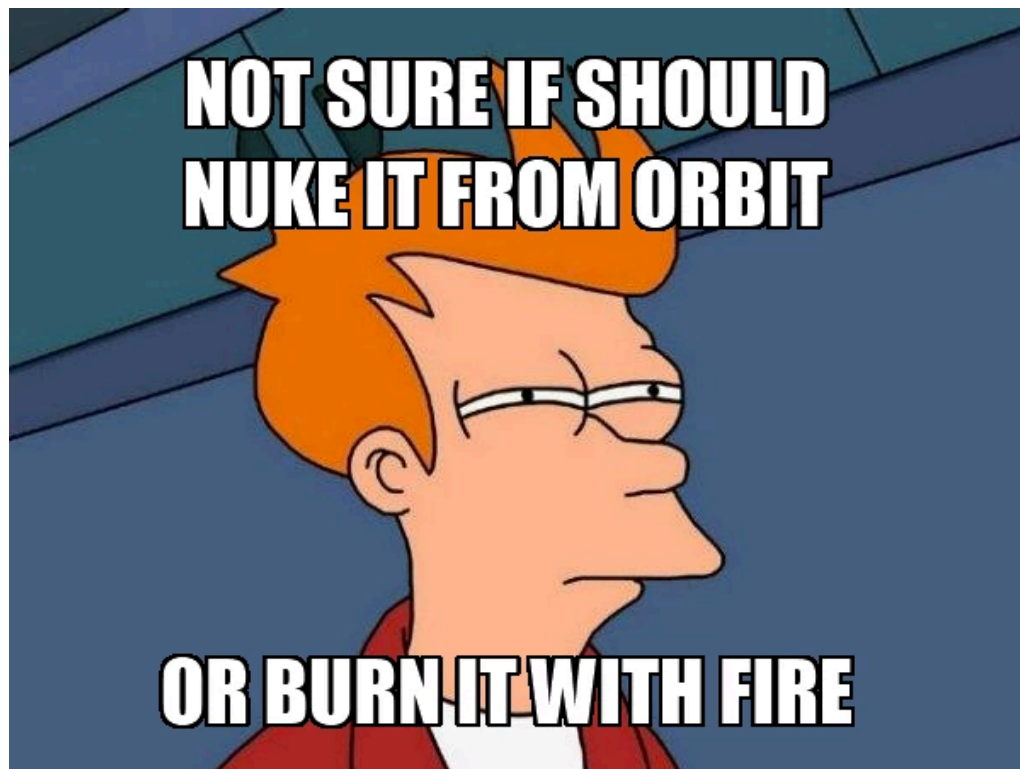


Tor + Nukes



Vox

recode

Why did Iran shut off the internet for the entire country?

After protesters railed against increased fuel prices, connectivity fell to just 5 percent. The *Reset* podcast investigates.

By **Delia Paunescu** | Nov 21, 2019, 7:40pm EST

[f](#) [t](#) [SHARE](#)



Iran imposed a nationwide internet outage after citizens flooded the streets to protest the government's hike in fuel prices. At least five people were killed in the demonstrations, which show no sign of subsiding. | ATTA KENARE/AFP via Getty Images

The Latest

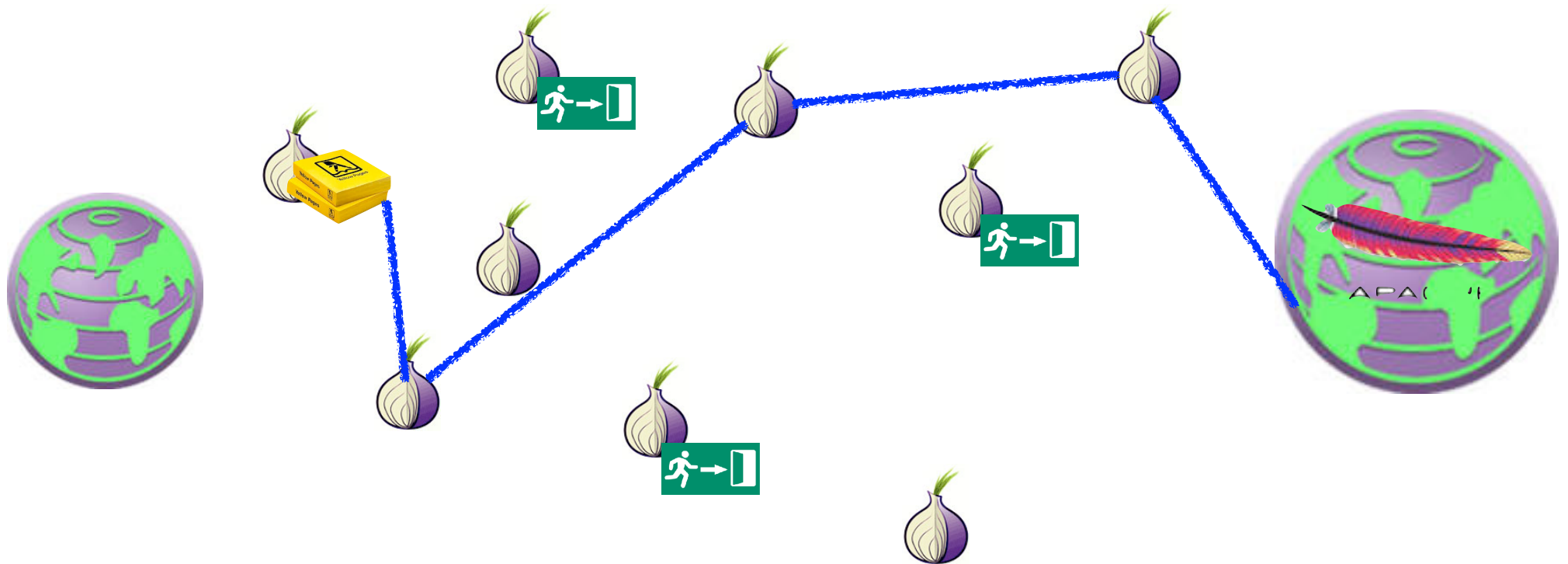


Barack Obama tells Silicon Valley's |

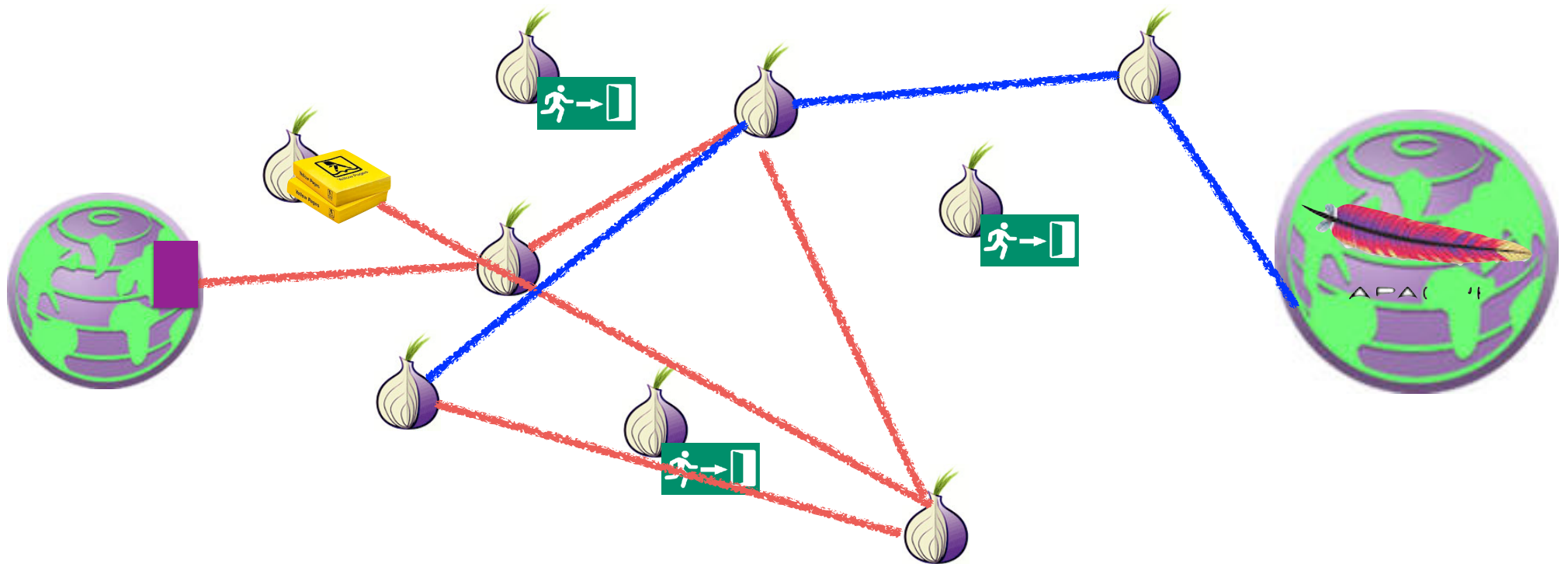
Tor Browser is also used to access Tor Hidden Services aka .onion sites

- 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://facebookcorewwi.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

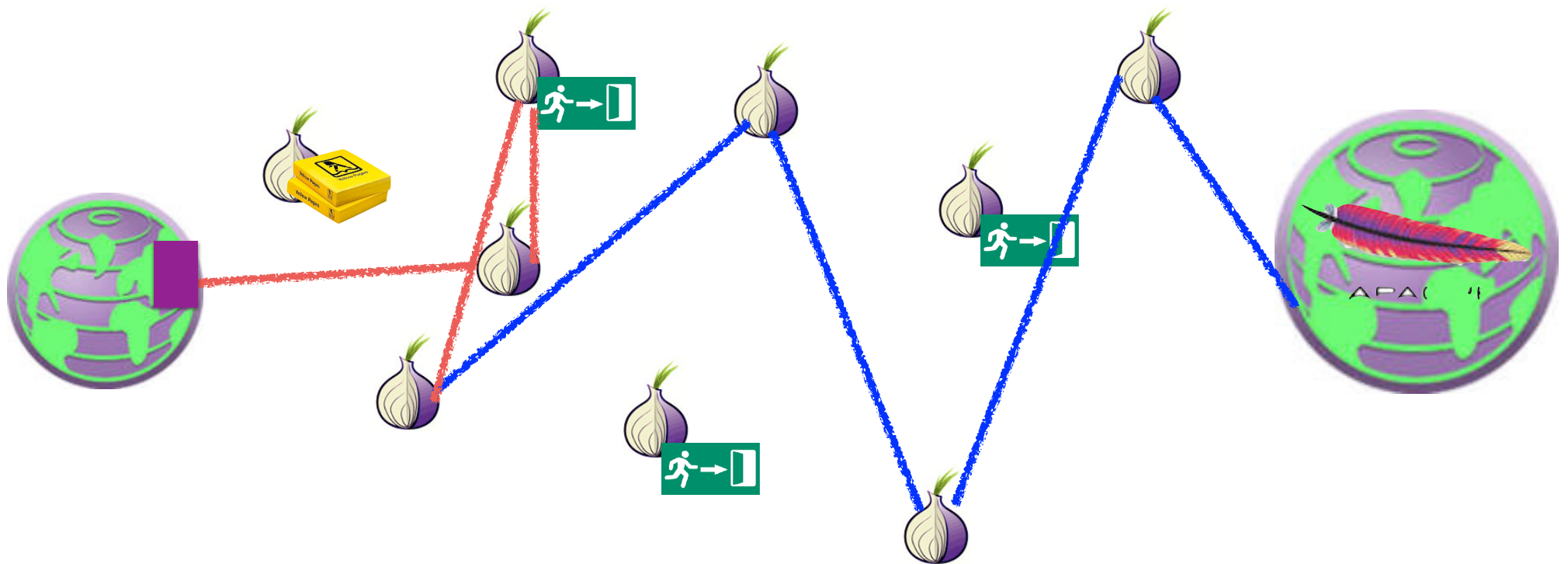
Tor Hidden Service: Setting Up Introduction Point



Tor Hidden Service: Query for Introduction, Arrange Rendezvous



Tor Hidden Service: Rendezvous and Data



Home | Alphabay Market x About Tor x +

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



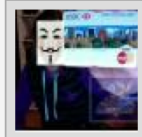

Home

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.

Featured Listings

 <p>[FE 100%] FRESH CC/CVX USA VISA/MASTERCARD /DISCOVER/AMEX (OLD MAGIC QUALITY/VALIDITY) - (New Stock OF CC +10K) - (Delivery Instantly) - (Always Online)</p>	 <p>[Bulk] USA HIGH LEVEL CC - VISA RANDOM CREDIT - BUSINESS/SIGNATUREWORLDWIDE - GET /PLATINUM [AUTO FULFILL ON - DAILY SUPPORT] Browse store for more types and levels CCs! # 6329 - CVV & Cards - st0n3d Buy USD 8.50</p>	 <p>[MS] EDITABLE HQ TEMPLATES OF DOCUMENTS VERIFIED EVERYWHERE INSTANTLY! - OVER 250 TEMPLATES TO CHOOSE FROM, SAMPLES ON ymhulceusuzrj3i5.onion # 51105 - Other</p>	 <p>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</p>
---	---	--	---

CC / ACCOUNT AUTOSHOP

Access the CC autoshop

Access the account autoshop

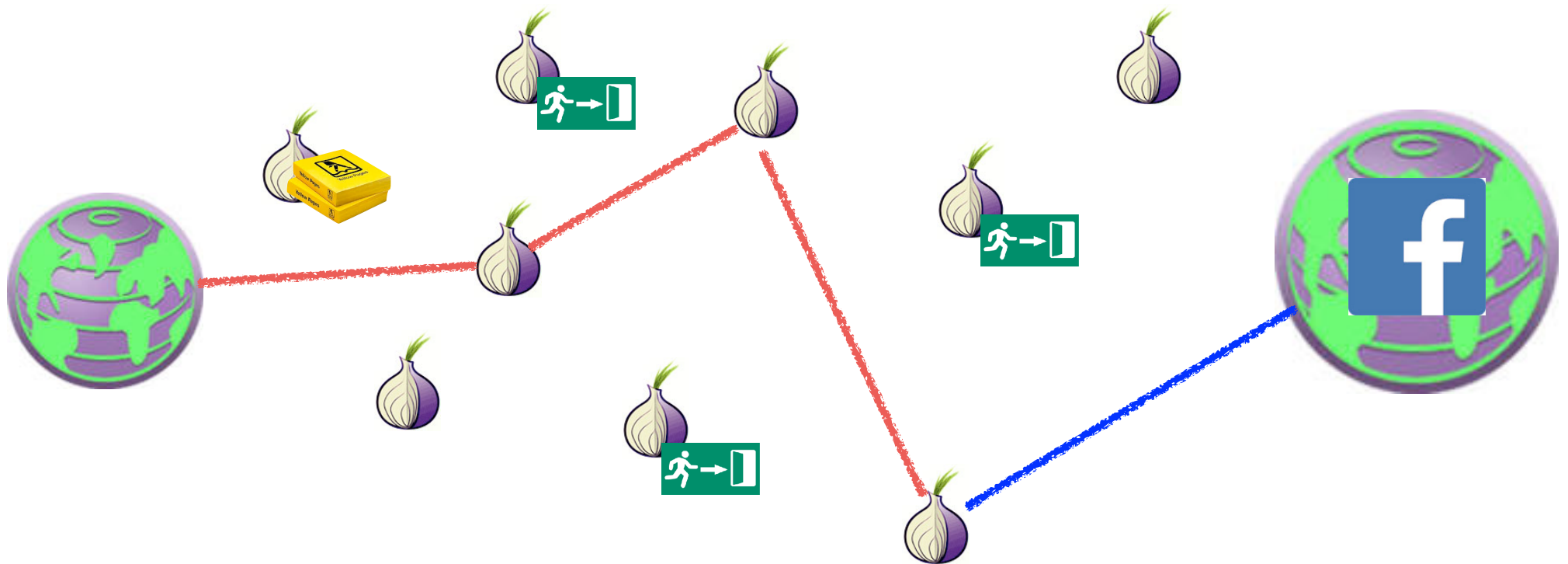
BROWSE CATEGORIES

- Fraud 25438
- Drugs & Chemicals 136335
- Guides & Tutorials 10029

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
- 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!

And That's Tor...

- Global view of the network
 - So the client can know every relay's keys
- Create hop-by-hop circuit and session keys
 - Starts out Client \leftrightarrow Hop1 (the "Guard node")...
 - Extend circuit to Hop2, create session key Client \leftrightarrow Hop2
 - Extend circuit to Hop3, create session key Client \leftrightarrow Hop3...
- Each hop decrypts/encrypts and forwards along the circuit
- Not that useful except for crooks
 - SLOW for censorship resistance
 - Good client anonymity but it just switches the adversary
 - Server anonymity only good for crooks

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

Computer Science 161 Fall 2019 Weaver

NUKEMAP 2.5 : FAQ You might also try: MISSILEMAP

1. **Drag** the marker to wherever you'd like to target.
San Francisco, CA, USA
Or type in the name of a city:
2. **Enter a yield** (in kilotons): 50000
"Tsar Bomba" - largest USSR bomb tested (50 Mt)
3. **Basic options:** Height of burst: [2] Airburst Surface
Other effects: Casualties Radioactive fallout

Advanced options: ▶

4. **Click** the "Detonate" button below.

Note that you can drag the target marker after you have detonated the nuke.

Estimated fatalities:
896,850

Estimated injuries:
1,751,400

In any given 24-hour period, there are approximately 5,437,467 people in the 1 psi range of the most recent detonation.

Modeling casualties from a nuclear attack is difficult. These numbers

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...
- **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

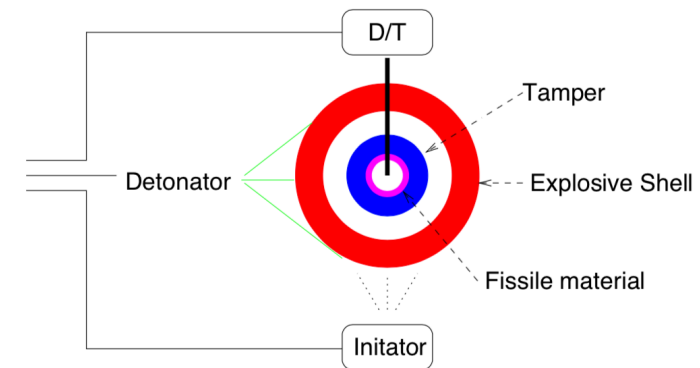
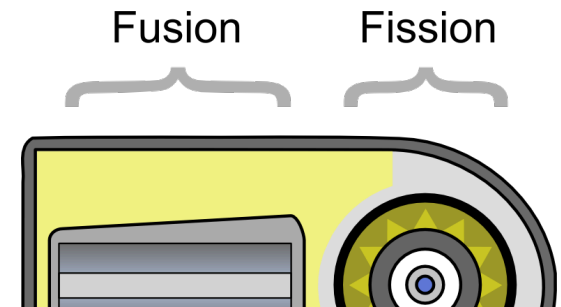


Diagram by Steve Bellovin

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...

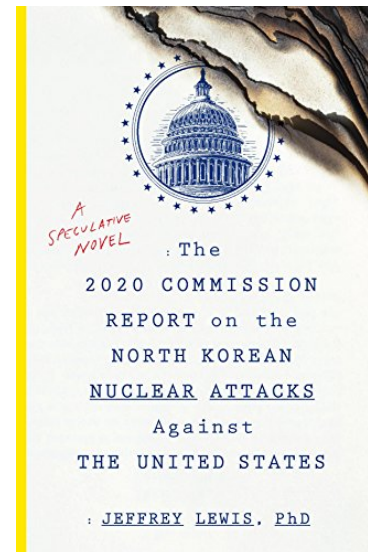
- Stick em on a rocket
 - This *is* rocket science: It is probably easier to build the nuke than build the ICBM...
 - Alternatively, stick it on an unmanned miniature airplane ("Cruise Missile") or just hang it under a plane as a old-fashioned bomb
- Then stick the rocket on something
 - In a hardened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



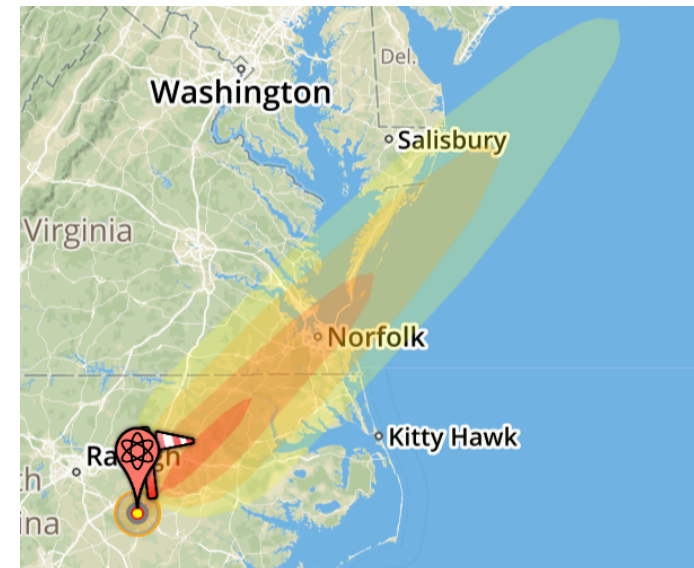
The Interesting Problem: Limiting Use

- 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)



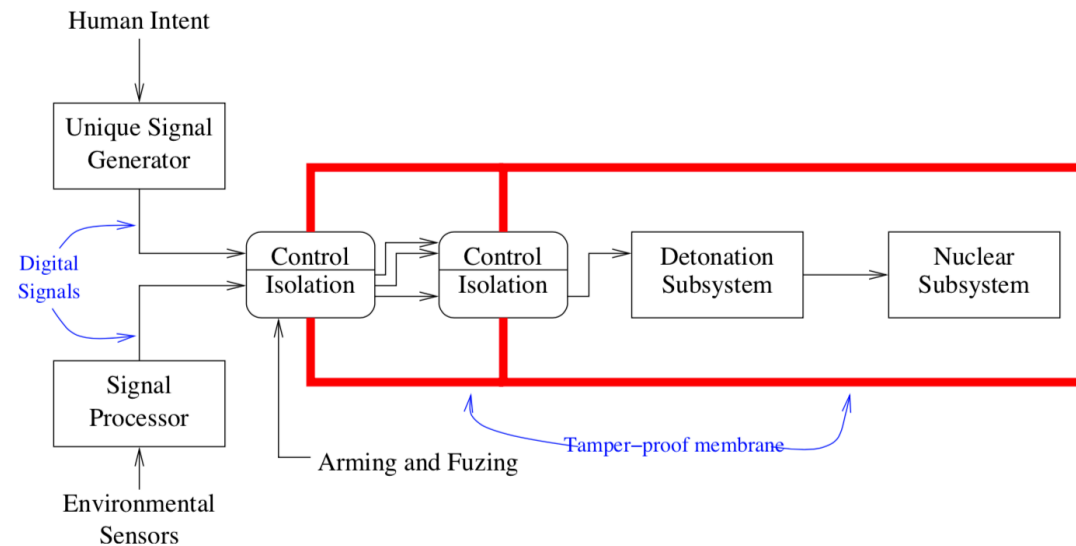
Nuke Safety Features

- 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?

Dragonfly...

- WPA2-PSK sucks...
 - An eavesdropper gains enough information for an **offline** attack on the pre-shared password
- What we really want is “Simultaneous Authentication of Equals”
 - Alice and Bob share the same password **PW**
 - Alice and Bob can negotiate a shared public-key based secret only if both know **PW**
 - If Alice or Bob doesn't know **PW**, then they don't learn anything about **PW** unless they successfully guessed **PW** during the protocol
- Enter Dragonfly (RFC 7664)
 - Has both EC and conventional DH based variants

DH-based Dragonfly

- Public parameters:
 - A prime p
 - A generator over this G
 - A (smaller) prime q
 - Size of the group defined by G and q is a large prime divisor of $(p-1)/2$
 - A selected generator g is valid if $g < p$ and $g^q \bmod p = 1$
- Identifiers for Alice and Bob
 - EG, MAC addresses, with an ordering function
- Key idea:
 - Select a *random* generator g , called P (or PE == Password Element) based on $H(ID_a || ID_b || PW)$
 - Hmm, I wonder where Nick got that idea for the WhyFi question? 🤔

Actually creating PE

```
found = False
counter = 1
n = len(p) + 64
do {
  base = H(max(Alice,Bob) | min(Alice,Bob) | password | counter)
  temp = KDF-n(base, "Dragonfly Hunting And Pecking")
  seed = (temp mod (p - 1)) + 1
  temp = seed ^ ((p-1)/q) mod p
  if (temp > 1)
  then
    if (not found)
      PE = temp
      found = 1
    fi
  fi
  counter = counter + 1
} while ((!found) || (counter <= k))
```

Remarks...

- Called “Hunting and pecking”:
 - Select a (pseudo)-Random element, check if its valid
 - If not, repeat
- We need this to resist side-channel attacks
 - So we specify a minimum iteration count k
 - We may select the first one, but we keep at it for a suitable k so the probability of failure is low enough
- We can't precompute this because we include Alice and Bob's identity in determining P

Now to prove that everybody knows the same PE

- Alice creates two random values:
 - $1 < r_a < q$
 - $1 < m_a < q$
- Alice now computes
 - $s_a = (r_a + m_a) \bmod q$
 - $E_a = P\text{-mask}$
 - Sends those to Bob, Bob sends his counterparts
- Now the starting secret...
 - $ss = (P^{s_b} E_b)^{r_a} = (P^{(r_b + m_b - m_b)})^{r_a} = P^{r_a r_b}$
 - Sends those to Bob, Bob sends his counterparts
 - Verify P^{s_b} and S_b are valid
 - Computes $H(ss|E_a|s_a|E_b|s_b)$ and sends that to Bob
 - verifies Bob's counterpart
- Final $K = H(ss|E_a * E_b|s_a + s_b)$

Use in WPA3

- WPA3 does this
 - Well, over an elliptic curve instead, but same idea: Generate a random generator and use that
- But it is not during the 4-way handshake...
- Instead, it is 2 additional handshakes **before** the 4-way handshake