13. Web Authentication and Session Hijacking
ENEE 757 | CMSC 818V

Prof. Tudor Dumitraș
Assistant Professor, ECE
University of Maryland, College Park

http://ter.ps/757
https://www.facebook.com/SDSAtUMD

Today’s Lecture

• Where we’ve been
  – Authentication and access control
  – Security of Internet protocols – TCP/IP, BGP, DNS

• Where we’re going today
  – Web authentication
  – Web session hijacking attacks

• Where we’re going next
  – Project checkpoint #1
  – Web security
Project Checkpoint #1

- Prepare short presentations about your progress on the group project
  - 15 minutes: teams with 3 members
  - 10 minutes: individual projects

- Focus on the progress since the pilot project
  - Project goal: depth and quality adequate for publication in a workshop associated with IEEE Symposium on Security and Privacy

- Allow 2-3 minutes at the end of your presentation time for questions and answers

HTTP Digest Authentication

client

Request URL with GET or POST method

server

HTTP 401 Unauthorised Authentication "realm" (description of system being accessed)
Fresh, random nonce

H1=hash(username, realm, password)
H2=hash(method, URL)

Recompute H3 and verify

WWW-Authenticate: Basic realm="Password Required"
Problems with HTTP Authentication

• Can only log out by closing browser
  – What if user has multiple accounts? Multiple users of the same browser?
• Cannot customize password dialog
• Easily spoofed
• In old browsers, defeated by TRACE HTTP
  – TRACE causes Web server to reflect HTTP back to browser
  – Cross-site tracing (XST): malicious scripts injected in the page may access cookies and HTTP headers normally inaccessible to Javascript
    • May reveal passwords and authenticators
• Hardly used in commercial sites

Sessions

• HTTP is a stateless protocol

• Need to provide the concept of a session: a sequence of requests and responses from one browser to one or more sites
  – Can be long or short (Gmail – 2 weeks)
  – Without session management, users would have to constantly re-authenticate

• Session management
  – Authorize user once
  – All subsequent requests are tied to user
**Primitive Browser Session**

- View catalog
- Select item
- Check out

Store session information in URL; easily read on network.

**Bad Idea: Encoding State in URL**

- Unstable, frequently changing URLs
- Vulnerable to eavesdropping
- There is no guarantee that URL is private
  - Early versions of Opera used to send entire browsing history, including all visited URLs, to Google
  - URLs are stored in Web server logs
Storing State in Hidden Forms

- Dansie Shopping Cart (2000)
  - "A premium, comprehensive, Perl shopping cart. Increase your web sales by making it easier for your web store customers to order."

```html
<form method="post" action="http://www.dansie.net/cgi-bin/scripts/cart.pl">
  Black Leather purse with leather straps<br>Price: $20.00<br>
  <input type="hidden" name="name" value="Black leather purse">
  <input type="hidden" name="price" value="20.00">
  <input type="hidden" name="sh" value="1">
  <input type="hidden" name="img" value="purse.jpg">
  <input type="hidden" name="custom1" value="Black leather purse with leather straps">
  <input type="submit" name="add" value="Put in Shopping Cart">
</form>
```

Shopping Cart Form Tampering

http://xforce.iss.net/xforce/xfdb/4621

- Many Web-based shopping cart applications use hidden fields in HTML forms to hold parameters for items in an online store. These parameters can include the item’s name, weight, quantity, product ID, and price. Any application that bases price on a hidden field in an HTML form is vulnerable to price changing by a remote user. A remote user can change the price of a particular item they intend to buy, by changing the value for the hidden HTML tag that specifies the price, to purchase products at any price they choose.

- Platforms affected:
  - 3D3.COM Pty Ltd: ShopFactory 5.8 and earlier
  - Adgrafs: Check It Out Any version
  - ComCity Corporation: SalesCart Any version
  - Dansie.net: Dansie Shopping Cart Any version
  - Make-a-Store: Make-a-Store OrderPage Any version
  - McMurtrey/Whitaker & Associates: Cart32 3.0
  - Rich Media Technologies: JustAddCommerce 5.0
  - Web Express: Shoptron 1.2

- @Retail Corporation: @Retail Any version
- Baron Consulting Group: WebSite Tool Any version
- Crested Butte Software: EasyCart Any version
- Intelligent Vending Systems: Intellivend Any version
- McMurtrey/Whitaker & Associates: Cart32 2.6
- pknusen@nethut.no: CartMan 1.04
- SmartCart: SmartCart Any version
Other Risks of Hidden Forms
[K. Mitnick, The Art of Intrusion]

Estonian bank’s Web server...
- HTML source reveals a hidden variable that points to a file name
- Change file name to password file
- Server displays contents of password file
  - Bank was not using shadow password files!
- Standard cracking program took 15 minutes to crack root password

Session Tokens (Identifiers)

<table>
<thead>
<tr>
<th>Browser</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET /index.html</td>
<td>check credentials</td>
</tr>
<tr>
<td>set anonymous session token</td>
<td>validate token</td>
</tr>
<tr>
<td>GET /opencontent.html</td>
<td>anonymous session token</td>
</tr>
<tr>
<td>anonymous session token</td>
<td>logged-in session token</td>
</tr>
<tr>
<td>POST /do-login</td>
<td>check credentials</td>
</tr>
<tr>
<td>Username and password</td>
<td>validate token</td>
</tr>
<tr>
<td>set logged-in session token</td>
<td>logged-in session token</td>
</tr>
</tbody>
</table>
Generating Session Tokens (1)

- Option #1: minimal client state
- Token = random, unpredictable string
  - No data embedded in token
  - Server stores all data associated with the session: user id, login status, login time, etc.
- Potential server overhead
  - With multiple sessions, lots of database lookups to retrieve session state

Generating Session Tokens (2)

- Option #2: more client-side state
- Token = [ user ID, expiration time, access rights, user info ... ]
- How to prevent client from tampering with his session token?
  - HMAC(server key, token)
- Server must still maintain some user state
  - For example, logout status (check on every request) to prevent usage of unexpired tokens after logout
Examples of Weak Tokens

- Verizon Wireless: counter
  - Log in, get counter, can view sessions of other users

- Apache Tomcat: generateSessionID()
  - MD5(PRNG) … but weak PRNG
  - Result: predictable SessionID’s

- ATT’s iPad site: SIM card ID in the request used to populate a Web form with the user’s email address
  - IDs are serial and guessable
  - Brute-force script harvested 114,000 email addresses

Binding Token to Client’s Machine

Embed machine-specific data in the token...

- Client’s IP address
  - Harder to use token at another machine if stolen
  - If honest client changes IP address during session, will be logged out for no reason

- Client’s browser / user agent
  - A weak defense against theft, but doesn’t hurt

- HTTPS (TLS) session key
  - Same problem as IP address (and even worse)
Storing Session Tokens

- Embed in URL links
  - https://site.com/checkout?SessionToken=kh7y3b

- Browser cookie
  - Set-Cookie: SessionToken=fduye63sfdb

- Store in a hidden form field
  - `<input type="hidden" name="sessionid" value="kh7y3b">`

- Window.name DOM property

Issues

- Embedded in URL link
  - Token leaks out via HTTP Referer header

- Browser cookie
  - Browser sends it with every request, even if not initiated by the user (cross-site request forgery)

- Hidden form field
  - Short sessions only

- DOM property
  - Not private, does not work if user connects from another window, short sessions only
Cookies

Web Authentication with Cookies

• Cookie = mechanism for web servers to store state on the clients
  — Set-cookie: key=value

• Authentication system that works over HTTP and does not require servers to store session data
  — ... except for logout status

• After client successfully authenticates, server computes an authenticator token and gives it to the browser as a cookie
  — Client should not be able forge authenticator on his own
  • Example: HMAC(server’s secret key, session information)

• With each request, browser presents the cookie; server recomputes and verifies the authenticator
  — Server does not need to remember the authenticator
Typical Session with Cookies

client

- POST /login.cgi
- Set-Cookie:authenticator
- GET /restricted.html
- Cookie:authenticator
- Restricted content

server

- Verify that this client is authorized
- Check validity of authenticator – recompute hash(key, session)

Authenticators must be unforgeable and tamper-proof
(malicious client shouldn’t be able to compute his own or modify an existing authenticator)

.NET 2.0

  - Secret Web server key intended for cookie protection
  - Stored on all Web servers in the site

- Creating an encrypted cookie with integrity
  - HttpCookie cookie = new HttpCookie(name, val);
    HttpCookie encodedCookie = HttpSecureCookie.Encode (cookie);

- Decrypting and validating an encrypted cookie
  - HttpSecureCookie.Decode (cookie);
Cookie Theft: SideJacking

- **SideJacking** = network eavesdropper steals cookies sent over a wireless connection
- Case 1: a website uses HTTPS for login, the rest of the session is unencrypted
  - Cookies must not be marked as “secure” \( \textbf{why?} \)
- Case 2: accidental HTTPS→HTTP downgrade
  - Laptop sees Wi-Fi hotspot, tries HTTPS to Web mail
  - This fails because first sees hotspot’s welcome page
  - Now try HTTP... with unencrypted cookie attached!
  - Eavesdropper gets the cookie – user’s mail is pwned

Cookie Theft: Surf Jacking


It is possible to force an HTTPS→HTTP downgrade

- Victim logs into https://bank.com
  - Cookie sent back encrypted and stored by browser
- Victim visits http://foo.com in another window
- Network attacker sends “301 Moved Permanently” in response to the cleartext request to foo.com
  - Response contains header “Location http://bank.com”
- Browser thinks foo.com is redirected to bank.com, starts a new HTTP connection, sends cookie in the clear – network eavesdropper gets the cookie!
Session Fixation Attacks

- Attacker obtains an anonymous session token (AST) for site.com
- Sets user’s session token to attacker’s AST
  - URL tokens: trick user into clicking on URL with the attacker’s token
  - Cookie tokens: need an XSS exploit (more on this later)
- User logs into site.com
- Attacker’s token becomes logged-in token!
- Can use this token to hijack user’s session

Preventing Session Fixation

- When elevating user from anonymous to logged-in, always issue a new session token
- Once user logs in, token changes to value unknown to attacker
Logout Issues

• Functionality: allow login as a different user
• Security: prevent others from abusing account

• What happens during logout?
  1. Delete session token from client
  2. Mark session token as expired on server

• Some sites forget to mark token as expired, enabling session hijacking after logout
  – Attacker can use old token to access account

Sources

• Various slides from Vitaly Shmatikov
Review of Lecture

• What did we learn?
  – Web authentication
  – Web session hijacking attacks

• Paper discussion: “The Dos and Don’ts of Client Authentication on the Web”
  – Discussion lead: Wei
  – Scribe: BumJun

• What’s next?
  – Project Checkpoint #1
  – Web security