ComputerScience

Sean Smith, Amalia Safer, Kyle Holzinger
Boston University

Security analysis of GitHub

Background:

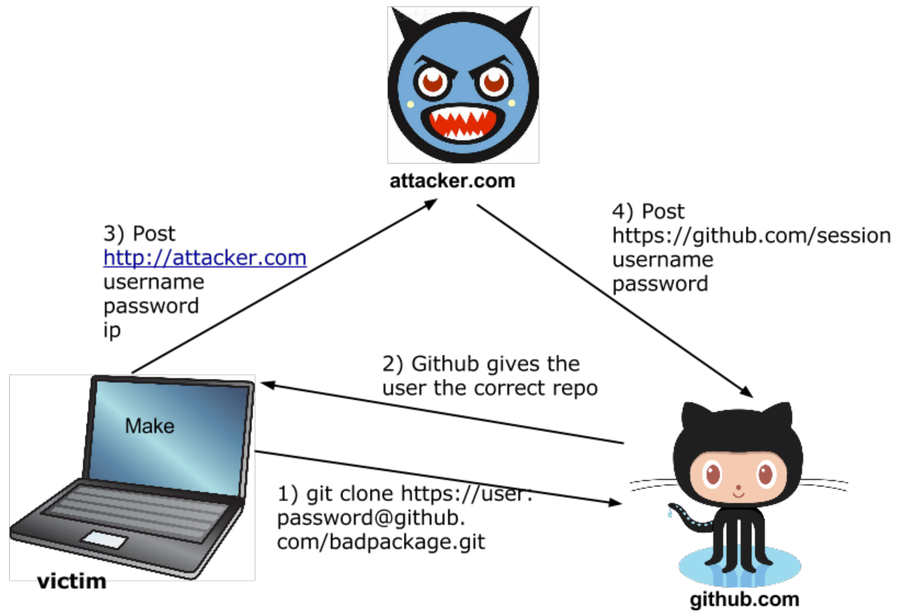
Github is a website that makes it easy to collaborate on code. In the past it has been targeted by foreign governments over hosting software that allows citizens to avoid censorship. It has over 8 million users and hosts code that would be of interest to many governments.

Cookies:

Cookies are used to track users even when they log out. This allows sites to sites to keep users logged in even after the session ends.

A session cookie called user session is stored which contains a seemingly random nonce. When a get request is made to https://github.com, the cookie is sent and the database is queried to see if the cookie is valid. If the cookie is valid it will return user data as if the user is logged in. To impersonate a user, only the user session is needed.

One attack is to guess a random cookie and query to see if it's valid. There are approximately 8 million active github users at a time. The length of the cookie is 80 characters and it is base-64 encoded. Say the set of correct cookies S has size $|S| = 8,000,000$, the universe U has a size of $|U| = 64^{80}$. The probability of guessing a correct cookie c is about $1/10^{138}$. This is too low to be a reasonable attack.



Attack:

1) First the user clones the repository using the command
git clone https://kholzinger:>password<@github.com/kylelh/linkeffects
2) Then the user runs the Makefile, a standard procedure on any operating system.
make
3) The Makefile parses the git username and password which are stored in .git/config file. The git username and password are also the github.com username and password.
4) We send the username, password, and ip address to the com- mand and control server. We can then log into the users ac- count.

User Tracking:

Github does not serve ads as its business model revolves around selling premium subscriptions. However, it does track users for analytics purposes via Google analytics. It does this in two ways:

1) Google analytics sticks cookies on the user's browser.
2) In the rare event that a user removes these cookies, Google analytics tries to fingerprint the user.

Browser Characteristic	Bits of identifying information	One in x browsers
User Agent	12.92	7752.4
HTTP_ACCEPT Headers	6.72	105.71
Browser Plugin Details	11.11	2205.31
Time Zone	4.06	16.67
Screen Size and Color Depth	4.18	18.16
System Fonts	17.21	151725.49
Are Cookie Enabled?	0.43	1.35
supercookie test	0.86	1.81

SSL:

All connections to github.com are done via https. This is enforced via HTTP strict transport security (HSTS). Github sets the Strict-Transport-Security header to max-age=31536000; includeSubdomains; preload. This ensures that for the next year, the browser will only accept connections from github.com over SSL. To further this Github is now included in the chrome STS file. This is a file that ships with Chrome and ensures that whenever Chrome goes to github.com it will only accept connections over SSL. Since Chrome is open source we dug up the STS (strict transport security) file and found the entry that corresponds to Chrome.

{ "name": "github.com", "include subdomains": true, "mode": "force-https" }