Routing Area Security Presentation

Christopher Inacio

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Legalese

This material is based upon work supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University of its Software Engineering Institute.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Routing Area Security Awareness Agenda

Routing for Defense/Offense

Security Operations View of Routing

Making the Internet Safer via Routing

Passive Pervasive

Thought games

Routing for Defense/Offsense

Using routing to Advantage

Defense

- Routing is useful as another information source
  - E.g. RouteViews
  - Like to be able to trace traffic backwards*
- Use good routing and connectivity
  - Path diversity
  - Provider diversity

Using routing to Advantage

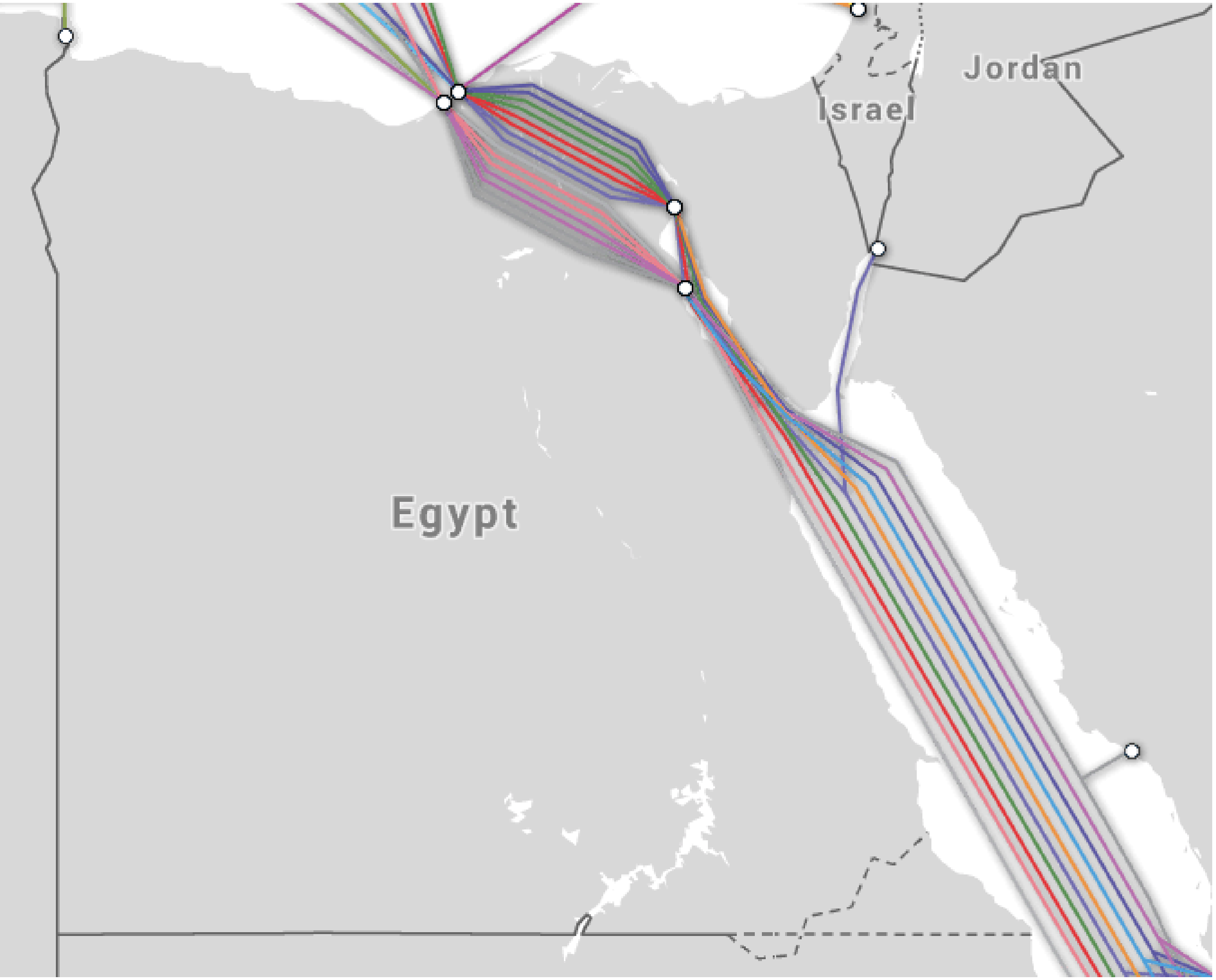
Offense

- Chose attack paths wisely, prefer path diversity
- Use RouteViews, chose highly variable routes

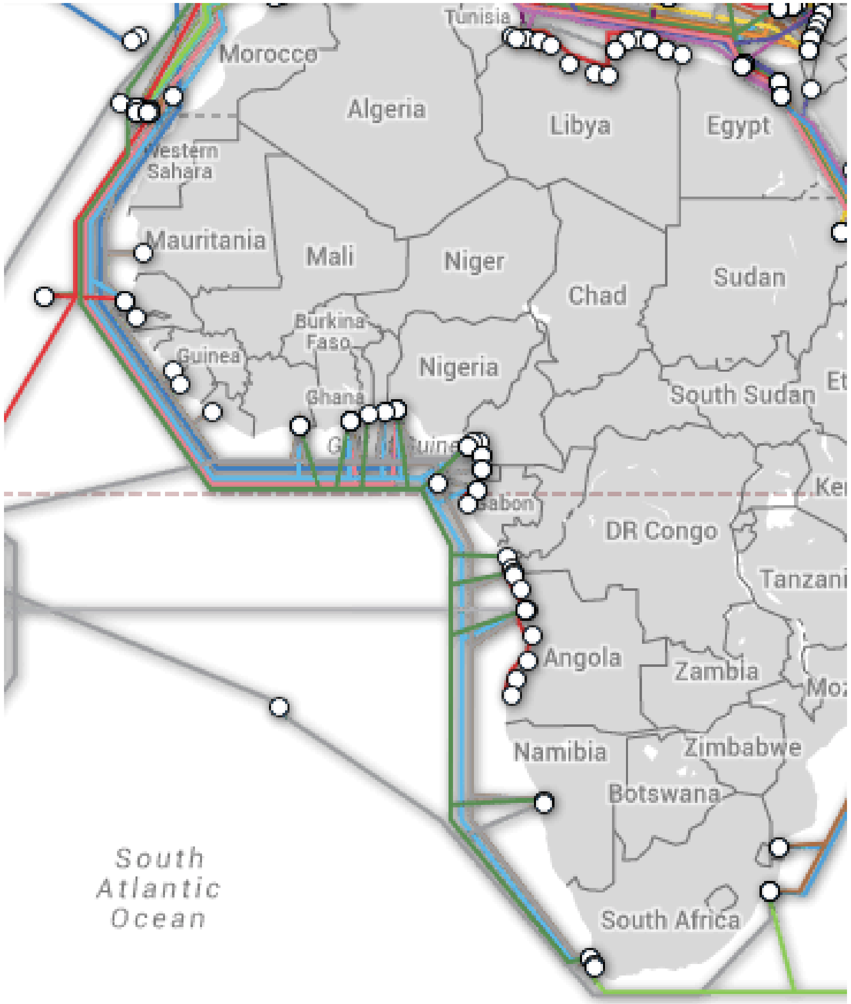
- Internet structure
  - Routes indicate physical structures
  - Undersea cable maps
  - Determine highest value points

- EPEG cable example

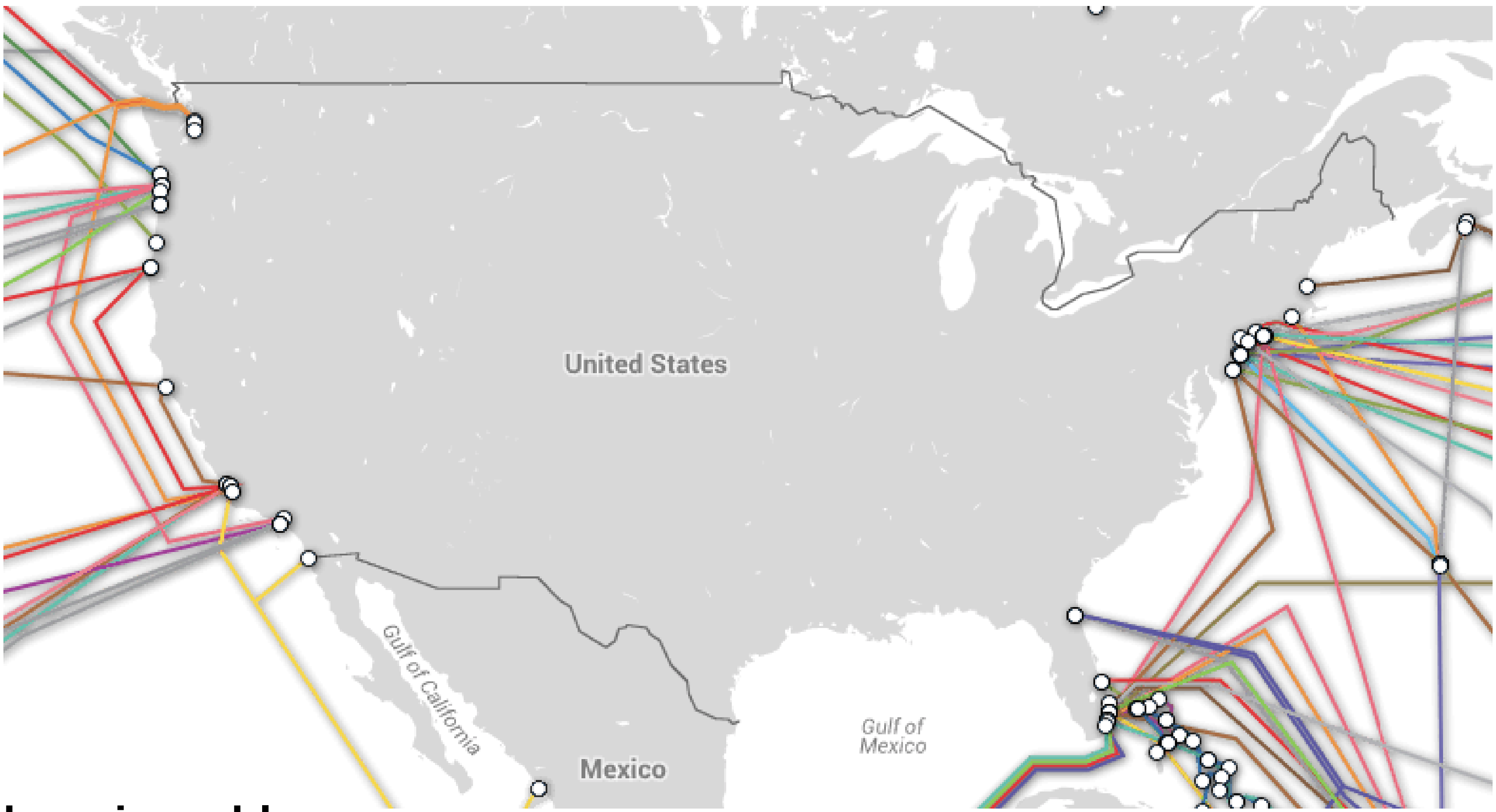
Using routing to Advantage



Submarinecablemap.com



Submarinecablemap.com



Submarinecablemap.com

Security Operations View of Routing

Name optional

Security Operations View of Routing

For most security operations:

- NOT routing experts
- Know how to use traceroute
- Assume routing is fairly static
  - Path congestion, maintenance windows, etc
- Love ASN’s*

Security Operations View of Routing

Generalized Data Enrichment

1. Network ``event’’ occurs – (scariest is IDS outbound event)
2. Get IDS alert type and get associated CVE
3. Get OS type, version, patch level, etc. for internal IP, check for CVE match
4. Use passive DNS logs to search for DNS lookup match for external IP address
5. Fingerprint OS of external IP if possible

Security Operations View of Routing

Generalized Data Enrichment (continued)

1. **Get ASN for external IP**
2. **Lookup ASN in whois database mirror to get organization info**
3. **(maybe) traceroute to trace back packet source**
4. **Geolocate IP address**
5. Add internal IP tracking history
6. Check event type and internal IP address
    1. Can our internal asset even participate in event type (e.g. Inbound Solaris attack against our Linux machine – ignore)

Security Operations View of Routing

- ASN’s
  - Conveniently placed into the Internet so that defense network operations can attribute packets
  - Used to determine potential badness of slices of Internet
  - Might legitimately indicate a ”bullet proof host”
- Most net defenders are not analyzing route views
- Most net defenders (possible including this one :) aren’t routing experts

Making the Internet Safer via Routing

Name optional

Making the Internet Safer Via Routing

Why does this still happen?

- February 2008 – Pakistan hijacks YouTube (
- April 2010 – China hijacks part of Internet, including NIPRNet
- February 2013 – Belarus hijacks traffic from Mexico destined to US (Renesys)

Making the Internet Safer Via Routing

Good behavior from ISPs:*

- Use the best practices
  - Deploying antispoofing measures
  - Have max prefix filters from downstream partners

- Global Tier 1 forces best practices downward*
  - All tier 1 providers have to do participate
  - Refuse/block updates from misbehaving downstream ISPs
  - Communicate / Educate customers downstream
  - Require downstream customers to require this implemented as well
- Use new protocols and security functions too.

*** - suggestions from Rachel Kartch**

Passive Pervasive

Name optional

Passive Pervasive

- Really hard to prevent
  - Require encryption down to layer-2
    - Key management?
    - Large data volume + probably not frequently enough rotated key = ??
    - New hardware to handle this
    - REALLY hard to keep a secret if you give it to EVERYBODY
      - Just ask the DVD crypto people about this…
  - Relatively small amount of data to grab – IP + transport + ports + number of packets & bytes
    - We can store these flow records in under 15 bytes per record

Passive Pervasive

- Generally not too hard to ``guess'' at traffic for first order understanding:
  - IP 1.2.3.4 <-> 5.6.7.8, proto TCP, ports 22 <-> 3847
  - SSH session

- More sophisiticated:
  - Number of packets + size of packets
  - Interpacket timing
  - = human or machine using flow

- Slightly harder (exercise for the reader)
  - Method to find FTP file transfers
  - http://tools.netsa.cert.org/silk/analysis-handbook.pdf (shameless plug)

Passive Pervasive

- If one knows the physical structure of the Internet
- If one can get access to physical Internet Exchanges
- If one can find submarine cable choke points

- Then passive pervasive is potentially really cheap and really effective
- It’s also really hard to mitigate

Thought Games

Name optional

Thought Games

- What if a rogue ISP can inject some Anycast routes?
- What if those Anycast routes were only visible by a relatively small targeted set of users?
- What if that was used to hijack DNS
  - How would you find it?
  - What would you do to fix it?