Comp215: Web security

Dan S. Wallach (Rice University)

Copyright © 2015, Dan S. Wallach. All rights reserved.
What is security?
Security 101

The word “security” doesn’t mean very much, we need better terms

**Confidentiality**: keeping things secret (security for *who* can read *what*)

**Integrity**: keeping things from changing (security for *who* can write *what*)

**Availability**: keeping the system up and running (vs. “denial of service”)

Other terms that tend to come up:

- **Authentication**: figuring out *who* is there (for making access control decisions)
- **Trusted computing base**: all the code that needs to be “correct” for your security

  Smaller TCB = better chance at your security being strong
What exactly is “hacking”?  

“Hacking”: finding a way around the security features
What exactly is “hacking”?

“Hacking”: finding a way around the security features

Somebody Just Claimed a $1 Million Bounty for Hacking the iPhone

November 2, 2015 // 01:35 PM EST

Apple devices are widely considered extremely secure and hard to hack. But as the Internet adage says, everything can be hacked—even the new iPhone.

Over the weekend, somebody claimed the $1 million bounty set by the new startup Zerodium, according to its founder Chaouki Bekrar, a notorious merchant of unknown, or zero-day, vulnerabilities.

The challenge consisted of finding a way to remotely jailbreak a new iPhone or iPad running the latest version of Apple’s mobile operating system iOS (in this case iOS 9.1 and 9.2b), allowing the attacker to install any app he or she wants with full privileges. The initial exploit, according to the terms of the challenge, had to come through Safari, Chrome, or a text or multimedia message.

This essentially meant that a participant needed to find a series, or a chain, of unknown zero-day bugs, not just one, according to Patrick Wardle, a researcher that works at security firm Synack. For example, the Chinese white hat hacking team Pangu already found a way to jailbreak the new iPhone, but that method didn’t work remotely.
What exactly is “hacking”? By James O'Malley 4 days ago Mobile phones

A bug has been found in the Android version of Chrome that could potentially enable hackers to install and run whatever apps they like on your phone. The Register first reported that the bug was found in Chrome’s JavaScript v8 engine, meaning that the dodgy code could conceivably be loaded onto your phone if you visit a malicious website.

Worse still, as this bug was found in one of the newest Android handsets – Google’s own Nexus 6 (Project Fi version) – it suggests the problem could affect lots of phones. Which is bad.

The good news, however, is that the bug wasn’t discovered by evil hackers but by one of the good guys. Chinese hacker Guang Gong showcased the exploit at the MobilePwn2Own part of the Pwn2Own conference in Tokyo – a meeting of security experts who show off what they’ve discovered for the kudos.

In fact, Gong could even be in line for a cash reward from Google for finding the problem, as part of its Android Security Rewards Program. So there’s no need for him to become a super villain.
What exactly is "hacking"?

"Hacking": finding a way around the security features.

Major Android Chrome exploit could make millions of phones vulnerable

By James O'Malley, 4 days ago Mobile phones

At least the good guys found the problem first.

A bug has been found in the Android version of Chrome that could potentially enable hackers to install and run whatever apps they like on your phone.

The Register first reported that the bug was found in Chrome's JavaScript engine, meaning that the dodgy code could conceivably be loaded onto your phone if you visit a malicious website.

Worse still, as this bug was found in one of the newest Android handsets – Google's own Nexus 6 (Project Fi version) – it suggests the problem could affect lots of phones. Which is bad.

The good news, however, is that the bug wasn't discovered by evil hackers but by one of the good guys. Chinese hacker Guang Gong showcased the exploit at the MobilePwn2015 part of the Pwn2Con conference in Tokyo – a meeting of security experts who show off what they've discovered for the kudos.

In fact, Gong could even be in line for a cash reward from Google for finding the problem, as part of its Android Security Rewards Program, so there's no need for him to become a super villain.

Thousands of Java applications vulnerable to nine-month-old remote code execution exploit

A flaw in the Apache Commons Collections component puts Java application servers at risk of compromise.

Somebody Just Claimed a $1 Million Bounty for Hacking the iPhone

November 2, 2015 // 01:36 PM EST

Apple devices are widely considered extremely secure and hard to hack. But as the Internet adage says, everything can be hacked—even the new iPhone.

Over the weekend, somebody claimed the $1 million bounty set by the new startup Zerodium, according to its founder Chaouki Bekrar, a notorious merchant of unknown, or zero-day, vulnerabilities.

The challenge consisted of finding a way to remotely jailbreak a new iPhone or iPad running the latest version of Apple's mobile operating system iOS (in this case iOS 9.1 and 9.2b), allowing the attacker to install any app he or she wants with full privileges. The initial exploit, according to the terms of the challenge, had to come through Safari, Chrome, or a text or multimedia message.

This essentially meant that a participant needed to find a series, or a chain, of unknown zero-day bugs, not just one, according to Patrick Wardle, a researcher that works at security firm Synack. For example, the Chinese white hat hacking team Pangu already found a way to jailbreak the new iPhone, but that method didn't work remotely.
Who are the players in this game?

Different attacker “types”:
0: Script kiddies (i.e., no skills but can operate tools that others make)
1: Smart, motivated people with time on their hands (i.e., you)
2: Industrial research labs (i.e., you, plus more experience, plus a big budget)
3: Nation-state military/intel (i.e., research labs with no legal constraints)

Many other players:
Vendors, sometimes offering “bugs bounties” (worth $10k’s and more)
“Zero-day” brokers (offering even more money than the vendors)
Penetration testing consultancies (“pay us, we attack you!”)
Software static analysis tooling (“find your security bugs automatically!”)
   Plus “formal” analysis systems (“prove your system is secure!”)
Firewalls, intrusion detection systems (“build walls around your systems!”)
“Is iOS more safe than Android?”

We don’t know how to “measure” security; we can’t answer this question!

But we can compare security features across these systems

<table>
<thead>
<tr>
<th></th>
<th>iOS</th>
<th>Android</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>App isolation</strong></td>
<td>Unix process-based</td>
<td>Unix process-based</td>
</tr>
<tr>
<td><strong>App permissions</strong></td>
<td>Requested at time of use (originally, too many were granted by default)</td>
<td>Originally requested at install time, now also requested at time of use</td>
</tr>
<tr>
<td><strong>Malware detection</strong></td>
<td>In the app store (mysterious, undefined process)</td>
<td>In the app store (mysterious, undefined process)</td>
</tr>
<tr>
<td><strong>Likelihood of apps or system having exploitable bugs</strong></td>
<td>Higher than you’d think (Objective-C has buffer overflow issues)</td>
<td>Lower than you’d think (Java is mostly safe against buffer overflows)</td>
</tr>
</tbody>
</table>
Security is a process, not a destination

Microsoft, Once Infested With Security Flaws, Does an About-Face

By NICK WINGFIELD  NOV. 17, 2015

REMOND, Wash. — Microsoft was once the epitome of everything wrong with security in technology. Its products were so infested with vulnerabilities that the company’s co-founder, Bill Gates, once ordered all of Microsoft engineers to stop writing new code for a month and focus on fixing the bugs in software they had already built.

But in recent years, Microsoft has cleaned up its act, even impressing security specialists like Mikko Hypponen, the chief research officer for F-Secure, a Finnish security company, who used to cringe at Microsoft’s practices.
Security is a process, not a destination

Microsoft, Once Infested With Security Flaws, Does an About-Face

“It’s kind of like going to the gym every day,” said Mr. Nadella, who himself runs about three miles a day. “You can’t say I’m serious about security without exercising the regimen of keeping security top of mind every second, every hour of the day.”

... Microsoft estimates that it now spends more than $1 billion a year on security-related initiatives, including acquisitions. It acquired three security start-ups in the last year alone, and the number of security employees at the company increased 20 percent during that time.
Example: You’re an NSA researcher and you discover a remote exploit for Android phones. What do you do?
Option 1: Immediately report it to Google because it could impact U.S. citizens!
Option 2: Weaponize it so you can listen in on foreign leaders.
Example: You’re an NSA researcher and you discover a remote exploit for Android phones. What do you do?

Option 1: Immediately report it to Google because it could impact U.S. citizens!

Option 2: Weaponize it so you can listen in on foreign leaders.

*File Is Said to Confirm N.S.A. Spied on Merkel*

By MELISSA EDDY  JULY 1, 2013

BERLIN — More than three years ago, Chancellor Angela Merkel “professed to be at a loss” over the option of debt relief that would best stem the crisis in Greece. Yet even then, she feared that no amount of coaching from visiting experts would resolve the problems in Athens.

The chancellor’s musings over whether it would be better to allow private investors to incur losses on their bond holdings or to create a transfer union within the eurozone come from a protocol or memorandum dated 2011 that was said to have been intercepted by the United States’ National Security Agency.

Ms. Merkel’s conversation with an unidentified adviser, along with another document from the chancellor’s top aide for European affairs and a list of 69 telephone numbers said to belong to members of the German government and their aides, were made public Wednesday by the anti-secrecy group WikiLeaks.
NSA: Ethical? Rational? Legal?

Ethics: You need a framework to help decide what’s okay.

Hippocratic oath: “Do no harm!”
- But harms are relative. There’s no clear right answer.
- Consider “quarantines”: what happens to the infected people?

Rationality: This is where things get interesting.
The NSA has an “offensive” and a “defensive” mission.
They “need” vulnerabilities for the offensive missions.
“Weapons” have limited shelf-life. Single-use.

Legality: Way beyond the scope of Comp215.
Ethics for college students

For you, there’s zero ambiguity about this

**You cannot attack anything other than yourself**
Totally cool: Attack your own phone, attack your own browser, etc.
Somewhat cool: Attack your own Gmail account
  If you figure out how to “steal” credentials from yourself and then reuse them, that’s fine
  If you want to probe at Gmail and break into the whole thing, that’s going to land you in jail
Entirely uncool: Attack Owlspace, change your grades

**Standard operating procedure: “responsible disclosure”**
You first notify the vendor and given them an “appropriate” chance to respond
You then are free to go public and describe how it worked
  But if it’s going to take the vendor years to fix it, you might withhold critical details
Common vulnerability patterns
How about our RPN calculator?

Here's the JavaScript that adds text to the screen

```javascript
function printRaw(text) {
    var textBox = document.getElementById('textOutput'); // locate the textOutput widget on the screen
    textBox.innerHTML += text; // append the supplied text to the end of the widget
    textBox.scrollTop = textBox.scrollHeight; // scroll the page so we always see the newest stuff we just added
}
```

Q: What happens if the “text” has JavaScript in it?
A: Remote code injection

If “untrusted” content can make it back to the user (e.g., if this was Twitter or Facebook or whatever), then this could be exploitable

“Cross-site scripting” (XSS) attack
Live-coding demo time: XSS
What can XSS do?

Social networking: force users to post something, like something, etc. Instant viral spreading!

“Phishing”: pop up a dialog, “you need to enter your password again” Sometimes this happens anyway, so users won’t find it suspicious

When the attacker gets to run arbitrary code (JavaScript or otherwise), they can violate confidentiality, integrity, and availability.
How do you fix XSS?

Option 1: Escaping / filtering
The j2html library can do this - arbitrary text in a tag will be safely escaped
Putting it together - make sure that raw user input can’t flow into “innerHTML”

Option 2: Set rules in the browser that ban JavaScript
Mozilla’s “Content Security Policies” (now supported everywhere)
- Bans all inline JavaScript
- Bans JavaScript’s “eval” and other ways of generating dynamic code
- Sets rules about where JavaScript will be allowed from (i.e., <script> tags in the HTML header)

Lots of nitty gritty details to do this right
https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
More fun: cross-site request forgery (CSRF)

Let’s say you want to force me to buy your stuff on Amazon. What if there was an Amazon link to do it? One-click purchasing!

Attacker gets me to visit the attacker’s home page, forces a click
<img src="http://amazon.com/buy/my/thing/">

If you’re logged into Amazon, this will pass your cookies along, perform a HTTP “GET” request.
How do you fix CSRF?

Option 1: GET requests should have no side effects (no mutation!)
It’s much harder for an attacker to cause a PUT or POST request

Option 2: “Hidden form fields” or other secrets the attacker can’t see
Sent alongside XMLHttpRequests, etc.

Again, many subtleties to getting this right
https://www.owasp.org/index.php/CSRF_Prevention_Cheat_Sheet

Ever wonder why your bank’s website logs you out so fast?
They’re paranoid about this class of attack and they’re proactively trying to defeat it.
SQL injection attacks?

Similar to XSS: untrusted data being fed into a SQL (database) query
Similar solutions: use a library to help you build your SQL query, don’t just concatenate strings together.
Buffer overflow attacks?

**Programs in C and C++ use arrays in a dumb way**
It’s not a crash-bug to index beyond the end of an array! It works!
You’ll learn more about how call stacks work in Comp321, 412, 427, ...
In short: you can write binary code to the stack then force a jump to it.

**How do you fix it?**
Very expensive static analysis tools (Coverity, Fortify, etc.)
Don’t use C or C++ (Java programs don’t have this class of vulnerability)
More advanced tricks
  - fancy compilers, address space layout randomization, and much much more
More advanced stuff?

Security researchers keep inventing new kinds of attacks
Maybe it’s a new target to go after (e.g., self-driving cars)
Maybe it’s a new threat model (e.g., get somebody to do free computing for you)

They also keep inventing new general-purpose technologies
E.g.: “Two factor authentication” - getting fancier than passwords

And new ways of dealing with problems
E.g., Running in a virtual machine, to isolate the malware
Where's your attacker?
The attacker’s location matters

Web Service

Wherever

Firewall

Web client
The attacker’s location matters

Web Service

Wherever

Arbitrary location

Web client
The attacker’s location matters

Web Service

Co-resident in the cloud

Wherever

Firewall

Web client
The attacker’s location matters

Web Service

Wherever

“On path” in the network

Firewall

Web client
The attacker’s location matters

Behind the firewall

Web Service

Wherever

Web client
The attacker's location matters

Wherever - Web Service

On the target host - Web client
Examples where location matters

Co-resident (client or server)
Precise timing of network connections can leak crypto private keys!
  Taking large numbers to large powers takes a variable amount of time if you do it the obvious way.
  No “noise” from the network if you’re on the same machine.

On-path (network)
You can do a “man-in-the-middle” attack on the communications
  Passive surveillance
  Active blocking (e.g., China’s “Great Firewall”)
  “Racing” fraudulent responses back to the client

Behind the firewall
You can see open services that might not be meant for the public
  E.g., All Android apps have full network access; do you want an Android phone on your guest network?

More fun if you’re on the same WiFi segment
How does crypto help?
Crypto (ideal)

Passive man-in-the-middle adversaries learn nothing.
Active man-in-the-middle adversaries can drop or repeat traffic.
But they never learn anything beyond the network addresses of the endpoints.
The most they can accomplish is killing the connection, or traffic analysis.

Web client (with https) gains strong proof of the server’s identity.
Web server learns nothing about the client; typically do passwords, etc.
Crypto (in practice)

SSL (secure socket layer) / TLS (transport layer security) date to 1995
Lots of features to negotiate which specific cryptosystems, etc.
Version rollback attacks are significant
Modern practice: removing older crypto algorithms altogether

Especially “export modes” which were deliberately weakened cryptosystems

Dangerous implementation bugs (“Heartbleed” bug)

Weird questions about what capabilities the NSA (and friends) have
Example: OpenSSL Heartbleed bug

**HOW THE HEARTBLEED BUG WORKS:**

SERVER, ARE YOU STILL THERE? IF SO, REPLY "POTATO" (6 LETTERS).

User Meg wants these 6 letters: POTATO. User da wants pages about JLI games. Unlocking core records with master key 5138096573124.

POTATO

SERVER, ARE YOU STILL THERE? IF SO, REPLY "BIRD" (4 LETTERS).

User Meg wants these 5 letters: POTAT. User da wants pages about JLI games. Unlocking core records with master key 5138096573124.

POTATO
Example: OpenSSL Heartbleed bug

User Meg wants these 4 letters: BIRD. There are currently 500 connections open. User Brendan uploaded the file "Heartbleed exploit". User Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long. User Karen wants to see in car why. Note: Files for IP 375.381.30.17 are in /tmp/Files-3813. User Meg wants these 4 letters: BIRD. There are currently 500 connections open. User Brendan uploaded the file "Heartbleed exploit". User Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long. User Karen wants to see in car why. Note: Files for IP 375.381.30.17 are in /tmp/Files-3813.
Example: OpenSSL Heartbleed bug

User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long. User Karen wants to change account password to...
What are your attacker’s motives?
Different attackers have different goals

“Low-value targets” vs. “high-value targets”
There’s more value in hacking Obama’s Blackberry than your iPhone
If it costs $100k’s to get a previously unknown (“zero day”) vulnerability do you...

1) Use it to install malware on millions of computers, indiscriminately?
2) Use it to install malware on a small number of computers, because they’re important?

Most “botnet” attacks go after low-hanging fruit (e.g., unpatched Windows XP boxes), don’t use state-of-the-art methods.

Some attackers are incentivized to keep you happy!
Your machine is a platform to attack other machines.
Some attackers want to make you miserable

Several variations on this theme
You backup your computer, right?

It’s all about the money, of course
One by one, we’ve been making it harder for them to get paid

Notice how they don’t just ask for a credit card?
Nation-state attacks?

"Internet Giants Erect Barriers to Spy Agencies"

By DAVID E. SANGER and NICOLE PERLROTH  JUNE 6, 2014

Google servers in Douglas County, Ga. The company is encrypting more data as it moves between servers. (Condé Nast/Google)

MOUNTAIN VIEW, Calif. — Just down the road from Google’s main campus here, engineers for the company are accelerating what has become the newest arms race in modern technology: They are making it far more difficult — and far more expensive — for the National Security Agency and the intelligence arms of other governments around the world to pierce their systems.
Eric Grosse, Google’s security chief, suggested in an interview that the N.S.A.’s own behavior invited the new arms race.

“I am willing to help on the purely defensive side of things,” he said, referring to Washington’s efforts to enlist Silicon Valley in cybersecurity efforts. “But signals intercept is totally off the table,” he said, referring to national intelligence gathering.

“No hard feelings, but my job is to make their job hard,” he added.
An interesting trend...

**Old school (Windows 3.x, Windows 95, even Windows XP)**
User is running with full (root/admin) privileges, all the time
WinXP’s non-admin accounts were virtually unusable

**New school (Windows Vista and later, standard Unix and OS X)**
You have to type a password to “elevate” privileges
Default apps are limited in what they can do

**The latest (Android, iOS, Chromebook, others)**
You cannot elevate your privileges. You don’t have “root” on your phone.
  - Requires “jailbreaking”.
  - Jailbroken phones sometimes are missing features (e.g., disables Android Pay).

Harder for you to “steal” DRM-protected video.
Harder for malware to install itself.
Future trends...

Increasingly ambiguous attackers
Nation-states demand “backdoor” access to phones, demand local servers
Advertisers (and apps) want to profile you, monetize you

Internet reaching more and more devices, which aren’t secure (yet)
SCADA (industrial control systems)
“Internet of Things” (light bulbs, etc.)

Curiosity: Whose fault if an attacker uses a bug to steal your car?
Remotely unlock the doors, start the ignition, drive away with your car!
Who’s incentivized to fix the problem? Who’s skilled to fix it?

The manufacturer? The insurance company? The end user?
Arguably, this is nudging us away from car ownership, and toward “Zipcar” models.