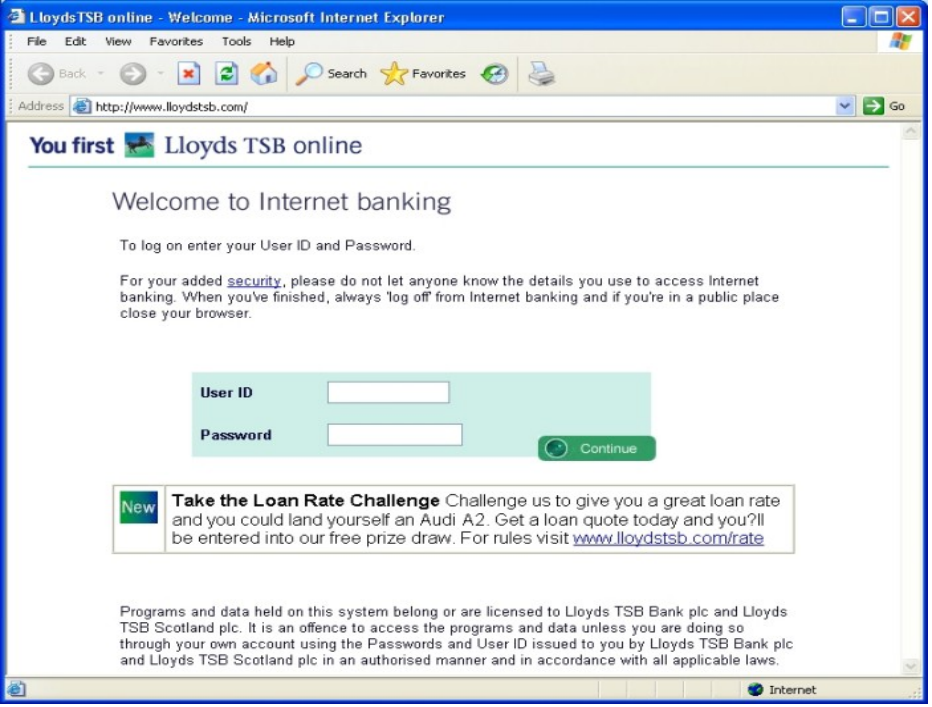
ViWiD : Visible Watermarking based Defense against Phishing

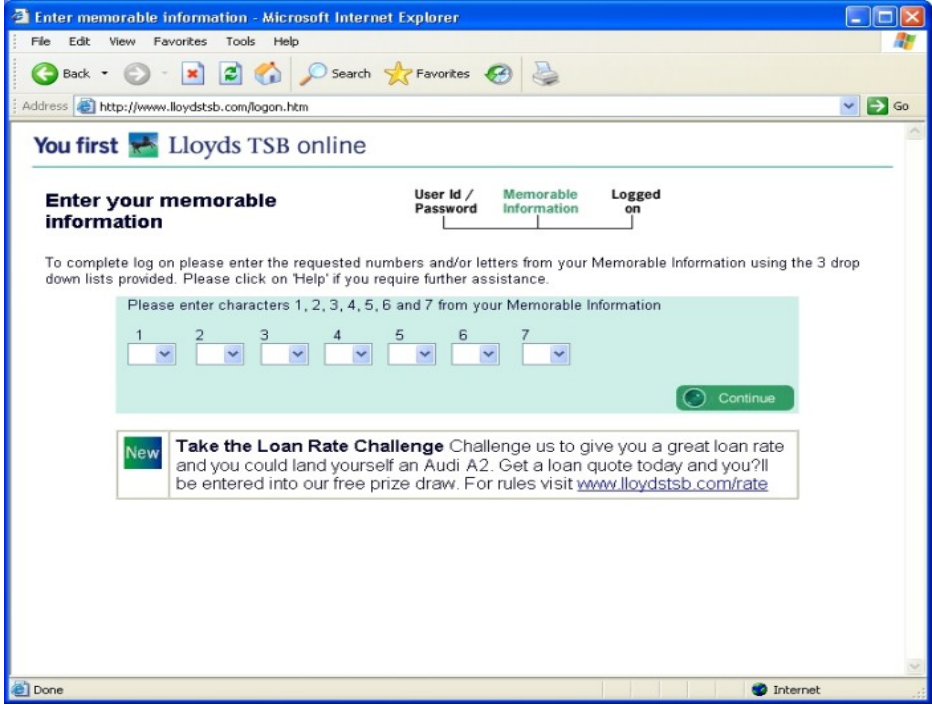
Mercan Topkara
Ashish Kamra
Mikhail J. Atallah
Cristina Nita-Rotaru

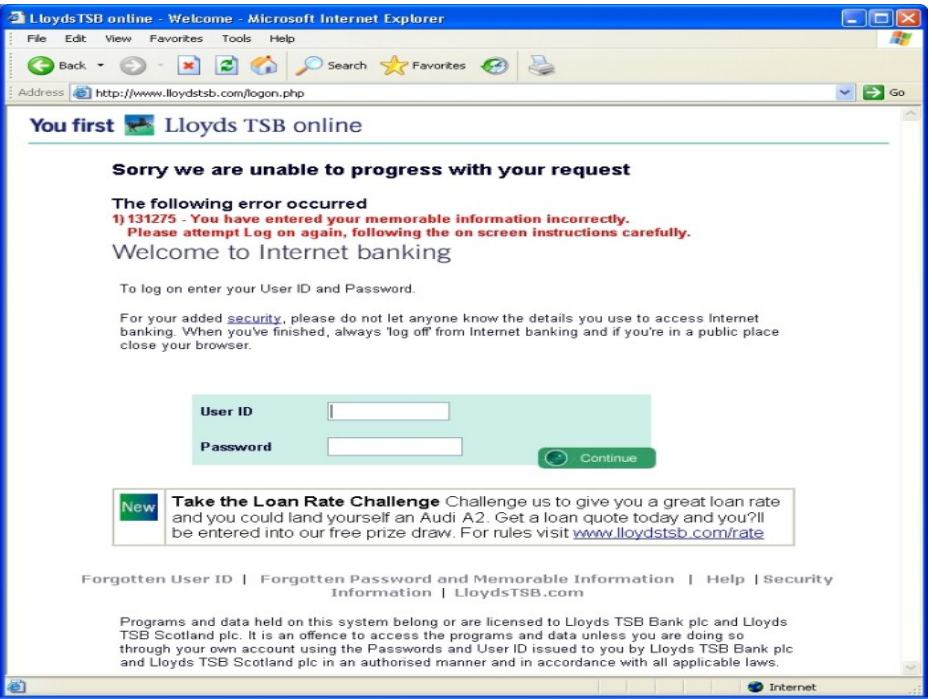
Department of Computer Sciences
Center for Education and Research in Information Assurance
{mkarahan,akamra,mja,crisn}@cs.purdue.edu

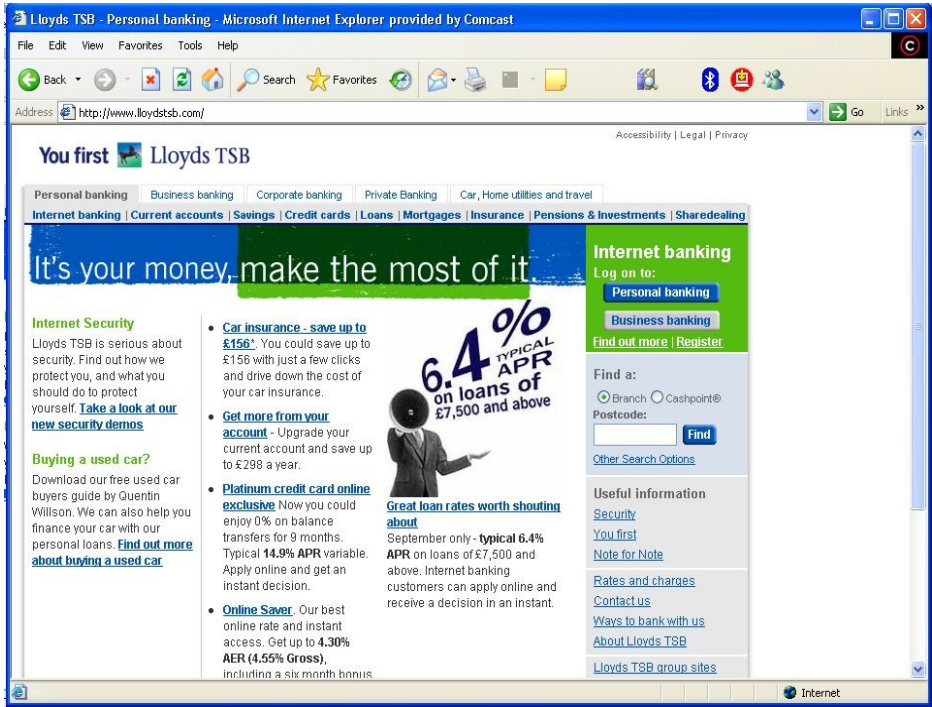
CERIAS

PURDUE UNIVERSITY


LloydsTSB online - Welcome - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.lloydstsb.com/
Go
You first Lloyds TSB online
Welcome to Internet banking
To log on enter your User ID and Password.
For your added security, please do not let anyone know the details you use to access Internet banking. When you've finished, always 'log off' from Internet banking and if you're in a public place close your browser.
User ID
Password
Continue
New
Take the Loan Rate Challenge Challenge us to give you a great loan rate and you could land yourself an Audi A2. Get a loan quote today and you?ll be entered into our free prize draw. For rules visit www.lloydstsb.com/rate
Programs and data held on this system belong or are licensed to Lloyds TSB Bank plc and Lloyds TSB Scotland plc. It is an offence to access the programs and data unless you are doing so through your own account using the Passwords and User ID issued to you by Lloyds TSB Bank plc and Lloyds TSB Scotland plc in an authorised manner and in accordance with all applicable laws.
Internet


Enter memorable information - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.lloydstsb.com/logon.htm
Go
You first Lloyds TSB online
Enter your memorable information
User Id / Password
Memorable Information
Logged on
To complete log on please enter the requested numbers and/or letters from your Memorable Information using the 3 drop down lists provided. Please click on 'Help' if you require further assistance.
Please enter characters 1, 2, 3, 4, 5, 6 and 7 from your Memorable Information
1 2 3 4 5 6 7
Continue
New
Take the Loan Rate Challenge Challenge us to give you a great loan rate and you could land yourself an Audi A2. Get a loan quote today and you?ll be entered into our free prize draw. For rules visit www.lloydstsb.com/rate
Done
Internet


LloydsTSB online - Welcome - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.lloydstsb.com/logon.php
Go
You first Lloyds TSB online
Sorry we are unable to progress with your request
The following error occurred
1) 131275 - You have entered your memorable information incorrectly.
Please attempt Log on again, following the on screen instructions carefully.
Welcome to Internet banking
To log on enter your User ID and Password.
For your added security, please do not let anyone know the details you use to access Internet banking. When you've finished, always 'log off' from Internet banking and if you're in a public place close your browser.
User ID
Password
Continue
New
Take the Loan Rate Challenge Challenge us to give you a great loan rate and you could land yourself an Audi A2. Get a loan quote today and you?ll be entered into our free prize draw. For rules visit www.lloydstsb.com/rate
Forgotten User ID | Forgotten Password and Memorable Information | Help | Security Information | LloydsTSB.com
Programs and data held on this system belong or are licensed to Lloyds TSB Bank plc and Lloyds TSB Scotland plc. It is an offence to access the programs and data unless you are doing so through your own account using the Passwords and User ID issued to you by Lloyds TSB Bank plc and Lloyds TSB Scotland plc in an authorised manner and in accordance with all applicable laws.
Internet


Lloyds TSB - Personal banking - Microsoft Internet Explorer provided by Comcast
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.lloydstsb.com/
Go
Links
Accessibility | Legal | Privacy
You first Lloyds TSB
Personal banking
Business banking
Corporate banking
Private Banking
Car, Home utilities and travel
Internet banking | Current accounts | Savings | Credit cards | Loans | Mortgages | Insurance | Pensions & Investments | Sharedealing
It's your money, make the most of it.
Internet Security
Lloyds TSB is serious about security. Find out how we protect you, and what you should do to protect yourself. Take a look at our new security demos
Buying a used car?
Download our free used car buyers guide by Quentin Willson. We can also help you finance your car with our personal loans. Find out more about buying a used car
Car insurance - save up to £156*. You could save up to £156 with just a few clicks and drive down the cost of your car insurance.
Get more from your account - Upgrade your current account and save up to £298 a year.
Platinum credit card online exclusive Now you could enjoy 0% on balance transfers for 9 months. Typical 14.9% APR variable. Apply online and get an instant decision.
Online Saver. Our best online rate and instant access. Get up to 4.30% AER (4.55% Gross), including a six month bonus
6.4% TYPICAL APR on loans of £7,500 and above
Great loan rates worth shouting about
September only - typical 6.4% APR on loans of £7,500 and above. Internet banking customers can apply online and receive a decision in an instant.
Internet banking
Log on to:
Personal banking
Business banking
Find out more | Register
Find a:
Branch Cashpoint®
Postcode:
Find
Other Search Options
Useful information
Security
You first
Note for Note
Rates and charges
Contact us
Ways to bank with us
About Lloyds TSB
Lloyds TSB group sites
Internet

Outline

- The Phishing Problem
- Previous Approaches
- ViWiD System Overview
- Experimental Results
- Security Analysis and Discussion
- Conclusion

Mercan Topkara
mtopkara@cs.purdue.edu
September 2005

PURDUE UNIVERSITY

Phishing

- **Online deception for malicious purpose**
  - Attackers send fake e-mails and use web sites that spoof a legitimate business
  - Lure unsuspecting customers into revealing personal information like password, credit card number, SSN etc
- **Huge financial losses and damage to reputations**
  - **Lost Dollars …**
    - 70,000 calls/hour for 12 hours
    - Banks and card issuers lost $1.2 billion in 2003
  - *"It's a question of trust, a question of brand", says Tom Salmond, manager of the E-Banking Fraud Liaison Group at the APACS*
- **Exploits**
  - Unauthenticated E-mail
  - User Actions
  - Deceptive View

Mercan Topkara
mtopkara@cs.purdue.edu
September 2005

Players: the Phisher

- **Impersonates a trusted source**
- **Misuses legitimate content for convincing the user into revealing personal information**
- **Can carry out 'man-in-the-middle' attack in some cases**

Mercan Topkara
mtopkara@cs.purdue.edu
September 2005

PURDUE UNIVERSITY

Players: the Victims

- **Legitimate Company:**
  - provides trusted online services
  - has a database of customer information
  - needs to maintain its brand image
  - has high computational power
- **Average User:**
  - busy or lazy
    - disables security options
    - uses same login/password for different sites
    - trusts e-mails
  - not tech savvy
  - uses multiple computers

Mercan Topkara
mtopkara@cs.purdue.edu

Defense Against Phishing

- **Secure E-mail**
  - Privacy Enhanced Mail (PEM), Secure Multipurpose Internet Mail Extension (S/MIME) and Pretty Good Privacy (PGP)
- **Client Side Defense**
  - SpoofGuard, NetCraft, Trusted Credentials Area, Firefox Pet Name Extension
- **Cryptography-based Defense**
  - TriCipher Armored Credential System
- **Shared Secret Schemes**
  - 2-Way Authentication Tool, Dynamic Security Skins

Mercan Topkara
mtopkara@cs.purdue.edu

Limitations of Previous Approaches

- **Hard to widely deploy due to**
  - Difficulty to use
  - Must download on all client computers
  - Update on the browser view
- **Vulnerable**
  - Mosaic attack
- **False Alarms**
- **No tie of what is displayed on a web page to its origin**

Mercan Topkara
mtopkara@cs.purdue.edu

Introducing ViWiD …

- **Visible Watermarking based Defense against Phishing**
- **Mitigating phishing attacks through integrity checking of web site logos using visible watermarking techniques**
- **All of the integrity related computation on the company's web server**
- **Unique watermark message for each user**
- **Thwart the "one size fits all" attacks**

Mercan Topkara
mtopkara@cs.purdue.edu
September 2005

PURDUE UNIVERSITY

Challenges

- **Communicating to naive users the true identity of the web site**
- **Maintain the aesthetics of the watermarked logo**
  - Preserve its marketing value
- **Robust visible watermarking of logo images that have large uniform areas and very few objects in them**

Mercan Topkara
mtopkara@cs.purdue.edu

PURDUE UNIVERSITY

Features of ViWiD Approach

- **Integrity check "travels with the content"**
- **Visible watermark avoids key distribution issue**
- **Thwarting the "one size fits all" attacks**
  - A user-specific time-stamped message
  - Carelessly using non-secure connection is less deadly
- **Can use multiple browsers / computers**
  - Compromise of one is less disastrous (mnemonic is not stored)

Mercan Topkara
mtopkara@cs.purdue.edu

PURDUE
UNIVERSITY

Watermark Messages

- **The time alone:**

- **The time and the mnemonic:**

Mercan Topkara
mtopkara@cs.purdue.edu
September 2005

PURDUE UNIVERSITY

ViWiD Framework

- **Recall that in visible watermarking**

$$I' = K_1 \times I + K_2 \times W$$

$$D(E_I(I'), E_I(I)) < Threshold_I$$

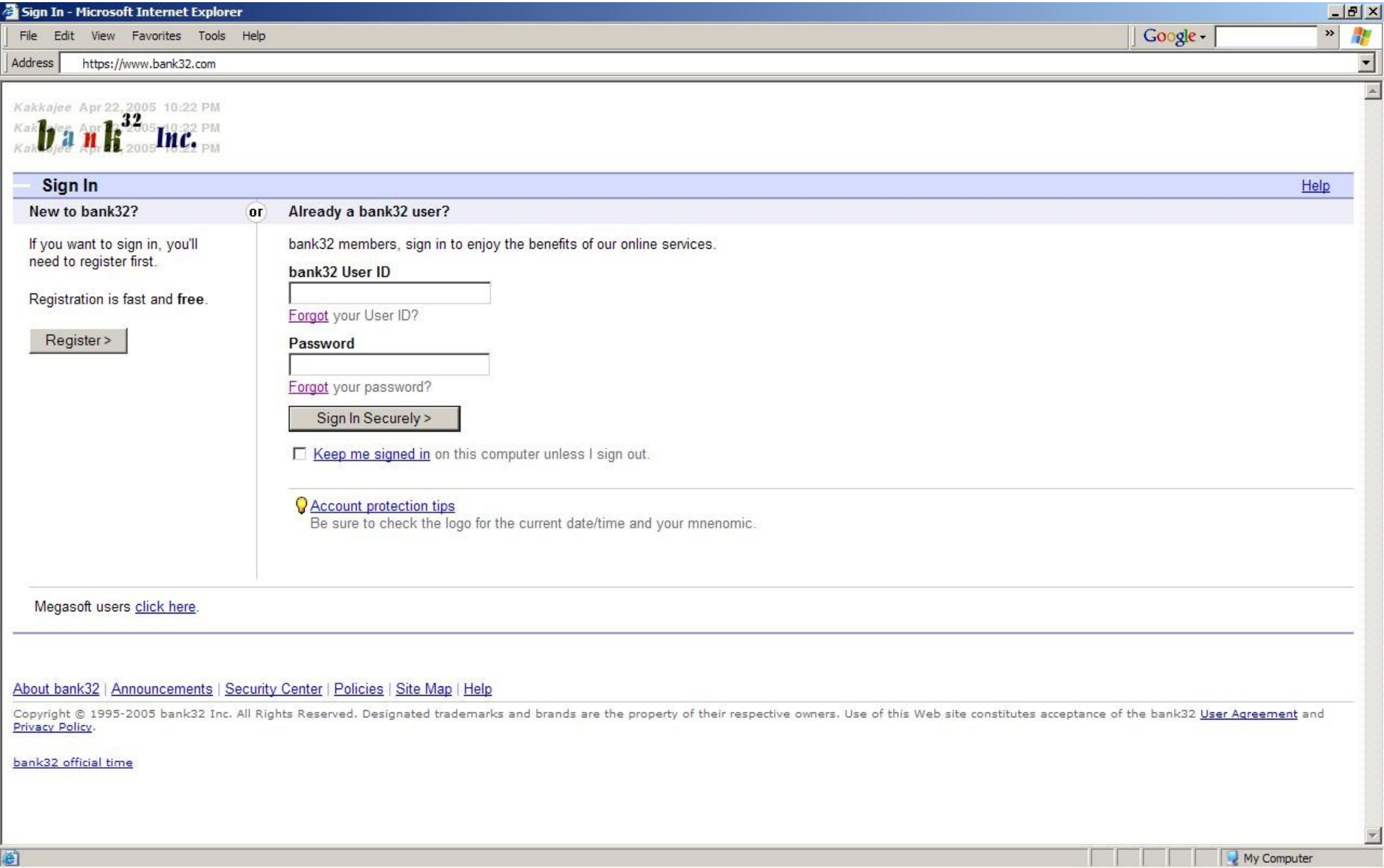
$$D(E_W(I'), E_w(I)) < Threshold_W$$

- **Two Types of Displays**

Mercan Topkara
mtopkara@cs.purdue.edu
September 2005

PURDUE UNIVERSITY

Screen Shot


Sign In - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Google
Address https://www.bank32.com
Kakkajee Apr 22, 2005 10:22 PM
bank32 Inc.
Sign In
Help
New to bank32?
or
Already a bank32 user?
If you want to sign in, you'll need to register first.
Registration is fast and free.
Register >
bank32 members, sign in to enjoy the benefits of our online services.
bank32 User ID
Forgot your User ID?
Password
Forgot your password?
Sign In Securely >
Keep me signed in on this computer unless I sign out.
Account protection tips
Be sure to check the logo for the current date/time and your mnenomic.
Megasoft users click here.
About bank32 | Announcements | Security Center | Policies | Site Map | Help
Copyright © 1995-2005 bank32 Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the bank32 User Agreement and Privacy Policy.
bank32 official time
My Computer

Experimental Setup : ImageMagick™

$$\text{midpoint} = \frac{\text{maxRGB}}{2}$$

$$offset_{i,j}^{w} = I_{i,j}^{w} - \text{midpoint}$$

$$B'_{i,j} = B_{i,j} + \frac{(p \times offset_{i,j}^{w})}{\text{midpoint}}$$

p=10

p=15

p=20

p=30

p=40

Mercan Topkara
mtopkara@cs.purdue.edu
September 2005

PURDUE UNIVERSITY

Experimental Setup : Mohanty et. al's Technique

- **Modifies the gray values of the host image based on both its local and global statistics.**

$$I_n^{'} = \alpha_n \times I_n + \beta_n \times I_n^w$$

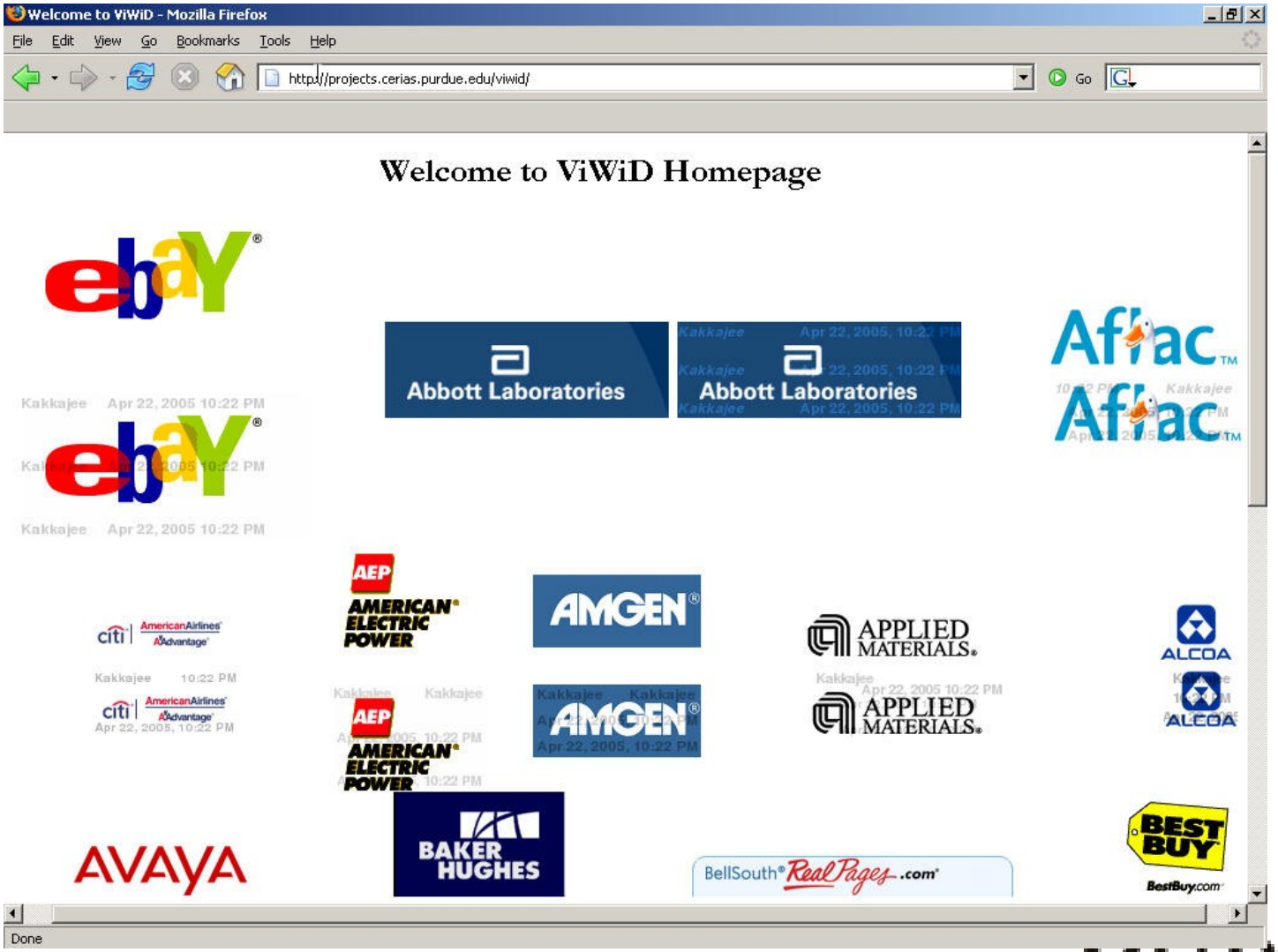
- **Y component vs K component**

Mercan Topkara
mtopkara@cs.purdue.edu
September 2005

PURDUE UNIVERSITY

Results

- http://projects.cerias.purdue.edu/viwid/



Mercan Topkara
mtopkara@cs.purdue.edu
September 2005

PURDUE UNIVERSITY

Attacker Behaviors Outside Our Model

- **Replace a watermark by another**
  - Removing can be done through the use of (e.g.) the Huang and Wu scheme, which requires human intervention for every image
  - Requires man-in-the-middle
- **Recreate the logo image and insert a valid watermark**
  - Recreating a logo image is hard
  - Requires man-in-the-middle
- **Man-in-the-middle without image processing**
  - ViWiD mitigates this attack

Mercan Topkara
mtopkara@cs.purdue.edu

Security Analysis and Discussion

- **If the shared secret between server and client would simply be presented as is (e.g. in text or image format) without ViWiD, why wouldn't that work?**
  - Puts the message in a place conspicuous to the user
  - Binds it to the legitimate site's logo
  - Forces the attacker to do image processing on the logo

Mercan Topkara
mtopkara@cs.purdue.edu

Conclusion

- **ViWiD mitigates phishing attacks through integrity checking of web site logos using visible watermarking techniques.**
- **ViWiD performs all of the computation on the company's web server and does not require installation of any tool or storage of any data on the user's machine.**
- **ViWiD also involves the user's mind in the integrity checking process, making it harder for the phisher to engineer an attack.**

Mercan Topkara
mtopkara@cs.purdue.edu

PURDUE UNIVERSITY