Regional cyber security considerations for network operations

Eric Osterweil
Principal Scientist, Verisign
Internet operations and cyber security

• These two fields are deeply intertwined

• But, one could argue these are different communities

• There are many cases where Internet operations can provide critical insights to cyber security

• There are cases where cyber security practices can guide Internet operations
Cyber security problems and core protocols

- Cyber security concerns come from a wide range
  - Mobile malcode
  - DDoS attacks
  - Data exfiltration
  - Watering hole attacks
  - etc.

- We have become comfortable with looking at these attacks in isolation
  - Malcode is an OS problem, DDoS is a resource problem, etc.

- We need to realize that adversaries have goals, and “attacks” can be mere components in campaigns

- From this realization, Internet operations can address weaknesses in attack campaigns
Outline

• How have core protocols succeeded, this long

• Liabilities and problems

• Remediations

• Conclusions
Core protocols are the foundations of cyber security

• Routing (BGP) and naming (DNS) underlie most online activities
  • One way to look at BGP: establishes reachability between those holding IPs and ASNs
  • One way to look at DNS: lets those holding names map them to resources (services, etc.)

• These protocols enable pretty much every service on the Internet (HTTP[S], SMTP, etc.)
• This makes them very relevant to cyber security

• However, much of the development of these protocols has been to make them more scalable and resilient
How things have been able to scale

• Administrators have had the ability manage our own resources
  • We decide how our IP allocations should be announced
  • We decide what names to map to services
  • We chose where eyeballs land
  • We have servers and racks, and we decide who we get our connectivity from

• More autonomy lets us optimize, customize, react to problems, etc.
But, this is also an Internet-wide leap-of-faith

• We *trust* the configurations of these protocols
  • We learn others’ configurations, and believe what we hear

• This *trust* means good network hygiene is important
  • Mistakes can generally be overcome, when everyone is well intending

• But, a way to verify network configurations is missing
  • Who holds which resources, who is authorized to speak for resources, what are their intentions

• Some call this *Resource Certification*

• What happens when intentions are less pure?
Today’s threatscape varies in so many ways

• Defenders often focus on our core competencies
  • Should a routing operator just tighten peering infrastructure?
  • Should a cloud service just harden virtualization services?

• Sometimes attacks seem to be focused on technologies, but might just be opportunistic
  • Does a BGP route leak concern anyone other than routing operators?

• Sure, BGP route leaks can cause outages, but they can also facilitate Man-in-the-Middle attacks
  • This could motivate a cloud provider to worry about BGP

• Does this mean that attacks like data breaches can be affected by BGP route leaks and DDoS too?
An illustration – cross-modal hijacking

• In 2009, BGP was used to leak routes to DNS root servers
  • Protocol manipulation of BGP interfered with DNS and affected HTTP
  • Result, HTTP Man in the Middle (MitM) attacks were possible on major websites

Systemic dependencies

• **Consider this case**
  • To BGP, these cases looked like expanded anycast catchments
  • To DNS, they looked like a detectable error
  • To anyone not looking at their own systemic dependencies, these were undetected attacks

• **Attackers capitalize on the fact that layering isolates protocols from each other**
  • Just because protocols don’t know how they depend on each other, doesn’t mean attackers don’t
More illustrations

- In 2010-2013, temporally narrow BGP route leaks from regions/ISPs [2,3]
  - At first, connectivity interruptions announced leaks
  - Progressively, end-to-end connectivity was maintained during attacks (MitM)
- BGP route leaks can enable MitM attacks

Systemic dependencies (2)

- User-facing services depend on many infrastructure protocols
- Many user-facing services depend on each other [3]

So, what should we do?

- **Prudence**: we should treat the symptoms *and* the cold
  - Tactical and strategic remediation

- **Consider DDoS reflector attacks**: these attacks may use DNS, NTP, SNMP, etc.

- **Good advice is to follow Best Current Practices (BCPs) for hardening deployed systems**
  - DNS: close open resolvers, NTP: disable monlist, etc…

- **Strategic**: focus on the root too
  - The IP layer is a component of reflector attacks too
  - Source spoofing enables these reflector attacks… *that* is a filtering problem

- **Consider Resource Certification**
Some examples of good hygiene

- Keep services hardened
  - NTP [5], closing DNS resolvers [6], etc
- The set of recommendations is long, and groups have come together expressly for this
  - Example: US FCC Communications Security, Reliability and Interoperability Councils (CSRICs) [7]
- But, source spoofing is used on a variety of protocols, remediating *that* is a more strategic goal
- Ingress filtering: BCP 38 [8]

More strategy: cyber herd immunity!

• There’s more to this than defending ourselves in isolation
• Operators need to work together
• In fact, these hygienic practices can be made to work together
  • Proto hardening is good, but also kind of whack-a-mole
  • Often, plugging one hole opens another (or another hole gets exploited)
• To protect each other, we need cyber security
  Information Sharing
  • Share relevant information!
Information sharing

• Much of what info sharing platforms have focused on is Indicators of Compromise (IOCs)

• But, network attack telemetry can be helpful to share too…

• Sharing networks have formed in many ways
  • This can be what CSIRTs, trust groups, etc. are used for

• But, be focused on what you want and want to share
  • Is DDoS telemetry helpful, mobile malcode infections, etc.

Suppose…

• Suppose a DDoS attack is underway

• What if the victim can share attacking sources with likeminded operators

• What if those operators can help filter traffic because a trusted peer shared incident information?
Information sharing challenges

• **There can be liabilities in info sharing**
  • If I share information, that may be Personally Identifiable Information (PII)
  • I might be liable to my customers if I disclose a data breach (or I might be liable if I don’t)

• **Reporting incidents (vs. indicators or observables)**
  • Rather than admitting a compromise (or breach), I might share indicators
  • Is that enough without context of an incident?

• **Making threat intelligence actionable**
  • What info can be shared and acted upon
  • Sharing info without action is not terribly useful
Conclusion

• Take-homes: good hygiene is critical
  • One suggestion: but when short on resources, focus efforts on core payoffs: filtering and info sharing

• Tactical and strategic foci
  • Hardening + filtering + resource certification

• Herd immunity: proactive information sharing
  • Love your local CSIRTs, sharing groups are good
Thank You