Crypto without a Ph.D.

Announcements

- ToB Winternships
- No meeting December 14th

News of the Week

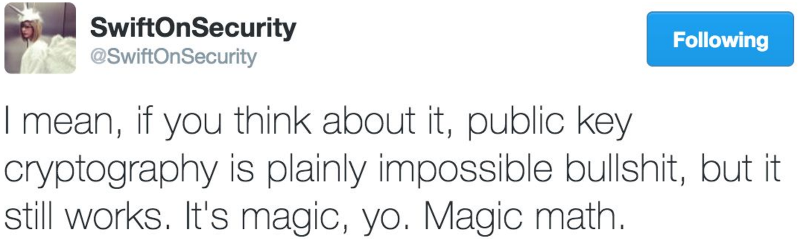
- Lmao @ Apple
  - Secure Enclave Firmware Decrypted
- Uber breach

What is crypto?

- Math used to secure information
- Examples:
    - I want to send a message to Bob, but Eve can’t be able to read it
    - I want to store verify that users of my site have the right password, but if someone hacks my server, they shouldn’t just have a list of passwords
    - I want to “sign” a piece of information and confirm it could only have been sent by me
    - Bitcoin! (more on this later)

What isn’t crypto

- Most things in a CTF “Crypto” category
- “Secret codes”
- “Encryption”
- COMSEC (Worth reading)
- A magic bullet



SwiftOnSecurity
@SwiftOnSecurity

I mean, if you think about it, public key cryptography is plainly impossible bullshit, but it still works. It's magic, yo. Magic math.

How should I use crypto?

- As little as possible
- Don’t write it yourself
- If you have to type the letters A-E-S into your code, you’re doing it wrong
- Pay someone else to
- Using strong, well-vetted libraries without going and breaking a bunch of shit
  - NaCl/libsodium
  - Scrypt
  - AWS ELB
  - OpenSSL

What we’re covering today

How to use crypto to do real things you’ll probably want to do at some point securely

What we’re not covering

- How to do crypto
  - This doesn’t fit in two hours
- How to break crypto
  - Also doesn’t fit in two hours, but there will be challenges!
- Really anything under the hood of crypto
  - Skip to the end if you want resources on this

If you wanna mostly skip the next half hour

https://gist.github.com/atoponce/07d8d4c833873be2f68c34f9afc5a78a

Symmetric encryption

- I can securely exchange a key beforehand
- No one should be able to read my messages without the key
- No one should be able to modify my messages without the key
- No one should be able to figure out the key
- No one should be able to do any of these things partially

Use NaCl defaults!

Asymmetric encryption

- I have to securely exchange a key while people may be listening
- I don’t have to ever talk to the other person before
- No one can pretend to be this other person
- All the stuff from the last slide

Use NaCl defaults!

Asymmetric signatures

- I have some information I don't want to keep secret, but I want to "sign" to say it was absolutely from me
- No one can modify this information and keep my signature valid
- No one can sign other information as me
- Anyone can verify something I've signed is mine

Use NaCl defaults!

Password verification

- I can verify a user's password is what they set it to
- Users cannot login without their correct password
- If my box is compromised, no passwords can be recovered

Use Scrypt! If you're reading this in ~2020, use Argon2

Random numbers

- No one can see any amount of past random numbers and use them to predict future random numbers
- No one can influence future random numbers
- The numbers are *really really* random
- This is not a CSPRNG, those are actually hard

Use `/dev/urandom`

SSL

- A whole bunch of shit oh my god it’s a mess

Use AWS ELB if you can, or OpenSSL! (yes, really)

Client-server transport

- You have an app that needs to talk to a server over the internet
- It’s not just a webapp (then you can just use SSL)
- You want all the asymmetric encryption stuff, but specifically for the client-server model

Use TLS! (yes, really)

Secure Chat

- You wanna buy some drugs from your friends and not get arrested
- Or you're an activist or something I guess

Use Signal! If you can't use Signal, use something that uses its protocol (WhatsApp, encrypted FB messenger)

Don't use whatever the fuck free "secure chat" app you saw on twitter (unless it's Signal)

Secure internet browsing

- You are on a network with possibly malicious people
- They cannot modify any traffic you send
- They cannot modify any traffic you receive
- They cannot monitor anything you do on the internet (other than “connect to it”)

Use Algo! (eventually wireguard?)

Anonymous internet browsing

- You want to buy some drugs from your friends and not get arrested *but on the internet*
- No one can know what computer you're using
- Probably all the stuff model from last time

Use TOR!

How should I learn crypto?

- Dan Boneh’s Coursera course
- Matasano Cryptopals (will also get you a job)
- 20 Years of RSA Attacks - Good for ~80% of CTF Problems
- Pretty much nothing easy will teach you crypto well

CTF Time!

- http://challenge.multiwack.science/challenge/de-radaction/
- https://transfer.sh/HthDo/tls-16970cb3b09a9dd01f5b82449d9c1795.tar.gz (the goal is to get the private key) (credit to davidw)