DTLS-SRTP における共有鍵交換の課題

高原　尚志[†]　　中村　素典[††]

[†]新潟県立大学　　[††]国立情報学研究所

安全な VoIP 通信を実現する方式として DTLS-SRTP が提案されている。DTLS-SRTP は、SIP シグナリングで端末同士の通信路を確立した直後に、SRTP で用いる共有鍵を TLS のハンドシェイクプロトコルを用いて交換する。この際、TLS で用いる公開鍵の真正性を、先だって行われる SIP シグナリングにおいてプロキシが保証する方式が、DTLS-SRTP-Framework として併せて提案されている。ここで、SIP プロキシの信頼性が崩れ、SIP プロキシが通信に介入する可能性があるとするならば、安全な通信は期待できない。そこで発表では、SIP プロキシが信頼できない場合の課題を明らかにし、その解決に向けて、知見者の意見を広く求める。

Problems on Shared Secret Exchange of DTLS-SRTP over unreliable proxies

Hisashi TAKAHARA[†]　　Motonori NAKAMURA[††]

[†]University of NIIGATA PREFECTURE　[††]National Institute of Informatics

The DTLS-SRTP was proposed for secure VoIP communication. In the DTLS-SRTP, after establishing an end-to-end communication channel with signaling, they exchange a shared key for SRTP using handshake of TLS. A method to protect public keys for the TLS is also proposed as DTLS-SRTP-Framework that SIP Proxy assures integrity of the public keys provided by the end entities. If reliability of a proxy is lost and MITM attack is made by the proxy, secure communication channel cannot be established. This presentation tries to make clear problems in such cases and opinions for the solution from participants are widely expected.

1. まえがき

現在、VoIP のメディア通信を安全に行う方式として、共有鍵暗号化通信である SRTP[2]が広く知られ、この共有鍵を安全に交換方式する方式として、DTLS-SRTP[8]が提案され、標準化されている。この際、メディア通信に先だって行われるシグナリング通信において、共有鍵交換の際に用いる公開鍵証明書の真正性を保証する方式 DTLS-SRTP-Framework[7]も併せて提案されている。この方式では、シグナリング通信として、広く知られている SIP[1]を用い、通信の真正性及び完全性を保証するための仕組みである SIP Identity[4]で公開鍵証明書の真正性及び完全性を送信側の SIP プロキシが保証する。そのため、SIP プロキシは正しく動作することが前提となるが、この前提が崩れてプロキシが通信への介入を行う可能性があれば通信の安全性が損なわれる。本発表では、途中のプロキシが通信に介入する場合の課題を整理し、既存の方式で解決済みのものと、解決されていないものを明らかにした上で、その解決に向けて議論する。

2. 既存の方式と課題

2.1 前提条件

本論文で扱う通信では、次の前提条件を置く。

(1) SIP 通信においては、送信側／受信側、それぞれプロキシを介した通信を行うものとする
(2) 送信側／受信側の各端末は PKI を用いない
(3) 送信側／受信側の SIP プロキシは PKI を用いる

2.2 DTLS-SRTP

DTLS-SRTP は、SIP シグナリングによって、端末同士のダイレクト通信路（メディア通信路）を確立した直後に、端末同士で end-to-end の DTLS[3]共有鍵暗号通信路を確立する。この際、DTLS で用いるために交換された共有鍵を SRTP で用いて通信を行う方式である。

DTLS では、通信路を確立するために、まず初めにハンドシェイクプロトコルを実行し、互いの真正性を保証するための証明書を交換するが、両端の端末が PKI を採用していない場合、この証明書の真正性は保証されない。そのため、DTLS に先だって行われる SIP シグナリング通信において、fingerprint を交換し、プロキシが保証することによって、証明書の真正性を保証する仕組み[7]も併せて提案されている。

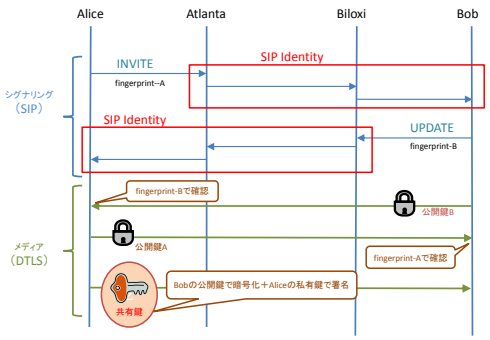

図 2　DTLS-SRTP 及び DTLS-SRTP-Framework

この場合、証明書を保証するプロキシ（送信側）が正しく動作する必要がある。もし、通信路に送信側プロキシが介入する場合、これを防ぐことはできない。

レスポンス方向（受信端末→送信端末）の第三者の介入を防ぐ方式として、UPDATE をレスポンス方向に送信し、これを受信側プロキシが SIP Identity で保証する方式[5]が提案されているが、この方式を用いれば、送信側プロキシの介入を防ぐことができる。

これにより、送信側・受信側プロキシの単独での介入や両方のプロキシが独立に介入することを防ぐことができる。

2.3 現在の課題

2.2 の方式を用いても、送信側・受信側、双方のプロキシが結託した場合には、送信側及び受信側が送信した公開鍵の改ざんを許すこととなり、介入を防ぐことができず、これが現在の課題となっている。

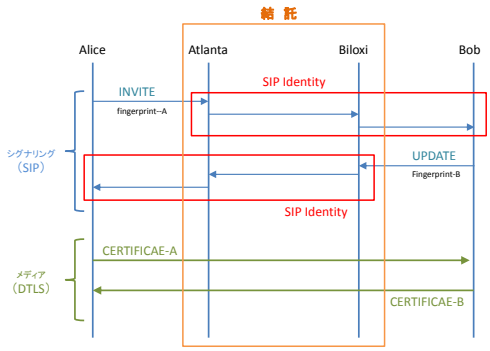

図 5　結託したプロキシによる介入

3．むすび

本論文では、VoIP 通信を安全に行うために提案された方式 DTLS-SRTP について述べ、解決された課題と現在解決されない課題について整理した。このようにすることによって、解決へ向けてのヒントを得ようと考えた。

文　献

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. SIP: Session Initiation Protocol. IETF, June 2002. RFC3261.

[2] M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman. The Secure Real-time Transport Protocol (SRTP). IETF, March 2004. RFC3711.

[3] E. Rescorla, N. Modadugu. Datagram Transport Layer Security. IETF, April 2006. RFC4347.

[4] J. Peterson, NeuStar, C. Jennings. Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP). IETF, August 2006. RFC4474.

[5] J. Elwell. Connected Identity in the Session Initiation Protocol (SIP). IETF, June 2007. RFC4916.

[6] T. Dierks, E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. IETF, August 2008. RFC5246.

[7] J. Fischl, H. Tschofenig, E. Rescorla. Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS). IETF, May 2010. RFC5763.

[8] D. McGrew, E. Rescorla. Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP). IETF, May 2010. RFC5764.

謝　辞

本研究は JSPS 科研費 23500096 の助成を受けたものです。