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

辛 星漢
しん しぇんはん（右）
seonghan.shin@aist.go.jp

セキュアシステム研究部門
セキュアサービス研究グループ
研究員
（つくばセンター）

産総研に入所以来、情報漏えい、端末の紛失・盗難、フィッシング詐欺などに強い相互認証技術とそれらの応用技術の研究開発に従事してきました。現在はより広いインターネットサービスを安全に実現するための要素技術や応用技術に関する研究課題に取り組んでいます。

古原 和邦
こばら かずくに（左）
k-kobara@aist.go.jp

制御システムセキュリティ研究グループ
研究グループ長
（つくばセンター）

産総研に入所以来、情報セキュリティの基礎理論から応用・実用化に至るまでの研究に従事し、2010年4月には産総研技術移転ベンチャー会社の設立も行いました。2012年4月からは重要インフラをサイバー攻撃から防護するための包括的なセキュリティ対策の研究に取り組んでいます。

パスワード認証の問題点

インターネットなどの公衆回線上でサーバーがユーザーを認証する方法として、パスワードが広く使われています。しかし、現在普及しているパスワード認証は、以下のいずれかの問題を抱えており、それらへの解決策が求められてきました。

- 古いシステムなどではパスワードが暗号化されずに公衆回線にそのまま流れる。
- 公衆回線上の通信が暗号化してあっても、パスワードのオフライン全数探索*により復号できる場合がある。
- フィッシング詐欺によりパスワードを盗まれる場合がある。
- サーバーからパスワードなどを含むデータが漏えいした場合、オフライン全数探索を適用することなく、即座に利用者になりすませる場合がある。

AugPAKEの開発

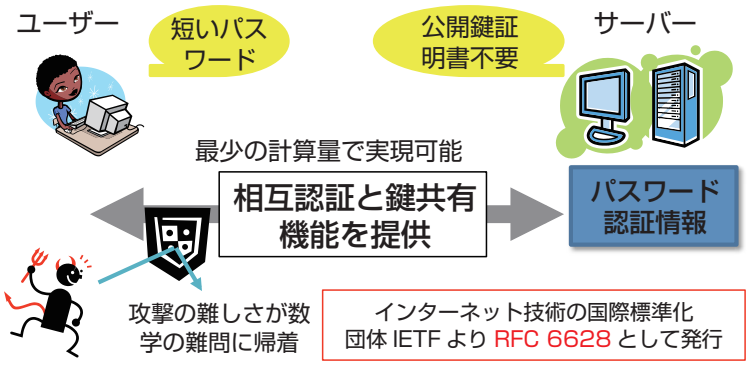
これらの問題を解決するためにいくつかの提案が行われていますが、これまでの方法では、既知の攻撃方法のみを回避する修正が提案されるとそれに対する新たな攻撃方法が発見され、そしてまた、その修正が提案されるといった小手先の対応が繰り返されてきました。これに対して近年では、提案方式の安全性が数学の難問と等価であることを証明することによって解読が事実上困難となることを示す方法が学会や標準化団体において主流となってきました。このような考えにより示された安全性は、証明可能安全性と呼ばれており、新たな方式を提案・選定したりする際の必要条件の一つになりつつあります。

今回私たちは、オフライン全数探索が適用された際に、正しいパスワードが試された状態と、そうでない状態の識別を困難にするために必要な最小限の数学的な構造の研究を行い、その構造を整数論に基づいた難問を用いることで構成できることを示しました。そして、その構造を応用したパスワード認証方式（AugPAKE）の提案および開発を行いました（図）。

AugPAKEを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）へ適用した場合の仕様を国際標準団体IETF（Internet Engineering Task Force）に提案し、2012年6月にRFC 6628として承認・出版されました。

今後の予定

引き続き学会、標準化団体、各種実装プロジェクトなどにおける発表や広報などを通じてこの方式の利点を主張していくとともに、共同研究などを通して実装ノウハウの提供を続けていきます。



研究開発したパスワード認証技術の特徴

関連情報：

● 参考文献

S.H. Shin, K. Kobara: *IETF RFC (Request for Comments)*, 6628, 1-20 (2012).

● 用語説明

＊オフライン全数探索：通信路を盗聴するなどして入手したデータに対して、攻撃者がサーバーやクライアントと通信することなくパスワードを試す攻撃。

● プレス発表

2012年9月4日「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」

●この研究開発の一部は、科学研究費助成事業「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」（2010～2012年度）の支援を受けて行いました。