PROTOCOL OF AUTHENTICITY TO PROVIDE LEGAL SECURITY IN E-CONTRACTS

A Prototype

João Fábio de Oliveira, Cinthia O. de A. Freitas and Altair Santin
Pontifical Catholic University of Parana - PUCPR
R. Imaculada Conceição, 1155, Prado Velho, 80215-901, Curitiba - PR, Brazil

Keywords: Law and Internet, Consumer Protection, Authenticity.

Abstract: This paper discusses the security problems on the contracts deals over the Internet and describes a protocol of authenticity that will keep audit trails from the activities during the Web hiring. These audit trails will be stored digitally, either on the side of the provider or on the consumer. It is understood that it is legal obligation of the provider to logs and ensure the integrity of the data related to the operations on the Internet-based commerce. because in situations of dispute can occur a reversal of the burden of proof. Thus, this prototype ensures confidence on the e-contracts, logging relevant information that help in the identification of the parties, using a Plug-in software installed on the e-commerce provider and in the consumer machine, executable in the Web. Moreover, it is important to remind about the security in contracts agreements over the Internet is an essential feature because it allows the consumer a guarantee of contract award, since it maintains the integrity of the document, and also can be presented as evidence to the Judiciary, helping in litigation and satisfying the premises of the legal acceptance of digital documents.

1 INTRODUCTION

The increased use of Internet in people's daily lives is already a reality as a basic and essential tool in day-to-day of the societies, for things like paying bills, consulting phone catalogs and maps, relationship between people, electronic messaging and even to buy objects and consumer services.

According to the Center for Studies of Information and Communications Technology (Brazilian Internet Management Committee, 2006), about 14.49% of Brazilian homes already have Internet access, this information are from the last poll done in 2006, which represents a 1.56% growth over the 12.93% of 2005. This growing universe of users and potential consumers of online products represents a great concern from the technical and legal point of view, due to the yearly increase in the number of problems that need to be handled by each of the related sciences.

On the other hand, Internet brings some information security concerns, since the documentation is no longer kept in physical form, such as paper, but rather stored electronically through digital means. While the Internet simplifies commercial operations that take place in the digital environment, it introduces a restricting factor and leads us to a universe of studies on the security, trustworthy, confidentiality, integrity, and authenticity aspects. As well as the legality of such operations given the doubtful facts questionable by any of the parties involved in the transaction (e-contract).

In face of this, there is a search for technical solutions for security infrastructure for e-business including the security of the information exchanged and the storage of this information, especially when it comes to making it trusted as far as accuracy of the content stored. In this sense, the cryptography and digital signing methods have contributed for the security of online transactions: e-contract, e-commerce, e-business (Behrens, 2007) (Garfinkel, 1997).

Thus, this paper discusses our prototype for authentication protocol based on the consumer–provider relationship on the contracts over the Internet, since this protocol defines technical and traceable parameters of the transaction, and provides legal security in e-contracts, both in the provider's server and in the consumer's equipment. We discuss our prototype for demonstrating the practical feasibility of the proposed protocol. This protocol

Fábio de Oliveira J., O. de A. Freitas C. and Santin A. (2008).
PROTOCOL OF AUTHENTICITY TO PROVIDE LEGAL SECURITY IN E-CONTRACTS - A Prototype.
In *Proceedings of the International Conference on e-Business*, pages 378-383
DOI: 10.5220/0001907903780383

must be used along with the web server of the provider and the Web browser of the consumer, and is been developed as a Web Plug-in.

This paper is divided into five sections. Section 2 highlights the security issues on the web. Section 3 summarizes the e-contracts since its definition and the relevant aspects for the protocol of authenticity, which provides legal security in e-contracts. The proposed protocol is presented in Section 4. Some final considerations are given in Section 5.

2 SECURITY ISSUES ON THE WEB

There are different aspects of security issues on the web, such as physical security, personal security, operations security, communications security, and network security. Normally, the systems are concerned about the application of the protection in e-anything or e-initiative, or specifically e-business, taking into account the state of the art technological infrastructure. The main goal of security for e-business applications is to protect networks and their applications against attacks, ensuring information availability, confidentiality, integrity, auditing, authorization, and authentication (Huang et al., 2008) (Meier, 2003). This paper goes beyond to provide a secure environment. We are here considering legal security of e-contracts.

A secure environment is ensured by combination of different factors, such as data security, networking security, policy, and management of information system security (ISS) (Akhter & Kaya, 2008). Therefore, we need discuss the basis of the information transferred during transactions over the Internet.

The starting point of the information transferred on Internet is the TCP/IP *(Transmission Control Protocol/Internet Protocol*) protocol. This protocol, in its version 4, has been consolidated for using in Internet (Comer, 1991). This protocol does not include security mechanisms for information transfer, leaving this for the applications which are developed for the end users, which is the reason for the concern about the related criteria to the protection of the content in transit. This means that the transferred information between two different places on Internet, regardless of its physical location, can be captured by a protocol analyser (WireShark, CommView, Ghost). So the desired information can be visualised.

The TCP/IP protocol specification has a conceptual segmentation into five layers, as shown in Table 1 (Comer, 1991). Each layer solves a set of problems involving the transmission of data, and provides a well-defined service to the upper layer protocols based on using services from some lower layers. Upper layers are logically closer to the user and deal with more abstract data, relying on lower layer protocols to translate data into forms that can be physically transmitted. Layer 5, nominated as application layer, specifies and implements the software which interact with the end users. It is at this level that all concerns related to the information security should be implemented, in other words, the applications at the user level must include treatment mechanisms that are considered secure enough to, on one hand, give the end user the assurance that his network transaction is secure, free of risks of content modifications, and on the other hand, provide verified technical conditions of mechanisms considered secure, such as the use of cryptography algorithms at the applications level (Schneier, 1996).

Table 1: The 5-Layer TCP/IP Model.

Layer	Protocol
5 – Application	HTTP, DNS, SMTP,...
4 – Transport	TCP, UDP, DCCP...
3 – Network	IP, IGMP, ICMP...
2 – Data	Ethernet, Wi-Fi, 802.11(WLAN)...
1 – Physical	Modem, PLC, optical fiber...

Traffic on the Internet is a client-server software application, which is executed through a direct user interface, known as the *web browser*. In this environment, several applications are written in the application layer protocol of the TCP/IP known as http (hypertext transfer protocol) (Garfinkel, 1997). Since there are no mechanisms defined in the TCP/IP protocol itself, the application is responsible to define and implement additional security algorithms; minimizing the impact of the vulnerabilities that exist on the internet protocol. Thus, the security issues on the Web are divided into three categories (Garfinkel, 1997):

- *Security of the Web server, the server's activities, and stored data:* guarantee that the information was not modified or distributed without user authorization;
- *Data security in the computers network:* guarantee that the transmission of information between the server and the Web browser has a security level based on well-known standards, such as cryptography or digital signature (Meier, 2003). Cryptography refers to how your application enforces confidentiality and integrity. Digital signature corresponds a

countermeasure techniques that can be used to reduce risk of tampering with data (Meier, 2003);

- *Data security in the user computer:* guarantee that user's computer is as protected as possible (firewalls, antivirus, anti-spyware, anti-spam, etc.). A typical firewall helps to restrict traffic to HTTP, but the HTTP traffic can contain commands that exploit application vulnerabilities (Meier, 2003).

Therefore, taking into consideration the security problems on Internet, these vulnerabilities can be analyzed from the point of view of the contracts deals over the Internet. In this case, it is not necessary provide information security but is primordial provide legal security for e-contracts.

3 E-CONTRACT

A contract is a legally binding agreement. Agreement arises as a result of offer and acceptance, but a number of other requirements must be satisfied for an agreement to be legally binding as following (Martin, 2003):

- The parties must have an intention to create legal relations;
- The parties must have capacity to contract;
- The agreement must comply with any formal legal requirements (it may be oral, written, partly oral and partly written, or even implied from conduct);
- The agreement must be in accordance of the law;
- The agreement must not be rendered void either by some common-law or statutory rule or by some inherent defect, such as operative mistake.

However, when such a contract becomes valid, that is, legally binding and enforceable, is regulated by contract law that may differ from country to country, even if subject to International Law. Based on these considerations, an e-contract is a valid contract deals over the Internet. Simplest example is Amazon book store buying. When everything goes right, it is of no major importance when exactly a contract is concluded and according to which law. However, when something goes wrong such as, the product does not delivery, payment is not effectuated or is wrongly charged, or the product is damaged; then information about the contract conclusion as well as governing law may be crucial. This is the main problem of cross-border e-commerce, but this topic is beyond this paper.

Recognising the value of arbitration as a method of settling disputes arising in the context of international commercial relations and being convinced that the establishment of rules for ad hoc arbitration that are acceptable in countries with different legal, social and economic systems would significantly contribute to the development of harmonious international economic relations; the United Nations Commission on International Trade Law (UNCITRAL) was established by the United Nations General Assembly in 1966 to promote the progressive harmonization and unification of the law of international trade. Brazil not adopts these rules and there are no clear rules or a specific law for litigation situations involving e-commerce.

Chiu et al. (2003) presents that e-contract enforcement can be divided into multiple layers and perspectives, which has not been adequately addressed in the literature. This problem is challenging as it involves monitoring the enactment of business processes in counter parties outside an organization's boundary. The authors present an architecture for e-contract enforcement with three layers: document layer, business layer, and implementation layer. In the document layer, contracts are composed of different types of clauses. In the business layer, e-contract enforcement activities are defined through the realization of contract clauses as business rules in event-condition-action (ECA) form. In the implementation layer, cross-organizational e-contract enforcement interfaces are implemented with contemporary Enterprise Java Bean and Web services. They present a methodology for the engineering of e-contracts enforcement from a high-level document-view down to the implementation layer based on this architecture, using a supply-chain example. As a result, e-contracts can be seamlessly defined and enforced.

This paper present an authentication protocol to provide legal security in e-contracts implemented in application layer based on document-view. The idea is to be able answering some questions such as: Does the consumer want to buy, is s/he able to buy? When is the contract considered to be concluded? There is no clear rule. To avoid problems and protect the consumer (as provided in the Brazilian Consumer Code) we are developing the protocol to capture and save a set of data from consumer and provider. This set of data can be easily visible and accessible by the consumer and accepted by him/her. Thus, when constituting the contract elements in a virtual environment, the following fundamental structure items must be established: user-consumer, provider, e-contracts and contract location.

4 PROTOCOL OF AUTHENTICITY

In e-contract, such as in the purchase of consumer goods from e-commerce Web sites, the consumer will be taking advantage all infra-structure of communication defined in the Internet network. When the consumer performs a purchase operation on the providers' server through her Web browser, she lacks the mechanisms to provide physical and legal evidence of the content accepted during the transaction at a technical level. In other words, there are no effective logs on your computer that store or restore the history of transaction between the consumer and the provider. Therefore, this Section presents the theoretical aspects explored in the proposed protocol and the implementation issues.

4.1 Theoretical Aspects

In practice the hiring conducted on the Internet can be done by e-mail or directly at the Web site (e.g. in clicking a button "I accept"). This implies that specifically in the context of Web communication, the level of information security applied in http protocol guarantees a minimum of security based on mechanisms of encryption. Indeed, the use of SSL (Secure Sockets Layer) in Web applications applies encryption namely, point-to-point, so that the information is transferred ciphered on the Internet (Garfinkel, 1997). The encryption point-to-point means doing a cryptographic channel between the provider and consumer applications layers.

The applications developed for the Internet environment, following the client-server architecture, employ the standard TCP/IP protocol infra-structure, remaining however, vulnerable to the various problems typical to this environment. Specifically in Web communication, when communications between the server and the contractors' web browser employ the SSL protocol in the cryptography of the data transferred over the network, the risk of fraud in the transferred content is reduced by the cryptography (Garfinkel, 1997). However, in litigation situations it is necessary restore the history of transaction between the consumer and the provider and there is no protocols or tools that capture, store and restore this kind of information, specially providing legal security. In this context, legal security represents the consumer's guarantees that the transaction hired on the Internet can be presented in Judicial processes. Thus, the proposed protocol of authentication (Plug-in) is organized in two parts:

- *Server:* is installed on the Web server provider and follows the standards of the http protocol and Java-web, and is configured as an extension of the services of the server and offered to the consumer as a Plug-in for web browser of provider;
- *Client:* is installed on the consumer's computer and follows a specific procedure for initial installation of the Plug-in, considering the consent of the consumer to accept the installation of this software on her computer. The Java programming language was chosen due to its flexibility in selecting of information on Internet environment.

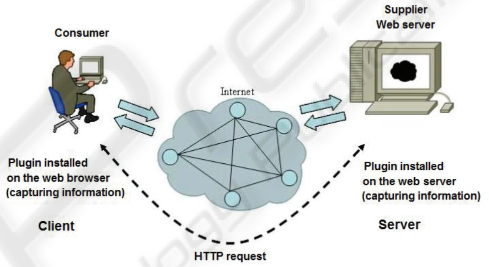


Figure 1: Plug-in model.

It is possible, therefore, to present an overview of the authentication protocol, in which the consumer possesses in her computer the record of the transactions done in the web site of the providers, in order to extract a report with the information regarding such transaction. On the other hand, the protocol allows to confront the information transferred between both parties, as shown on Figure 1. The request done by the consumer is based on the http protocol, then the Plug-in captures the packages on this level of the protocol as well as other technical information on the TCP/IP level and stores all data in the log files.

4.2 Implementation Issues

Considering the theoretical aspects presented before, the proposed protocol defines that the consumer, when accessing the web site of the providers through her browser, has an icon with information about the authentication protocol available in order to allow her with explicit consent and authorization, to download the Plug-in to her computer.

The protocol determines the capture of consumer information, as shown in Table 2, which takes place during the initial interaction process when the consumer accepts the installation of the Plug-in.

This initial registration makes up the official identification of the consumer.

Table 2: Consumer Information – Initial Registration.

Field	Description
name_contr	Consumer's name
address_contr	Consumer's address
phone_home_contr	Consumer's Home Telephone
phone_celular_contr	Consumer's Mobile Phone
id_contr	Consumer's Legal Identification
type_id	ID, Drivers License, Passport, Working Papers
tax_id_contr	Consumer's tax ID

After this initial registration, the algorithm provides verification of the Plug-in installed on the equipment of the provider, installing it when it is not already done. From this point on, the operations performed by the consumer on the web site of the provider keep all information stored in a log file recorded on both sides (provider and consumer), as specified in Table 3.

The log file is encrypted through the Triple DES (Triple Data Encryption Standard) algorithm, developed at IBM and published as a standard in 1977 (Schneier, 1996). Generally TDES uses three different keys and has a key length of 168 bits (3 x 56-bit DES), resulting in a symmetric algorithm. Thus, by being symmetric, the key used for encryption and decryption of the file is the same, making it a fast processing algorithm, considering the log file to be processed and ensuring access to the information.

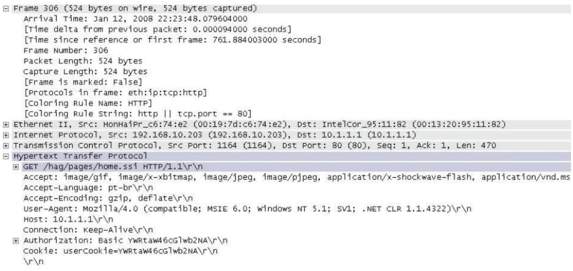
In this way, the consumer will be able to generate her report directly through her computer, without depending on the information saved in the server of the provider, as is the case with the use of other cryptography algorithms that apply asymmetric keys (which relies on the exchange of public between both parties).

In the Plug-in installed on the computer of the consumer is the function to visualize the log file stored, allowing her extracting the information about the operations accomplished in printed format as evidence of the various Web interactions performed at the web site of the providers. In legal terms, this report will allow the consumer to provide evidence as an official document registered at Notary's Office (Rezende, 1997).

The capture data follows the structure defined in Figure 2, which is an example of the data capture using the Wireshark software, keeping the reference to the TCP/IP protocol. The information necessary to comply with the fields defined in the authentication protocol are available in the data package captured in the Ethernet frame, as shown in Figure 3. The information captured are stored in the log file in a sequence and logically structured in data files in encrypted text format.

Table 3: e-Contracts Information.

Field	Description
IP_consumer_Internet	Consumer's IP number as an Internet user
IP_consumer_real	Consumer's IP number (consumer machine)
Mask_IP_consumer_real	Networking mask (consumer machine)
Gateway_consumer_real	Default gateway (consumer machine)
DNS_consumer_real	DNS configured (consumer machine)
IP_provider_Internet	Provider's IP number (provider server)
IP_ provider_real	Provider's IP number (LAN server)
Mask_IP_provider_real	Networking mask (provider server)
Gateway_provider_real	Default gateway (provider server)
DNS_provider_real	DNS configured (provider server)
date_acess	Date: DD/MM/YYYY
time_acess_consumer	Hour: HH:MM:SS
time_acess_provider	Hour: HH:MM:SS
port_acess_consumer	Consumer's TCP or UDP port number
porta_acess_provider	Provider's TCP or UDP port number
URL_provider	web address accessed by the consumer
route_IP	Route between consumer's IP and provider's IP



```
⊟ Frame 306 (524 bytes on wire, 524 bytes captured)
    Arrival Time: Jan 12, 2008 22:23:48.079604000
    [Time delta from previous packet: 0.000094000 seconds]
    [Time since reference or first frame: 761.884003000 seconds]
    Frame Number: 306
    Packet Length: 524 bytes
    Capture Length: 524 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80]
⊞ Ethernet II, Src: HonHaiPr_c6:74:e2 (00:19:7d:c6:74:e2), Dst: IntelCor_95:11:82 (00:13:20:95:11:82)
⊞ Internet Protocol, Src: 192.168.10.203 (192.168.10.203), Dst: 10.1.1.1 (10.1.1.1)
⊞ Transmission Control Protocol, Src Port: 1164 (1164), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 470
⊟ Hypertext Transfer Protocol
  ⊞ GET /hag/pages/home.ssi HTTP/1.1\r\n
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms
    Accept-Language: pt-br\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)\r\n
    Host: 10.1.1.1\r\n
    Connection: Keep-Alive\r\n
  ⊞ Authorization: Basic YWRtaW46cGlwb2NA\r\n
    Cookie: userCookie=YWRtaW46cGlwb2NA\r\n
    \r\n
```

Figure 2: Capturing the Data Package.

The technique for capturing the packages is based on the use of the libpcap/winpcap libraries, which are low level software libraries available for programming code of development. These libraries come from network traffic information according to the interface used, for example, Ethernet and Wireless WIFI.

Global Header	Package Header	Package Data	Package Header	Package Data	Package Header	Package Date

Figure 3: Format of the Captured Data Package.

This library provides functions that capture packages in the format of the basic network, on which there are the header and the individually separate data. Inside of the TCP/IP protocol in its didactic classification, it is possible to separate the various levels of information (protocol and user information) allowing for the recording of this information to the log file (Comer, 1991).

In future work, we plan to conduct case studies to evaluate our protocol taking into consideration the following parameters:

- *Performance:* computing the impact of the protocol in the consumer machine and on the e-commerce provider based on CPU use. The data collecting will be done using the SNMP (Simple Network Management Protocol);
- *Response time:* which is the time a generic system or functional unit takes to react to a given input. In this case, we will verify the response time between the consumer machine and e-commerce provider. The data collecting will be done using the ICMP (Internet Control Message Protocol) considering the echo-request and echo-reply facilities.

This evaluations can demonstrate potential scenarios that may benefit from this research.

5 FINAL CONSIDERATIONS

In litigation situations involving e-commerce, the greatest difficulty is in verifying proof of the contract established. This difficulty arises due to the fact that the relations are no longer necessarily face-to-face, therefore requiring the use of additional mechanisms to carry out these contracts as well as computer tools that allow the registration and evidence that the contract was made. Thus, the authentication protocol proposed in this article allows both interested parties, consumer and provider, to keep registry logs with information about the dealing contract. This audit trail is composed of a variety of information, such as the IP record of the equipment involved in the transaction. Therefore, the consumer can issue reports on the access to the providers, as well as the contracts over the Internet. In this situation, is important that the consumer can restore, from her own computer, data and information on the litigated web site. Or, furthermore, the consumer should be in condition to validate the information given by the provider. Thus, the use of the authentication protocol will be, in fact, mapping the operation accomplished through the Internet by means of the log file, with a full and secure record of the main elements of the e-contract.

ACKNOWLEDGEMENTS

The authors wish to thank Dr. Antonio Carlos Efing (PPGD-PUCPR) which have collaborated to this work. This work has been supported by CNPq (grant 471627/2006-2 and grant 476637/2006-6).

REFERENCES

Atkins, D., Buis, P., Hare, C., Kelley, R., Nachenberg, C., Nelson, A.B., Phillips, P., Ritchey, T., Sheldon, T., Snyder, J. (1997). *Internet security professional reference*, New Riders Publishing, 2nd edition.

Behrens, F. (2007). *Digital signature and legal business*. Jurua, 1st edition.

Brazilian Internet Management Committee (Comitê Gestor da Internet Brasil), Center for Studies of Information and Communications Technology (2006). TIC Domicílios e Usuários (ICT Homes and Users. Available: http://www.cetic.br/, [11-march-2008].

Chiu, D.K.W., Cheung, S.C., Till, S. A. (2003). Three-layer architecture for e-contract enforcement in an e-service environment. In *36th Annual Hawaii International Conference on System Sciences*.

Comer, D. E. (1991). *Internetworking with TCP/IP: principles, protocols, and architecture*, Prentice-Hall International, Inc., 2nd edition, Vol. 1.

Garfinkel, S., Spafford, G. (1997). *Web security & commerce*. O'Reilly & Associates, Inc.

Martin, E.A. (2003). *A Dictionary of Law*. Oxford University Press.

Meier, J.D., Mackman, A., Vasireddy, S., Dunner, M., Escamilla, R., Murukan, A. (2003). *Improving web application security: threats and countermeasures*, Microsoft.

Rezende, A.C.F. (1997). *Notary's Office and the perfect notary: property law and notary's activities*. Copola Livros. 1st edition.

Schneier, B. (1996). *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, Inc., 2nd edition.