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 Authentication Handshake provides end-to-end AuthentiCall uses an auxiliary data connection (e.g., LTE, WIFi) to authentication of identity authenticate calls end-to-end over the existing phone network and call content for modern Server (S) Caller (R) Callee (E) phone calls Call PhNum(E)Incoming call from ${\cal R}$ $E \in AuthentiCall User$ (2)**Possible Attacks** ID(R), PhNum(R), Cert(R),ID(E), PhNum(E), Cert(E) $TS_1, N_R, DH_R, Sign_{K_R^-}$ $TS_2, N_E, DH_E, Sign_{K_E^-}$ (4a) - -- (4b) Sophisticated and unsophisticated $HMAC_{K_{EB_1}}(msg_{4a}, msg_{4b}, "Caller")$ $HMAC_{KEB_{2}}(msg_{4a}, msg_{4b}, "Callee")$ ---- (5b) adversaries can spoof Caller ID and even intercept and modify call audio Message via Server TLS TLS to Server Voice Cal Telenhon **Content Authentication** Handshake Core ID Snor Performance Performance Average Handshake Time Telenhony Bit Errors Caused by Audio Modification Telenhony 10 Core Core 10ms Delay 9 AuthentiCall Time ontent Injectio 8 Voice Call Establishment 30dB Noise 7 6 (s) GSM-ER Lime 5 GSM-FR 5 %loss The inability to know the true source of 4 3 AMR-NB calls facilitates prank calls, robocalls, 2 scams, "swatting" attacks, and other Transcoding+Loss 1 +Delay+No problems in the phone network. 0 0.1 0.4 0.5 0.6 0.7 0.0 0.2 0.3 3G WIFI RER Network Legitimate audio modifications change Why Phone Networks Have 10-20% of digest bits, while content AuthentiCall adds only 1 to 1.41 seconds to call establishment substitution changes 48% of bits on Poor Authentication average Histogram of Adversarial BERs ははは **Content Digests** PSTN Carrie 70,1 **(6)** DCT DCT 0.0 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1.0 BER Intermediary AuthentiCall can detect 99% of Telco Networks tampered audio frames with a false Audio Features positive roughly once every 6 years Call content naturally changes as it is Receiver operating characteristic 1.00 VOI Cellular transcoded in the network, and Internet Carrie Carrier 9.95 Audio cryptographic hashes over call audio cannot distinguish legitimate changes

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

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

* 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.

