Planecrashes, Nukes, and More Abuse

All these are Blue Slides...

- There may be important takeaways however...
  - Both in class and in life
- When we get to Tor stuff the serious content warning again kicks in
  - Feel free to leave the lecture/stop watching then if the problem of child abuse makes you uncomfortable

Safety and Security

- Safety and Security are closer than two sides of the same coin...
  - Both have the objective of ***maintaining system properties*** under all conditions
- The only real difference are the source of deviance
  - Security we deviate because of ***deliberate action by an adversary***
  - Safety we deviate because of ***chance, failure, and inadvertent actions***

The Airline Industry...

- A rough rule of thumb I once heard about an airline's costs:
  - 1/3 for fuel
  - 1/3 for people
  - 1/3 for the aircraft
- And the business is brutally competitive
  - Warren Buffett once joked that if he had a time machine he'd take a shotgun to the runway at Kitty Hawk to save subsequent investors a huge amount of money
- So when developing a new aircraft...
  - Make it ***cheap***:
    Limit the necessary retraining
    Limit the fuel costs

The Boeing 737...

- Probably the most successful commercial airliner
  - First flown in 1967, over 10,000 of various types sold!
- The first version: 737-100 and 737-200
  - Notice the relatively tiny jet engine... We will get back to that later
- Consequence of a design choice:
  - Wing mounts to the low part of the plane...
  - And can't have the plane too high off the ground because you needed to unload luggage on unimproved airfields
  - But at the same time, under-wing engines allowed the airframe to evolve: Stretch it to make it longer with each revision

Then the "737-Classic": -300, -400, -500

- First major revision
  - Sold from 1984-2000
- Bigger, Better, More Efficient
  - Major change in the concept of how the engines are mounted...
- Not quite a "separate plane"
  - But substantial retraining necessary for pilots & crew to shift from the original to the "classic"

Then the 737-NG -600, -700, -800, -900

- Almost a new plane
  - Bigger wings, new cockpit, new engines, more people etc...
  - Notably the "flat bottomed" engines to get them to fit!
- First on sale in 1997
- Really a "new plane"
  - Completely different cockpit for the pilots

In The Meantime: Enter Airbus

- The A320 family
  - Entered service in 1987...
- Slightly bigger than a 737
  - And claimed to be cheaper...
  - And not so close to the ground on the wings/engines
- A major new version entered service in 2016: the A320neo (New Engine Option)
  - Moderate pilot retraining necessary:
    it flies different from the A320 due to significantly larger engines
  - But they had higher wings to begin with so it was easier to put on bigger engines

Why Larger Engines?

- Bigger engines that burn hotter are ***much*** more fuel efficient
  - Thermodynamic efficiency of the engine core
  - Bigger bypass fans move more air
- Core problems:
  - Efficiency of the core is improved by making it bigger
  - Thrust goes up by moving a bigger volume of air ("high bypass")
    - $E=mv^2$, but $p=mv$
  - And the area of the engine is ~r^2

The 737-MAX program

- In 2011, Boeing responded to the A320...
  - American Airlines just ordered a bunch of A320ceo and A320neo planes
- Effectively sidelined the planned 737 replacement...
  - It would have been close to a "baby Dreamliner (787)"
  - And instead decided to "re-engine" and improve the 737-NG in other ways
  - Goal was 14% improvement in efficiency
- Fatal Decision #1:
  - Unlike the A320neo, there must be ***no significant pilot retraining***:
    If a pilot is certified for a 737-NG,
    the pilot should be able to fly the
    737-MAX with just a bit of written material

Fatal Decision #2: Larger Engines

- Went from a 61" engine to a 69" engine
  - But the previous 61" engine already had the minimum available ground clearance!
  - Oh, and still not as good as the A320neo, which has 20% higher bypass
- Forced to move the engines further forward and upward
  - Which changes the dynamic balance of the aircraft
  - Other option would have required effectively reengineering the entire wing setup
    - At which point, why not just design a new plane from scratch: the initial 737 design had much much smaller engines
- Dynamic balance changes are significant
  - Significantly higher tendency to want to pitch the nose up under acceleration

Fatal Decision #3:
The "Software" Fix

- If the plane goes too nose-up, it wants to stall
  - aka, "just drop from the sky", major not-good
- The larger nacels for the engines also act like wings
  - Even further increasing the propensity to stall
- "Hey, we have a computer that can fly the plane..."
  - So lets modify the computer to have the plane try to adjust itself so it flies like the 737-NG:
    MCAS: Maneuvering Characteristics Augmentation System

Fatal Decision #4: Engineering the software fix

- In an Airbus, the computer is the boss
  - So the computer design is very paranoid: Each computer can listen to all relevant sensors
- In a Boeing, the ***pilot*** is supposed to be the boss
  - So although there are two flight computers, each one only listens to its ***own set of sensors***...
  - Because on all previous 737s, the computer ***mostly*** acted as an advisor
    - Which means you can be fairly slack with things
- MCAS program stuck with the 737 design
  - So if the computer saw that ***it's*** pitch sensor said the nose was too high, it would act
- Plus other factors:
  - If you fight the computer on the 737-NG, the computer gives up
  - But on MCAS, it just tries again... and again... and again...

Fatal Decision #5: Regulatory Capture

- In the old days, the FAA certified planes...
  - But this requires significant expertise
  - And the government can't pay nearly as much as Boeing
- Now, the aircraft is ***mostly*** self certified by the company...
  - And even here they screwed up!
- MCAS was determined to create a "hazardous" condition if it erroneously activated at the wrong time...
- ***Yet they kept the single-sensor design!***

So How To Crash a 737-Max....

- Have the angle of attack sensor on one side of the plane break
  - On the same side as the currently active flight computers
- Makes the plane think the nose is pitching up
  - So MCAS pitches the plane down...
- The pilot fights MCAS to pitch back up...
  - So MCAS pitches the plane ***further down...***
- Lather/Rinse/Repeat...
  - Until the plane goes nose-first into the earth

Magnifying Culpability: Blaming the user...

- After the first crash, Boeing blamed the pilots
  - "Yeah, we didn't tell them about MCAS, but it should have been treated just like a runaway stabilizer, where the autopilot goes wonky..."
- But that wasn't true!
  - Runaway trim, you fight it and it stops fighting
- And they are ***still*** blaming the pilots!

Asked about what led to the safety flaws in the 737 Max, Muilenburg said Boeing didn't make any mistakes in its design of the planes. "There was no surprise or gap or unknown here or something that somehow slipped through the certification," Muilenburg said. "We know exactly how the airplane was designed, and we know exactly how the airplane was certified."

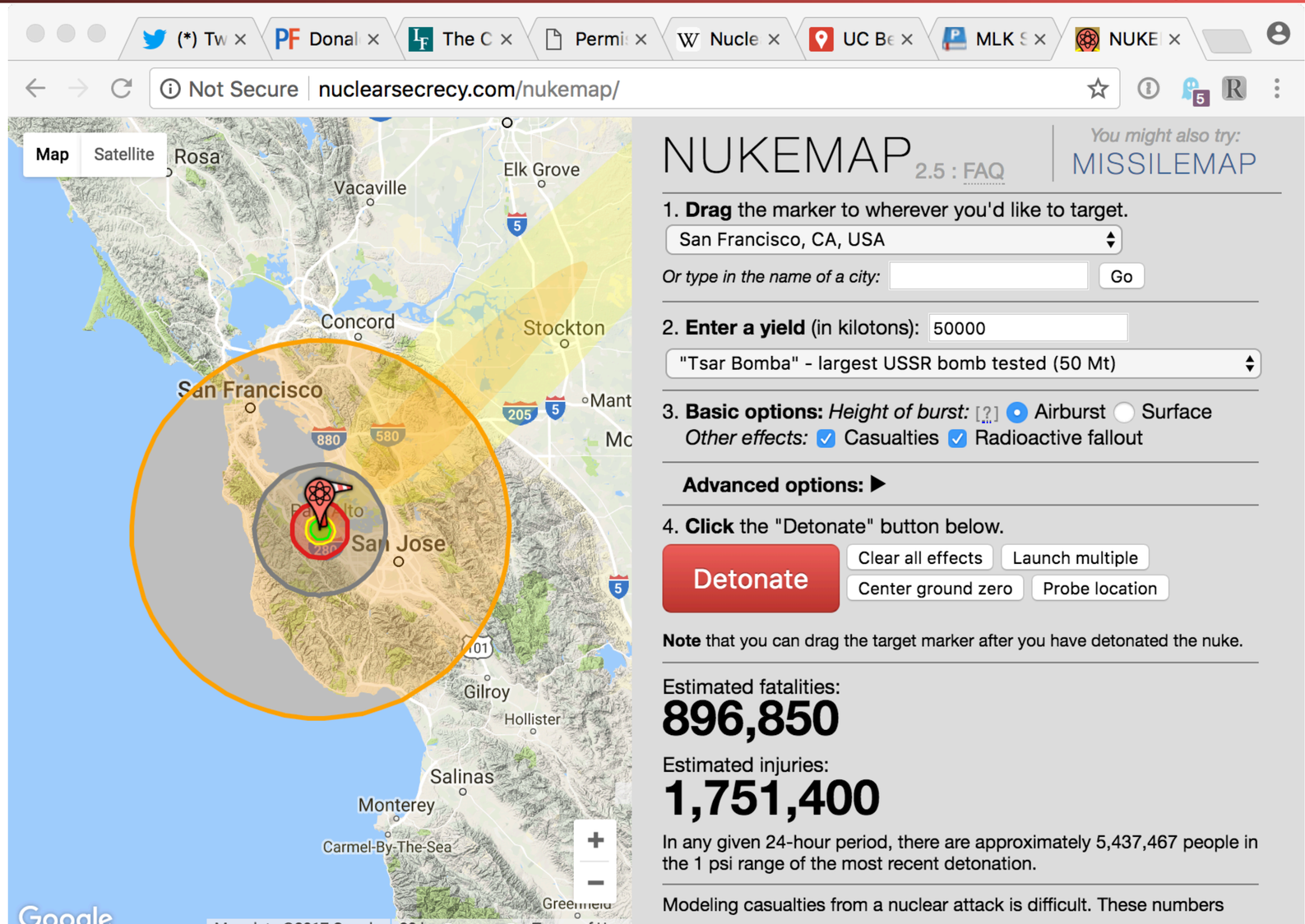
The CEO said both crashes were caused by a "series of events" that included erroneous sensor data being fed into the maneuvering characteristics augmentation system, or MCAS, an anti-stall system that played a role in both crashes. "There were actions — or actions not taken — that contributed to the final outcome," he said, alluding to the role of the pilots.

Conclusions and non-tested Takeaways...

- It is a massive Charlie Foxtrot of epic proportions
- If it was an American or Southwest plane involved, there would already be indicted ***executives*** rather than just the single chief test-pilot
- Every system on the 737-Max that changed needs to be viewed with suspicion
  - And I won't fly on one for at least 3 years post recertification
- Oh, and don't let the "Business" types take over an engineering firm
- Oh, and never buy a Tesla:
  Their software development flow and autonomous concept is similarly fatally flawed, just with a lower body count

Why talk about nukes?

- Nukes are big and scary and in the news...
  - But have interesting security and safety properties
- Lots of material ~~stolen~~ borrowed from Steve Bellovin's excellent talk on PALs



How a Nuclear Weapon Works...

- 1940s-level technology...
  - A hollow sphere of fissile material
    - Plutonium and/or Plutonium + Uranium
  - Use this as a primary to ignite a Teller/Ulam secondary to make it a hydrogen bomb...

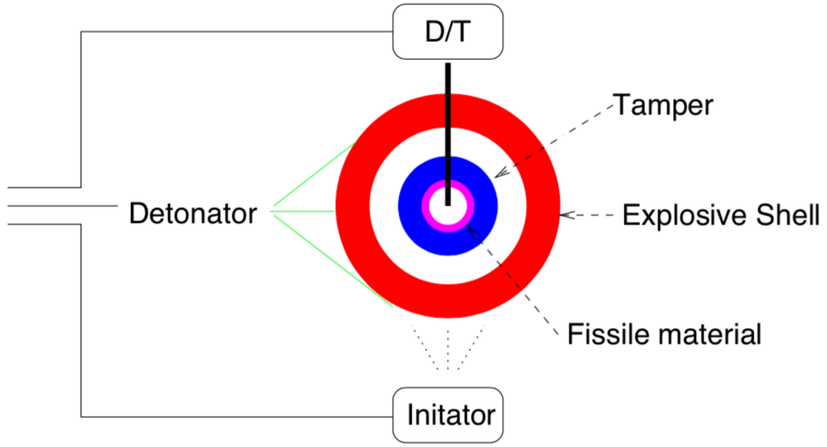
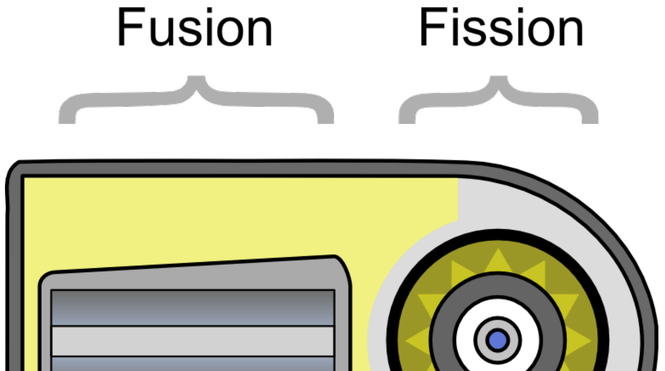


Diagram by Steve Bellovin

- Very careful sequencing needed
  - D/T pump to fill the hollow with Deuterium & Tritium ("Boost gas")
    - Not needed for the earliest bombs, but most modern bombs need boosting to work
  - Initiator sprays neutrons to start the chain reaction
  - Detonator needs to trigger multiple points on the explosive shell
    - Squiggly-traces of explosive so that all around the shell everything detonates at once
- We could make a 194 "design a nuke" class and probably get something that would work!

And H-Bombs...

- A "Tellar/Ulam" 2-stage device:
  A A-bomb ignites a fusion stage
  - Fusion stage has Lithium Deuteride...
    - Neutrons and pressure from the A-bomb convert the Lithium to Tritium
    - Then Deuterium/Tritium fusion makes it go boom!
- Still 1960s technology!
  - Biggest issue overall is ***materials***:
    6 or 7 countries have built H-Bombs



And How To Deliver Them...

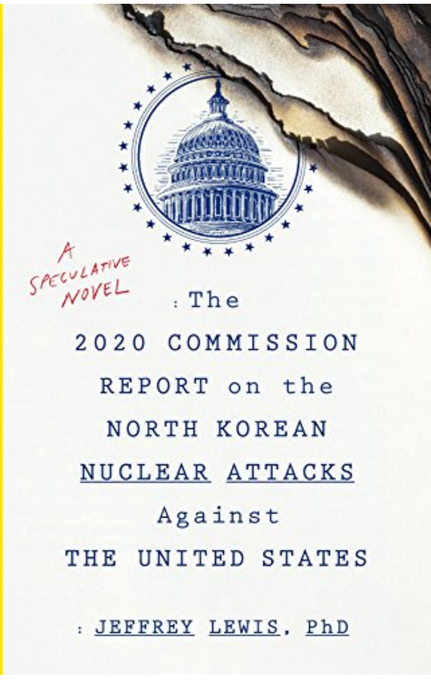
- Stick em on a rocket
  - This ***is*** rocket science: It is far easier to build the nuke than build the ICBM...
  - Alternatively, stick it on an unmanned miniature airplane ("Cruise Missile") or just hang it under a plane as a old-fashioned bomb
- Then stick the rocket on something
  - In a hardened silo
    - But the other side can drop a nuke on it...
  - On a truck
  - In a sub
  - On a plane...

The Problem: When To Use Nukes...

- Nuclear weapon systems can fail in two ways:
  - Launch the nukes when you shouldn't...
  - Fail to launch the nukes when you should...
- The latter is (badly) addressed by how our nuclear decision making happens
  - "Launch on warning": If we ***think*** we are under attack, the President has a couple minutes to decide to order a nuclear strike before the attacker hits our ICBMs!
    - This is often regarded as ***insanely*** stupid: We have both nuclear bombers with long-range cruise missiles and nuclear armed submarines, both of which ***will*** be able to launch enough retaliatory hellfire
  - Far better is the "French model" (cite @armscontrolwonk):
    "We have subs. You nuke us ***or*** attack our strategic weapons and we nuke you":
    - This removes the time pressure which can cause errors

"Launch on Warning" and North Korea...

- Let us assume that North Korea's leadership are ***rational*** actors
  - They act in what they perceive as their self interest: survival!
- North Korean leadership ***will eventually lose*** a war with South Korea and the US
  - So they may be provocative, but they want to make ***sure*** the US and South Korea won't start a war
- Nukes are a critical deterrent for them
  - Especially when Donald Trump didn't seem to care that a war would kill hundreds of thousands in South Korea
- IRBMs and ICBMs are as important as the nukes themselves!
  - Need to be able to hit the US bases in Okinawa and Guam as military targets
  - And last year Mar-a-lago and Washington DC to dissuade Trump personally: The Hwasong-15 ICBM can just barely range South Florida.
- "***Empathy*** for the devil"
  - Computer security is adversarial, think about your adversary's needs, wants, and desires



Launch on Warning and the US C&C Structure

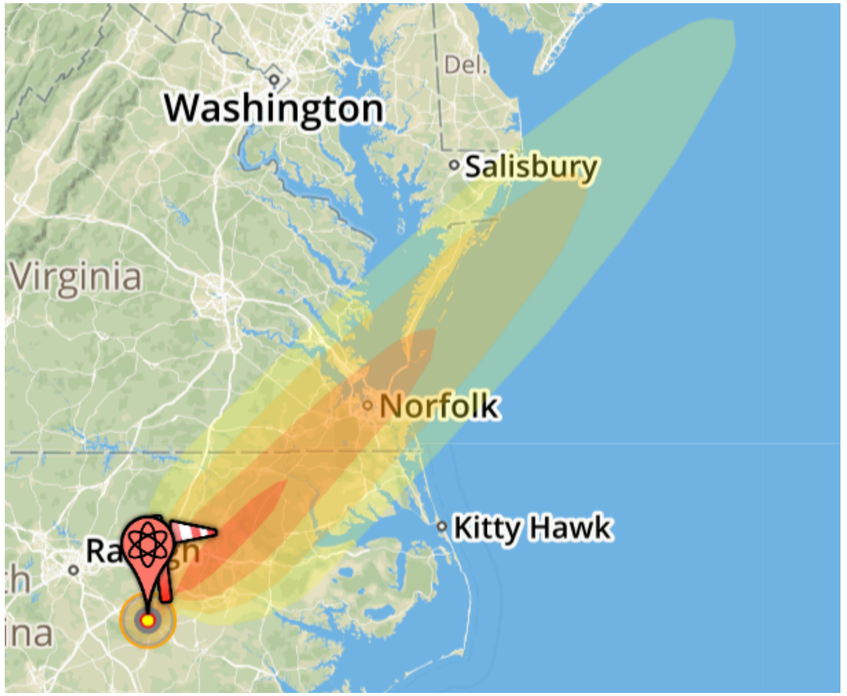
- The President has three items:
  - A “biscuit” of authentication codes kept on his person
  - The “football”: containing a menu of options for ordering a nuclear strike
  - An encrypted secure phone
- The President has a bad day…
  - He calls over the football
    - Picks out the menu option he wants to use..
  - He calls NORAD on the phone
    - Taking out the biscuit, opening it, and getting the authentication code of the day
    - Saying what menu option he wants
  - < 5 minutes later, the ICBMs leave their silos
    - And there is no “recall code”

The Interesting Problem: Limiting Use

- Who might use a nuke without authorization?
  - Our "allies" where we station our nukes
    - Original motivation: Nukes stored in Turkey and Greece
  - Someone who can capture a nuke
    - This is what sold the military on the need for the problem:
      We had nukes in Germany which ***would*** be overrun in case of a war with the USSR
  - Our own military
    - General Jack D Ripper scenario
- The ***mandated*** solution:
  - Permissive Access Link (PAL)

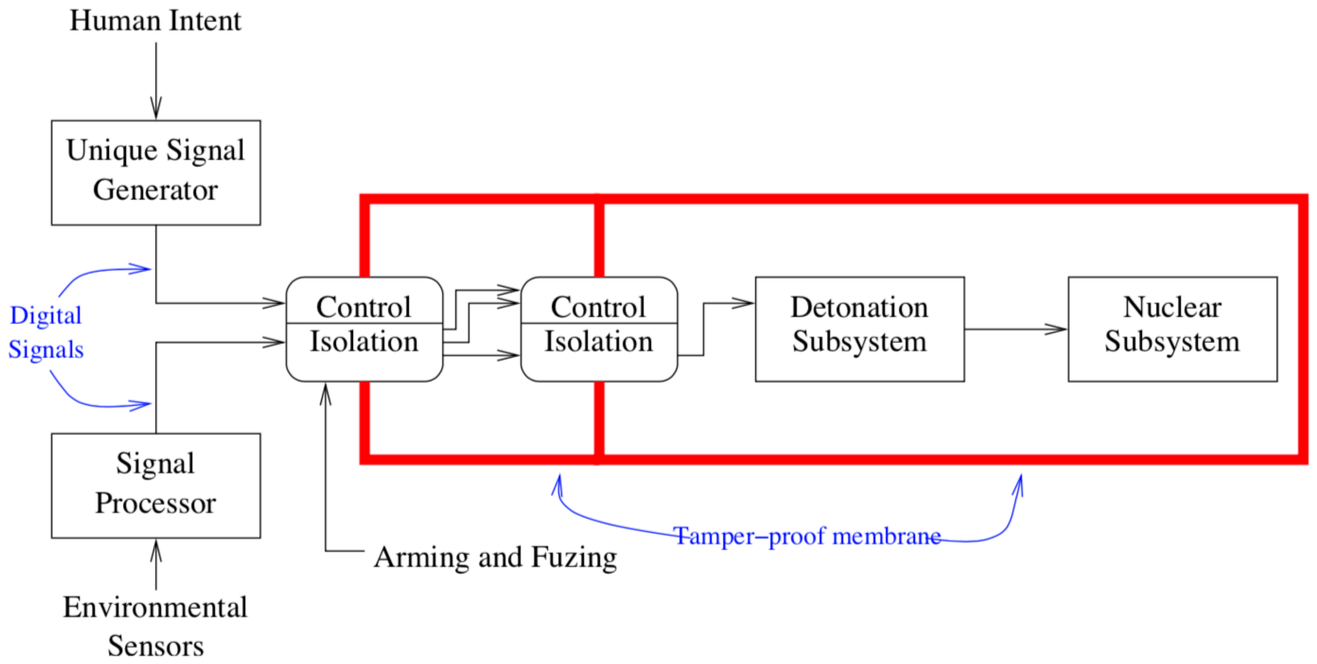
Nuke Safety Features

- One-point safety – no nuclear yield from detonation of one explosive charge.
- Strong link/weak link –
  - strong link provides electrical isolation;
  - weak link fails early under stress (heat, etc.)
- Environmental sensors – detect flight trajectory.
- Unique signal generator – digital signal used for coupling between stages.
- Insulation of the detonators from electrical energy.
- “Human intent” input.
- Tamper-resistant skin (Personal bet: dump the boost gas)
- Use Control Systems
- Not always the case: In 1961 in South Carolina a B52 broke up
  - One of the two 4MT bombs ***almost*** detonated on impact, since it thought it was being dropped!



Bomb Safety Systems

- We have a "trusted base"
  - Isolated inside a tamper-detecting membrane
    - Breach the membrane -> disable the bomb
- We have human input
  - Used to generate a signal saying "its OK to go boom"
    - The user interface to the PAL can follow the same path/concepts
- We have critical paths that we can block
  - Complete mediation of the signal to go boom!



Unique Signal Generator

- Part of the strong link
  - Prevent any detonation without clear, unambiguous showing of “human intent”
- A ***safety*** system, not a security system
- Looks for a 24-bit signal that is extremely unlikely to happen during any conceivable accident. (Format of input bits not safety-critical)
  - Accidents can generate random or non-random data streams
  - Desired signal pattern is unclassified!
- Unique signal discriminator locks up on a ***single*** erroneous bit
- At least partially mechanical

PALs

- Originally electromechanical. (Some weapons used combination locks!)
- Newest model is microprocessor-based. There may still be a mechanical component.
  - Recent PAL codes are 6 or 12 digits.
- The weapon will permanently disable itself if too many wrong codes are entered.
- PALs respond to a variety of codes – several different arming codes for different groups of weapons, disarm, test, rekey, etc.
- It was possible, though difficult, to bypass early PALs.
  - Some even used false markings to deceive folks who didn't have the manual.
- It does not appear to be possible to bypass the newest "CAT F" PAL.
  - Modern bombs don't work without the tritium boost-gas:
    If you blow the gas you disable the nuke. Don't know if this is done or not

How are PALs built?

- We don't know, but some informed speculation from Steve...
- It is ***most likely*** based around the same basic mechanism as the unique signal generator
  - Gives a single point of control already in the system
  - Reports about it indicate that it was successfully evaluated in isolation
  - Take advantage of the existing trusted base of the tamper-resistant barrier around the warhead to protect the device

Deployment History

- Despite Kennedy's order, PALs were not deployed that quickly.
  - In 1974, there were still some unprotected nukes in Greece or Turkey
- PALs and use control systems were deployed on US-based strategic missiles by then
  - But the launch code was set to 00000000
  - Rational: the Air Force was more worried about failure to launch!
- A use control system was added to submarine-based missiles by 1997
- In 1981, half of the PALs were still mechanical combination locks

Steve Bellovin's Lessons Learned
Aka ***Takeaways***

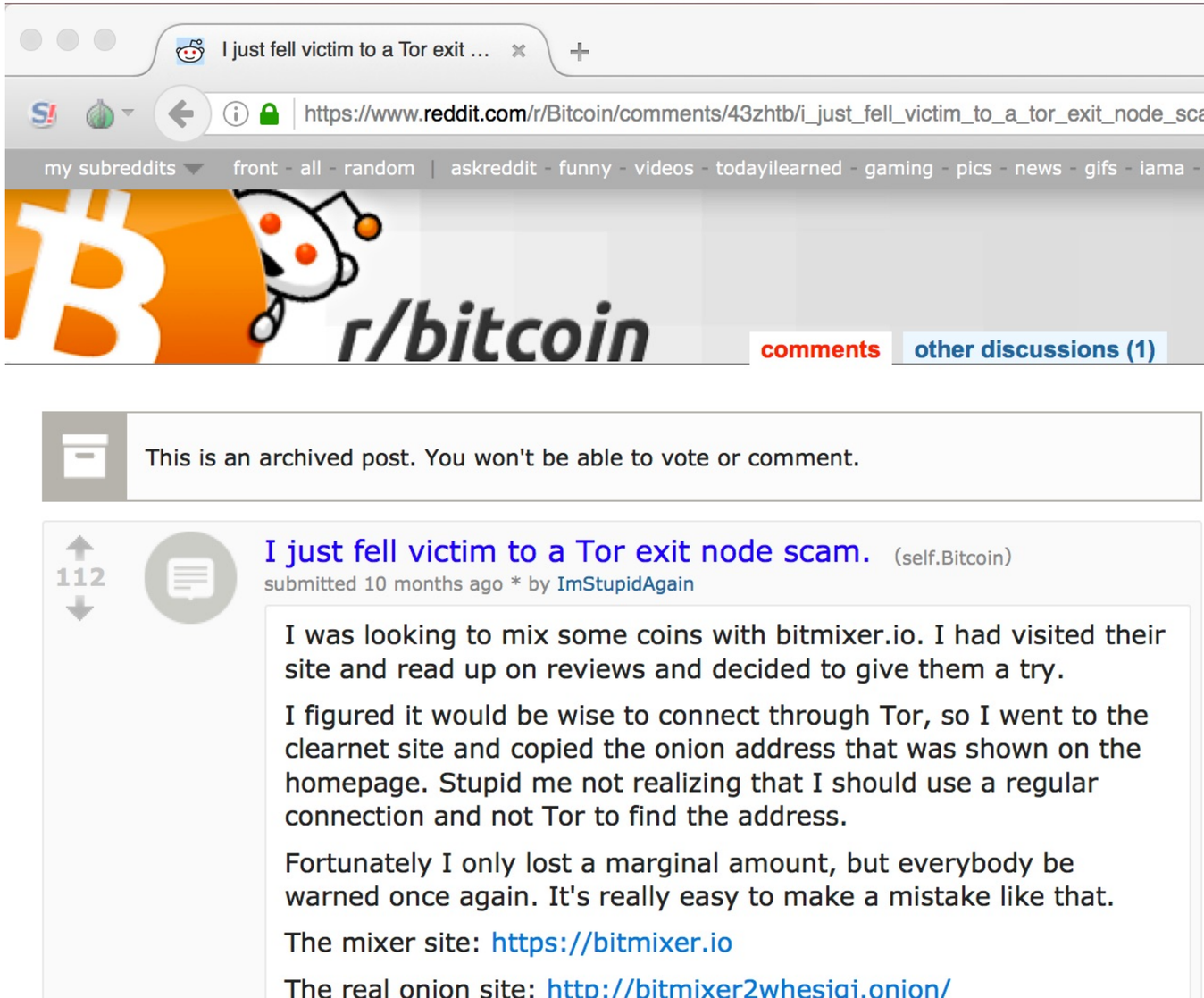
- Understand what problem you're solving
- Understand ***exactly*** what problem you're solving
- If your abstraction is right:
  you can solve the key piece of the overall puzzle
- For access control, find the One True Mandatory Path — and block it.
  - And if there is more than one, you're doing it wrong!
- What is the real TCB of our systems?

Some More on Tor

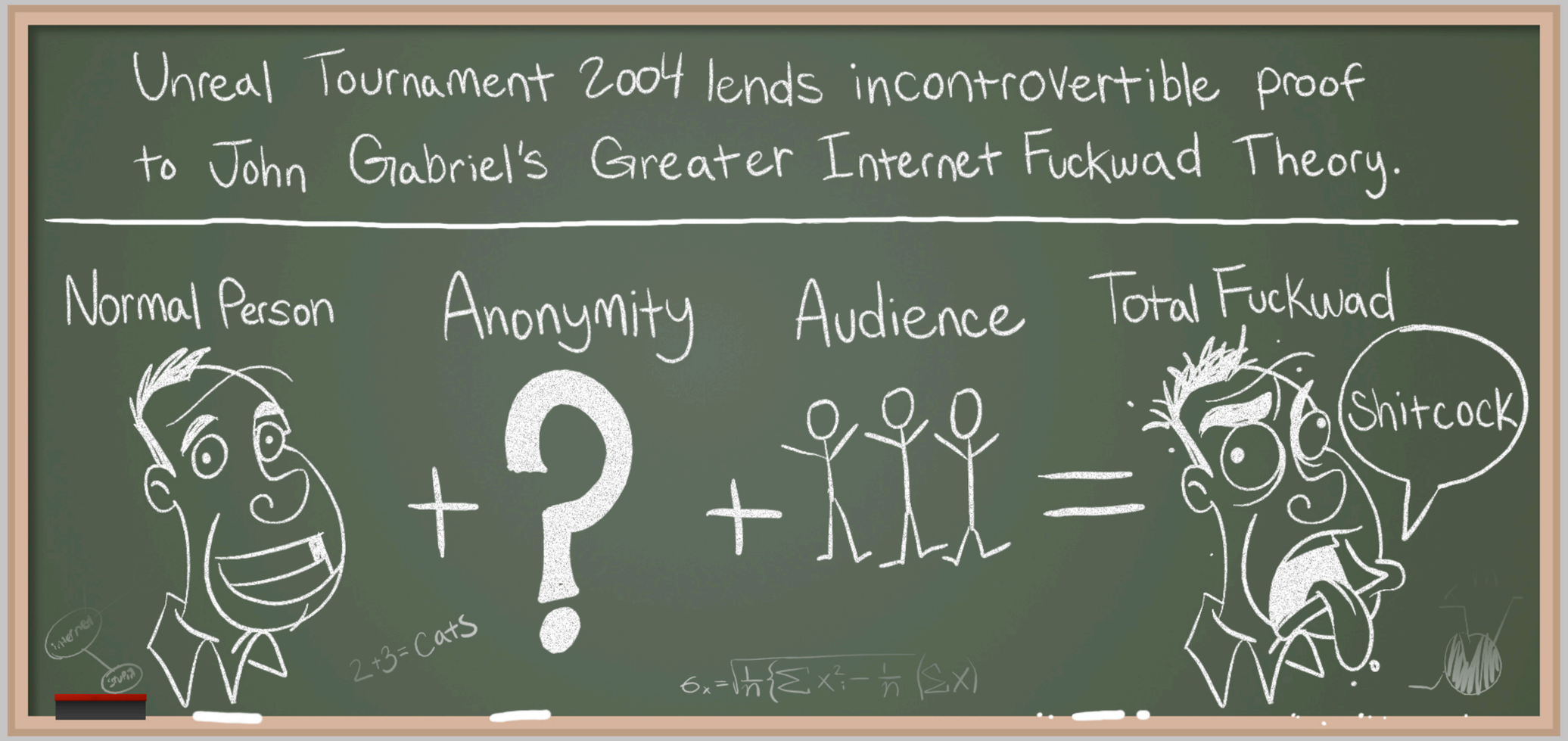
- Picking up from last week...
- Why Tor is painful for clients
- Why Tor is only so-so for counter-censorship
- Why Tor Hidden Services are a plague

In Tor You Are Relying On Honest Exit Nodes…

- The exit node, where your traffic goes to the general Internet, is a man-in-the-middle…
  - Who can see and modify all non-encrypted traffic
  - The exit node also does the DNS lookups
- Exit nodes have not always been honest…



Anonymity Invites Abuse… (Stolen from Penny Arcade)



This Makes Using Tor Browser Painful…
Due to "Fate Sharing"

And Also Makes Running Exit Nodes Painful…

- If you want to receive abuse complaints…
  - Run a Tor Exit Node
- Assuming your ISP even allows it…
  - Since they don't like complaints either
- Serves as a large limit on Tor in practice:
  - Internal bandwidth is plentiful, but exit node bandwidth is restricted
- Know a colleague who ran an exit node for research...
  - And got a ***visit from the FBI***!

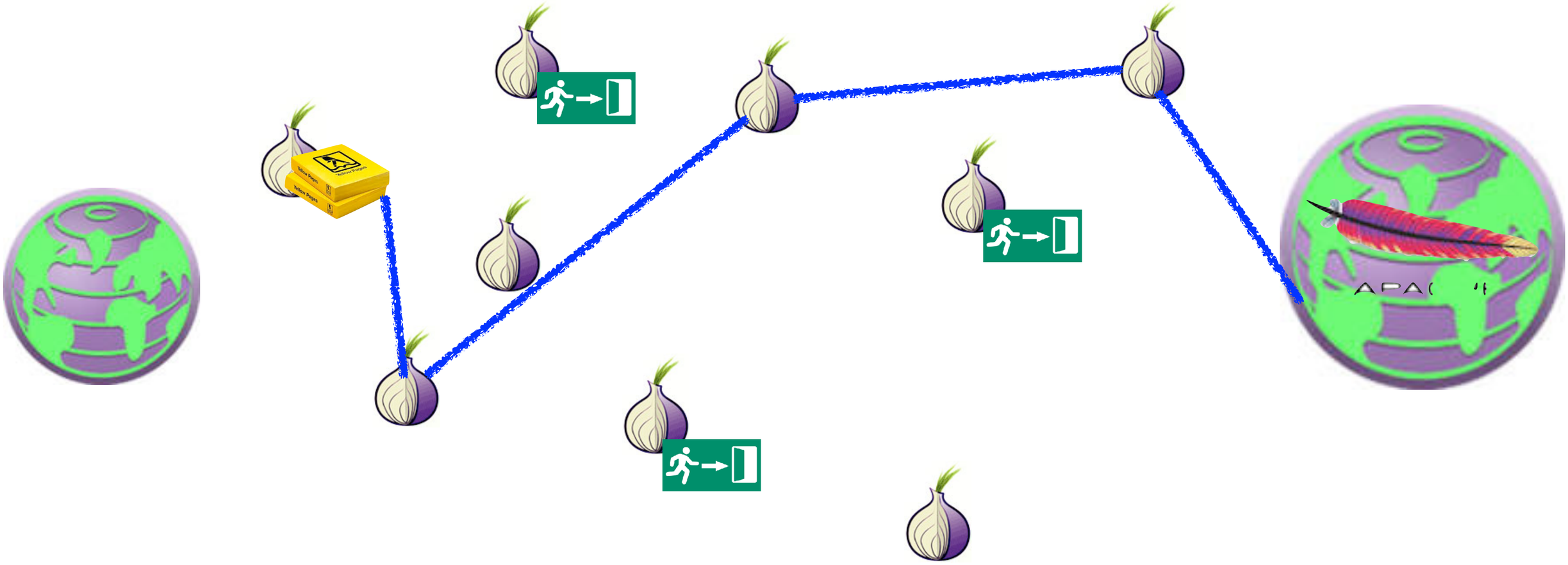
Censorship Evasion...

- Tor is actually really ***bad*** for evading censorship
  - It is trivial to tell that someone on the network is running Tor
- There are ***optional*** pluggable transports that attempt to hide the traffic
  - The problem is you have to learn about these...
    Yet if the censor does, it won't work!
- And then the user has all the bad of Tor...
  - Fate sharing with all other users of the exit nodes
  - Significantly worse latency
  - Oh, and Tor Browser's not saving history is not necessarily nice!
- Only good thing is it is "free"
  - Tor project gets paid largely for counter-censorship
  - Users are "paying" by providing traffic for those who want anonymity to hide in

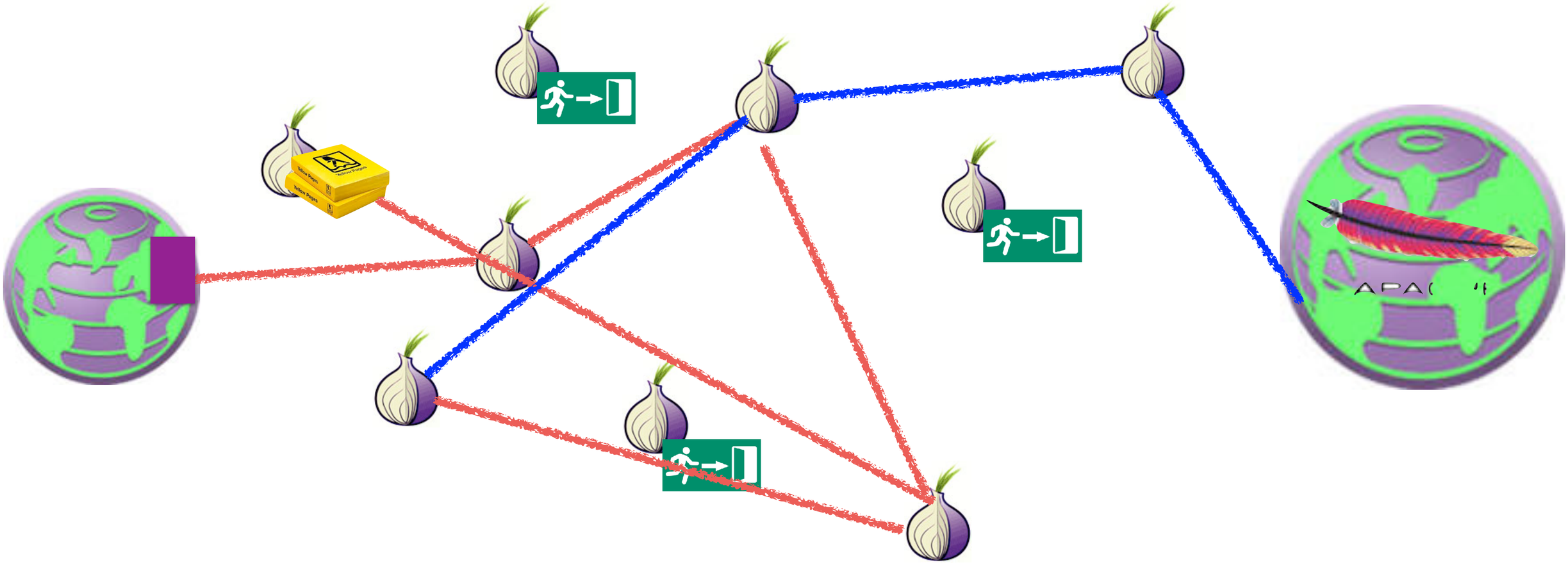
Tor Browser is also used to access Tor Hidden Services aka .onion sites

- Services that only exist in the Tor network (the "Dark Web")
  - So the service, not just the client, has possible anonymity protection
- A hidden service name is a hash of the hidden service's public key
  - Used to be smaller: https://facebookcorewwwi.onion
    - In this case, Facebook spent a lot of CPU time to create something distinctive
  - Now larger: https://facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion
    - Change was designed to prevent one attack at the cost of forcing records of .onion domains to be unmemorizeable
- Using this key hash, can query to set up a circuit to create a hidden service at a rendezvous point
  - And because it is the hash of the key we have end-to-end security when we finally create a final connection

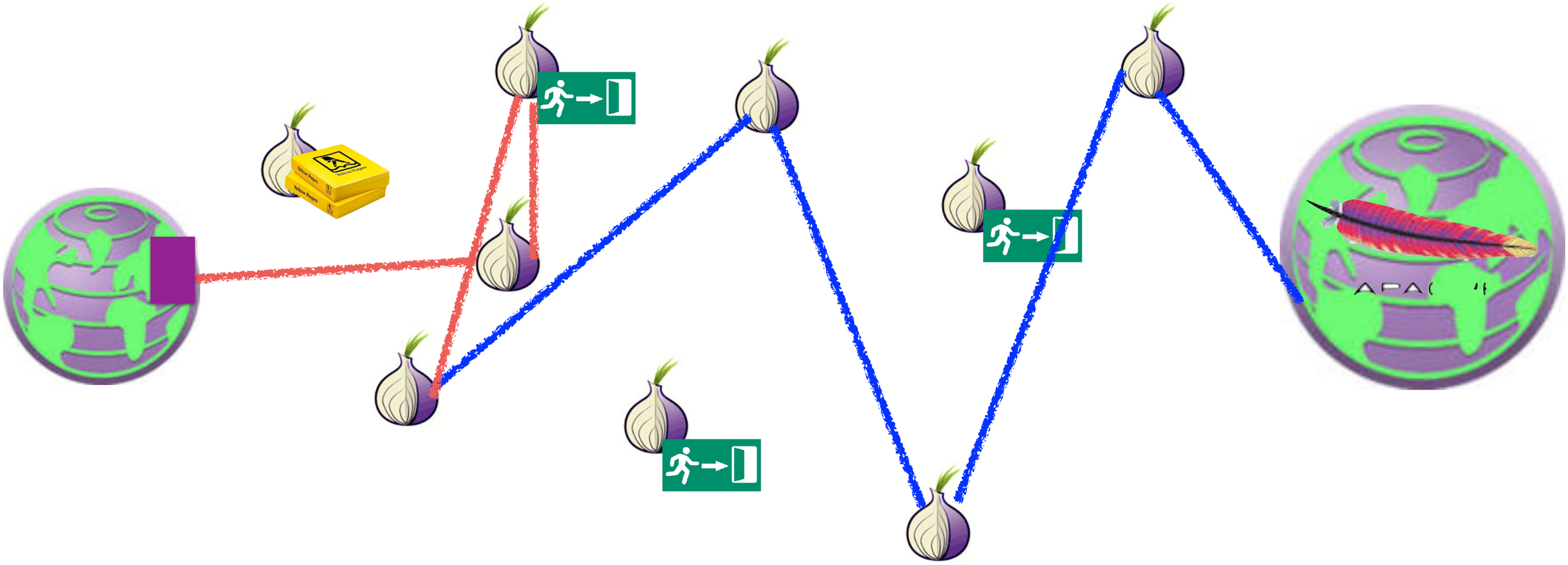
Tor Hidden Service: Setting Up Introduction Point



Tor Hidden Service:
Query for Introduction, Arrange Rendevous



Tor Hidden Service: Rendevous and Data



Home | Alphabay Market | About Tor

pwoah7foa6au2pul.onion/index.php

Search

AlphaBay Market

Logged in as seanbridges
Balance: BTC 0.0000 / XMR 0.0000
Autoshop Logout

▲USD 573.53 ▲CAD 735.76 ▲EUR 506.38 ▲AUD 753.03 ▲GBP 437.84

HOME SALES MESSAGES ORDERS LISTINGS BALANCE FEEDBACK FORUMS API SUPPORT

Home

seanbridges

Joined: Aug 30, 2016
Trust level: Level 1
Total sales: USD 0.00
Total orders: USD 0.00

Search: Search

⚠ We **highly recommend** that you disable Javascript when viewing the marketplace for better security.

CC / ACCOUNT AUTOSHOP

Access the CC autoshop

Access the account autoshop

BROWSE CATEGORIES

Fraud	25438
Drugs & Chemicals	136335
Guides & Tutorials	10029

Featured Listings

[FE 100%] ▶ FRESH CC/CVV USA VISA/MASTERCARD /DISCOVER/AMEX (OLD MAGIC QUALITY/VALIDITY) - (New Stock OF CC +10K) - (Delivery Instantly) - (Always Online)

[Bulk] USA HIGH LEVEL CC - VISA RANDOM CREDIT - BUSINESS/SIGNATURE /PLATINUM [AUTO FULFILL ON - DAILY SUPPORT] Browse store for more types and levels CCs!
 # 6329 - CVV & Cards - st0n3d

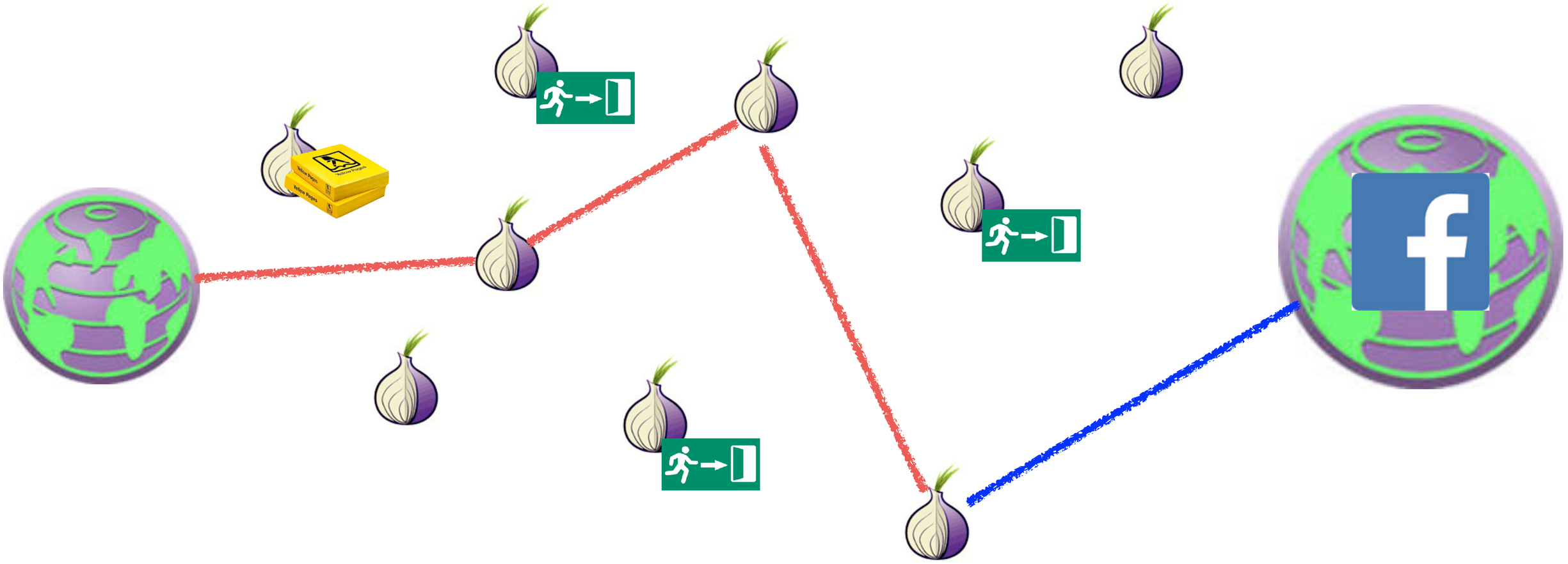
[MS] EDITABLE HQ TEMPLATES OF DOCUMENTS WORLDWIDE - GET VERIFIED EVERYWHERE INSTANTLY! - OVER 250 TEMPLATES TO CHOOSE FROM, SAMPLES ON ymhulceusuzrj3i5.onion

Double Your Bitcoins in ONE Day ! GUARANTEED! (2 in 1) $7000+ in 20 TWENTY MINUTES (50 + COPIES SOLD 100% POSITIVE FEEDBACK!)
 # 183848 - Other - BitcoinThief
Buy: USD 600.00

Remarks…

- A hidden service wants to keep the guard node constant for a long period of time…
  - Since the creation of new circuits is far easier to notice than any other activity
- Want to use a different node for the rendezvous point and introduction
  - Don’t want the rendezvous point to know who you are connecting to
- These are ***slow!***
  - Going through 6+ hops in the Tor network!

Non-Hidden Tor Hidden Service: Connect Directly to Rendezvous



Non-Hidden Hidden Services Improve Performance

- No longer rely on exit nodes being honest
  - No longer rely on exit node bandwidth either
- Reduces the number of hops to be the same as a not hidden service
- Result: Huge performance win!
  - Not slow like a hidden service
  - Not limited by exit node bandwidth
  - Facebook does this
- Any ***legitimate*** site offering a Tor hidden service should use this technique
  - Since legitimate sites don't need to hide!

Real use for ***true hidden*** hidden services

- "Non-arbitrageable criminal activity"
  - Some crime which is universally attacked and targeted
    - So can't use "bulletproof hosting", CloudFlare, or suitable "foreign" machine rooms
- Dark Markets
  - Marketplaces based on Bitcoin or other alternate currency
- Cybercrime Forums
  - Hoping to protect users/administrators from the fate of earlier markets
- And worse...

The Dark Market Concept

- Four innovations:
- A censorship-resistant payment (Bitcoin)
  - Needed because illegal goods are not supported by Paypal etc
- An eBay-style ratings system with mandatory feedback
  - Vendors gain positive reputation through continued transactions
- An escrow service to handle disputes
  - Result is the user (should) only need to trust the market, not the vendors
  - The market is *shifting* trust, not eliminating it
- Accessable *only* as a Tor hidden service
  - Hiding the market from law enforcement

The Dark Markets: History

- All pretty much follow the template of the original “Silk Road”
  - Founded in 2011, Ross Ulbricht busted in October 2013
- The original Silk Road actually (mostly) lived up to its libertarian ideals
  - Including the libertarian ideal that if someone rips you off you should be able to call up the Hell’s Angels and put a hit on them
    - And the libertarian idea if someone is foolish enough to THINK you are a member of the Hell’s Angels you can rip them off for a large fortune for a fake hit
- Since then, markets come and go...
  - And even information about them is harder:
    Reddit no longer supports them, deepdotweb got busted...
    Leaving "Dread": Reddit as a Tor Hidden Service

The Dark Markets: Not So Big, and ***Not Growing!***

- Kyle Soska and Nicolas Christin of CMU have crawled the dark markets for years
  - These markets ***deliberately*** leak sales rate information from mandatory reviews
- So simply crawl the markets, see the prices, see the volume, voila…
- Takeaways:
  - Market size has been relatively steady for years, about $300-500k a day sales
    - Latest peak got close to $1M a day
  - Dominated by Pot, MDMA, and stimulants, with secondary significance with opioids and psychedelics
  - A few sellers and a few markets dominate the revenue: A fair bit of “Winner take all”
    - But knock down any “winner” and another one takes its place

The Scams…

- You need a reputation for honesty to be a good crook
  - But you can burn that reputation for short-term profit
- The “Exit Scam” (pioneered by Tony76 on Silk Road)
  - Built up a positive reputation
  - Then have a big 4/20 sale
  - Require buyers to “Finalize Early”
    - Bypass escrow because of “problems”
  - Take the money and run!
- Can also do this on an entire ***market*** basis
  - The “Sheep Marketplace” being the most famous

And Now Once Again a ***SERIOUS*** Content Warning...

- The rest of the lecture is going to talk about the Elephant in the Room with Tor...
  Tor hidden services facilitate child abuse on an industrial scale
  - And the Tor project ***DOES NOT CARE***!
- I will be talking about actual cases and the scope of the problem
  - I studied these cases because they touched on significant policy issues surrounding searches and government hacking
- This will not be on the test beyond the following:
  "Nick hates Tor's Hidden Services with the fires of a thousand suns"
  and this is why...
  - And for the love of everything do not ever build something that has proved as loathsome as Tor

February 2, 2020, Sunrise, Florida

- A team of FBI agents in the Violent Crimes Against Children division, including special agents Daniel Alfin and Laura Schwartzenberger, attempted to serve a search warrant as part of a CSAM (Child Sexual Abuse Material) investigation
  - Agents Alfin and Schwartzenberger were murdered by the suspect and three other agents injured
- I knew Dan professionally from his previous work involving CSAM and Tor...

The "Playpen" Investigation

- In 2015 the FBI managed to identify and capture the server hosting the "Playpen" child exploitation site:
  Daniel Alfin was one of the lead investigators
- Playpen operated as a hidden service image board for posting CSAM
  - 250,000+ registered users, 20,000+ images
  - This represents thousands of abused children!
- But the site operator's are not the only problem...
  The site users are a problem
  - A significant number are "hands-on" abusers:
    Both because of their predilections and because creating new "content" is currency in these communities

To Deanonymize the Users...

- The FBI took over Playpen and ran the site for 2 weeks
- During those two weeks...
  - Disabled posting of new content, but continued to serve old content...
  - And added a post-login bonus: A zero-day attack on the Tor Browser Bundle
- Exploit payload: "phone home"
  - Not a general purpose shellcode, instead collect Ethernet Addresses, current user, and similar identifying information and contact an FBI server
- FBI calls this a NIT: "Network Investigation Technique"
- They had a warrant:
  - It described with particularity what it would search for, how it would work conceptually, etc...

Significant Impact

- 25 producers prosecuted, 350 arrests in the US alone
- Nearly 300 children identified or rescued from abusive situations worldwide, over 50 in the US
- But also two significant controversies:
- Was the warrant actually valid?
  - Answer ended up being "No, but 'good faith'....":
    At the time there was no way to write a warrant that says "I want to search these computers, but we don't know where they are!"
- What should defendants be able to examine with regard to the exploit?
  - Answer largely ended up being "No, not actually relevant"
  - An in the weeds discussion by Susan Hennesey and myself is available here: https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques

The Problem:
These are communities of abusers

- There have been others both before and since
  - Before Playpen there was "Freedom Hosting": hosted close to 50 CSAM sites.
    If you want to be nauseated read the Freedom Hosting NIT warrant application
  - In 2017 an FBI style NIT was deployed on "GiftBox" (probably by the French):
    But it was captured by a site user and posted to Reddit...
  - In 2018 "Welcome to Video" was busted: Pay for CSAM with Bitcoin!
    Again, if you want to vomit read the indictments
- Communities create dangerous cycles of normalization
  - And larger communities are more dangerous:
    See more mild versions that happened on Reddit with TheDonald, jailbait, creepshots, etc...
    - Self reinforcement behavior: "Its normal because others in the community do it" and the community becomes self justifying
    - See the "Jailbait" analysis in ***Twitter and Tear Gas***
  - Drives to extremes: Over the past decade, the age of CSAM victims has basically gotten younger... To the point where average age really can't get much lower

The Problem #2:
The Tor Project ***JUST DOES NOT CARE!***

- They treat this as "collateral damage" with a series of excuses.
  Here are actual justifications by Roger Dingledine (Founder):
- "But hidden services are in their infancy"
  - And in the same presentation talk about it being a 10 year old idea...
- "But hidden services are end-to-end authenticated"
  - Yeah, there is this thing call TLS...
- "But hidden services work through NATs"
  - Yeah, there is this thing called uPNP: You ask the NAT to allow inbound connections
  - Oh, or just use EC2...
- "But dissidents..."
  - Well, running Tor is very noticeable...
  - Plus you can "arbitrage host": Want to piss off China? Host in the US. Piss off the US? Host in Russia...
- "But Facebook/SecureDrop/Etc... has an onion service"
  - Uh, they don't actually need to be hidden! And work better when they aren't!

And A Different Problem: Grooming

- I never encountered Agent Schwartzenberger, but this was her specialty...
  people who use electronic chat to groom child victims for exploitation
- In unencrypted chats, the chat-provider can ***theoretically*** try to detect this behavior
  - A case where classic Machine Learning tends to work pretty well if the results are human-reviewed for false-positives
- The problem grows even harder when dealing with encrypted chats
  - Since there is no longer a central server that can try to detect the behavior...
  - And the developers would probably resist adding an AI-snitch to the client

So Remember:
Child Abuse IS REAL

- Too often those in favor of security/privacy view claims about child abuse and CSAM as disingenuous...
  - It isn't helped that those wanting encryption backdoors will use claims about child abuse and CSAM in a disingenuous manner!
- But these problems are real
  - Grooming over messenger systems is a serious problem
    - Usually starting over some open system where children frequent...
    - Before moving onto encrypted messengers like iMessage and Facebook Messenger
  - Tor hidden services have created a CSAM "industry"