Home Cybersecurity

Steven M. Bellovin
https://www.cs.columbia.edu/~smb

About Me

- I started learning programming in 1965
- I caught my first hackers around 1971
- Cybersecurity became my primary research interest around 1987
- I co-authored the first-ever book on Internet security, back in 1994
- I've worked in industry, academe, and government
- (If you care, you can find more about me online)

Disclaimers

- I’m not going to recommend specific products
  - They change all the time
  - It’s been a *long* time since I’ve used Windows
- Some of what I say may contradict what you read in the popular press or see on TV. Generally, that’s because they’re behind the times.
  - Little, if anything, of what I say would be controversial to other experts

It’s Not Your Fault

- No matter how careful you are, sometimes scammers and hackers can evade your defenses
- There are successful bank robberies
- Some spies are never caught
- In the computer world, sometimes attackers use “zero days”—attacks that software vendors don’t know of, and hence can’t protect you against
- (I suspect that I was successfully hacked about 3 years ago)
- The *purpose* of a computer is to be used, not to be turned off in fear

CS@CU

Two Terms

- Threat model
- Attack surface

Threat Model

- Who is your enemy? What are their powers?
- For most of us, it's someone who wants our money
  - Second choice: they want to use our computers for spamming, cryptocurrency calculations, etc.
- If you think you're likely to be targeted by foreign intelligence agencies or industrial espionage hackers—well, that's a different talk; this is just a starting point and you need to do more

Threat Model: Stealing a Bike

(Why Do I Use a Mac?)

Do I think it's more secure?

- Macs are probably not inherently more secure than Windows (though Microsoft seems to have slipped badly of late)
- However—I *personally* find myself more productive on Macs, and I find MacOS more pleasant to use
- *My personal threat model does not include intelligence agencies, industrial espionage, etc.*
  - Ordinary security precautions are good enough
- Macs *may* be more secure in practice, because attacks will often target more popular platforms, but that isn't an inherent property
  - Remember: The purpose of a computer is to be used, not to be turned off in fear

Attack Surface

How Many Ways Can you be Attacked?

- Think building security
  - The front door
  - Garage doors
  - Ground floor windows
  - Someone using an extensible ladder to get into an upper floor window (the Louvre)
  - Someone rappelling down from an upper floor via a rope (American Museum of Natural History, 1964)
- Note how this interacts with threat models!

Attacker Techniques

- Buggy software
- Stolen credentials, e.g., passwords
- “Social engineering” (tricking you)
- Some combination of the above

Software

Buggy Software

- All software has bugs—*all* of it
- Sometimes, these bugs are serious enough that they let attackers in
- No one—and I mean *no one*—can write all of their own software (and if they tried, it would probably be buggy, too)
- Major vendors use all sorts of sophisticated techniques to find bugs before they ship their code—and they never completely succeed
- So what do we do?

Defending Against Software Bugs

- Most important: apply all vendor patches
  - It's ok to wait a few days (but rarely more), because sometimes the updates are so buggy that they make your device useless
  - Corollary: when a device is so old that it no longer receives vendor security updates, it's time to replace it. Yes, that hurts.
- Don't install software from shady places (AKA "don't walk down deserted alleys in bad neighborhoods")
- Don't blithely click through warning messages

Software Attack Surface

What Software Is the Most Vulnerable?

- Your email program—anyone can send nasty stuff to it
- Your browser
  - Visiting sketchy sites is bad, but attackers can and do buy ad space on legitimate sites to exploit bugs in your browser or to trick ("social engineer") you
  - (Your instincts may be wrong—one study found that religious sites were more likely to host nasty stuff ("malware") than porn sites)
- Your text message program
- Perhaps your word processor or PDF viewer, if people send you documents
- More complex stuff (*maybe!*), if you use your laptop in coffee shops or other public hotspots

CS@CU

And?

- You have to have a mailer, web browser, word processor, etc.
  - Again: The purpose of a computer is to be used, not to be turned off in fear
- If you're sent a document that you have to read but you're suspicious of, open it on a tablet if you have one, or on Google Docs if you know how to use it
  - Tablets are much more secure than laptops or desktops—we've learned a lot more about security since Windows and MacOS were developed
  - Google is *really* good at security—and if there's a failure, it infects them, not you, but that's a risk they've chosen to take
- All other things being equal, newer hardware and software are more secure

Antivirus Software

- Expert opinion on antivirus software is mixed
- AV software itself has a large attack surface—and it's complex software, which means it's buggy
- Modern operating systems have very strong built-in defenses
- High-end attackers can probably bypass those defenses, but in general AV software can only detect *known* viruses and malware, which a high-end attacker won't use against a hardened target
  - Corollary: you really do have to keep paying the subscription fee for your AV software, or it won't pick up newer threats
- Run AV if you want to or are required to, but don't feel bad if you don't or can't
  - But do run a modern OS if you can

If You Can’t Upgrade Your Devices…

- If you can, use cloud-based services like Google’s gmail
  - You’ve outsourced your risk
- Do as much as you can via your web browser, and try to keep it up to date
- Google’s Chrome browser is very secure, and they update it automatically (because it also has bugs)
  - (I don’t use Chrome because I’m also a privacy fanatic…)
- Pay more attention to the next two parts of this talk
- Example: an older car doesn’t have all of the safety features of newer ones, but it’s still completely serviceable

Passwords and Authentication

Passwords

- We've all experienced the rules for strong passwords: mix in upper case letters, lower case letters, digits, special characters, two characters from a 19th century novel, and one character from a non-Latin (and preferably fictional or dead) alphabet—but don't use &, ?, λ, or ᚠ
- Also, change your password every 30 days and never, ever write it down
- That sort of advice dates to 1979 and is *obsolete*—technology, use patterns, and threat models have changed so much since then
- NIST's latest recommendations: password length is much more important than complexity, don't force changes unless there's evidence of a compromise, and avoid known bad passwords like "Iloveyou123!" and the like

CS@CU

The Real Danger

- The real danger from passwords is *reuse*: using the same password on multiple sites
- Why? If a site gets hacked and your password is stolen from there, you don't want any other site you use to be at risk
- In other words: for every site you use (and there are probably many), you want a long, random, unique password—but you can't possibly remember all of those
- Solution: a *password manager*

Password Managers

- Password managers securely store your passwords
- Most will generate random passwords for you
- Newer versions of MacOS and iOS have built-in password managers and will securely share your passwords between your devices
- But a paper notebook works just fine, if you don't lose it and if you trust everyone else in your household
  - Someone breaking in to your unit to copy that notebook? We call that a movie plot threat, but a domestic abuser is a very real threat for some people

Newer Standards: Two-Factor Authentication (2FA)

- Relies on a password (Factor 1) and something else, generally a device in your possession
- Most common form: a text message to you
  - Not the best—phone numbers can be stolen—but *far* better than no 2FA
- Many other types of 2FA, but those depend on what the far site supports
- Strongest of all: something called a “FIDO2 key” (via USB, very short-range wireless, etc.)
- But—make sure you have a backup of your 2FA device or code number
  - (Regular backups are a *huge* security advantage)

A Yubikey FIDO2 device

Passkeys

- A new authentication scheme that strongly authenticates you and is phishing-proof
- However—it can be hard to move your passkey between devices or to back it up
- Something to keep an eye on…

Resetting Passwords

- Passwords are generally reset by an email message
- Some sites use email messages instead of text messages for 2FA (which is often better for privacy)
- *This means that your email password is the most valuable one you have*

Social Engineering (AKA Tricking or Scamming)

Scammer’s Goals

They’re con artists; they operate by trickery to gain

- Access to your bank account or credit cards
- You buying something for them
- Malware on your computer
- More

Example: The Gift Card Scam

- You receive an email purporting to be from someone you know (I've seen such claiming to be from my department chair or dean)
- Scammer: "I'm in a meeting now, but really need you to buy some Apple iTunes Gift Cards for me. Buy them, send me the numbers, and I'll reimburse you."
- Obviously a scam—but look at the research that went into identifying my department chair and dean…

Defeating 2FA

Normal Behavior

- You use your username and password to log in to your bank, which uses 2FA
- You receive a text message with a security code
- You enter that and finish your login

Defeating 2FA

Normal Behavior

- You use your username and password to log in to your bank, which uses 2FA
- You receive a text message with a security code
- You enter that and finish your login

Scam Behavior

- You get a call: “We’re from your bank. We suspect a security breach; to test it, you’ll momentarily receive a text from the bank with a code number. What is that number?
- Scammer logs in to your bank account
- You receive the text message and tell the scammer the code
- They finish the login

Example: Gaining Your Confidence

- You receive a weird text message out of the blue; you reply
- “Oh, I’m sorry; my mistake”—followed by an attempt to engage you in “friendly” conversation
- Eventually, they hope, you’ll trust them—and listen when they ask you to do something unwise
- Oops…

Example: Tech Support Scam

- Scammer calls and claims to be from Microsoft: “Our Security Center has detected malicious activity from your computer; we’d like to help you clean it up”
- Scammer: “Please install this special security software”
- Victim does so
- Scammer gains full remote access, steals logins and passwords, connects to bank accounts, etc.
- (NY Times: “Tech Support Scammers Stole $85,000 From Him. His Bank Declined to Refund Him”)

Don’t Trust Anything You Receive

- It’s all but impossible to distinguish real messages from fake ones
  - What is the difference between **PayPal.com** and **PayPal.com**?

Don’t Trust Anything You Receive

- It’s all but impossible to distinguish real messages from fake ones
  - What is the difference between PayPa**l**.com and PayPa**l**.com?

Don’t Trust Anything You Receive

- It’s all but impossible to distinguish real messages from fake ones
  - What is the difference between **PayPal.com** and **PayPal.com**?
  - I’ll change the font: PayPa1.com versus PayPal.com — and now you see the difference between the digit “1” and the lower case letter “l”
  - This was in the first phishing message I ever received…
- You can’t always tell what’s real
  - https://www.cs.columbia.edu/~smb/SMBlog-in-PDF.pdf isn’t a PDF file.
- I can’t always tell what’s real

Sender Practices Make This Worse

- ApplyOnlineNow.com really is owned by Bank Of America—but how can you tell?
- I received (what I think is) a perfectly legitimate email from Medicare telling me to watch out for fraud, with a link I was supposed to click
  - A cursory examination showed that that link did not immediately go to medicare.gov—was it genuine?
  - From the NY Times: "Medicare Scammers Are Calling Seniors 50 Times a Day, Trying to Trap Them"
- There are technical mechanisms that will *sometimes* let you verify a site's identity, but they're often hard to find and hard to understand

Some Scams are Obvious

- “I’m dying, have no close relatives, and I want you to help me give my fortune to charity—and you can take some of the money”
- Obvious, but why?
- Sending bulk spam messages is cheap; interacting with real people takes in-person time, which is scarce
- Those who respond, despite the obvious flags, are much more likely to be gullible

What to Do?

- Ignore obvious scam emails, texts, and phone calls
- If your system has a “block and report as spam” button, use it
- Take control:
  - Call a phone number on the back of your credit card (CallerID can often be spoofed)
  - The web site you already know (and *not* the link in the message, and preferably not a Googled web site)
- *Never* give out sensitive information in response to unsolicited messages, calls, etc.

To Sum Up…

Recap

- Keep your software up to date
- Use a password manager and 2FA
- Don’t believe anything you receive

Questions?

CS@CU