平成 26 年度 委託研究

課題 179

暗号プロトコルの安全性評価手法の拡張に関する研究開発

研究計画書

独立行政法人
情報通信研究機構

１．研究開発課題

『暗号プロトコルの安全性評価手法の拡張に関する研究開発』

２．研究開発の目的

ネットワーク上で、通信相手を認証し、個人情報を秘匿した形で通信するなど、安全な通信を実現するため、TLS[11]や IPSec[9][10]など暗号を用いた通信手順（暗号プロトコル）が標準化され、広く利用されている。一方で、暗号プロトコルの設計に起因する問題が顕在化しており[1]、現在広く使われている（あるいは今後広く使われる見込みがある）暗号プロトコルがその使用環境で意図した通り機能すること（通信相手の認証機能、秘匿通信のための鍵交換機能などの実現）を確認できることが要求されている。実用上重要な暗号プロトコルについては、使用範囲の広さから全ての使用環境について個別に安全性を確認することは実質不可能である。よって、全ての使用環境に対する安全性を効率良く評価する技術が、利便性と安全性の観点から重要となる。

情報通信研究機構では、暗号プロトコルの安全性を効率的に評価するための理論的研究に着手している[14]。一方、安全性評価分野では、全ての使用環境に対する安全性評価を実現する手法が、情報セキュリティ分野の著名で権威ある国際会議[2][4][7]や論文誌[3]、代表的な論文アーカイブ[5][6]において発表され、着実な進展がみられている。これらの評価手法では、安全性として「汎用的結合可能性」を評価しており、その性質から暗号プロトコルの安全性を単一の使用環境で確認すれば、全ての使用環境での安全性を確認できたこととなり、安全性評価を劇的に効率化している。ただし、最新の成果[7]であっても評価対象とできる暗号プロトコルとその機能に制約があり、例えば、ハッシュ関数や共通鍵暗号、メッセージ認証子を使用する暗号プロトコルは評価対象外である。また、汎用的結合可能性のいずれの評価手法もツールとして実装されておらず、実用上の有効性が明らかでない。

現在 IETF では、鍵交換機能として Internet Key Exchange Protocol Version 2 が標準化され、認証機能として Mutual Authentication Protocol for HTTP が標準化されつつあり、それぞれ広く使われる見込みがある。しかし、標準化における現時点の安全性評価では、全ての使用環境に対する安全性までは十分確認されていない。よって、鍵交換機能と認証機能について全ての使用環境に対する安全性を効率良く評価する実用的な手法を確立することは特に重要となる。さらに将来的に様々な機能が実現される可能性があることより、あらゆる機能の構成要素とできる暗号的機能、紛失通信機能を効率良く評価する実用的な手法の確立も長期的な観点では重要となる。

本研究開発では、実用上重要な暗号プロトコルの鍵交換機能と認証機能、将来的に重要となる紛失通信機能について、全ての使用環境における安全性を効率的に評価する実用的な手法の確立を目標とする。そのために、まず従来の「汎用的結合可能性」の評価手法の評価機能をツール化し、標準化され実際に使用されている、あ

るいは標準化されつつあり実際に使われる見込みがある暗号プロトコル（実プロトコルと呼ぶ）を用いてツールの実用上の有効性を評価する。そこで明らかとなった重要な課題の解決と、既知の課題である暗号プロトコルへの制約を解決し、従来では検証できなかった実プロトコルを新たに検証可能とすることで、有効性を向上させる。

この研究開発により、将来的にツールを何らかの形で展開し、実プロトコルの安全性を向上させると共に、我が国における暗号プロトコルの汎用的結合可能性による効率的な安全性評価手法に関する知見を集約させることを目的とする。

３．採択件数、研究開発期間及び予算

採択件数：１件

研究開発期間：契約締結日から平成２８年度までの３年間。

予算：各年度、総額３０百万円（税込）を上限とする。（提案の予算額の調整を行った上で採択する提案を決定する場合がある。）

４．研究開発の到達目標

１）従来の安全性評価手法のツール化

⑴必須となる要件

全ての使用環境における安全性を効率良く評価するための汎用的結合可能性の従来手法[2]-[7]がもつ全ての評価機能をソフトウェアで実現し、ツール化する。ツールは入力として、暗号プロトコルと目標とする機能の理想的なふるまい（理想プロトコルと呼ばれる）の記述を受け取り、内部処理で記号論理学に基づく解釈に変換（すなわち抽象化）した上で、汎用的結合可能性を満たすか否かを判定し出力する。ここで、内部処理の抽象化による攻撃見逃しはないとする。入力となる暗号プロトコルとその機能のクラスは従来手法から縮小しないとする。具体的には、対象とする暗号プロトコルのクラスとその機能は以下のものとする。

- 対象とする暗号プロトコルのクラス

  以下の暗号演算と基本演算が使用でき、条件分岐が可能な、ループを含まない線形的なプログラムで記述できるアルゴリズムからなるプロトコルのクラス

  - 暗号演算：公開鍵暗号、電子署名、Diffie-Hellman 鍵交換、準同型公開鍵暗号、コミットメント、ゼロ知識証明、乱数生成
  - 基本演算：データの入出力、送受信、結合、分割
- 対象とする機能：鍵交換、相互認証、紛失通信

実装したツールを用いて、従来手法が提案された論文[2]-[7]に記述された内容を確認できることとする。実装したツールは NICT が事務局をつとめる暗号プロトコル評価技術コンソーシアム CELLOS に提供した際に、そ

のメンバーの使用に耐えるとする。

⑵実施することが望ましい要件

1. 実装したツールを、暗号プロトコル分野の研究者に使いやすい形とする。例えば、ツールへの入出力を分かりやすくすることが挙げられる。なお、入力の記述形式として、[2]-[7]があり、最新の[7]が記述形式として分かりやすく、暗号プロトコルの記述として曖昧性が少ない。
2. 従来手法では既存の検証ツールをサブルーチンとして使用することを想定しているが、代表的な検証ツールをサブルーチンとして使用することが望ましい。
3. サブルーチンとして使用できる検証ツールが多ければ多いほどよい。

２）従来の安全性評価手法の実用上の有効性評価

⑴必須となる要件

実装したツールを実プロトコルに適用し、既に明らかな実用上の課題（すなわち、評価可能な暗号プロトコルとその機能に関する制約）以外の、従来手法の有効性・効率・実用上の課題を明らかとする。また、既に発見されている、もしくは未発見の仕様上の欠陥を検知できた場合には、それを示し、すでに発見されている欠陥を検知できなかった場合には、その結果に基づいて、検知できなかった理由をまとめる。さらに、従来手法が前提としている条件を系統的に分類し、従来手法で評価可能か否かの見極めを容易とする。

⑵実施することが望ましい要件

1. 機構の暗号プロトコル評価ポータルサイト[13]（CPVP, Cryptographic Protocol Verification Portal）に掲載された実プロトコルのうち、攻撃未発見のものについて、以下を明らかとする。
   - 従来手法の対象か否か
   - 対象外の場合、従来研究[3]で指摘されている仕様上の欠陥と同様の欠陥をもたないか否か
   - 対象の場合、ツールを適用して実行時間が数日内で終了するか否か
   - 終了した場合、安全か否か、安全でない場合はその証拠（攻撃）
2. CPVP で攻撃が既に発見されている実プロトコルに適用する。
3. 現在広く使われている、あるいは今後広く使われる見込みがある実プロトコルに適用する。例えば TLS1.3 など。また、数が多いほど良い。
4. 評価結果の寄書を標準化団体に提出する。
5. 必須となる要件で得た知見を研究者・開発者コミュニティに展開する。

３）安全性評価手法の拡張

⑴必須となる要件

従来手法が対象とする暗号プロトコルとその機能への制約を緩和し、従来手法では検証できなかった実プロトコルを新たに検証可能とする。なお、暗号プロトコルへの制約の緩和として、少なくともハッシュ関数も使用できるようにする。そして、NICT が事務局をつとめる暗号プロトコル評価技術コンソーシアム CELLOS に提供した際に、そのメンバーの使用に耐えるツールとして実装する。

⑵実施することが望ましい要件

1. 従来手法の評価機能を実装したツールに拡張機能を追加する形でツール化する。
2. 暗号プロトコルへの制約の緩和として、メッセージ認証子（MAC）、共通鍵暗号を使った暗号プロトコルも検証可能とする。
3. 現在広く使われている、あるいは今後広く使われる見込みがある実プロトコル（例えば、Internet Key Exchange Protocol Version 2, Mutual Authentication Protocol for HTTP）を新たに検証可能とする。
4. 新たに検証可能となる実プロトコルの数が多い程良い。
5. 拡張した評価手法を、国際的な論文アーカイブや学会・論文誌で発表する。
6. 評価結果の寄書を IETF に提出する。

５．研究開発の運営管理及び評価について

研究開発に当たっては、機構の自主研究との連携を図り、1 ヶ月に 1 回程度、NICT セキュリティアーキテクチャ研究室と研究方針や進捗について定期的に打ち合わせを行うこと。また複数の機関が共同で受託する場合には、代表提案者が受託者間の連携等の管理運営を行うこと。

機構は研究開発の進捗状況等を把握するために、ヒアリングを実施することがある。

平成２８年度に終了評価を行う。終了評価の結果等を踏まえ、研究開発終了後に追跡評価を行う場合がある。

６．参考

（１）研究課題設定の背景及びその必要性

現在、機構の自主研究では、ネットワークセキュリティ技術に関して、「サイバーセキュリティ」、「セキュリティアーキテクチャ」、「セキュリティ基盤」の３つの研究開発を柱に、三位一体として国民誰もが安心・安全に情報通信を行うことができるように、社会が必要とする技術の研究開発を進めている。

特に、「セキュリティアーキテクチャ」の研究開発では、モバイル、クラウ

ド、新世代ネットワークを含めた、セキュアネットワークの最適構成技術と設計・評価技術を確立し、安全なネットワークを提供することを目指している。

近年、ネットワークを流通する情報のセキュリティの確保、プライバシの保護の要求は高まっており、暗号アルゴリズムを用いた通信手順、いわゆる「暗号プロトコル」がその要求に応えるために数多く開発されており、ITU-T, ISO/IEC, IETF などで国際標準化されるとともに、ネットワーク製品に搭載されて、幅広く利用されている。

暗号プロトコルの部品となる暗号アルゴリズムについては、これまで CRYPTREC（Cryptography Research and Evaluation Committees）を始めとして十分な安全性評価が行われているが、暗号プロトコルについては、十分に安全性評価が行われているとは言えない。実際、WEP や WPA などの無線 LAN における暗号プロトコルに対する攻撃が発見され、１分以内で無線 LAN のパスワードを明らかにするツールが公開され、Web や smtp、VPN 等、通信内容の秘匿と認証で広く利用される SSL/TLS において、一部の暗号アルゴリズムを用いたときに簡単に鍵が導出できる攻撃[8]などが示されている。

一方で暗号プロトコルの安全性評価の分野では、従来から安全性評価手法が自動化されて利用され、数多くの攻撃の発見に役立っているだけでなく、その評価結果から、国際標準の仕様の修正が行われている。ただし、安全性評価手法には、対象とする暗号プロトコルとその機能について制約があることや、実装されたツールを実プロトコルの評価に適用した際に状態爆発などの効率上の問題があることが知られている。さらに、安全性評価手法によっては、ツールとして実装されておらず、実用上の課題が不明確なものもある。そのため、実プロトコルの安全性を確認するためにも、従来手法をツール化し、実プロトコルに対して実用性を評価し、その課題を明らかとすることは、重要となっている。さらに、新たな暗号プロトコルが標準化されつつ現状では、対象となる暗号プロトコルやその機能への制約を緩和することは特に重要となる。

実際、「暗号プロトコル評価技術コンソーシアム CELLOS（Cryptographic protocol Evaluation toward Long-Lived Outstanding Security）」[12]では活動の一環として、既存の安全性評価理論、手法、ツール、評価結果の情報集約が挙げられている。なお、CELLOS では暗号プロトコルの安全性評価結果が掲載された機構の暗号プロトコル評価ポータルサイト（CPVP, Cryptographic Protocol Verification Portal）を関連サイトとして引用している。

（２）本研究開発による効果

（１）で述べたように、従来の形式的検証手法をツール化し、実用上の課題

を明らかとし、従来手法が対象とする暗号プロトコルとその機能の制約を緩和することは、より多くの実プロトコルの安全性を誰もが確認できるようになることを意味する。

また、暗号プロトコルの安全性評価の技術開発では、特にツール化において国外の大学や研究機関が世界をリードしており、ツールの開発能力やノウハウを蓄積することは、この分野を日本がリードしていくために重要である。本研究開発を通じてその基盤を構築する。

（3）本課題と機構の自主研究の関係

「セキュリティアーキテクチャ」の研究開発では、ICT の利用方法に応じたセキュリティ要件を、様々なセキュリティ技術を用いて過不足無く満たす方法を研究しており、安全性がどの程度満たされているかという評価結果を、セキュリティ知識ベース・分析エンジン REGISTA に蓄積している。本研究開発によって、暗号プロトコルが全ての使用環境において安全かという新たな評価結果が REGISTA に蓄積でき、リスク評価の詳細化に資することができるようになる。

また、評価結果を暗号プロトコル評価ポータルサイト CPVP に掲載することで、実プロトコルがどの程度安全か（どこで使用しても安全か、特定の使用環境に限るのか）という情報をプロトコルユーザに広く提示でき、安心な利用あるいは暗号プロトコル改善に貢献する。

さらに、暗号プロトコル評価コンソーシアム CELLOS にツールを提供することで、評価手法や評価結果について、技術的妥当性や学術的理想論に偏らない現実的な解釈や対処に関する議論の精緻化に資することができる。

参考文献

[1] N. J. AlFardan and K. G. Paterson, “Lucky Thirteen: Breaking the TLS and DTLS Record Protocols,” http://www.isg.rhul.ac.uk/tls/TLStiming.pdf.

[2] Ran Canetti, “Composable Formal Security Analysis: Juggling Soundness, Simplicity and Efficiency,” ICALP 2008, LNCS 5126, pp.1-13, July 2008.

[3] Ran Canetti and Jonathan Herzog, “Universally Composable Symbolic Security Analysis,” J. Cryptology, vol.24, no. 1, pp. 83-147, 2011.

[4] Ran Canetti and Jonathan Herzog, “Universally Composable Symbolic Analysis of Mutual Authentication and Key-Exchange Protocols,” TCC 2006, LNCS 3876, pp.380-403, March 2006.

[5] Ran Canetti and Jonathan Herzog, “Universally Composable

Symbolic Analysis of Cryptographic Protocols (The case of encryption-based mutual authentication and key exchange)," IACR Cryptology ePrint Archive 2004: 334 (2004).

[6] Ran Canetti and Sebastian Gajek, "Universally Composable Symbolic Analysis of Diffie-Hellman based Key Exchange," IACR Cryptology ePrint Archive 2010: 303 (2010).

[7] Morten Dahl and Ivan Damgård, "Universally Composable Symbolic Analysis for Two-Party Protocols Based on Homomorphic Encryption," EUROCRYPT 2014, LNCS 8441, pp.695-712, May 2014.

[8] Erik Tews, Ralf-Philipp Weinmann, and Andrei Pyshkin, "Breaking 104 bit WEP in less than 60 seconds," IACR Cryptology ePrint Archive 2007: 120 (2007),

[9] RFC2409: "The Internet Key Exchange (IKE)," Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc2409.txt, Nov. 1998.

[10] RFC4301: "Security Architecture for Internet Protocol," Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc4301.txt, Dec. 2005.

[11] RFC5246: "The Transport Layer Security (TLS) Protocol Version 1.2," Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc5246.txt, Aug. 2008.

[12] 暗号プロトコル評価技術コンソーシアム, http://www.cellos-consortium.org

[13] 暗号プロトコル評価ポータルサイト, http://crypto-protocol.nict.go.jp

[14] 吉田真紀, 鈴木斎輝, 藤原融, "Externalized Universally Composable の枠組みに対する記号的モデル," 日本応用数理学会 2014 年研究部会連合発表会「数理的技法による情報セキュリティ」(FAIS)セッション, 2014 年 3 月.