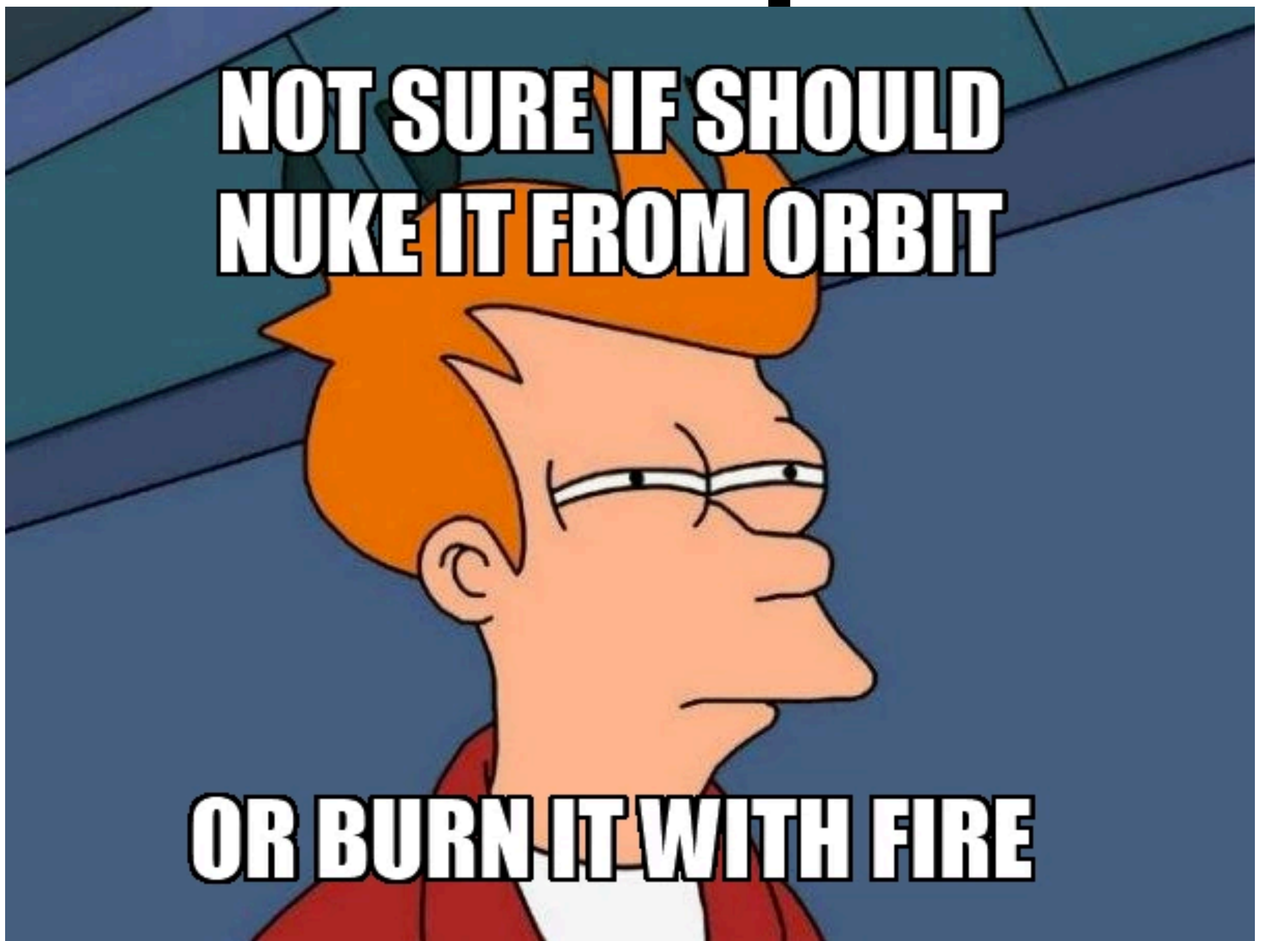
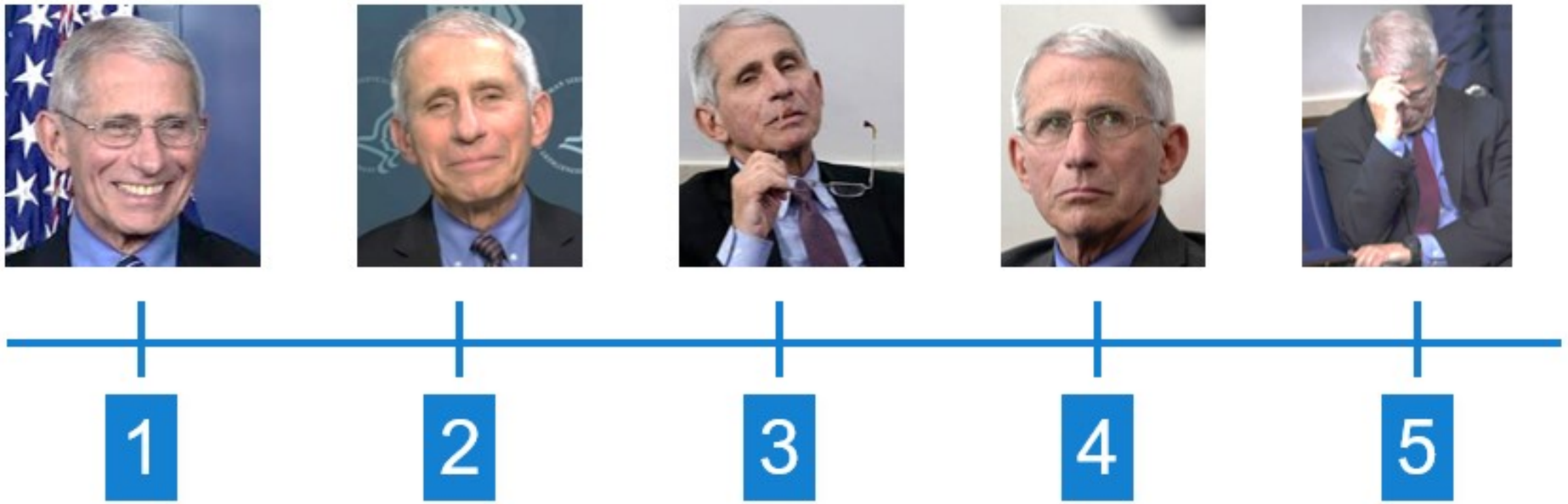
Misc Topics



Welcome to Hell Week....

- Mental pressure of "Curl up in a ball with a rifle" vs "Pretend everything is normal"
  - But at this point in the morning it is looking like Y2K...
- In Y2K we had to upgrade a ***ton*** of computing systems which used 2-digit dates
  - It ***could*** have been an utter disaster...
  - But everybody spent a ton of effort and as a consequence, ***almost nothing happened***
- Nevertheless, today is Off Topic Stuff:
  - 737 Max
  - Quantum
  - Nukes
  - Tor Hidden Services

And Checking In With Everyone...
How Are You on the Fauci Scale?



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...

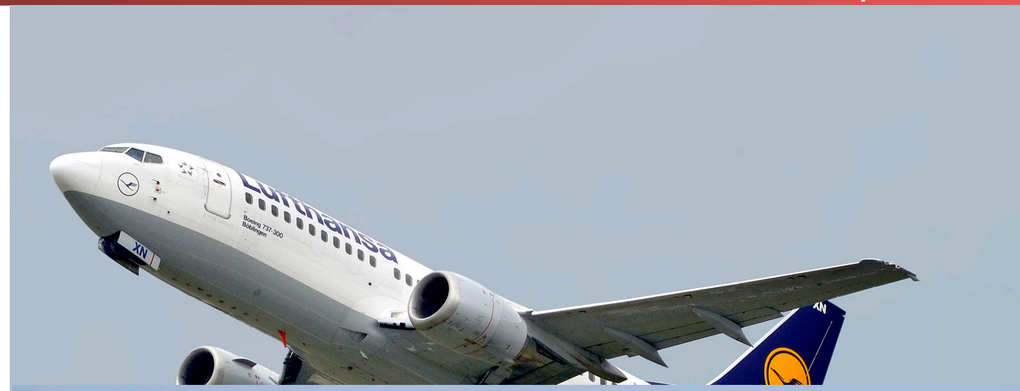
- A rough rule of thumb I once heard about an airline's costs:
  - 1/3 for fuel
  - 1/3 for people
  - 1/3 for the aircraft
- And the business is brutally competitive
  - Warren Buffett once joked that if he had a time machine he'd take a shotgun to the runway at Kitty Hawk to save subsequent investors 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

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...
- 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, t he 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...

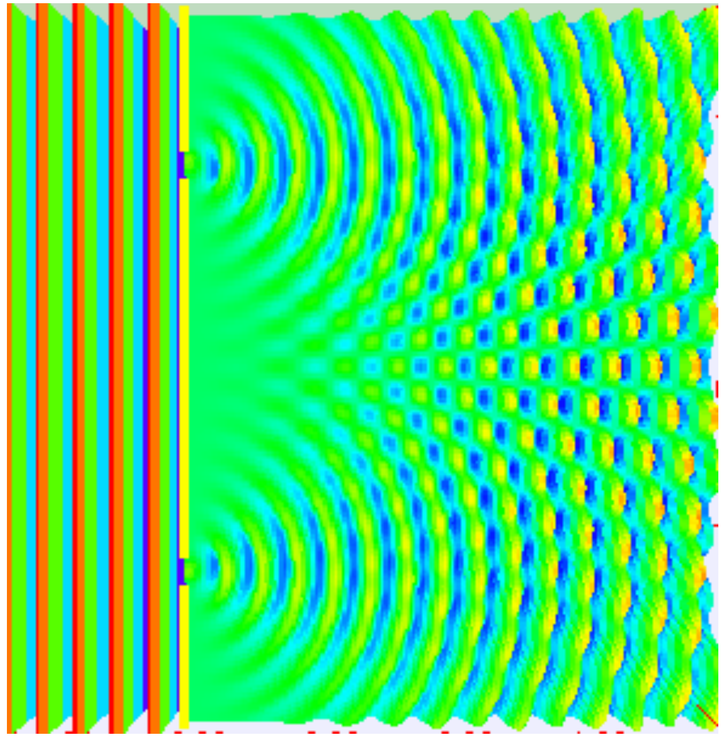
- It is a massive Charlie Foxtrot of epic proportions
- If it was an American or Southwest plane involved, there would already be indicted executives
- Every system on the 737-Max that changed needs to be viewed with suspicion
  - And I won't fly on one for at least 3 years post recertification.

Quantum Mechanics: The Weird Reality...

- At the scale of individual atoms, our intuition breaks down...
  - Things behave like both particles and waves
  - Things can pass through other things
  - Things can be in multiple states at once
  - Probabilities matter
- I don't think anyone really intuitively ***understands*** Quantum...
  - But it works...
- Disclaimer: I'm a failure at Quantum:
  - I got a C (I deserved an F) in Physics 137A, this is truly weird stuff!

Example Weirdness: The Double Slit Experiment

- If you beam a light at a set of double slits
  - You get a wave diffraction pattern 🙂
- If you bean a beam of electrons...
  - You get a wave diffraction pattern?! 🤔
- But light is composed of "photons" and electrons are clearly particles
  - If you send them one at a time, each one arrives at single points, but…
  - Taken together you get a diffraction pattern 🤷‍♂️
- But if you ***measure*** which slit each particle went through...
  - You eliminate the diffraction pattern!
  - Single electrons and photon "particles" are interfering ***with themselves*** like a wave does! 😐



So What Does This Mean?

- Things are both particles and waves?!?
- Things can be in two places at once?
- When you measure something, it behaves differently?
- EG, Schrodinger's cat...
  - A thought problem: You have a cat in a sealed box, a vial of poison, and a single radioactive atom...
    - At time T, there is a 50% chance the atom decayed, broke the poison, and killed the cat
  - Is the cat alive? Dead? Both?
    - "Yes", until you open the box!

Another Weirdness: EPR entanglement

- Einstein ***hated*** quantum mechanics...
  - "God does not play dice with the universe"
  - Plus his genius idea, relativity, doesn't actually work with quantum...
    - If you can unite general relativity and quantum mechanics, you are getting a flight to Sweden to pick up your Nobel prize
- Einstein–Podolsky–Rosen came up with a "paradox"...
  - The "EPR pair"
  - Intended to go "See, this Quantum 💩 makes no sense..."
  - The problem is, it actually ***works!***

EPR "Paradox" in action

- We have two particles, A and B...
  - A is in an unknown state, 50% of the time A = 0, 50% of the time A = 1
    - Really, A is in a superposition of both states:
      The cat is alive and dead
  - If we measure A, we have a 50/50 chance at the time of measurement
  - But until we measure A, it continues to exist as probabilistic superposition of both states
- We then "entangle" B without measuring A
  - So that A=0 <-> B=0 and A=1 <-> B=1
  - And then separate the two, perhaps even by light years distance!
- Now when we measure
  - If A = 0 we will ALWAYS see B =0…
    - But if A = 1 we will see B = 1
- And it doesn't matter which way we order our observations
  - and it is still random which one it is?!?

As long as we maintain coherence...

- We can keep this up!
  - So lets take several bits, B_0, B_1, B_2
  - Put each one in an independent 50/50 state. These are now qbits (Quantum Bits)
- Now we do a computation:
  - $B_3 = B_0 \oplus B_1 \oplus B_2$
  - But while maintaining coherence
- Now the spooky thing...
  - We've really computed all quantum superposition of all possible values of B_3 as a function of B_0-B_2...
    - In hardware language it is like we computed the ***entire*** truth table in one go and things are existing in that superposition
- But if we ***measure*** them, we get just a single input/output pair

And Now The Quantum Miracle...

- So far, this is no more powerful than a conventional computer
  - After all, we still only get a single output for a single set of inputs...
- But then we get to the Quantum magic...
- We now take B_0-B_3 and pass them through another transformation
  - That basically self-interferes between the superposition of all the input/output pairs
- And now when we look...
  - We see some information about the ***relationship*** between all the bits!
- But we need to maintain this in a quantum state (coherence) to work...
  - Any little noise or interaction with the outside world and the wave function collapses to a single Input/Output pair!

So What Good Is This?

- Shor developed an algorithm to solve two different & related group theory problems
  - Find the order of a group
    - Given a group ***G***, a generator ***g***, how many elements are in the group?
    - You can reduce factoring to this problem
  - Find the discrete log
    - Given a group ***G*** of known order, a generator ***g***, and a value g^x mod ***G***, what is ***x***?
- The number of quantum bits (qbits) required:
  - $O((\log N)^2 (\log \log N) (\log \log \log N))$ with ***N*** the number to be factored
  - So still a lot of quantum state: millions of qbits for a 2048b RSA key
- Oh, and this is just about the only thing it is good for

This Breaks All Major Public Key

- Diffie/Hellman: Break discrete log
- RSA: Break factoring
- Elliptic Curve
  - It's more complicated because you don't know the order of the group...
  - Well, its not actually. See the footnote on the "factoring" algorithm!
    - You use the RSA algorithm to get the order of the group
    - And then use the discrete log problem
- But what does this actually mean?

Implications #1: Is ECC better?

- In conventional computing: ECC is the same strength with fewer bits
  - 256b ECC ~= 2048b RSA & DH
    - There are sub-exponential shortcuts for the group-theory problems in the integers not present on elliptic curves
- But this isn't the case with quantum computing!
  - So if we could only build a "medium-sized-ish" quantum computer (tens of thousands rather than millions of qbits), ECC breaks first
- Speculation: Is this why in going from Suite B to CNSA, the NSA said...
  - "Whoah, hold off on going to ECC until we have post-Quantum public key... and until then you can use 3096b RSA and DH as well"

Implication #2:
Lots of work on "Post-Quantum Public Key"

- A major area of active research: public key algorithms without a quantum shortcut
  - Significantly larger keys: 400B (same as 3096b RSA) to 10,000B depending on the algorithm
- In practice, never used alone!
- EG, the "NewHope" TLS handshake experiment
  - Does both an ECDHE and post-quantum public key agreement: Both would have to be broken to break the system

Implication #3:
***Don't Worry*...**

- There may be exponential or near exponential difficulties in maintaining coherence as a function of the # of qbits
  - Open question: There is a lot of work on this, but 🤷.
  - I've heard "Quantum Computers Real Soon Now" for nearly 25 years!
- The current "Quantum" computers really aren't
  - D-Wave is actually "quantum annealing":
    2-D simulated annealing with Quantum acceleration. Open question whether it is fundamentally faster
  - Google's "Quantum Supremacy":
    Better than a classical computer at computing how it will compute?!?
    Again, only 2D not generic operations
- True generic quantum computers have been built...
  Capable of factoring "15"

Post Quantum Cryptography...

- Just because ***you*** don't need to worry...
  - Doesn't mean the cryptographers aren't worried
- So repeating the success of AES and SHA3:
  - A NIST organized contest to develop new algorithms
    Now a set of finalists
- Two main primitives:
  - Key exchange (analogous to Diffie/Hellman)
  - Signatures
- Designed to be used in concert with a conventional key exchange
  - That way you'd have to break both:
    Use ***KDF(PostQuantum || Classic)*** to generate the session keys

But What About "Quantum Cryptography"

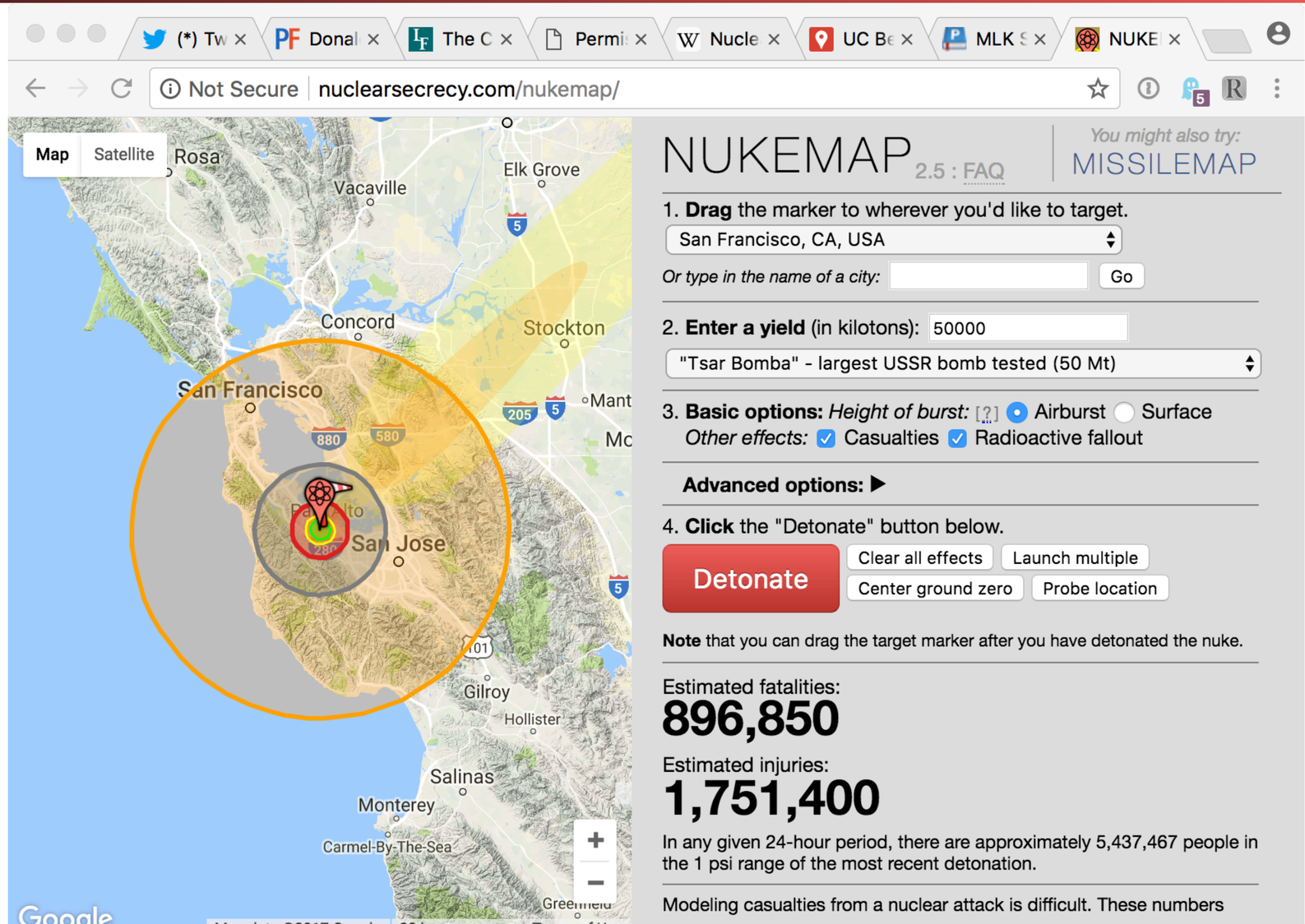
- Really, its Quantum Key Exchange...
- Take a single photon:
  - We can measure its polarization in either **+** or **X** orientation, and select it randomly
    - Gives us a single photon with a random polarization
  - We then transmit to the photon to the recipient... Who then does the same thing
- We then broadcast which orientations we used...
  - If they chose the different orientation, they end up with a random value
  - If they chose the same one, they end up with the ***same*** value...
    - But if there is an eavesdropper, an eavesdropper adds noise

Quantum Key Exchange is a Total Waste...

- Of course this requires sending single photons with no effective noise to a recipient
- If we can't build a large Quantum computer or break existing public key, it is completely worthless
- If we can build a large Quantum computer but can make post-Quantum public key work, it is completely useless
- If we can build a large Quantum computer and post-Quantum Public Key fails, it is ***still*** completely useless!
  - This only works for point to point, so you might as well just ship around USBs full of random key material!

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...

- 1960s-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...

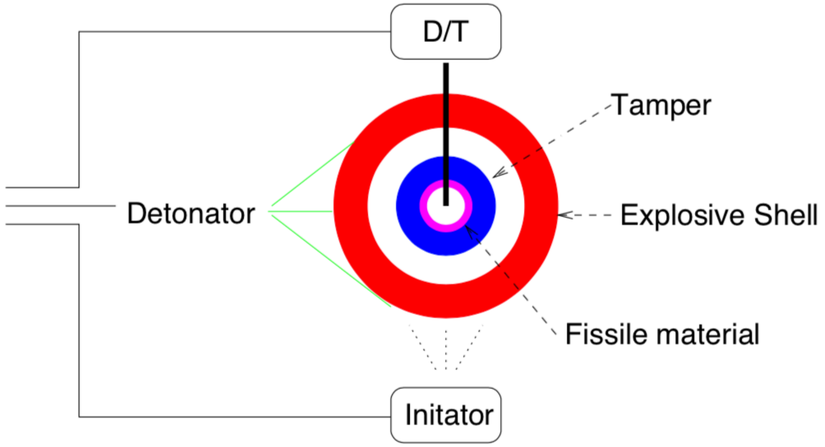
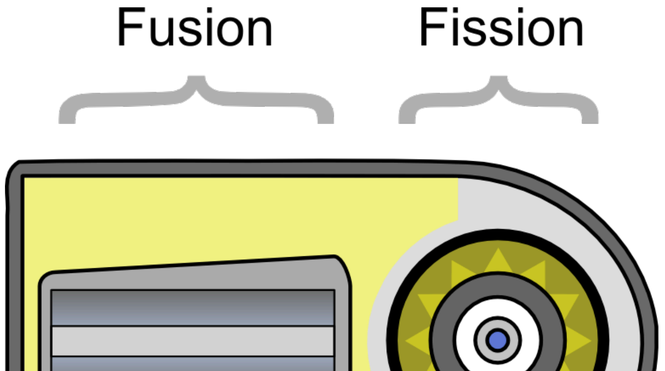


Diagram by Steve Bellovin

- 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

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...

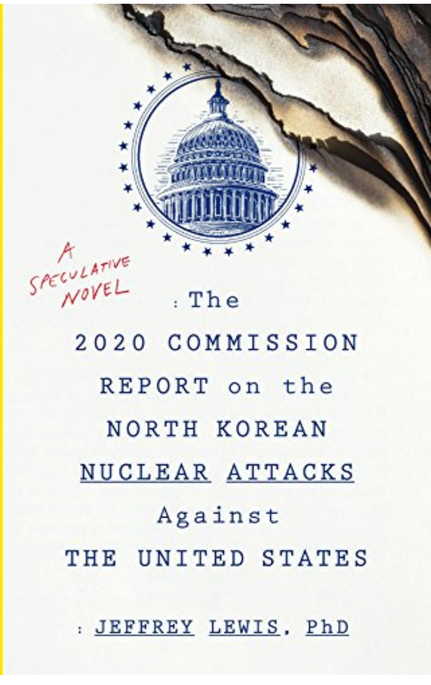
- Stick em on a rocket
  - This ***is*** rocket science: It is far easier to build the nuke than build the ICBM...
  - Alternatively, stick it on an unmanned miniature airplane ("Cruise Missile") or just hang it under a plane as a old-fashioned bomb
- Then stick the rocket on something
  - In a hardened 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 since Donald Trump doesn'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 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

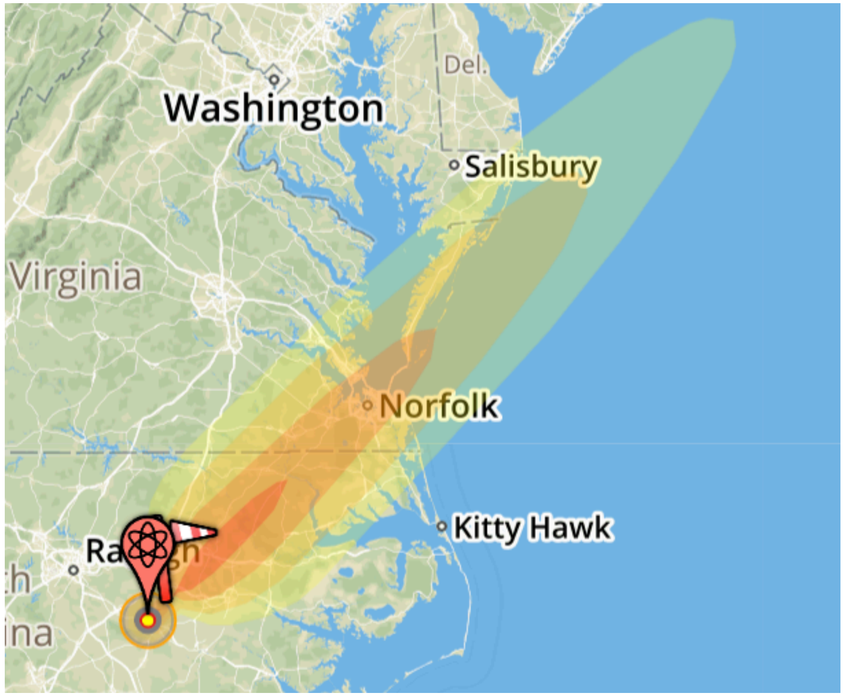
- The President has three items:
  - A “biscuit” of authentication codes kept on his person
  - The “football”: containing a menu of options for ordering a nuclear strike
  - An encrypted secure phone
- The President has a bad day…
  - He calls over the football
    - Picks out the menu option he wants 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)

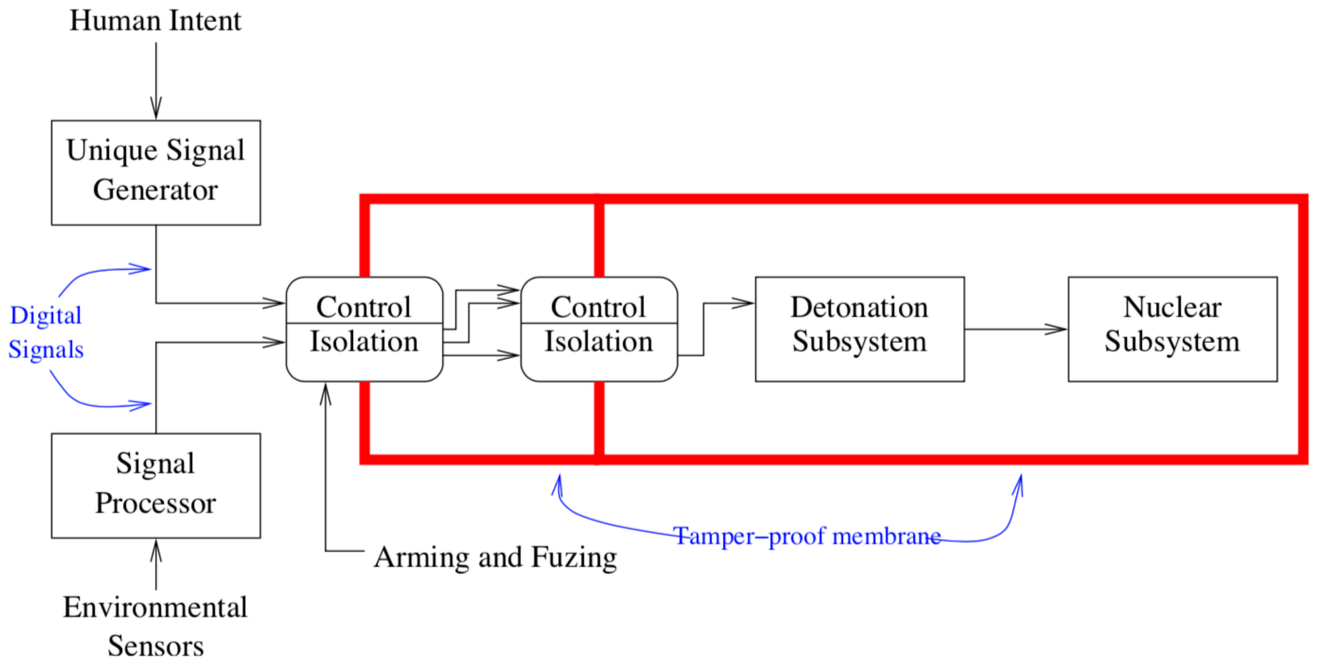
Nuke Safety Features

- 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
- 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

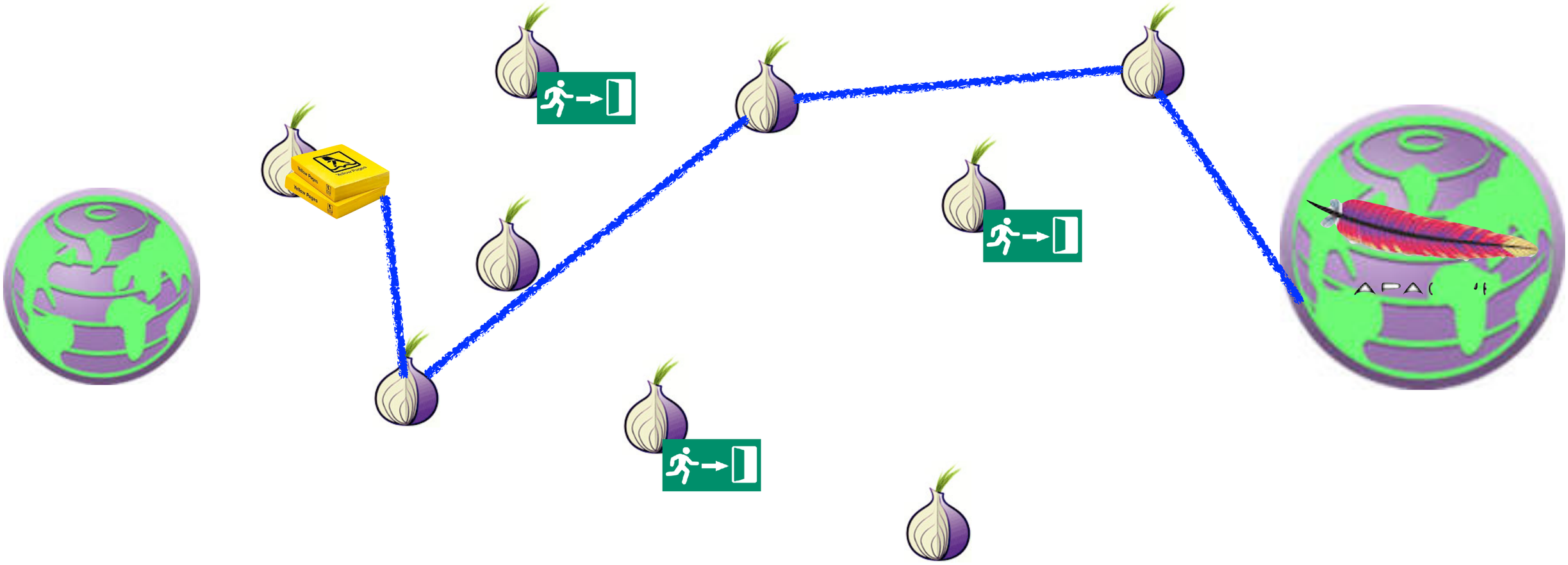
Steve Bellovin's Lessons Learned

- 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?

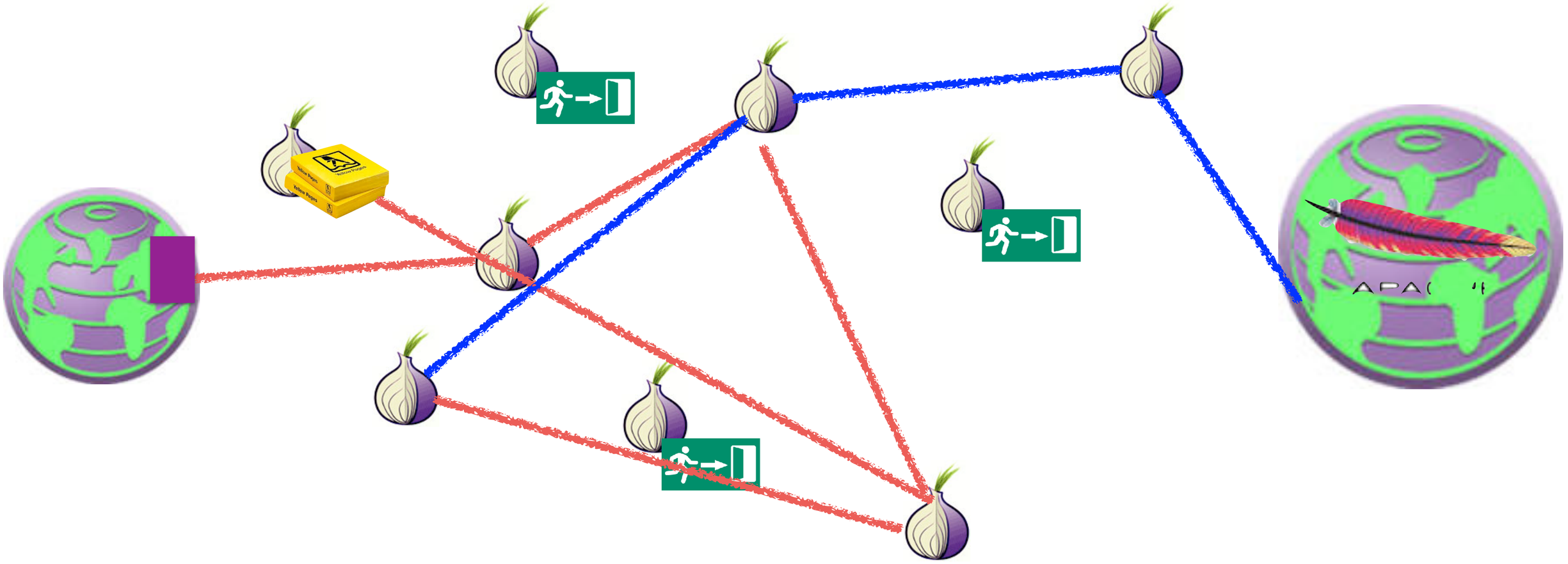
Tor Browser is also used to access Tor Hidden Services aka .onion sites

- Services that ***only*** exist in the Tor network
  - So the service, not just the client, has possible anonymity protection
  - The “Dark Web”
- A ***hash*** of the hidden service's public key
  - http://pwoah7foa6au2pul.onion
    - AlphaBay, one of many dark markets
  - https://facebookcorewwwi.onion
    - In this case, Facebook spent a lot of CPU time to create something distinctive
- 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

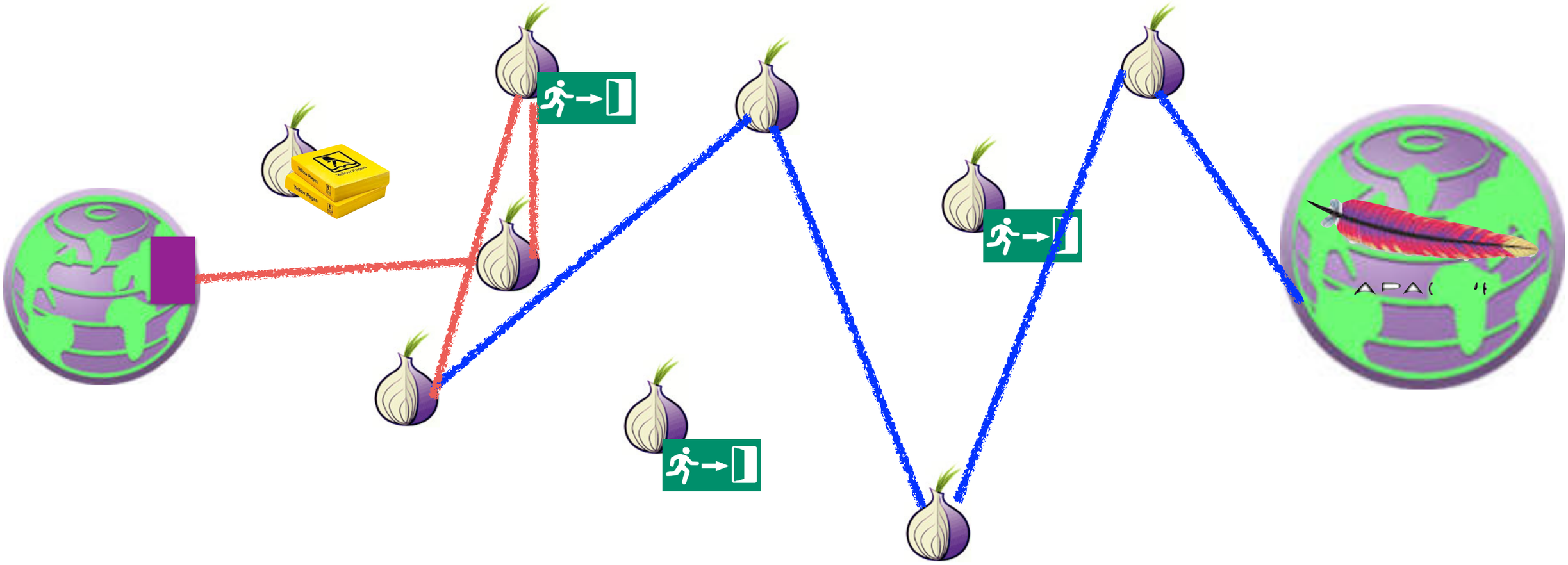
Tor Hidden Service: Setting Up Introduction Point



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

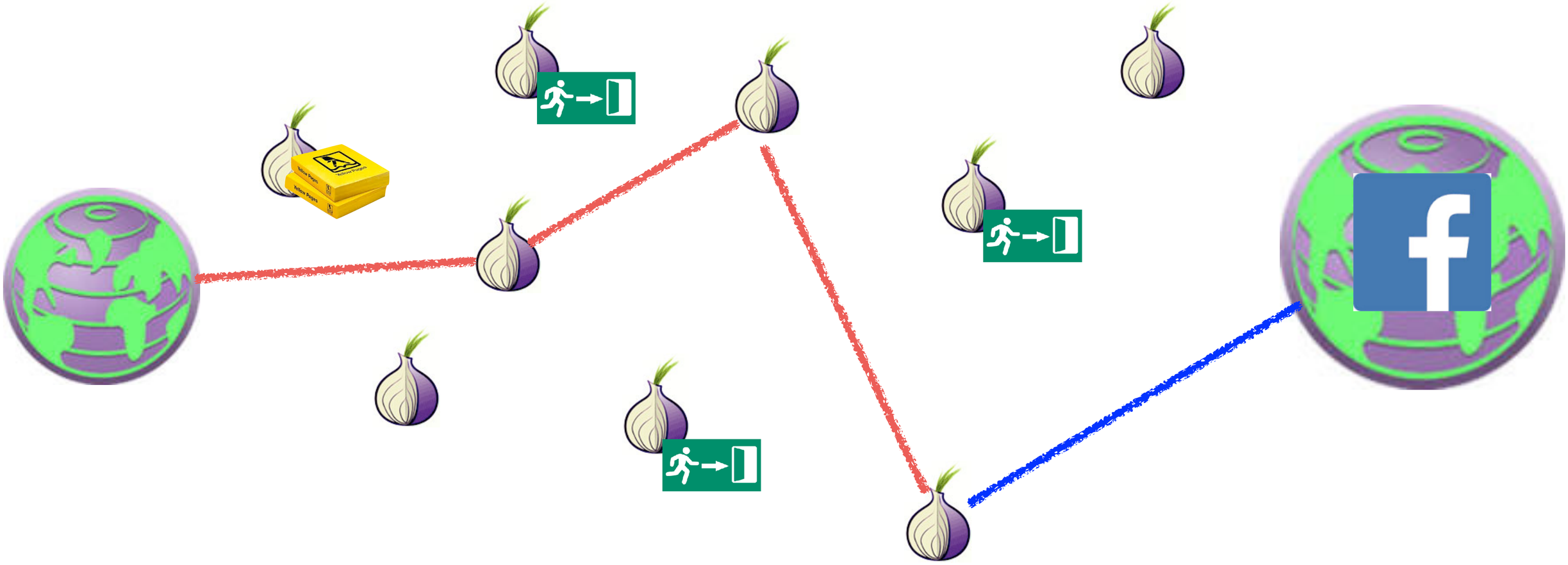
[MS] EDITABLE HQ TEMPLATES OF DOCUMENTS WORLDWIDE - GET VERIFIED EVERYWHERE INSTANTLY! - OVER 250 TEMPLATES TO CHOOSE FROM, SAMPLES ON ymhulceusuzrj3i5.onion

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…

- Want to keep your 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", CDNs like CloudFlare, or suitable "foreign" machine rooms:
      And since CloudFlare will service the anti-Semitic shitheads like gab.ai and took forever to get rid of the actual nazis of Stormfront and the murderous shits of 8chan...
- Dark Markets
  - Marketplaces based on Bitcoin or other alternate currency
- Cybercrime Forums
  - Hoping to protect users/administrators from the fate of earlier markets
- Child Exploitation

The Dark Market Concept

- Four innovations:
- A censorship-resistant payment (Bitcoin)
  - Needed because illegal goods are not supported by Paypal etc
    - Bitcoin/cryptocurrency is the ***only game in town*** for US/Western Europe after the Feds smacked down Liberty Reserve and eGold
- 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
- 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" (e.g. 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 then the Child Exploitation types

- This is ***why*** I'm quite happy to see Tor Hidden Services ***burn!!!***
  - Because these do represent a serious problem:
    The success against "PlayPen" shows just how major these are
- A far bigger systemic problem than the dark markets:
  - Dark markets are low volume, and not getting worse
    - Plus the libertarian attitude of "drug users are mostly harming themselves, its the drug-associated crime that is the problem"
      - No indication of any ***successful*** murder resulting from dark market activity
  - But these are harming others
- They are also harming Tor:
  Tor itself is a very valuable tool for many legitimate uses, but the presence of the child exploitation sites on hidden services is a stain on Tor itself

Deanonymizing Hidden Services: Hacking...

- Most dark-net services are not very well run...
  - Either common off-the-shelf drek or custom drek
- And most have now learned ***don't ask questions on StackOverflow***
  - Here's looking at you, frosty…
- So they don't have a great deal of IT support services
  - A few hardening guides but nothing really robust

Onionscan…

- A tool written by Sarah Jamie Lewis
  - Available at https://github.com/s-rah/onionscan
- Idea is to look for very common weaknesses in Tor Hidden services
  - Default apache information screens
  - Web fingerprints
  - I believe a future version will check for common ssh keys elsewhere on the Internet
- Its really "dual use"
  - .onion site operators should use to make sure they aren't making rookie mistakes
  - Those investigation .onion sites should use to see if the target site made a rookie mistake!

Deanonymizing Visitors To Your Site FBI Style

- Start with a Tor Browser Bundle vulnerability…
  - Requires paying for a decent vulnerability:
    Firefox lacks sandboxing-type protections but you have to limit yourself to JavaScript
- Then take over the site you want to deanonymize visitors to…
- And simply hack the visitors to the site!
  - With a limited bit of malcode that just sends a “this is me” record back to an FBI-controlled computer

A History of NITs

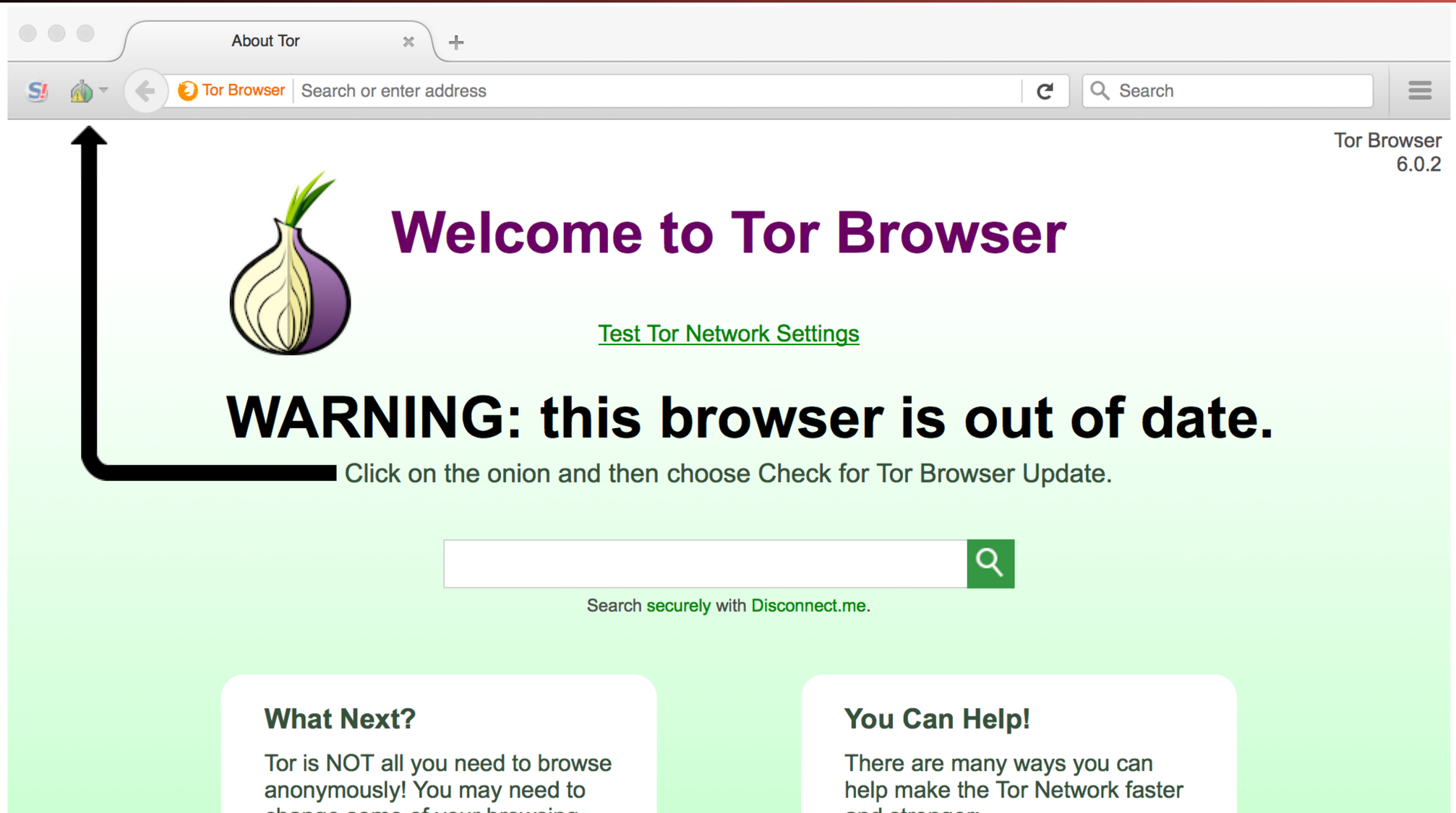
- The FBI calls their malicious code a NIT or Network Investigatory Technique
  - Because it sounds better to a magistrate judge than saying "we're gonna go hacking"
- The exploit attempts to take over the visitor's browser
- But the payload is small: just a "I'm this computer" sent over the Internet to an FBI controlled Internet address

A History of NITs: PedoBook

- The first known NIT targeting a hidden service was “PedoBook” back in 2012
  - Back then, many people used other web browsers to interact with Tor hidden services
  - NSA kept a database of these people, called ***EPICFAIL!***
- The NIT actually didn’t even qualify as malcode
  - And a ***defense*** expert actually argued that it isn’t hacking and probably didn’t actually need a warrant
- Instead it was the “Metasploit Decloaking” flash applet:
  - A small bit of Flash which contacts the server directly, revealing the visitor’s IP address

A History of NITs: Freedom Hosting

- The second big NIT targeted FreedomHosting
  - A hosting provider for Tor Hidden services with an, umm, generous policy towards abuse
    - Hosted services included TorMail (a mail service through Tor) and child porn sites
- FBI replaced the entire service with a NIT-serving page
- Fallout:
  - Very quickly noticed because there are multiple legit users of TorMail
  - Targeted an older Firefox vulnerability in Tor Browser
- Tor browser switched to much more aggressive autoupdates: Now you ***must*** have a zero-day for a NIT payload to work


About Tor
Tor Browser
Search or enter address
Search
Tor Browser
6.0.2
Welcome to Tor Browser
Test Tor Network Settings
WARNING: this browser is out of date.
Click on the onion and then choose Check for Tor Browser Update.
Search securely with Disconnect.me.
What Next?
Tor is NOT all you need to browse anonymously! You may need to
You Can Help!
There are many ways you can help make the Tor Network faster

A History of NITs: Playpen

- The big one: PlayPen was a hidden service for child pornographers
  - In February 2015, the FBI captured the server and got a warrant to deploy a NIT to logged in visitors
    - The NIT warrant is public, but the malcode itself is still secret: >100,000 logins!
- What we do know:
  - This was big: hundreds of arrests, many abuse victims rescued
  - It almost certainly used a zero-day exploit for Tor Browser
- Courts are still hashing this out over two big questions
  - Is it valid under Rule 41?
    - ***Most*** have conclude "no, but a technical not constitutional flaw":
      Good faith says that previous violations are OK, but not future violations
  - Does the defense have a right to examine the exploit?
    - I'll argue no, but some defense attorneys have successfully used a graymail technique initially
      But followup hasn't replicated that success

A History of NITs: Three Years Ago

- Someone (probably the French police) captured a child porn site called the "GiftBox"
  - They modified it to serve up a NIT
- The NIT payload was almost identical to the one in the Freedom Hosting case
  - Suggesting assistance from either the FBI or the FBI's contractor
- The exploit was a ***new*** zero-day exploit targeting Firefox
  - Patch released within ***hours***
    - And yes, it was a C-related memory corruption (naturally)

NITs won't work well in the future against Tor!

- The current Tor browser is a ***hard*** target
- Hardening will require that breaking Tor browser, even to just send a "I'm here" message, will require a chain of exploits
  - An information leakage to determine the address of a function and enough content in that function to enable an attack (break ASLR)
  - PLUS a conventional vulnerability
  - And now the Firefox rendering engine got sandboxed too…
  - And add in darknet users who are running without JavaScript
- Upshot: the current FBI exploit will need a massive upgrade if it will work at all!
  - And future exploits will be ***vastly*** more expensive and rarer
  - We should thank the FBI for their very valuable contributions to software hardening