PIDを用いた社会システムにおける認証プロトコルの安全性評価

野原, 康伸
九州大学大学院システム情報科学府情報工学専攻

浜崎, 陽一郎
九州大学システムLSI 研究センター

萩原, 大輔
九州大学大学院システム情報科学府情報工学専攻

井上, 創造
九州大学大学院システム情報科学研究院 | 九州大学システムLSI 研究センター

他

出版情報：マルチメディア, 分散, 協調とモバイル (DICOMO2003) シンポジウム, pp.753-756, 2003-06.
Information Processing Society of Japan
バージョン：
権利関係：

PIDを用いた社会システムにおける認証プロトコルの安全性評価

野原 康伸 † 浜崎 陽一郎 ∗ 萩原 大輔 † 井上 創造 ‡,∗ 安浦 寛人 ‡,∗

† 九州大学大学院システム情報科学府 情報工学専攻
‡ 九州大学大学院システム情報科学研究院
∗ 九州大学システム LSI 研究センター

The Security Evaluation of the Authentication Protocol for PID System

Yasunobu Nohara† Yoichiro Hamasaki* Daisuke Hagiwara† Sozo Inoue‡,* Hiroto Yasuura‡,*

†Graduate School of Information Science and Electrical Engineering, Kyushu University
‡Department of Computer Science and Communication Engineering, Kyushu University
∗ System LSI Research Center, Kyushu University

1 はじめに

インターネットをはじめとするネットワークの急速な普及を背景に、インターネットバンキングといった新しいサービスへの取り組みが本格化してきた。我々の生活はより便利により効率的になると思われるが、電子的であるがために発生する安全性の問題は大きな課題である。痕跡を残さない改竄、なりすましや盗聴といった数々の脅威から我々を守り、被害を最小限に留める社会の構築は重要であると考えられる。

現在 PKI(Public Key Infrastructure) による社会システムが構築されようとしている。PKI ではシステムに対する様々な脅威への耐久性を向上させることに、安全対策の主眼が集中している。このため、脅威が現実化した場合の被害額や被害範囲、修復に要する費用・期間といった問題への配慮が軽視されている。システムが様々な脅威への耐久性を持つことは当然必要であるが、仮に脅威が現実化したとしても被害を最小限に留めるような社会システムの構築が必要であると考えられる。

我々は、上記の問題に対応した PID(Personal IDentifier) という一種の個人 ID を用いた社会システムを提案している [1][2]。PID を用いた社会システムでは、PID の一部である subPID をユーザとサービス提供者が互いに共有し、subPID を用いて互いに相手が正当な者であるかを確認し合ったり、暗号通信などを行うことで安全な電子サービスが実現される。

本論文では、PID を用いた社会システムの中で特に重要と思われるユーザとサービス提供者間の PID を用いた認証プロトコルについて、PKI を用いた認証プロトコルと比較しながら、安全性の評価を行った。

まず安全性の評価を行うに先立って安全性の定義について議論を行い、次の 3 つを安全性として定義した。

1. 攻撃の抑止　2. 攻撃への耐性　3. 被害の最小化

そして、経済学の理論である**期待効用最大化理論**を用いることにより、どのような指標を安全性評価指標として用いるべきかを明らかにした。これを用いて評価した結果、我々の提案する PID を用いた認証プロトコルは、PKI を用いた認証プロトコルに比べて、攻撃による被害の最小化できる点や攻撃の抑止の点で優れており、安全性を高くすることが可能であると分かった。

2 PIDを用いた社会システムにおける認証プロトコル

本章では、我々が提案している PID(Personal IDentifier) を用いた社会システムにおける認証プロトコルについて概説する。

PID を用いた社会システムにおいて、ユーザとサービス提供者は図 1 のようなデータを所持している。

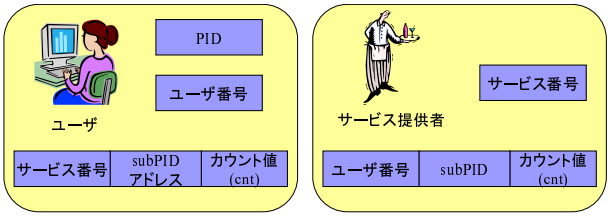

図 1: ユーザとサービス提供者の保持するデータ

ここで、用語の意味は次の通りである。

- **PID**：ユーザごとに割り当てられる十分に長いビット列
- **subPID**：PID の一部分のビット列
- **ユーザ番号**：サービス提供者がユーザを特定するために用いるユーザ固有の番号
- **サービス番号**：ユーザがサービス提供者を特定するために用いるサービス提供者固有の番号
- **カウント値** cnt：ユーザとサービス提供者がワンタイムパスワードによる相互認証を行うための可変認証情報

- **subPID アドレス**：ユーザが PID から subPID を選択するためのアドレス

PID を用いた認証プロトコルは、次の手順の通りである。なお、認証プロトコルの内容や暗号化関数のアルゴリズムは公開されているものとする。

STEP1: ユーザ・サービス提供者の subPID の共有　本ステップでは、ユーザとサービス提供者との間で subPID の共有を行う。subPID 共有の手順は次の通りである。

Phase1: ユーザはサービス提供者に対してサービス要求とユーザ番号を送付する。

Phase2: サービス提供者は送付されたユーザ番号を用いて DB から subPID とカウント値を取り出す。

Phase3: サービス提供者はユーザに対してサービス番号を送付する。

Phase4: ユーザは送付されたサービス番号を用いてカウント値とアドレスを取り出し、PID を用いて subPID を生成する。

STEP2: 相互認証　本ステップでは、前ステップで共有された subPID を用いて、ユーザとサービス提供者との間でワンタイムパスワードを用いた相互認証を行う。相互認証の手順は次の通りである (図 2 参照)。ただし、$E_{key}(X)$ はデータ X を鍵 key で暗号化したもの、$D_{key}(X)$ はデータ X を鍵 key で復号化したものを表すものとする。また、$X\|Y$ はデータ X とデータ Y を結合したものを表すものとする。

Phase1: ユーザとサービス提供者は、図 2 のように subPID を α と β に 2 分割する。

Phase2: ユーザは、$OTP_{user} = E_{\alpha\|cnt}(\beta)$ を生成し、サービス提供者に送付する。

Phase3: サービス提供者は、送付された OTP_{user} から $D_{\alpha\|cnt}(OTP_{user})$ を計算し、β と一致するか検証する。

Phase4: サービス提供者は、$OTP_{service} = E_{\beta\|cnt}(\alpha)$ を生成し、ユーザに送付する。

Phase5: ユーザは送付された $OTP_{service}$ から $D_{\beta\|cnt}(OTP_{service})$ を計算し、α と一致するか検証する。

Phase6: ユーザとサービス提供者は、カウンタをカウントアップする。

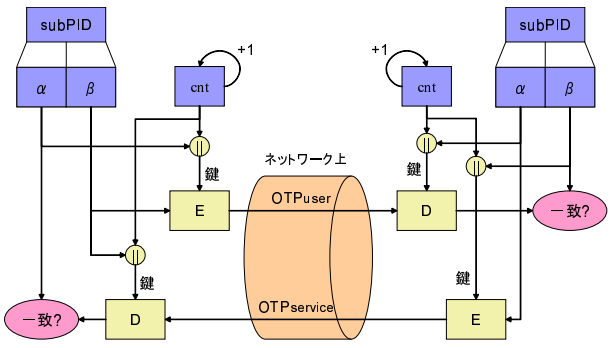

図 2: 相互認証

3　認証プロトコルの安全性評価の方法

本章では、認証プロトコルの安全性評価の方法について述べる。

3.1　認証プロトコルの安全性とは

認証の目的を考えると、第三者が別人の振りを行う**なりすまし**の脅威に対する対策が認証の安全性を考えるに当たって最も重要である。本論文では、なりすましの脅威に対する認証プロトコルの安全性を検討するものとする。

従来プロトコルの安全性というと、プロトコルに対する様々な脅威への耐久性を向上させることに主眼が置かれていた。しかし、全ての脅威を洗い出して安全対策を行うことは現実的に不可能であり、技術の進歩によって効率良く攻撃できるようになることは十分考えられることである。つまり、どのような認証プロトコルであっても、攻撃の脅威は常に存在することになる。そこで、仮に攻撃に成功したとしても、攻撃による被害や復旧コストをできる限り抑えることが重要となってくる。

また、人々に攻撃を行ってみよう思わせないことも重要だと考えられる。なぜならば、人々が攻撃を行わなければ被害は発生しないからであり、攻撃者となる人間、すなわち犯罪者を減らすことが社会システムとして望ましいからである。

以上の議論より、本論文では認証プロトコルの安全性を次のように定義する。

1. **攻撃の抑止:** 攻撃を実行してみようと思わせないものか
2. **攻撃への耐性:** 攻撃が行なわれたとしても、どれだけ攻撃を防ぐことができるか
3. **被害の最小化:** 仮に攻撃が成功しても、どれだけ被害が少なくて済むか

以下では、本節の安全性の定義に沿って、議論を進める。

3.2　安全性 1:攻撃の抑止 の検討

人がある行動をするかしないかを説明するものとして**期待効用最大化理論**がある [4]。期待効用最大化理論は、「個人や企業は自分にとって最も効用の期待値 (期待効用) が高くなるような行動を選択する」ということを述べており、経済学の土台となる理論である。

期待効用最大化理論を用いて安全性評価指標を考えるため、攻撃による期待利益を導出すると次のようになる。

攻撃による期待利益＝攻撃成功確率・攻撃成功利益
－攻撃発覚確率・ペナルティコスト　(1)
－攻撃コスト

人々に攻撃を実行しようと思わせないためには、次式が満たされる必要がある。

攻撃による期待利益 < 攻撃をしない場合の期待利益　(2)

(1)(2) 式より、小さいほうが望ましい安全性評価指標としては次の 2 つが挙げられる。

- 攻撃成功確率
- 攻撃成功利益 (対象リンク数、なりすまし可能回数等)

また大きいほうが望ましい安全性評価指標としては、次の 4 つが挙げられる。

- 攻撃発覚確率
- ペナルティコスト (損害賠償額・刑事罰の重さ等)
- 攻撃コスト (金銭、計算量や盗聴回数等)
- 攻撃をしない場合の期待利益

これらの安全性指標は安全性 2,3 と密接に関わっており、攻撃への耐性を上げることや被害を最小化することが攻撃の抑止につながっていることが分かる。

なお、本論文では、安全性評価にあたり攻撃コスト (計算量と盗聴回数) と成功確率、攻撃成功利益 (対象リンク数、なりすまし可能回数) を安全性評価指標として用いる。

3.3 安全性 2:攻撃への耐性と安全性 3:被害の最小化 の検討

認証プロトコルに限らず、暗号技術を用いたシステムに対する攻撃は、一般に以下の 3 つのパラメータにより規定できる [3]。

- **攻撃者の能力**
  攻撃者はどのくらいの費用と時間を攻撃にかけることができるのか。どのような立場にいるのか。
- **攻撃のシナリオ**
  攻撃者は、どのような情報を利用できるのか。どのような攻撃を仕掛けることが出来るのか。
- **攻撃の成果**
  攻撃者の行った攻撃が成功することにより、どのような結果となるのか。

安全性 2:攻撃への耐性は、攻撃パラメータである「攻撃者の能力」と「攻撃のシナリオ」から求められる。また、安全性 3:被害の最小化は、攻撃パラメータの「攻撃の成果」を言い換えたものである。つまり、攻撃を規定することによって安全性 2:攻撃への耐性と安全性 3:被害の最小化を求めることが出来ることになる。

4 認証プロトコルの安全性評価

本章では、攻撃者がネットワーク上の第三者である場合の PID を用いた認証プロトコルと PKI を用いた認証プロトコルである SSL/TLS 認証プロトコルの安全性評価を行い、両者を比較・検討する。ただし、以下の議論では subPID の長さを $2l$、カウント値 cnt の長さを l_c、subPID を分割した α や β、OTP の長さを l とする。また、ユーザ・サービス提供者の総数を N とする。

4.1 PID を用いた認証プロトコルの安全性

本節では、PID を用いた認証プロトコルの各種攻撃に対する安全性について考察する。想定する攻撃のタイプは次の 3 つの方法である。

攻撃 A: 盗聴回数・計算量ともに攻撃コストをかけない攻撃

攻撃 B: 盗聴回数に攻撃コストをかける攻撃

攻撃 C: 計算量に攻撃コストをかける攻撃

ただし、本節では計算量として暗号化・復号化関数 E, D の使用回数を用いものとする。

4.1.1 攻撃 A に対する安全性

OTP_{user} や $OTP_{service}$ として考えられる組合せは、2^l 通りである。よって、2^l 通り考えられる OTP の内、どれかを送付すれば 2^{-l} の確率でなりすましに成功する。本攻撃に必要な計算量・盗聴回数は、ともに 0 である。対象リンク数は 1 回線のみであり、なりすましは 1 回限りしか出来ない。

4.1.2 攻撃 B に対する安全性

OTP_{user},$OTP_{service}$ は、カウンタの変化に伴い毎回変化するが、2^{l_c} 回認証を行えば、カウンタの値は再び同一値に戻ると考えられる。つまり、OTP_{user},$OTP_{service}$ は、周期 2^{l_c} で変化することになる。よって、2^{l_c} 回盗聴を行えば (=盗聴回数)、次回から盗聴した順に OTP_{user} や $OTP_{service}$ を送信することによりある 1 回線において、ユーザやサービス提供者として多数回なりすましが可能になる。必要な計算量は 0 であり、成功確率は 1 である。

4.1.3 攻撃 C に対する安全性

OTP を解析することにより α, cnt, β を入手して、なりすましを行う攻撃法についての安全性を考える。攻撃の方法は、次の通りである。ただし、OTP_A^n は主体 A が n 回目に送付した OTP を表すものとする。

STEP1: 考えられる α と cnt の組合せ ($= 2^{l+l_c}$ 個) を鍵として、OTP_{user}^1 を復号化関数 D で復号化する。この作業によって得られた 2^{l+l_c} 組の $\{\alpha, cnt, \beta\}$ の集合を C_1 とする。また、$n \leftarrow 1$ とする。

STEP2: C_{2n-1} の $\{\alpha, cnt, \beta\}$ の集合の中で、$E_{\beta \| cnt+n-1}(\alpha) = OTP_{service}^n$ を満たす $\{\alpha, cnt, \beta\}$ の集合を C_{2n} とする。

STEP3: C_{2n} の数が 1 個ならば終了。そうでなければ、次の STEP へ進む。

STEP4: C_{2n} の $\{\alpha, cnt, \beta\}$ の集合の中で、$E_{\alpha \| cnt+n}(\beta) = OTP_{user}^{n+1}$ を満たす $\{\alpha, cnt, \beta\}$ の集合を C_{2n+1} とする。

STEP5: C_{2n+1} の個数が 1 個ならば終了。そうでなければ、$n \leftarrow n+1$ として STEP2 に戻る。

では、平均して何回絞込みを行えば、真の組合せを見つけることが出来るか検討してみる。C_1 のある真でない組合せ $\{\alpha, cnt, \beta\}$ が $C_n (n \geq 2)$ に残っている確率は、$(2^{-l})^{n-1}$ であるから、C_1 のある真でない組合せ $\{\alpha, cnt, \beta\}$ が C_n に残っていない確率は、$1 - 2^{-(n-1)l}$ で与えられる。n 回目までに成功する確率 P_n は、真でないすべての集合 ($= 2^{l+l_c} - 1$ 個) が C_n から外れる確率と同じであるから、

$$P_n = (1 - 2^{-(n-1)l})^{2^{l+l_c}-1}$$

となる。P_n を用いると n 回目に成功する確率は、$P_n - P_{n-1}$ と表せるから、成功までの平均回数は、

$$\text{平均回数} = \sum_{n=2}^{\infty} n(P_n - P_{n-1})$$

となる。必要な盗聴回数は成功までの平均回数と同じである。

平均計算量は、真の組合せを除いて C_1 の導出に $2^{l+l_c}-1$ 回、$C_n(n \geq 2)$ の導出に $(2^{l+l_c}-1)2^{-(n-2)l}$ 回計算が平均して必要であることから、

$$\begin{aligned} \text{平均計算量} &= (2^{l+l_c}-1)(1+\sum_{n=0}^{\infty} 2^{-nl}) + \text{平均回数} \\ &= (2^{l+l_c}-1)(1+\frac{1}{1-2^{-l}}) + \text{平均回数} \end{aligned}$$

で与えられる。なりすましは多数回可能である。

4.2 SSL/TLS 認証プロトコルの安全性

本節では、PKI を用いた認証プロトコルである SSL/TLS 認証プロトコルの安全性について考察する。

公開鍵暗号として RSA を用いる場合、現在知られている最も効率のよい攻撃方法は公開鍵の法となる合成数 $n = pq$ を素因数分解して秘密鍵を求めるという方法である [3]。

そこで攻撃者は秘密鍵を入手しようとする。CA の公開鍵は公開されているので盗聴をする必要はない。また、ユーザ・サービス提供者の公開鍵は、彼らの通信を 1 回盗聴することにより公開鍵証明書を手に入れ、これを CA の公開鍵で復号化することによって得ることができる。公開鍵を得た後は、上記の素因数分解による攻撃法により秘密鍵を求める。ユーザやサービス提供者は、自分の秘密鍵を自分に繋がっている全回線 $N-1$ に使用しているので、対象リンク数は $N-1$ となる。また、CA の秘密鍵は全てのユーザ・サービス提供者における全ての回線 ${}_NC_2 = N(N-1)/2$ において用いられているので、対象リンク数は、$N(N-1)/2$ となる。

なお、CA やユーザ・サービス提供者の秘密鍵解析による攻撃法の成功確率は 1 であり、なりすましは多数回可能である。

4.3 両認証プロトコルの安全性の比較

PID を用いた認証プロトコルと SSL/TLS 認証プロトコルの両認証プロトコルの安全性を実際にパラメータを代入して検討する。表 1 にその結果を示す。ただし、PID を用いた認証プロトコルにおいては、$l = 128$, $l_c = 64$ とし、暗号関数として AES を用いるものとする。また、SSL/TLS 認証プロトコルにおいては暗号方式としては RSA を用いるものとし、ユーザの鍵長を 1024bit、CA の鍵長を 2048bit とする。なお、素因数分解に必要な計算量は文献 [5] から引用した。

種類	攻撃法	安全性 1:攻撃の抑止				
		安全性 2:攻撃への耐性			安全性 3:被害最小化	
		計算量 [MIPS 年]	盗聴回数	成功確率	対象リンク数	なりすまし可能回数
PID	A	0	0	2^{-128}	1	1
	B	0	2^{64}	1	1	多数回
	C	$8.7*10^{47}$	3	1	1	多数回
SSL	C	$3*10^{11}$	1	1	N-1	多数回
	C	$1*10^{21}$	0	1	N(N-1)/2	多数回

表 1: 認証プロトコルの安全性の比較

表 1 の結果から、PID を用いた認証プロトコルは、攻撃を行うための計算量が SSL/TLS 認証プロトコルよりも多く必要であること (攻撃への耐性が大) がわかる。また、攻撃が成功してしまった場合に被害を受けるリンク数は、PID を用いた認証プロトコルの方が SSL/TLS 認証プロトコルよりも少なくて済む (被害の最小化) こともわかる。

さらに、被害を最小化することは攻撃の抑止にもつながることから、PID を用いた認証プロトコルの方が SSL/TLS 認証プロトコルに比べて安全性を高くすることができると分かった。

5 おわりに

本論文では、まず認証プロトコルの安全性評価の方法について、従来から用いられている**攻撃への耐性**の観点のみでなく、**攻撃の抑止**、**被害の最小化**といった観点から安全性評価を行うために必要な考察を行った。そして、攻撃を抑止する観点から、どのような指標を安全性評価指標として用いるべきかを**期待効用最大化理論**を用いて明らかにした。続いて、PID を用いた認証プロトコルと PKI を用いた認証プロトコルである SSL/TLS の安全性の考察をした後、両者の安全性の比較を行った。その結果、我々の提案する PID を用いた認証プロトコルは、PKI を用いた SSL/TLS 認証プロトコルに比べてなりすましの脅威に対して安全性が高くすることが可能であると分かった。

今後の課題として、今回想定しなかった各種攻撃に対する PID を用いた認証プロトコルの安全性の評価を行っていく必要があると考えられる。また、安全性の観点のみでなく、社会システムの構築や運営に必要なコストまで含めた総合的な評価を行い、PID を用いた認証プロトコルが、SSL/TLS 認証プロトコルよりも総合的な評価で優れていることを示していきたいと考えている。

謝辞

本研究をするにあたって様々な角度から指摘を下さった九州大学システム LSI 研究センターの納富貞嘉研究員、安浦/村上/松永研究室の諸氏に感謝します。なお本研究は、文部省科学研究費補助金学術創成研究「社会基盤を構築するためのシステム LSI 設計手法の研究」(14GS0218) による。

参考文献

[1] 浜崎陽一郎, 安浦寛人,“PID を用いた安全な社会システムの構想”, DICOMO2002 シンポジウム論文集 pp.535-538 , 2002 年 7 月

[2] 浜崎陽一郎, 安浦寛人,“PID を用いた安全な社会システムの構想”, 九州大学大学院システム情報科学紀要 第 7 巻第 2 号 pp.139-148, 2002 年 9 月

[3] 情報通信セキュリティ技術研究開発プロジェクト,“共通鍵ブロック暗号の選択／設計／評価に関するドキュメント”, 通信・放送協会, http://www.shiba.tao.go.jp/kenkyu/yokohama/guidebook.pdf, 2000 年 6 月

[4] 武隈慎一,“新経済学ライブラリ 4 — ミクロ経済学”, 新世社, 1989 年 11 月

[5] 電子商取引実証推進協議会セキュリティー WG,“暗号利用技術ハンドブック第 2 版”, 電子商取引実証推進協議会, http://www.ecom.or.jp/report/wg24/e11-sec3.pdf, 2000 年 3 月