情報通信研究機構

NICT 先端研究 (199)

エンドツーエンド暗号化 ビデオ会議 安全運用

ビデオ会議システムのZoomやWebexなどで幅広く導入されているエンドツーエンド暗号化技術。TLS通信のようなサーバー・クライアント暗号化通信とは異なり、通信相手との間でのみメッセージの送受信が可能であり、サービスプロバイダーであってもメッセージの盗聴、改ざんができない暗号化通信技術である。

新型コロナウイルス感染症の世界的流行を受け、テレワークやオンライン教育の場でビデオ会議システムの利用が拡大していることを踏まえると、安心・安全なテレワーク時代のセキュリティー確保に欠かせない技術である。

情報通信研究機構（NICT）では、兵庫県立大学やNECと共同で、Zoomに導入されているエンドツーエンド暗号化技術やGoogle Duo、Cisco Webex、Jitsi Meetなどで導入予定のエンドツーエンド暗号化技術SFrameの安全性評価に関する研究開発を実施している。

Zoomの安全性評価では、他人へのなりすまし、メッセージの改ざん、サービス利用の拒否に繋がる6個の脆弱性を発見し、これらの脆弱性を利用した8種類の攻撃手法を提示するとともに、これらの攻撃に対する防御対策について提案した。特に、Zoomの安全性評価チームが想定するよりも強力な攻撃として、我々が提示する条件を満たす場合に任意のユーザーになりすますことができることを指摘した。

SFrameの安全性評価では、他人へのなりすましに繋がる3個の脆弱性を発見し、これらの脆弱性を利用した3種類の攻撃手法を提示するとともに、これらの攻撃に対する防御対策について提案した。特に、SFrameがメッセージの真正性を保証するために電子署名方式を採用しているにもかかわらず、会議に参加している別のユーザーになりすますことができることを指摘した。

Zoomの安全性評価チームとSFrameの設計者に対して速やかに脆弱性報告を実施したところ、ZoomとSFrameの仕様が速やかに修正されていることを確認した。

我々の安全性評価は、なりすまし、改ざん、サービス利用拒否などの攻撃手法に対して耐性のあるシステムを設計する場面で効果を発揮し、テレワークなどで利用するビデオ会議システムの安心・安全な運用に貢献できるものとして期待されている。

（火曜日に掲載）

サイバーセキュリティ研究所・セキュリティ基盤研究室 主任研究員
伊藤 竜馬

19年阪大院博士後期課程修了、20年4月NICT入所。共通鍵暗号の安全性評価に関する研究開発に従事。博士（工学）。