What were the four requirements for a secure communications channel?

- Availability (Can I reach the destination?)
- Authentication (Who am I talking to?)
- Confidentiality (Is my data hidden?)
- Integrity (Has my data been modified?)

sli.do time…
(yell at me if I don’t notice?)
A Chinese ISP momentarily hijacks the Internet (again)

By Robert McMillan
IDC News Service / April 9, 2003 13:45 P.M.

For the second time in two weeks, bad networking information spreading from China has disrupted the Internet.

On Thursday morning, bad routing data from a small Chinese ISP called IDC China Telecommunication was re-transmitted by China’s state-owned China Telecommunications, and then spread around the Internet, affecting Internet service providers such as AT&T, Level3, Deutsche Telekom, Great Communicaions and Telefonica.


Internet-Wide Catastrophe—Last Year

One year ago today TTNet in Turkey (AS9121) pretended to be the entire Internet. And unfortunately for the rest of the Internet, many large network providers believed them (or at least believed them in part). As far as anyone knows, it was a mistake, not a malicious act. But the consequences were far from benign: for several hours a large number of Internet users were unable to reach a large number of Internet sites. Twelve months later we can take a look at what happened, and whether we’ve learned much in the intervening time.

Early Christmas Eve morning 2004, TTNet (AS9121) started announcing what appeared to be a full table (well over 100,000 entries) of Internet routes to all of their transit providers. I was on call that Christmas (as I am this Christmas; I’m sensing a bad pattern here). So around 4:30 in the morning US Eastern Standard Time, I started getting paged.

DDoS Attack Hits 400 Gbit/s, Breaks Record

A distributed denial-of-service NTP reflection attack was reportedly 33% bigger than last year’s attack against Spambase.

ProtonMail On Battling A Sustained DDoS Attack

Encrypted email provider, ProtonMail, has been fighting a wave of DDoS attacks since November 9 that, by last Friday had taken its services offline for more than 24 hours. At the time of writing the attacks are still coming.

They have included what ProtonMail co-founder Andy Green described as a “leopard” attack on its NTP that exceeded 110Gbps and “attacked not only the NTP servers but monitors in various locations where the NTP has nodes — taking multiple services offline, not just ProtonMail’s email.”
Goals of this lecture

- Understand attacks on availability in the network.
- Many attacks at the application layer — bugs in code — go take 18-487 to learn more about those.
- This class focuses on attacks on availability in the network.

Two classes of attacks on availability we will discuss today

- **Routing Attacks**
  - We’ll talk about flaws in BGP
- **Resource Exhaustion**
  - DDoS
  - SYN Floods
- There are so many kinds of attacks we’re not discussing though!
  - Take 18-487 with Prof. Sekar!

Recall: Internet routing

- Internet relies on hierarchical routing
  - An Interior Gateway Protocol (IGP) is used to route packets within an AS: Intra-domain routing
  - An Exterior Gateway Protocol (EGP) to maintain Internet connectivity among ASs: Inter-domain routing

What kind of routing algorithm is BGP?
What are the other kinds of routing algorithms we discussed in this class (not BGP)?

How does BGP work?
Internet routers communicate using the Border Gateway Protocol (BGP):
- Destinations are prefixes (CIDR blocks)
  - Example: 128.2.0.0/16 (CMU)
- Routes through Autonomous Systems (ISPs)
  - Each ISP is uniquely identified by a number
    - Example: 25 (UC Berkeley)
  - Each route includes a list of traversed ISPs:
    - Example: 9 ← 5050 ← 11537 ← 2153

Principles of operation
- Exchange routes
  - AS100 announces 128.1.1.0/24 prefix to AS200 and AS300, etc
- Incremental updates

Recap by doing!
BGP UPDATE message

- Announced prefixes (aka NLRI)
- Path attributes associated with announcement
- Withdrawn prefixes

Route propagation

All you need is one compromised BGP speaker
Pakistan Telecom: Sub-prefix hijack

### Potential attack objectives

- **Blackholing** – make something unreachable
- **Redirection** – e.g., congestion, eavesdropping
- **Instability**
- **But more often than not, just a mistake!**
Unauthorized origin ISP (prefix theft)

M's route to G is better than B's

AS-path truncation

M's route to G is better than D's

AS path alteration

M's route avoids C

How can we fix this problem?
What tools from the last two lectures might we use?

BGP Security Requirements

- Verification of address space "ownership"
- Authentication of Autonomous Systems (AS)
- Router authentication and authorization (relative to an AS)
- Route and address advertisement authorization
- Route withdrawal authorization
- Integrity and authenticity of all BGP traffic on the wire
- Timeliness of BGP traffic

Securing the Internet: RPKI

Resource Public Key Infrastructure (RPKI): Certified mapping from ASes to public keys and IP prefixes.

China Telecom
ISP 1
66.174.161.0/24

Level 3, VZW, 22394
66.174.161.0/24

Verizon Wireless
22394
66.174.161.0/24

Why is this solution insufficient?

RPKI shows China Telecom is not a valid origin for this prefix.

RPKI: Invalid!
But RPKI alone is not enough!

Resource Public Key Infrastructure (RPKI): Certified mapping from ASes to public keys and IP prefixes.

Malicious router can pretend to connect to the valid origin.

S-BGP [1997]: RPKI + Cannot announce a path that was not announced to you.

S-BGP Secure Version of BGP

- Address attestations
  - Claim the right to originate a prefix
  - Signed and distributed out-of-band
  - Checked through delegation chain from ICANN

- Route attestations
  - Distributed as an attribute in BGP update message
  - Signed by each AS as route traverses the network
  - Signature signs previously attached signatures

- S-BGP can validate
  - AS path indicates the order ASes were traversed
  - No intermediate ASes were added or removed
What might be hard about upgrading BGP to S-BGP?

S-BGP Deployment Challenges

- Complete, accurate registries
  - E.g., of prefix ownership
- Public Key Infrastructure
  - To know the public key for any given AS
- Cryptographic operations
  - E.g., digital signatures on BGP messages
- Need to perform operations quickly
  - To avoid delaying response to routing changes
- Difficulty of incremental deployment
  - Hard to have a “flag day” to deploy S-BGP

S-BGP Deployment Challenges

- Need ISPs to agree on and deploy a new protocol!
  - These are competing organizations!
- Economic incentives?
  - Doesn’t improve performance
  - Hard to convince customers to pay more for security
- No benefit to unilateral deployment
  - Need entire path to deploy SBGP/soBGP before you get any benefit
  - Like IPv6…. But worse

We need path validating protocols

- S-BGP: Secure BGP
  - Each AS on the path cryptographically signs its announcement
  - Guarantees that each AS on the path made the announcement in the path.
- soBGP: Secure origin BGP
  - Origin authentication +
  - …Trusted database that guarantees that a path exists
  - ASes jointly sign + put their connectivity in the DB
  - Stops ASes from announcing paths with edges that do not exist
  - What challenges might soBGP face for deployment?
  - Origin authentication +
  - …Trusted database that guarantees that a path exists
  - ASes jointly sign + put their connectivity in the DB
  - Stops ASes from announcing paths with edges that do not exist
  - What challenges might soBGP face for deployment?
Has this been adopted?

- Sadly, no
- If you solve this or want to solve this you can go to grad school
  - Or join a big company’s networking team
  - Lots of people will thank you
  - You will be very popular at Internet parties 😊

Summary

- BGP was built on the assumption of cooperation
- Assumption fails due to attacks… and just to errors.
- Proposed fixes are many, but all have some limitations
  - S-BGP
    - Relies on a PKI
    - Potentially significant overhead
- Very hard to retrofit security in an existing model!

DoS: General definition

- DoS is **not** access or theft of information or services
- Instead, goal is to stop the service from operating
- Deny service to legitimate users

- Why?
  - Economic, political, personal etc..

“Resource Asymmetry”

- One attacker with one server generating traffic probably cannot completely overwhelm the victim.
- Smurf and DNS attacks:
  - Attacker can harness arbitrary machines (lots of them!)
  - Receiver is just one server.
- “Resource Asymmetry” is the problem.
Evolution of (D)DoS in history

- Point-to-point DoS attacks
- TCP SYN floods, Ping of death, etc..
- Smurf (reflection) attacks
- Coordinated DoS
- Multi-stage DDoS
- P2P botnets

Smurf amplification DoS attack

- Send ping request to broadcast addr (ICMP Echo Req)
- Lots of responses:
  - Every host on target network generates a ping reply (ICMP Echo Reply) to victim

Prevention: reject external packets to broadcast address

Modern day example (May ’06)

DNS Amplification attack: \(( \times 50 \) amplification\)

580,000 open resolvers on Internet (Kaminsky-Shiffman’06)

Coordinated DoS

- Simple extension of DoS
- Coordination between multiple parties
  - Can be done off-band
  - IRC channels, email…
Goal: Overload the Host and Disable their Availability

- Multiple ways to achieve overload!
  - Smurf and DNS amplification attacks overload the network link.
  - Botnets can do that too.
DoS Attacks Characteristics

- Link flooding causes high loss rates for incoming traffic
- TCP throughput

\[ BW = \frac{MSS \cdot C}{RTT \cdot \sqrt{q}} \]

- During DoS few legitimate clients served

Content Distribution Networks (CDNs)

- CDN company installs hundreds of CDN servers throughout Internet
- Replicated customers' content

- How can this help DDoS?
- Legitimate requests can still go through
- Attack scale must be higher

Some CDNs even specialize in DDoS Defense!

Finding the Zombies and Killing Them

Bot Detection and Removal

Detection, notification, and prevention against malicious software. Have you noticed any suspicious email account activity, unusual error messages, or unfamiliar browser? Your computer may be infected by a "bot," malicious software that secretly uses your computer to send spam, host phishing sites, and steal your personal information.

How our proactive bot notification works

The Constant Guard bot detection tool sends you emails whenever it finds signs of a bot infection. Click on the bot notification alert to access detailed information about the bot threat.
Goal: Overload the Host and Disable their Availability

- Multiple ways to achieve overload!
  - Smurf and DNS amplification attacks overload the network link.
  - Botnets can do that too.
- May also try to overload at the application or transport layer, e.g.:
  - Send a database a lot of very large queries
  - Open lots of TCP connections — “SYN attack”

TCP SYN Flood I:  

<table>
<thead>
<tr>
<th>OS</th>
<th>Backlog queue size</th>
<th>Backlog timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux 1.2.x</td>
<td>10</td>
<td>3 minutes</td>
</tr>
<tr>
<td>FreeBSD 2.1.5</td>
<td>128</td>
<td></td>
</tr>
<tr>
<td>WinNT 4.0</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

⇒ Attacker need only send 128 SYN packets every 3 minutes.
⇒ Low rate SYN flood

How to prevent SYN flood attacks

- Non-solution:
  - Increase backlog queue size or decrease timeout

- Correct solution (when under attack):
  - Syncookies: remove state from server
  - Small performance overhead
Syncookies [Bernstein, Schenk]

- Idea: use secret key and data in packet to gen. server SN
- Server responds to Client with SYN-ACK cookie:
  - $T = 5$-bit counter incremented every 64 secs.
  - $L = \text{MACKey}((SAddr, SPort, DAddr, DPort, SN_C, T))$ (24 bits)
  - key: picked at random during boot
  - $\text{SN}_S = (T \cdot \text{mss} \cdot L) \mod 2^{24}$
- Server does not save state (other TCP options are lost)
- Honest client responds with ACK ($AN=\text{SN}_S$, $SN=\text{SN}_C+1$)
- Server allocates space for socket only if valid SNs.

What about attacks on applications — like RPC calls and database queries?

Client puzzles

- Idea: slow down attacker

- Moderately hard problem:
  - Given challenge $C$ find $X$ such that
  
  $\text{LSB}_n(\text{SHA}-1(C || X)) = 0^n$
  
  - Assumption: takes expected $2^n$ time to solve
  - For $n=16$ takes about .3sec on 1GHz machine
  - Main point: checking puzzle solution is easy. Pushes resource requirements to attacker!

- During DoS attack:
  - Everyone must submit puzzle solution with requests
  - When no attack: do not require puzzle solution

What about a DDoS attack on a web server?
(There is a simple mechanism, invented at Carnegie Mellon, that you have all used)
CAPTCHAs

- Idea: verify that connection is from a human
- Applies to application layer DDoS [Kilbobs '05]
  - During attack: generate CAPTCHAs and process request only if valid solution
  - Present one CAPTCHA per source IP address.

What do net operators do?

- Best common operational practices:
  - Often, blackholing malicious looking IPs and rerouting to custom “Scrubbers” / Firewalls

THIS IS A SAD STORY

I HAVE JUST LISTED A TON OF PROBLEMS WITH THE INTERNET NONE OF WHICH ARE FULLY SOLVED
What needs to happen to fix BGP? Why is solving the BGP security problem challenging?

Why is solving the DDoS security problem challenging?

Summary…
• Today: two classes of attacks on Internet availability.
  • Routing attacks on BGP to prevent traffic from reaching victim
    • Need to validate routes… but getting all 50k+ networks to upgrade is challenging.
  • DoS and DDoS to overwhelm resources of victim
    • Modern bonnets mean attackers can amass large amounts of resources to overrun victims
    • No “off button” on the Internet — all traffic is allowed through by the network, even if it is unwanted 😞

Thank you!
Feedback Form
https://tinyurl.com/441SannanFeedback