International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:5, No:2, 2011

Digital Forensics for Electronic Commerce on the Web

Ryuya Uda

***Abstract*—**On existing online shopping on the web, SSL and password are usually used to achieve the secure trades. SSL shields communication from the third party who is not related with the trade, and indicates that the trader's web site is authenticated by one of the certification authority. Password certifies a customer as the same person who has visited the trader's web site before, and protects the customer's privacy such as what the customer has bought on the site. However, there is no forensics for the trades in those cased above. With existing methods, no one can prove what is ordered by customers, how many products are ordered and even whether customers have ordered or not. The reason is that the third party has to guess what were traded with logs that are held by traders and by customers. The logs can easily be created, deleted and forged since they are electronically stored. To enhance security with digital forensics for electronic commerce on the web, I indicate a secure method with cellular phones.

***Keywords*—**Cellular Phone, Digital Forensics, Electronic Commerce, Information Security

I. Introduction

NOWADAYS, online shopping sites spread world-widely and become popular. We can find many kinds of product on the web and can buy them, even in foreign countries. To trade on the web securely, SSL and password are usually used.

SSL is used for confidentiality and authentication. In communication, data is encrypted by SSL to make it invisible to the third party who is not related with the data. SSL also assure the person who has the web site, since the public key of the web site is signed by a certification authority and the sign is attached with the key as the certificate of the key. Therefore, with SSL, customers can see whether a shopping site is phishing one or not, while most of customers do not usually see certificates on SSL.

Password is also used to enter shopping sites. On most of the shopping sites, customers register themselves to the sites to skip filling in their personal information when they come to the same site again. Traders of shopping sites also receive benefit from customers' passwords, since the traders can pile up knowledge of customers' preference by binding customers' ID and their shopping history on the site. Of course, passwords protect customers' personal information and their privacy from the third party who is not related with the shopping.

In this paper, a secure method for electronic commerce on the web with cellular phones is indicated in order to enhance security with digital forensics. Related works are described in section II. A new method is indicated in section III. Existing security problems and their solutions are explained in section IV. Implementation of digital signature on cellular phones is evaluated in section V. The research is summarized in section VI.

Ryuya Uda is with Tokyo University of Technology, 1404-1 Katakuramachi, Hachioji City, Tokyo 192-0982, JAPAN (corresponding author to provide phone: +81-42-637-2111; fax: +81-42-637-2112;
e-mail: uda@cs.teu.ac.jp).

II. Related Works

One of the most famous protocols to login web sites securely is HTTP over TLS [1]. Its scheme is well known as HTTPS (HTTP over SSL/TLS). HTTPS provides server authentication and client authentication. Customer can confirm the owner of the web site and confirm that the owner is the same as the trader who the customer is trading with. Moreover, information in communication is encrypted and no one except the customer and the trader can see that information.

There are services that bind some of web based login services called single sign-on [2]. Single sign-on is more secure than usual web based login in terms of security. In usual web based login service, customers are sometimes caught by phishing sites. Phishing becomes smart year by year, e.g. some of phishing servers have correct certificate for HTTPS. The smarter phishing becomes the more important single sign-on becomes.

OpenID [3] is one of the single sign-on systems. It is an open source project with a community driven standardization process. Brad Fitzpatrick originally invented the protocol for his blogging application. OpenID is supported by major industry vendors.

There is a study for cellular phone based user authentication system called SUAN [4]. QR code, one of 2D code, is used to login a server and the server authenticates users with information by cellular phones without giving any personal information to client PC.

Those methods and services described above are effective for authentication and confidentiality. However, they cannot prevent falsification and denial when there is a malicious trader or a customer. Transaction logs stored on both side can easily forged or deleted, since no one has evidence that is electronically provided. Therefore, I design a method that keeps evidence electronically for digital forensics to enhance security in electronic commerce on the web.

III. Order Confirmation Method with Digital Forensics

In this section, explanation of the proposed order confirmation method is described. Overview of the method is shown in section A. Reasons for choice of cellular phones as digital forensic devices are explained in section B. How to

verify and create certificates for trades on traders' side is directed in section C. How to verify and create certificates for trades on customers' side is directed in section D.

A. Overview of the Order Confirmation Method

Figure 1 shows deployment of servers and arrangement of cellular phones connected to computers where the whole system works securely.

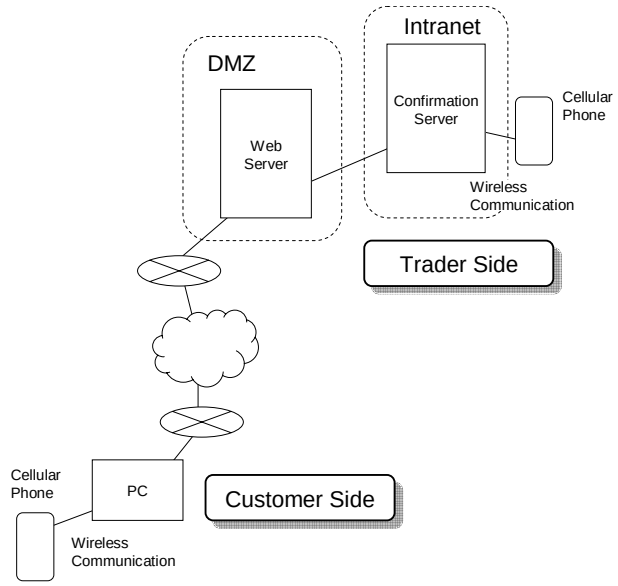

Fig. 1 Overview of the order confirmation method

On trader side, web server for shopping is deployed in DMZ (Demilitarized Zone) and confirmation server is deployed in intranet. The reason why those two servers are deployed in different segments is keeping the confirmation server safe from several attacks, since web servers are usually under the security risk of vulnerability. For example, programming languages used on server side such as Java, PHP and Ruby are always added some functions by updating their version or revision, and bugs or vulnerabilities are often found by the updating, since the updating is not for security but for adding new functions. Moreover, since designers who make web sites are not specialists of security, web sites sometimes have security problems caused by some types of attacks such as SQL injection or cross site scripting, and still worse, the attacks can be automatically created [5]. If web server and confirmation server are built in one server, the worth of digital signatures by the trader will be lost, even when the web site has only one vulnerable factor. Simply because invaders in the web server might be able to make signatures arbitrarily or might be able to make fake contents arbitrarily to lead signers to sign any document different from signers' intent. Therefore, signatures for trades should be written on the different server from the web server, and the server should not deployed in DMZ. Moreover, signature for trades should be written not by computer but by human i.e. the signatures should not be written automatically. Signatures on trader side are better to be made on traders' cellular phones if possible, since some kind of phones are safer than usual computers as is mentioned in section B.

On customer side, signature for trades must be made on customers' cellular phones, since customers' PC is not usually safe. If someone states that customers PC should be safe, they cannot install any application software freely though they own their PC. There are lots of bugs in application software on the market, and still worse, we sometimes hear that serious bugs are found in OS. Moreover, some customers sometimes use a PC that is not theirs, e.g. one in network cafes, one in hotels or one of their friend's. If their private keys for signatures are stored in their PC beforehand, they cannot use another PC that does not belong to them. And if they input their private keys when they use a PC, they have to remember a lot of bits of the keys in their remembrance.

Cellular phones both on trader side and customer side are connected to computers by wireless communication such as blue tooth or IrDA. No additional authentication server for cellular phones is required with the method.

B. Cellular Phones for Digital Forensics

A kind of cellular phones which are called smart phones can execute application software on OS (Operating System) of the phones. Nowadays, smart phones are extremely spread in USA, Europe and East Asia. Some kinds of smart phones can execute Java application software, and it is said that Java VM (Virtual Machine) on the phones loads software on the memory of a phone independently. Specifically, each of software on the Java VM is independent from others and the region of the memory allocated by Java VM is under access control of the OS. Especially, some of the phones produced by DoCoMo have special and non-volatile memory region for Java applications. Therefore, in my laboratory, some studies [6][7][8][9] of using cellular phones for digital forensics started.

The first implementation [10] of public-key cipher algorithm as application software on cellular phones appeared in a domestic symposium held in Japan in 2005. RSA, one of public-key cipher algorithms, was implemented on cellular phones produced by DoCoMo in that implementation. Several reports [11][12] about implementation of cipher algorithms on cellular phones produced by other communication carrier have been published after the first implementation. Using public key cipher is the best way for digital forensics. Our team opens a web site [13] of our studies about digital forensics using cellular phones. We have customized implementation of public-key cipher algorithms by Bouncy Castle [14], and succeeded to make the implementation faster. Source codes of that implementation are able to be downloaded from the web site.

C. Method on Trader Side

In the method, signature for trade is sent in HTTP response header as shown in Figure 2.

```
DF-Algorithm: public-key-cipher-algorithm=algorithm1?hash-algorithm=algorithm2
DF-Signature: body=signature?id1=hashdigest2?id2=hashdigest2...?idn=hashdigestn
```

Fig. 2 Original headers in HTTP response

DF-Algorithm and DF-Signature are designed as original headers for digital forensics on online shopping. HTTP application is allowed to define original headers in RFC2616 [15]. Those two headers are added to HTTP response header from the web server of traders'.

DF-Algorithm header defines algorithms of public key cipher and hash function which are used making a signature from a trader whom a customer is trading with. RSA-PSS, ECDSA or other public key based cipher algorithms can be defined in this header.

DF-Signature header shows a signature of the body of HTTP response, i.e. data come after HTTP response header and one blank line. The signature is defined as "body" and concatenated with a character "=".

Of course, HTML that is sent in HTTP response can include other contents in it. For example, HTML can show pictures, Java applets, and sometimes inline-frames - inline-frame should not be used in terms of security - in one page. Therefore, DF-Signature header also shows hash digests of those contents shown inline in HTML. As shown in Figure 3, each html tag can have different ID as an attribute of its tag. Hash digest of each inline content is defined as its ID, e.g. "idx", and its digest is concatenated with a character "=".

```
<img id="id1" src="somewhere" alt="something">

<iframe id="id1" src="somewhere">...</iframe>
```

Fig. 3 ID attribute on HTML tag

Signature and hash digests are trans-coded into BASE64 format and they are concatenated with a character "?" in the header of DF-Signature. Each of data that is sent from a web server can be signed one by one. However, no one can prove the relation among each of data when each of data is signed one by one. Therefore, in the method, hash digest of each of data is added in DF-Signature header to bind main HTML, called "body", with other inline content. For example, when a receipt that is constructed of strings and images is shown as one page of a web site, those strings and images must not be separated to prevent from falsification of the receipt.

All contents for signature are sent to confirmation server. If the trader who owns the server uses cellular phones for making signatures, all contents are transferred to the cellular phones. Watching the monitor of the confirmation server or the monitor of the cellular phone, the trader signs the contents about trading. HTML based contents that are displayed on those monitors are the same as those that are sent to customers. Even if the web server is cracked and invaders request the confirmation server to sign forged contents, the traders never sign content different from what they see on their display.

D. Method on Customer Side

Method on customer side is almost the same as the method on trader side mentioned in section C. In the method, signature for trade is sent in HTTP request header as shown in Figure 4.

```
DF-Algorithm: public-key-cipher-algorithm=algorithm1?hash-algorithm=algorithm2
DF-Signature: body=signature
```

Fig. 4 Original headers in HTTP request

DF-Signature header in HTTP request does not include "id" element, since no inline content is included in HTTP request. If HTTP request method is "get", customers sign QUERY_STRINTG which is defined in HTTP. If HTTP request method is "post", customers sign the body of HTTP request, i.e. data come after HTTP request header and one blank line.

In the same way as trader side, all contents for making signatures are transferred to the customer's cellular phone. Watching the monitor of the cellular phone, the customer signs the contents about trading. HTML based contents that are displayed on the monitor of customer's cellular phone are the same as those that are sent to traders. Even if the trader's web server is cracked and invaders request customers to sign forged contents, the customers never sign content different from what they see on the display of their phones.

IV. Security Problems and Solutions

In this section, security problems of web services and solutions of the problems are described. HTTP header injection attack is shown in section A. Security problems in using e-mail are explained in section B. The way to extend the method to escrow service and existing problems are argued in section C.

A. HTTP Header Injection

HTTP header injection is a kind of attacks such as injecting HTTP header into existing HTTP header. Example is shown in Figure 5.

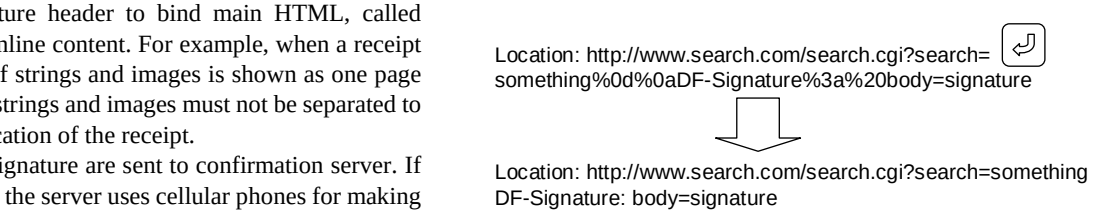

Fig. 5 Example of HTTP header injection

"%0d" is CR code and "%0a" is LF code. In ordinary operation system such as Microsoft Windows, "CR+LF" means new line.

To avoid the above injection, one might think that character "%" for making control code should be eliminated from all HTTP headers. However, as shown in Figure 5, "%3a" is needed to show ":" and "%20" is needed to show space code.

When implementing the method on this manuscript, HTTP header injection should be regarded. If the same header such as DF-Signature appears more than once on the system where the method is implemented, it is doubtful whether it is HTTP header injection or not. Not all HTTP daemons confirm "%0d%0a" in HTTP header.

Moreover, receipt and confirmation of orders should contain time stamps and order numbers in HTML based documents in which users can see the stamps and numbers directly, so that receipt and confirmation of orders with correct signature might not be used again by malicious people.

B. Security Problems on E-mail

Receipt and confirmation of orders must be sent by HTTPS. Some of existing web sites send URL for confirmation by e-mail. However, e-mail is unsafe when secret information, e.g. privacy or personal information, is sent. SSL turns communication encrypted. Moreover, using SSL, customer can confirm that the owner of the certificate of the web site is the same as the trader - although most of customers seem not to confirm the certificate of the web site.

Of course, e-mail has encryption and authentication methods such as S/MIME and PGP. However, S/MIME and PGP have not been popular yet, though they appeared many years ago. The reason is that no one knows the best way for managing their private keys securely. If once keys are leaked, all signatures by the leaked key are void and all of information that is encrypted by the leaked key is exposed. Using plain e-mail for authentication is also unsafe. The header "From: " can be easily forged by malicious people.

Therefore, in this paper, cellular phones are used to authenticate customers. Private keys for the customers are made in the phones and the keys are never sent anywhere forever.

C. Extension to Escrow Service

In this section, the flow of money is argued. Using credit card is the best way for security when implementing the method in this paper, since card companies may collect customers' order forms with their signatures. No one can file a claim without customers' signatures.

However, if money is transferred directly from customers to traders, any shopping service with security system does no work well, since malicious traders can break the promise whether there are signatures or not. Even if those traders are arrested, there is no assurance that the paid money will be back.

Therefore, escrow service is one of the solutions for managing customers' money safely, since escrow service managers do not send money to traders before the traders send products to customers regarding to order forms that are signed by customers.

TABLE I
TIME FOR SIGNING ON CELLULAR PHONES

Model	Average (ms)	Max (ms)	Min (ms)	Std. Deviation (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

TABLE II
TIME FOR VERIFICATION ON CELLULAR PHONES

Model	Average (ms)	Max (ms)	Min (ms)	Std. Deviation (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

TABLE III
TIME FOR KEY GENERATION ON CELLULAR PHONES

Model	Average (ms)	Max (ms)	Min (ms)	Std. Deviation (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

V. EVALUATION

Some models of Japanese cellular phones are called smart phone. Original application software is available on those phones. It is said that memory area of application software is secure from malware, since each package of that application software working on VM (Virtual Machine) on a phone is independent from each other unless the VM has vulnerability.

A team in my laboratory has implemented some algorithms of cipher on smart phones produced by DoCoMo. ECDSA algorithm seems one of the best choices for the method indicated on this paper regarding to the length of one signature and calculation performance. The implemented ECDSA algorithm is originally from Bouncy Castle library and it is improved to work faster. Table I, II and III shows calculation time for ECDSA on some smart phones to prove how useful the method is. Each value of those three tables is based on 100 times measurement.

Table I shows time for making one digital signature on cellular phones. The table indicates that time for making one signature is kept within one second on almost all phones except one. On several hi-performance models, one signature is made within about 0.2 second.

Table II shows time for verifying one digital signature on

cellular phones. The table indicates that time for verifying one signature is kept within one second on almost all phones except one. On several hi-performance models, one signature is made within about 0.3 second.

Table I and II prove that some models of cellular phones have enough performance for the method indicated in this paper, since customers ordinary don't order products more than once within one second, and one second seems short for traders in confirming one order.

Table III shows times for generating a pair of keys on cellular phones. The keys once generated are used until they are expired, and the term for expiration might be from several months to several years. Therefore, the performance shown in table III is good enough for traders and customers.

VI. Summary

In this paper, the method for digital forensics for electronic commerce on the web is described. Existing shopping services only focus confidentiality of orders. SSL provides authentication between servers and clients, but nothing is assured about information exchanged between customers and traders. The method in this paper especially pays attention to denial by traders or by customers. With this method, web shopping service will be safer than existing one. Moreover, smart phones have extremely spread in recent years. The phones seem to be the best security devices for digital forensics when application software on the phone can be executed independently.

Acknowledgment

This research was partially supported by the Grant-in-Aid for Young Scientists (B), 21700088, 2010, the Ministry of Education, Culture, Sports, Science and Technology.

References

[1] E. Rescorla: HTTP Over TLS, RFC 2818, 2000.
[2] Shakir James, "Web Single Sign-On Systems", http://www.cse.wustl.edu/~jain/cse571-07/ftp/websso/index.html
[3] OpenID, http://openid.net/
[4] Michiru Tanaka and Yoshimi Teshigawara, "A Method and Its Usability for User Authentication by Utilizing a Matrix Code Reader on Mobile Phones" *Lecture Notes in Computer Science*, Vol.4298/2007, pp.225-236, 2007.
[5] Adam Kiezun, Philip J. Guo, Karthick Jayaraman, Michael D. Ernst, "Automatic Creation of SQL Injection and Cross-Site Scripting Attacks", *International Conference on Software Engineering archive, Proceedings of the 31st International Conference on Software Engineering*, pp.199-209, 2009.
[6] Ryuya Uda, Masahito Ito, Kohei Awaya, Hiroshi Shigeno, Yutaka Matsushita, "E-Ticket Issuing System with 3-D Pattern Recognition for Mobile Terminals", *IFIP 17th International Conference on Information Security, SEC 2002*, pp.399-410, 2002.
[7] Ryuya Uda, "Proposal of Method for Digital Forensics in Physical Distribution", *2010 The 2nd International Conference on Telecom Technology and Applications (ICTTA 2010)*, pp.211-216, 2010.
[8] Yui Kunii, Ryuya Uda, "A Proposal of A Distributed File Backup System for Digital Forensics Using Cellular Phone", *IPSJ - Proceedings of Multimedia, Distributed, Cooperative, and Mobile Symposium 2009*, pp.671-678, 2009. (Japanese)
[9] 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 (ICUIMC 2010)*, pp.294-299, 2010.
[10] Kei Ozaki, Ryuya Uda, Akio Tojo, "A Mutual Authentication System with Public Key Cryptosystem on A Cellular Phone" *IPSJ - Proceedings of Computer Security Symposium 2005*, Vol.2, pp.535-540, 2005. (Japanese)
[11] Motoi Yoshitomi, Tsuyoshi Takagi, Shinsaku Kiyomoto, Toshiaki Tanaka, "Efficient Implementation of the Pairing on Mobilephones Using BREW", *IEICE - Transactions on Information and Systems archive*, Vol.E91-D, Issue 5, pp.1330-1337, 2008.
[12] Yuto Kawahara, Tsuyoshi Takagi, Eiji Okamoto, "Efficient Implementation of Tate Pairing on a Mobile Phone Using Java", *Lecture Notes In Artificial Intelligence, Computational Intelligence and Security: International Conference, CIS 2006*, pp.396-405, 2007.
[13] Research for Digital Forensics by Using Cellular Phones, http://dfcp.u-lab.cs.teu.ac.jp/
[14] The Legion of the Bouncy Castle, http://www.bouncycastle.org/
[15] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee: Hypertext Transfer Protocol -- HTTP/1.1 (RFC 2616), 1999.