Web Security and the OWASP Top 10: The Big Picture

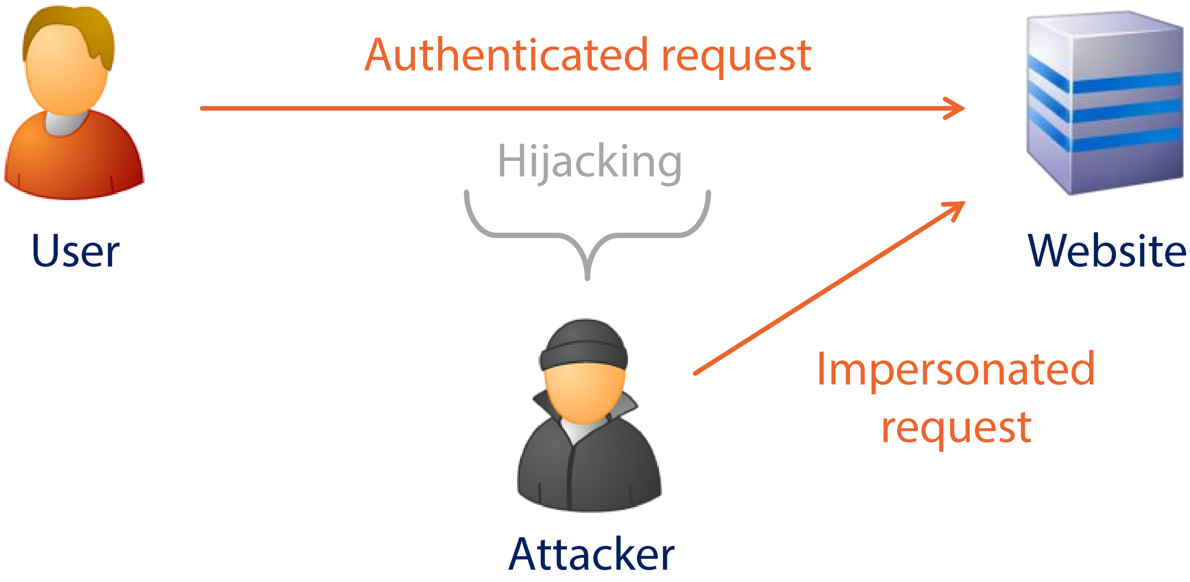
Broken Authentication and Session Management

Troy Hunt
troyhunt.com
@troyhunt

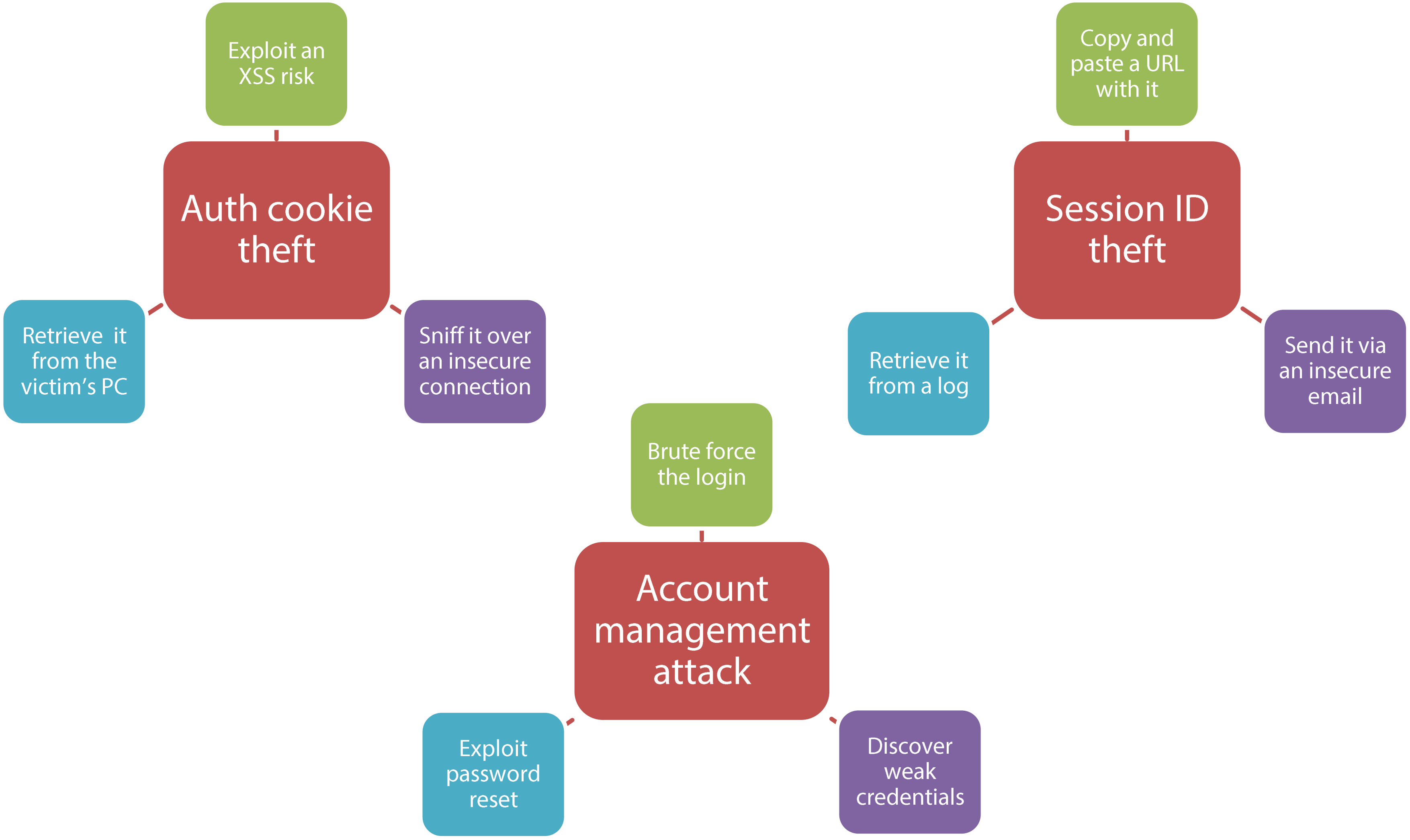
pluralsight
hardcore developer training

Broken Authentication & Session Management Overview

Attack Vectors	Security Weaknesses		Technical Impacts
Exploitability Average	Prevalence Widespread	Detectability Average	Impact Severe



Understanding Hijacking



Auth cookie theft

Exploit an XSS risk

Retrieve it from the victim's PC

Sniff it over an insecure connection

Session ID theft

Copy and paste a URL with it

Retrieve it from a log

Send it via an insecure email

Account management attack

Brute force the login

Exploit password reset

Discover weak credentials

Common Defences Against Broken Authentication

Protect the cookies

- Use the HttpOnly flag
- Make sure they're flagged as "Secure"

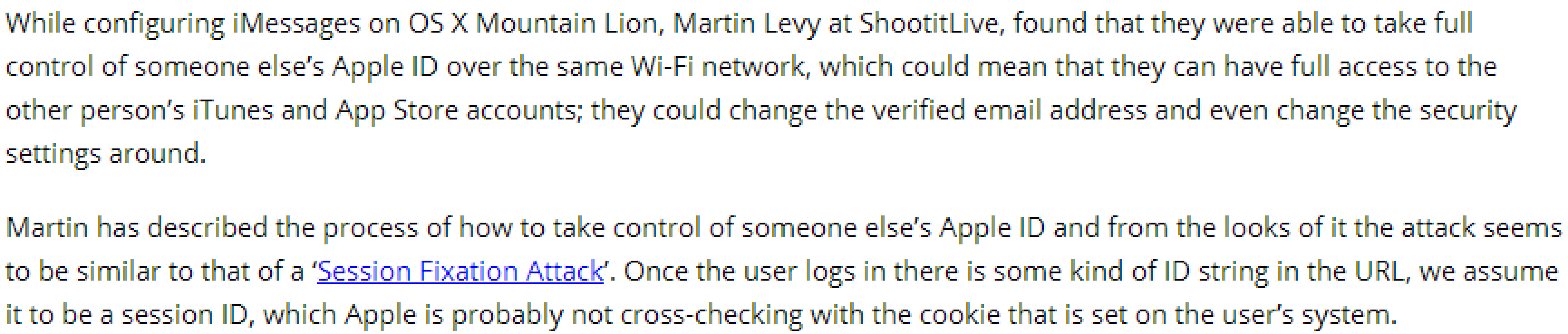
Decrease the window of risk

- Expire sessions quickly
- Re-challenge the user on key actions

Harden the account management

- Allow (and encourage) strong passwords
- Implement login rate limiting and lockouts

Broken Authentication in the Wild – Apple Hack



While configuring iMessages on OS X Mountain Lion, Martin Levy at ShootitLive, found that they were able to take full control of someone else's Apple ID over the same Wi-Fi network, which could mean that they can have full access to the other person's iTunes and App Store accounts; they could change the verified email address and even change the security settings around.

Martin has described the process of how to take control of someone else's Apple ID and from the looks of it the attack seems to be similar to that of a 'Session Fixation Attack'. Once the user logs in there is some kind of ID string in the URL, we assume it to be a session ID, which Apple is probably not cross-checking with the cookie that is set on the user's system.