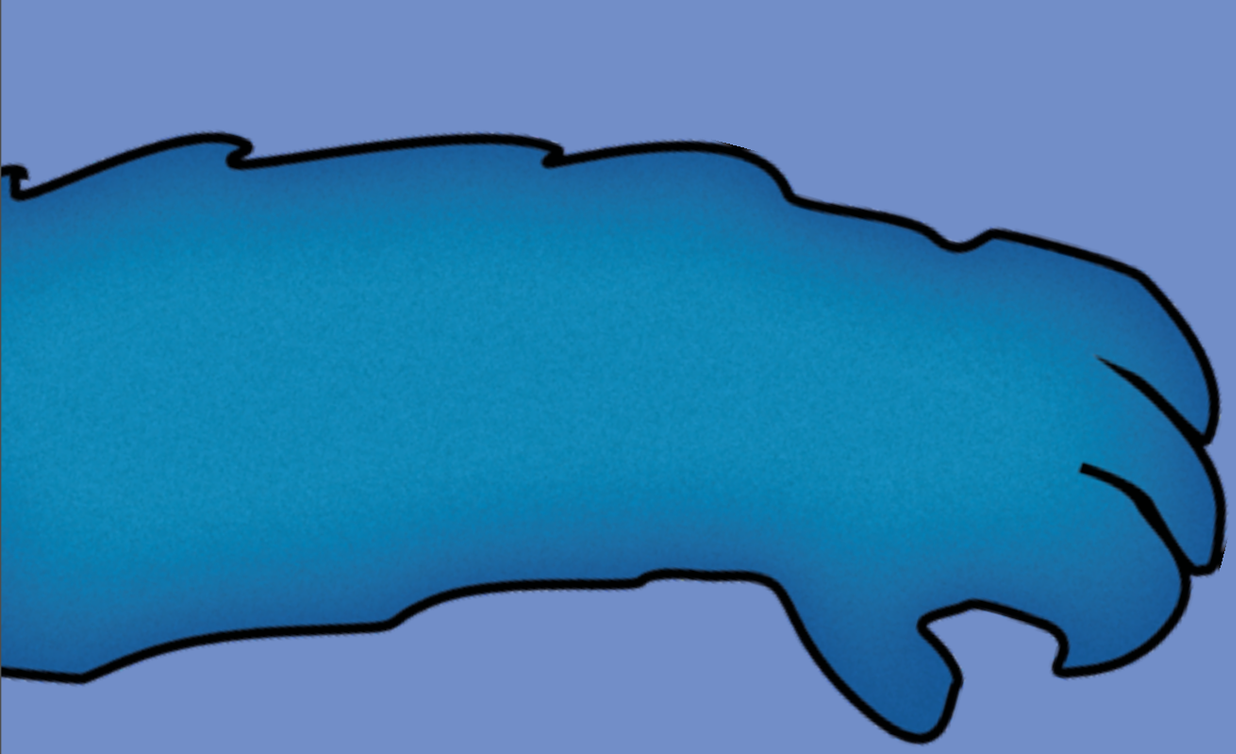
CookieMonster

Thomas Chopitea - Adrien Gsell



CookieMonster Wall

Home Open Wifi networks

Info HTTP Sessions, OSWAP #3 issue

Profile Our attack

Privacy How to protect against it

Share How to extend it

Home

Open Wifi networks

Open WiFi networks (such as Chalmers' Nomad) are unprotected even if they require to log in.

The communication is not encrypted and can be sniffed.

With such WiFi networks, gaining unauthorized access to critical websites can be trivial if they are not protected enough.

CookieMonster

Info

Thomas Chopitea Adrien Gsell 03/13

HTTP cookies

An HTTP cookie is a piece of text stored on a user's computer by their web browser.

A lot of websites use them for session management and authentication.

If the connection with a website is not secured (HTTPS), these cookies are transmitted in clear text!

Even worse on unencrypted WiFi APs...

Session hijacking

Session hijacking is the exploitation of a valid computer session to gain unauthorized access to services

Broken Authentication & Session Management is OSWAP #3 issue

CookieMonster

Profile

Thomas Chopitea Adrien Gsell 05/13

Our Attack

Written in Python

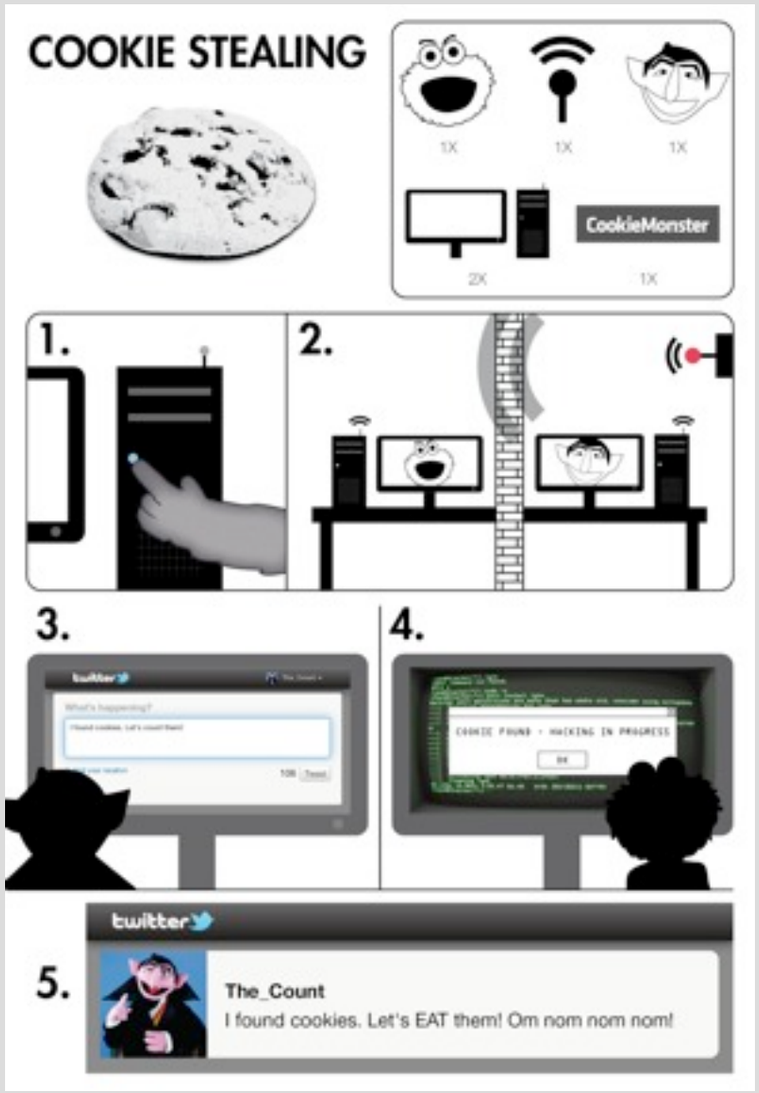
Uses the Scapy library to deal with sniffing

Only interested in packets containing web cookies (hence its name)

Flexible: can easily be customized for any vulnerable website

Work in progress...

User guide


COOKIE STEALING
1X
1X
1X
CookieMonster
2X
1X
1.
2.
3.
4.
5.
twitter
The_Count
I found cookies. Let's EAT them! Om nom nom nom!

Vulnerable websites (among others):

Facebook

Twitter

Flickr

Yahoo

Reddit

Google (Web search and maps)

Youtube

Blogger

MySpace

Campus Efrei (Our home university student portal)

Chalmers?

(Demonstration)

Privacy

How to protect against this attack

For Users:

Protect your WiFi Network (WPA, WPA2...)

Force HTTPS usage when available

SSH tunnels

VPN

How to protect against this attack

For Web Developers:

Always set up an HTTPs server

Smart cookie management

Share

How to extend this attack

ARP poisoning

Fake certificates

Questions?