Rumbling in the Plumbing: Security and Internet Routing

Leslie Daigle
ldaigle@thinkingcat.com
October 2018

Overview

- Why Routing Security Matters
  - And, a bit about what it is
- A step back – consider the Internet
  - Compare and contrast with telephony network
  - Diversity is a strength (monoculture kills)
  - Advances are made through collaboration
    - However challenging that may be
- Routing Security, revisited
  - Finding solutions that fit at Internet scale
  - How to move forward

Why Routing Security Matters

And, a bit about what it is

An Army may march on its stomach…

- … but the Internet's security rests on its plumbing
- Application and service security can literally be undermined by a poor foundation of routing security.

What We're Looking for: A Secure and Stable Network

Ideal

- Your network is used (only) by authorized entities to carry out approved activities
  - No unwanted traffic
  - Not being used to launch attacks elsewhere
- Your users' activities are carried out without illicit observation, interception, disruption or corruption
  - No snooping
  - No hijacking
  - No modification

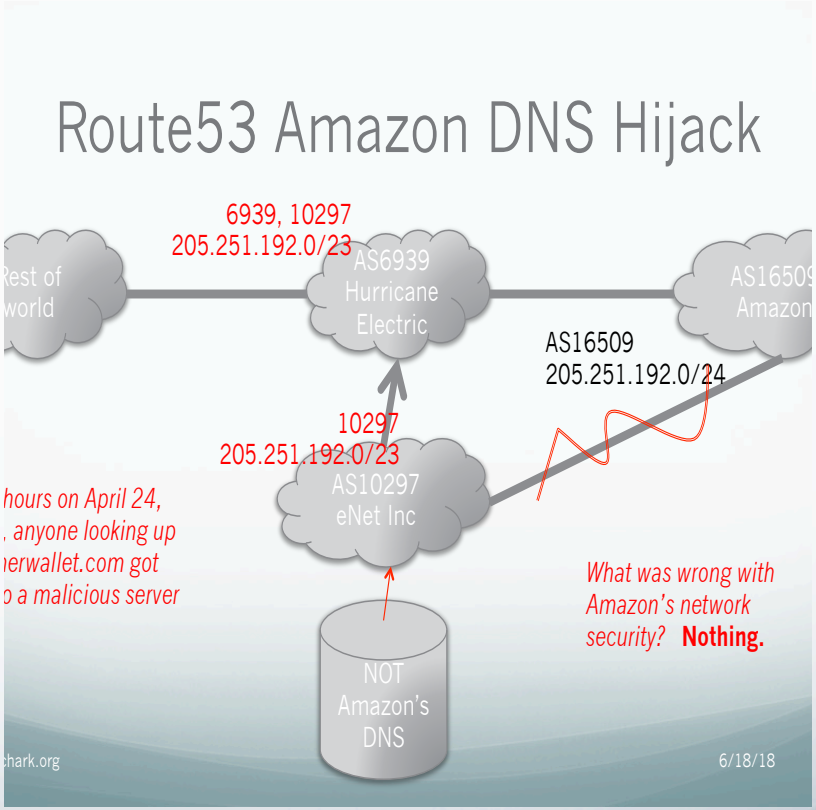
Network Security: Top 5 Fundamentals*

- Keep patches and updates current
- Use strong passwords
- Secure your VPN
- Actively manage user access privileges
- Clean up inactive accounts

*According to: http://www.itmanagerdaily.com/network-security-fundamentals/

Reflections on the advice

- They are good suggestions
- However, they are for perimeter security
  - They only address incursions of your network / access to your resources
- Nothing in that helps with
  - DDoS against your network
  - Treatment of your communications once they leave your network / services
  - Route hijacking
- The reality is: you can't build a perimeter around your network interactions, and secure that perimeter



Thinking at Internet Scale…

Paths forward

There oughtta be a law against that!

- Identify bad behaviour
- Impose sanctions
- But
  - What happens when the actors are in different jurisdictions?
  - What happens when you can't distinguish between activity that is okay sometimes but not always?

'No Man is an Island' – John Donne

- No man is an island entire of itself; every man is a piece of the continent, a part of the main; if a clod be washed away by the sea, Europe is the less, as well as if a promontory were, as well as any manner of thy friends or of thine own were; any man's death diminishes me, because I am involved in mankind. And therefore never send to know for whom the bell tolls; it tolls for thee.

'No Network is an Island'

- **With apologies to John Donne**
- No network is an island entire of itself; every network is a piece of the Internet, a part of the main; if a server be washed away by the DDoS attack, the Internet is the less, as well as if an access network were, as well as any manner of thy friends or of thine own were; any network's problem diminishes me, because I am involved in the Internet. And therefore never send to know for whom the bell tolls; it tolls for thee.

Awesome. Now, how do we make this actionable?

A Step Back

Consider: the Internet

Compare & Contrast: Telephony Network

	Traditional Telephony Network
Ownership	• Initially, government owned (PTT – post, telegraph, telephony). • Variously privatized in different countries.
Standards – setting	• International standards organization – International Telecommunications Union (ITU) • Country representatives – one country, one vote
Standards – adherence	• Imposed – by international treaty • Important – sending the wrong current on a line could blow up another country's phone system
Addresses	• ITU-managed country code assignation • Countries manage allocation within their code • "1" is US, Canada, Carribean • Managed under NANP contract

	Traditional Telephony Network	The Internet
Ownership	• Initially, government owned (PTT – post, telegraph, telephony). • Variously privatized in different countries.	• (Generally) privately-held companies own individual networks • No "Internet" owner
Standards – setting	• International standards organization – International Telecommunications Union (ITU) • Country representatives – one country, one vote	• Internet Engineering Task Force (IETF) • Individual (not corporate) participants) • Consensus-based decision making
Standards – adherence	• Imposed – by international treaty • Important – sending the wrong current on a line could blow up another country's phone system	• Voluntary • But, if you don't follow them, you'll have few networks to connect to
Addresses	• ITU-managed country code assignation • Countries manage allocation within their code • "1" is US, Canada, Carribean • Managed under NANP contract	• Managed for scarcity (~4B addresses in IPv4) • Open, transparent, bottom-up policy organizations manage allocations (5 regional internet registries)

Implications

	Traditional Telephony Network	The Internet
Ownership	• Mostly monopolies	• Non-geographically limited networks
Standards – setting	• Innovation at the speed of international negotiations	• Innovation at the speed of the market
Standards – adherence	• Standards-body-driven changes of greater and lesser scale	• Making change across the entire network can be hard – impossible require changes

Addresses	• Geopolitical disputes trump access
	  • Taiwan and country code for long distance dialling
	  • Carry over concerns with Internet country codes (for the domain name system) being controlled
		• Address scarcity has been managed for 20 years beyond the point they were expected to run out

Today's focus

	Traditional Telephony Network	The Internet
Ownership	• Mostly monopolies	• Non-geographically limited networks
Standards – setting	• Innovation at the speed of international negotiations	• Innovation at the speed of the market
Standards – adherence	• Standards-body-driven changes of greater and lesser scale	• **Making change across the entire network can be hard – impossible to require changes**

Addresses	• Geopolitical disputes trump access
	  • Taiwan and country code for long distance dialling
	  • Carry over concerns with Internet country codes (for the domain name system) being controlled
		• Address scarcity has been managed for 20 years beyond the point they were expected to run out

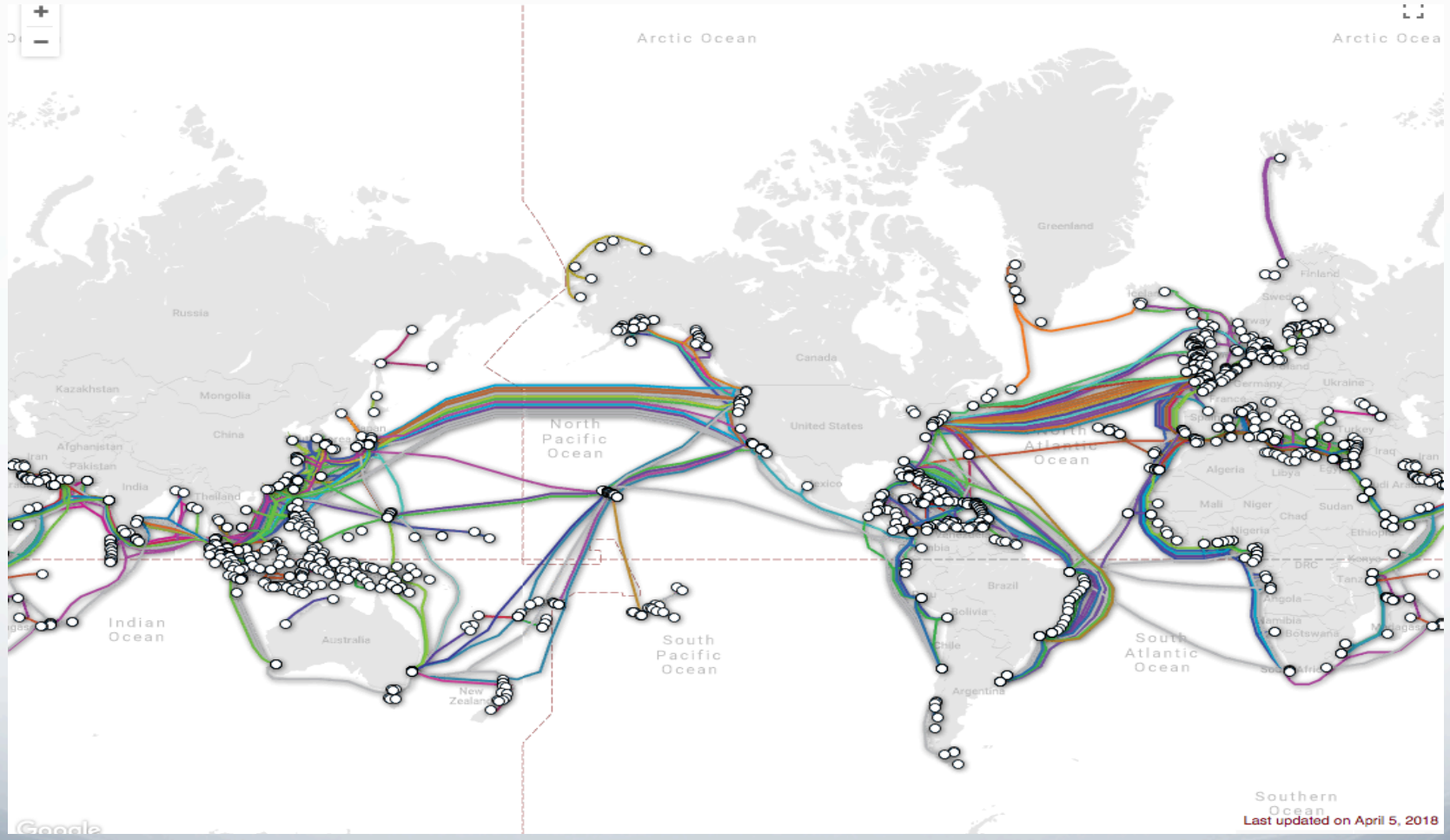
Diversity is a Strength

Monoculture kills

The Internet, ca. 1993

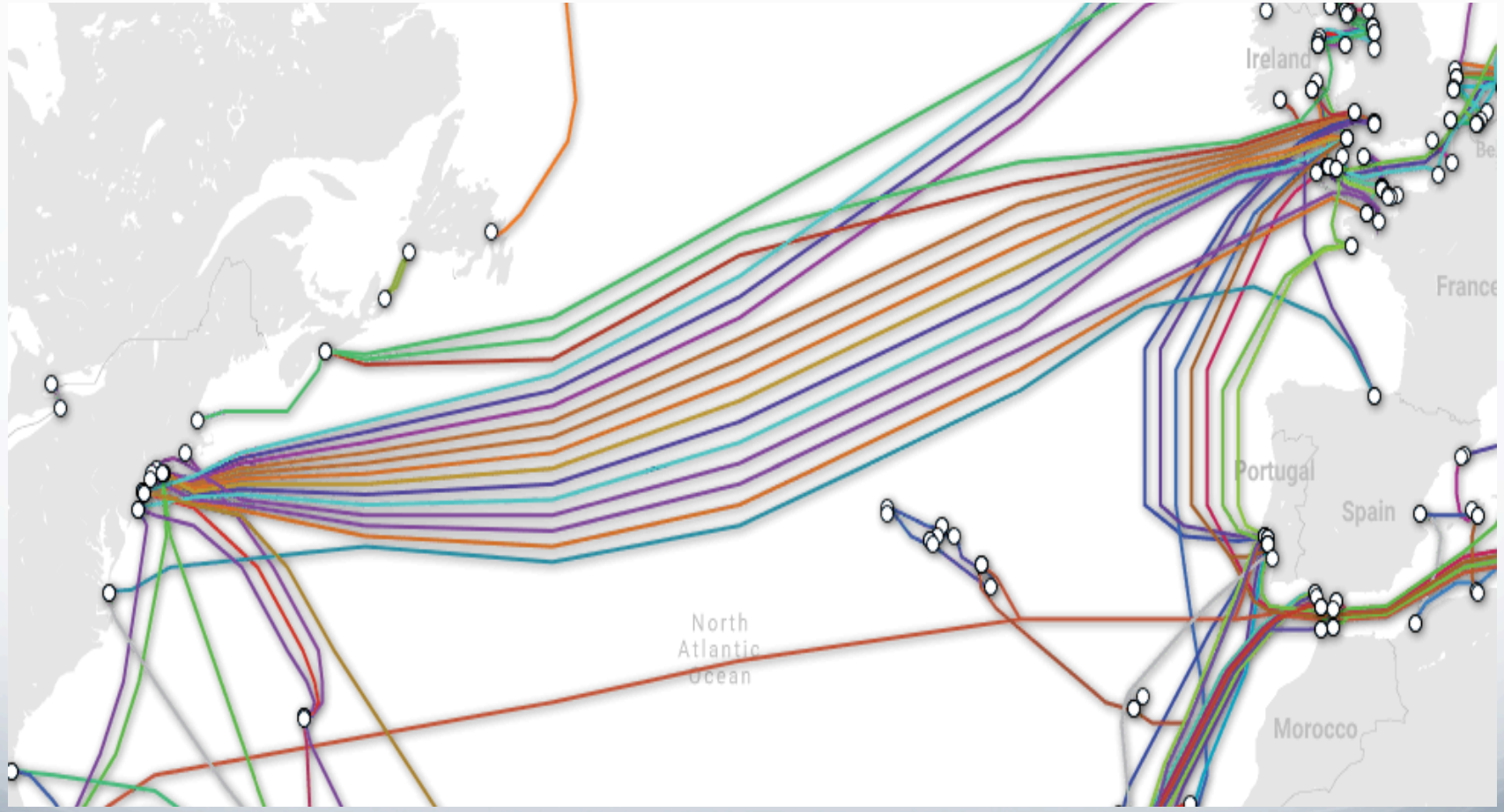
https://cdn0.vox-cdn.com/assets/4463763/world_large.gif

A submariner's perspective 2018



Telegeography: https://www.submarinecablemap.com/

The Atlantic links



Telegeography: https://www.submarinecablemap.com/

Resilience in the face of disaster

Diversity is good!

New York – 9/11

- New York was the landing site for many important trans-oceanic network links
- 9/11 – had a significant impact on key pieces of physical infrastructure
- Andy Ogielski and Jim Cowie of Renesys Corporation shared an analysis of the impact on network reachability and stability
  - March 5-6, 2002, "National Research Council, Workshop on The Internet Under Crisis Conditions"

Physical Impact of 9/11

- As noted by Ogielski & Cowie:
  - "World Trade Center 1 & 2: Below-ground-level fiber from the Telehouse to 60 Hudson St, and to transatlantic cables."
    - Cables were lost in the destruction of WTC buildings on 9/11
  - "60 Hudson St: A large carrier hotel, termination of multiple transatlantic cables, with many PoPs at 25 Broadway"
  - "NYIIX at 25 Broadway Telehouse: A peering site serving about 40 Internet providers from NYC area, Europe, South America, and South Africa. Claims about 70% of Europe to US traffic."
    - 25 Broadway suffered power failure on 9/13 when backup generator failed; back on 9/15 and failed again.

Internet Impact of 9/11

- Reachability issues to fewer than 1,000 Internet destinations
  - On either side of the Atlantic
  - Due to physical implications
- No noticed routing stability issues
  - In fact, fewer transient route announcements – less normal maintenance on near, but unaffected networks?
- "There has been a sufficiently high peering redundancy, and so far single localized events such as the 9/11 attacks, or the 7/18 Baltimore tunnel fire, do not cause widespread global routing problems. Lack of redundancy is fatal: cf. South Africa"

Takeaways

The Internet may not have been designed to withstand a nuclear attack, but the:

- highly interconnected,
- collaborative,
- resilient failover nature of the technology and provisioning

have in fact allowed it to substantially survive significant physical disasters

Lack of Diversity

Business dominance can show a counter example

Research in Motion: Blackberry

- Research In Motion built the market for mobile work platforms
  - 1999: the first truly usable e-mail over mobile networks
  - Conservative use of data made it responsive and affordable (data plan usage)
  - 8 years later, the iPhone doesn't touch it for performance or affordability

However…

- October 2011: RIM network failure halts BlackBerry services for all 70M customers, for three days
  - Finger pointed at a faulty router in their network
  - Because RIM built and relied on their own massive application network overlay, they had insufficient diversity or resiliency
  - From an enterprise perspective, that puts your threat surface outside your 4 walls
- Other mobile platforms, which use (chatty) Internet standard application protocols, leverage the resiliency of the Internet

Takeaways

At a business level, there are times when it makes most sense to collaborate – even with competitors

- This isn't just "old school Internet"
- It's not about ideals.

Advances are made through collaboration

However challenging that may be

Collaboration Among Competitors

- There's a whole other talk on this topic alone...
- For today, consider this:
  - Open source software

Routing Security Revisited

Inter-networking means global challenges

- The Internet is not a globally managed network with universally defined service level assurances
  - This diversity is what gives it all the resiliency we've been discussing so far
- When there are updates and challenges, like IPv6 deployment, the best and only way to ensure success in overcoming them is through collaboration

Security of routing packets

- When you send packets from your network into the wilds of the Internet, you can worry whether they will:
  - arrive at the intended destination;
  - be copied or read; and/or
  - be tampered with en route.
- When you take in packets from the wilds of the Internet, you may wonder whether
  - you actually want them; and/or
  - they are who they say they are.

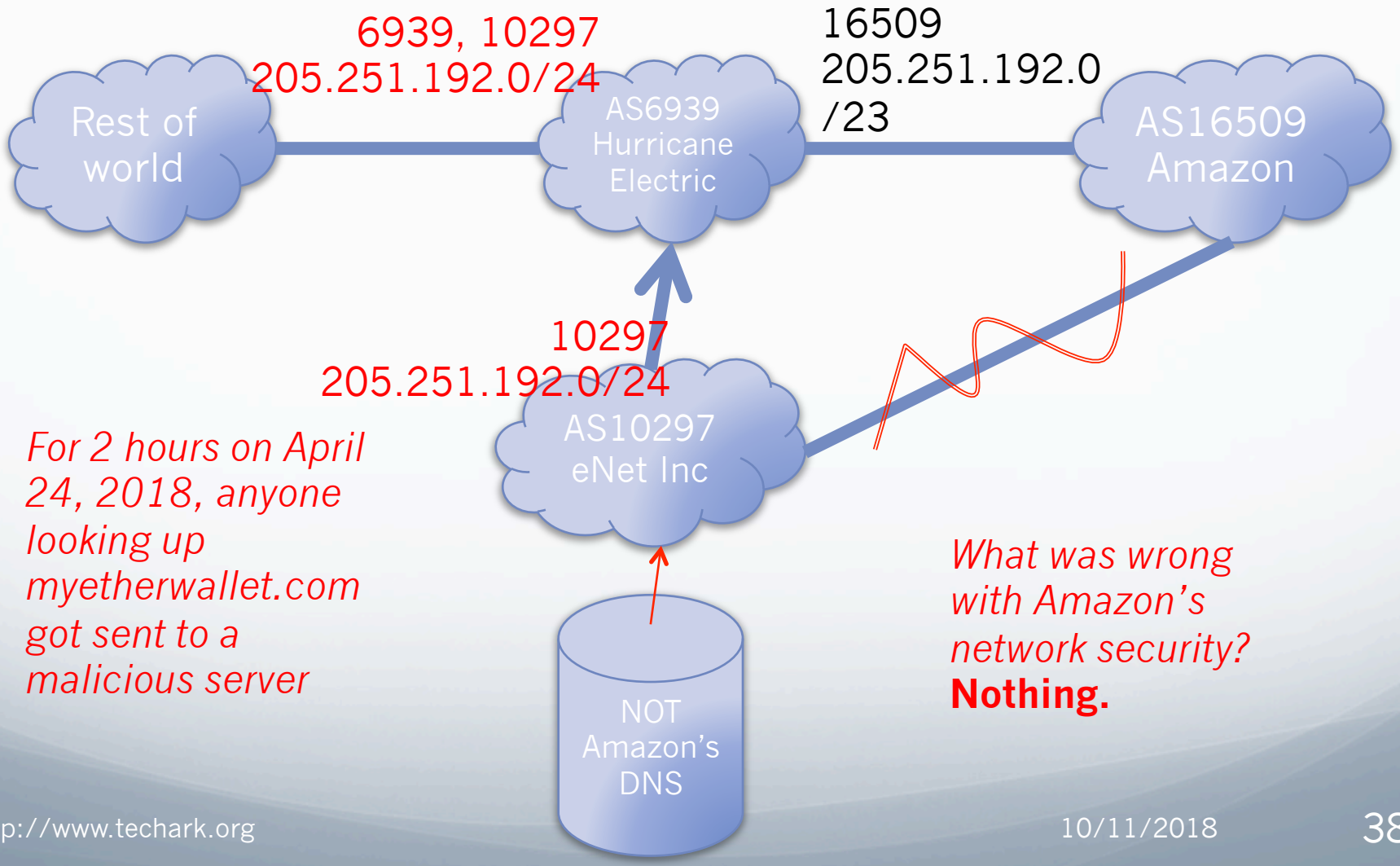
InSecurity of routing packets

- When you send packets from your network into the wilds of the Internet, you can worry whether they will:
  - arrive at the intended destination;
    - Route hijacking
  - be copied or read; and/or
    - Crypto can help; though not for metadata
  - be tampered with en route.
    - Crypto can help; though not for metadata
- When you take in packets from the wilds of the Internet, you may wonder whether
  - you actually want them; and/or
    - Unwanted traffic – DOS attack?
  - they are who they say they are.
    - Spoofed source addresses

Where the issues are

- Generally – business agreements between networks mean it's not completely "the wild West" and these are not normal, expected conditions
  - But, bad actors can still cause problems
- The problems
  - Route hijacking
    - Or, fat-fingering
  - Address spoofing
    - Facilitates DDoS

Route53 Amazon DNS Hijack



For 2 hours on April 24, 2018, anyone looking up myetherwallet.com got sent to a malicious server

What was wrong with Amazon's network security?
Nothing.

What is wrong in that picture…

- eNet Inc (AS 10297) should not have advertised a path to Amazon's address space
  - That was malicious, a man in the middle attack with a more specific route advertisement
  - The target was cryptocurrency servers at myetherwallet.com
- But, also, Hurricane Electric (AS 6939) should not have shared it
  - It did, because it was a customer link ($$)
  - And, how to detect it was inappropriate?
    - Not an advertisement for eNet Inc's address space
    - Not an advertisement for eNet Inc's customers

    ⇒Hurricane Electric should conclude eNet Inc should not be advertising it, and therefore drop it

But wait…

- How does Hurricane Electric know who is/isn't an eNet Inc customer?
  - Industry resistance to publicizing all neighbour links
    - Competitive intelligence
    - Some relationships may be ephemeral
      - Backup links
      - DDoS mitigation links
  - Lack of agreement on reliable sources
    - Which is *your* favourite IRR?
    - How to tell if data is up to date?

Current Work

Crypto for routing

- Using RPKI to verify ownership of resources, and to encase announcements in crypto
- Resistance in deployment
  - Computationally expensive
  - Encasing -> reduced flexibility
  - Requires trust in external entities (RIRs)
  - Difficult to express actual networking relationships well

Collaborative agreements for best practices: MANRS

- "Mutually Agreed Norms for Routing Security"
  - https://www.manrs.org/
  - Includes, as a best practice, filtering routes from customers
    - I.e., not propagating the false Amazon Route53 announcement
    - Interestingly, MANRS signees *did* filter that announcement, and therefore limited the damage
  - ~60 networks signed up (April 2018)

URSA – Unwedging Routing Security Activity

- Shameless plug :^) http://www.techark.org/ursa
- Collaborative effort of operators to define practical steps forward

What have we learned?

Diversity and Collaboration

- Surviving catastrophes through diversity, collaboration
  - 9/11
- Creating catastrophe through lack of diversity and monopoly
  - Blackberry
- Collaboration solves business problems and is business-smart
  - Open source software

And…

- Wicked problems can be solved through collaboration
  - Routing security ← get involved!

So: get involved! Because your network is not an island…

Additional Material

Resources

- Route53 Amazon DNS hack
  - https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/
- 9/11
  - March 5-6, 2002, “National Research Council, Workshop on The Internet Under Crisis Conditions”, Andy Ogielski and Jim Cowie of Renesys Corporation
    - https://web.stanford.edu/class/msande237/viewgraphs/911.pdf
  - https://www.nap.edu/read/10569/chapter/4#29
- Blackberry outage
  - https://www.theguardian.com/technology/2011/oct/14/blackberry-outage-faulty-router-suspected