様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　２５　日現在

機関番号：　８２６３６
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００１９６

研究課題名（和文）ネットワークに連動したセキュリティレベルによる暗号プロトコル安全性評価技術の開発

研究課題名（英文）Network-Dependent Security Evaluation for Cryptographic Protocols

研究代表者
吉田　真紀（Maki, Yoshida）

国立研究開発法人情報通信研究機構・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

研究者番号：５０３３５３８７

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：インターネットで安全に通信するための手順(暗号プロトコル) に欠陥が無いこと，すなわち安全であることの確認が喫緊の課題となっている．本研究の目的は，今後の進展が見込まれるモノのインターネット(Internet of Things: IoT) において，End-to-End のネットワークに連動したセキュリティレベルで安全性を評価する技術の開発である．そのために，SSL/TLS，QUIC，秘密計算などの実用的にも学術的にも重要な暗号プロトコルを対象とした安全性評価を研究し，従来のセキュリティの定式化の問題点を指摘，さらにはセキュリティと効率の改善方法を提案した．

研究成果の概要（英文）：An important issue of cryptographic protocols is to evaluate the security. The purpose of this work is to evaluate the security in IoT environments according to the End-to-End network between users and devices. We study the security evaluation of well-known and important protocols such as SSL/TLS, QUIC, and multi-party computation, find a flow of the previous security model of QUIC, and present some improvements on both security and efficiency.

研究分野：　情報セキュリティ

キーワード：　暗号プロトコル　安全性評価　IoT　セキュアネットワーク

１．研究開始当初の背景

インターネットに広く普及した暗号プロトコルの仕様上の欠陥が深刻な問題となっている．2014年10月14日(日本時間15日)，SSLv3 (Secure Socket Layer version 3.0)に，POODLE と呼ばれる致命的な脆弱性が発見された．本脆弱性は，約 15 年見逃されており，その間に SSLv3 の普及が進み，後継プロトコル TLS (Transport Layer Security) が規格化された現在でも，SSLv3 しかサポートしていないインターネット機器やフィーチャーフォンが数多くあり，本脆弱性の影響は大きい．今後の進展が見込まれている IoT では，PC や携帯端末だけでなく，数兆個の多種多様なモノが暗号プロトコルを用いて通信することになる．もし暗号プロトコルの欠陥が見逃されたまま普及すれば，将来の情報化社会が崩壊しかねない．よって，IoT でユーザと多種多様なモノ(すなわちサービス) を結ぶ暗号プロトコルの組み合わせに 欠陥が無いことの確認，すなわち安全性を評価する技術の開発が喫緊の課題となっている．

２．研究の目的

本研究の目的は，今後の進展が見込まれるモノのインターネット(Internet of Things: IoT) において，End-to-End のネットワークに連動したセキュリティレベルで，ユーザとモノを結ぶ暗号プロトコルに対して安全性を評価する技術の開発である．そのために，セキュリティレベルを定式化し，安全性評価の枠組みと評価を自動化する手法を提案することを目的とする．

３．研究の方法

暗号プロトコルの安全性評価技術の確立に向け，以下の手順で研究を遂行した．

- ネットワークに連動したセキュリティレベルの定式化：ネットワークによって求められるセキュリティレベルが異なることは，ユーザとモノが接続されているネットワークによって，攻撃の容易さが異なるためである．よって，攻撃の容易さを元にセキュリティレベルを多段階で定式化する．なお，ネットワークの型としては一対一と一対多(スター型，放送型) の両方を対象とした．
- 安全性評価の枠組みの提案：完全な安全性評価は計算不能であることが証明されているため，半判定の枠組みを構築する．すなわち，安全であることの検証の枠組みと，脆弱であることの検証の枠組みである．暗号プロトコルやそのセキュリティレベルによって，求められる安全性評価の内容が異なるため，必要に応じて枠組みを適切に選択できるようにする．
- 安全性検証法の設計：安全性検証の自動化のため，セキュリティレベルに対応する安全性を形式化して表現する記号的モデルを定義し，その安全性を検証する手法を提案した．さらに，脆弱性検証の自動化のため，脆弱であるための十分条件を導出し，条件判定式を提案した．
- 提案法の主要部分の試作と適用実験による有効性確認：学術と産業の両方の暗号プロトコルを対象にすることで，理論と実用の両面で有用な知見を得ると共に，提案法が実用レベルに達していることを示す．
- 研究成果のまとめと公表：得られた成果は暗号プロトコルの評価結果や試作結果を含めて広く公表し，再試できるようにする．

４．研究成果

本研究における主要な研究成果を以下に示す．本研究においては，インターネットにおいて実際に使用されている代表的な暗号プロトコル SSL/TLS と QUIC，将来の IoT のネットワークにおいて重要な役割を果たす暗号プロトコルを対象とした．

（１）SSL/TLS と QUIC の安全性評価

まず，SSL/TLS で使用されている最新の TLS1.2 について以下の成果を得た．

【研究の主な成果】

- ネットワークに連動したセキュリティレベルの定式化：Logjam 攻撃はセキュリティレベルが低い暗号を使わせる（ダウングレードさせる）中間者攻撃である．本攻撃を扱うため，暗号のセキュリティレベルを階層化した定式化を示した．
- 安全性評価の枠組みの提案：Logjam 攻撃への安全性を評価可能とするため，攻撃者によるダウングレードと，セキュリティレベルが低い暗号の解読を可能とする枠組みを構築した．
- 安全性検証法の設計：Logjam 攻撃への安全性検証法として，代表的な検証ツールである ProVerif を用いた手法を確立した．
- 提案法の主要部分の試作と適用実験による有効性確認：当該手法を用いることで SSL/TLS の最新バージョンである TLS1.2 で脆弱性の抽出に成功すると共に，Logjam 攻撃に対して安全となる改良案を提示した．

【国内外における位置付けとインパクト】

本成果は，最新の攻撃を初めて検証可能にしたという点で意義も大きい．

【今後の展望】

暗号プロトコル開発者にとって，既知の様々な攻撃を検証の手間が減ることは，安全性向上に注力する時間ができるという点で望ましい．今後も引き続き新たな攻撃を検証可能とすることが考えられる．

次に，SSL/TLS の最新バージョンとして規格化が進んでいた TLS1.3，および，Google が

開発しブラウザ Chrome で使われている暗号プロトコル QUIC に対して以下の成果を得た.

【研究の主な成果】

- ネットワークに連動したセキュリティレベルの定式化： 調査の結果, TLS1.3 と QUIC のためのセキュリティとして, QACCE モデルと呼ばれる定式化が, IEEE のセキュリティにおける旗艦会議である 36th IEEE Symposium on Security and Privacy (S&P 2015)で示されており, 本研究ではそれに従った. なお, 本定式化は暗号理論に基づいており, 安全性評価の自動化を可能とする定式化は未解決問題として残されていた.
- 安全性評価の枠組みの提案：TLS1.3 と QUIC の安全性を検証可能とするため(すなわち評価の自動化を可能とするため), 形式理論に基づく安全性評価の枠組みを構築した. その際, S&P2015 の定式化に数多くの typo があったため, その修正も示した.
- 安全性検証法の設計：本研究課題に取り組んでいた時点において, TLS1.3 が標準化の途中であったのに対し, QUIC はデスクトップブラウザの世界シェアの 6 割を占める Google Chrome で実際に使用されていた. よって, QUIC を対象にし, 代表的な検証ツールである ProVerif を用いた手法を確立した.
- 提案法の主要部分の試作と適用実験による有効性確認：検証の結果, QUIC に対する新たな攻撃を発見した. さらに, 攻撃を解析し, 従来の安全性証明(S&P 2015 で発表されていた) の誤りを指摘し, さらには原因の解明と安全性修正案を提示した.

【国内外における位置付けとインパクト】

本成果は, 発表前の段階において標準化団体 IETF の QUIC WG のメーリングリストで紹介されるなど注目されていた. さらに, 国際会議で発表した際には, 標準化に貢献しているコミュニティから多数の質問を受けるなど, 大きなインパクトを与えた成果である.

【今後の展望】

2018 年 3 月に TLS 1.3 のドラフト 28 が正式な規格として承認された. 今後は, TLS1.3 の安全性検証が挙げられる.

（2）IoT 向けプロトコルの安全性評価

将来の IoT のネットワークにおいて重要な役割を果たす暗号プロトコルとして, IoT デバイスが取得した位置情報や稼働状況を安全に集約する秘密計算プロトコルを対象として以下の成果を得た.

【研究の主な成果】

- ネットワークに連動したセキュリティレベルの定式化：情報を集約するサーバよりも IoT デバイスへの攻撃が容易なため, 2 段階のセキュリティレベルを定式化した.
- 安全性評価の枠組みの提案：多様な IoT デバイスとサーバ間の暗号プロトコルの脆弱を検証可能とするため, 安全性の種別によらない, 計算量的安全と情報理論的安全の両方に適用可能な枠組みを提案した. 基本アイデアは, 対象とする暗号プロトコルの正当性を用いて脆弱であるための十分条件を導出する.
- 安全性検証法の設計： 対象とする暗号プロトコルの正当性から複雑性の下限を導出し, 下限を侵した場合, 安全性に影響すること（すなわち脆弱であること）を証明した. これにより, 与えられた暗号プロトコルの複雑性が下限を侵しているか確認することで脆弱性を検証できる.
- 提案法の主要部分の試作と適用実験による有効性確認：暗号分野おけるトップ会議である CRYPTO2015 で提案された暗号プロトコルに対して, 脆弱性検証法を適用した. その結果, 安全ではあるが, 効率を大幅に犠牲にしていることが明らかとなった. その原因を解明し, 安全性と効率のトレードオフを大幅に改善した暗号プロトコルを提案した.

【国内外における位置付けとインパクト】

本成果は, 暗号分野のトップ会議である Eurocrypt2018 で best known fully robust NIMPC protocol として引用されており, 効率の良さについて初めて保証を与えたという点でもインパクトが大きい. さらに, 著名で権威ある論文誌にも採録されており, 研究コミュニティに広く周知されると期待できる.

【今後の展望】

本成果では暗号プロトコルの安全性評価で得られた知見が効率向上に寄与した. 他の様々な暗号プロトコルに対しても, 本研究で得られた知見を, 安全性と効率の良いトレードオフの達成に活用できると予想している.

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計３件）


① Maki Yoshida and Satoshi Obana, “On the (In)Efficiency of Non-Interactive Secure Multiparty Computation,” Designs, Codes and Cryptography, 査読有, vol.86, no.8, pp.1793-1805, 2018. DOI:10.1007/s10623-017-0424-7

② Maki Yoshida and Toru Fujiwara, “Efficient Usage of Cover Free Families in Broadcast Encryption,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 査読有, vol.E99-A, no.6, pp.1216-1221, 2016. DOI:10.1587/transfun.E99.A.1216

（他１件）

〔学会発表〕（計８件）

① Hideki Sakurada, Kazuki Yoneyama, Yoshikazu Hanatani, and Maki Yoshida “Analyzing and Fixing the QACCE Security of QUIC,” Security Standardisation Research 2016, 2016. (Gaithersburg, MD, USA) DOI:10.1007/978-3-319-49100-4_1

② 木村　文哉, 吉田　真紀, 米山　一樹, “TLS への Logjam 攻撃の ProVerif による形式化と検出,” 2016 年暗号と情報セキュリティシンポジウム, 1A1-3, 2016. (ANA クラウンプラザホテル熊本ニュースカイ, 熊本県熊本市)

（他６件）

６．研究組織

(1)研究代表者

吉田　真紀（YOSHIDA MAKI）

国立研究開発法人情報通信研究機構・サイバーセキュリティ研究所・主任研究員

研究者番号：50335387