AntiPhish: An Anti-Phishing Browser Plug-in based Solution

IT UNDERGROUND

Technical University of Vienna
Politecnico di Milano

Engin Kirda
Christopher Kruegel
Angelo P. E. Rosiello

TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

POLITECNICO MILANO

March 2007 | Prague

Outline

- Introduction
- Phishing definitions
- Phishing menace, the economic point of view
- Types of Phishing Attacks
- A typical Attack
- Antiphishing Solutions
- AntiPhish as a reference model
- Conclusions

Introduction

- In this presentation an anti-phishing browser plug-in based solution will be described.
- The implementation of the proposed solution was realized in javascript for firefox by Engin Kirda and is freely downloadable from: http://www.infosys.tuwien.ac.at/antiphish/

Phishing: some Definitions (1/2)

- Phishing is a form of online identity theft that aims to steal sensitive information from users such as online banking passwords and credit card information [Kruegel et al.].
- The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information [Webopedia].

Phishing: some Definitions (2/2)

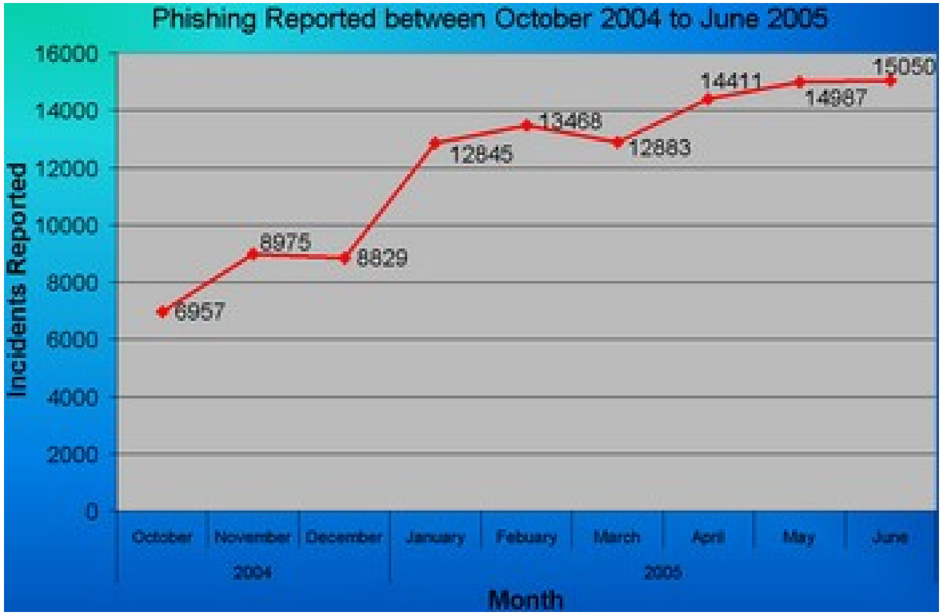
- Phishing is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message [Wikipedia].

Definitely Phishing Attacks…

- Phishing attacks use a combination of social engineering and technical spoofing techniques to persuade users into giving away sensitive information (e.g. using a web form on a spoofed web page) that the attacker can then use to make a financial profit.

Is Phishing a Serious Problem?

- According to a study by Gartner, 57 million US Internet users have identified the receipt of e-mail linked to phishing scams and about 2 million of them are estimated to have been tricked into giving away sensitive information.



Example of Phishing message

- A phishing message described by Gordon and Chess is shown below:

Sector 4G9E of our data base has lost all I/O functions. When your account logged onto our system, we were temporarily able to verify it as a registered user. Approximately 94 seconds ago, your verification was made void by loss of data in the Sector 4G9E. Now, due to AOL verification protocol, it is mandatory for us to re-verify you. Please click 'Respond' and re-state your password. Failure to comply will result in immediate account deletion.

Types of Phishing Attacks

- We can distinguish two main types of Phishing attacks:
  1. Spoofed e-mails and web sites.
  2. Exploit-based phishing attacks.

Spoofed e-mails

- The earliest form of phishing attacks were e-mail-based and date back to 1995 (more or less).
- The idea here to persuade the victim to send back sensitive information, using an e-mail formal request.
- Similar to *scam* where the attacker send a fake winning notification to the victim asking for his credit card number and so on…

Spoofed Web Sites

- Many organizations, such as banks, do not provide interactive services based on e-mail where the user has to provide a password but use their websites to provide such interactive services (even on SSL!).
- Why not faking organizations’ websites? ☺

Some Phishing Tricks

- Attacker’s objective: Not to raise suspicion and to make the setting as authentic as possible:
  - URLs may be obfuscated so that they look legitimate to the victim:
    - e.g: http://www.attacker.com/www.onlinebanking.com/login.pl
  - Use of real logos and corporate identity elements in the spoofed Web site.
  - Some attacks make use of hidden frames, images and Javascript to control the way the page is rendered.

A Typical Attack (1/3)

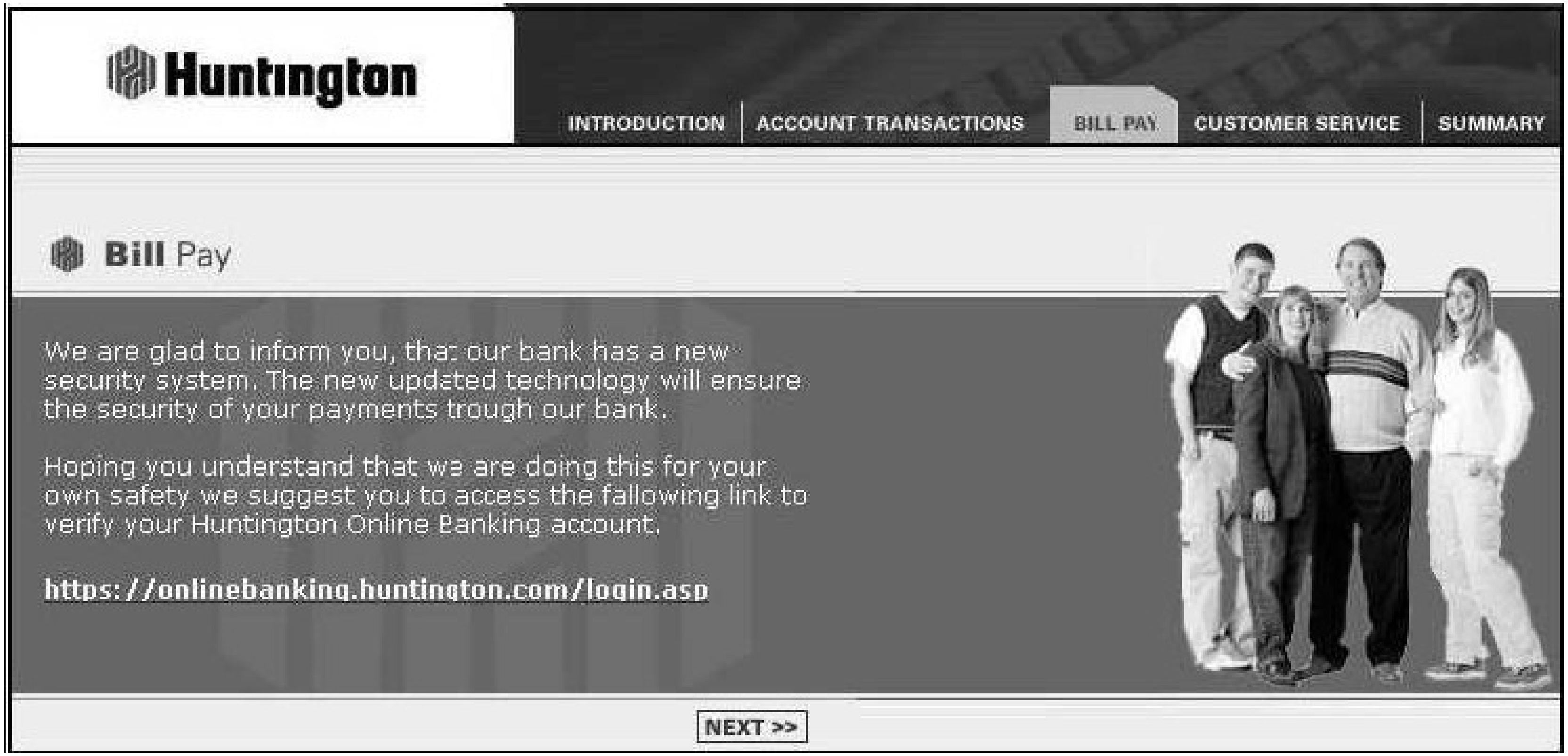
- In a typical attack, the attackers send a large number (to enlarge the probability of success) of spoofed e-mails that appear to be coming from a legitimate organization to random users and urge them to update their personal information.
- The victims are then directed to a web site, that is under the control of the attacker, looking and feeling like the true banking web site.
- Victims are then asked to enter their personal information.

A Typical Attack (2/3)

- Statistically, the probability of success using fake emails+phishing websites are much higher than using only fake emails [Gartner].
- New attacks started using other kind of communication channels such as IRC, ICQ, MSN and so on.

A Typical Attack (3/3)

- An example of a real phishing e-mail.



We are glad to inform you, that our bank has a new security system. The new updated technology will ensure the security of your payments trough our bank.

Hoping you understand that we are doing this for your own safety we suggest you to access the fallowing link to verify your Huntington Online Banking account.

https://onlinebanking.huntington.com/login.asp

Exploit-based Phishing Attacks

- Some phishing attacks are technically more sophisticated and make use of well-known vulnerabilities in popular web browsers such the Internet Explorer to install malicious software that collects sensitive information about the victim.
- Which malware will the attackers use?
  - Key loggers.
  - Remote machine controllers.

A Real World Mass Phishing Attack

- On February 18th 2005, a mass e-mail was sent to thousands of Internet users asking them to verify their Huntington online banking account details.
- The attackers have supposedly inserted a legitimate URL https://onlinebanking.huntington.com/login.asp to the bank’s online banking web site but actually pointing to a spoofed page on the server with the IP address 210.95.56.101, that is not the legitimate one!

AntiPhishing Solutions

- There are mainly two types of antiphishing solutions:
  - Browser (plug-in) based.
  - Server based.
- The browser based solution tries to defend the customer from the client-side point of view.
- The server based solutions try to collect information about phishing websites (also behavioural based) to build a black list (see VeriSign).

Which is the “best “Antiphishing Solution?

- In October, a Microsoft-commissioned report on various antiphishing solutions was released. The testers found that Microsoft Internet Explorer (IE) 7.0 has better antiphishing technology than competing solutions. The products tested included IE 7.0 Beta 3, EarthLink ScamBlocker, eBay Toolbar with Account Guard, GeoTrust TrustWatch, Google Toolbar for Firefox with Safe Browsing, McAfee SiteAdvisor Plus, Netcraft Toolbar, and Netscape Browser with built-in antiphishing technology.
- The Mozilla Foundation commissioned its own study to gauge the effectiveness of Mozilla Firefox 2.0's antiphishing technology as compared with IE 7.0's. This study found that Firefox's antiphishing technology was better than IE's by a considerable margin.
- Wow…, who should we trust ? ☺

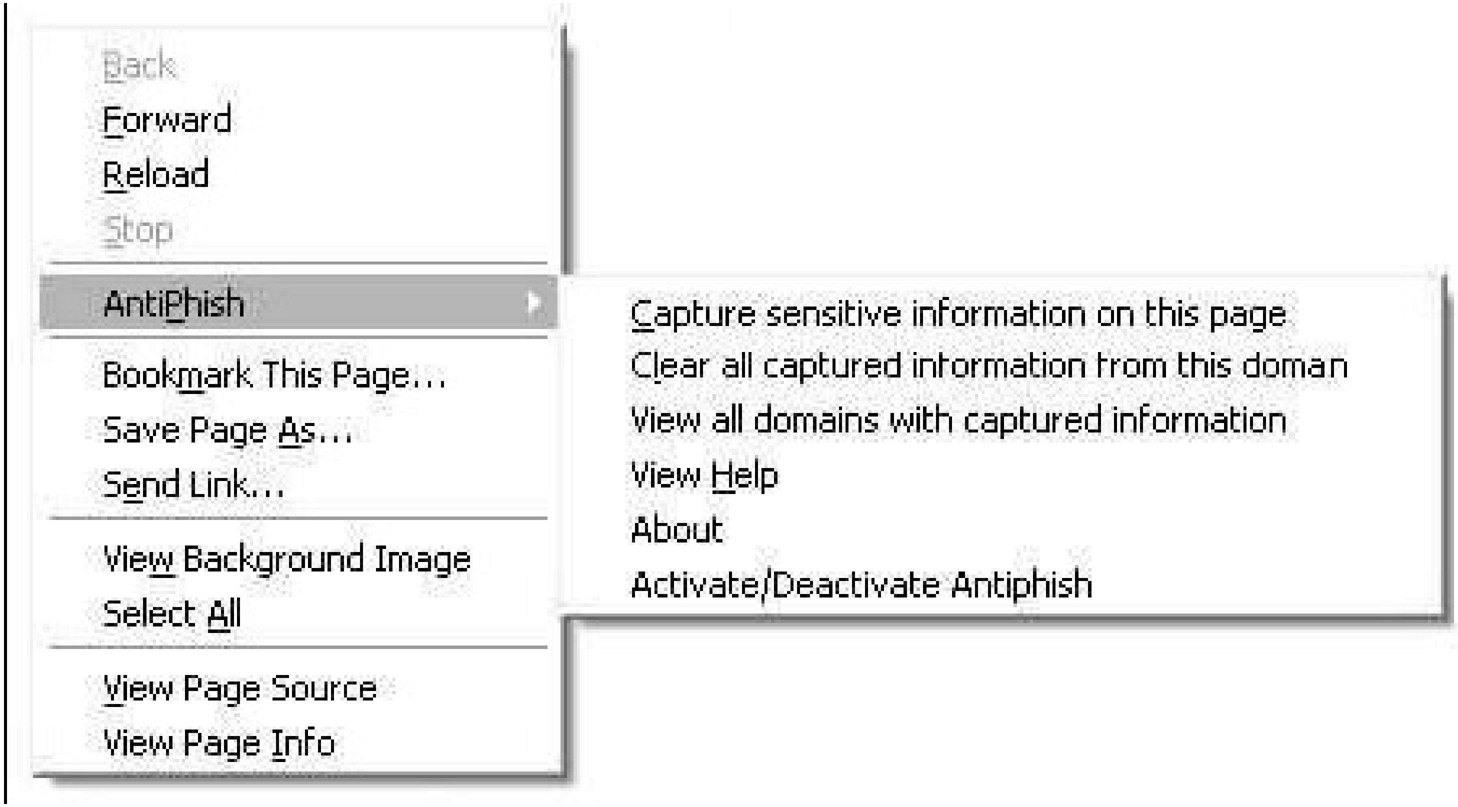
AntiPhish: an Overview

- AntiPhish is an application that is integrated into the web browser, thus, it is a browser based solution.
- AntiPhish keeps track of a user’s sensitive information and prevents this information from being passed to a web site that is not considered “trusted”.

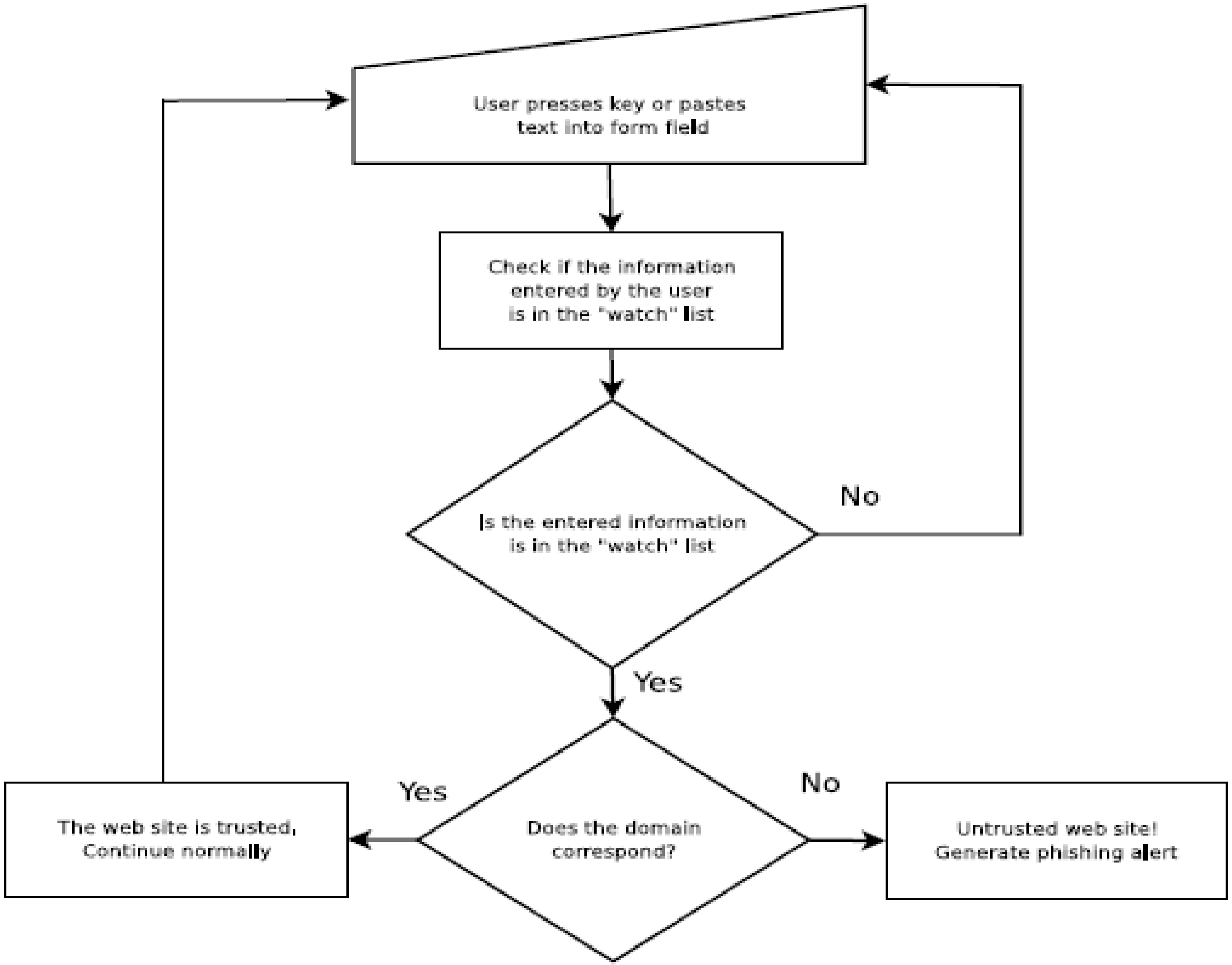
AntiPhish: how Does it Work?

- After AntiPhish is installed, the browser prompts a request for a new master password when the user enters input into a form for the first time.
- The master password is used to encrypt the sensitive information before it is stored (using DES).
- After the user enters sensitive information such as a password, the AntiPhish menu is used to scan the page and to capture and store this information with the domain of the website, too.

AntiPhish: how Does it Look like?


Back
Forward
Reload
Stop
AntiPhish
Bookmark This Page...
Save Page As...
Send Link...
View Background Image
Select All
View Page Source
View Page Info
Capture sensitive information on this page
Clear all captured information from this doman
View all domains with captured information
View Help
About
Activate/Deactivate Antiphish

AntiPhish: the Execution Flowchart


User presses key or pastes text into form field
Check if the information entered by the user is in the "watch" list
Is the entered information is in the "watch" list
No
Yes
Yes
Does the domain correspond?
No
The web site is trusted, Continue normally
Untrusted web site! Generate phishing alert

AntiPhish: limitations (1/2)

- As long as the web page that the user is viewing is pure HTML, AntiPhish can easily mitigate phishing attacks, because the attacker can only steal the sensitive information in the page after the user performs a submit.
- AntiPhish detects that sensitive information has been typed into a form of an untrusted domain and cancels the operation.

AntiPhish: limitations (2/2)

- Instead of just waiting for the submission of the form, the attacker can also create hooks for intercepting user generated events using Javascript embedded into the HTML page.
- For now AntiPhish just temporarily deactivates javascript in web pages with a form.

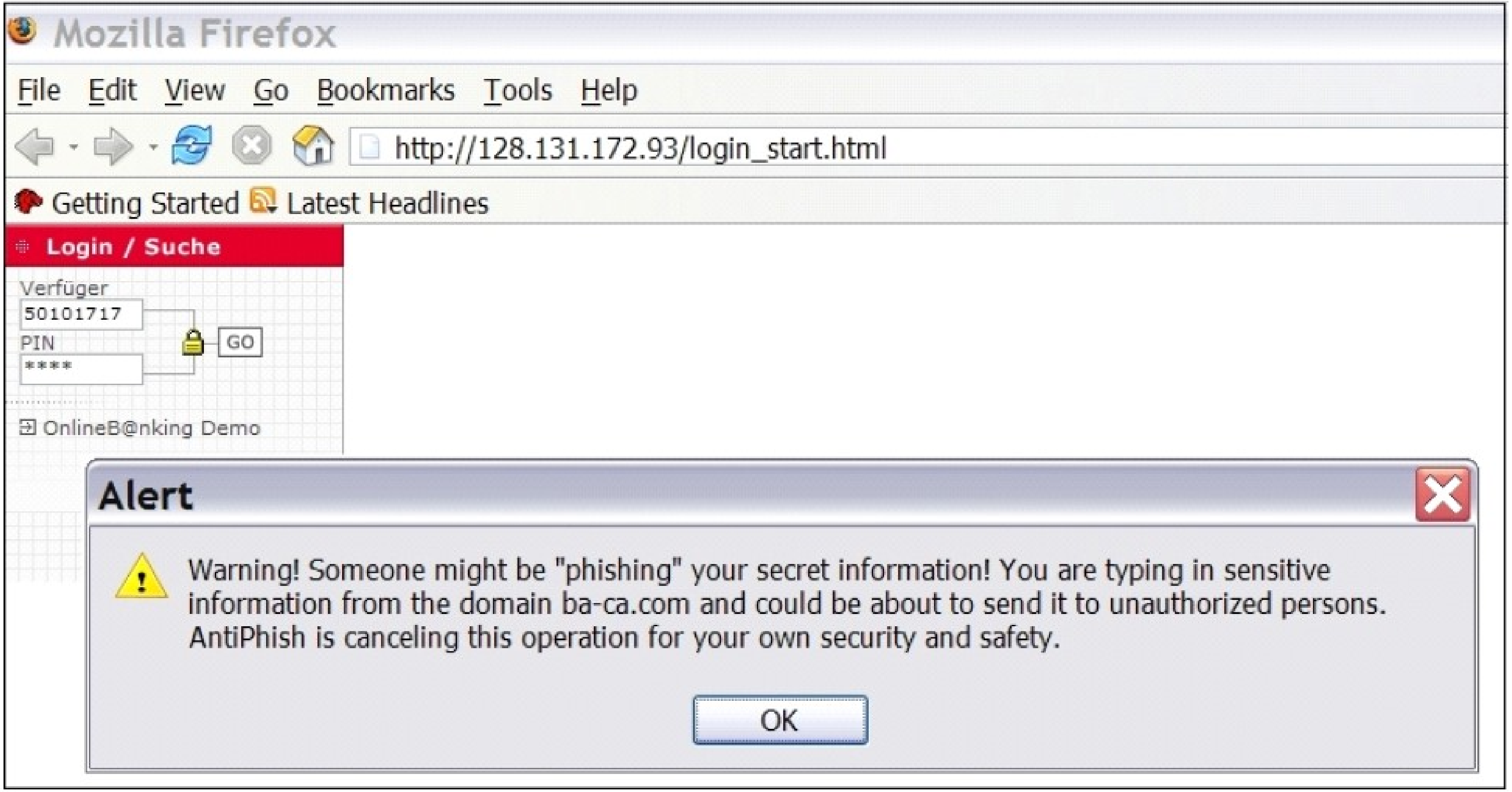
Controlling the Information Flow

- As far as AntiPhish is concerned, every Web page surfed is a potential phishing page.
  - Every time information is entered into a form element (e.g., text field, text area, etc.), AntiPhish goes through its list of captured/cached information.
  - If there is a mismatch between the domain and sensitive information that has been typed, a warning is generated and the operation is canceled
  - Interaction events the user generates within the browser (key presses, submissions, mouse clicks & focus) are intercepted before information can flow to untrusted web site.

AntiPhish Implementation Details

- The prototype implementation of AntiPhish.
  - Mozilla (Firefox) extension (i.e., plug-in)
  - Written in Javascript and the Mozilla XML User Interface Language (XUL)
  - A public DES library is used for the safe storage of the captured sensitive information.
  - The application has a very small footprint.
    - 900 LOC Javascript, 200 LOC user interface code.

AntiPhish in Action



http://128.131.172.93/login_start.html

Verfüger 50101717

PIN ****

Warning! Someone might be "phishing" your secret information! You are typing in sensitive information from the domain ba-ca.com and could be about to send it to unauthorized persons. AntiPhish is canceling this operation for your own security and safety.

AntiPhish Related Solutions

- Phishing is a difficult problem because the victims are technically "unsophisticated" and naïve.
- Only few related solutions have been introduced to date:
  - *PwdHash* and *SpoofGuard* from Stanford University.

Conclusions (1/2)

- The most effective solution to phishing is training users not to follow links to web sites where they have to enter sensitive information such as passwords (unrealistic!).
- The problem with server based solution is that crawling and black listing will find organizations in a race against the attackers.
- Detecting anomalous behaviours (mainly for banks) means *a-posteriori* solution.

Conclusions (2/2)

- AntiPhish is a free, easy and clear reference model for browser based solutions.
- AntiPhish tracks the sensitive information of a user and generates warnings whenever the user attempts to transmit this information to a web site that is considered untrusted.
- Challenge: reduce the false-positive warnings when customers use the same password in different websites.

Q&A

Thanks for your attention….

Engin Kirda	engin@infosys.tuwien.ac.at
Christopher Kruegel	chris@auto.tuwien.ac.at
Angelo P.E. Rosiello	*angelo@rosiello.org*