Chapter XI
Defeating Active Phishing Attacks for Web-Based Transactions

Xin Luo
Virginia State University, USA

Teik Guan Tan
Data Security Systems Solutions Pte Ltd, Singapore

ABSTRACT

Till now, the best defense against phishing is the use of two-factor authentication systems. Yet this protection is short-lived and comparatively weak. The absence of a fool-proof solution against Man-in-the-Middle, or Active Phishing, attacks have resulted in an avalanche of security practitioners painting bleak scenarios where Active Phishing attacks cripple the growth of web-based transactional systems. Even with vigilant users and prudent applications, no solutions seem to have addressed the attacks comprehensively. In this chapter, the authors propose the new Two-factor Interlock Authentication Protocol (TIAP), adapted from the Interlock Protocol with two-factor authentication, which is able to defend successfully against Active Phishing attacks. They further scrutinize the TIAP by simulating a series of attacks against the protocol and demonstrate how each attack is defeated.

INTRODUCTION

The current wave of phishing attacks against Internet Banking and Transaction web sites is only the tip of the hacking iceberg in the field of information systems security. Yet, these relatively unsophisticated attacks have already catastrophically resulted in significant monetary loss and a major source of embarrassment to the financial institutions. This predicament has drawn increasing attention from both security researchers and practitioners. Early research has shed light on
Defeating Active Phishing Attacks for Web-Based Transactions

such tactical anti-phishing methods as having
Internet service providers (ISPs) involved to
close phishing websites and launching retaliatory
services to proactively block phishing traffic.
However, these approaches are time-consuming
and expensive, and are even useless in countries
that lack relevant anti-phishing regulations (Geer,
2005). While organizations are scrambling to
deploy costly two-factor authentication solutions
(i.e. having a one-time password in addition to a
normal password) to cope with the problem, such
remedies may just be short-lived as the hackers
can easily deploy the more sophisticated active
phishing attacks to thwart the security and the
additional effort could cause consumers to avoid
Internet banking (Geer, 2005).

Defined as attacks that use both social engi-
neering and technical subterfuge to steal consum-
ers’ personal identity data and financial account
credentials (Goth, 2005), phishing incidents have
gradually eroded consumer confidence in online
banking (Geer, 2005) and further imposed im-
measurable losses for corporations in terms of
time and resources. In addition to public educa-
tion, authentication such as one-time password
technology may be successful at preventing off-
line or Static Phishing attacks (Bellovin, 2004).
While researchers have previously addressed
the technological concerns of Static Phishing
and proposed relevant solutions such as phishing
webpage detection based on visual similarity (Liu
et al., 2005), mail filtering method (Inomata et al.,
2005) and XUL and JavaScript-based browser
extensions (Kirda and Kruegel, 2005), the field
of Active Phishing is still unexplored as the pos-
sibility of Active Phishing or on-line Man-in-
the-Middle attacks has been troubling security
practitioners and consultants (Schneier, 2005)
for a while already. In general, Active Phishing
can be defined as the use of a reverse proxy in the
middle to dynamically access the actual site while
phishing the user, thus giving the impression that
the user is communicating with the correct site,
while the hacker in the middle has actual control
of the session and may modify the contents to
achieve illegitimate gains.

Along with Herzberg’s argument that SSL/
TLS is limited and weak for site impersonation
and scam sites (Herzberg, 2004), we believe that
the difficulty in preventing Active Phishing at-
tacks for web-based transactions is due to the
fact that the HTTP-over-SSL protocol is easily
reverse-proxied. In fact, all SSL-VPN solutions
exploit this reverse-proxy capability somewhat
to support a seamless VPN tunnel between the
browser through the SSL-VPN gateway to the
backend application server. Hence, the SSL-VPN
gateway is in fact functioning as a “good” man-
in-the-middle to provide the VPN encryption
functionality.

The problem is further acerbated by the in-
herent fact that the Client executable content (i.e.
the HTML/JavaScript in the browser) is actually
downloaded from the Server. This means that the
server with which the browser is communicat-
ing with has full control over whatever content
is executed on the browser. Should the browser
be communicating with a phishing server, there
is no way that the actual server is able to bypass
this problem.

The painted scenario is bleak. A security-
conscious bank with a security-conscious user
base does not guarantee that the Internet banking
sessions between them are secure. Already, a case
of active phishing has been reported (Kirk, 2005),
and it is only a matter of time before the exploita-
tion of the vulnerability becomes widespread.

THEORETICAL BACKGROUND

The Interlock Protocol by Rivest and Shamir
(1984) is an elegant solution designed to defeat
hackers who attempt to eavesdrop on the com-
munication. In Figure 1, Alice and Bob is using
the Diffie-Hellman exponential key exchange
protocol (Diffie and Hellman, 1976) to establish a
shared secret key which can be used subsequently