ISPEC 2006 – HangZhou, China

Preventing Web-Spoofing with Automatic Detecting Security Indicator

Fang Qi, Feng Bao, Tieyan Li, Weijia Jia & Yongdong Wu

Systems and Security Department (SSD)

Institute for Infocomm Research (I²R)

Apr. 11, 2006

A*STAR I²R

Outline

- Introducing phishing and web spoofing
- Some countermeasures against phishing
  - Trustbar (TCA)
  - BSCI (personal image)
  - Dynamic security skin
    - PwdHash
    - Active cookies
    - Phoolproof
- Our approach (ADSI)
  - Trust model
  - ADSI scheme
  - Illustration
  - Discussion
- Conclusion and future works

What is Phishing?

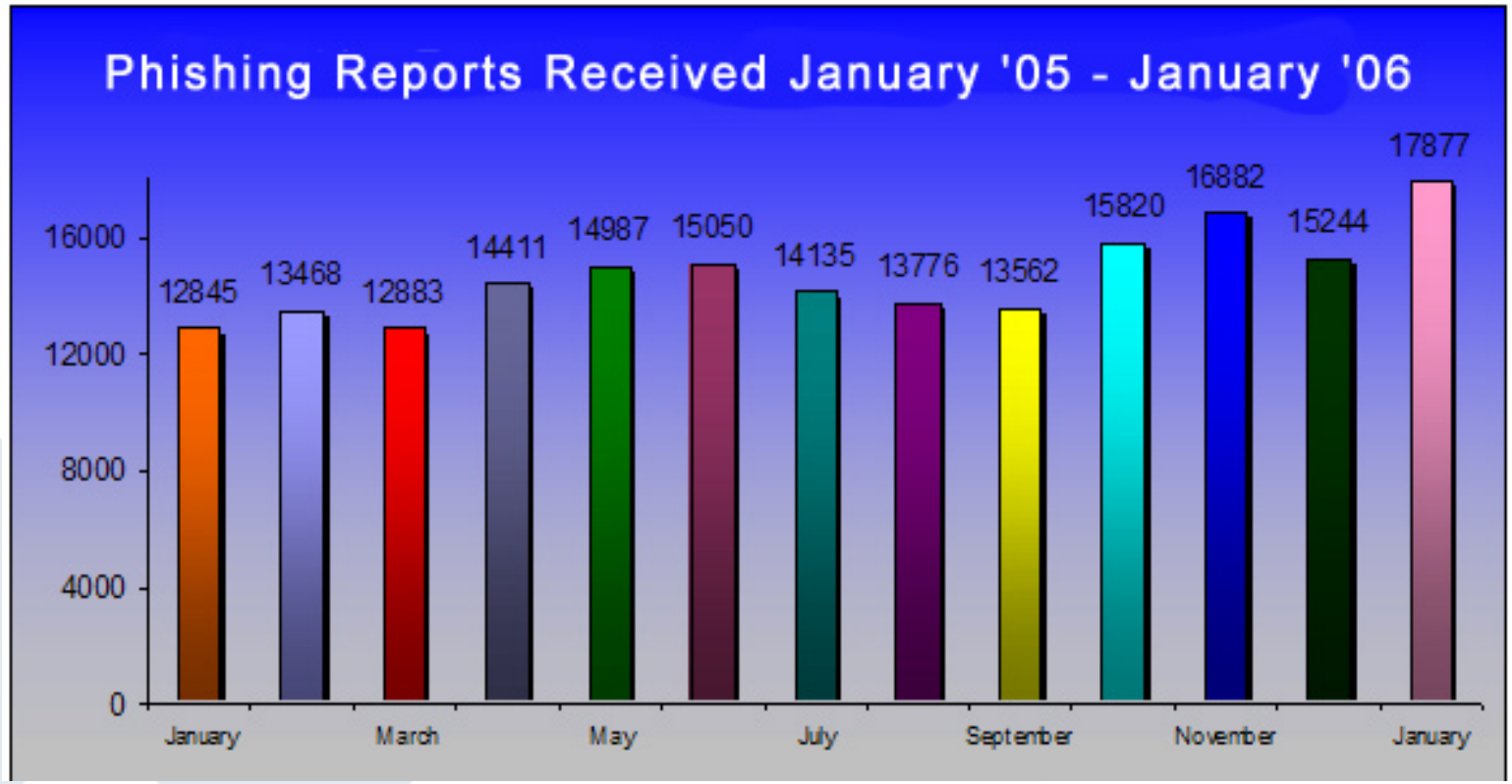
From Anti-Phishing Working Group (APWG)

Phishing is a form of online identity theft that employs both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials.

- Social-engineering schemes use 'spoofed' emails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as account usernames and passwords. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond.
- Technical subterfuge schemes plant **crimeware** onto PCs to steal credentials directly, often using key logging systems to intercept consumers online account user names and passwords, and to corrupt local and remote navigational infrastructures to misdirect consumers to counterfeit websites and to authentic websites through phisher-controlled proxies that can be used to monitor and intercept consumers' keystrokes.

A*STAR I²R

Trend on Phishing

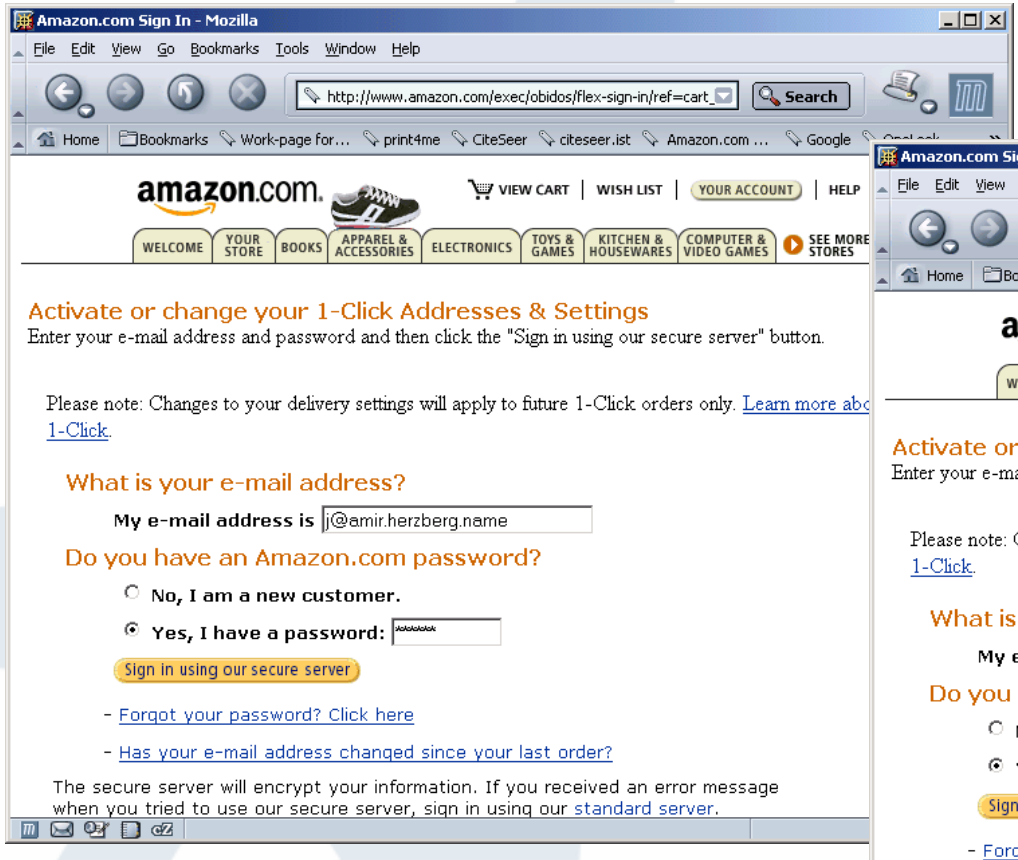


January Report Brings 2nd Record High In Two Months – APWG, Jan. 2006

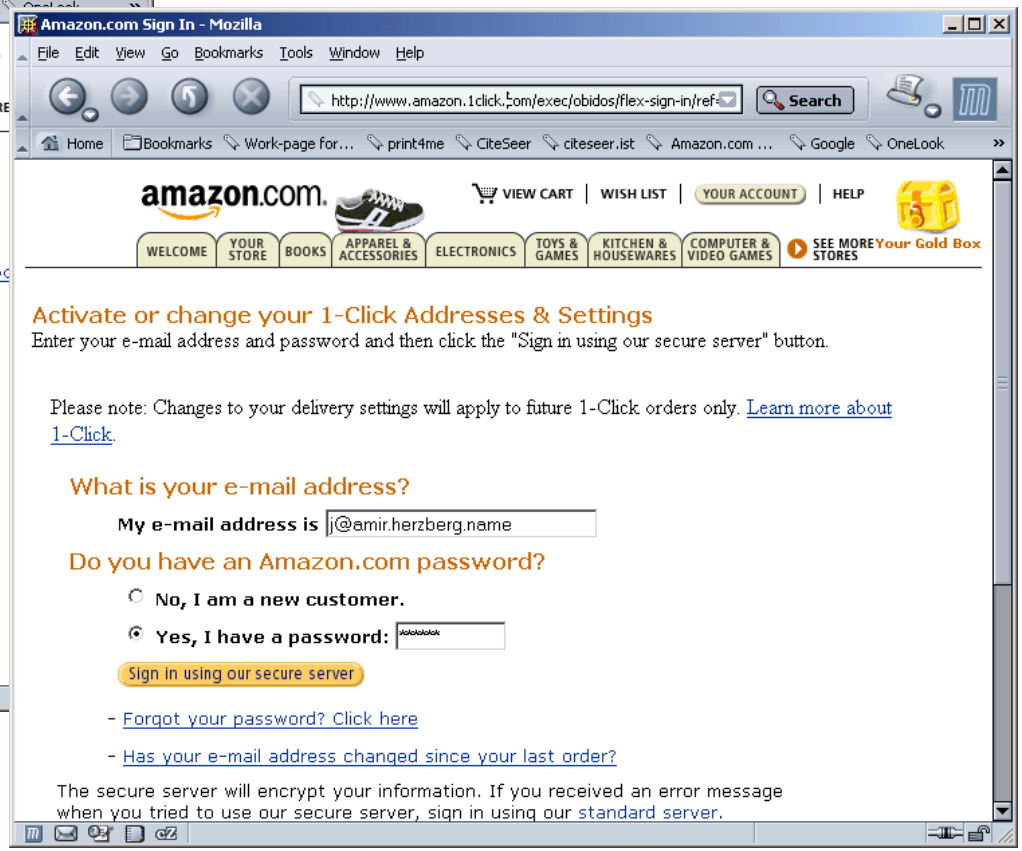
The number of *unique* phishing websites detected by **APWG** was **9715** in January 2006, a huge increase in unique phishing sites from the previous two months.

A*STAR I²R

Phishing and web spoofing (not protected by SSL/TLS)



Authentic Amazon Website



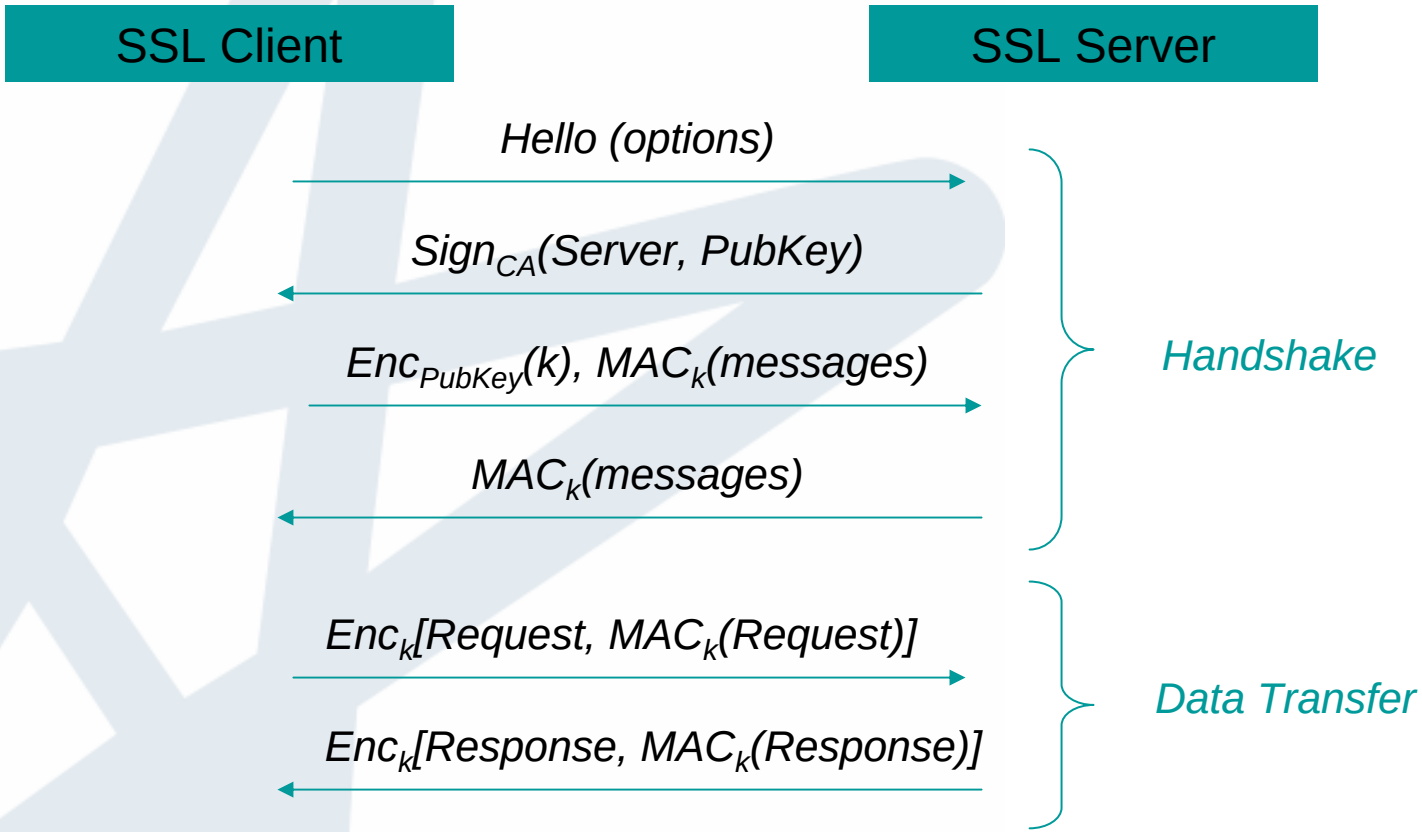
Spoofed Amazon Website

Many sites are not protected:

Chase, PayPal, MS Passport, EquiFax, SmithBarney…

I²R A*STAR

Web-spoofing over SSL/TLS



Simplified SSL/TLS Protocol

A*STAR I²R

Web spoofing over SSL/TLS (ideally)

- **Sensitive sites are protected via SSL/TLS:**
  - *Site* identified by URL, PK in cert, signed by CA
  - Without SSL: identify only by URL (fails against MITM)
  - *CA* identified by PK list in browser (init by vendor)
  - *User* identified by <uid,pw> (encrypted by SSL)
  - User identification by certificate exists but rarely used
  - Present credentials as “seals” (click to validate?)
- **Users are responsible to:**
  - Validate domain of sites (from URL) [SSL and non SSL!]
  - SSL sites: validate padlock/https indicators
  - SSL sites: validate that the CA (or all CAs) are trustworthy

A*STAR I²R

Web spoofing over SSL/TLS (reality)

However, user rarely (from an investigation)

- Notice SSL indicators (padlock, https)
  - Tests: most (77%) did *not* detect SSL indicators!
  - Many login sites are not protected by SSL
  - E.g. Chase, PayPal, MS Passport, EquiFax, SmithBarney…
- Notice URL in wrong domain
  - Wrong domain login: http://www.citibanks.com
  - Tests: most (65%) did *not* detect wrong domain and no SSL!
- Are aware of and trust the CAs
  - Almost none identified CAs correctly
- Validate credentials (“seals”) presented in sites
  - Although seals often link to a validation page of issuer

A*STAR I²R

Previous works

First work:

- Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Web Spoofing: An Internet Con Game. Proceedings of the Twentieth National Information Systems Security Conference, Baltimore, October 1997.

Following ups:

- Serge Lefranc and David Naccache, “Cut-&-Paste Attacks with Java”. 5th International Conference on Information Security and Cryptology (ICISC 2002), LNCS 2587, pp.1-15, 2003.
- Yee, K.-P.. User Interaction Design for Secure Systems, University of California Berkeley Tech report, May 2002, Tech Report CSD-02-1184
- Zishuang (Eileen) Ye, Sean Smith: Trusted Paths for Browsers. USENIX Security Symposium 2002, pp. 263-279.
- Eileen Zishuang Ye ,Yougu Yuan, Sean Smith. Web Spoofing Revisited: SSL and Beyond . *Technical Report TR2002-417* February 1, 2002.
- Tieyan Li, Yongdong Wu. "Trust on Web Browser: Attack vs. Defense". International Conference on Applied Cryptography and Network Security (ACNS'03). Kunming China. Oct. 16-19, 2003.

A*STAR I²R

Recent works (Visual Spoofing)

- Amir Herzberg, Ahmad Gbara, TrustBar: Protecting (even Naive) Web Users from Spoofing and Phishing Attacks. 2004:Cryptology ePrint Archive: Report 2004/155.

- Andre Adelsbach, Sebastian Gajek, and Jorg Schwenk. Visual Spoofing of SSL: Protected Web Sites and Effective Countermeasures. In Proceedings of Information Security Practice and Experience '2005, LNCS 3469, pp.204-216, 2005.

- Rachna Dhamija, J.D.Tygar, The Battle Against Phishing Dynamic Security Skins, Proceedings of the 2005 ACM Symposium on Usable Security and Privacy, July 2005.

In fact, practical web-spoofing attacks deployed so far, do not use such techniques, or use just basic scripts and browser vulnerabilities e.g. to present fake location bar [APWG04] -- almost all of the many reported attacks left significant clues for the expert, attentive user, such as the lack of use of SSL/TLS, and/or the use of a URL from a domain not owned by the victim web site. **Less user involved checking is the key!**

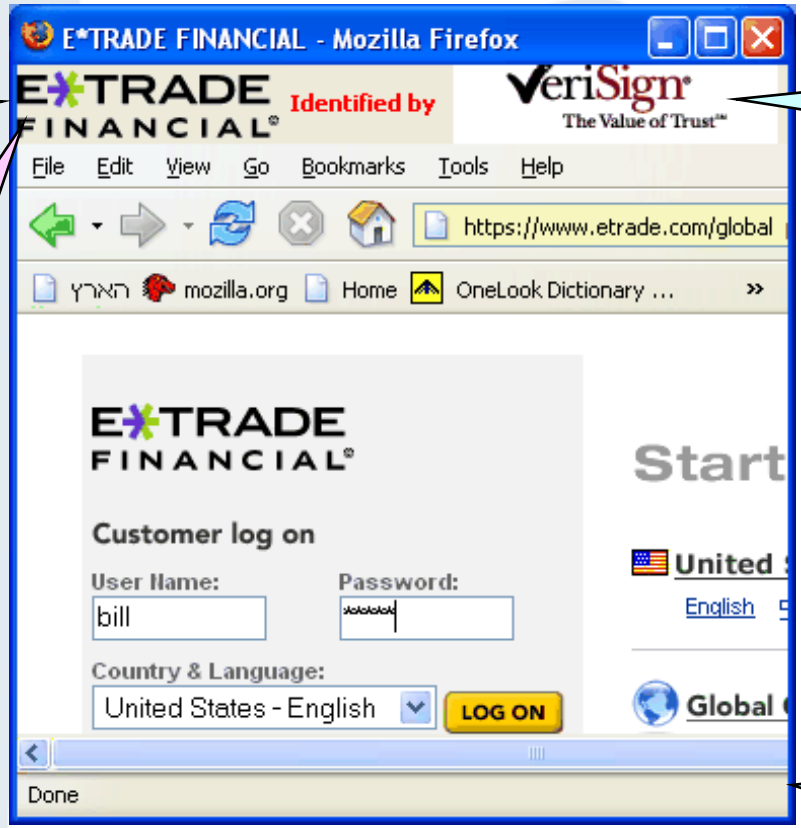
A*STAR I²R

Countermeasure (I)

TrustBar: Re-establishing Trust in the Web by Amir Herzberg, 2004

http://www.cs.biu.ac.il/~herzbea/TrustBar/index.html

Identify site by logo or name



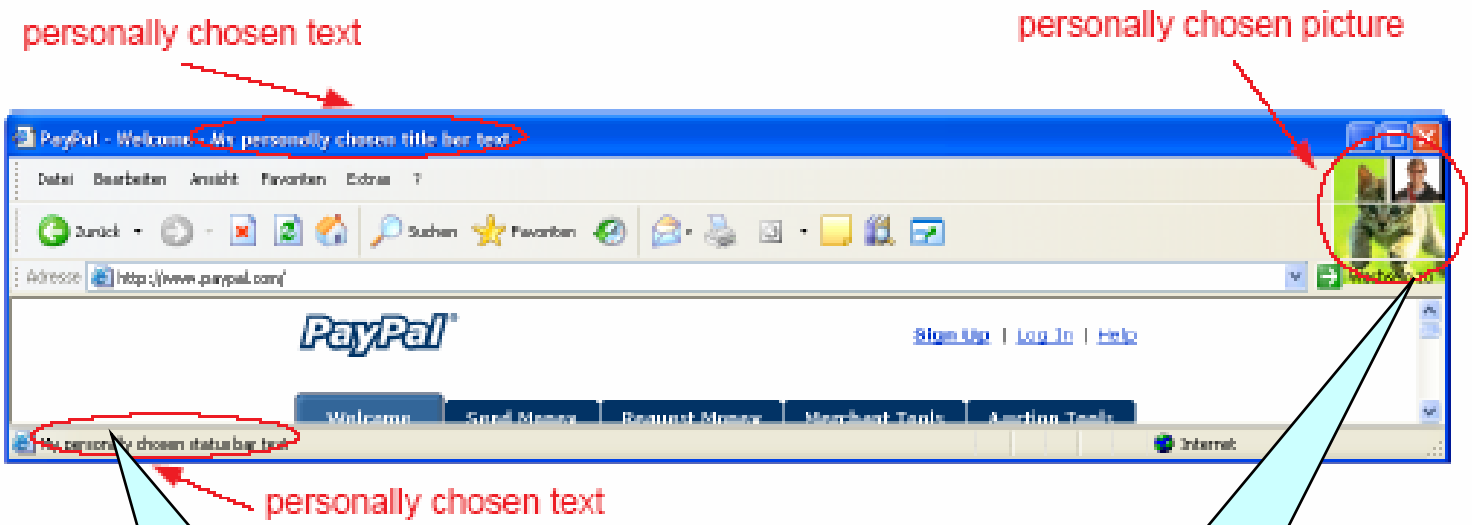
Identify CA by logo or name

TrustBar appears in every window to prevent spoofing, only user can disable

Window too small for `regular` padlock

Countermeasure (II)

BSCI, Browser Secure Connection Indicator, Adelsbach et. al (2005)

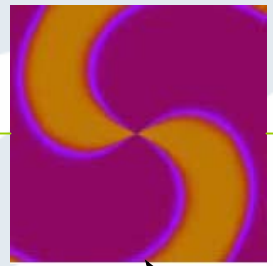


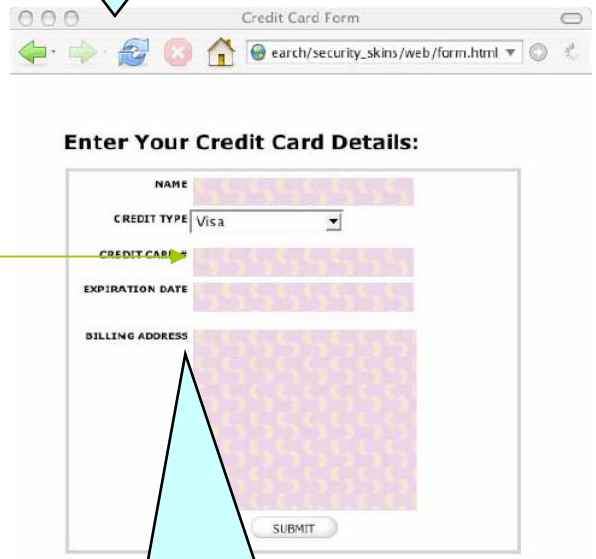
Countermeasure (III)

Dynamic security skin: Dhamija et. al 2005

(0) Trusted password window with personal images.

(1) A verifier (SRP) is exchanged between user and bank at set-up phase.





(3) Visual hash generated by browser and server independently after a successful authentication

(4) Trusted password window displays the visual hash.

(5) Visual hash appeared in the background of logon window

A*STAR

Problems in related works

- **TrustBar (TCA):**
  - How to design the indicator for insecure windows that can detect spoofed credentials?
  - How logos are certified and how to resolve disputes of similar logos (attackers evolve to register similar logos just like they registered similar domain names)?
  - Banks need to have their logos certified.
- **BSCI (Personal image):**
  - Rely on user's skill on recognizing the security indicators.
  - Client must has personal folder to store the pictures.
  - Hard to remember individual images for different SSL servers.
- **Dynamic Security Skins:**
  - Complex and difficult to implement on browser (trusted password window is not standard browser).
  - Need personal image folder at client PC.
  - Need first time set-up via SRP protocol.
  - Bank server needs to remember all customers' verifiers.
  - Additional computation and customization for each login request.

A*STAR I²R

Other works (Non-visual Phishing)

- Markus Jakobsson, Modeling and Preventing Phishing Attacks. Phishing Panel in *Financial Cryptography '05*. 2005.

- B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. Mitchell, Stronger Password Authentication Using Browser Extensions. In proceedings of Usenix security '05.

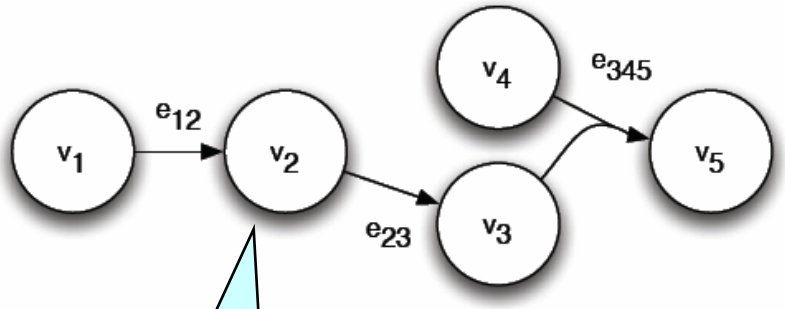
- A. Juels, M. Jakobsson, and T. Jagatic. Cache Cookies for Browser Authentication. IEEE Security and Privacy 2006.

- Bryan Parno, Adrian Perrig, Cynthia Kuo Phoolproof Phishing Prevention. To appear at Financial Cryptography and Data Security (FC'06).

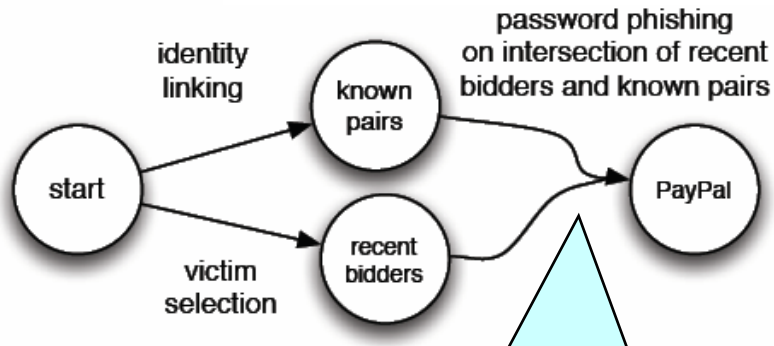
A*STAR I²R

Non-visual countermeasure (I)

Theoretical phishing model, Markus Jakobsson et. al (2005)



A simplified phishing graph of a man-in-the-middle attack on a domain name server

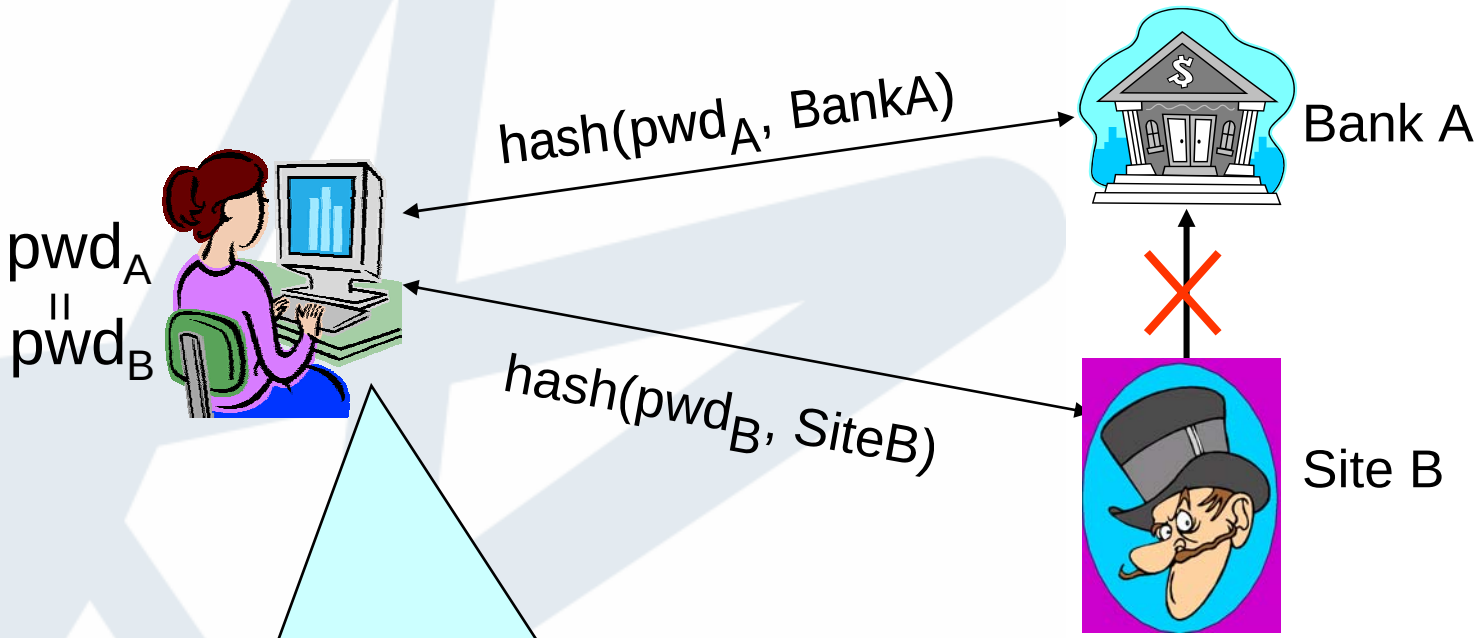


A context aware attack on an eBay bidder. The attack is performed on victims that have been selected both in the recent bidder selection, and for whom identify linking has succeeded.

I²R
A*STAR

Non-visual countermeasure (II)

PwdHash, Ross et. al (2005)



Generate a unique password per site:

HMACfido:123(banka.com) ⇒ Q7a+0ekEXb

HMACfido:123(siteb.com) ⇒ OzX2+ICiqc

Non-visual countermeasure (III)

Active cookies, or cache cookies, Ari Juels et. al (RavenWhite Inc., 2006)

(0) At 1st login, setup a cookie in browser

(1) Next, browser ID

(2) C, (a challenge)

(3-1) $Enc_{Key}(C)$, (HTTP channel)

(3-2) $Enc_{Key}(C)$, (another trusted IP route)

(4) Authenticated browser, start secure session

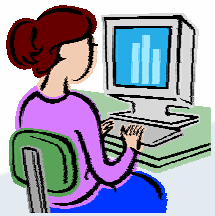
A cookie is a piece of cached and sandboxed executable code, e.g., a JavaScript object, stored as a browser extension.
A cookie = $ID_{browser}$ + Key + IP_{server}

Server needs to maintain an identifier tree. Additional memory and computation.

A*STAR I²R

Non-visual countermeasure (IV)

Phoolproof, Bryan Parno et. al (2006)



A shared secret is sent to the trusted device over a out-of-band channel at account setup phase. On the device are $Cert_{server}$ + secret + Public Key Pair.

(0) Initially setup a secret on device (via an out-of-band channel)

(1) Next, Hello

(2) $Cert_S$, DH_S

(3) $Cert_S$

(4) $Cert_k$

(5) h

(6) h_k^{-1}

(7) $Cert_k$, DH_C, h_k^{-1}

Secure session

Server needs to assist the first time account setup and further the DH key exchange with the trusted device.

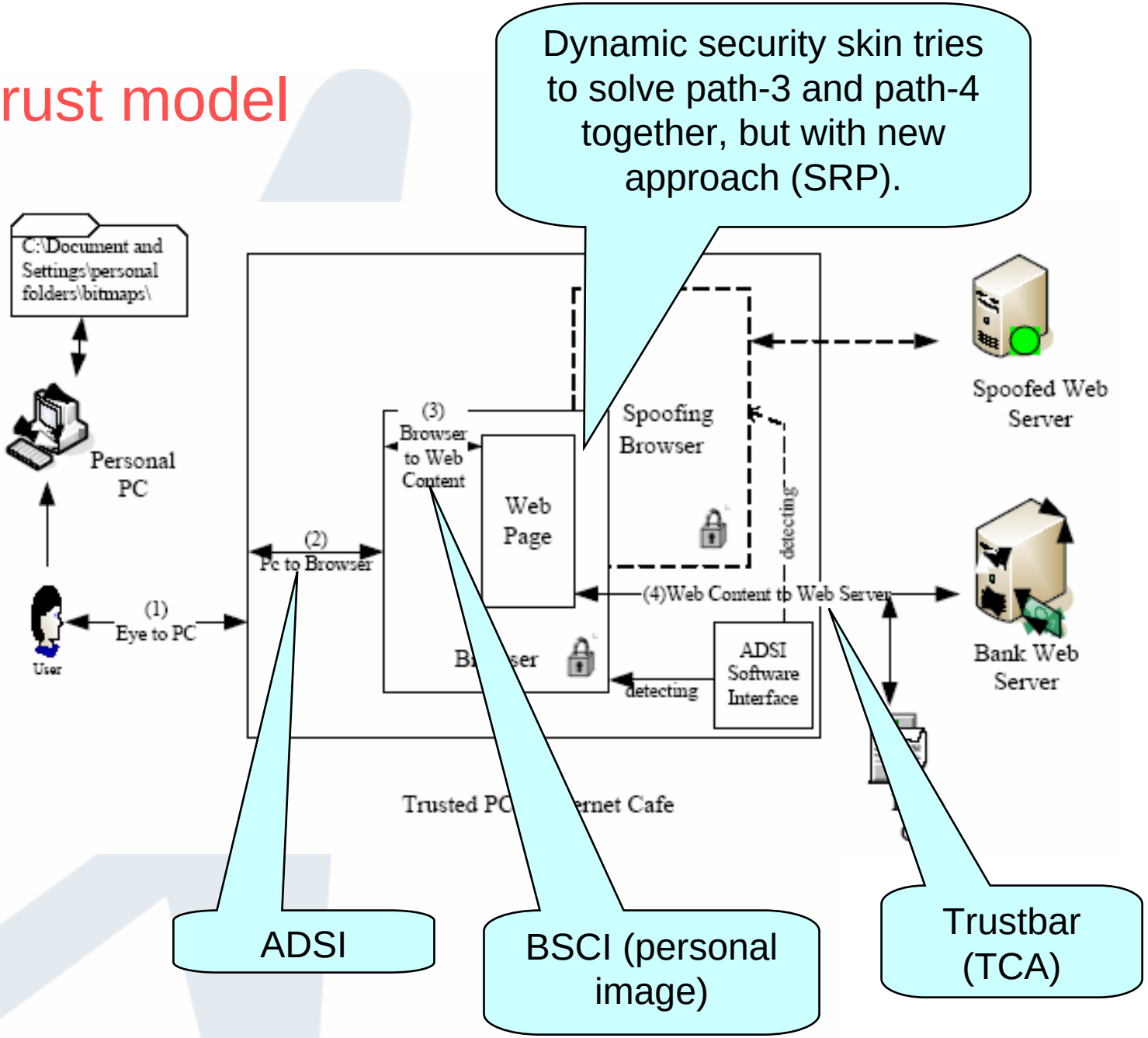
A*STAR I²R

Problems with non-visual phishing techniques

- **Phishing model:**
  - Not much useful against practical attacks.
- **PwdHash:**
  - Ineffective against pharming or DNS spoofing attack.
  - Still suffer from dictionary attack on a weak password.
- **Active cookies:**
  - Rely on first time login for setting up cookies.
  - Server side needs to maintain an identifier tree and needs additional computation on every new session.
  - Users are limited by the necessary cookies (can not securely login without them)
- **Phoolproof:**
  - Rely on a trusted hardware device as an additional authenticator.
  - First time account setup is needed.
  - Any *update* on account or server certificate would need re-establish the secrets.
  - Users are limited by the *necessary* trusted devices.

A*STAR I²R

Trust model



A*STAR I²R

ADSI scheme

- **Goals:**
  - Relax user's burden: automate the process of detection.
  - Ease of usage: little intrusive on the browser
  - Machine independent: trusted PC at Internet Cafe.

- **Assumptions:**
  - **Trust PC vs. personal PC:**
    - A user has partial control over trust PC, but total control of a personal PC (no personal folder on a trust PC).
    - No spyware or virus is existed in the current session for both PCs.
  - **Secure Browser Session:**
    - Started immediately as opening a browser.
    - Keep activated in the whole browsing session.
    - Multiple SBSs are allowed on a trusted PC.

A*STAR I²R

ADSI scheme

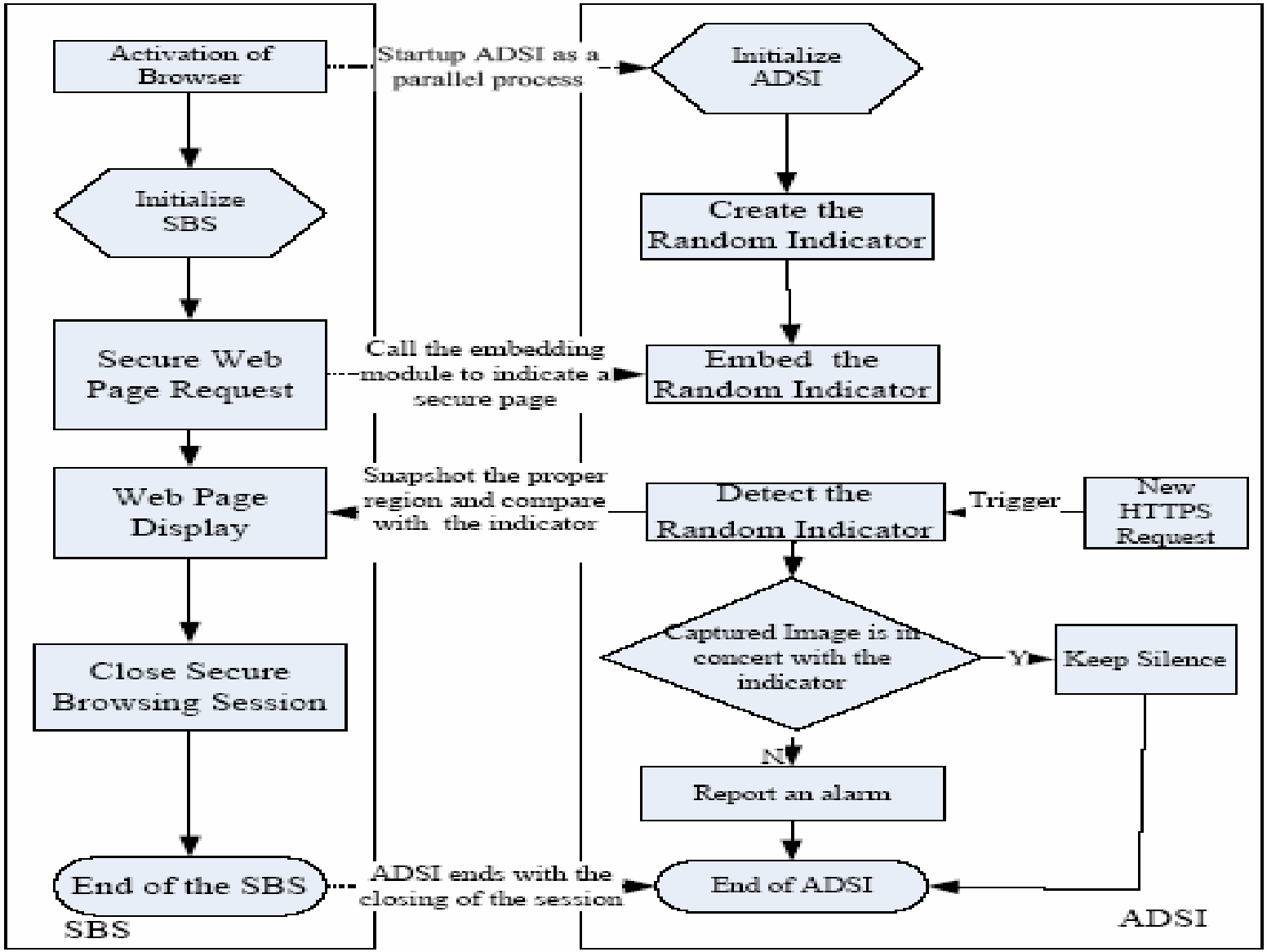
- **Creating the random indicator**
  - A random seed with URL, Screen data, system time and file record.
  - Random art to generate a unique image from the random seed.

- **Embedding the random indicator:**
  - Embedding the random image onto a random position of the browser (SBS will store the status information).
  - Faked popup window can not predict the position and the content.

- **Detecting the random indicator**
  - ADSI will be triggered on checking any new action.
  - ADSI will snapshot the region and compare it with the random image
  - Report spoofing if there is a mismatch.

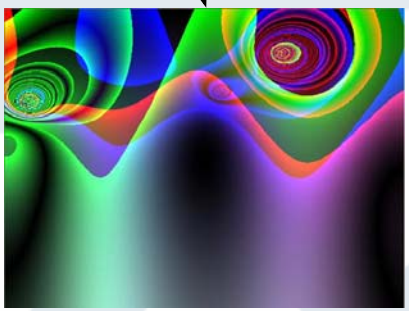
A*STAR I²R

Process flow of ADSI



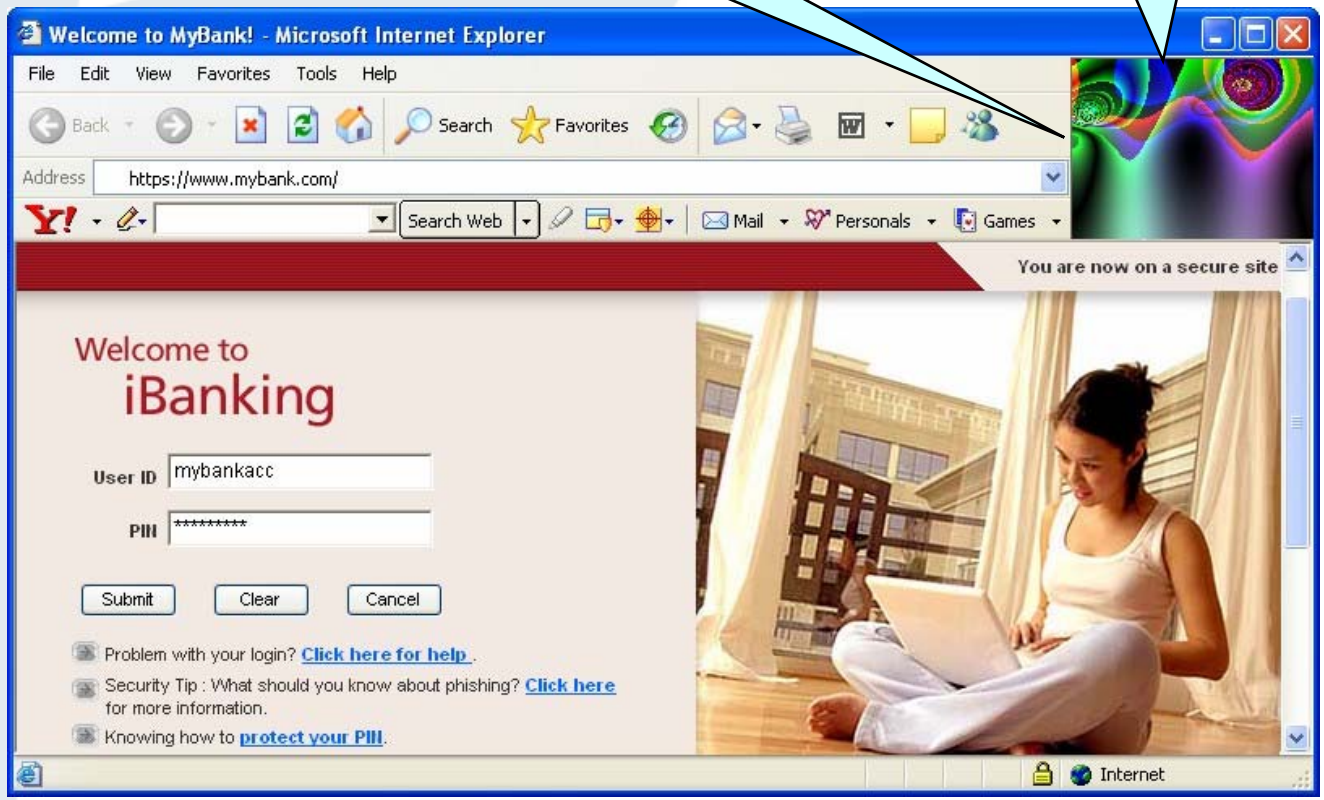
Illustration

(0) A picture is generated by random art and stored in SBS



(2) Snapshot the picture in from a region in current SBS and compare (valid or not?)

(1) Randomly inserted into a position of the current browser



Discussion

- **We have introduced the features of ADSI like Automatic detection, Ease of usage and Machine independent.**
- **Moreover:**
  - Protected path-2: PC to web browser.
    - A simple and effective way cleanly defending only the popup window spoofing attack. (Trusted browser)
  - Extension
    - Personal image protecting path-3 (browser to web content): randomly generated image is not that attractive, which is compensated by automatic checking mechanism. On a home PC with personal image folders, ADSI can still help the user check wrong signals automatically. (path-2 + path-3)
    - Trusted Credential Area protecting path-4 (web content to web server): no conflict to combine these two solutions. (path-2 + path-4)
    - Finally, a full trusted path (path-2 + path-3 + path-4)

      = ADSI + personal image + TCA

A*STAR I²R

Conclusions and future works

- We analyzed web spoofing attacks as well as the major countermeasures under our trust model.
- We proposed an approach-ADSI on preventing web spoofing with the weakest security assumption, which is secure, efficient and easy to use.
- However, it can not protect path 3 and path 4, so in practical, it can be combined with other protection schemes to form a syndicated anti-spoofing solution.

Thank you!

Q & A

A*STAR I²R