Security

Brian Srivastava

Administrative note

- Where relevant the sources for these slides are in the powerpoint notes, which may not show up in PDF or in a Google document viewer

Security is More than Security

- Security is how you keep information private
- Security keeps systems available
- Security makes software reliable
- Security helps minimise waste and reduces cost

E.g. Hacking a Car

- http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
- (Watch the video during class)

Or a House

- https://www.cbc.ca/news/technology/smart-home-hack-marketplace-1.4837963

- (From Sept 2018)

Simplified Definitions

- Privacy: The ability to control information about yourself
- Availability: People can access your service
- Reliability: The service is running and can be available.

- (Availability vs. Reliability example: Not being able to connect to a service like Google is an availability problem for Google, even if that is because a network is unreliable, reliability is that the service is able to run and be connected to at all).

- Waste: Computers cost money to run. You don't want them doing someone else's calculations for them.

Security in Software Engineering

- Software is rarely designed with security first (even security software)
- Software has functionality and features which meet some customer desire, those come first, everything else, second.
- Given the choice customers want security, but over time customers want new features which may conflict with security, or may require a complete re-envisioning of what security means.
- That means general security (even in security software) is sometimes an afterthought to the core selling feature.

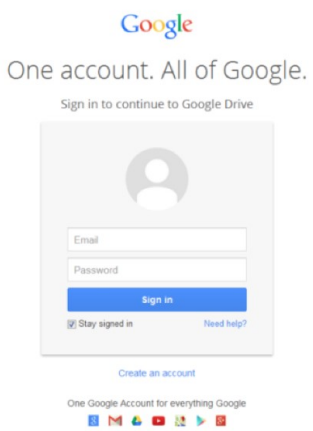
Software Engineering is Trade-offs

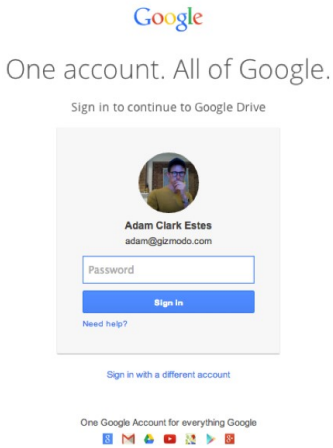
- Features can make security challenging
- E.g. Messaging. Do you end to end encrypt, but then what if people are sending illegal things or spam or the like, how do you check?
- Can you search for messages if the content is encrypted (or deleted)?
- How do you host pictures, and make sure only allowed people can view them, when the list of 'allowed' can be huge?
- How much data should companies retain on you, even when that provides benefits (e.g. real time traffic, search personalisation etc.)

Security is Confusing to End Users

- Most security problems happen because a person didn't understand what they were doing was dangerous/bad, or because functionality conflicted with security
- That 'person' isn't necessarily the victim of the security breach
- Most security jargon and presentation is confusing to users. There's no magic "Make this secure" button, and "private" means different things in different contexts
- (e.g. your student number is private… but obviously faculty can see it)

Phishing





Spam (Super Easy)

Facebook Oct 6 at 4:03 AM
To sljudd@yahoo.com

How are you sexy?

Its me Adriana you remember me from Facebook? I saw your pictures today and you're CUTE!

Imagine me giving you a massage and later a bj :) you would love it. Wouldn't you?

Get dirty with me Hun.

xoxo
Adriana

My Naughty Pictures-CLICK HERE

And Find Naughty Pictures Here: http://MYONLINECAMSPACE.COM
Or Even Beltter just text my cell :) (203) 5134882

Reply, **Reply All** or **Forward** | **More**

Note: That's not even my e-mail address

Facebook Phishing (actually legitimate)

[redacted] commented on a post you were tagged in.
Facebook <update+cge6gcgf@facebookmail.com>
Sent: Mon 8/15/2011 9:57 AM
To: [redacted]

facebook

Hi Ed,

[redacted] commented on a post you were tagged in.

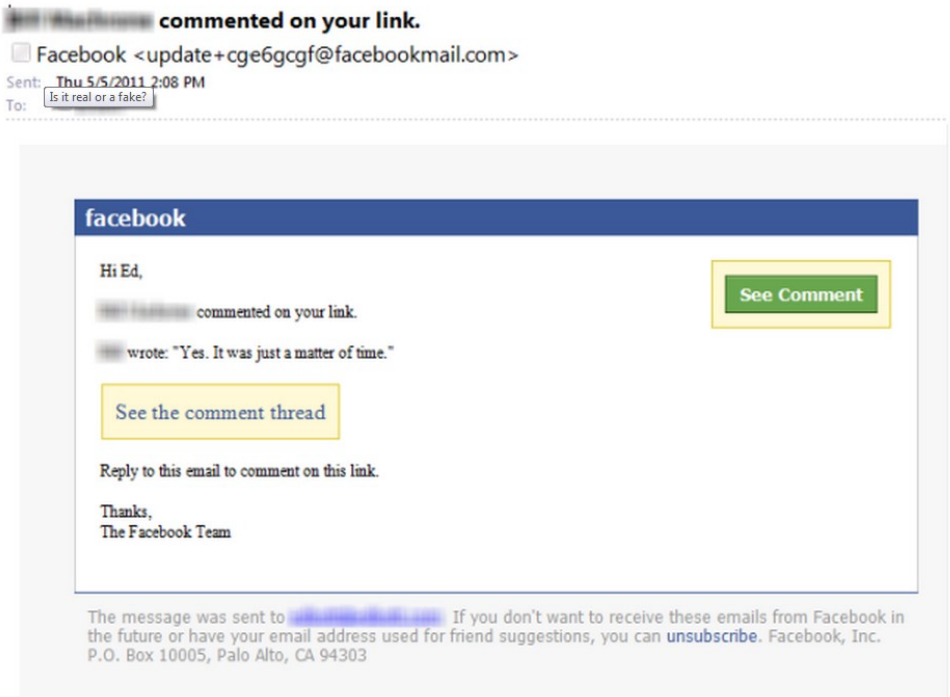
"Can we go right now? Huh? Please! <grin>"

To see the comment thread, follow the link below:
http://www.facebook.com/n/?[redacted]%2Fposts%2F10150285030850308&mid=4b33f0bG2243dc69G7625c46G5b&bcode=Op2xQh6S&n_m=[redacted]

Reply to this email to comment on this status.

Thanks,
The Facebook Team

The message was sent to [redacted]. If you don't want to receive these emails from Facebook in the future or have your email address used for friend suggestions, you can **unsubscribe**. Facebook, Inc. P.O. Box 10005, Palo Alto, CA 94303



Pups

- Pup is Microsoft speak for "Potentially Unwanted Program"
- These aren't strictly malware, but they're things that come bundled that you don't want. MacAfee Antivirus (now from Intel) anyone?
- These things are deliberately constructed to make users accidentally install them
- (Irony: MacAfee actually developed the 'Pup' terminology after a lawsuit over calling some program 'spyware')

Pups

Pups

- Search redirect (e.g. sending all your searches through some other company)
- Ad redirects
- Unwanted data gathering
- Packet sniffers, remote administration, Port Scanners, FTP servers, Keyloggers can all be both legitimate and illegitimate (hence 'Potentially unwanted')

Exclusive: Top 10 Flashlight Apps Are Stealing Your Data, Even Pics Off Your Phone

Snoopwall has just released a THREAT ASSESSMENT REPORT
Summarizing privacy and risk Analysis of top 10 Android flashlight Apps. According to Snoopwall, all of the top 10 apps are doing more than what consumers are expecting from a flashlight. For instance, the number 1 flashlight app for Android is the "Super Bright LED Flashlight". This app has between 100 million and 500 million installs worldwide. So what does the app actually have the ability to do?

- retrieve running apps
- modify or delete the contents of your USB storage
- test access to protected storage
- take pictures and videos
- view Wi-Fi connections
- read phone status and identity
- receive data from Internet
- control flashlight
- change system display settings
- modify system settings
- prevent device from sleeping
- view network connections
- full network access

Others like the Brightest Flashlight Free App, have been sued by the FTC . According to Snoopwall, *"But while the FTC.gov has gone after Flashlight Free App, it seems they are still at it*

These guys are only slightly misleading.

Apps get permission to do lots of stuff, even when they aren't being bad. But then if they decide to become bad, they have permission.

(Link to the original story in the PPT note)

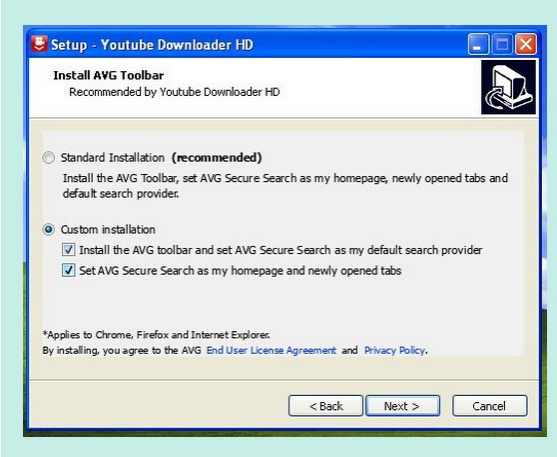
https://www.youtube.com/watch?v=-irnH0h3Wd8#t=111 (you don't need to watch this)

Notice the Tradeoff - Free

- People who write software need money
- So how are they getting paid?
- What do you actually pay Google for with Gmail or www.google.com/google.ca?

BS1

Youtube Downloader – Not a Surprise



Youtube downloader is not from Alphabet/Google (who own Youtube)
anyone who lets you download youtube videos is at least somewhat sketchy

Where We Have a Real Problem

- Java (from Oracle) is a massive legitimate piece of software that has huge money behind it
- So why are they trying to redirect your searches to “Ask”?

Slide 19

BS1 Brian Srivastava, 9/29/2018

Pups

- The trick with Pups is that you are agreeing to install them – Try not to. **They aren't required.**
- What they're doing isn't technically a virus (it's not trying to destroy data or completely hijack your machine).
- It's usually trying to monetize you.

Security is Subtle

- So last week(sept 2018) Facebook announced a breach of 50 million accounts, but you don't need to change your password and they don't know what data was breached…
- What does that even mean? As a user what (if anything) could you have done? (Other than not use _____ but this happens to everything)
- What does it mean when a company has encrypted your password?

Subtlety

- Authentication and Authorisation
- Encryption and Hashing (and Salting)
- End to end Encryption

Two Factor Authentication

- By now you should all know what two-factor authentication is even if you don’t have much that uses it
- It’s where you for example, have a random number device/app or get a text message in addition to using a password

WoW versus a Bank

- Your world of Warcraft account, if you have an authenticator is significantly more secure than your bank account
- Blizzard has support costs associated with fixing it
- Banks have insurance
- There are legal mandates banks have to follow… and usually they do a terrible job of it.

WoW authenticator

- Synchronized clocks with a pre-determined
- Random number generation

- If the authenticator system fails everything
- Protected by it goes to hell fast

- If WoW security fails it costs Blizzard money

- Keyloggers can compromise the system, but
- Users need to have gotten a keylogger somehow

RSA token

- RSA took a 10 million dollar payout from the NSA to deliberately weaken their Random number generator in their tokens
- (technically it was to use the NIST standard RNG that the NSA was on a standards committee for, and deliberately weakened).

Security: Trust

- Security is in part a trust relationship between the user and the product manufacturer
- You are trusting that they will give you something that reasonably secure.
- And that they have the resources and willingness to fix problems

	Vendor Name	Number of Products	Number of Vulnerabilities	#Vulnerabilities/#Products
1	Microsoft	484	5879	12
2	Oracle	533	5292	10
3	Apple	116	4272	37
4	IBM	972	4067	4
5	Google	69	3598	52
6	Cisco	2666	3568	1
7	Adobe	124	2723	22
8	Linux	17	2157	127
9	Mozilla	23	2048	89
10	Redhat	269	1957	7

- That #vul/#products is crazy
- Note that this chart is cumulative from 1998

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Linux Kernel	Linux	OS	2142
2	Mac Os X	Apple	OS	2084
3	Android	Google	OS	1926
4	Firefox	Mozilla	Application	1742
5	Debian Linux	Debian	OS	1723
6	Chrome	Google	Application	1546
7	Iphone Os	Apple	OS	1495
8	Ubuntu Linux	Canonical	OS	1145
9	Windows Server 2008	Microsoft	OS	1116
10	Flash Player	Adobe	Application	1062
11	Safari	Apple	Application	984
12	Windows 7	Microsoft	OS	974
13	Internet Explorer	Microsoft	Application	952
14	Acrobat	Adobe	Application	951

- Again, cumulative so don't read too much into it
- But that's a LOT of bugs over 20 years
- (Note that the same bug can occur in multiple versions of related software, so it gets counted multiple times)

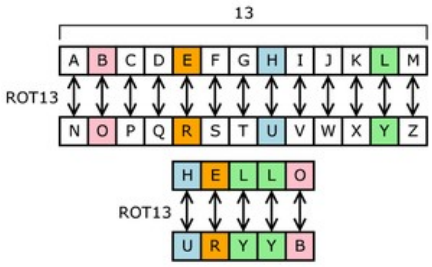
Security As a Technical Matter

- Encryption/Decryption
- Salting + Hashing
- Biometrics
- Tools

Encryption

- Take something, jumble it up, so that it's difficult to reconstruct
- Ideally, even if I know the algorithm but not the key this should be nearly impossible to do.
- Cryptographic algorithms are call cyphers – we will look at a super quick history

Substitution Cypher



- Rotate/replace/shift by some fixed unchanged amount
- E.g. on the right from Wikipedia is a 13 place rotation to the right (every letter is encrypted with the letter 13 places right of it in the alphabet)

Vigenère Cypher

- This was an extremely strong cypher until the advent of mechanical computers
- Take a sentence, and a vector. Shift the first letter by the first digit of the vector, the second letter by the second digit of the vector etc.

Vigenère Example

- Lets choose “vector” as our key (21,4,2,19,14,17)
- Note that “a” is 0, “z” 25

- Hereishow

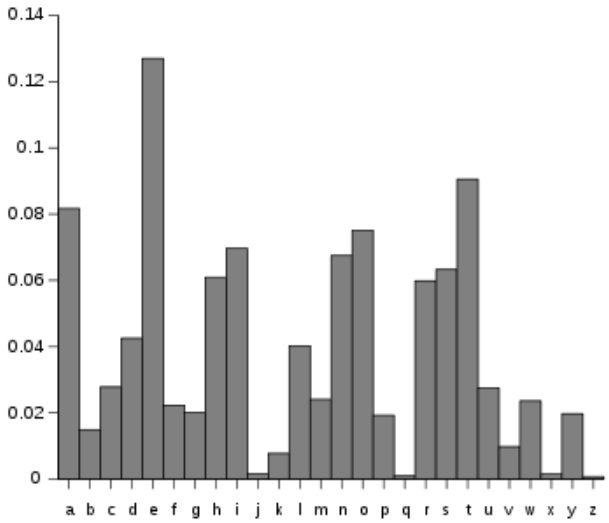
- CITXWJCSY

- (Shift the first letter by 21 places, the second 4, the third 2, the 4th 19 etc.)

End of Vigenere

- A statistical analysis of a language (which is really hard to do) will tell you about letter frequency
- From that you can reconstruct the vector, and the original message.
- A machine blindly encrypting can reveal the vector by inputting a long string of aaaaaaaaaaa if you manage to acquire a machine

Relative Frequency of Letters



Advanced Encryption

- Obviously we don't do that anymore
- The underlying mathematics is quite complicated (take 3rd year crypto from maths if you really want to learn)

Key Exchange

- One of the challenges with encryption is that you need a way to get the key to someone else, and if that key is intercepted the encryption is compromised
- The solution to this turns out to be math, but math which is difficult to do by hand, people understood most of these concepts a couple of hundred years ago, but many techniques simply didn't work when calculations were by hand.
- Key exchange is the idea that if I give you this key you can encrypt stuff for me, but only I can decrypt it (having the private key), and an observer can see all of our traffic but not know what the key actually is.

- https://www.youtube.com/watch?v=U62S8SchxX4

Prime numbers

- Without getting into the maths
- The trick to picking good keys is to pass around the product of two prime numbers, and then another prime number between them
- E.g. 7, and 33 (3x11, and 7 is between 3 and 11).
- Only for numbers that are many digits long

E.g.

- 261798184036870849 x 421538917598915629

- With the one in between as 316227766016837933

Modular Arithmetic

- Modulo arithmetic is like a clock. 8:00 + 5 = 1, 1 + 24 = 1. That sort of thing
- More formally, and what we're interested in is the modulo operation
- $2 \equiv 14(mod\ 12)$, that is to say (14 = 2 + 1*12)
- Another way to think of this is $\frac{14}{12} = \frac{12}{12} + \frac{2}{12}$, that is, 2 is the remainder when you divide 14/12 and you ignore the whole multiples of 12
- There are a number of rules of modular arithmetic… which we don't care about for this.

Modulo Arithmetic

- Lets broadcast 3 and 17, Alice and Bob have secret keys 15 and 13
- Alice computes 3^{15}mod17 = 6, and so Alice sends 6 to Bob.
- Bob computes 3^{13}mod 17 = 12 So sends 12 back to Alice.
- Alice computes 12^{15}mod17 = 10
- Bob computes 6^{13}mod 17 = 10
- Alice and Bob now have a shared key of 10
- (These keys are short, but in the real world 17 would have be chosen as a product of two prime numbers and the secret keys would be 64 bits)

- (3^15 = 14 348 907, 6^13 = 13 060 694 016, 12^15 = 15 407 021 574 586 368)
- Notice that computing 15407021574586368/17 is… not exceptionally easy by hand.
- Math problem

Another Key Exchange with Modular Arithmetic

- Everyone sees two numbers: 23 and 5
- Alice generates a secret key: 4
- Alice computes 5^4 mod 23 (which happens to equal 4) and sends 4 to bob
- Bob generates secret key 3
- Bob computes 5^3 mod 23 = 10, and sends 10 to alice
- Alice computes 10^4 mod 23 = 18
- Bob computes 4^3 mod 23 = 18
- 18 is our secret key

Factorization

- What prime numbers multiply to:
- 6
- 15
- 77
- 323
- 1517

- Factoring the product of 2 (or 3) very large primes is extremely hard computationally

Factorization Continued

- That it is hard to do prime factorization for two large primes multiplied together is the basis of computer security
- If that turns out to not be true we are all screwed.
- * Screwed is a totally serious technical term. Honestly. Really. Definitely.

Primitive root Modulo N

- https://en.wikipedia.org/wiki/Primitive_root_modulo_n

Primeness

- Up until 2005 it was assumed that proving something was prime was hard…
- Then some Indian guys had a crack at it..
- The AKS primality test is a fast test of primeness

Biometrics

- Biometric devices use some physical property for authentication
- Fingerprints, retina scans, images of faces etc.
- Most of these systems are pretty terrible at actually working.

Biometrics

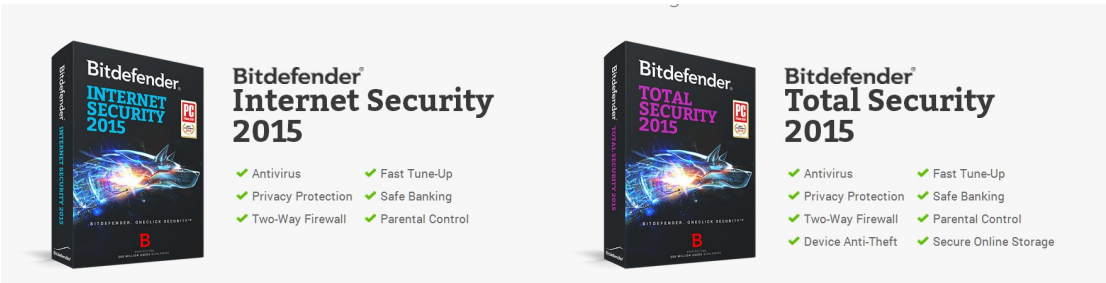
- If your password gets compromised (someone steals it) you can make a new one
- Can you change your fingerprint?
- What if you involuntarily change your fingerprint (or lose your finger)
- Even though we see a lot of use for biometrics in security, biometrics are basically usernames, not passwords.

Tools

- Firewalls
- Anti Virus/Anti Rootkit
- Anti Spyware
- (all 3: Security Suite)
- Ad blockers (including host file based blocking)
- VPNs

Packaged security tools

Different versions contain different stuff, but most ‘security’ programs have several options



While Bit Defender is very well rated, don’t take this as an endorsement of their products

Compare Products

	Norton Security	Norton Security with Backup
Offers one service to protect your devices	•	•
Provides protection against viruses, spyware, malware and other online attacks	•	•
Maintains your privacy, no matter what device you're using	•	•
Avoids unsafe websites and suspicious downloads	•	•
Allows you to move protection from one device to another	•	•
Lets you add more protection as you get more devices	•	•
Easily locates lost or stolen smartphones and tablets	•	•
Automatically backs up 25 GB worth of photos, movies and files you choose from your PC to our secured online storage		•
Delivers enough flexibility to protect your entire family's digital life		•
	$79.99 per year	$89.99 per year Learn More

	File Detection Test March 2015	Proactive Test March 2015	Performance Test May 2015	Real-World Protection Test (March-June 2015)	Malware Removal Test (March-September 2015)	File Detection Test September 2015	Performance Test October 2015	Real-World Protection Test (August-November 2015)
Kaspersky Lab	***	***	***	***	***	***	***	***
Bitdefender	***	***	***	***	***	***	***	***
ESET	**	***	***	***	**	***	***	***
AVIRA	**		***	***	***	***	***	***
Emsisoft	**	*	***	**	**	***	***	***
eScan	**	**	***	**	**	***	***	**
Avast	*	tested	***	***	***	**	***	***
AVG	*		***	***	***	*	***	***
Tencent	**		***	***		**	***	***
Fortinet	***	*	**	***	**	**	*	**
Sophos	**		***	**	**	**	***	**
BullGuard	**	**	**	**	**	***	**	*
F-Secure	**	**	**	**	**	**	**	**
Panda	**		**	**	**	***	**	**
McAfee	***		***	*		**	***	**
Lavasoft	**	tested	**	*	**	***	**	*
Trend Micro	*		**	**		**	**	**
QuickHeal	**		*	**		**	**	*
Microsoft	tested	*	**	*	**	tested	**	*
Baidu	tested		***	**		tested		**
Vipre	*	tested	*	tested	*	**	*	tested

AV Comparison

	Malware Protection Test March 2016	Performance Test May 2016	Real-World Protection Test February - June 2016	Malware Removal Test March - September 2016	Malware Protection Test September 2016	Performance Test October 2016	Real-World Protection July - November 2016
Bitdefender	★★★	★★★	★★★	★★★	★★★	★★★	★★★
Kaspersky Lab	★★★	★★★	★★★	★★★	★★★	★★★	★★★
VIPRE	★★★	★★	★★★	★★★	★★★	★★★	★★★
Avira	★★★	★★★	★★★	★★	★★	★★★	★★★
Avast	★★	★★	★★★	★★	★★★	★★★	★★★
AVG	★★	★★★	★★★	★★	★★★	★★★	★★★
Tencent	★★★	★★★	★★★	★★★	★★	★★	★★★
eScan	★★★	★★★	★★	★★★	★★★	★★★	★
ESET	★	★★★	★★	★★	★★★	★★★	★★★
F-Secure	★★★	★★	★★	★★	★★	★★★	★★
Emsisoft	★★	★★★	★	★★	★★★	★★	★★★
BullGuard	★★★	★	★★	★★	★★★	★★★	★★
Panda	★★★	★★	★★★		★★	★★★	★★★
McAfee	★	★★★	★		★★★	★★★	★★★
Trend Micro	★★	★	★★	★★	★	★★	★★★
Seqrite	★★	★★★	TESTED	★	★★★	★★★	★
Symantec	TESTED	★★★	★★★		TESTED	★★★	★★
Adaware	★★	★	★★	★★	★★★	★	TESTED
Fortinet	TESTED	★★	★★	★	★	★★	★★
CrowdStrike	TESTED	★★	★★		TESTED	★★	★★
Microsoft	★	★	★★	★	TESTED	★	★★

★★★ Advanced+
★★ Advanced
★ Standard

An empty box indicates that the vendor did not participate in the options

Firewall

- Firewalls block remote connections to or from your computer
- The basically have a giant whitelist of stuff that's allowed. And block everything else.

Anti Virus/Rootkit/Spyware

- These programs scan what is on your computer for known threats
- Then try and fix the problem (if that's possible)
- Usually you want at least one running in real time, in case you accidentally download or run something you shouldn't.

Spyware

- Spyware is more about Pups and tracking and stuff that is legal but that you probably don't want on a home machine.
- For that you may need a second tool
- See PPTx note for some discussion

Some common big names

- Microsoft Defender/security essentials – free
- Bitdefender – very good, expensive
- Kaspersky – very good, affordable. Russian.
- Norton – Slow, expensive, only good in some cases, but popular for corporate

More

- AVIRA – German, decent
- Malware Bytes – decent free version
- Avast – decent free version
- AVG – decent free version
- Lesser Known or not as popular
- Spybot, Avira, Comodo, Panda, Ad-Aware

What Does Sri Use?

- Right now I have bit defender on my home computers

But I have a Mac!

- Mac's are about 12% of the overall desktop market, which makes them a much smaller target
- But they are also much more vulnerable, and people don't typically run security tools on them.

Apple

- Some very good ideas in the latest versions – easy encryption (in case your device is stolen)
- Windows supports more robust full encryption, but only in expensive versions, and it's a pain to configure

New Apple malware is undetectable, unstoppable, and can infect any Thunderbolt-equipped device

By Joel Hruska on January 8, 2015 at 9:00 am | 111 Comments

Share This Article

Apple products have long enjoyed a reputation for superior security in relation to Windows systems, but a new proof-of-concept malware delivery method could put a serious dent in that reputation. The exploit, dubbed Thunderstrike, currently can't be detected or removed by any known process without using specialized hardware. Security researcher Trammell Hudson has demonstrated how to use a Thunderbolt peripheral to load what he's calling a "bootkit" via the device's Option ROM.

The Sad Truth – It's Apps Not OS's

- Regardless of your OS, If you run Java, Flash or any of the browsers there are problems
- More of our lives are run through Browsers and mobile phones – particularly Android which is really bad about actually getting updates into the hands of users (security fixes that never make it to devices are useless)

Open Source?

- Linux – notably Ubuntu can be very secure (though not in 2016 apparently, see previous slides). But it's compatibility is limited (games and office tools). And Ubuntu is the most usable linux distro.

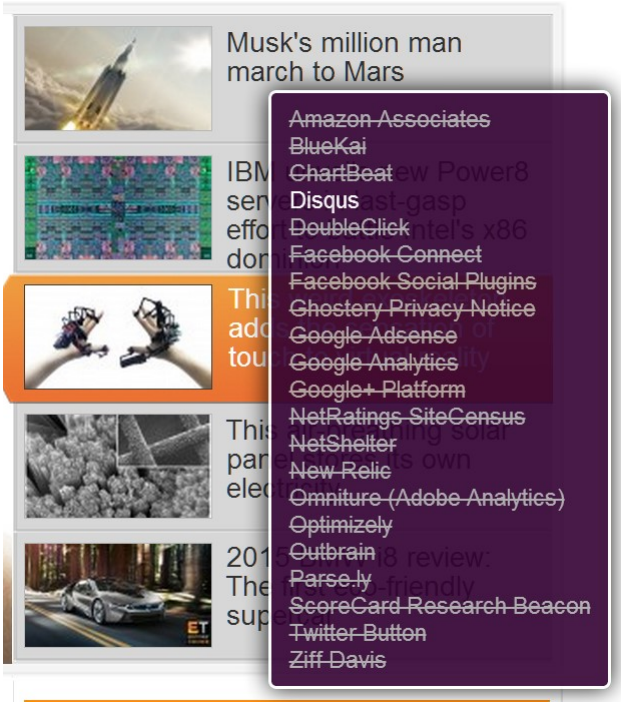
- Open source doesn't necessarily translate into security

Heartbleed, Shellshock

- Two major exploits last in 2014
- Heatbleed was a bug in OpenSSL (an implementation of the thing makes HTTPS work)
- Shellshock (aka Bashdoor) – serious problem with every Linux/OSX computer that was acting as a server
- Both open source, both written by smart people.

Ad Blockers

- Tools that block ads, or trackers for ads
- The most common is, well, Adblock plus… which is for all the major browsers
- Adblock plus allows big companies to buy their way past the blocking
- I'm Partial to Ghostery + ublock origin
- (make sure you turn them on in incognito too)



Passwords, Some More Details

- We should delve a bit more into Passwords

- One of the very interesting elements of computer security is that much of it is maths, but there's a bit part of human psychology to get people to use the math/protocols etc. well.

Pwd complexity

- The key to password strength is to understand the search space.
- Knowing nothing, how hard is it to find these?
- Q6FMmrbqjpzeQNQqSLkGfv2A
- 123456
- Password
- Password_For_1_Website

Complexity

- Lowercase characters 26
- Uppercase - another 26
- Symbols (depends how many are valid) ~20
- Numbers – 10
- Pwd search space is
- $(26 + 26 + 20 + 10)^{Length}$
- But only if you use something from everywhere

Passwords

- People have too many passwords, and have a habit of picking them with semi-regular patterns
- Turns out that makes it MUCH easier to hack them brute force (not all passwords are equally likely, start by trying ones that are likely)
- (So alternatives are needed to prevent brute force attempts etc.)

Search Order

- Computer science spends a lot of time on search and sorting
- Practical cryptanalysis is figuring out how to sort the possible search space so you search likely passwords first, and unlikely (pure random pwds) last.

Dictionaries

- 123456 and Password are very common passwords
- So they are searched first, because everyone knows that

20 most Common Passwords

- 123456
- 123456789
- qwerty
- 12345678
- 111111
- 1234567890
- 1234567
- password
- 123123
- 987654321
- qwertyuiop
- mynoob
- 123321
- 666666
- 18atcskd2w
- 7777777
- 1q2w3e4r
- 654321
- 555555
- 3rjs1la7qe

Salting a Password

- Real security tries to combine your password with a 1 time code
- Password_Oct_8_2015 (or more sophisticated) and encrypt that
- But doing this is still a new technique, and lots of companies screw it up
- It only protects against password discovery if the encrypted passwords are stolen.

- (This way if two people pick the same password they won't be the same in the database, because the salt will alter the PWD. Even if someone knows the salt, they still need to brute force the rest of the PWD)

"Dictionary" attacks

- Hackers build dictionaries of possible passwords
- These include everything in a regular dictionary
- And 2 and sometimes 3 word phrases
- And known passwords from previous hacks
- (Remember that list of 20 most common passwords from a few slides ago?)

- If your password has been hacked before it will be in a 'dictionary'

Rainbow Tables

- Rainbow tables are just *all* possible outputs from all possible inputs
- Only work when storage is cheap.
- Lets say I develop a hash (1-way function) to apply to a password.
- If I have a table of all possible input-output pairs I can just look up the password.

MD5 Example

Value	The MD5 of that Value
1	c4ca4238a0b923820dcc509a6f75849b
2	c81e728d9d4c2f636f067f89cc14862c
3	eccbc87e4b5ce2fe28308fd9f2a7baf3
4	a87ff679a2f3e71d9181a67b7542122c
5	e4da3b7fbbce2345d7772b0674a318d5
6	1679091c5a880faf6fb5e6087eb1b2dc
7	8f14e45fceea167a5a36dedd4bea2543
8	c9f0f895fb98ab9159f51fd0297e236d
9	45c48cce2e2d7fbdea1afc51c7c6ad26
10	d3d9446802a44259755d38e6d163e820

Obviously you aren't supposed to remember any of this

The point is to illustrate what a Rainbow Table does.

Keyloggers and Passwords

- Lets say I use
- Q6FMmrbqjpzeQNQqSLkGfv2A
- As a password.
- That's essentially impossible to guess. And impossible to remember.
- But a keylogger doesn't care.

Designing Strong Passwords

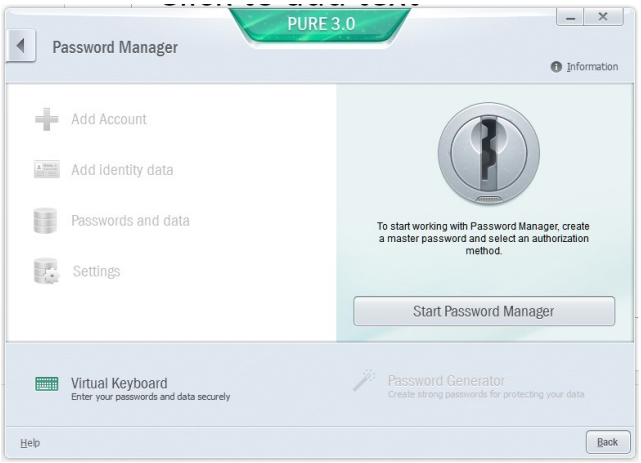
- Two theories, one is long random ones the other is pass phrases
- "These days, use pass phrases" is an example of a pass phrase. "I have 1_Totally$awesome*PassPhrase" is strong but difficult to remember.
- "Jamie, when are you coming over to play Portal2?" is easier to remember.

- (Note: It's been 4 years of this slide, she still hasn't played portal 2)

But!

- You will find that some places (including banks) don't support long passwords, or don't support special characters.
- This is where you need a password manager.
- My PWD manager has 125 entries. I cannot possibly remember all of those.

Password Manager



Passwords and Mobile

- What happens if your phone is stolen?
- How much can you log into, and how much are you logged into with your mobile?
- Lots of Password Managers work on mobile

Security Questions

- Security questions are usually weakly enforced
- What University did your mother attend: "Trent" and "trent" would both be valid answers.
- They are often reused in many websites
- In many cases they, and answers are stored in plaintext, so… don't put your pwd as a hint
- Many security questions rely on demographic information (Grandfather middle name on mother's side) which is easy to get. This makes public figures vulnerable to attacks

Points of Failure and Attack Vectors

- User Security is a balance between convenience, points of failure, and expected attack vectors.
- Your GF/BF/Wife/Husband/Parents/Children are attack vectors
- But so are random hackers on the web

- Password managers, and writing down passwords make you vulnerable to in person attacks but safer from distant ones.

What if your (Online) Password Manager is hacked?

- Then… you're in big trouble
- And they are, understandably, big targets
- Small PWD manager companies are smaller targets, but have less to invest in security.

- As an end user there's only so much you can do

LastPass … Ooops

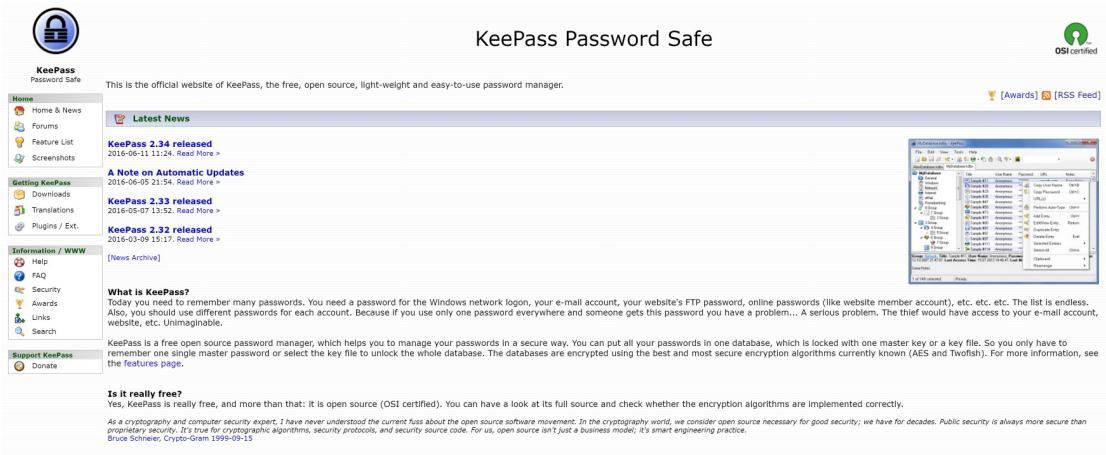
LastPass Hacked, Change Your Master Password Now

Eric Ravenscraft
Filed to: HACKED 6/15/15 12:30pm

204,892 15

Bad news first, folks. LastPass, our favorite password manager (and yours) has been hacked. It's time to change your master password. The good news is, the passwords you have saved for other sites should be safe.

Enter KeePass



http://keepass.info/

KeePass

- Works based on a file that is strongly encrypted (even if someone gets into your Google drive they don't get your passwords)
- Passwords can be pasted into pwd fields to dodge keyloggers
- It can be used to generate unique strong passwords for every website

Security As a Policy

- Social Engineering
- Rules and Procedures

User behaviour: Social Engineering

- This is the psychology question
- How many people would tell me their password for a chocolate bar? And those sorts of questions

User Behaviour 5 common tricks (These are Social Engineering Attacks)

- Familiarity - (Act like you belong)
- Hostile situation – (Act Angry)
- Gather information – (Trust/threaten)
- Learn body Language – (Be attractive, learn to read signs)
- Become an employee – (real or fake)

Finding Vulnerabilities

searchcode | if(version,startswith("windows 9") | search

About 4,342 results

WindowsAttachProvider.java in jdk-6 (https://bitbucket.org/nkabir/jdk-6)

```
40.         String os = System.getProperty("os.name");
41.         if (os.startsWith("Windows 9") || os.equals("Windows Me")) {
42.             throw new RuntimeException(
```

MaxPathLength.java in ManagedRuntimeInitiative (git://github.com/GregBowyer/ManagedRuntimeInitiative.git) Show 2 matches

```
46.             isWindows = true;
47.             if (osName.startsWith("Windows 9") ||
48.                 osName.startsWith("Windows Me"))
```

MaxPathLength.java in java-1.7.0-openjdk (git://pkgs.fedoraproject.org/java-1.7.0-openjdk) Show 2 matches

```
46.             isWindows = true;
47.             if (osName.startsWith("Windows 9") ||
48.                 osName.startsWith("Windows Me"))
```

Disclosure

- When you discover a problem you want to do something with that information
- Disclose publicly – and make systems insecure
- Tell the company, and give them time to fix it
- Sell it to a government agency
- (Or you can just exploit it and be a criminal)

Google Vs Microsoft

- Back in January 2015 Google released an exploit after their 90 day window, MS was patching a fix on day 92.
- MS has patch Tuesdays
- Even when Google patches things there's no guarantee your mobile carrier pushes it out to your phone

Politics (As part of Research In Security)

- Standards bodies decide on what is considered good practices and technology
- Researchers sit on standards bodies
- So does the NSA (NIST is the standards body in the US)

NIST, the NSA and Security

- This creates an odd problem
- The NSA is trying to break encryption to spy on things
- NIST is trying to Secure things
- The NSA sits on the Cryptography oversight board of NIST

The NSA the good

- The NSA has some of the best cryptographers in the world
- Most of the time they suggest sensible things
- They have more experience than anyone at hacking and defending against hacks

The Naughty NSA

- In the 1970's the NSA put a deliberately short key on an otherwise good cypher (DES)
- In 2003:

```
if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
        retval = -EINVAL;
```

- In 2004: Dual_EC_DRBG, weak RNG, and the Payoff of RSA to use it*

Note: Disclosure about Freedom to Tinker. Also, * - oddly, they were caught doing this at the time.