Phishing Secrets: History, Effects, and Countermeasures

Antonio San Martino and Xavier Perramon
(Corresponding author: Antonio San Martino)
Department of Information and Communication Technologies, Universitat Pompeu Fabra, Barcelona, Catalonia, Spain
Roc Boronat 138, E-08018 Barcelona, Catalonia, Spain
(Email: asm@dp-security.com, xavier.perramon@upf.edu)
(Received June 13, 2009; revised and accepted Nov. 11, 2009)

Abstract

This paper presents the results of a study performed over phishing threats and vulnerabilities present in nowadays authentication environments. The main goal of this paper is to present our solution, the anti-phishing model which can be applied to any web environment, and not just to e-banking or the financial sector, without limitations nor additional requirements. We start presenting a brief history of phishing, common solutions, some statistics about phishing attempts, social impact and monetary losses and our patented anti-phishing model. Following is an explanation about how different vulnerabilities have been addressed such as Man-In-The-Middle attacks, phishing, pharming, SQL injection, social engineering, format string attacks, buffer overflow, brute force and many other vulnerabilities. The proposed method has been the basis of a PhD thesis aimed at defining a model for secure operation of an Internet Banking environment, even in the presence of malware on the client side. The authentication model is based on a mutual multi-factor authentication process where both entities must be authenticated with more than one authentication factor. The proposed model has been designed to be easily applicable with minimum impact to the current Internet banking systems. Its goal is to be resistant to the nowadays too frequent phishing and pharming attacks, and also to more classical ones like social engineering or man-in-the-middle attacks. The key point of this model is the need for multi-factor mutual authentication, instead of simply basing the security on the digital certificate of the financial entity, since in many cases users are not able to discern the validity of a certificate, and may not even pay attention to it. Thanks to the rules defined in this proposal, the security level of the Web Banking environment will increase and customers' trust will be enhanced, thus allowing a more beneficial use of this service. The proposed model has been simulated in order to demonstrate its effectiveness and feasibility.

Keywords: Authentication, bank, e-banking, phishing

1 Introduction

Phishing, as defined in Wikipedia, is "the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication" [17]. Normally phishers hijack a bank's web page and send emails to the victim in order to trick the victim to visit the malicious site (apparently the real bank site) in order to collect victim bank account information and card numbers. Pharming is "a hacker's attack aiming to redirect a Web site's traffic to another, bogus Web site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software" [16]. Man in the Middle (MITM) is "a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker" [15].

A number of techniques and standards have been developed for providing information security against common threats, but currently there is no official preventive standard solution for phishing and pharming threats. There are an increasing number of new attacks and viruses against web pages of financial entities [12], such as "phishing" and "pharming" frauds that must be addressed in order to guarantee customers' trust in web banking services.

No standard exists in order to address and manage phishing and pharming attacks. The proposed multi-factor mutual authentication process presented here allows to detect and then to address these two threats. Our authentication model works in a secure way also in the presence of these threats.

The specific novelty of this work is the mutual authentication method, which if correctly implemented avoids many threats such as phishing, pharming, man in the middle attacks and identity theft. A mutual authentication

process (Server and User) is required and necessary to circumvent phishing and pharming threats. The problem is actually wrong server authentication. Nowadays a digital certificate is considered as a valid solution for server authentication, but it is not enough for the final user. This is because many users are not able to see the difference between a valid and a non-valid certificate. Many times the false certificate is a very good copy and it is very hard to detect if it is a false copy or the original certificate. Additionally many users do not pay attention to details of the site's certificates, so it is impossible to detect if the certificate is bad or not [2]. The system proposed herein is easily applicable to current banking systems as they only have to change the authentication process by adding a previous server authentication step to the user authentication. First, the server is authenticated and next, if the result of the server authentication is successful, the user will provide his credentials. In this manner user credentials are prevented from being stolen by a hijacking server.

In the development of this work a number of different authentication scenarios have been considered. We have developed a prototype of the anti-phishing model in order to demonstrate the effectiveness of the proposed solution.

In this paper, after a brief overview of the state of the art of phishing threats, we discuss the social and monetary impacts of phishing on our society. Next, common phishing defense mechanisms are presented and next our solution [5] is presented: The multi-factor mutual authentication environments are enumerated and a threat solution approach is presented. Our solution is composed of two parts: Software and hardware. In particular the hardware solution consists in a secure device which implements the mutual authentication process and deploys some security measures in order to work in a secure way also under compromised environments.

Finally, in the conclusions section the achievements are summed up.

2 State of the Art

The word "phishing" originated in the 1996 timeframe [9, 13]. The term was coined based on the analogy that fraudsters used email as a fishing hook to "phish" usernames, passwords and other sensitive information. The use of the letters "ph" is believed to have been derived from the word "phreaking". "Phishing" first surfaced around 1996, when criminals stole American Online (AOL) accounts by "phishing" the passwords from AOL users. In order to understand the potential impact of such vulnerabilities in our society, we report some phishing statistics for the most popular phishing targets with the relative number of attacks received per month. On February 2007/2008/2009 the most popular phishing victims were respectively: PayPal/Ebay/PayPal with more than 2511/5750/6240 attacks received. Next, in the second position were Fifth Third Bank/PayPal/Internal Revenue Service with over 1180/3795/325 phishing attempts. Finally in the third position we find Ebay/Bank of America/EBay with more than 795/570/290 respectively [14].

In addition, from a research performed by Dhamija [2], it is possible to appreciate the factors which take part in the phishing attacks success. Dhamija first analyzed a large set of captured phishing attacks and developed a set of hypotheses about why these strategies might work. She then assessed these hypotheses with a usability study in which 22 participants were shown 20 web sites and asked to determine which ones were fraudulent. She found that 23% of the participants did not look at browser-based cues such as the address bar, status bar and the security indicators, leading to incorrect choices 40% of the time. In addition, as reported by research performed by Litan [3], some phishing attacks got more than 5% of their potential victims to provide sensitive information to malicious Web sites. Another research, performed by Loftesness [4], reports that two million users gave information to a hijacking site, resulting in direct losses over $1.2 billion for U.S. in 2003 [1].

We can find many preventive and detective solutions for phishing threats as provided by MarkMonitor, Panda Security, Verisign, Internet Identity, Cyveillance, RSA, WebSense, etc. [10], most of them are based on detecting fraudulent emails and embedded URL, identifying and closing down the scam site, bombing phishing sites with dummy information (but apparently real) in order to confuse the attacker making it difficult to distinguish real data from dummy data. The use of digital certificates is also a solution proposed as a countermeasure for phishing attacks. From our investigation we concluded that the use of digital certificates for server authentication is not enough against phishing and pharming threats. This is for many reasons, for example many users do not pay enough attention to the digital certificate details or many others do not have the knowledge to perform a correct validation of the digital certificate [21, 22]. In addition we want to remind the fact that the attacker could decide not to use encrypted traffic (HTTP instead of HTTPS).

We consider that all previous listed solutions are not enough in order to provide a secure environment because some of them are reactive solutions and others do not comply with security policies (e.g. deny as default, allow only permitted, etc.). In particular for blocking an attacker site, detecting fraudulent emails is like making a black list, and this is the opposite of allowing only permitted.

Other solutions such as the use of two factor authentication are not enough: if we only authenticate the user, we have to authenticate also the server because we consider that both entities must be considered mutually untrusted. For this reason, in order to work in a secure way in presence of phishing attempts we propose a multi-factor mutual solution.

Secure Electronic Transaction (SET) was a standard protocol for securing credit card transactions over insecure networks, specifically, the Internet [18]. SET is based

Table 1: Phishing statistics for year 2006

2006			
	Oct	Nov	Dec
Valid Phishes	3678	10044	11309
Invalid Phishes	7061	18130	20352

Table 2: Phishing statistics for year 2007

2007			
	Jan	Feb	Mar
Valid Phishes	18077	19947	10515
Invalid Phishes	30509	25647	11620
	Apr	May	Jun
Valid Phishes	40549	43789	11124
Invalid Phishes	77709	53263	15529
	Jul	Aug	Sep
Valid Phishes	9847	8835	10613
Invalid Phishes	13417	12490	14174
	Oct	Nov	Dec
Valid Phishes	5997	10044	11247
Invalid Phishes	9230	14432	15529

on digital certificates and has the same limitations discussed for digital certificates solutions. In addition SET does not address expressly other threats such as Man-In-The-Middle.

Next, we report phishing statistics about total submissions and valid phishing attempts of the first day of each month. Total submissions comprise all submissions, not yet verified, delivered to PhishTank. Valid phishes are all submissions verified by PhishTank as real phishing attempts. These statistics are elaborated by PhishTank [14]:

As shown in Table 1, in 2006 only statistics from October are available. On 1st December, 20352 phishing submissions were reported and 11309 were valid phishing attempts [14].

In Table 2, phishing statistics for year 2007 are reported, taken from PhishTank [14].

In Table 3, the statistics from January to June 2008 are reported. It is possible to appreciate an average of 10000 scams every month.

As shown in Table 2, the biggest number of reported valid phishing attempts happened on May 2007 with more than 53000 of total submissions and more than 43000 were valid scam attempts. Normally just half of the reported sites are real scam sites but in this case valid submissions are more than 80 percent. On March 2007 valid submissions were more than 90 percent with more than 10000 valid submissions. From data reported for years 2006, 2007 and 2008 we can estimate an average of 15000 submissions reported to PhishTank and around 10000 valid phishing attempts. If the cost for each phishing incident is around 900$, as reported by Gartner [3], we can calculate a direct monetary loss of 90 million dollars per month just considering only those reported to PhishTank. By addressing phishing threats it is possible to save a loss of money and in addition new businesses will be made thanks to the increment in the customer trust and confidence and a consequent increment in the service demand.

Table 3: Phishing statistics for year 2008

2008			
	Jan	Feb	Mar
Valid Phishes	11364	13208	11153
Invalid Phishes	15339	17303	15543

Nowadays there are many organizations devoted to collecting phishing information as phishing attempts or phishing statistics, so the data reported above represent just one of these sources. This implies that the statistics reported here are not the total but can give an idea about the phishing presence in our society. The most popular phishing targets are financial entities but this kind of threats is affecting also non-financial entities. On June 2008 in first position we find PayPal with 5743 valid phishing attempts, second is JPMorgan with 1594 and so on.

As presented in the previous paragraph, a huge number of phishing attempts exist, this implies a social and economical impact [1, 20]. The social impact is reported by Bajaj [1]: "Phishing has already taken its toll. Consumer confidence in email is at an all time low. Sixty-seven percent, or 150 million, U.S. consumers don't use banking online today. And, over 88 million online banking customers would switch bank, or reduce online banking usage".

In addition to the indirect losses produced by the low demand and usage of the e-banking services, there are direct losses. The Computer Crime Research Center (CCRC) is a non-profit, non-governmental and scientific research organization. CCRC reported on 2004 an article entitled: "The financial losses of Russian businesses caused by "carder" reached $20,000,000". Carders are illegal organizations specialized on counterfeiting plastic cards and to use Internet for receiving information on card holders and card numbers [11].

Gartner reports that the average dollar loss per incident in 2007 was $886 and the cost of phishing attacks is calculated on 3.2 billion dollars for 2007 in US only [3]. Virus Bulletin, on 2007, reports that Malware and Phishing cost more than 7 billion dollars in two years [19]. In order to show an example of personal losses we report the case between the Bank of Ireland and a group of customers that fell victim to a phishing scam that drained 160,000 Euros ($202,000) from their accounts [6].

Consequently to the huge losses we consider to study accurately the phishing problem in order to provide a preventive solution. The use of a preventive solution implies

that it is possible to save more than 3.2 billion dollars only in the US and in addition new businesses are assured thanks to the increment in the customer security which directly influences with an increment in the customer confidence and in the service demand [1].

3 Proposed Method

3.1 Authentication Threats and Scenarios

We made a detailed study of the authentication process and the vulnerabilities that affect this process. In this section we present the authentication process risk analysis. Next, a few scenarios are presented, each of them with their corresponding vulnerabilities. The first scenario is the common authentication method currently used by the web-banking pages of most financial entities. This scenario is vulnerable to phishing and pharming as server identity and authentication resides in logo and web appearances, and in the server digital certificate respectively. This is an improper authentication method as the logo and appearance can be easily copied by an attacker. Regarding digital certificates, many users do no validate them correctly for many reasons: they don't have enough skills to do it or they don't pay the necessary attention. Digital certificates are better validated by software.

Other vulnerabilities of this system are Man-In-The-Middle (MITM) and Spyware, as user authentication is based on a constant value, so that if an attacker gets user credentials he will be able to use them wherever he wants. In order to work in a safe way under this kind of attacks, we need to introduce One Time Passwords. In this manner the attacker, even if he gets authentication details, will not succeed anymore.

Another threat that affects this authentication model is malware or banking Trojans which could be able to affect the user environment and take complete control over it. In order to mitigate this risk we need to provide a safe and certified environment.

The first scenario is based on one factor authentication. The server requires the customer to introduce username and password in order to be authenticated. Obviously we found that the system is vulnerable to phishing and pharming attacks as the server authentication process is absent or weak.

In the next scenario, the phishing threat is intended to be addressed. In this case, the user requests for server authentication first by introducing the customer identification. Here the vulnerability exists in using a fixed identifier to request the server authentication. This vulnerability exposes the system to Spyware and man-in-the-middle threats. In addition, after identifier interception it would be possible to perform a phishing or pharming attack against the falsified user identifier. If identifiers are generated sequentially, the system would be easily compromised by requesting all server authentication values and incrementing and decrementing users' identifiers. This scenario is vulnerable to phishing after key interception, to Man in The Middle as no one time password has been used, and to Malware or Banking Trojan because if the customer operating system has been infected we cannot trust on it.

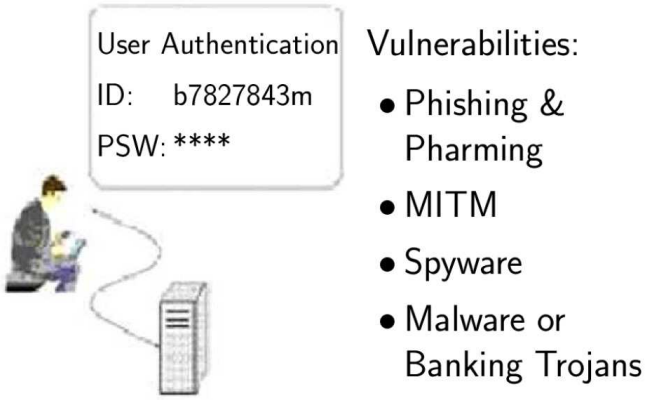

Figure 1: Common authentication scenario vulnerabilities

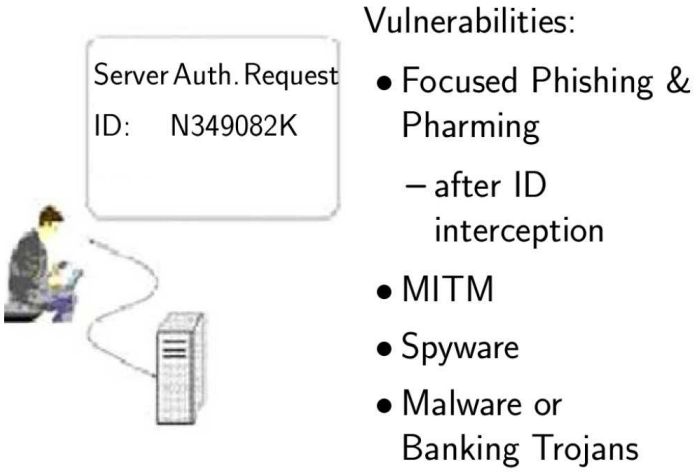

Figure 2: Server authentication request

In order to work in a secure way in a compromised environment, as could be the user operating system infected by a banking Trojan, we need to use a trusted environment where we can assure that data cannot be tampered.

In the next scenario, Scenario Three, phishing and pharming threats are addressed in the same way as in the previous scenario. Passive interception attacks and Spyware are also addressed by introducing One Time Password property for authentication requests and an additional authentication factor for user and server authentications. Unfortunately Scenario Three cannot work in a secure way when the user environment is compromised by Malware, banking viruses or Trojans. This is because if the user's operating system has been infected, we cannot trust it. The malware could modify any data, e.g. destination account number, amount of transaction, etc.

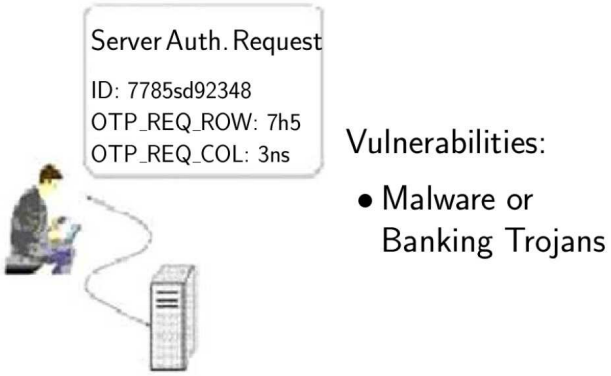

Figure 3: Scenario 3 - Server authentication request

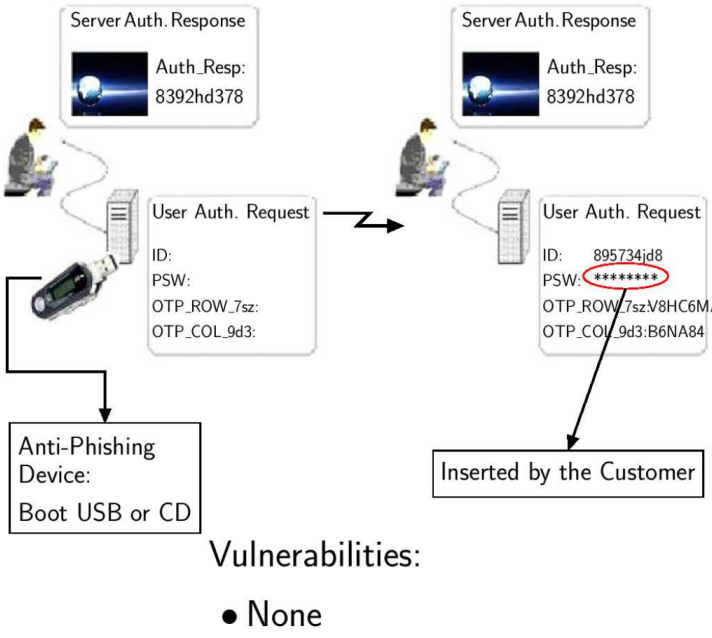

Figure 4: Anti-phishing device usage

Under the presence of phishing or pharming attacks, this scenario would expose the most sensible authentication factor. This is because in order to authenticate an entity, all credentials are requested together. In order to address this problem, we must use the proposed Factor Protection Model (see below) because by requesting and verifying one authentication factor at a time, sequentially and mutually, as soon as we detect an authentication fault, we will not continue with the authentication process. In this way, if less sensitive factors are requested first, the integrity of the most sensitive authentication factor can be preserved.

In the following scenario, we present the most secure scenario. The idea is to try to provide a possible solution to an infected user network or operating system. This would be absolutely the worst case and the most difficult to be addressed. If the user boots the computer from a secure device with all software unchangeable and digitally signed (e.g. CD or USB), then this environment cannot be infected by viruses or malware residing on the customer's machine.

The user operating system is not used, instead an inalterable, trusted and signed operating system is used.

3.2 N-Factors Mutual Authentication

Web banking systems, as any other web application, use HTTP for data transfer. Regarding HTTP, all communications must be secured with the SSL/TLS protocol (i.e. HTTPS), and it is strongly recommended to use the POST method for sending data wherever possible. This is because when using the GET method, data is stored on history and URL caches in the local machine.

The best authentication method is mutual multi-factor authentication, as when carried out in a proper way, it helps to detect, in a preventive manner, phishing and pharming attacks. Such authentication process comprises key interchange, server authentication, and user authentication.

A part of our work has consisted in defining security requirements for mutual authentication, and every detail has been taken into account and included in the risk analysis; any non-compliance of the defined rules will make the application vulnerable and the purpose of mutual authentication will fail drastically.

The goal of any authentication method is to work reliably under adverse security conditions in a hostile environment, and in particular it must be resistant to "man-in-the-middle" attacks.

Thanks to this model, the more sensible authentication factor will be protected from theft because at first, if there is no coincidence between the actual server response and the expected server response, the user will not follow with the authentication process as he o she will have detected the hijacking attempt.

Thanks to all security requirements defined, this system is able to provide the maximum and most secure authentication method.

The authentication process will involve two parts: for easy understanding we will call one "user" and the other "server". In order to consider all possible situations, three authentication models have been defined. Each of these models is based on a different hypothesis. All three models can work with 3 authentication factors. The three factors are: something you have, something you are, or something you know. As reported by [7, 8], Three factor authentication is the highest authentication level.

3.2.1 Basic Model

This model is based on the hypothesis that only one of the parts involved in the authentication process is the potential hijacking victim. For this reason it is required that the potential hijacking victim (e.g. Server) must be authenticated first. In this authentication model all authentication factors will be requested and evaluated in

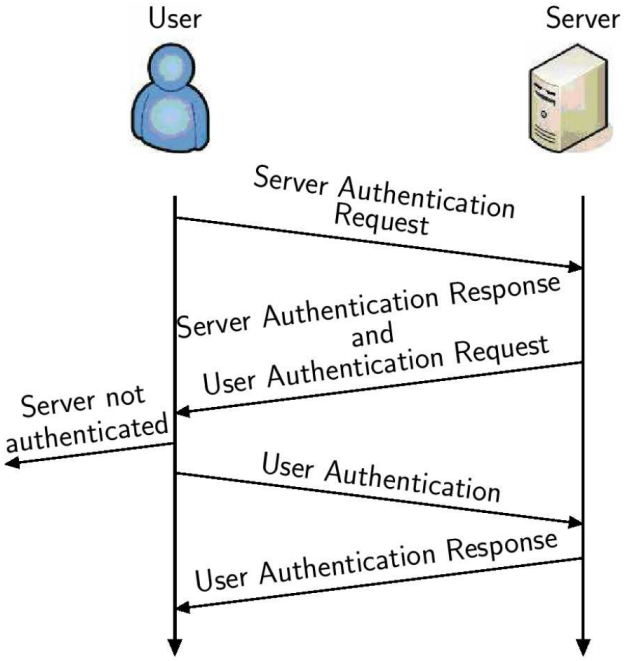

Figure 5: Basic model

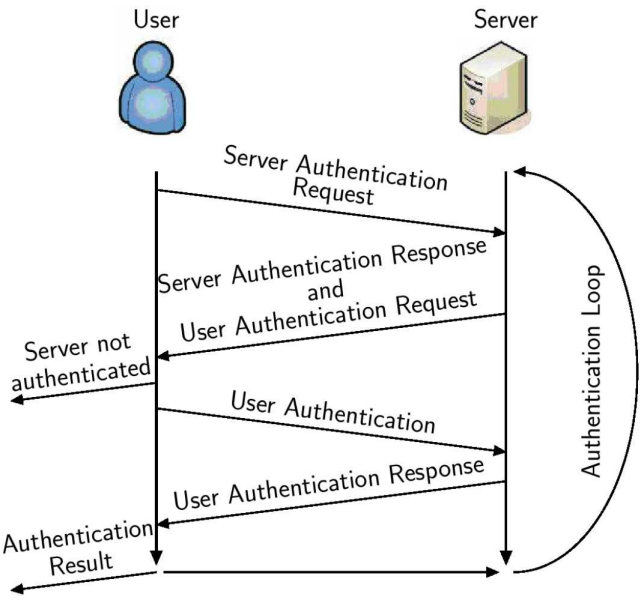

Figure 6: Factor protection model

the same request. This model is faster than the other two, the factor protection model and the factor protection mixed model. The basic model authentication process is shown below:

As shown in Figure 5, first the user requests server authentication. If the server response matches correctly the expected data, the server will request user authentication. It is very important to introduce one time password on each authentication and to provide confidentiality in order to be resistant also to Man in the Middle attacks. It is also important to be resistant to brute force attacks and then to block the account temporally at the N-th consecutive authentication failure. N must be fixed to a number small enough in order to avoid credentials enumeration.

Following the model proposed in Figure 1 it is clear that phishing cannot work properly as the user verifying the server response would realize immediately the hijacking attempt, because the server will be authenticated by an authentication factor which has been chosen by the user at the account creation time. The proposed model is expected to be easy to complete and understand by more than 99,9 percent of customers; instead, the percent of customers able to recognize a valid certificate is much lower, confirmed by Dhamija's research [2].

The proposal consists in a unique authentication flow composed by two parts, one is the server authentication and the other is the user authentication; in this way it is not possible to complete successfully the authentication process without a correct validation of all authentication factors. Another benefit of the proposed model is that it is easily applicable to the nowadays used authentication process. This is because only few changes on the actual authentication model must be applied in order to implement our Base Model, Factor Protection Model or Mixed Factor Protection Model.

In order to demonstrate that the Basic Model is the right weapon to be used against phishing, pharming and information interception, we summarize the benefits of this solution: the impact of adapting current login systems to the proposed model would be very low, it is easily understandable by the user, it provides a very high security level, it works securely in presence of phishing attempts and information interception, and under phishing attacks it preserves user keys.

3.2.2 Factor Protection Model

This model is based on the following two hypotheses:

- Both parts involved in the authentication process are equally potential hijacking victims.
- At least one authentication factor is more sensible than the others.

Under these hypotheses we want to save the most sensible authentication factors. In this case there is no requirement about who will be authenticated first. Here the restriction is that each part must be verified in a sequential order factor by factor. The factors are evaluated from lowest to highest factor sensitivity level. The first part will verify authentication of one factor of the other part and then this latter part will verify an authentication factor of the first part. In this way the most sensible factor will be protected by the verification steps of the previous authenticated factors. Only if all previous authentication steps have successful results, will it be possible to evaluate the next authentication factor.

As shown in Figure 6, the Factor Protection Model verifies factor by factor, this is because the parts involved in the authentication process are mutually un-trusted and both are equally potentially hijacking victims. In this way it is possible to preserve most sensitive credentials. In our classification we consider that the least sensitive authentication factor is the user digital certificate, next is the One time password and last the symmetric key (e.g. user password). Obviously, the digital certificate does not represent a danger because if it is not affected by any vulnerability, the private key should be safe. One time password is sensitive because it allows performing one step forward in the authentication process or in the requested service. The most sensitive factor is the symmetric key because it is valid for a long period of time, much longer than one time passwords as the latter expire at first use.

3.2.3 Mixed Factor Protection Model

This model is based on the hypothesis that both parts involved in the authentication process are potential hijacking victims. Another assumption is that all authentication factors have the same sensitivity level. This model is a combination of both previous cases. In this case at least one factor must be evaluated after the successful evaluation of another authentication factor. No restrictions have been defined for other potential factors involved in the authentication process. This process is faster than Factor Protection Model as it allows the simultaneous evaluation of more than one factor.

Mixed Factor model would be a good choice in order to make a flexible and faster authentication system. A possible implementation of the Mixed Factor Protection Model would be as follows:

1) Server Digital Certificate Validation;
2) Customer Digital Certificate Validation;
3) Other Server authentication factors;
4) Other Customer authentication factors.

3.2.4 Anti-phishing Device

This device will perform part of the entire authentication process.

In this device a maximum of two of the three required authentication factors will be stored. One factor, the "know factor", must not reside on this device. The device will not store "know factors" of either user or server entities. In this way, to be able to successfully complete the authentication process customer contribution is required. This is because in the case of losing the device, if someone found it, he or she would not be able to perform the authentication process correctly.

The device stores a little auto boot operating system, which cannot be altered. All software is signed and when it communicates with the server, the digital signature of both parties will be verified. It is not possible to continue without valid signatures. The idea is to provide a system similar to Knoppix boot CDs.

In this way, if the device has its own operating system, the system is also secure if the customer operating system is infected by malware which could potentially alter data such as the amount of money or transaction destination, bank account number, etc.

The device will perform integrity controls and will provide a further layer of confidentiality by encrypting with asymmetric encryption all information travelling between both entities.

The authentication factor with One Time Password property, for both entities, could be stored on the device. The user digital certificate will also be stored in the device.

3.2.5 A Real Case of the Basic Model

In the example of Figure 7, an implementation of the basic model is presented. In particular, two factor authentications are required for both entities. The process is the following: first the user requests for login page (1), after the page reception (2), the user requests server authentication (3), if the server response is correct (4), the user provides his credentials (5); if user credential matches correctly (6) then the authentication process ends successfully.

Below are reported the requirements for credentials and data that take part in the authentication process shown in Figure 3.

- **Id_Card:**
  Length = at least N digits *
  Char Space = [a-zA-Z][0-9]
  Generation: Random
- **Req_Auth:**
  Length = at least O digits * Char Space = [a-zA-Z][0-9] Generation: Random
- **Auth_Code:**
  Length = at least M digits *
  Char Space = [a-zA-Z][0-9]
  Generation: Random
- **UserPredefinedObject:**
  Type: Object, image, interface appearances, logo
  Char Space = [a-zA-Z][0-9]
  Generation: User chosen
- **USR_ID:**
  Length = at least R digits *
  Char Space = [a-zA-Z][0-9]
  Generation: Random
- **USR_KEY_DER:**
  HASH(SRV_RND_KEY + USR_KEY)
- **USR_KEY:**
  Length = at least P digits *
  Char Space = [a-zA-Z][0-9]
  Generation: Random

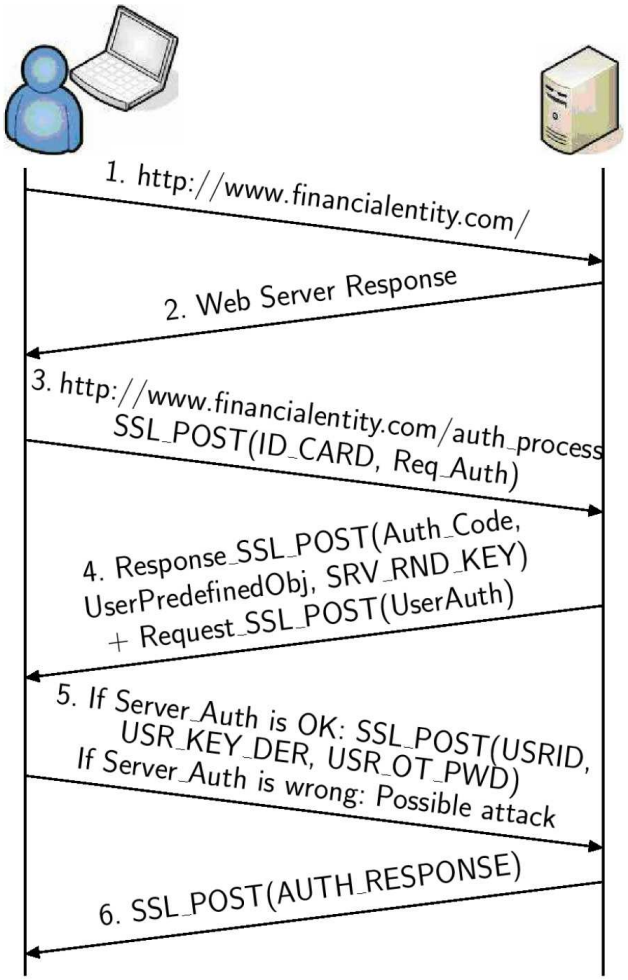

Figure 7: An implementation of the basic model

- **USR_OT_PWD:**
  Length = at least Q digits *
  Char Space = [a-zA-Z][0-9]
  Generation: Random

The numbers N, O, M, P, Q, R, must be fixed to a value which avoids key enumeration. It can be changed depending on the key length.

4 Conclusions

Our objective was to propose an authentication method resistant to phishing, pharming attacks.

The goal has been reached by basing the protection on the mutual multi-factor authentication process, of which each detail has been accurately studied. As mentioned, the main proposed novelty is this mutual authentication process, which is responsible for making the financial entity system highly invulnerable and immune to phishing and pharming attacks. In addition, security is provided against a compromised client environment, like virus or spyware infections on the client side, as such malware could be able to steal the banking customer's account access information. Another benefit of the proposed solution is that it is easily applicable to the current systems and easily understandable by the customers. This implies that no technical knowledge is required in order to distinguish a valid digital certificate from a non-valid digital certificate.

In order to take into account all security topics not covered by the mutual multi-factor authentication method, a number of security policies have been defined in this research project. These policies are very important in order to develop a "secure" E-Banking platform. Specific security policies have not been explained in this paper for obvious reasons. This authentication model has been simulated in order to demonstrate its robustness. Simulation results confirm that the model is not vulnerable to phishing and pharming attacks. We got more than 350 users opinion and more than 99 % detected the attack when the server response did not match as expected.

References

[1] S. K. Bajaj, S. Hansen, "Social effects of phishing on e-commerce," *International Conference on e-Commerce*, pp. 215-219, Netherlands, July 2008.

[2] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," *Proceedings SIGCHI Conference Human Factors in Computing Systems*, pp. 581-590, Montréal, Canada, Apr. 2006.

[3] A. Litan, *Phishing Attack Victims Likely Targets for Identity Theft*, Gartner First Take FT-22-8873, Gartner Research, 2004.

[4] S. Loftesness, *Responding to "Phishing" Attacks*, Glenbrook Partners, 2004.

[5] A. S. Martino, *Security Policies Proposal for E-Banking Services: Anti-Phishing Approach*, Ph.D. thesis, Universitat Pompeu Fabra, Barcelona, Spain, 2008.

[6] R. Miller, *Customers spar over phishing losses*, 2010. (http://news.netcraft.com/archives/2006/09/13/bank_customers_spar_over_phishing_losses.html)

[7] New Zealand State Services Commission, *Guidance on multi-factor authentication*, 2010. (http://www.e.govt.nz/standards/e-gif/authentication/guide-multi-factor-auth/chapter3.html)

[8] Thales ISS, *Advanced authentication*, 2010. (http://www.thales-esecurity.com/Whitepapers/documents/Advanced_Authentication.pdf)

[9] Anti-Phishing Working Group, 2010. (http://www.antiphishing.org/)

[10] Anti-Phishing Working Group, *Vendor solutions*, 2010. (http://www.antiphishing.org/solutions.html)

[11] T. Saytarly, *Phishing costs $20,000,000 for Russian businesses*, 2010. (http://www.crime-research.org/news/14.10.2004/707/)

[12] Hispasec Lab, *Banking trojuan captures user's screen in video chip*, 2010. (http://www.hispasec. com/ laboratorio/ banking_trojan_capture_video_clip.pdf)

[13] D. Watson, T. Holz, and S. Mueller, *Know your enemy: phishing*, 2010. (http://www. honeynet. org/ papers/phishing/)
[14] OpenDNS, 2010. (http://www.phishtank.com/)
[15] Wikimedia Foundation, *Man in the middle attack*, 2010. (http://www.wikipedia. org/ wiki/ Man-in-the-middle_attack)
[16] Wikimedia Foundation, *Pharming*, 2010. (http:// www.wikipedia.org/wiki/Pharming)
[17] Wikimedia Foundation, *Phishing*, 2010. (http:// www.wikipedia.org/wiki/Phishing)
[18] Wikimedia Foundation, *Secure electronic transaction*, 2010. (http://www.wikipedia.org/wiki/ Secure_electronic_transaction)
[19] Virus Bulletin Ltd., *Malware and phishing cost US users $7 billion in two years*, 2010. (http://www. virusbtn.com/ news/2007/08_08.xml)
[20] T. N. Jagatic, N. A. Johnson, M. Jakobson, and F. Menczer, "Social phishing," *Communications of the ACM*, vol. 50, no. 10, pp. 94-100, Oct. 2007.
[21] R. S. Katti and R. G. Kavasseri, "Nonce Generation For The Digital Signature Standard," *International Journal of Network Security*, vol. 11, no. 1, pp. 23-32, July 2010.
[22] C. Yang, "Secure Internet Applications Based on Mobile Agents," *International Journal of Network Security*, vol. 2, no. 3, pp. 228-237, May 2006.

Antonio San Martino Pace Antonio is currently the CEO of D&P Security and teacher at Universitat Politecnica de Catalunya (UPC). Antonio is also a PhD with more than 8 years experience in information security (Chief Security Officer in a multinational company, information security researcher, system administrator, IS auditor, European projects leader and currently Chief Security Officer).

Xavier Perramon is a lecturer and researcher at the Department of Information and Communication Technologies of Universitat Pompeu Fabra (UPF), Barcelona, Spain, since 2000. He graduated in Telecommunications Engineering (1989) and received his Ph.D. degree (1997) from Universitat Politecnica de Catalunya (UPC), Barcelona, Spain. From 1992 to 2000 he was a lecturer and researcher at the Computer Architecture Department, UPC.

Dr. Perramon has participated in standardisation activities in the area of interchange and manipulation of structured multimedia information, serving as one of the editors of the Open Document Architecture (ODA) standard from 1991 to 1997, and has also participated in research activities in various EC-funded projects in the areas of multimedia interchange since 1990 and information security since 1996. His current research interests are in the protection of multimedia communications.