標的型攻撃メール対策を目とした送信者認証

青山, 尚史 / AOYAMA, Hisashi

(出版者 / Publisher)
法政大学大学院理工学・工学研究科
(雑誌名 / Journal or Publication Title)
法政大学大学院紀要. 理工学・工学研究科編 / 法政大学大学院紀要. 理工学・工学研究科編
(巻 / Volume)
55
(開始ページ / Start Page)
1
(終了ページ / End Page)
4
(発行年 / Year)
2014-03-24
(URL)
https://doi.org/10.15002/00010455

標的型攻撃メール対策を目的とした送信者認証

A SENDER AUTHENTICATION APPROACH TO PREVENT ADVANCED PERSISTENT THREAT

青山 尚史
Hisashi AOYAMA
指導教員　金井 敦

法政大学大学院工学研究科情報電子工学専攻修士課程

Advanced persistent threat (APT) has been becoming familiar at resent time. A content of the mail is very similar to usual personal mail messages, so that the user cannot suspect the mail is malicious. In this paper, we propose the easy e-mail sender authentication system using the IC card and ID based encryption, as compared to the authentication method of mail being currently available. Then the prototype of proposed system is developed and the feasibility of proposed system is evaluated.
***Key Words** : APT , ID-Based Encryption, Electronic signature, Certification*

１．はじめに

特定の軍事産業，化学産業，政府機関など機密性の高い組織を対象に情報窃取や破壊的な活動等を行う標的型攻撃が近年多くなっている．不特定多数ではなく特定の対象を

狙って攻撃が行われることから標的型攻撃と呼ばれている．中でもメールを使用した標的型攻撃メール[1] はソーシャルエンジニアリングの手口を使っていて，メールの受信者は非常に騙されやすくなっている．標的型攻撃メールでは，悪意のある迷惑メールのように添付ファイルやメール本文の URL を経由してウイルスに感染させる攻撃パターンを含み，なおかつ，あたかも正当な業務連絡や依頼であるかのように見せかける件名や本文でメールを送りつけ，受信者が騙されやすいような仕掛けになっている．特に昨今は，受信者に関係のある実在の発信元を詐称するケースが増加しており，被害に遭いやすくなっている．攻撃者にとっての利点は，情報を窃取することで依頼者から報酬を得たり，自らの政治的なものを含めた欲求を満たすことにある．ビジネスとして成立している場合は，依頼内容を完遂するまで手法を変えながら攻撃を繰り返す．標的型攻撃メールによる被害として以下のものが挙げられる．

- 標的型攻撃メールの班別に時間をとられ，業務の妨げになる
- 偽装された添付ファイルによって受信した端末がウイルスに感染する
- メールの本文の URL に誘導されて，ウイルスに感染させられる，詐欺に巻き込まれる（フィッシング，ワンクリック詐欺など）
- 標的型攻撃メールによる被害を受けた端末の情報が，次への標的型攻撃メールによる攻撃を成功させうる情報を悪用される

このような被害を防ぐためには，送信元が改ざんされていない，なりすましがされていないかどうかを検証できれば良い．送信者がウイルスに感染していない限り，同時に添付ファイルの安全性も保証される．

そこで本稿では，新たに ID ベース暗号と手持ちの IC カードを利用した受信者が送信者を検証できるメールの認証システムを提案する．

２．既存の認証方法・技術

既存の認証方法として S/MIME (Secure/Multipurpose Internet Mail Extensions)[2] や PGP(Pretty Good Privacy)[3]が挙げられる．

ネットエージェント株式会社の製品「防人」[3]は，標的型攻撃メールを防御するための製品である．これはメール中継サーバーとして動作し，メールの添付ファイルを画像化し，有害な添付ファイルを無効化するものである．

これらの方法では，CA(Certificate Authority，認証局)の利用や公開鍵サーバーなどの設置が必須になる．メール送信の対象規模が大きいほど有効な手段であるが，規模が小さい個人などで利用する場合は非効率的となる．

また，標的型攻撃メールの予防対策[5] に関する研究もされている．接種直後であれば免疫力が上がっていて攻撃への耐性も高くなるが，完全な防御法では無い上に，時間とともに耐性が低くなる可能性が高く，定期的に予

防対策を行う必要がある．

送信者がメールアドレスを偽装している場合はドメイン認証である，Sender ID や SPF(Sender Policy Framework)，DomainKeys，DKIM(DomainKeys Identified Mail）なども有効であるが，標的化攻撃メールはメールアドレス偽装の確率は低いと思われる．これは送信元 IP アドレスを参照し問い合わせを行い送信元を検証したり，電子署名を付与して送信元を検証する認証技術である．送信者のアドレスが正規なものであることを証明する（なりすましを防ぐ）技術で，主にスパムの根本的な対策として利用されている．

３．提案手法

本稿では，以下を満たすシステムを提案する．

- 互いが知人であり，メールにて通常のコミュニケーションをとっている相手を対象とする
- 使用するネットワークは盗聴の可能性を考慮する
- 盗用の可能性を考慮する
- S/MIME や PGP と比較して導入が容易である
- 送信者が受信者に正当性を証明できる
- 送信者のなりすましを防ぐ
- 再送攻撃対策をしているか

３．１．導入

本稿では，IC カード，ID ベース暗号[6]を使用する．IC カードは交通系 IC カードや IC 免許証などすでに所持しているものを利用し，その IC カードの製造番号などの不変情報を用いる．

ID ベース暗号とは，公開鍵暗号の一種であり識別子を利用した暗号方式である．この暗号では，利用者の公開鍵として，利用者の識別子を利用者の公開鍵として用いる．今回は ID ベース暗号に基づいて署名を作成･添付し，その署名を受信者が検証を行う．

３．２．認証手順

メールの送信者を Alice，受信者を Bob とする．PKG（秘密鍵生成局）を送信側に設置する．本稿では PKG と役割上，分けてと記してはいるが，基本的に動作環境は全てスマートフォン上である．

（１）パラメータの定義

PKG は以下のものを生成する．

- 楕円曲線群のセット(G_1, G_2, G_T)
- 楕円曲線上の点$P \in G_1, Q \in G_2$
- ペアリング（双曲線写像）$\hat{e}(\cdot,\cdot): G_1 \times G_2 \to G_T$
- ハッシュ関数 H

送信者 Alice は ID（IC カード情報：IC）と受信者 Bob の Email アドレス(Email)を持つ．また乱数$r(\in Z/pZ)$を生成する（p は素数）．

（２）認証セットアップ１

送信者 Alice は PKG から楕円曲線上の点 P を受け取り，

$$C_{key} = r \times IC \times Email \times P$$

を計算する．受信者 Bob と盗聴の可能性がある安全でない通信路を用いて，事前の秘密情報の共有なしで暗号鍵の共有を行う，ディフィー・ヘルマン鍵共有法[7]を用いて鍵交換を行ったのち，C_{key}を暗号化し，送信する．受信者 Bob は共有鍵で復号化を行い，送信者と鍵データを対応付け，保存する．信頼できるネットワークを利用できる場合は直接受け渡しを行っても良い．図１に認証セットアップ１の概要を示す．

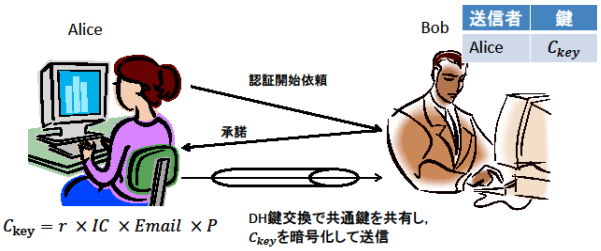

図１．認証セットアップ１

（３）認証セットアップ２

送信者 Alice は以下の２つを計算する．

$$S = H(IC \times Email)$$

$$E = H(\hat{e}(P, IC \times Email \times Q)^r)$$

そして，

$$A = S \oplus E$$

を認証データとして受信者 Bob に送信する．ここで S をシード認証値と呼ぶ．

受信者 Bob は A を受信し，ペアリングの双線形性より以下の計算を行う．

$$A \oplus H(C_{key},, Email \times Q)$$
$$= H(IC \times Email) \oplus H(\hat{e}(P, IC \times Email \times Q)^r) \oplus H(\hat{e}(r \times IC \times P \times Email, Q))$$
$$= H(IC \times Email) \oplus H\left(\hat{e}(P,Q)^{IC \times Email \times r}\right) \oplus H(\hat{e}(P,Q)^{IC \times Email \times r})$$
$$= H(IC \times Email)$$
$$= S$$

受信者 Bob はシード認証値 S を認証セットアップ１で対応付けたデータに認証回数（初期値０）とともに追加し，保存する．図２に認証セットアップ２の概要を示す．

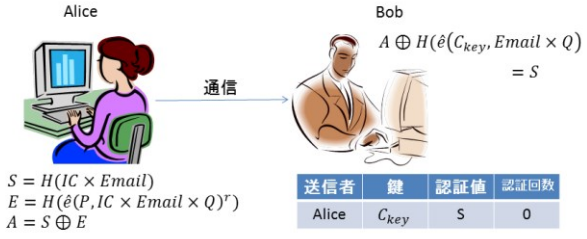

図２．認証セットアップ２

（4）**メールの送信**

送信者 Alice はシード認証値 S にハッシュ関数をかけて暗号化したA_1をメールに添付し，送信する．

$$S_1 = H(S)$$

$$E = H(\hat{e}(P, IC \times Email \times Q)^r)$$

$$A_1 = S_1 \oplus E$$

二回目以降の送信時では，再送攻撃対策として，

$$S_2 = H(H(S)), \quad S_3 = H\left(H(H(S))\right), \ldots$$

とシード認証値 S にハッシュ関数を数珠繋ぎに計算し，E で暗号化する．通信路において認証情報 A を盗聴されたとしても，再利用も次回の認証情報の予測もできないため安全である．

（5）**署名の検証**

受信者 Bob は，認証情報が添付されたメールを受信したら，認証セットアップ２と同様の計算をC_{key}を用いて行い，署名の検証を行う．

$A_n \oplus H(C_{key},, Email \times Q)$

$= S_n$

同時に，保存している送信者 Alice のシード認証値 S に認証回数分だけハッシュ計算を行いS_n'とする．$S_n = S_n'$が成立すれば送信者が認証され，受理される．不成立であるならば不正なメールと判断することができる．認証が受理された場合は，送信者との認証回数を１増やす．

４．実装

実装はスマートフォンの Android 端末上で動作するプロトタイプアプリケーションを作成し，評価を行う．近年，携帯端末の性能向上はめざましく，様々な機能が増えており，IC カードの読み取りを行える NFC 搭載端末が増加している．そういった背景から，特に事前準備をすることなく認証を行えるためである．

アプリケーションの機能として，

- 鍵の生成
- IC カードの読み取り
- 署名の作成
- 署名の検証
- 鍵共有機能

を実装する．

アプリケーションでは，IC カード情報を読み取って署名を生成し，インテント（他のアプリやデバイスから簡単に情報を受け渡す機能）を用いて常用しているメーラーへ受け渡す．受信側では，逆に添付ファイルを開く際にインテントによって，署名データを本アプリへ受け渡す．この方法を用いることで，ユーザの環境を変えずに署名の作成・検証が可能となり，汎用性が高くなる．

ペアリング計算はペアリング暗号ライブラリである PBC の Java 移植で，Android 端末でも動作する JPBC(Java Pairing-Based Cryptography)ライブラリ[8]を使用する．計算方法は前述のとおりである．今回の実装での楕円曲線は$y^2 = x^3 + x$を選択した．ハッシュ関数は SHA256 を使用した．

５．評価

（1）なりすましが出来ない

署名の生成に IC カードを必要としているため，端末の盗用やメールヘッダによる書き換えを行って送信者を騙ったとしても，同じ IC カードは用意できないので受信者は判別することができる．

IC カードが紛失や更新などで変更になった場合は，再び認証セットアップ１・２を行うことで認証の再開をすることができる．

署名はハッシュ計算をした上で，暗号化を行っているため署名の再利用（再送攻撃）も防ぐことができ，次回の署名の予測も困難なため安全である．

（2）暗号の安全性

楕円曲線の離散対数問題に帰着するため安全である．一般に，楕円曲線上の点P，任意の整数kに関して$N = k \times P$と乗算を行った場合，Nからkを特定することは困難である．また，RSA 暗号で 1024bit は，楕円曲線暗号の 160bit に相当すると言われていて，RSA 暗号を用いた場合よりも署名長を短くすることが可能である．近年，RSA 暗号は 2048bit 必要と言われているため，（明確な対応方法は存在しないが）楕円曲線暗号では 256bit 程度あれば安全性が保証されると考えられる．

楕円曲線の選択によっても暗号強度が変化するため，利用する環境によって（同時に計算時間も変化するため）楕円曲線の使い分けをすることが必要である．

（3）導入の容易さ

S/MIME や PGP は事前に CA を必要としたり，公開鍵サーバーを用意するなど準備が多く手間がかかるが，本手法では ID ベース暗号を用いているため，準備が簡易化されている．

（4）計算時間

Nexus7 上で実装したアプリケーションを実行した時の鍵やハッシュ計算にかかる時間を計測した．図 3 に暗号強度別の鍵C_{key}の平均生成時間，図 4 に数珠つなぎにハッシュ計算をした時にかかった平均時間を示す．

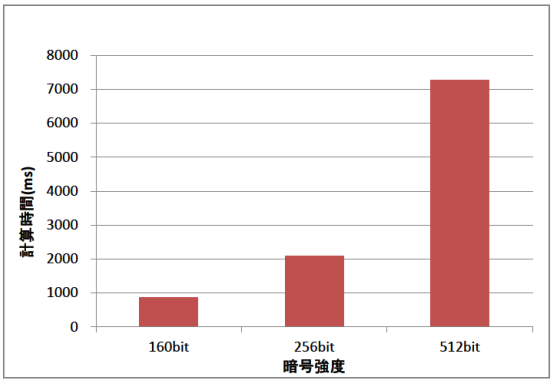

図 3. 暗号強度別鍵C_{key}の平均生成時間

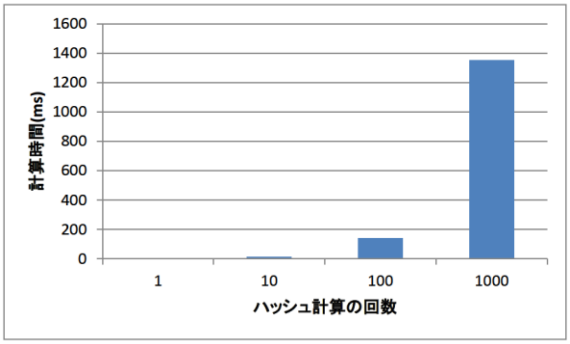

図 4. 数珠つなぎにハッシュ計算をした時にかかった平均時間

暗号強度は前述のとおり，256bit 程度で安全性が保証される．512bit で鍵を生成するときは平均で約 7 秒と時間がかかるが，256bit で安全性と計算時間の実用性のバランスがとれている．ハッシュ計算もメールの送信回数を考慮すると，特に問題は無いといえる．コンピューター上でこれらの計算を行うと，CPU 性能が格段に上がるためどの条件で計算したとしても操作には全く支障が出ない結果となった．

６． おわりに

本研究では，標的型攻撃メール対策を目的とした送信者認証の提案を行った．既存手法よりも ID ベース暗号によって簡単化されたセットアップで送信者の認証を実現した．手持ちの IC カードの利用で物理的な送信者のなりすましに対応し，低コストで標的型攻撃メール対策を目的とした認証方法の実現可能性を示すことが出来た．また，スマートフォンとの連携や，IC カードリーダーを用いることでコンピューター上での実現が可能であると言える．

謝辞：本稿の作成にあたり，多くのご助言とご指導くださいました金井敦教授に深く感謝します．また，日頃より多くの助言を頂いた金井研究室の皆様方や友人たちに感謝の意を示します．

参考文献

[1] IPA：“IPA テクニカルウオッチ『標的型攻撃メールの分析』に関するレポート”, http://www.ipa.go.jp/about/technicalwatch/20111003.html ,2011
[2] B Ramsdell, Brute Squad Labs, S. Turner ほか: “S/MIME Version 3．2 Message Specification”, RFC5751,2010
[3] J. Callas, PGP Corporation, L. Donnerhacke ほか: “OPEN PGP Message Format” ,RFC4880, 2007
[4] ネットエージェント株式会社:“標的型攻撃メール対策 防人” ,http://www.netagent.co.jp/product/sakimori/ ,2012
[5] 伊藤史人，高見澤秀幸，佐藤郁哉: “標的型攻撃メールの予防対策”，学術情報処理研究 No.16 p100-110, 2012
[6] CRYPTREC：“ID ベース暗号に関する調査報告書” ,http://www.cryptrec.go.jp/report/c08idb2008.pdf , 2008
[7] W. Diffie, M. E. Hellman : "New Directions in Cryptography", IEEE Transactions on Information Theory, vol.IT-22, No.6, pp.644-654, 1976.
[8] Angelo De Caro and Vincenzo Iovino : ” JPBC: Java pairing based cryptography”， Proceedings of the 16th IEEE Symposium on Computers and Communications, ISCC 2011,http://gas.dia.unisa.it/projects/jpbc/,2011
[9]青山尚史，折茂潤一，金井敦：“標的型攻撃メール対策を目的とした送信者認証の提案”，第 21 回 マルチメディア通信と分散処理ワークショップ (DPSWS2013), 2013