様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年　5 月　31 日現在

機関番号：82626
研究種目：若手研究（B）
研究期間：2010～2012
課題番号：22760285

研究課題名（和文）　よりよい効率性と厳密な安全性証明を有する新しいパスワード認証方式に関する研究開発

研究課題名（英文）　A Study on New Password Authentication Schemes with More Efficiency and Provable Security

研究代表者
辛　星漢（SHIN SEONGHAN）
独立行政法人産業技術総合研究所・セキュアシステム研究部門・主任研究員
研究者番号：20443195

研究成果の概要（和文）：本研究開発では、既存のパスワード認証方式を理論的に分析した上、効率がよくてかつ厳密な安全性証明ができる新しいパスワード認証方式を提案する理論研究とともに国際標準団体でのその標準化活動を行った。理論研究の成果としては、既存のパスワード認証方式の安全性を分析し、新たな（匿名）パスワード認証方式を提案した。国際標準化活動の成果としては、IKEv2 へ適用したパスワード認証方式（AugPAKE）の仕様が国際標準団体 IETF　より新たな規格 Experimental RFC 6628 として承認・発行された。

研究成果の概要(英文):In this study, after analyzing the previous password authentication schemes we propose new password authentication schemes with more efficiency and provable security, and make an effort for the international standards. As the first result, we thoroughly analyzed security of the previous schemes and proposed new (anonymous) password authentication schemes. As the second result, the internet-draft that integrates the password authentication scheme (AugPAKE) into IKEv2 was published as experimental RFC 6628 by the international standards organization IETF.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1,400,000	420,000	1,820,000
2011 年度	800,000	240,000	1,040,000
2012 年度	800,000	240,000	1,040,000
総　計	3,000,000	900,000	3,900,000

研究分野：工学
科研費の分科・細目：電気通信工学、通信・ネットワーク工学
キーワード：暗号・セキュリティ

１．研究開始当初の背景

安全・安心できるネットワーク社会を支える暗号技術の中で、盗聴・なりすまし・通信データの改ざんなどを行うアクティブな攻撃者に対しても目に見えない相手を正しく認証しながら安全な通信路を確立する認証付き鍵共有方式（Authenticated Key Exchange: AKE）は欠かせない要素技術のひとつである。実際に認証付き鍵共有方式は SSL/TLS, SSH などで頻繁に使われている。認証付き鍵共有方式では相手を認証するために様々な秘密情報（例えば、公開鍵証明書、

パスワードあるいはそれらの組み合わせなど）を用いている。その中でパスワードだけを秘密情報として用いるパスワード認証付き鍵共有方式（ここでは、簡単に“パスワード認証方式”と呼ぶ）はユーザへの利便性や実世界で広く導入されているなどの利点から長い間盛んに研究が行われている。しかしながら、ユーザが覚えているパスワードの情報量はもともと少ないためオフライン全数探索攻撃が多くのパスワード認証方式において有効になっている。

1992 年に発表された EKE (Encrypted Key Exchange) を始め、多数のパスワード認証方式 (Password-Authenticated Key Exchange: PAKE) が現在 IEEE 1363.2, ISO/IEC 11770-4, IETF, ITU-T などの国際標準団体で標準化されて（または、されつつで）ある。一般にパスワード認証方式は Balanced PAKE と Augmented PAKE に分けられる。前者ではユーザとサーバは同じパスワードを共有しており、ネットワーク上のアクティブな攻撃者に対して安全性を有するものである。後者ではユーザはパスワードを覚えてサーバはパスワードを一方向関数で算出した検証データ (verification data) を保持している。特に、Augmented PAKE はネットワーク上のアクティブな攻撃者に対する安全性に加えて、サーバが compromise されてもユーザのなりすまし攻撃 (server-compromise impersonation (SCI) attacks) に対しても耐性を有するためより高い安全性が提供できる利点がある。また、既存の Augmented PAKE はユーザとサーバの間でやり取りする通信の回数によって 3-pass と 4-pass に分けられる。殆どの 3-pass Augmented PAKE はもともとの Balanced PAKE に冗長性を付加して設計したのに対して、4-pass Augmented PAKE はそのアプローチとは違う設計になっている。

２．研究の目的

既存の 3-pass Augmented PAKE は上に述べたようにもともとの Balanced PAKE に冗長性を加えるため通信量・計算量の効率が悪くなる問題がある。そして、4-pass Augmented PAKE は IEEE 1363.2, ISO/IEC 11770-4 で標準化されるほど高い評価を得ているものの、実際には厳密な安全性証明（数学的に難しい問題への帰着）がついてない問題がある。

本研究開発では、既存のパスワード認証方式を理論的に分析した上、効率がよくてかつ厳密な安全性証明ができる新しいパスワード認証方式を提案する理論研究とともに国際標準団体でのその標準化活動を行う。

３．研究の方法

本研究の目的を達成するためには、コア技術をベースにした新しいパスワード認証方式の研究開発と国際標準化活動という二つの項目について研究開発を行う。「コア技術をベースにした新しいパスワード認証方式の研究開発」は本研究開発で一番重要な基礎研究課題であり、具体的にはコア技術とパスワード認証方式の動向調査と分析、コア技術をベースに効率がよくてかつ厳密な安全性証明ができる新しいパスワード認証方式を提案することである。「国際標準化活動」では国際標準団体が定めているそれぞれの標準化スケジュールに従ってパスワード認証方式の標準化活動を行う。

４．研究成果

(1) 既存のパスワード認証方式の安全性分析　サーバからパスワード認証情報が洩れてもユーザのなりすまし攻撃 (server-compromise impersonation attacks) ができない Augmented PAKE として IEEE P1363.2 standard working group へ

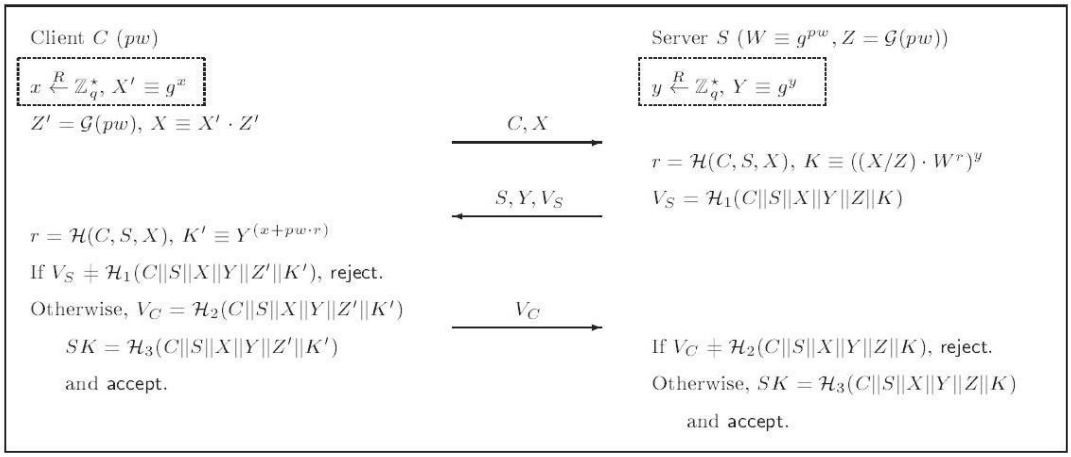

図 1. パスワード認証方式

	Anonymous PAKE ($t = 1$)	Threshold Anonymous PAKE ($t > 1$)
Our Works	–	D-NAPAKE (insecure against insider attacks [Section 2.2])
		Formal model and definition [Section 3.1]
		TAP$^+$ [Section 4] (secure against active and insider attacks)
		ThresholdVEAP [Section 5.1] obtained by applying our RATIONALE to VEAP [23] (secure against active and insider attacks)

図 2. 匿名パスワード認証における結果のまとめ

提出されたパスワード認証方式と IEEE Communications Letters へ載録されたパスワード認証方式を徹底的に分析した。実際にはそれぞれの方式が server-compromise impersonation attacks に対して安全ではないことを証明し、その結果を国際学術誌へ掲載した。

この成果では server-compromise impersonation の一般的な攻撃方法が示されており、新しいパスワード認証方式を設計する際の一つの設計方針に繋がると考えられる。

(2) パスワード認証方式の提案

これまで厳密な安全性を有する Balanced PAK を拡張した Augmented PAK が多数提案されているが、それぞれが通信量や計算量など効率が悪くなる問題がある。それに対して、もともとの PAK の効率性を維持しながら server-compromise impersonation attacks へ安全な方式を提案し、国内学会で発表した（図 1 参照)。

(3) ユーザの匿名性を確保するパスワード認証方式の提案

パスワードだけでユーザの匿名性を保障する匿名パスワード認証方式がいろいろ研究されている。まず、既存の匿名パスワード認証方式が内部攻撃者に対して安全ではないことを示した。そして、匿名パスワード認証における内部攻撃を正式にモデル化し安全性の定義を行った後、その安全性を満たす新しい匿名パスワード認証方式と証明可能安全性を提案した（図 2 参照、国際論文誌へ掲載)。

この成果は、新しい匿名パスワード認証方式の設計方針や厳密な証明可能安全性を議論するにあたって大きな意義があると考えられる。現在、ISO/IEC 20009 Part 4 で匿名パスワード認証方式の国際標準化が始まる予定になっているため、今後その標準化活動が必要になる。

(4) パスワード認証方式の国際標準化活動

国際標準団体 IETF (Internet Engineering Task Force) の IPsecME (IP Security Maintenance and Extensions) WG で IKEv2 向けのパスワード認証方式に関する CFP (Call For Proposals) があったため、サーバからパスワード認証情報が漏えいされてもユーザの成りすまし攻撃ができないパスワード認証方式（AugPAKE）の I-D (Internet-Draft)を提出した。その後、I-D（version 00）を WG や IESG (Internet Engineering Steering Group) で議論しながら要求に応じて内容を version 15 まで更新した。

2012 年 6 月にインターネットの標準的な認証鍵交換モジュール IKEv2 (Internet Key Exchange Protocol version 2)へ適用した仕様が国際標準団体 IETF より新たな規格

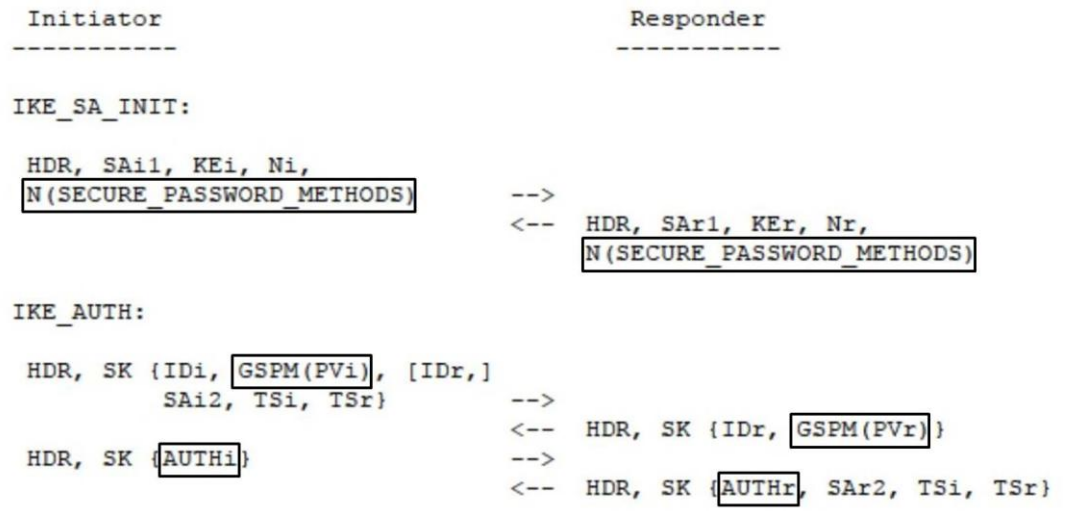

図 3. IKEv2 への適用（四角形は変更各所を表す）

Experimental RFC 6628 として承認・発行された（図３参照）。そして、その紹介記事を産業技術総合研究所公式 HP の主な研究成果（2012 年９月）と産業技術総合研究所広報誌の産総研 TODAY(2013 年２月)に掲載した。

また、パスワード認証方式 AugPAKE を TLS (Transport Layer Security)へ適用した I-D を 2013 年３月に IETF TLS Working Group へ提案した。

これらの成果は、今後パスワード認証方式の社会への普及にも重要な役割を果たすと考えられる。

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４件）

① SeongHan Shin, Kazukuni Kobara, and Hideki Imai, “Threshold Anonymous Password-Authenticated Key Exchange Secure against Insider Attacks”, IEICE Transactions on Information and Systems, 査読有, Vol. E94-D, 2011, pp. 2095-2110
DOI: 10.1587/transinf.E94.D.2095

② SeongHan Shin, Kazukuni Kobara, and Hideki Imai, “Security Analysis of Two Augmented Password-Authenticated Key Exchange Protocols”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 査読有, Vol. E93-A, 2010, pp. 2092-2095
DOI: 10.1587/transfun.E93.A.2092

③ SeongHan Shin, Kazukuni Kobara, and Hideki Imai, “An RSA-Based Leakage-Resilient Authenticated Key Exchange Protocol Secure against Replacement Attacks, and Its Extensions”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 査読有, Vol. E93-A, 2010, pp. 1086-1101
DOI: 10.1587/transfun.E93.A.1086

〔学会発表〕（計３件）

① 辛星漢、グループ間でのファイル共有を柔軟かつ安全に行うための新方式検討、コンピュータセキュリティシンポジウム 2011、2011 年 10 月 21 日、朱鷺メッセ新潟コンベンションセンター（新潟市）

② SeongHan Shin、Efficient Augmented PAK Protocols、ISEC2010-32、2010 年７月２日、弘前大学　（弘前市）

〔その他〕
ホームページ等

① パスワード認証に関する研究
http://www.rcis.aist.go.jp/project/PAKE-ja.html

② IETF Experimental RFC 6628
http://www.rfc-editor.org/rfc/rfc6628.txt

③ IETF I-D (draft-shin-tls-augpake-00)
http://tools.ietf.org/id/draft-shin-tls-augpake-00.txt

④ 盗聴やフィッシング詐欺などを防御する認証技術の開発と国際標準化
http://www.aist.go.jp/aist_j/new_research/nr20120904/nr20120904.html

⑤ 盗聴やフィッシング詐欺を防御する認証技術　証明可能安全性をもち効率のよいパスワード認証
http://www.aist.go.jp/aist_j/aistinfo/aist_today/vol13_02/vol13_02_p12.pdf

６．研究組織
(1)研究代表者

辛　星漢（SHIN SEONGHAN）
独立行政法人産業技術総合研究所・セキュアシステム研究部門・主任研究員
研究者番号：20443195