Raluca Ada Popa
Spring 2018

CS 161
Computer Security

Discussion 11

Week of April 16, 2018

Question 1 ***Clickjacking*** **(20 min)**

Users take actions on the web based on clicking on links or buttons, yet they may not be taking the action that they think. Clickjacking hijacks their click from the action they intended to do, such as canceling some request, to one an attacker wants them to do, such as enabling remote access to a camera.

(a) How can the attacker trick the user into clicking on something they do not mean to?

(b) What are some defenses against clickjacking?

Solution:

(a) Attacks include

onMouseDown Attacker in control of the page can add onMouseDown command to normal hyperlinks. The user sees a normal link target in the bottom of the browser, but the action taken can be a different site, that only shown up in the browser bottom once the link is clicked. The attack works in the current Chrome and Firefox.

```
<a href=http://www.google.com/
   onmousedown="this.href='http://www.dilbert.com';"
   >Go to Google</a>
```

For Firefox and Chrome this shows google as target, until go to evil once, then each shows evil as target (as of 4/2018).

Changing Curser The attacker can add an extra, and more visible, cursor to the users screen. If the user concentrates on this extra cursor and clicks on a benign button, the real cursor is positioned over a button that gives the attacker extra privileges, such as access to the camera.

Temporal Attacker can get user to engaged in repeated clicking as part of a game to click on targets. This gives the attacker the timing of the user's clicks. The attacker then presents a new target to the user, but changes the user interface, just before the click is expected, to a button asking for some access that the attacker wants. User has already started their finger at clicking on the target when it changes to the attack button.

Browser in Browser

(b) Defenses

As a user, enter sensitive sites directly into the url bar and ensure they are the only site in the window.

As a developer, the main technique to prevent click jacking between sites has been frame busting, but it is not completely effective.

The newer X-Frame-Options allow the server to specify if the browser is allowed to place the page in a frame. Options are:

DENY prevents any domain from framing

SAMEORIGIN allows if same origin

ALLOW-FROM uri allows from specified uri

DENY and SAMEORIGN are supported in recent browsers, as well as ALLOW-FROM uri or an alternative, Content Security Policy (CSP) frame-ancestors.

Question 2 ***Phishing*** **(10 min)**

Phishing tries to gain sensitive user information by tricking users into going to a fake version of a website they trust. The attacker might convince the user to go to what appears to be their bank and to enter their username and password.

(a) What are some ways that attackers try to fool users about the site they are going to? How do they convince people to click on links to sites?

(b) What are some defenses you should employ against phishing?

Solution:

(a) Attacks include:

Sub domains that look like top level domains.

Look alike UNICODE urls: bankofamerca.com, bankofthevvest.com

Look alike unicode characters.

Mentioning recent information. Compromising an email account and then sending emails to people that account has recently corresponded with.

(b) Defenses include:

Some phishing emails or sites are not very well crafted. Subtle language or spelling errors, that should be out of place for the legitimate site, can be a warning sign that you should heed.

Do not click on unexpected links in emails.

If your bank sends you an email about your account, go to your browser and separately type in the banks url, or call them. Do not click on links to sensitive sites that others provide you.

Type sensitive domains directly into the address bar, or create a short cut that way and then use it.

Question 3 ***Web tracking*** **(15 min)**

Sites use information about us to better display information, but also to sell us services, or to sell access to our screen views to advertisers.

(a) What kind of information do sites gain about you to run the technical aspects of the pages they serve?

(b) What other information could a site learn about you? How could a business learn about many of the sites you visit and construct a detailed profile of you based on your web habits.

(c) What measures do you have to restrict this tracking?

Solution:

(a) Technical information that sites learn includes: the time of the request, your browser, OS, language, IP, and general location from your IP address.

They also receive any cookies for that domain, allowing the site to provide continuity of an activity that spans several pages, or required a login.

(b) A business that provides ads analytics services can have client websites provide any information about you to the ads company as part of an image request.

and the characteristics of those users. The site would load an image from this provider that

(c) Defenses include:

Legal protections of user agreements.

States fining companies that allow breath of user data.

Personal defenses include using browser modes that limit tracking scripts, such as Firefox tracking protections.

Question 4 ***Review: Buffer Overflow*** **(5 min)**

Circle and explain all possible issues with the code shown below.

```
1  void print_name(char *first, char *last) {
2      char full[256] = "echo ";
3      if (strlen(first) + strlen(last) + strlen(full) >= sizeof(full))
4          return;
5
6      strcat(full, first);
7      strcat(full, " ");
8      strcat(full, last);
9      system(full);
10 }
```

Solution:

- It is possible that the summation `strlen(first) + strlen(last) + strlen(full)` overflows, causing the comparison to pass even though the copy is unsafe.
- There is an off-by-one error, since the current code does not account for the space between the two names.
- The `system` command is vulnerable to command injection.

A final note: do not hesitate to ask for help! Our office hours exist to help you. Please visit us if you have any questions or doubts about the material.