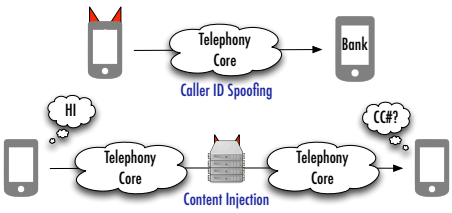
AuthentiCall: Efficient Identity and Content Authentication for Phone Calls

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

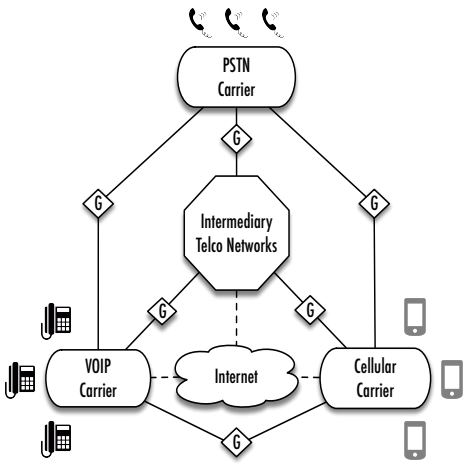
Possible Attacks

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.

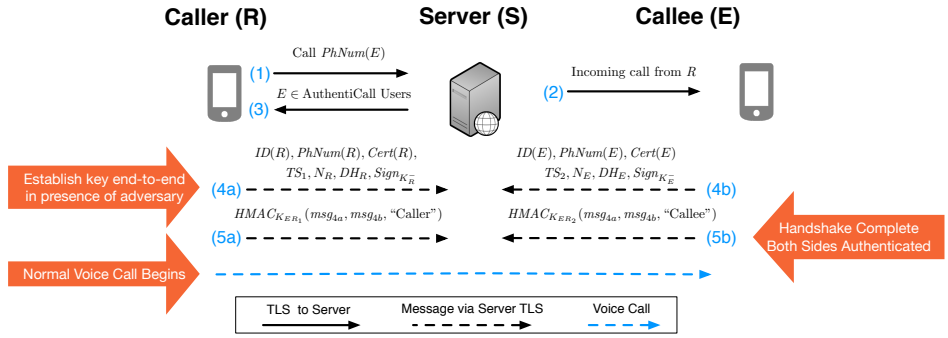
Why Phone Networks Have Poor Authentication



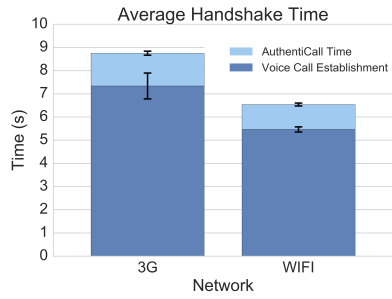
In the modern phone network, calls are routed through gateways at network boundaries that remove authentication information and modify call audio.

Authentication Handshake

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

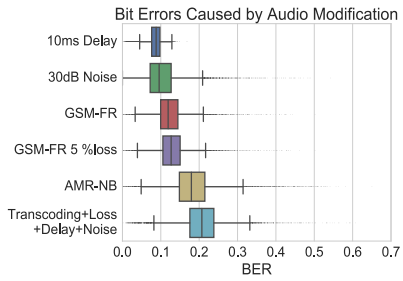


Handshake Performance



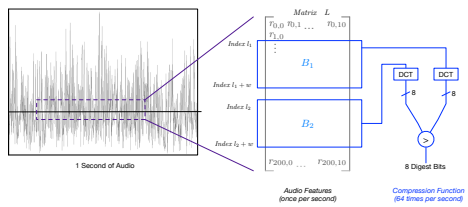
AuthentiCall adds only 1 to 1.41 seconds to call establishment

Content Authentication Performance

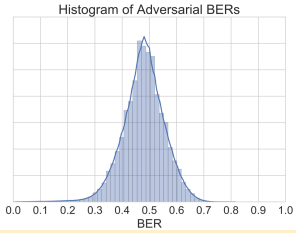


Legitimate audio modifications change 10-20% of digest bits, while content substitution changes 48% of bits on average

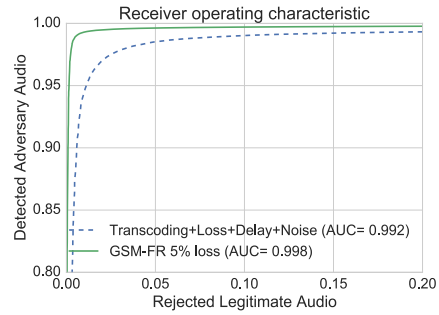
Content Digests



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.