Introducing a Verified Authenticated Key Exchange Protocol over Voice Channels for Secure Voice Communications

Piotr Krasnowski, J. Lebrun, B. Martin

Introducing a Verified Authenticated Key Exchange Protocol over Voice Channels for Secure Voice Communications

P. Krasnowski, J. Lebrun, B. Martin

krasnowski@i3s.unice.fr
Université Côte d'Azur • I3S-CNRS • BlackBoxSecu

The Crypto Box

Figure: The Crypto Box visualization

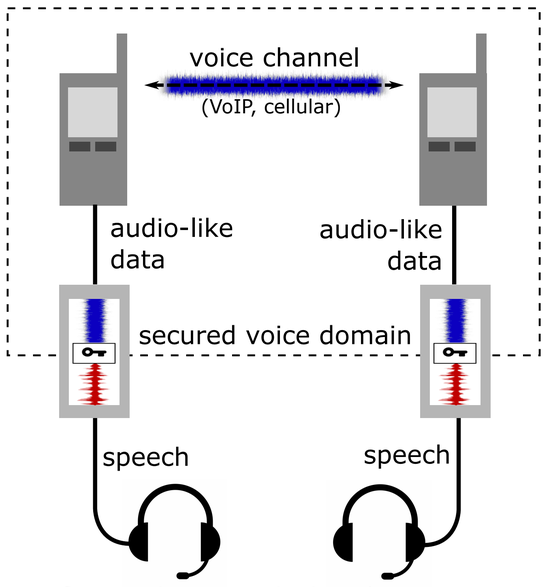


Figure: Secure voice communication scheme

The Crypto Box provides real-time secure voice communications over 2G-4G networks and VoIP (Skype, WhatsApp, Signal...).

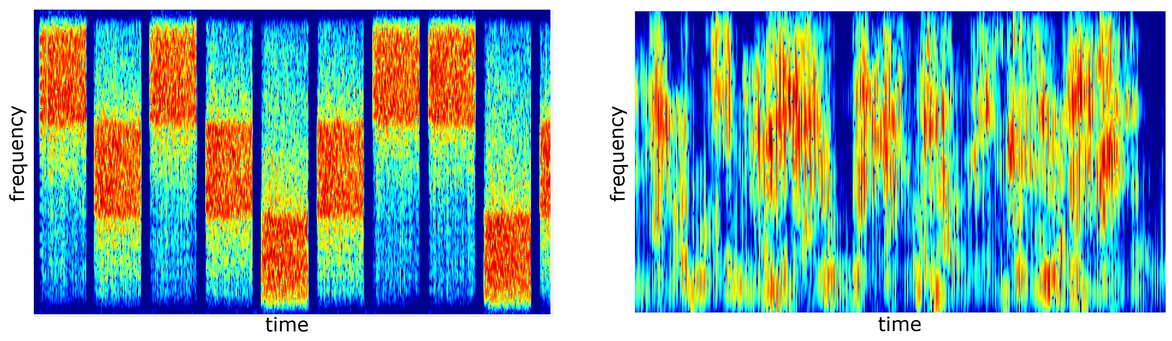
Recorded speech is encrypted into audio signal, adapted to transmission over voice channels in a presence of Voice Activity Detection.

Received signal can be decoded and decrypted only by a paired Crypto Box sharing the cryptographic key.

The Session Key is freshly generated for each secure call, requiring a dedicated authenticated KE protocol.

Sending data over voice channel

Voice compression, filtering and quantization introduced by digital voice channels significantly distort the signal. Data over Voice (DoV) technique encodes binary data into a waveform with voice-like properties. The DoV signal is robust against blockage by voice detection algorithms and withstands voice compression by popular voice coders like AMR or Silk.



Figures: Spectrum of two different DoV techniques.

Protocol design challenges

- low bandwidth (~ 2kbps)
- long round-trip time (~ 2s)
- signal distortion (~ 5-10% BER)
- no Public Key Infrastructure
- flexible authentication (no shared secret by default)

Short Authentication String (SAS)

Short string of digits or words displayed on two Crypto Boxes after each key exchange. SAS is cooperatively compared vocally by speakers in order to verify the equality of strings.

- Speaker's voice recognition
- Session Key validation
- detecting a MITM adversary

Figure: The Crypto Box in *encryption mode*.

ECDHE Authenticated Key Exchange

Unsecured call initiation

Alice $\longleftrightarrow$ vocal agreement on protocol initialization $\longleftrightarrow$ **Bob**

Setup

$1: N_A \leftarrow_s \mathbb{Z}^*_{32}$ $\longleftrightarrow$ A/B role negotiation $\longleftrightarrow$ $N_B \leftarrow_s \mathbb{Z}^*_{32}$

$2: d_A \leftarrow_s \mathbb{Z}^*_{256}$ $\qquad$ $d_B \leftarrow_s \mathbb{Z}^*_{256}$

$3: Q_A = d_A G$ $\qquad$ $Q_B = d_B G$

$4: R_A \leftarrow_s \mathbb{Z}^*_{128}$ $\qquad$ $R_B \leftarrow_s \mathbb{Z}^*_{32}$

Key exchange and authentication

$5:$ $\xrightarrow[h_{128}(ID_A \| N_A \| Q_A \| R_A)]{ID_A,\ N_A,\ Q_A}$

$6:$ $\xleftarrow[Sign_{S_B}(\text{'B'} \| ID_A \| N_A \| Q_A \| ID_B \| N_B \| Q_B)]{ID_B,\ N_B,\ Q_B,\ R_B}$

$7: Z = d_A Q_B$ $\xrightarrow[Sign_{S_A}(\text{'A'} \| ID_B \| N_B \| Q_B \| ID_A \| N_A \| Q_A)]{R_A}$ $Z = d_B Q_A$

$8: K_S = h_{256}(Z \| \bullet)$ $\qquad$ $K_S = h_{256}(Z \| \bullet)$

Acknowledgment

$9:$ $\longleftarrow$ ACK

SAS comparison over Encrypted Channel

$10: SAS = h_{32}(\blacklozenge)$ $\longleftrightarrow$ SAS vocal comparison $\longleftrightarrow$ $SAS = h_{32}(\blacklozenge)$

$\bullet \equiv ID_A \| N_A \| ID_B \| N_B$ $\qquad$ $\blacklozenge \equiv R_A \| R_B \| ID_B \| Q_B \| N_B$

Formal Verification with Tamarin Prover

Authentication scenario:	mutual signature	unilateral signature	vocal verification	nothing
Session Key secrecy	✓	✓	✓	✗
forward secrecy	✓	✓	✓	✗
injective agreement	✓	✓	✓	✗
reflection attack	✓	✓	✗	✗
key compromise impersonation	✓	✓	-	-

Conclusions

The proposed ECDHE key exchange protocol is highly adapted to the constraints of real-world voice-channels and is based on well-established and easily implementable primitives.

The security of the protocol relies on a scrupulous and cooperative authentication of speakers. Careless signature distribution or vocal verification are the biggest security threats.

New advances in artificial speech synthesis pose risk to security of vocal verification. Level of authentication can be improved by introducing contextual questions.

Acknowledgement:
This work is supported by grant DGA Cifre-Defense program No 01D17022178 DGA/DS/MRIS.