

# **Analyzing Websites for User-Visible Security Design Flaws**

**Laura Falk, Atul Prakash, Kevin Borders  
University of Michigan**

**Symposium on Usable Privacy and Security  
July 23-25, 2008**

# Motivation: Authors' Personal Experiences

- On-line banking
  - Login boxes on insecure pages
- Need to reach customer service
  - Contact information on an insecure page
- Setting up retirement account on-line
  - User id was SSN
- Decided to analyze other banks to see if the problems were more common and if we could help nudge banks in the right direction

# Goals

- We mostly focus on security problems that should be visible to careful users of a web site
  - Most make it hard for even careful users to make correct judgement calls
- We picked on financial sites because they are assumed to be designed by security experts and their users are frequently targeted

# Our Study

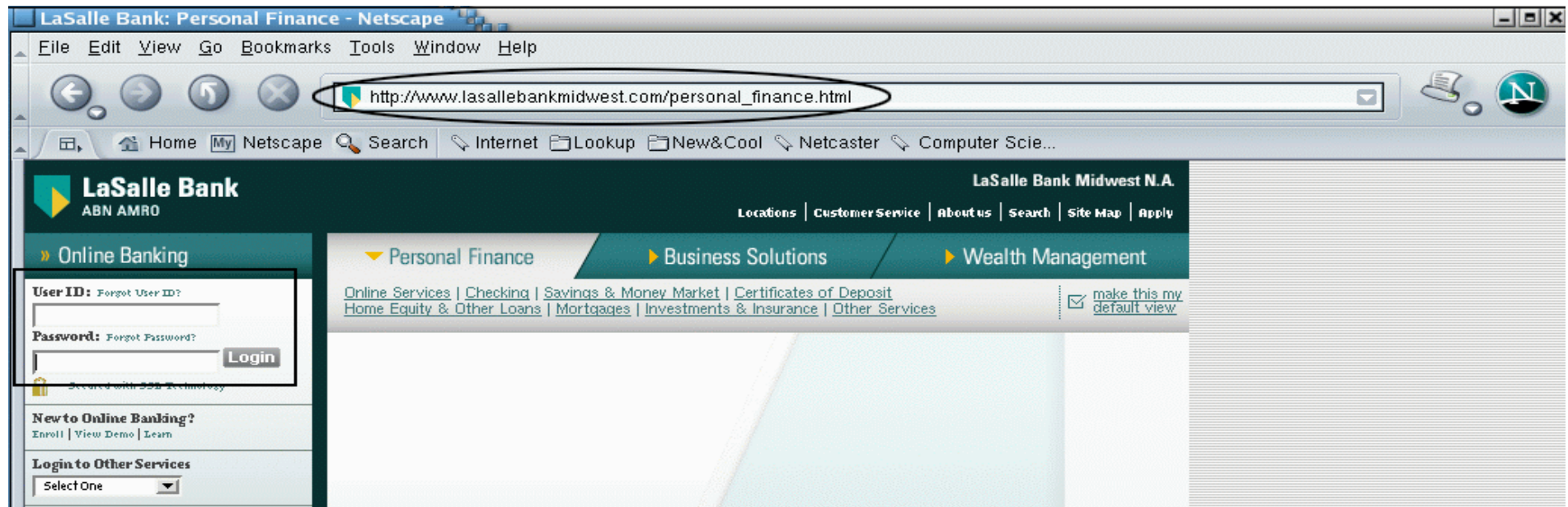
- We chose not to examine “bugs” or browser flaws
  - E.g., buffer overflows, cross-site scripting, etc.
  - The flaws we discuss affect users who are using bug-free client software
- Could not analyze all flaws (e.g., those that require login at the bank sites)

# Methodology

- A combination of automated and manual analysis of 214 websites (mostly banks)
- Source of list:  
<http://www.quazell.com/bank/bank-usa.html>
- Study initiated in Fall of 2006
  - Used 5 visible flaws found in initial analysis of 20 sites
  - Downloaded website contents to disk
  - Searched files containing web pages using scripts

# Login Window on an Insecure Page

- Presenting secure login options on insecure page
  - Attacker could modify insecure page
  - Forward login credentials to another destination



Short Video Illustrating an Attack  
on Insecure Login Pages  
(Recorded on July 20<sup>th</sup>, 2008)

# Example Risk Scenario

Coffee Shop



Router/Access Point



Rogue Router/Access Point



**DNS flaws [see recent bug report by Dan Kaminsky] could potentially allow even remote, large-scale exploits**



# Contact Information on an Insecure Page

TIAA-CREF - Updating Personal Information - Netscape

File Edit View Go Bookmarks Tools Window Help

http://www.tiaa-cref.org/support/help/maintenance/update\_address.html

Home My Netscape Search Internet Lookup New&Cool Netcaster Computer Scie...

A: To change your address, retirement start date, telephone number and/or email address online, log in to your TIAA-CREF account and select the "Personal Info" tab. Enter your new information on the following page, and then submit your changes. Your new information will be effective immediately. If you want to change your address on fewer than ALL contracts, or to enter a foreign address, you will need to select "click here" located under the email section of the page.

**Q: I was recently married, how can I change my name?**

A: You can change your name on an Annuity contract funded with TIAA-CREF Retirement Annuity account by sending your request in writing.

Include the following information in your letter:

- Old name with signature
- New name with signature
- Social Security number
- Contract/account numbers

The letter should be mailed to:

TIAA-CREF  
730 Third Avenue  
New York, NY 10017

If you own a Mutual Fund account you will need to complete a new application to change the registration on your account. In addition to the revised application also include a letter of instruction stating the change of name and a signature in both your former and new name with a signature guarantee by an official bank representative who can verify your signature to one that is on file.

[back to top](#)

**Q: How do I update my address?**

A: If you have a User ID and Password you can change your address by logging into Secure Access, then select Personal Info from the dashboard. If you do not have a login you can create one online.

Our Telephone Counseling Center can also update your address, please call 1 800 842-2776 weekdays from 8 a.m. to 10 p.m. (ET), and on Saturday from 9 a.m. to 6 p.m. (ET). Certain changes must be processed by mail, such as if you have a "payout" contract.

Letters should be mailed to:

TIAA-CREF  
730 Third Avenue  
New York, NY 10017-3206

Please note your payout contract number(s) in your request.  
Please note: If you want to change your address on fewer than ALL contracts or to enter a foreign address you will need to select "click here" located under the email section of the page. Address changes for pay out contracts must be mailed in.

[back to top](#)

**Q: When I change the address on one of my accounts, does it affect the address listed for my other accounts?**

A: Address changes are made according to the Social Security number (SSN) associated with an account. When you change the address on one of your accounts, it changes the address for all the

**Need Help?**

- [View Site Map](#)
- [Meetings & Counseling](#)

Video illustrating the compromise  
of “Contact Us” Pages  
(Recorded on July 20<sup>th</sup>, 2008)

# Should this be a concern?

- Exploits would not be straightforward (e.g., may require setting up a rogue call center), but attackers are becoming more organized
  - Other customer service channels, such as chat, may also be created that could be exploited cheaply
- **Bottom Line:** No good reason why banks should not securely deliver all content

# Use of Third-Party Sites

- Break in the chain of trust
  - Forward user to new pages that have different domains
  - Often no notification of any 3rd party transition
  - Potential for customer confusion
    - User has no straightforward way of knowing if 3rd party domain is trustworthy

# Example

Bank - Open 7 Days - Netscape



File Edit View Go Bookmarks Tools Window Help

TCF <http://www.tcfbank.com/>

Home My Netscape Search Internet Lookup New&Cool Netcaster Computer Scie...

[Locations](#) | [Careers](#) | [About TCF](#) | [Contact Us](#) | [Customer Service](#)

**Personal Banking** Small Business Commercial Leasing





Search

[Online Banking >](#)

[Online Brokerage >](#)

**Personal Banking**

**TCF Totally Free Checking**  
 Sign up today for a TCF Totally Free Checking

**Great Home Equity Rates**  
 Get a great rate of Prime minus .77% (.748% APR)

**TCF Miles Plus<sup>SM</sup>**  
[Sign In](#)

# Example (contd.)

- Transition to 3rd party site (2006 example)

TCF Bank - Sign in to Online Banking - Netscape

File Edit View Go Bookmarks Tools Window Help

https://secure.mvnt4.com/tcf/OnlineBanking/index.jsp

Home My Netscape Search Internet Lookup New&Cool Netcaster Computer Scie...

Locations | Careers | About TCF | Contact Us | Customer Service

Personal Banking Small Business Commercial Leasing

**TCF**  
Since 1925  
Open 7 Days<sup>SM</sup>

Search  
 Go

Online Banking >

Online Brokerage >

Enroll in Online Banking  
Online Banking Tour  
Online Banking FAQ  
Online Bill Payment  
Privacy Policy  
Security Policy  
TCF Mortgage Online

**Sign in to TCF Online Banking**

If you are already enrolled as a TCF Online Banking customer, sign in below:

Sign-in ID\*:

Password:  [Forgot My Password](#)

**Access Accounts**

**Purchase-Fee Free  
TCF Visa Gift Cards  
for TCF Customers.**

Short Video demonstrating User  
Confusion with Third-Party  
Domains

(Recorded on July 24<sup>th</sup>, 2008)

# Informal Poll

- Visit your bank(s) web page
  - Locate login window
    - Is it on an insecure or secure page?
  - Locate the contact information
    - Is it on an insecure or secure page?
  - Is your bank using 3<sup>rd</sup> party sites?
- We will ask for a show of hands for these questions at the end of the talk



# Policies on User Ids and Passwords

- Inadequate or unclear policies for user ids and passwords
  - Some sites used social security numbers for login (e.g., TIAA-CREF in 2006. We contacted them about it. Since changed the policy)
  - May not require or recommend strong passwords

# Ambiguity in Policies

- E-mailing security sensitive information insecurely
  - Sites offered to send statements and passwords through e-mail
  - As we know and banks know, email is not a secure medium
- (Caveat: It is possible that the sites will only send you a notification, not the the actual statement. But this was often not apparent from the wording.)

# Example

- Offering to e-mail security sensitive information

## EDUCATION & SUPPORT

Search

[Learning Center](#) | [Forms](#) | [Tools](#) | [News](#) | [Publications](#) | [FAQs](#)

### Account Features

#### E-Delivery

#### Using Quicken

### E-DELIVERY

- [Can I have printed statements as well as an electronic copy sent to me?](#)
- [How do I sign up for electronic delivery?](#)
- [How do I update my email address?](#)
- [When logged in to Secure Access, I receive a message stating that I have "no mail." How do I get mail?](#)
- [How do I change the electronic delivery preference back to postal mail?](#)
- [When I attempt to view my quarterly report, I get an error stating that my password does not match. Why can't I view my statements online?](#)

### Can I have printed statements as well as an electronic copy sent to me?

You can elect e-delivery of your statements via the email tab in Secure Access. In addition, when your statement is available there is also an option within Documents to receive a hard copy by selecting the "send by mail" tab. This will generate a hardcopy of your report.

[back to top](#)



### GLOSSARY

[Look up a word or phrase»](#)

### In Control of Your Account, Anytime

[Take a guided tour of online access](#)

### Need Help?

- [View Site Map](#)
- [Meetings & Counseling](#)

# Results

- List of Design Flaws and Percentage of Sites Affected

Specific Design Flaw	% of Sites Affected
Login window on insecure page	47%
Contact info on insecure page	55%
Inadequate policies on user ids/ passwords	28%
E-mailing sensitive information	31%
Use of 3 <sup>rd</sup> party sites	30%

# Key Points

- Several of these design flaws were widespread
- 76% had at least one design flaw (note: use of non-SSL pages more critical than others)
- Almost half the sites presented login boxes on insecure pages
- Use of 3rd party domains was fairly common
- Less than half secured their contact information
- Scope for improvement in other areas, such as better policies on userids, passwords, and email use by the site

# Some Limitations of Our Study

- We may have failed to completely retrieve all relevant pages
  - Impact: our results likely to under-estimate flaws
- Only looked financial institutions in U.S.
  - Results could be different in other countries.
- We used heuristics for automated analysis
  - Could cause us to under or over estimate errors
- Human errors where we did manual inspection

# Some Related Work

- Users may make errors even if banks fix the design flaws [Schechter et al.]
- Implementation flaws are also common
  - Application level website scanners
- Rogerio de Paula et al., discovered that implementation and integration of technical components is hard with respect to security
  - Perhaps, bank sites have multiple domains and administrators. No one looking at the “big picture”

# Usability Lessons for Web Sites

- Provide a *consistent* experience to users so that it is easier for users to spot deviations from the norm
  - Stay on the same hostname (www.bank.com)
  - Next best: *www.bank.com* to *secure.bank.com*
  - Next best: make “proper introduction”
    - From the original domain over HTTPS
    - Say whether the new domain can be trusted
  - Use SSL throughout the site.



# The Big Picture – Take Away

- We want to help banks by this study recognize the importance of usable security – problems are common
- **Key recommendations:**
  - Use SSL for entire site (no exceptions)
  - Discontinue use of 3<sup>rd</sup> party domains if possible (especially for services for the same bank) or introduce them securely
  - Improve security policies and state them clearly
- **Benefits:** Hopefully, that will make it easier for careful customers to notice inconsistencies because most financial sites will use a simple, consistent model

# Informal Poll

- Did your bank's login window reside on an insecure page?
- Did the contact information on your bank's site reside on an insecure page?
- Did your bank use 3<sup>rd</sup> party domains during authentication?

Questions?