A Mechanism for e-Banking Frauds Prevention and User Privacy Protection

Rosalia D’Alessandro • Manuel Leone

G. R. Romoli 274, 10148 Turin, Italy – Telecom Italia SpA
{rosalia.dalessandro | manuel.leone}@telecomitalia.it

Abstract

In this paper we will discuss how recent trends in malware evolution will probably require a change of the internet banking security paradigms currently in use. Specifically, we will demonstrate how next generation malware may defeat the most recent strong authentication mechanisms put in place by several financial institutions. These new attacks clearly require a change on current schemes and, at the same time, a definitive reduction in the final user responsibility. Too often the user's behavior adds a weak layer which can be exploited by several techniques, such as Social Engineering attacks. Therefore, a new generation of automatic and hardware-based mechanisms should be deployed, in order to both increase the security level intrinsically offered by the technology, and reducing the exposure to Social Engineering risks. They have to work transparently, minimizing any kind of misuse that could be source of vulnerabilities.

1 Introduction

Convenience is the key reason of why millions of people are opting out of traditional banking services for the online version. This change is promoted by banks and other financial institutes in order to make saving on operating costs. However, fraudulent activities have recently increased just due to this migration, at least according to most analysts.

Traditional online frauds typically occur in a two-step process. Firstly, the offender steals the customer’s account information (e.g. her credentials); secondly, the offender will use that information to move victim’s money to another account or withdraw it, usually involving some other third party.

The most popular schemes include:

- Phishing or Passive Attacks Scheme: representing a well-known technique to retrieve confidential information from a user by posing as a trusted authority. Most often, with the help of a deceptive email, the attacker redirects the victim to a mirror site to obtain the consumer’s personal information such as online banking username and password. Typically this type of attacks is clientless because it does not make use of any software component installed onto the user’s PC.

- Trojan Horse or Active Man In The Middle Attack (MITM) Scheme: unfolds when malicious software (malware) embeds to a consumer’s PC without the user’s consensus. Trojans often come in links or as an attachment from unknown email senders. After installation, the software detects whether a person is accessing banking sites and, in this case, it records...
username, password and any other user’s sensitive data. Soon after, the stolen data will be transmitted to a collector component notifying the attacker on the availability of new data.

Since the end of the last year, a new malware trend has been showing an interesting switch from the traditional passive scheme to an active form, the phishing attack. In this case, typically with the help of a Trojan, an attacker can take the control of the link between the IP address and the DNS server name it is responding to. In this way, any data sent and received by the legitimate server can easily be manipulated in real-time.

A case in point is the ZEUS Trojan (also known as Zbot, PRG, W32/Exe, Gorgon and Kneber), firstly identified in July 2007 but mainly spread in 2009 through drive-by downloads and phishing schemes. It has been estimated this Trojan infected, at the end of 2009, approximately 1% of the PCs in the US (around 3.6 million) [Ref109] and it is still active in 2010. This malware family can be considered the largest botnet over the internet (although the estimation of a botnet size is still an open problem in literature).

Top 10 Victim Countries

![Pie chart showing top 10 victim countries](image)

**Fig. 1**: Top 10 country affected by the Zeus botnet [NetW10].

It infected consumer PCs, waited for them to log onto a list of targeted banks and financial institutions [StDo10], and then stole their credentials, sending them to a remote server in real time [FaCh10]. The estimated targets counted about 950 different financial institutes.

Zeus provides a ready-to-deploy package easily purchased and also freely traded online, so that for hackers it was very easy to distribute their own botnet. In addition, the ease-of-use of Zeus means the malware can be used widely and is highly prevalent, allowing the most novice hackers to easily steal credentials and other sensitive data for financial gain.

Furthermore, its malware family was totally undetectable by the traditional anti-virus [Trus09]. Due to the most recent techniques, such as polymorphism, metamorphism, packing and emulation, traditional anti-malware solutions are unable to detect completely new or just variants of well-known malware. In a recent study, NSS Labs [NaaL10] shows, starting from well-known malware based on Operation Aurora payload (Hydra variant), how simple is building malicious code unidentifiable by anti-malware products. Although the original version was caught by six out of seven anti-viruses tested, just one product had been able to detect the NSS variant, too.

In this scenario, several countermeasures have been proposed and deployed to reduce the risk related to online banking frauds. One of the most adopted schemes is the strong authentication mechanism based on the one-time passwords (OTPs). According to this scheme, the authentication/authorization credentials are generated "on the fly" by either hardware or soft-