Lecture 14 - Web Security

CSE497b - Spring 2007
Introduction Computer and Network Security
Professor Jaeger
www.cse.psu.edu/~tjaeger/cse497b-s07/
Network vs. Web Security
What is the web?

- A collection of application-layer services used to distribute content
  - Web content (HTML)
  - Multimedia
  - Email
  - Instant messaging

- Many applications
  - News outlets, entertainment, education, research and technology, …
  - Commercial, consumer and B2B

- The largest distributed system in existence
  - threats are as diverse as applications and users
  - But need to be thought out carefully …
Secure socket Layer (SSL/TLS)

• Used to authenticate servers
  – Uses certificates, “root” CAs

• Can authenticate clients

• Inclusive security protocol

• Security at the socket layer
  – Transport Layer Security (TLS)
  – Provides
    • authentication
    • confidentiality
    • integrity
SSL Handshake

(1) Client Hello (algorithms, …)

(2) Server Hello (alg. selection, …)

(3) Server Certificate

(4) ClientKeyRequest

(5) ChangeCipherSuite

(6) ChangeCipherSuite

(7) Finished

(8) Finished
Simplified Protocol Detail

Participants: Alice/A (client) and Bob/B (server)

Crypto Elements: Random R, Certificate C, $k_i^+$ Public Key (of i)

Crypto Functions: Hash function $H(x)$, Encryption $E(k, d)$, Decryption $D(k, d)$, Keyed MAC $HMAC(k, d)$

1. Alice $\rightarrow$ Bob $\quad R_A$

2. Bob $\rightarrow$ Alice $\quad R_B, C_B$
   
   Alice pick pre-master secret $S$
   
   Alice calculate master secret $K = H(S, R_A, R_B)$

3. Alice $\rightarrow$ Bob $\quad E(k_B^+, S), HMAC(K', CLNT' + [\#1, \#2])$
   
   Bob recover pre-master secret $S = D(k_B^-, E(k_B^+, S))$
   
   Bob calculate master secret $K = H(S, R_A, R_B)$

4. Bob $\rightarrow$ Alice $\quad HMAC(K', SRV R' + [\#1, \#2])$

Note: Alice and Bob: IV Keys, Encryption Keys, and Integrity Keys 6 keys, where each key $k_i = g_i(K, R_A, R_B)$, and $g_i$ is key generator function.
SSL: Tradeoffs

• Advantages
  – Confidential session
  – Server authentication*
  – GUI clues for users
  – Built into every browser
  – Protocol has heavily analyzed

• Disadvantages
  – Users don’t check certificates (don’t know meaning)
  – Too easy to obtain certificates
  – Too many roots in the browsers
  – Some settings are terrible
    • ssl v2 is on, totally insecure cipher suites included
Reality of SSL

• SSL is here to stay no matter what
• credit card over SSL connection is probably safer than credit card to waiter

• biggest hurdles:
  – performance
  – user education (check those certificates)
  – too many trusted sites (edit your browser prefs)
  – misconfiguration (turn off bad ciphersuites)
  – can be used for many non-web applications

• Now used for more than https, base for many distributed applications, etc.
Library Attack …

- I am sitting in the local library using the computer …
- … to buy some stuff …
- … and walk away …
Cookies

- Cookies were designed to offload server state to browsers
  - Not initially part of web tools (Netscape)
  - Allows users to have cohesive experience
  - E.g., flow from page to page,
- Someone made a design choice
  - Use cookies to authenticate and authorize users
  - E.g. Amazon.com shopping cart, WSJ.com
Cookie Issues …

• New design choice means
  – Cookies must be protected
    • Against forgery (integrity)
    • Against disclosure (confidentiality)
• Cookies not robust against web designer mistakes
  – Were never intended to be
  – Need same scrutiny as any other tech.

Many security problems arise out of a technology built for one thing incorrectly applied to something else.
Cookie Design 1: mygorilla.com

• Requirement: authenticate users on site

mygorilla.com

• Design:
  1. use digest authentication to login user
  2. set cookie containing hashed username
  3. check cookie for hashed username

• Q: Is there anything wrong with this design?
Cookie Design 2: mygorilla.com

- Requirement: authenticate users on site mygorilla.com

- Design:
  1. use digest authentication to login user
  2. set cookie containing encrypted username
  3. check cookie for encrypted username

- Q: Is there anything wrong with this design?
Web Content

• All providers serve up content …
• All sorts of technologies to improve content
  – Interactivity: Forms, CGI, Javascript, …
  – Web applications: Java, Flash, ActiveX…
  – Dynamic content: Servlets, Active Server Pages …
• However, these come with risks …
  – Both clients and servers must use complex and
    sometimes untried technologies …
  – … that have led to some nasty security problems.
**JavaScript**

- Scripting Language used to improve the quality/experience
  - Create dialogs, forms, graphs, …
  - Built upon API functions (lots of different flavors)
  - No ability to read local files, open connections …

- Security: No ability to read local files, open connections, but …
  - DOS – the “infinite popup” script
    - Often could not “break out” with restarting computer
  - Spoofing – easy to create “password” dialogs
Applications/Plugins

• A *plugin* is a simply a program used by a browser to process content
  – MIME type maps content to plugin
  – Like any old application (e.g., RealAudio)
  – Newer browsers have autoinstall features

• A kind of plug-in …
  – “Free pornography …”

• Moral: beware of plugins
Drive by downloads

• Using a deceptive means to get someone to install something on their own (spyware/adware)

  – Once you have one, then it starts downloading lots of others, their friends, …

  – A personal favorite: extortion-ware -- pay us 40$ for our popup blocker, etc ….

    • The real gambit is that they demand 40$ for the uninstall option

• Answer: go get ad-aware and install it (its free)!
Spyware

• Definition: hidden software that uses local host to transmit user secrets
  – e.g., browsing habits, forms data

• Typically found in “free” software
  – Gnutella, game tools, demo software, MP3 tools ...
  – Implemented using spyware “engines” - *gator*

• Embeds in local host to
  – Adds shared libraries (.dlls), adds to startup as TSR programs (in registries, start)
  – Often difficult or impossible to remove
    • You are never really sure it is gone (advice: reinstall)

• Gets installed by user action or via some of IEs ability to “help” the user via tools such as *Active-X*
Active X

• Active X is a MS windows technology
  – Really, just a way to run arbitrary code
  – Called controls (.OCX), just programs
  – Conforms to MS APIs to interact with web

• Extends user experience in lots of nice ways
  – Microsoft upgrade, BIOS Upgrades, Lookup services

• Active X controls are automatically downloaded and run by browser
  – Must pass authenticode “trust” check
  – Must be marked as “safe for scripting”
    • Assumed promise of sandboxing …

• Massive security hole ….
**Authenticode**

- Problem: I need to run an application code on my machine, but I worry about security
- Solution: Make sure code only comes from people that you trust.
- Authenticode
  - Sign download content
  - Check that signer is “trusted”
  - Used for all Win* content
  - Problem: Jan 2001
    - Verisign issued two bad MS
Java

• Platform and language for writing applets
  – Sun Microsystems platform for set-top boxes
  – Applets embedded in web pages (or native)
  – Language loosely resembling C++
  – Runs in a Java Virtual Machine (JVM)
    • Every platform has JVM
    • Platform runs arbitrary code (bytecode)
    • Hence: one application runs on a bunch of platforms
    • Great way to take advantage of the web
    • Slow for data/processing intensive applications
Java Security

• Problem: running arbitrary code downloaded from the network is inherently dangerous
  – **Safety** - Restrict the language such that the programmer cannot do anything unsafe
    • No pointers, bounds checking, type safety
    • Automated memory management
    • Access checking
  – **Security** - Restrict the environment such that the program cannot do anything insecure
    • Sandbox, signed code (often .jar files)
    • Bytecode verifier - checks for forged pointers, access violations, type safety violations
    • SecurityManager class – validates operations
    • ClassLoader – safe class loading
Extending the Sandbox

• Netscape uses strict sandbox
  – No local disk access
  – No connections to hosts other than webserver

• Internet Explorer has “Security Zones”
  – Zones: Internet, Trusted, Restricted, Local Intranet, MyComputer
  – Each zone has a range of enabled features
  – Customizable, also pertains to ActiveX controls
  – Nice, but largely unused (at least by me)