Chapter VII

Strong Authentication for Financial Services: PTDs as a Compromise between Security and Usability

Gianluigi Me
University of Rome, Italy

Daniele Pirro
University of Rome, Italy

Roberto Sarrecchia
University of Rome, Italy

ABSTRACT

Currently the most popular attacks to the E-Banking Web applications target the authentication systems relying on the single-side client authentication, showing their definitively ineffectiveness for financial services. Furthermore, most of the Web authentication systems have been developed on the classic username/password mechanism or One time Password systems using a single channel, either mobile or Web, generating an authentication system at inadequate level, enforcing a false perception of security, as phishing shows. The two factors authentication is not the panacea, but mitigates many threats, especially when combined with a Personal Trusted Device, as the popular smartphones represent. As a rule of thumb, the adoption of authentication systems to provide services B2C is driven by its ease-to-use more than the robustness of the adopted security system. For this reason, the proposed solution represents a system which tries to preserve the usability and to strengthen the authentication, with a combined Web/mobile authentication system.
**INTRODUCTION**

A very crucial phase of a web transaction is represented by the user authentication. During this step many problems can occur and many attacks are possible, whose target is to access the restricted resources. In order to face this threat, current systems frequently adopt the HTTP basic authentication mechanism even if the applications are critical. Further authentication mechanisms, described in the following sections, have been proposed to improve web authentication security with regard to user friendliness, not yet representing a panacea, still being prone to different attacks. As Schneier (2005) suggests, two-factor authentication mitigates, but not definitively solves, this problem and no solution is foolproof.

According to the Gartner survey of 5,000 online adults in August 2006, an estimated 24.4 million Americans have clicked on a phishing e-mail in 2006, up from approximately 11.9 million in 2005, while 3.5 million have given sensitive information to the phishers, up from 1.9 million adults last year. Currently, the phishing effectiveness has not changed since August 2006, revealing, instead, a slight raising shape of the victims. For this reason, new forms of combined attacks appear, as for the man-in-the-browser attack, where trojan horses can modify the transactions on-the-fly. Furthermore, one of the most famous recent wiretapping scandal (Prevelakis & Spinellis, 2007), the greek cellphone caper, confirms that the definitive solution for financial services over external, untrusted networks is to embed security in the end-to-end partecipant terminals.

In this paper we firstly classify the e/m-banking threats, based on an attack tree model, then we introduce the state of the art of the e/m-banking authentication systems and, finally, we will present a new authentication system, based on a combined web/mobile procedure, taking into account security and usability as major requirements. The basic authentication mechanism is integrated with a challenge/response process and an One Time Password (OTP). The challenge is issued from an authentication server and has to authenticate a mobile device, typically a cell phone with Java capabilities. This device can communicate with any other involved part through a fixed terminal, typically a personal computer, via a Bluetooth connection. The mobile device, once accepted, performs the authentication with the web site or application. This final step is accomplished using a temporary one-time password.

**STATE OF THE ART**

**The Attack Tree for Bank Account Compromising**

A threat model describes threats than can be realized by the exploitation of vulnerabilities, through attacks. The graphical description of the threat model is based on attack trees (Schneier, 1999), which provide a formal methodology to analyze the security of systems in a tree structure, with the goal as the root node and different attacks as leaf nodes. The Figure 1 presents the threat model, which studies attacks against e/m-banking applications through current and next generation terminals.

The root node represents the final target of the attacker, which is the compromise of the user’s bank account: we characterize the attacks by four main targets, the User, the User Terminal, the communication link and the banking server. We will use the usual notation, per level: root node is level 0 (indicated as 0), the nodes at j-th level are numbered [0,...]n starting by the left side (e.g., the Web page obfuscation node will be indexed as 1.6.5.5).

Since many attacks are, unfortunately, well known, we define the most meaningful from an overall security perspective and new ones. (see Table 1)

1.1.2.1: Hidden Code. The use hidden code within a web-page that exploits a known vulner-