資料配布				
月/日 (曜日)	担当課	電話	発表者	その他 配布先
8 / 30(木) 14 時	兵庫県立大学 神戸情報科学キャンパス 経営部 総務学務課	(078) 303-1901	応用情報科学研究科長 西村 治彦 (総務学務課長 酒井康裕)	県政記者 クラブ

LINE®の暗号化機能「Letter Sealing」の安全性解析

-エンドツーエンド暗号化プロトコルに複数の問題点を発見-

兵庫県立大学大学院 応用情報科学研究科の五十部 孝典 准教授は，メッセージアプリケーション LINE®のエンドツーエンド暗号化「Letter Sealing」に複数の問題点があることを突き止めました．エンドツーエンド暗号化はサービス提供者の不正があった場合でもユーザのプライバシを保護する技術であり，本研究では「Letter Sealing」がエンドツーエンド暗号化として理想的な安全性を有していないことを示しました.

LINE®は日本およびアジア各国にて広く使われているメッセージアプリケーションです．東アジアでは支払いや購買などのサービスへも発展を続けており，特に日本ではマイナポータルと連携するなど，メッセージアプリケーションの枠を超え， コミュニケーションプラットフォームとなっております. LINE®のエンドツーエンド暗号化機能「Letter Sealing」は，メッセージサービスにおいて，ユーザのメッセージを暗号化することでユーザのプライバシを守り，安全な通信を行うために用いられています.

今回，五十部准教授は，LINE 社が公開している「Letter Sealing」の暗号プロトコルの仕様に対して，暗号学的観点から解析を行い，複数のアルゴリズムレベルの問題点を見つけました．これらの問題点により，LINE 社が不正を行った場合などの特定の条件のもと他のユーザへのなりすましや，メッセージの改ざん攻撃が可能になります．本研究は，「Letter Sealing」に対しての初めての第三者による包括的な評価であり，エンドツーエンド暗号化機能として理想的な安全性を有していないことを示しています．また，今回発見した問題点に対する対策方式も考案しており，問題点とともに LINE®社には報告済みです.
情報セキュリティ，特に暗号技術では，第三者による安全性評価が極めて重要です．本研究で得られた評価結果および発見された問題点を暗号プロトコル設計者にフィードバックすることにより，より高い安全性を有する暗号化機能の設計に寄与すると期待されます.
本研究の初期成果は，2018 年 1 月に開催された国内会議 SCIS2018 で発表済みであり，発表論文のなかで特に優れた論文に送られるイノベーション論文賞（注 1）を受賞しております．また，対策方法も含めた成果を，スペイン，バルセロナにて 2018 年 9 月 3 日から 5 日（太平洋標準時）に開催される国際会議 ESORICS 2018（注 2）にて発表します.

（注 1） SCIS 2018 イノベーション論文・SCIS 論文賞について
https://www.ieice.org/~isec/award-SCIS.html
（注 2）European Symposium on Research in Computer Security (ESORICS) 2018
https://esorics2018.upc.edu/

LINE®の暗号化機能「Letter Sealing」の安全性解析

――エンドツーエンド暗号プロトコルに複数の問題点を発見――

【概要】

- LINE®の暗号化機能「Letter Sealing」に対し安全性評価を行い，暗号プロトコルに複数の問題点を発見しました．
- 今回見つけた問題点に対しての対策方式を考案しました．

【背景】

エンドツーエンド暗号化（End-to-End Encryption, E2EE）とは，通信する 2 者間でのみメッセージの送受信が可能であり，通信システムやサービスの提供者であってもメッセージの盗聴，改ざんができない暗号通信方式です．2013 年の元 NSA 職員のスノーデン氏の暴露事件により，国家規模の監視，盗聴に対して E2EE の必要性が注目されるようになりました．実際，WhatsApp™, Facebook Messenger™, Skype™, LINE®, Viber™ 等の主要なメッセージアプリケーションでは，サービス提供者の不正があった場合でもユーザのプライバシを守り，安全な通信を実現するために，E2EE が用いられています．

LINE®は，日本およびアジア各国にて広く使われているメッセージアプリケーションで，日本国内，台湾，タイ，インドネシアでのアクティブユーザ数は約 1.7 億（2017 年 12 月時点）です．東アジアを中心に支払いや購買などのサービスへも発展を続けており，特に日本ではマイナポータルと連携も発表されるなど，メッセージアプリケーションの枠を超え， コミュニケーションプラットフォームとなっております．LINE® が 2015 年に開発した E2EE は「Letter Sealing」と呼ばれており， 2016 年にはデフォルトで利用されるようになり，サービス提供者の不正があったとしても，ユーザのプライバシを保護しております．「Letter Sealing」のプロトコル仕様は 2016 年に LINE 社が発行したホワイトペーパーにより公開されております．しかしながら，E2EE の安全性については， 第三者による包括的な評価はありませんでした．

【研究成果】

五十部准教授は，LINE® の E2EE「Letter Sealing」で用いられている暗号プロトコルの安全性評価を行い，3 つのアルゴリズムレベルの問題点を明らかにしました．一つ目は，グループ間メッセージングの方式の問題点であり，悪意のあるグループメンバによる他のメンバへのなりすましや他のメンバのメッセージの改ざんが可能であることを示しました．二つ目は，1 対 1 メッセージングの暗号鍵交換の方式に問題があり，悪意のユーザによるなりすましやメッセージの改ざんが特定の仮定の元で可能であることを示しました．3 つ目はメッセージの暗号化や改ざん検知を行っている暗号方式自体に問題があり，国家レベルの

高い計算能力を有している攻撃者に対しては十分な安全性を有していないことを明らかにしました．前述の通り，E2EE は国家規模の監視に対しても安全である必要があるため，E2EE の暗号方式として問題があることを示しています．

本研究で発見した問題点に関しては，2017 年 11 月に LINE 社への情報開示を事前に行っております．LINE 社からは，ホワイトペーパーに未記載のサーバ側の運用により，LINE 社自体が積極的に不正に関わらない限りは，一般ユーザからの攻撃は対策できると回答を得ました．しかしながらサービス運用者の不正を防ぐのが E2EE の主要な目的であり，サービス運用者が信頼できない場合，すべての攻撃は成立するため，「Letter Sealing」が E2EE としての理想的な安全性を有していないことを示しています．ただし，今回の結果は，サーバ側の不正があった場合にメッセージのなりすましや改ざんが可能であることを示すものであり，サーバ側の不正があった場合でも平文の情報は洩れません．

これらの問題点は，2017 年 12 月に，LINE 社が運営する Bug Bounty Program によって Encryption Break の問題点として正式に LINE 社より認定されました．また今回発見した問題点に対する対策案も開発し，LINE 社に提示いたしました．

【結果の意義・今後の展望】

LINE®を用いたサービスにおいて，安全な通信を実現する E2EE 技術「Letter Sealing」は，ユーザのプライバシを守るために非常に重要です．本研究では，その「Letter Sealing」に対して包括的な安全評価を与え，E2EE として安全性上に問題があることを初めて明らかにしたものです．本研究で得られた評価結果，並びに対策技術を設計にフィードバックすることによって，より高い安全性を有する暗号化方式を設計することへ繋がります．

【発表詳細】

国際会議: ESORICS 2018 (エゾリクス 2018，https://esorics2018.upc.edu/)

論文タイトル: "Breaking the Message Integrity of an End-to-End Encryption Scheme of LINE

著者: 五十部　孝典（兵庫県立大学大学院），峯松　一彦（ＮＥＣ）

【本件に関する一般の方からのお問い合わせ先】

兵庫県立大学大学院　応用情報科学研究科　准教授　五十部 孝典（いそべたかのり）

E-Mail: takanori.isobe@ai.u-hyogo.ac.jp