社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2007－MBL－40 (27)
2007－UBI－13 (27)
2007／2／23

追跡不能アクセス制御プロトコルとその実装

申吉 浩[†] 和田 康[††] 平岡 真樹[††]
前田 勝之[†††] 保黒 政大[†††]

ユーザがドメインを横断して多様なサービスを享受するユビキタス・コンピューティングでは、システムがユーザの行動を追跡することにより、プライバシーに対する脅威が顕在化し、ネットワーク検閲社会を生み出す危険がある。第12回研究会では、匿名性と追跡不能性を満足しながらも、確実にアクセス制御を実行するプロトコルの原理を発表した。本論文では、本プロトコルの安全性について考察し、更に、当プロジェクトで開発したプロトタイプシステムについて報告する。

Unlinkable Access Control Protocol and its Implementation

KILHO SHIN,[†] KOU WADA,[††] MASAKI HIRAOKA,[††]
KATSUYUKI MAEDA[†††] and MASAHIRO HOGURO[†††]

Invasion of privacy will be a serious issue in the ubiquitous computing, where environments and users' portable devices frequently communicate each other without letting the users know it. This paper presents a proposal of protocols that support unlinkability to protect users' privacy. Also, we will provide a brief description of the prototype system that our project developed based on the proposed protocols.

1. はじめに

1.1 ユビキタス情報社会

「ユビキタス情報社会」という言葉が人口に膾炙するようになって久しく、その実現に向けて産学官の取り組みも本格化してきている。市場では、より高機能を追求した携帯電話や携帯端末が続々と導入され、商用のモバイル・ネットワーク環境も急速に整備されつつある。

移動するコンピュータと環境に埋め込まれたコンピュータとの相互作用としてユビキタスコンピューティングを捉えた場合、最重要のキーワードは「シームレス（seamless）」である。環境側のコンピュータは、その所属するドメインに依存して、運用ポリシー、機器構成、ネットワーク構成、サービス種別等が異なる。ユーザがドメインからドメインへと移動した場合にも、携行するコンピュータのコンフィギュレーションやデバイスの変更をユーザに強制することなく、コンピュータ間の相互作用を保証し、サービスをシームレスに提供し続けることができること、これがユビキタスコンピューティングの最も基本的な要件である。

サービスのシームレスな提供は、ユーザに大きな利便を提供する一方、プライバシーに対して深刻な脅威となり得る両刃の剣でもある。サービスのシームレスな提供は、サービスの提供者の側から見れば、シームレスなアクセス制御を意味する。現行のアクセス制御技術では、個人の身許の認証を前提とすることが通常であり、そのため、ユーザのプライバシーは否応無く露出せざるを得ない。しかも、商業的であれ公共的であれ、適正な提供のためにアクセス制御を必要としないサービスは存在しないといってよいのである。

このように、ユビキタス情報社会では、サービスや情報資源の「安全」の観点から、アクセス制御そのものもシームレス、透過的、統合的、広範囲に行われることとなるが、これは個人のプライバシーにとっての「安全」とは相反するのは明らかである。収集された個人情報はそれこそ「シームレス」にシステムによって共有される危険があるからである。

1.2 匿名性と追跡不能

前節で述べたように、プライバシーの保護なしでは、ユビキタス情報社会は検閲社会に陥る危険性が高い。プライバシーの問題は人々の中心的な関心であるという調査報告もある[2),13)]。一般に、アクセス制御における

† *Rules* 東京大学先端科学技術研究センター
RCAST, The University of Tokyo
†† *Rules* 株式会社ソルコム
SOLCOM Co., Ltd.
††† *Rules* 株式会社ディー・ディー・エス
DDS Inc.

プライバシー保護の概念として、匿名性（Anonymity）と追跡不能性（Unlinkability）の二つが重要である。

匿名性をサポートするアクセス制御は、サービスへのアクセスに際して、身許を明らかにすることをユーザに求めない。一方、追跡不能性は、匿名性を更に進めた概念である。単に個々のアクセスが匿名で行われることを要求するだけではなく、2つの独立したアクセスが同一のユーザによるという事実さえも隠蔽されることを要求する。例えば、匿名性を実現する手段としては仮名（Pseudonym）の利用が考えられるが、一連のアクセスイベントが同一のユーザによって行われた事実を隠蔽することはできない。アクセス制御が、個々のアクセスイベントにおける匿名性のみをサポートし、アクセスイベントの追跡を許すとすると、実際にはユーザの匿名性すらも侵害される危険がなお残る。アクセスのパターンから個人を特定できるかも知れないし、また、特定のアクセスイベントにおいて個人が特定された場合、それを手掛りに、芋蔓的に他のアクセスイベントにおける匿名性が破られる恐れもある。

このように、アクセス制御におけるプライバシー保護に完全を求める場合、追跡に利用可能な情報がユーザの手許から一切漏洩することのない、絶対的な追跡不能性を要件とするのが正しい。

一方、サービスの保護、或いは、社会の安全の観点から、匿名性や追跡不能性を優先することが困難な場合があることは、前節でも述べた。戸籍の閲覧のために身分証の提示を求めることは防犯上合理的であり、また、米国の公安当局による通信の傍受はテロの予防に効果をあげているとされる。同様に、個人の観点からも、プライバシーの完全な保護が、必ずしも、金科玉条であるわけではなく、「プライバシーとパブリシティの境界はいかにあるべきか」という問いかけに対して応えなければならない。

2. Consensual Disclosure

本論文の主たる研究テーマは、ユビキタス情報社会におけるプライバシーに対する要件を明確にし、かつ、その要件をサポートするアクセス制御方式を提案することであり、当然、1.2で述べたプライバシーとパブリシティーの境界に関する問いへの回答も含まれる。

本論文では、ユビキタス情報社会においてはドメインを横断するアクセス制御インフラストラクチャが提供され、プライバシーとパブリシティの境界に関しては、以下の条件を満たすべきであると主張する。

- アクセスのための認証が透過的かつシームレスに実行される場合には、インフラストラクチャはアクセスが絶対的に追跡不能であることを保証する。
- アクセスの追跡を可能とする情報がユーザの端末からインフラストラクチャを経由して開示される場合には、ユーザの明示的な同意を必須とする。また、インフラストラクチャを経由して開示される追跡情報は必要最小限とし、付加的な情報が必要な場合にはアプリケーションが独自に対応する。

本論文では、プライバシーとパブリシティの境界に関する上記の考え方を、**Consensual Disclosure** と名付け、ユビキタス情報社会におけるプライバシーの基本原則として強く主張するとともに、Consensual Disclosureを機能としてサポートするアクセス制御インフラストラクチャのための技術を提案することを目的とする。

最後に、本研究は、経済産業省商務政策局「平成17年度新世代情報セキュリティ研究開発事業（平成17・11・25財情第2号）」及び「平成18年度新世代情報セキュリティ研究開発事業」の研究として行われたものであることを附記する。

3. 関連技術

3.1 下位通信層における追跡不能性

本論文では、アプリケーション層における追跡不能性をテーマとするが、ここではセッション(IP)層以下における追跡不能性について述べる。

3.1.1 仮名 (pseudonym) 通信

仮名アドレスを用いた追跡不能通信とは、ユーザが動的に選択したアドレスを利用することで、追跡不能性を実現しようとする通信方式であり、赤外線通信やスマートカードにおいて実現性がある。

IrDA (Infrared Data Association) の通信規約である IrLAP (Infrared Link Access Protocol)[11] や、NFC (Near Field Communication) の通信規約である ISO/IEC 18092[12] では、アドレスの衝突を回避するメカニズム (address collision avoidance mechanisms) を規定しているため、動的アドレスによる演繹可能な追跡不能性を実現することが可能となる。

この手法は、衝突回避メカニズムが存在しない IP 通信層やデータリンク層にも適用できる可能性はあるが、アドレスの衝突の問題を上位のアプリケーションで解決しなければならない。例えば、仮名に利用できる MAC アドレスの有効長は 3 バイトであるので、Birthday Problem の理論から、n ユーザの間で衝突が発生する確率は約 $1 - e^{-n(n-1)/2^{13}}$ となる。これは、ネットワークに 581 以上のデバイス (NIC 等) が同時に存在すると、$\frac{1}{100}$ より大きい危険率で衝突が発生することを意味し、また、危険率を $\frac{1}{10}$ まで許容しても、

許容されるデバイス数は 1,880 程度となる。

3.1.2 ブロードキャストを利用した通信方式

ブロードキャスト通信も、追跡不能性を実現する目的に利用することができる。例えば、デバイスは、パケットを送信する際、ブロードキャスト・アドレス (IP アドレスでは 255.255.255.255、MAC アドレスでは FF:FF:FF:FF:FF:FF:FF:FF) をパケットの Source フィールドに指定し、サーバブロードキャストで返信を行う。デバイスは、ブロードキャストされたパケットから、P が自分宛のパケットを選択できるできる必要があるとともに、ブロードキャスト通信では V は P と TCP セッションを構成できないので、通信の信頼性 (*e.g.* reliability, in-order delivery) をサポートする必要がある。

3.1.3 システムの安全性に依存する仮名通信方式

インターネット・プロキシにより IP アドレスを隠蔽したウェブアクセスが可能であることは知られている。また、NAT 或いは NATP をサポートするルータは、プライベート IP アドレスとルータのグローバル IP アドレスの変換を行う。このように、インターネット・プロキシやある種のルータは、通信において仮名アドレスによる通信を提供する。ただし、実際のユーザの追跡不能性は、プロキシとルータの信頼性に依存している。

3.2 グループ署名

グループ署名は、以下の特徴を備えた署名方式である。

(1) グループのメンバーはグループを代表して、任意に署名を生成することができる。

(2) グループの公開検証鍵にアクセスできる誰でもが署名を検証することが可能であるが、検証により署名者の身許が明らかになることはない。

(3) グループの管理者 (Trusted Group Authority, TGA) は、署名から署名者を特定することが可能であり、紛争等、必要に応じて署名者の身許を特定する。

更に、Ateniese、Camenisch、Joye と Tsudik [1] による方式は、証明可能な安全性を有するグループ署名方式としては従前の方式に比較して効率的であり、日本においてもこの方式をベースに携帯電話による匿名注文システムを開発している[16]。

グループ署名をユビキタスアクセス制御に適用する上での最も重大な課題は、計算量が大きい点にある。実際、Iachello 等は、Camenisch 等が提案した Anonymous Credential システム[6),7)] を評価して、ユビキタスコンピューティングに適用するには不適当であると結論し、安全性を犠牲にしても、暗号処理を含まない単純なシステムを提案している[10]。

この観点から、Ateniese 等による提案[1] 以降、グループ署名の計算量を軽減し、計算効率を向上させようとする試みがなされてきた[3)~5),9),14),15)]。表 2 に、佐古等[17] によって報告された各グループ署名方式の計算量の比較を示す。比較に当たっては、楕円曲線上のスカラー倍演算の実行回数に換算してある。

表 1 下位通信層における追跡不能
Table 1 Unlinkability in the lower layers

	Deducible Unlinkability	Trusted Unlinkability
IrDA NFC Bluetooth 非接触 IC カード	動的アドレシングによる仮名通信 (衝突は ACAM により回避)	
MAC	動的アドレシングによる仮名通信 (衝突はアプリケーションで対処) Broadcast による匿名通信	
IP	Boadcast による匿名通信 (アプリケーション層で信頼性を保証)	Internet Proxy、NAT, NATP による匿名通信

表 2 グループ署名の計算量の比較[17]

アルゴリズム	署名	検証	合計
Ateniese-Camenisch-Joyce-Tsudik[1]	2700	2475	5175
Boneh-Boyen-Shacham[3]	20	33	53
Camenisch-Lysyanskaya[5]	42	69	111
Camenisch-Groth[4]	28	38	66
Teranishi[15]	65	86	151
Nguyen-Safavi-Naini[14]	38	37	75
Furukawa-Imai[9]	19	39	49

(楕円曲線上のスカラー倍演算の実行回数に換算)

4. 本論文の狙い

本論文の主要な研究テーマのひとつは、追跡不能性と Consensual Disclosure とを実現し、かつ、グループ署名に比較して少ない計算量で実行が可能であるユビキタスアクセス制御方式を提案する点にある。

5. プロトコルの提案と安全性の証明

5.1 プロトコルの提案

本論文で提案するプロトコルでは、以下のプレイヤーを仮定する。

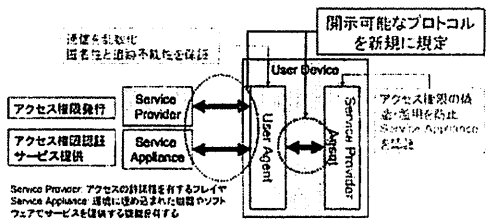
Service Provider (*SP*) サービスに対するアクセス権限を発行が許される唯一の権限発行者

Service Appliance (*SA*) *SP* の委託を受けて、サービ

スをユーザに直接提供する権限検証者

Service Provider Agent (*SpA*) ユーザデバイスに常駐する Service Provider のエージェントであり、耐タンパー処理装置として実装

User Agent (*UA*) ユーザのエージェントであり、*SpA* が追跡情報を漏洩しないよう、*SpA* からの出力の乱数化を行う



Access ID *aid* は *SP* がユーザ (*UA*) に発行するデータであり、*SP* がユーザに許諾するアクセス権を表現する。Access ID (*aid*) は、*SP* と *SpA* との通信を介して、以下の手順で生成される。

(1) *SpA* と *SP* は、例えば、MQV 鍵交換プロトコルを介して、k を秘密裏に共有する。k は一様に分布する乱数である。

(2) *SP* は、*aid* を下式を満たすように生成する。

$$\sigma \equiv aid + k \bmod n_S$$

aid はユーザに発行されたアクセス権限の識別子の役割を果たす。

UA は、*aid* を秘密に保存しておいて、*SA* には、下式によって暗号化された *anm* をアクセス権限の証拠として提示する。匿名化された *anm* は、*UA* が生成する秘密の乱数 $\rho \in [0, n_S)$ により、σ を二重にマスクした値となる。

$$anm = aid - \rho \bmod n_S = \sigma - k - \rho \bmod n_S$$

追跡情報を開示しない基本的な追跡不能権利認証プロトコルは Unlink-Verify(図 1)、Consensual Disclosure に基づいて ρ、即ち、*aid* を開示する追跡可能権利認証プロトコルは Link-Verify(図 2) で与えられる。

5.2 安全性の証明

Unlink-Verify において、*UA* 及び *SA* は、以下により r' 及び r の値を検証する。

$$\begin{aligned} r'G_S &\stackrel{G_S}{=} \big(\omega(\pi(W)|c|*)\mu(k,*) + w' + w''\big)G_S \\ &\stackrel{G_S}{=} \omega(\pi(W)|c|*)\big(\sigma - (\sigma - \mu(k,*))\big)G_S + W \\ &\stackrel{G_S}{=} \omega(\pi(W)|c|*)\,(S - aid \cdot G_S) + W \end{aligned}$$

$$\begin{aligned} rG_S &\stackrel{G_S}{=} \big(\omega(\pi(W)|c|*)(\mu(k,*) + \rho) + w' + w''\big)G_S \\ &\stackrel{G_S}{=} \omega(\pi(W)|c|*)\big(\sigma - (\sigma - \mu(k,*) - \rho\big)G_S + W \\ &\stackrel{G_S}{=} \omega(\pi(W)|c|*)\,(S - anm \cdot G_S) + W \end{aligned}$$

一方、Unlink-Verify においては、*UA* は下式をあわせて検証する。

$$\begin{aligned} & x(S - anm \cdot G_S) + y \cdot \pi^{-1}(e_P \oplus \rho) \\ &\stackrel{G_S}{=} x(\mu(k,*) + \rho)G_S + y(\mu(k,*) + \rho)Q \\ &\stackrel{G_S}{=} (\mu(k,*) + \rho)(xG_S + yQ) \\ &\stackrel{G_S}{=} V \end{aligned}$$

不正な *UA* が排除される、所謂、プロトコルの健全性は以下の定理により証明される。

定理 1. *Unlink-Verify* 及び *Link-Verify* は健全である。

(証明のスケッチ) Fiat-Shamir heuristic[8] に従えば、*UA* が出力する (W, r) をメッセージ $c \mid *$ に対する電子署名と見做すことができ、同様に、*SpA* の出力も $c \mid *$ への署名となる。署名の検証は、公開鍵 $S - aid \cdot G_S$、或いは、公開鍵 $S - anm \cdot G_S$ による。このような見做しのもとで、Unlink-Verify 及び Link-Verify の健全性は、以下の Claim で表現することができる。

Claim . *SA* が *UA* が提出した電子署名 (W, r) の検証に成功するならば、無視しえる確率を除いて、*UA* にとって *Authentic* な *SpA* が少なくともひとつ存在して、同一のメッセージ $c \mid *$ に対して署名を生成している。

上記の Claim は、ベースとなる電子署名方式の選択メッセージ攻撃 (adaptive message attack) のもとでの偽造不能性 (non-forgeability) に帰着する。□

一方、Unlink-Verify 及び Link-Verify の追跡不能性は以下の定理による。

定理 2. *Unlink-Verify* は追跡不能である。

(証明のスケッチ) 次の Claim が成立する。

Claim . *UA* による *SA* への出力 (anm, W, r) は、他のいかなる事象とも独立に、

$D_{c,*} = \{(x, Y, z) \mid zG_S \stackrel{G_S}{=} \omega(\pi(Y) \mid c \mid *)(S - xG_S) + Y\}$

上で一様に分布する。

Claim から定理が導かれることは、以下のように分かる。$D_{c,*}$ の定義は S と $(c, *)$ のみに依存し、*aid* には依存しない。即ち、*UA* が正しい処理を行う限りにおいては、*aid* の値にも認証イベントにも依存せずに、(anm, W, r) は独立に一様に分布することから、

SA		UA		SpA
			$\xleftarrow{W'}$	$w' \in_R [0, n_S)$, $W' \overset{\mathcal{G}_S}{=} w'G_S$
		$\rho, w'' \in_R [0, n_S)$ $anm = aid - \rho \bmod n_S$ $W \overset{\mathcal{G}_S}{=} w''G_S + W'$		
	$\xleftarrow{W, anm}$			
$c \in_R [0, n_S)$	$\xleftarrow{c}$	$\xrightarrow{c, w''}$		$W \overset{\mathcal{G}_S}{=} w''G_S + W'$ $a = \omega(\pi(W) \mid c)$
			$\xleftarrow{r}$	$r' = ak + w' + w'' \bmod n_S$
		Unless (W, r') is valid, abort the session. $a = \omega(\pi(W) \mid c)$ $r = r' + a\rho \bmod n_S$		
Unless (W, r) is valid, abort.	$\xleftarrow{r}$			

図 1　追跡不能権利認証プロトコル: Unlink-Verify

SA		UA		SpA
				$w', q' \in_R [0, n_S)$
			$\xleftarrow{W', Q'}$	$W' \overset{\mathcal{G}_S}{=} w'G_S$, $Q' \overset{\mathcal{G}_S}{=} q'G_S$
		$\rho, w'', q'', x, y \in_R [0, n_S)$ $anm = aid - \rho \bmod n_S$ $W \overset{\mathcal{G}_S}{=} w''G_S + W'$, $Q \overset{\mathcal{G}_S}{=} q''G_S + Q'$ $U \overset{\mathcal{G}_S}{=} xG_S + yQ$		
	$\xleftarrow{anm, W}$			
$c \in_R [0, n_S)$	$\xleftarrow{c}$		$\xrightarrow{c, w'', q'', U, \rho}$	$W \overset{\mathcal{G}_S}{=} w''G_S + W'$ $a = \omega(\pi(W) \mid c)$ $r = a(k + \rho) + w' + w'' \bmod n_S$ $Q \overset{\mathcal{G}_S}{=} q''G_S + Q'$ $e_P = \pi((k + \rho)Q) \oplus \rho$ $V \overset{\mathcal{G}_S}{=} (k + \rho)U$ $b = \omega(r \mid e_P \mid \pi(Q))$
			$\xleftarrow{r, s, e_P, V}$	$s = b(k + \rho) + q' + q'' \bmod n_S$
		Unless W, r, Q, s, e_P, V are valid, abort the session.		
Unless (W, r, Q, s, e_P) is valid, abort.	$\xleftarrow{r, Q, s, e_P}$			

図 2　追跡可能権利認証プロトコル: Link-Verify

(anm, W, r) は一切の追跡情報を含み得ない。□

(Q, e_P) は公開鍵 $S - anm \cdot G_S$ による ρ の ElGamal 暗号であるので、σ を知っている *SP* にのみ復号可能である。従って、Link-Verify が Consensual Disclosure をサポートしていることを示すためには、以下の 2 項目を示すことが必要かつ十分である。

- *SpA* が不正であっても、*UASP* に対して *aid* のみを開示し、他のエンティティには一切の追跡情報を開示しない。
- *UA* が不正であっても、*SP* は *UA* が認証に用いた *aid* を特定することが可能である。

定理 3. *Link-Verify* において、*UA* は *SP* に対して *aid* のみを開示し、他のエンティティには一切の追跡情報を開示しない。

(証明のスケッチ) 正しい *UA* の出力 (anm, W, r, Q, s, e_P) において、(anm, W, r, Q, s) は、S にのみ依存して定義される曲面上を一様に分布する。つまり、e_P 及び e_P と関連するデータのみが追跡性に影響するので、*UA* は (anm, Q, e_P) のみを出力すると仮定しても一般性は失われない。今、以下の性質を満足する多項式時間の攻撃者 A を考える。

- 事前に $(\mathcal{G}_S, G_S, n_S, S)$ の知識を有しているが、σ に関する知識はない (A は *SP* と異なる)。
- 任意に *UA* にアクセスして出力を得ることができる。
- 入力 $(x, Y, z) \in [0, n_S) \times \mathcal{G}_S \times \{0, 1\}^k$ に対して、0 または 1 を出力する。

更に、公平なコインを振り、表がでれば *UA* にアク

セスして

$$aid = anm + \pi(\sigma Y) \oplus z \bmod n_S$$

を満足する (x, Y, z) を取得して A に入力し、裏がでれば一様にランダムに $(x, Y, z) \in_R [0, n_S) \times \mathcal{G}_S \times \{0,1\}^k$ を生成して A に入力する。

SP 以外のエンティティに対する追跡不能性は、次の Claim から導かれる。

Claim . 下式で定義される A の優位性 Adv^A は無視しえる程小さい。

$$\mathrm{Adv}^A = \Pr[A \to 1 | (x, Y, z) \leftarrow UA] - \Pr[A \to 1 | (x, Y, z) \in_R [0, n_S) \times \mathcal{G}_S \times \{0,1\}^k]$$

A をオラクルとして利用し、Decisional Diffie-Hellman 問題を解く多項式時間チューリング機械 $\tilde{P}$ が存在し、$\tilde{P}$ の優位性を

$$\mathrm{Adv}^{\tilde{P}} = \Pr[\tilde{P} \to 1 | \mathrm{mult}_{G_S} S = \mathrm{mult}_Q R] - \Pr[\tilde{P} \to 1 | \mathrm{mult}_{G_S} S \neq \mathrm{mult}_Q R(x, Y, z)]$$

で定義するとき、下式が成り立つ。

$$\mathrm{Adv}^A = \mathrm{Adv}^{\tilde{P}}$$

ベースの群 $\mathcal{G}$ を、Decisional Diffie-Hellman 問題が困難な群ととることにより、有意な優位性を有する A が存在しないことが分かる。□

計算量の評価は以下である。

プロトコル	署名	検証	合計
Unlink-Verify	5	2	7
Link-Verify	17	4	21

† 楕円曲線上のスカラー倍演算の実行回数に換算

6. プロトタイプ

プロトコルに対する評価用プロトタイプを開発した。この節では、特に、メッセージ規定、セキュア OS への組み込み方法、イメージとしてのアプリケーション例の 3 点について述べる。

6.1 Ubiquitous Access Control Message Layer

USCML は、Service Provider、Service Provider Agent、User Agent、及び、Service Appliance の間で交換されるメッセージに関して、構文・意味 (セマンティクス)・符号化方式を厳密に定義することで、ドメインを横断したシームレスなアクセス制御を可能とする。

前述したように、ユビキタスコンピューティングでは、下位通信層における通信手段はドメインに依存し、無線 LAN、赤外線通信、Bluetooth、非接触 IC カード、NFC 等、複数の選択肢が存在するのみならず、将来に新しい方式が実用化される蓋然性も高い。サービスへのシームレスなアクセスを実現するためには、アクセス制御のプロトコルは、下位通信層の手段に依存しないように設計されるべきである。更に、衝突の処理、通信の信頼性の保証等、アクセス制御プロトコルが満足しなければならない要件も存在する。

USCML では、位通信層との接続性の観点から、以下の性質を満足するように設計する。

- 下位通信層に通信の信頼性が期待できないケースであっても、メッセージを検査することにより、パケットの部分的喪失や順序の狂いを検知し、再送を要求できること。
- 異なるユーザに対するメッセージが混在し、通信が輻輳する場合においても、メッセージに記載された情報から自分宛のメッセージを確実に選択できること。
- 更に、複数のセッションが存在する場合においても、メッセージに記載された情報から、セッション毎に仕分けができること。

6.2 セキュア OS への組み込み

ここでは、サーバは攻撃を受ける危険が大きいので、セキュリティ機能が強固で、きめ細かく実装できる SELinux を、ユーザ端末は LinuxOS のカーネル 2.4 に対応可能な LIDS を以下のように実装し、システムを高セキュア化する。

サーバには、SELinux における MAC、TE、ドメイン遷移、RBAC 等の機能を利用してシステム管理者、セキュリティ管理者、ユーザへの最小限の権限付与、プロセス、ファイル、ディレクトリ、子プロセスなどに綿密にアクセス制御機能設定し、攻撃への耐性強化、被害の拡大防止を図る。すなわち、SA,SP とも Web サーバ (Apache) が走り、データベース (PostgreSQL) を利用し、プロトコルモジュール (SA, SP) を夫々走らせる。構成が複雑であるため、高いセキュリティ性能を得るために、複数のシステム管理者と多数の端末ユーザに権限を細分化して最小権限を与え、攻撃耐性を強化すると共に、システム関係者がアクセス可能なプロセス、データ、通信ポートの等の資源や起動可能プロセスなどをポリシーファイルに基づいて最低限の範囲に利用限定して、被害の拡大を防止する。

ユーザ端末に実装する LIDS というセキュア OS は、Linux カーネルに LSM (Linux Security Module) によるセキュリティ拡張を施す点では SELinux と同様であるが、2 種類のカーネル (2.4 系/2.6 系) の両方に対応し、それぞれ 1 系、2 系と呼んでいる。一般に、組込み系機器の Linux の場合、大多数は 2.4 系が利用されており、ユーザ端末 (Zaurus) においてもカーネルは 2.4 が搭載されている。このため 1 系 LIDS を用いる。

なお、2系の方が機能は豊富であるが、LIDSコミュニティでは組込み系への利用拡大を目指して1系へのバックポーティングも積極的に進めている。LIDSを利用したセキュリティ設定では、端末内にはUA、httpdのプロセスが走行するが、各プロセスに与える入出力ファイル、通信ポートなどの資源利用の範囲と4種類(DENY,READONLY,APPEND,WRITE)のポリシーをアクセス制御リストに記載する。さらに、ケイパビリティ(細分化された個別の権限付与)機能によりプロセス動作を強制的に最小限に指定し、ログファイルを強制取得状態にした上でカーネル封印を行なう。

6.3 アプリケーション例

これまで、ユビキタスネットワークは多くの利点を有する反面、個人の行動の追跡の危険性があることを述べ、その対応として、「追跡不能性」を含むプライバシーの確保の認証プロトコル(以下、匿名プロトコルと略記)を述べた。買物を例にとると、従来から我々は現金で買物をする場合、匿名で取引できる。しかし、商品がかさ張った物の場合、ショップに配達を依頼する必要が生じ、この時はショップに送り先を明らかにしなければならない。電子モールで買物をする場合も同様で、電子マネーを匿名化した場合でも商品配送を委託する場合、相手に送り先を知らせることが必要で、この場合、顕名取引となる。勿論、ユーザがショップを訪問して、直接商品を受取れば、電子マネーで支払っても追跡不能の匿名取引が可能である。以上のことを検証するために、顕名取引と匿名取引の応用例として、前者は電子モール、後者はジューク・ボックスで有料の音楽を聴くという例をシステム化した。

ここで、図3のプロトタイプ・システム構成図を例に説明する。本図は紙面の都合で、電子モールとジューク・ボックスの両方をまとめた説明図になっている。また、ユーザが商品購入の権利(以下、ポイントと略記)を入手する手順も省略しているので、予めポイントを購入済であるとご理解願いたい。その代金支払いが端末ユーザからSPへ行なわれることのみが図には示されている。処理手順は以下の通りである。

1) 電子モール場合:携帯端末から商品選択し、商品送付先を通知する(顕名取引)

(1) ユーザは端末から電子モール(サービスエージェント(SA))のWebサーバへhttpにより商品を問合わせる。SAは、ユーザが既に持っているポイント数を本匿名プロトコルで問合わせ、そのポイント数をユーザ端末に商品と共に表示する。

(2) ユーザは買いたい商品をポイント数の範囲内で選ぶ。

(3) ユーザは配達を依頼する場合は、そのアドレス(住所情報)をSAへ伝えねばならない。そのために、SAがサービスプロバイダ(SP)から住所情報を取得することを承認し、SAはSPから本匿名プロトコルで問合わせて得た住所情報をWeb(https)上に表示する。

(4) 希望の配達先がユーザの住所情報と異なるときは、端末から配送先を書込んで注文を完了する。

(5) SAは注文を受理した結果情報、差引いたポイント数などの処理結果を端末に表示すると共に、匿名プロトコルにより、ユーザ端末のSDカード内のポイントの減数を行なう。

2) ジューク・ボックスの場合:ジューク・ボックス内の音楽コンテンツを直接サーバ上で指定し、匿名取引で決済し、直接音楽を聴く。すなわち、図中のSAをジューク・ボックスに見立てた場合には配送先指定手続きは不要で、この場合、上記の(3)、(4)の手順を省いたシーケンスにより実施することとなる。

実装に当たっては、電子モール、ジューク・ボックスともWebサーバを包含するサーバマシンへ実装し、携帯端末機能は、PDAおよび通常のPCに実装した。アプリケーションを組込むオープン性と商品検索のための画面サイズを考慮してPDAを選択したが、携帯端末は普及促進の点で、将来は携帯電話への実装を進めたい。開発効率を上げ、アプリケーションを普及させたために、オープン性を意識して、Linux、PHP、PostgreSQLなどGPLソフトを利用した。

7. 結　　論

追跡不能性を有するアクセス制御プロトコルを提案し、その安全性を議論した。更に、提案するプロトコルのプロトタイプについて述べた。

参 考 文 献

1) G.Ateniese, J.Camenisch, M.Joye, and G.Tsudik. A practical and provably secure coalition-resistant group signature scheme. *Lecture Notes in Computer Science*, 1880:255 – 270, 2000.

2) L.Barkhuus and A.Dey. Location-based services for mobile telephony: a study of users' privacy concerns. In *INTERACT 2003, 9th IFIP TC13 International Conference on Human-Computer Interface*, 2003.

3) D.Boneh, X.Boyen, and H.Shacham. Short group signatures. In *Proceedings of Crypto '04*, 2004.

4) J.Camenisch and J.Groth. Group signatures: better efficiency and new theoretical aspects, 2004.

5) J. Camenisch and A. Lysyanskaya. Signature schemes and anonymous credentials from bilinear

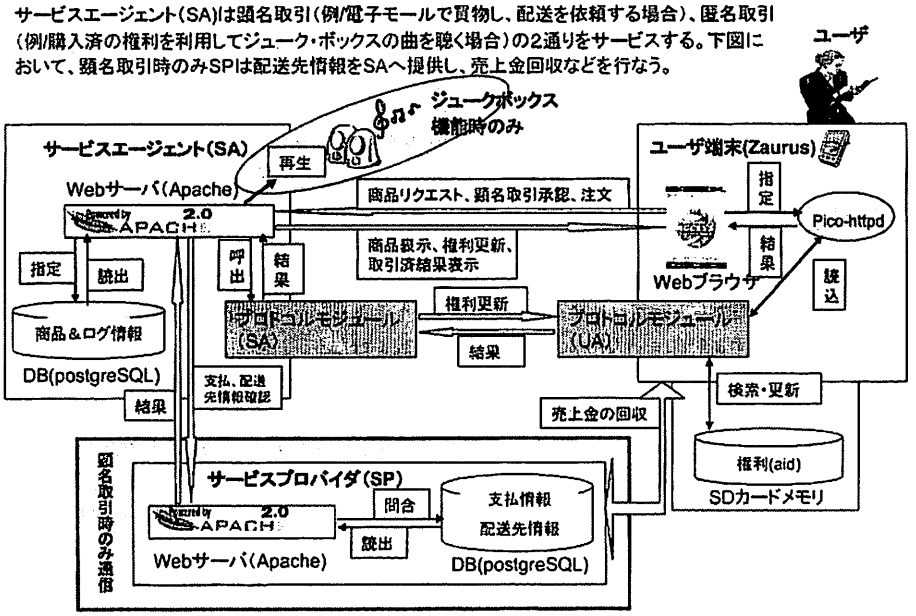


図 3 取引システム

maps. In *Proceedings of Crypto '04*, 2004.

6) Jan Camenisch and ElsVan Herreweghen. Design and implementation of the idemix anonymous credential system. In *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*, pages 21–30, New York, NY, USA, 2002. ACM Press.

7) Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *EUROCRYPT*, volume 2045 of *Lecture Notes in Computer Science*, pages 93+, 2001.

8) A.Fiat and A.Shamir. How to prove yourself: Practical solution to identification and signature problems. In *Crypto '86, LNCS 263*, pages 186–194. Springer-Verlag, 1987.

9) J. Furukawa and H. Imai. An efficient group signature scheme from bilinear maps. In *ACISP 2005*, pages 455–467, 2005.

10) G. Iachello and G.D. Abowd. A token-based access control mechanism for automated capture and access systems in ubiquitous computing. GIT Technical Report GIT-GVU-05-06, Georgia Institute of Technology, GVU Center, June 2005.

11) Infrared Data Association. *Infrared Data Association: Serial Infrared Link Access Protocol (IrLAP) Version 1.1*, 1996.

12) International Organization for Standardization. *ISO/IEC 18092-3: Information technology – Telecomunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)*, 2004.

13) Eija Kaasinen. User needs for location-aware mobile services. *Personal Ubiquitous Comput.*, 7(1):70–79, 2003.

14) L.Nguyen and R.Safavi-Naini. Efficient and provably secure trapdoor-free group signature schemes from bilinear pairings. In *Proceedings of AsiaCrypt '04*, pages 372 – 386, 2004.

15) I. Teranishi, J. Furukawa, and K. Sako. *k*-times anonymous authentication. In *Proceedings of AsiaCrypt '04*, pages 308 – 322, 2004.

16) 加藤 岳久, 岡田 光司, and 吉田 琢也. 匿名認証技術とその応用. 東芝レビュー6, 東芝, 2005.

17) 佐古 和恵 米沢 祥子古川 潤. セキュリティとプライバシを両立させる匿名認証技術について. 情報処理, 47(4):410 – 416, April 2006.