Poster: AuthentiCall: Efficient Identity and Content Authentication for Phone Calls

Bradley Reaves* Logan Blue* Hadi Abdullah* Luis Vargas* Patrick Traynor* Thomas Shrimpton*
* University of Florida

***Abstract*—Phones are used to confirm some of our most sensitive transactions. From coordination between energy providers in the power grid to corroboration of high-value transfers with a financial institution, we rely on telephony to serve as a trustworthy communications path. However, such trust is not well placed given the widespread understanding of telephony's inability to provide end-to-end authentication between callers. In this poster, we address this problem through the AuthentiCall system. AuthentiCall not only cryptographically authenticates both parties on the call, but also provides strong guarantees of the integrity of conversations made over traditional phone networks. We achieve these ends through the use of formally verified protocols that bind low-bitrate data channels to heterogeneous audio channels. Unlike previous efforts, we demonstrate that AuthentiCall can be used to provide strong authentication before calls are answered, allowing users to ignore calls claiming a particular Caller ID that are unable or unwilling to provide proof of that assertion. Moreover, we detect 99% of tampered call audio with negligible false positives and only a worst-case 1.4 second call establishment overhead. In so doing, we argue that strong and efficient end-to-end authentication for phone networks is approaching a practical reality.**

A. Introduction

Telephones remain of paramount importance to society since their invention 140 years ago, and they are especially important for sensitive business communications, whistleblowers and journalists, and as a reliable fallback when other communication systems fail. When faced with critical or anomalous events, the default response of many organizations and individuals is to rely on the telephone. For instance, banks receiving requests for large transfers between parties that do not generally interact call account owners. Power grid operators who detect phase synchronization problems requiring careful remediation speak on the phone with engineers in adjacent networks. Even the Federal Emergency Management Agency (FEMA) recommends that citizens in disaster areas rely on phones to communicate sensitive identity information (e.g., social security numbers) to assist in recovery [5]. In all of these cases, participants depend on telephony networks to help them validate claims of identity and integrity.

NDSS '17, 26 February – 1 March 2017, San Diego, CA, USA

However, these networks were never designed to provide end-to-end authentication or integrity guarantees. Adversaries with minimal technical ability regularly take advantage of this fact by spoofing Caller ID, a vulnerability enabling over $7 billion in fraud in 2015 [6]. More capable adversaries can exploit weaknesses in core network protocols such as SS7 to reroute calls and modify content [2]. Unlike the web, where mechanisms such as TLS protect data integrity and allow experts to reason about the identity of a website, the modern telephony infrastructure simply provides no means for anyone to reason about either of these properties.

B. Accomplishments To Date

In this poster, we present AuthentiCall, a system designed to provide end-to-end guarantees of authentication and call content integrity over modern phone systems (e.g., landline, cellular, or VoIP). While most phones have access to some form of data connection, that connection is often not robust or reliable enough to support secure VoIP phone calls. AuthentiCall uses this often low-bitrate data connection to mutually authenticate both parties of a phone call with strong cryptography *before* the call is answered. Even in the worst case, this authentication adds at most a negligible 1.4 seconds to call establishment. Once a call is established, AuthentiCall binds the call audio to the original authentication using specialized, low-bandwidth digests of the speech in the call. These digests protect the integrity of call content and can distinguish legitimate audio modifications attributable to the network from 99% of maliciously tampered call audio even while a typical user would expect to see a false positive only once every six years. Our system is the first to use these digests to ensure that received call audio originated from the legitimate source and has not been tampered with by an adversary. Most critically, AuthentiCall provides these guarantees for standard telephone calls without requiring changes to any core network.

We make the following contributions to date:

- **Designs Channel Binding and Authentication Protocols:** We design and implement protocols that bind identities to phone numbers, mutually authenticate both parties of a phone call, and protect call content in transit.
- **Evaluates Robust Speech Digests for Security:** We show that proposed constructions for digesting speech data in systems that degrade audio quality can be made effective in adversarial settings in real systems.
- **Evaluates Call Performance in Real Networks:** Our prototype implementation shows that the techniques

pioneered in AuthentiCall are practical and performant, adding at most only 1.4 seconds to phone call establishment in typical settings.

We are not the first to address this problem [4], [7], [1], [11], [10], [3], [8], [9]. However, other approaches have relied upon weak heuristics, fail to protect phone calls using the public telephone network, are not available to end users, neglect to protect call content, are trivially evaded, or add significant delay to call establishment. AuthentiCall is the only system that authenticates phone calls and content with strong cryptography in the global telephone network with negligible latency and overhead.

REFERENCES

[1] "RedPhone :: Private Calls - Android Apps on Google Play," https://play.google.com/store/apps/details?id=com.littlebytesofpi.linphonesip&hl=en.

[2] S. Alfonsi, "Hacking Your Phone," 60 Minutes - http://www.cbsnews.com/news/60-minutes-hacking-your-phone/, 2016.

[3] V. Balasubramaniyan, A. Poonawalla, M. Ahamad, M. Hunter, and P. Traynor, "PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2010.

[4] R. Bresciani, S. Superiore, S. Anna, and I. Pisa, "The ZRTP Protocol Security Considerations," Tech. Rep. LSV-07-20, 2007.

[5] Federal Emergency Management Agency, "Call Toll-Free Number For Disaster Assistance," https://www.fema.gov/news-release/2003/09/25/call-toll-free-number-disaster-assistance, 2003.

[6] M. Huffman, "Survey: 11% of adults lost money to a phone scam last year," Consumer Affairs - https://www.consumeraffairs.com/news/survey-11-of-adults-lost-money-to-a-phone-scam-last-year-012616.html, 2016.

[7] T. H. A. C. Liath and R. Bresciani, "The ZRTP Protocol Analysis on the Diffie-Hellman Mode," *Foundations and Methods Research Group*, 2009.

[8] H. Mustafa, W. Xu, A. R. Sadeghi, and S. Schulz, "You Can Call but You Can't Hide: Detecting Caller ID Spoofing Attacks," in *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2014, pp. 168–179.

[9] B. Reaves, L. Blue, and P. Traynor, "AuthLoop: End-to-End Cryptographic Authentication for Telephony over Voice Channels," *25th USENIX Security Symposium (USENIX Security 16)*, pp. 963–978, Aug. 2016.

[10] P. Zimmermann, A. Johnston, and J. Callas, "RFC 6189 ZRTP: Media Path Key Agreement for Unicast Secure RTP," *Internet Engineering Task Force*, 2011.

[11] P. R. Zimmermann, "The Zfone™ Project," Zfone Project Home Page -http://zfoneproject.com/, 2016.

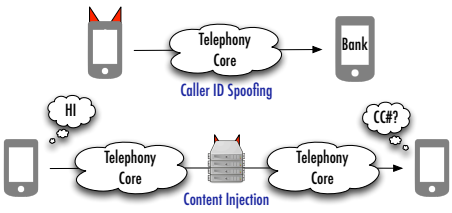
AuthentiCall: Efficient Identity and Content Authentication for Phone Calls

Bradley Reaves, Logan Blue, Hadi Abdullah, Luis Vargas, Patrick Traynor, Thomas Shrimpton
University of Florida

Takeaway: AuthentiCall provides end-to-end authentication of identity and call content for modern phone calls

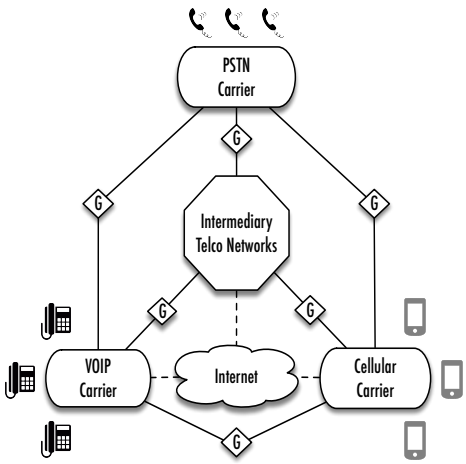
Possible Attacks

Sophisticated and unsophisticated adversaries can spoof Caller ID and even intercept and modify call audio



The inability to know the true source of calls facilitates prank calls, robocalls, scams, "swatting" attacks, and other problems in the phone network.

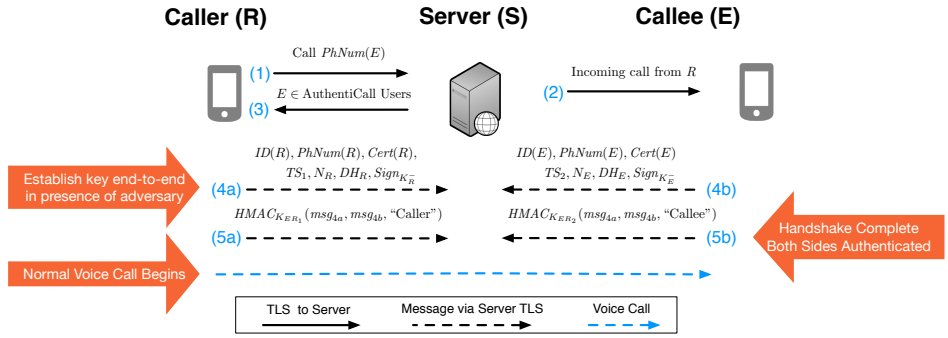
Why Phone Networks Have Poor Authentication



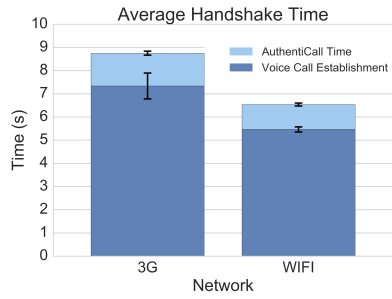
In the modern phone network, calls are routed through gateways at network boundaries that remove authentication information and modify call audio.

Authentication Handshake

AuthentiCall uses an auxiliary data connection (e.g., LTE, WIFi) to authenticate calls end-to-end over the existing phone network

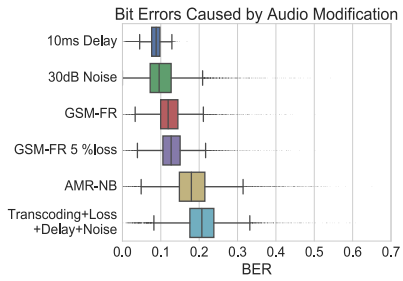


Handshake Performance



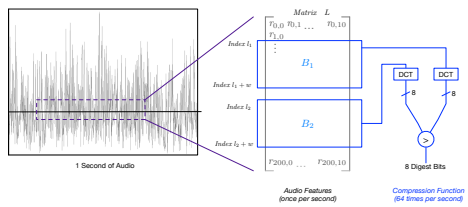
AuthentiCall adds only 1 to 1.41 seconds to call establishment

Content Authentication Performance

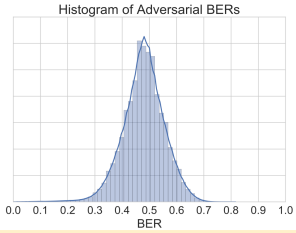


Legitimate audio modifications change 10-20% of digest bits, while content substitution changes 48% of bits on average

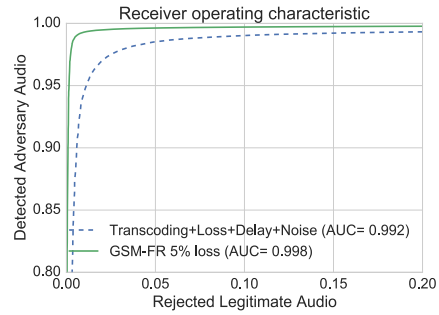
Content Digests



Call content naturally changes as it is transcoded in the network, and cryptographic hashes over call audio cannot distinguish legitimate changes from attacks. Instead, we use the RSH algorithm* to digest call content at a low bitrate to distinguish legitimate changes from attacks. Changes can be measured with bit error between digests



AuthentiCall can detect 99% of tampered audio frames with a false positive roughly *once every 6 years*



For further information, contact Brad Reaves (*reaves@ufl.edu*).

* Y. Jiao, L. Ji, and X. Niu, "Robust Speech Hashing for Content Authentication," IEEE Signal Processing Letters, vol. 16, no. 9, pp. 818–821, Sep. 2009.