Lecture 21 - misc stuff

Testing for Contract

Dennis Ritchie: “Software that is not tested is broken.”

Working with keys

Private keys - truffle - wallet tools like Metamask

You can test with mocha w/o doing this

If you want to call contracts with encrypted keyfiels you will need to do this

1. Generate keyfile for a “private key”.

```
$ cat pk
cb11e776020f6a98a484101403fb0d823412bfe94df62e5170ed7776f751785b
$
$ ./sig-test generate --privatekey pk --default-name
Passphrase:
Address: 0xc0c4B94355fD676a29856008e625B51d1acD04eD
File Name: UTC--2019-04-24T08-56-40.146086Z--c0c4B94355fD676a29856008e625B51d1acD04eD
```

2. Extract from keyfile the private key and use that in truffle

```
$ Key_File=UTC--2019-04-24T08-56-40.146086Z--c0c4B94355fD676a29856008e625B51d1acD04eD
$ Key_File_Password=password
$
$ ./get-private-key -keyfile "${Key_File}" -password "${Key_File_Password}"
Private Key: 0xcb11e776020f6a98a484101403fb0d823412bfe94df62e5170ed7776f751785b
To import into truffle:
At the console, `truffle(develop) >` or attach to truffle with
`$ geth attach http://127.0.0.1:9545`, then...
> web3.personal.importRawKey("0xcb11e776020f6a98a484101403fb0d823412b
 fe94df62e5170ed7776f751785b","password")
```

Get A Receipt

```
curl  \
-H "Content-Type: application/json" \
-X POST \
--data '{"jsonrpc":"2.0", "method":"eth_getTransactionReceipt","params":\
   ["0x3f3aa792dd4a76d6feea51d57fc6543e97031cb4fb53e76642243eab0dfdb343"],"id":1}' \
http://192.168.0.199:8545/
```

Get an Account Balance

```
curl  \
-H "Content-Type: application/json" \
-X POST \
--data '{"jsonrpc":"2.0", "method":"eth_getBalance", "params":[\
    "0x6ffba2d0f4c8fd7961f516af43c55fe2d56f6044", "latest"], "id":1}' \
http://192.168.0.199:8545
```

How to Launder Money.

From: https://www.washingtonpost.com/outlook/trumps-businesses-are-full-of-dirty-russian-money-the-scandal-is-thats-legal/2019/03/29/11b812da-5171-11e9-88a1-ed346f0ec94f_story.html

“According to Jonathan Winer, who served as deputy assistant secretary of state for international law enforcement in the Clinton administration, … “If you are doing a transaction with no mortgage, there is no financial institution that needs to know where the money came from, particularly if it’s a wire transfer from overseas,” … “The customer obligations that are imposed on all kinds of financial institutions are not imposed on people selling real estate. …”

“And without such regulations, prosecutors’ hands are tied.

“All of which made it easier for the Russian Mafia to expand throughout the United States.”

Document Security

A search under Fourth Amendment occurs when a governmental employee or agent of the government violates an individual’s reasonable expectation of privacy.

The 4th Amendment is:

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

Who protects our data:

From: http://blairreeves.me/2019/04/18/ai-is-not-coming-for-you/ “In an era when many of our political leaders, particularly in America, are 60 and 70-somethings who barely know how to use email, there is an understandable reluctance to entrust them with regulating technologically sophisticated industries. And for the most part, they don’t! Most of the political class, with some notable exceptions, is happy to let the tech lobby write its own regulatory scheme and pass it in exchange for contributions.”

2 of 9 Supreme court justices have ever used email.

News

1. Utah Bans Police From Searching Digital Data Without A Warrant, Closes Fourth Amendment Loophole https://www.forbes.com/sites/nicksibilla/2019/04/16/utah-bans-police-from-searching-digital-data-without-a-warrant-closes-fourth-amendment-loophole/#15b43cf07630

2. Supreme Court rules that police generally need a warrant to access cell phone data (June 22 2018) https://abcnews.go.com/Politics/supreme-court-rules-police-warrant-access-cell-phone/story?id=56086538

3. Border searches require warrant: U.S. Court of Appeals for the Eleventh Circuit in U.S. v. Vergara (March 2018) https://www.eff.org/deeplinks/2018/03/eleventh-circuit-judge-endorses-warrant-border-device-searches

How data degrades

1. Finite rate of loss of media
2. Systems like ZFS with checksums (hash/digital signatures) to verify integrity of data
3. 5-9s, 7-9s -- Amazon S3
4. Business Continuity - is a legal requirement - "Standards of Good Practice" https://www.geminare.com/wp-content/uploads/U.S._Regulatory_Compliance_Overview.pdf

How data is lost

Primarily lack of backup

1. Deleting files accidentally - 51%
2. Viruses and damaging malware - 18%
3. Mechanical damages of hard drive - 12%
4. Power failures - 8%
5. Spilling coffee, and other water damages - 7%
6. Theft of computer or of data - 2% - Experian, Target, Ashley Madison, OPM etc.
7. Fire accidents and explosions - 1%

OPM Hack: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ "OPM has a multifactor authentication scheme, but it wasn't fully implemented until January 2015—too late to prevent the PlugX attack."

Data Safe from...

Who can do a "Searches and Seizures" and when.

From: Brian Surber, Deputy General Counsel, Oklahoma Bureau of Narcotics
"If you have probable cause to search a mobile vehicle or boat you do not need a warrant. Because vehicles and boats are mobile and heavily regulated by society, you do not need a warrant to conduct a probable cause search of a vehicle. The Supreme Court has even held that an officer does not need a search warrant to conduct a search of a parked motor home if that officer has probable cause."

See Palmer 1977 or Morash 1984.

Can you put up a camera in a field and watch a person or actions in a private field?

Acts of God

Hurricane, Flood, Tornado, Earthquake

Disclosure of Keys to government officials

In United States v. Doe, the United States Court of Appeals for the Eleventh Circuit ruled on 24 February 2012 that forcing the decryption of one's laptop violates the Fifth Amendment.

Us Constitution:
"No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

The Federal Bureau of Investigation may also issue national security (NSL) letters that require the disclosure of keys for investigative purposes.

Warrant Canary https://en.wikipedia.org/wiki/Warrant_canary This riles on West Virginia State Board of Education v. Barnette and Wooley v. Maynard rule the Free Speech Clause prohibits compelling someone to speak against one's wishes. By implication this can easily be extended to prevent someone from being compelled to lie.

Disclosure under duress

Tokens can make you the "bank".