Trusted Paths to Combat Emerging Phishing Threats

Collin Jackson
Stanford University

http://crypto.stanford.edu/antiphishing
Visual Ambiguity

Which dialog is a fake?
Banking and online commerce

- Primary goal is customer acquisition and retention
- Willing to accept manageable fraud risk & use analytics
- Focus is on whether customers feel secure
Homograph attack

http://www.bankofthewest.com/BOW/home/index.html
Homograph attack

90% effective attack [DTH06]
Two-Way Authentication

(a.k.a. PassMark, SiteKeys, Signin Seal, eTrustID)

• Trusted image established during account setup
• “Before logging in, look for your trusted image.”
Pre-Authentication

• **Problem**: Can’t just show image to anyone
Error Tolerance

• **Problem**: Users have a (well-deserved) expectation of site errors

• 92% effective attack

[SDO07]
One-Time Passwords

• Put a short lifetime on stolen password
• Forces phisher to perform an online man-in-the-middle attack
• MITM attacks require sophistication...
MITM made simple
MITM toolkit

New tool enables sophisticated phishing scams

By Jon Evers
Staff Writer, CNET News.com
Published: January 16, 2007, 11:47 AM PST

Security experts at RSA have come across a new tool that automatically creates sophisticated phishing sites, a sign that cybercrooks are getting increasingly professional.

The tool, which RSA calls the "Universal Man-in-the-Middle Phishing Kit," is available on underground online marketplaces for about $1,000, Jens Hrinricht, RSA's product marketing manager for fraud services, said in an interview Wednesday.

"Unlike other phishing kits which have been in existence for quite some time, this kit is unique because with a very simple user interface you can choose whatever site you'd like to spoof," Hinricht said. "The arms race continues; we on the security side have to continue to escalate resources and invest in technology."

Phishing scams are a prevalent online threat that typically use fraudulent Web pages and spawned e-mail messages to trick people into giving up personal information such as user credentials or credit card data.

Using the new kit, a fraudster only has to enter variables such as which site should be spoofed and where the fraudulent page will be hosted. The tool then produces a dynamic Web page in the PHP (Hypertext Preprocessor) scripting language. The fraudster hosts this
Browser Phishing Defenses
Negative Trust Indicators

- Appear at dangerous sites
- **Advantages:**
  - Warnings are easy to notice
- **Limitations:**
  - Requires constantly polling a blacklist or using imperfect heuristics
  - Most up-to-date blacklist imposes privacy cost
  - Stigma of false positives; may lead to desensitization
  - Users may expect warning to appear at every bad site
Positive Trust Indicators

• Suggests that site is “safe” to use
• Lock icon indicates encryption
• EV indicates site is controlled by a legal entity

• Advantages:
  – Encourages visitor to use the site

• Limitations:
  – Hard to notice absence (~50%)
  – Site may inadvertently host bad content (XSS)
  – Prone to spoofing (~50%)
Picture-in-Picture Attack
Trusted Paths

• Secure attention sequence or prefix
  – limited portability
  – requires pre-authentication
• Trusted image/theme
• Off-limits screen area
• Out of band communication

Starts with @@
Authentication for Identity 2.0
Missing Trusted Path
Missing Trusted Path

Identity Selector

Please select a card for xmldap.org

New Card  Delete Card  Cancel
Missing Trusted Path
(Weak) Trusted Path
Missing Trusted Path
Summary

- Phishing will adapt to new defenses
  - MITM toolkits defeat 2-way auth and OTP
  - Browser-based defenses aren’t foolproof
- Trusted paths can help
- Not all trusted paths are created equal
  - Additional complexity does not always help
  - Test targeted social engineering scenario
  - Measure actual effect versus user perception
Collin Jackson
collinj@cs.stanford.edu
http://crypto.stanford.edu/antiphishing