CSF 434/534: Advanced Network and System Security

Week 02 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes

Dumpster Diving

Dumpster Diving

Dumpster Diving

- Mobile garbage bin
  - United States brand name "Dumpster"
  - Similar to a rubbish skip
- Important information thrown out with the trash
  - Thanks for bagging your garbage for me!
- Gather details that can be used for a different attack
  - Impersonate names, use phone numbers
- Timing is important
  - Just after end of month, end of quarter
  - Based on pickup schedule

Dumpster Diving

Is it legal to dive in a dumpster?

- I am not a lawyer.
- In the United States, it's legal
  - Unless there's a local restriction
- If it's in the trash, it's open season
  - Nobody owns it
- Dumpsters on private property or "No Trespassing" signs may be restricted
  - You can't break the law to get to the rubbish
- Questions? Talk to a legal professional.
- Secure your garbage
  - Fence and a lock

Dumpster Diving

Protect your rubbish

- Shred your documents
  - This will only go so far
  - Governments burn the good stuff
- Go look at your trash
  - What's in there?

Shoulder Surfing

Shoulder Surfing

Shoulder Surfing

- You have access to important information
  - Many people want to see
  - Curiosity, industrial espionage, competitive advantage
- This is surprisingly easy
  - Airports / Flights, hallway-facing monitors, coffee shops
- Surf from afar
  - Binoculars / Telescopes, webcam monitoring

Shoulder Surfing

Preventing shoulder surfing

- Control your input
  - Be aware of your surroundings
- Use privacy filters
  - It's amazing how well they work
- Keep your monitor out of sight
  - Away from windows and hallways
- Don't sit in front of me on your flight
  - I can't help myself

Hoaxes

Hoaxes

Computer hoaxes

- A threat that doesn't actually exist
  - But they seem like they COULD be real
- Still often consume lots of resources
  - Forwarded email messages, printed memorandums, wasted time
- Often an email
  - Or Facebook wall post, or tweet, or...
- Some hoaxes will take your money
  - But not through electronic means
- A hoax about a virus can waste as much time as a regular virus

Hoaxes

De-hoaxing

- It's the Internet. Believe no one.
  - Consider the source
- Cross reference
  - http://www.hoax-slayer.net
  - http://www.snopes.com
- Spam filters can help
- If it sounds too good to be true...
  - So many sad stories

Watering Hole Attacks

Watering Hole Attacks

Watering Hole Attack

- What if your network was really secure?
  - You didn't even plug in that USB key from the parking lot
- The bad guys can't get in
  - Not responding to phishing emails
  - Not opening any email attachments
- Have the mountain come to you
  - Go where the mountain hangs out
  - The watering hole
  - This requires a bit of research

Watering Hole Attacks

Executing the water hole attack

- Determine which website the victim group uses
  - Educated guess - Local coffee or sandwich shop
  - Industry-related sites
- Infect one of these third-party sites
  - Site vulnerability, email attachments
- Infect all visitors
  - But you're just looking for specific victims

Watering Hole Attacks

Watching the watering hole

- Defense-in-depth
  - Layered defense
  - It's never one thing
- Firewalls and IPS
  - Stop the network traffic before things get bad
- Anti-virus / Anti-malware signature updates
  - The Polish Financial Supervision Authority attack code was recognized and stopped by generic signatures in Symantec's anti-virus software

Principles of Social Engineering

Principles of Social Engineering

Effective social engineering

- Constantly changing
  - You never know what they'll use next
- May involve multiple people
  - And multiple organizations
  - There are ties connecting many organizations
- May be in person or electronic
  - Phone calls from aggressive "customers"
  - Emailed funeral notifications of a friend or association

Principles of Social Engineering

Social engineering principles

- Authority
  - The social engineer is in charge
  - I'm calling from the help desk/office of the CEO/police
- Intimidation
  - There will be bad things if you don't help
  - If you don't help me, the payroll checks won't be processed
- Consensus / social proof
  - Convince based on what's normally expected
  - Your co-worker Jill did this for me last week

Principles of Social Engineering

Social engineering principles (cont.)

- Scarcity
  - The situation will not be this way for long
  - Must make the change before time expires
- Urgency
  - Works alongside scarcity
  - Act quickly, don't think
- Familiarity / liking
  - Someone you know, we have common friends
- Trust
  - Someone who is safe
  - I'm from IT, and I'm here to help

Denial of Service

Denial of Service

Denial of Service

- Force a service to fail
  - Overload the service
- Take advantage of a design failure or vulnerability
  - Keep your systems patched!
- Cause a system to be unavailable
  - Competitive advantage
- Create a smokescreen for some other exploit
  - Precursor to a DNS spoofing attack
- Doesn't have to be complicated
  - Turn off the power

Denial of Service

A "friendly" DoS

- Unintentional DoSing
  - It's not always a ne'er-do-well
- Network DoS - Layer 2 loop without STP
- Bandwidth DoS - Downloading multi-gigabyte Linux distributions over a DSL line
- The water line breaks
  - Get a good shop vacuum

Denial of Service

Distributed Denial of Service (DDoS)

- Launch an army of computers to bring down a service
  - Use all the bandwidth or resources - traffic spike
- This is why the bad guys have botnets
  - Thousands or millions of computers at your command
  - At its peak, Zeus botnet infected over 3.6 million PCs
  - Coordinated attack
- Asymmetric threat
  - The attacker may have fewer resources than the victim

Denial of Service

DDoS amplification

- Turn your small attack into a big attack
  - Often reflected off another device or service
- An increasingly common DDoS technique
  - Turn Internet services against the victim
- Uses protocols with little (if any) authentication or checks
  - NTP, DNS, ICMP
  - A common example of protocol abuse

Man-in-the-middle

Man-in-the-middle

Man-in-the-middle

- How can a bad guy watch without you knowing?
  - Man-in-the-middle
- Redirects your traffic
  - Then passes it on to the destination
  - You never know your traffic was redirected
- ARP poisoning
  - ARP has no security

Man-in-the-middle

Man-in-the-browser

- What if the middleman was on the same computer as the victim?
  - The calls are coming from inside the browser!
  - Malware/Trojan does all of the proxy work
- Huge advantages for the bad guys
  - Relatively easy to proxy encrypted traffic
  - Everything looks normal to the victim
- The man-in-the-browser waits for you to login to your bank
  - And cleans you out

Buffer Overflows

Buffer Overflows

Buffer Overflows

- Overwriting a buffer of memory
  - Spills over into other memory areas
- Developers need to perform bounds checking
  - The bad guys spend a lot of time looking for openings
- Not a simple exploit
  - Takes time to avoid crashing things
  - Takes time to make it do what you want
- A really useful buffer overflow is repeatable
  - Which means that all systems are owned

Data Injection

Data Injection

Code Injection

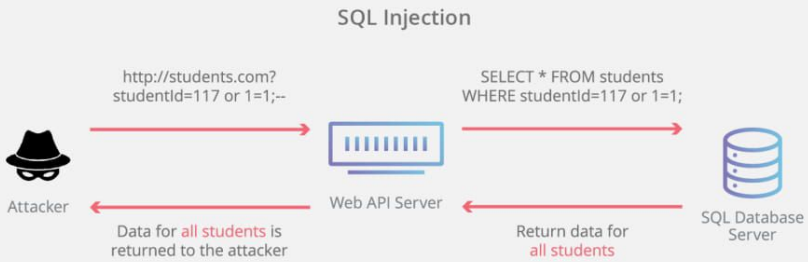
- Code injection
- Adding your own information into a data stream
- Enabled because of bad programming
- The application should properly handle input and output
- So many different data types
- HTML, SQL, XML, LDAP, etc.

Data Injection

SQL Injection

- SQL - Structured Query Language
  - The most common relational database management system language
- SQL Injection
  - Modifying SQL requests
  - Your application shouldn't really allow this

Data Injection



Data Injection

XML injection and LDAP injection

- XML - Extensible Markup Language
  - A set of rules for data transfer and storage XML injection
  - Modifying XML requests
  - A good application will validate
- LDAP - Lightweight Directory Access Protocol
  - Created by the telephone companies
  - Now used by almost everyone
- LDAP injection
  - Modify LDAP requests to manipulate application results

Cross-site Scripting - XSS

Cross-Site Scripting

Cross-Site Scripting

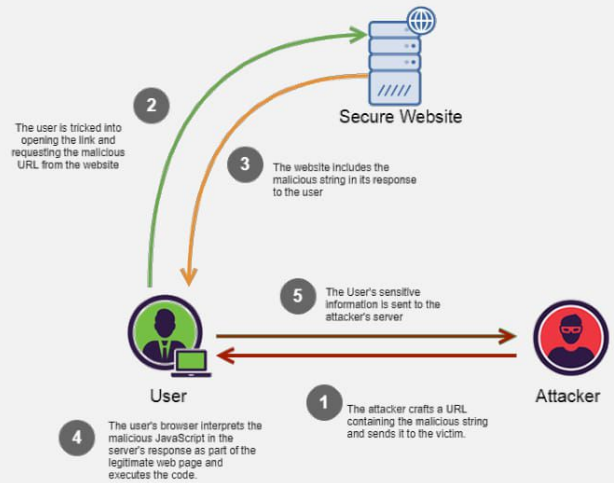
- XSS
  - Cascading Style Sheets (CSS) are something else entirely
- Originally called cross-site because of browser security flaws
  - Information from one site could be shared with another
- One of the most common web application development errors
  - Takes advantage of the trust a user has for a site
  - Complex and varied
- Malware that uses JavaScript
  - Do you allow scripts? Me too.

Cross-Site Scripting

Non-persistent (reflected) XSS attack

- Web site allows scripts to run in user input
  - Search box is a common source
- Bad guy emails a link that takes advantage of this vulnerability
  - Runs a script that sends credentials/session IDs/cookies to the bad guy
- Script embedded in URL executes in the victim's browser
  - As if it came from the server
- Bad guys uses credentials/session IDs/ cookies to steal victim's information without their knowledge
  - Very sneaky

Non-persistent (reflected) XSS attack

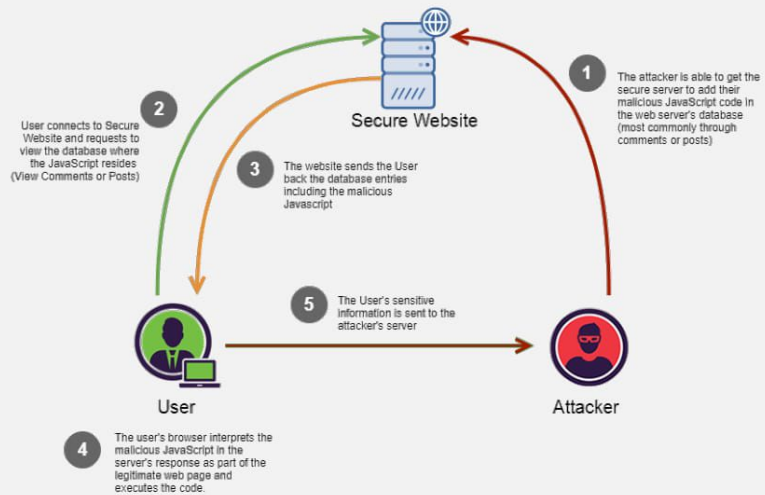


Cross-Site Scripting

Persistent (stored) XSS attack

- Bad guy posts a message to a social network
  - Includes the malicious payload
- It's now "persistent"
  - Everyone gets the payload
- No specific target
  - All viewers to the page
- For social networking, this can spread quickly
  - Everyone who views the message can have it posted to their page
  - Where someone else can view it and propagate it further...

Persistent (stored) XSS attack



Cross-Site Scripting

Protecting against XSS

- Be careful when clicking untrusted links
  - Never blindly click in your email inbox. Never.
- Consider disabling JavaScript
  - Or control with an extension
  - This offers limited protection
- Keep your browser and applications updated
  - Avoid the nasty browser vulnerabilities
- Validate input
  - Don't allow users to add their own scripts to an input field

Cross-site request forgery

Cross-site Request Forgery

Cross-site request forgery

- One-click attack, session riding
  - XFRF, CSRF (sea surf)
- Takes advantage of the trust that a web application has for the user
  - The web site trusts your browser
- Significant web application development oversight
  - The application should have anti-forgery techniques added
  - Usually a cryptographic token to prevent a forgery

CSF 434/534: Advanced Network and System Security

Week 02 - Review

"People always make the best exploits. I've never found it hard to hack most people. If you listen to them, watch them, their vulnerabilities are like a neon sign screwed into their heads."

– Elliot Alderson

Sources: Professor Messer's CompTIA SY0-501 Security+ Course Notes