1ZA-4

秘密情報を一切保持しないクライアントを利用できる認証プロトコルの提案

五 島 秀 典† 鈴 木 秀 和† 渡邊 晃†

名城大学理工学部†

1 はじめに

企業においては情報漏洩の防止が重要な課題である.情報漏洩の原因の 4 割はノート PC 等のモバイル機器の盗難,紛失によるものと言われている.そこで社外に情報を持ち出さずに,必要に応じてクライアント PC から社内システムにリモートアクセスする方法が注目されている.このときクライアントは固定されることなく選べることが望ましい.このようなシステムには確実な認証と暗号化が要求される. 本稿では近年普及が著しいスマートフォンに認証情報を保持させ,初期情報を一切所持しないクライアントを利用可能とするプロトコル MSAP(Mobility-based Secure Authentication Protocol)を提案する.

2 既存の方式

既存方式として非接触ＩＣカードに認証情報を保持させる事前鍵共有方式がある.(1)この方式ではセキュリティを確保するため,ＩＣカードとクライアントＰＣに共有鍵を埋め込んでおく必要がある.そのため,クライアントが固定されてしまうだけでなく,クライアントから共有鍵が漏洩する危険性がある.漏洩した場合システム全体に影響が及ぶという課題がある.

3 提案方式の概要

提案方式ではクライアントに認証に必要となる秘密情報を一切保持させないでよい.その代りにスマートフォンが自らの公開鍵を保持するものとする.表 1.に従来方式と提案方式の初期情報の違いを示す.ハッチング部分が異なるだけで,その他の初期情報は同じである.

表１ MSAP と既存技術の初期情報

	事前鍵共有方式	提案方式
スマートフォン	ユーザ ID パスワード サーバ公開鍵 SP 秘密鍵 事前共有鍵	ユーザ ID パスワード サーバ公開鍵 SP 秘密鍵 SP 公開鍵
クライアント	事前共有鍵	なし
サーバ	サーバ秘密鍵 SP 公開鍵 ユーザ ID	サーバ秘密鍵 SP 公開鍵 ユーザ ID

MSAP で想定するシステムモデルと認証の関係を図 1 に示す.ユーザは秘密情報を格納したスマートフォンを所持している.クライアントは Bluetooth 接続ができ,MSAP 対応するアプリケーションが搭載されていればどのようなものでもよい.スマートフォン-クライアント間の Bluetooth のプロファイルは 1 対 1 通信を前提とするＳＰＰ(Serial Port Profile)とする.そのため,この間での中間者攻撃は成り立たない.

MSAP ではスマートフォン/クライアント/サーバを独立したものとして環状の認証を行う.矢印を方向は認証の方向を示している.ユーザの持っているスマートフォンからパスワードを入力することによりサーバにてクライアントの認証を行う. スマートフォン内スマートフォンの秘密鍵から作成されたディジタル署名を検証することによりスマートフォンを認証する.サーバ秘密鍵から作成されたディジタル署名を検証することによりクライアントはサーバを認証する.

以上の３つの経路の認証を実現することによりクライアント/サーバ間の認証が実現する.

Proposal of an authentication protocol available to client that do not have any scret imformation.
†Hidenori Goshima ‡Hidekazu Suzuki †Akira Watanabe
Faculty of Science and Technology, Meijo University

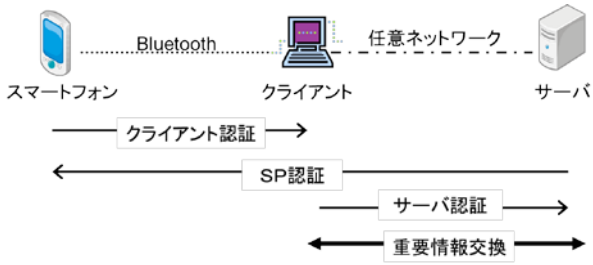

図1　想定するシステムモデルと認証の関係

4　MSAP の動作詳細

以下の説明で使用する記号の意味は以下の通りである.

1. uID=ユーザ ID
2. Ex[y]=鍵 X で y を暗号化
3. psp=スマートフォン公開鍵
4. ssp=スマートフォン秘密鍵
5. ps=サーバ公開鍵
6. ss=サーバ秘密鍵
7. kc=クライアントが生成する共通鍵
8. Nr=サーバが生成する乱数,この
9. Sx[y]=x で y にデジタル署名
10. Ci=クライアントが生成するクッキー
11. Cr=サーバが生成するクッキー
12. PW=パスワード

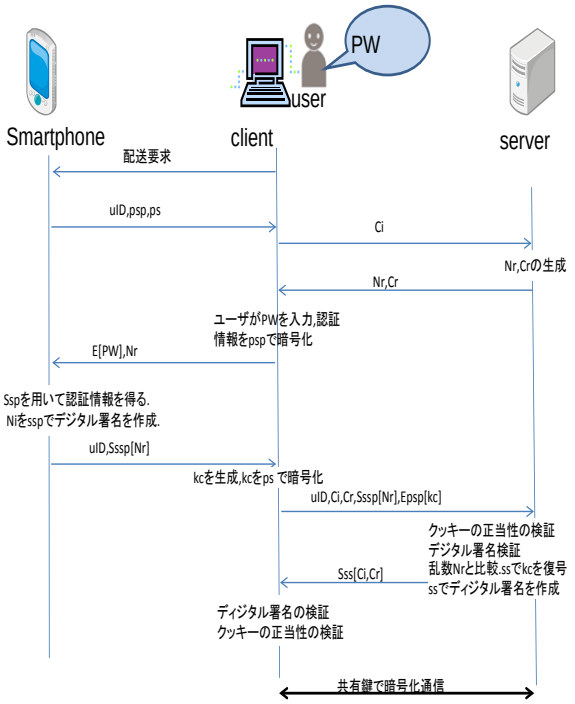

図2　MSAP のシーケンス

動作概要を図2に示す. スマートフォンを保持するユーザがクライアントに近づくと両者は bluetooth によるペアリングを実行する. 次にユーザがクライアント側の MSAP 用アプリケーションを起動する. クライアントからスマートフォンに配送要求が送信されることでスマートフォンの公開鍵, サーバ公開鍵をクライアントへ送信する. クライアントではクッキーCi を作成し, サーバへ送信する. サーバはクッキーCi を受け取るとクッキーCr, 乱数 Nr を生成し, クライアントへ送信する. この時クライアントにログイン画面が表示されるのでユーザはパスワードをクライアント PC へ入力する. クライアントではユーザ情報をスマートフォン公開鍵で暗号化し, サーバから受け取った乱数 Nr を付加してスマートフォンへ送信する. スマートフォンではスマートフォン秘密鍵 ssp を用いてパスワードを取り出し, 比較する. これでクライアント認証が終了する.

続いて Nr をスマートフォン公開鍵 psp を用いてディジタル署名を作成し, クライアントへ送信する. クライアントでは共通鍵 kc を生成し, サーバ公開鍵 ps で暗号化し, スマートフォンから受け取った情報にこれを付加してサーバへ送信する. サーバではクッキーの正当性を検証し, ディジタル署名の検証, Nr の確認も行う. ここでディジタル署名が正しいと判断されるとスマートフォン認証が終了する.

最後にサーバ秘密鍵 ss でディジタル署名を作成し, クライアントへ送信する. クライアントではクッキーの検証, ディジタル署名の検証を行う. ディジタル署名が正しいと判断されるとサーバ認証が終了する.

クッキーCi, Cr は DOS 攻撃を防ぐために使用され, Nr はリプレイアタック防止のために使用される。以上によりクライアント-サーバ間で重要な情報を安全に配送できる.

5 むすび

秘密情報を一切保持しないクライアントを利用できる認証プロトコルを提案した. 今後は実装, 評価を行っていく予定である.

6 参考文献

(1) IC カードシステム利用促進協議会：JICSAP IC カード仕様書 V2.0 (2001).
(2) 宮崎　雄介”中間者攻撃に対する安全性の検討” 平成 21 年度電気関係学会東海支部連合大会論文集, Sep. 2009.
(3) 束　長俊”非接触型 IC カードを用いた認証方式 SPAIC の提案” マルチメディア, 分散, 協調とモバイル (DICOMO2007) シンポジウム論文集, 情報処理学会シンポジウム, Vol.2007, No.1, pp.1332-1337, Jun. 2007.