フィッシング詐欺、情報漏えい、パスワードクラックなどに耐性のある次世代認証鍵共有方式

～使いやすさと安全性の両立とクラウドストレージへの応用～

（独）産業技術総合研究所 情報セキュリティ研究センター 主幹研究員
兼 BURSEC 株式会社 CTO
古原 和邦

認証鍵共有方式は、情報通信ネットワークやそれを経由して提供される各種サービスを安全に利用する上で欠かせない技術となっている。一方、フィッシング詐欺など利用者のうっかりミスを突く攻撃、情報漏えい、パスワードクラックなど既存方式では対処しきれない問題も出始めている。本稿では、これらの問題点を克服するために新たに考案・実用化された次世代認証鍵共有方式について紹介する。新方式は認証機能の強化に加えて、重要データのオンライン分散保存機能も備えており、クラウドストレージなどのオンラインストレージの可用性と情報漏えい耐性の向上にも利用できる。

はじめに

エンティティ（利用者、端末、サーバなど）がネットワーク上の相手を認証し、その認証されたエンティティとの間に安全な通信路を設立するための暗号鍵を共有する方式は、認証鍵共有方式と呼ばれている。例えば、Web ブラウザを使っている際にブラウザの右下などに現れる鍵マークは、通信相手と暗号化通信を行うための鍵が共有されたことを意味している。他にも、無線 LAN に接続する際や、VPN(Virtual Private Network)で社内 LAN に接続する際などにも認証鍵共有方式は利用されており、現在の ICT 社会の安全性を確保する上で欠かせない要素技術の１つになっている。

1990 年代初頭辺りまでのインターネットは、どちらかと言うと「つながること」、「使えること」が重要であり、相手認証はせいぜい送信元アドレスの確認、平文で送信された ID、パスワードの確認が主流であった。この世代を、鍵共有および通信路の暗号化・改ざん検出が行われていないという意味で第 0 世代と呼ぶことにする。1990 年代に入り WWW(World Wide Web)やインターネットの商用利用が普及してくると、それに伴い、通信内容を保護したり、相手を認証したりするための枠組みが導入されるようになった。代表的なものに、SSL/TLS (Secure Socket Layer/Transport Layer Security)、SSH (Secure Shell)、IPsec などがあり、現在それらで利用されている認証鍵共有方式を第 1 世代と呼ぶ

ことにする。第 1 世代認証鍵共有方式のおかげで、ネットショッピング、ウェブバンキングなどの各種電子商取引を自宅から行えるようになり、出先からの社内 LAN への接続、無線 LAN 接続なども第 0 世代と比べると格段に安全に行えるようになった。

ちなみに、認証鍵共有を行うための基本的な考え方や要素技術は 1970 年代に提案されており、その普及までに 20～30 年掛ったことになる。

第 1 世代認証鍵共有方式の限界

第 1 世代認証鍵共有方式はその利用開始から 15 年以上経過しているが、以下のような問題が浮上しており、有効な解決策が求められている。

1. **うっかりミスを突く攻撃の蔓延：** フィッシング詐欺など、うっかりミスを突く攻撃が行われ、実被害が出るようになった。
2. **情報漏えい事故の増加：** 情報漏えい事故の増加[JNSA09]により、鍵や認証情報が漏れる状況を考慮する必要性が出てきた。
3. **全数探索可能なパスワード範囲の拡大：** 計算能力の向上と計算資源の低価格化により、人間がストレスなく使える短いパスワードは全数探索により破られるようになってきた。
4. **通信路しか保護できない：** サーバやクライアントに保存されるデータは保護できない。

1.に対しては、利用者への教育も重要である。しかしながら、利用者にとって警告メッセージを正しく理解し、アドレスバー、鍵マーク、サーバ証明書の拇印などを確認することはめんどうな作業である。その上、これらの作業は強制ではないため利用者に徹底させることは容易ではない。攻撃方法は日々進化しており、例えば、警告の出ない公開鍵証明書が利用されたり、DNS が偽装され正しい URL が使用されたり、多言語文字を含む紛らわしい文字が URL に使用されたり、検索結果の上位にフィッシングサイトを表示させたり、表示ページ中に正しいアドレス、鍵マーク、グリーンのカラーアドレスバー（EV 証明書が検証されたことを示す）が描かれる Picture-In-Picture 攻撃[JSTB07]が行われた場合など、高度、あるいは新手の攻撃にも対処する必要がある。もはや、利用者への注意喚起だけでは限界が来ており、徹底可能で利用者に負担の掛らない対策が求められている。

2.に対しては鍵をスマートカードのような耐タンパーモジュールに格納することも可能ではある。しかしながら、コスト高になるという問題に加えて、モジュールを物理的にこじ開ける侵襲型攻撃や、消費電力や漏えい電磁波などを使って内部に格納されている鍵を抜き出すサイドチャネル攻撃も進化している。実際、自動車の電子鍵や交通系の決済で利用されるスマートカードから鍵が抜き出されるなど実被害も出始めており、耐タンパー性に強く頼らないシステムづくりが求められている。

3. に対しては生体認証を使うことも可能であるが、本人拒否率と他人受入率のバランスを取るためにパスワードと併用される場合も多く、その場合はパスワードの問題は残ってしまう。また、読み取り装置を備えるためにコスト高になるという問題もある。

4. については、認証鍵共有方式は通信路を保護する目的でしか設計されていないため、暗号化して送信されたデータは必ずサーバで平文に復号されてしまう。そのため、クラウドストレージ、モバイルＰＣのハードディスク、USB メモリなどの持ち出し可搬媒体など暗号化の用途には利用できない。

次世代の認証鍵共有方式

我々は従来より第１世代認証鍵共有方式で問題となっていた前述の問題に加えて、以下のような機能や特性を満たすための暗号プロトコルに関する基礎研究を行っており、それを解決するための基本プロトコル LR-AKE (Leakage-Resilient Authenticated Key Establishment) [LR-AKE]を提案していた。この度、その応用システムを実用化させ商用サービスを開始したので、その内容について紹介する。

実用化した次世代認証鍵共有方式 LR-AKE とその応用システムの特徴：

- **情報漏えい耐性：** 攻撃者がクライアント、サーバいずれに記録されている情報と、通信路を流れたデータを入手し、それらに対してパスワードのオフライン全数探索を試したとしても、利用者のパスワードや保存データを復元できない性質。この性質によりクライアント端末や認証トークンの盗難・紛失、サーバ管理者の不正、サーバからの情報漏えいに耐性を持たせることが可能となった。
- **耐タンパー性不要：** 記録情報の漏えいに強い構造を実現できたため、強い耐タンパー性は必ずしも必要では無くなった。そのため、USB メモリなどの安価な可搬媒体を認証トークンとして利用可能になった。
- **データのオンライン分散管理機能：** 情報漏えいに強い性質を応用し、複数のアカウントを使ってクラスタを組み、そこに重要なデータをオンラインで分散保存・復元することができる（図１参照)。この機能は、認証や重要データの保存が必要となるアプリケーションが LR-AKE クライアントを呼び出すことで利用可能になり、例えば、複数のＩＤ，パスワード、暗号鍵、署名鍵などを情報漏えいに強い形式で分散保存したり復元したりする機能を容易に組み込むことが可能となる。
- **短いパスワード１つ：** 利便性の観点から、複数のサービスを受ける場合でも利用者が記憶すべき秘密情報は短い系列１つでよい。この短い系列は、典型的にはパスワードであるが、生体情報から抜き出された短い系列、グラフィカルパスワード、ワンタイムパスワードなどでもよい。短いパスワードが安全に使える理由は、オフライン全数探索とオンラインで複数のアカウントに対してパスワードを試す並列オンラインパス

ワード全数探索を防止できているためである。なお、１つのマスターパスワードを使って複数のＩＤ、パスワードを管理する既存のアプリケーションも存在するが、それらは、管理するＩＤ、パスワードを平文、もしくは、マスターパスワードで暗号化してハードディスクに保存するため、暗号文が漏えいするとそのマスターパスワードの全数探索が可能になるという問題点がある。

- **うっかりミス対策：** サーバを検証するために、ＵＲＬ、鍵マーク、公開鍵証明書の拇印などの確認は不要。利用者は、通信相手を選択し、記憶している短いパスワードを正しい入力欄に入力するだけでよい（通信相手が検証され、検証されなかった相手とは通信は行われない。また、プロトコルの構成上ネットワーク上の攻撃者は打ち込まれたパスワードを入手できない。
- **利用者権限でのアカウントおよび端末管理機能：** 一人の利用者が複数の端末を利用することを想定して設計してあり、１つの端末や認証トークンを紛失したとしても、利用者の権限で、他の端末から紛失した端末のアカウントを無効にし、新たな端末にアカウントをセットすることが可能。また、他の端末からオンライン全数探索が行われたり、それにより端末がロックされたりすれば、その事実を他の端末利用時に通知される。これにより管理者の負担を軽減できると共に、アカウントの再発行までの業務停止期間を短縮できる。なお、既存のサービスでも、落とした端末と通信して、それをロックしたり、そこに保存してあるデータを消去したりするサービスがあるが、それらは端末がネットワークから遮断された場合に利用できなくなるという問題点があった。新方式はそのような状況においてもアカウントの無効化やロックが可能となる。
- **漏えい情報の自動無効化機能／侵入検知機能：** 仮に攻撃者が利用者になりすますためのすべての情報を入手できたとしても、正しい利用者がその攻撃者より先にサーバにログインすれば、それ以降その攻撃者の入手した情報は自動的に使えなくなる。また、逆に、攻撃者が先にログインした場合、正しい利用者はログインできなくなり、侵入の事実を知ることができる。
- **漏えい情報を利用したオンラインパスワード全数探索とミスタイプ切り分け機能：** ログインに失敗した場合に、それが第三者による漏えい情報を使った攻撃であるのか、それとも利用者のミスタイプであるかを判定し、攻撃が数回行われた場合のみ端末をロックすることができる。
- **強前方秘匿性：** 公開鍵暗号や関連する難問が完全に解かれたとしても、盗聴者に対して過去の通信内容を秘匿できる。類似の性質に前方秘匿性(Forward Secrecy)があるが、前方秘匿性だけでは、公開鍵暗号やそれを構成する難問が完全に解かれると過去の通信内容は暴かれてしまう。現在ＰＫＩなどで広く利用されている 1024 ビットの RSA 暗号は 2020 年頃には解読可能になると見積もられており[LV00]、現在 1024 ビットの RSA 暗号で暗号化されたデータはそれ以降に暴かれる可能性がある。

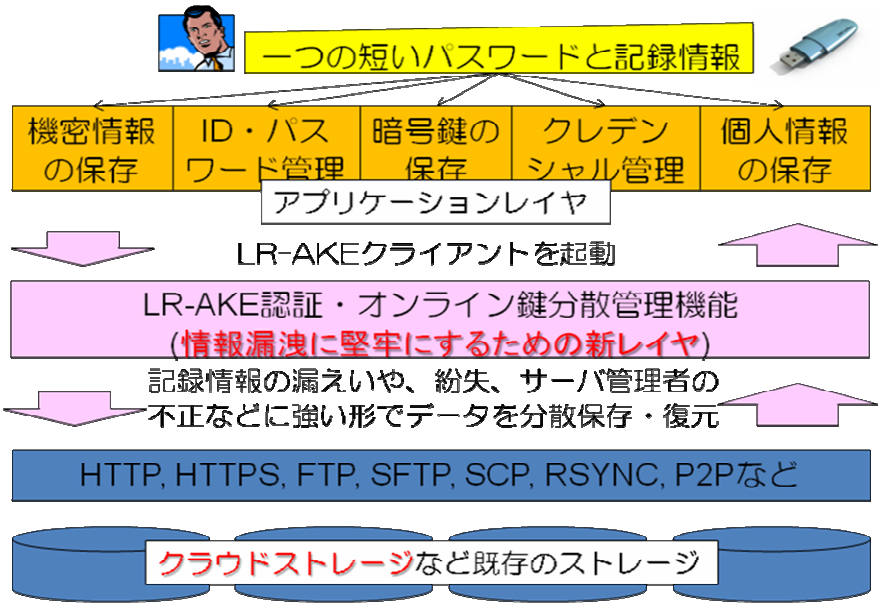

図１　次世代認証鍵共有方式 LR-AKE を応用した新セキュリティレイヤ。
認証や重要データの保存を行わなければならない既存アプリと、
既存ストレージの間に入って上記の機能を提供

LR-AKE 応用システムの実用化には、弊所ベンチャー開発センター[INCS]のスタートアップ開発戦略タスクフォース制度の支援を受けた。スタートアップ開発戦略タスクフォース制度とは、弊所の研究者とベンチャー創出のエキスパート（スタートアップ・アドバイザー）がタスクフォースを組み、ベンチャー起業を通して研究成果を社会に提供するための検討と計画立案を技術と経営の両面から行い、それを実行する制度である。この制度などを受け、現在までに 100 社程度が産総研技術移転ベンチャーとして創業している。

我々も、この制度の基で実用化のための研究開発と、ビジネス化に向けた検討を行い、今年の４月に BURSEC 株式会社というベンチャー会社を設立し商用サービスを開始した。主な事業内容は、社内ＬＡＮへ接続するための認証システムやクラウドストレージに LR-AKE を統合したり、認証や重要データの保存が必要となる各種アプリケーションへ LR-AKE を組み込んだりするためのサービスを行っている。より詳しい内容を知りたい方は下記までご連絡頂きたい。また、本技術の普及により、利用者の負担を軽減させつつ、安全性の向上に貢献できれば幸いである。

【連絡先】
商用サービスに関する問い合わせ先　：　BURSEC 株式会社
TEL: 03-5207-6025 , E-mail: info@bursec.com , Web: http://www.bursec.com

学術的な研究対象としての問い合わせ先 ：
（独）産業技術総合研究所 情報セキュリティ研究センター
E-mail: lrake@m.aist.go.jp , Web: http://www.rcis.aist.go.jp/project/LR-AKE

参考文献

[JNSA09] “JNSA2008 年情報セキュリティインシデントに関する調査報告書”,ver. 1.3, 2009

[JSTB07] C. Jackson, D. Simon, D. Tan and A. Barth, “An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks”, Usable Security (USEC'07), 2007.02

[LV01] Lenstra, A. and E. Verheul, "Selecting Cryptographic Key Sizes", Journal of Cryptology 14 (2001) 255-293, 2001

[LR-AKE] “LR-AKE Homepage”,
http://www.rcis.aist.go.jp/project/LR-AKE/publications.html

[INCS] （独）産業技術総合研究所 ベンチャー開発センター,
http://unit.aist.go.jp/incs/ci/index.html