Arthur Liou
CS373

Week 7 Writeup

Prompt: Submitting a write-up of your thoughts, impressions, and any conclusions based on the material from the week. Each week will have its own assignment in the grades page.

For the first part of this week's writeup, I'm reflecting on the topic – Web Security. MY work lies in SaaS, front and back end web development, so I loved reviewing and learning more about this week's topic, Web Security. I appreciated working through the lab as part of this week's topic – straightforward script and very in tune with what we learned right at the end of lecture – the URL classification system.

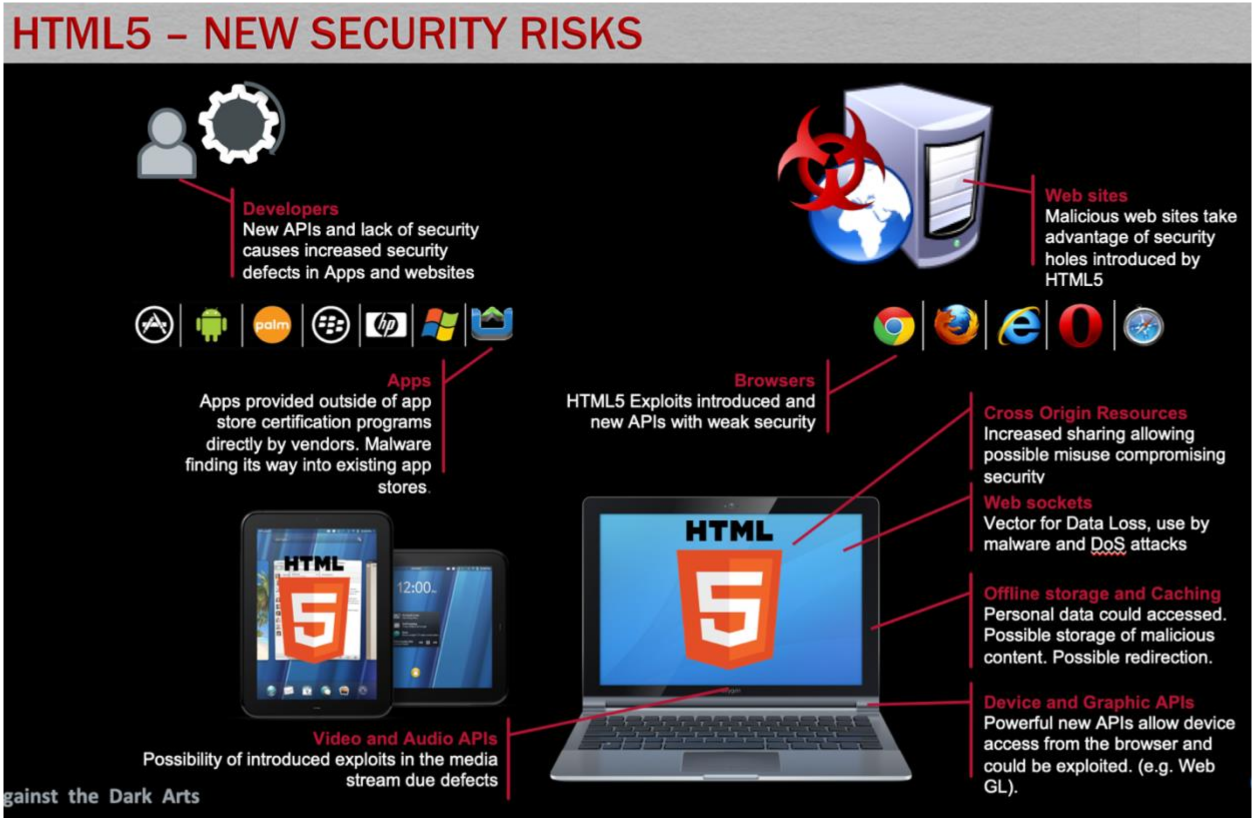
For what we covered and learned, see my lecture notes below.

Lecture Notes

Lesson 1 – Web Security

- Web – HTTP/HTML fundamentals
- Content, Search Engine, Browsers, WWW, Internet, Networks, Computers
- 95% of malware is delivered via the web
- Web Browsing basics. 1.0 &2.0
- Injection points – de-obfuscated content, Javascript, HTML (DOM Tree), HTML (Raw HTML), HTTP
- User-level attacks
- Social Engineering - In the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.
- Phishing, SEO Poisoning, Fake AV, Social Media Link Insertion, Forum Link Insertion, Malvertising
- A bunch of separate slides for the above 6 topics
- User Attack – Common Defenses
- URL / Domain Reputation Systems, Site Certification Services, Safe URL Shorteners, Client and Gateway AV/AM
- Browser-level attacks
- Security features of the modern browser – Content Security Policy Enforcement (Same Origin Policy (SOP), Cross Origin Resource Sharing (CORS), OS Isolation / Sandboxing, and long list of others
- Browser exploit – downloads, renders and executes, exploits vulnerabilities, typically a multi-step process
- Content/Script obfuscation

- Man in the middle attack – intercept and modify traffic in real-time. Requires ability fcor mid-traffic insertion, HTTP
- Man in the Browser – MITB - Dangerous cousin to the MITM attack - Intercept and modify traffic to/from the server, but INSIDE THE BROWSER
- DNS Spoofing - AKA “DNS Cache Poisoning”. Phishing, Exploits
- Clickjacking – UI Redressing – tricks the user into clicking a pre-determined link in a rendered HTML page.
- Example – Adobe Flash settings
- SQL injection. BIS, many flavors of SQL injection, not limited to Data
- Same Origin Policy - Core security feature in all browsers, although not standardized. “Resource from an origin may only access the same origin”
- Cross-site scripting (XSS) - Goal: Inject **client-side** script into **other user’s** browsers. (Bypassing SOP)
- Cross-site request forgery (XSRF) - The evil brother to XSS, also bypassing SOP
- Opposite of XSS - Exploit the server’s trust in the browser, not browser’s trust in the server. Goal: Execute malicious actions against a user (as that user!) on their trusted server (i.e. online bank account)
- Advanced HTML 5 threats – browsers will become more secure
- HTML5 – Benefits to the Web Designer and User, but also benefits to the malicious actor



HTML5 – NEW SECURITY RISKS

Developers
New APIs and lack of security causes increased security defects in Apps and websites

Web sites
Malicious web sites take advantage of security holes introduced by HTML5

Apps
Apps provided outside of app store certification programs directly by vendors. Malware finding its way into existing app stores.

Browsers
HTML5 Exploits introduced and new APIs with weak security

Cross Origin Resources
Increased sharing allowing possible misuse compromising security

Web sockets
Vector for Data Loss, use by malware and DoS attacks

Offline storage and Caching
Personal data could accessed. Possible storage of malicious content. Possible redirection.

Video and Audio APIs
Possibility of introduced exploits in the media stream due defects

Device and Graphic APIs
Powerful new APIs allow device access from the browser and could be exploited. (e.g. Web GL).

gainst the Dark Arts

Lesson 2

- Alexa – userful for determining general site popularity and prevalence, data collected via end-user toolbars, domain-based
- Archiev.org – useful for determining site changes
- IPVoid – check an IP against a large list of IP blacklists
- CheckShortUrl – Url Expander service for most short URL services
- Site Dossier – general site information
- Webutation – Url reputation clearinghouse
- Web inspector – online web scanning tool, also list of recently detected malicious sites, classification techniques
- Virus Total – URL Search, also list of malware files, classification techniques
- Linux Jwhois, Linux DIG
- IOC – indicators of compromise – threat feeds, connects the DOTs, provides contextual data around different malicious objects, shareable
- Research tools
- PhantomJS – Scripable, headless, webkit browser, executes all scripts and fully renders page, can be driven by many scripting languages, accepts user-defined handlers/callback
- JSUNPack – detects exploits that target browser and browser plug-in vulnerabilities
- Burp Suite – intercept and modify traffic to/from the remote site, log resource reqs
- Webscarab – intercept/modify requests, submission parameter fuzzing, spider
- Firebug – inexpect HTML elements, explore page script, modify the Dom, breakpoints
- URL Classification – Manual, Static, Low-interaction, high-interaction
- How to classify a URL without access to it's content. Lexical-based, host-based, graph-based