring users that their information is safe. Financial, medical, or other personal information is commonly communicated through phone calls or other telephony technology. In 2014, 17.6 million Americans lost an estimated total of $8.6 billion in fraudulent phone scams, most of which were a result of caller ID spoofing. Telephony advancement is failing to meet the need for more secure and trustworthy communication channels. Caller identity is currently verified through look-up services or biometrics, such as voice recognition, but neither protect against forgery.

Researchers at the University of Florida have developed the AuthentiCall system, which cryptographically authenticates both parties on a call. AuthentiCall can be implemented on both personal and professional communications servers or as a cellular application.

**Application**

Authentication system that verifies financial, medical, and personal information is communicated securely, decreasing privacy issues and phone fraud

**Advantages**

- Detects 99 percent of tampered audio calls, increasing the integrity and security of conversations
- Initiates call monitoring within the first second, preventing redirection of calls to an adversary
- Installs easily on servers or cellular devices, providing protection for corporations, businesses, and individuals

**Technology**

The AuthentiCall system uses cryptography to provide stronger authentication through the coding and decoding of secure messages in data and audio channels. Cryptographic authentication is more secure than the other available methods, because it provides end-to-end authentication between the callers. The use of formally verified protocols, which bind data and audio channels, provides a stronger guarantee of the integrity of conversations that occur over traditional phone networks. This authentication occurs within the first second after a call is answered, and continuously refreshes during the duration of the call. AuthentiCall detects tampered audio, spoofing calls, or unverifiable identities.
Inventors

**Patrick G. Traynor, Ph.D.** is an associate professor in the Department of Computer and Information Science and Engineering (CISE) at the University of Florida. Dr. Traynor earned his bachelor’s degree in computer science at the University of Richmond and his master’s degree and Ph.D. in computer science and engineering from Pennsylvania State University. Dr. Traynor’s research interests focus on the security of mobile systems, with a concentration on telecommunications infrastructure and mobile devices. He has uncovered critical vulnerabilities in cellular networks and made the first characterization of mobile malware in provider networks. Follow @PatrickGTraynor

**Bradley G. Reaves** is a Ph.D. candidate in the Department of Computer and Information Science and Engineering (CISE) at the University of Florida. He received his B.S. and M.S. in Computer Engineering from Mississippi State University. Mr. Reaves’ research interests include mobile security, from mobile applications to telephony networks. He has previous experience in web and software security, as well as secure wireless networks. In 2010, he was named an NSF Graduate Research Fellow and is currently the lead graduate student from the Florida Institute for CyberSecurity (FICS).

**Logan E. Blue** is a Ph.D. candidate in the Department of Computer and Information Science and Engineering (CISE) at the University of Florida. He received his bachelor's degree in mechanical engineering and master's degree in computer science from the University of Florida. Mr. Blue’s research interests include mobile security, telephony networking, and computer software within secure networks.

**Luis Vargas** is a Ph.D. candidate in the Department of Computer and Information Science and Engineering at the University of Florida. He earned his bachelor’s degree in computer engineering from the Florida International University. His research interests include data science and medical systems security.

**Hadi Abdullah** is a Ph.D. candidate in the Department of Computer and Information Science and Engineering at the University of Florida. He earned his bachelor’s degree in electrical engineering from the University of Richmond. His research interests include network security and oat recipes.

Contact:
Richard Croley • 352-392-8929 • rcroley@ufl.edu
UF #16591 • Patent Pending