様式 C-19

科学研究費補助金研究成果報告書

平成２３年　６月　３日現在

機関番号：３２６９２
研究種目：若手研究（Ｂ）
研究期間：2009～2010
課題番号：２１７００００８
研究課題名（和文）　携帯電話端末を用いたデジタルフォレンジック技術の研究開発

研究課題名（英文）　Research and Development of Technology for Digital Forensics Using Cellular Phones

研究代表者
宇田　隆哉（UDA RYUYA）
東京工科大学・コンピュータサイエンス学部・講師
研究者番号：５０３５０５０９

研究成果の概要（和文）：我が国の携帯電話端末は改竄耐性が高いという特徴を利用し、携帯電話端末上で作成、確認されたデジタル署名を信頼性の根拠としたデジタルフォレンジック技術に関する研究開発を行った。

研究成果の概要（英文）：Technology for digital forensics has been researched and developed on this project by using cellular phones on which digital signatures are generated and verified, having the advantage of high resistance to tampering with cellular phones maid in Japan.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	1,800,000	540,000	2,340,000
２０１０年度	1,600,000	480,000	2,080,000
年度			
年度			
年度			
総　計	3,400,000	1,020,000	4,420,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：ネットワークセキュリティ技術、デジタルフォレンジック

１．研究開始当初の背景

(1)　デジタルフォレンジックの必要性

我が国においては、電子署名及び認証業務に関する法律が 2000 年に施行されて以来、電磁的記録も署名、捺印と同等の法的効力を持つとされてきた。これに伴い、権威ある機関から発行された証明書に関しては、X.509 サイト証明書に代表されるウェブサイトの確認や本人確認などに広くデジタルデータが使用されるようになってきている。しかしながら、改竄や漏洩の脅威にさらされることなく、一般の利用者がデジタル署名を作成することが困難であるため、物理的な署名、捺印の代用としてデジタル署名が一般に利用されることは少ない。

(2)　我が国独自の携帯電話端末

我が国で開発された携帯電話端末は、その仕組みが堅牢であり、改竄耐性が高いとされてきた。また、携帯電話端末のメモリ領域は、一般的なパーソナルコンピュータのものとは異なり仮想マシン上でアプリケーションごとに独立して確保されているため、あるアプリケーションソフトウェアの脆弱性のせいで他のアプリケーションソフトウェアのメモリ領域にアクセスされてしまうことはない仕組みになっている。この性質を利用し、本プロジェクトでは我が国独自の携帯電話端末を電子的な印鑑の母体として利用することを考案した。

２．研究の目的

(1)　現状の問題点

FeliCa の 3DES に代表されるように、従来のセキュリティ技術は第三者に対する情報漏洩対策ばかりが注目され、暗号化通信に力が入れられてきた。その結果、成りすましによる詐欺や組織ぐるみでの証拠隠滅が横行し、現在の社会問題となっている。銀行などのシステムに見られるように、パスワードによる認証が指紋や IC カードに置き換わってもこの状況は変わらない。

(2)　本研究の主眼

本研究の主眼はデジタルフォレンジックにあり、本人が行った作業の否認防止や成りすまし対策を目標としている。そのためには、たとえパスワードであっても組織が管理する個人情報は流出し得る、組織が回収した記録は改竄され得るという前提のもとにシステムを設計せねばならない。

(3)　安全性の根拠

本研究では、個人が所有する秘密鍵を携帯電話端末の外部に出力せず、組織に一括管理させない方式でデジタルフォレンジックを実現する。携帯電話端末のメモリ領域は、パーソナルコンピュータのものとは異なり仮想マシン上でアプリケーションごとに独立して確保されているため、他アプリケーションの脆弱性のせいでコンピュータウイルスなどによる外部からの侵入を許すことはない。

(4)　本研究の意義

今日は、インターネットや ATM での振り込みなど電子機器を使用した詐欺による被害額が大きくなっており、組織ぐるみでの電子データの改竄や隠滅なども問題視されている。携帯電話端末を用いてデジタルフォレンジックを実現することで、そこに一石を投じることは意義が大きいといえる。

３．研究の方法

(1)　オープンソースソフトウェア

携帯電話端末上でデジタル署名の作成、検証を行うプログラムを、一般のプログラマが利用しやすい形式でまとめ、オープンソースソフトウェアとして公開を行った。

(2)　ウェブサイトにおけるデジタルフォレンジック技術

ウェブサイトにおけるデジタルフォレンジック技術として、ＨＴＴＰデーモンがウェブサイトのコンテンツにデジタル署名を施せるソフトウェアの開発を行った。利便性を考慮し、ＨＴＴＰデーモンのモジュールという形式で実装を行った。

４．研究成果

(1)　携帯電話端末におけるデジタル署名

携帯電話端末上でデジタル署名の作成、検証を行うプログラムを作成し、他の研究者もその成果を利用できるよう、オープンソースソフトウェアとしてウェブサイトにて公開を行った。ソースコードについての説明も他の研究者が参照しやすいようにまとめ、ソースコードとともに公開した。公開しているものに関しては、オープンソースソフトウェアの原則に則り、我が国以外の研究者も広く理解可能な言語で記述している。

(2)　携帯電話端末におけるデジタル署名の性能評価

携帯電話端末実機において、どの程度の速度でデジタル署名が作成、検証できるかについて実機による動作試験を行った。その結果を表 1～表 3 に示す。なお、表 1～表 3 は、研究成果のひとつである国際会議の文献②からの抜粋である。

表 1 携帯電話端末における署名時間

機種	平均 (ms)	最大 (ms)	最小 (ms)	標準偏差 (ms)
N06A	695	1265	592	99.0
F01C	209	250	201	5.9
L04B	7443	8568	3979	1478.4
P04B	586	800	555	51.5
F06B	217	371	204	23.1
SH01C	210	251	199	6.1
N02C	168	227	154	10.8
N04B	226	282	214	9.1

表 2 携帯電話端末における署名検証時間

機種	平均 (ms)	最大 (ms)	最小 (ms)	標準偏差 (ms)
N06A	934	1504	741	119.0
F01C	269	358	254	12.3
L04B	9828	11313	5164	2049.6
P04B	779	982	726	59.8
F06B	273	335	259	10.5
SH01C	270	370	254	11.5
N02C	214	245	192	9.5
N04B	290	333	270	11.3

表 3 携帯電話端末における鍵生成時間

機種	平均 (ms)	最大 (ms)	最小 (ms)	標準偏差 (ms)
N06A	732	1240	603	125.7
F01C	217	447	195	32.6
L04B	7696	8947	4053	1442.8
P04B	608	843	552	62.9
F06B	216	466	201	25.5
SH01C	214	497	203	28.9
N02C	171	349	155	20.8
N04B	231	584	214	36.6

表 1 は、携帯電話端末における ECDSA アルゴリズムによるデジタル署名作成時間、表 2 は、携帯電話端末における ECDSA アルゴリズムによるデジタル署名検証時間、表 3 は、携帯電話端末における ECDSA アルゴリズムによる公開鍵と秘密鍵ペアの作成時間である。特定の機種によっては 10 秒ほど時間が掛かる場合もあるが、概ねほぼ全ての機種において 1 秒以内に演算が完了しているため、実用的に問題はない範囲であるといえる。

(3)　ウェブサイトにおけるデジタルフォレンジック技術

従来、ウェブサイトではセキュリティ技術として一般的に X.509 サイト証明書とＨＴＴＰＳによる通信が用いられている。X.509 サイト証明書によりウェブサイトの所有者に対する認証が行われ、ＨＴＴＰＳによりクライアント、サーバ間の通信に対する秘密が守られている。しかしながら、ウェブサイトから発行されたコンテンツに関しては、その内容に関する保証が一切無い。つまり、ウェブサイトの所有者は、ウェブサイトが発行したコンテンツの内容をいつでも否認できる状態にある。そこで、本プロジェクトではウェブサイトにデジタルフォレンジック技術を導入し、ＨＴＴＰデーモンがウェブサイトのコンテンツにデジタル署名を施せるソフトウェアの開発を行った。利便性を考慮し、ＨＴＴＰデーモンのモジュールという形式で実装を行った。前述の携帯電話端末と連携すれば、携帯電話端末から任意のウェブコンテンツに署名することや、携帯電話端末におけるウェブコンテンツ署名内容の確認も可能となる。

(4)　研究成果からの派生プロジェクトとそれらの成果

本プロジェクトは、若手研究（B）という区分で、研究者が代表者のみとなっており研究室単位でのプロジェクトではないため、本研究の直接の成果ではないが、本研究の成果を受けていくつかのプロジェクトが成果を上げている。これは、本プロジェクトの成果を問う上での基本的な考えが、他の研究者がソースコードを広く利用できるようにすることである点にある。最終的には、本研究室のみならず、本プロジェクトの成果が国内外を越えて活用されることを望む。

派生プロジェクトの成果として 2009 年度に国内のシンポジウムにて発表された研究を「５．主な発表論文等」の⑤⑥に記載した。国内のシンポジウムではあるが、下記の発表の内、⑥は優秀論文賞を受賞している。

そして、2010 年 1 月 14 日～1 月 15 日に韓国の水原にて開催された国際会議に、先の DICOMO2009 優秀論文賞を受賞した論文⑥の内容を改善、英訳したものが優秀論文につき査読免除（参加費を支払っているため招待論文ではない）となり、採録になった。それが、「５．主な発表論文等」に記した④である。

また、2010 年度には本プロジェクトから派生した研究が 1 件、情報処理学会のシンポジウムにて発表されたため、「５．主な発表論文等」の②に記載した。

本プロジェクトでは、作成したアプリケーションソフトウェアプログラムソースコードの一部をオープンソースソフトウェアとしてウェブサイトにて一般に公開しているため、他の研究室でも同様の取り組みを行う際に本プロジェクトの成果を利用することが可能である。公開しているものに関しては、オープンソースソフトウェアの原則に則り、我が国以外の研究者も広く理解可能な言語で記述している。我が国独自の携帯電話端末を用いているため、諸外国の研究者にとっては実装に必要な実機が入手困難な場合も想定されるが、通信事業者から実機の挙動をソフトウェアにてエミュレートする環境が無償で提供されている。この環境を利用すれば、諸外国の研究者も、実装用の実機を入手することなく、本研究の成果であるオープンソースを利用したアプリケーションソフトウェアの開発、新規システムの提案を行うことが可能である。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔学会発表〕（計６件）

① Ryuya Uda, Digital Forensics for Electronic Commerce on the Web, World Academy of Science, Engineering and

Technology, International Conference on Electrical, Computer, Information and Communication Engineering 2011, 査読有, 2011, pp.605-609, 2011 年 2 月 22-24 日, Bayview Hotel, Penang (Malaysia)

② 黒岩謙、宇田隆哉、携帯電話を用いた本人認証と電子商取引システムの実装と評価、情報処理学会 マルチメディア, 分散, 協調とモバイル(DICOMO2010)シンポジウム、査読無、2010、pp.1253-1261、2010 年 7 月 7-9 日、水明館 (岐阜県)

③ Ryuya Uda, Proposal of Method for Digital Forensics in Physical Distribution, 2010 The 2nd International Conference on Telecom Technology and Applications, 査読有, 2010, pp.211-216, 2010 年 3 月 19-21 日, Bali Dynasty Resort, Bali Island (Indonesia)

④ Ken Kuroiwa, Ryuya Uda, Proposal of Electronic Commerce System with Cellular Phones for Digital Forensics, The 4th International Conference on Ubiquitous Information Management and Communication, 査読有(優秀論文につき査読免除), 2010, pp.294-299, 2010 年 1 月 14-15 日 Sung Kyun Kwan University, Suwon (Korea)

⑤ 國井優伊、宇田隆哉、携帯電話を用いてデジタルフォレンジックを実現するファイル分散保存システムの提案、情報処理学会 マルチメディア, 分散, 協調とモバイル(DICOMO2009)シンポジウム、査読無、2009、pp.671-678、2009 年 7 月 8-10 日、杉乃井ホテル (大分県)

⑥ 黒岩謙、宇田隆哉、携帯電話を用いた本人認証と電子商取引システムの提案、情報処理学会 マルチメディア, 分散, 協調とモバイル(DICOMO2009)シンポジウム、査読無 (優秀論文賞受賞)、2009、pp.655-662、2009 年 7 月 8-10 日、杉乃井ホテル (大分県)

〔その他〕
ホームページ等
http://dfcp.u-lab.cs.teu.ac.jp/

６．研究組織
(1)研究代表者

宇田　隆哉 (UDA RYUYA)
東京工科大学・コンピュータサイエンス学部・講師
研究者番号：５０３５０５０９

(2)研究分担者
(　　)

研究者番号：

(3)連携研究者
(　　)

研究者番号：