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 article, we 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. We further scrutinize the TIAP by simulating a series of attacks against the protocol and demonstrate how each attack is defeated.

Keywords: interlock protocol; phishing; two-factor authentication

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 are 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 such tactical antiphishing methods as having Internet service providers (ISPs) involved in closing phishing Web sites and launching retaliatory services to proactively block phishing traffic. However, these approaches are time-consum-
ing and expensive, and are even useless in
countries that lack relevant antiphishing
regulations (Geer, 2005). While organi-
zations 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 prob-
lem, 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
engineering and technical subterfuge to
steal consumers’ personal identity data and
financial account credentials (Goth, 2005),
phishing incidents have gradually eroded
consumer confidence in online banking
(Geer, 2005) and further imposed immea-
surable losses for corporations in terms of
time and resources. In addition to public
education, 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 Web
detection based on visual similarity
(Liu, Huang, Liu, Deng, & Zhang, 2005),
mail filtering methods (Inomata, Rahman,
Okamoto, & Okamoto, 2005) and XUL
and JavaScript-based browser extensions
(Kirda & Kruegel, 2005), the field of active
phishing is still unexplored. The possibility
of active phishing or online man-in-the-
middle attacks has been troubling security
practitioners and consultants (Schneier,
2005) for a while already. In general, ac-
tive 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 imper-
sonation and scam sites (Herzberg, 2004),
we believe that the difficulty in preventing
active phishing attacks for Web-based trans-
actions 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 sup-
port 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 inherent 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 communicating with
has full control over whatever content is ex-
ecuted 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.

A security-conscious bank with a secu-
ry-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
exploitation 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
An Exploration Regarding Issues in Insider Threat
*Cybersecurity Breaches and Issues Surrounding Online Threat Protection* (pp. 1-23).
www.igi-global.com/chapter/an-exploration-regarding-issues-in-insider-threat/173125?camid=4v1a

A Projection of the Future Effects of Quantum Computation on Information Privacy
www.igi-global.com/article/projection-future-effects-quantum-computation/2463?camid=4v1a