Security III: Availability, DDoS, and Routing Security

15-441 Spring 2019
Profs Peter Steenkiste & Justine Sherry
& (Guest Lecturer) **Sannan**

Slides almost entirely copied from **Vyas Sekar** who in turn borrowed them from other professors.

Carnegie Mellon University

sli.do time…
(yell at me if I don't notice?)

What were the four requirements for a secure communications channel?

What do we need for a secure comm channel?

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

A Chinese ISP momentarily hijacks the Internet (again)

By Robert McMillan

IDG News Service | Apr 8, 2010 5:59 PM PT

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, Qwest Communications and Telefonica.

MORE LIKE THIS

China's Great Firewall spreads overseas

China telecom operator denies hijacking Internet traffic

Research experiment disrupts Internet, for some

on IDG Answers
What is a BGP hijack?

http://www.computerworld.com/article/2516953/enterprise-applications/a-chinese-isp-momentarily-hijacks-the-internet--again-.html

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 Spamhaus.

ProtonMail On Battling A Sustained DDoS Attack

Posted 23 hours ago by Natasha Lomas (@riptari)

897 SHARES

Next Story

Encrypted webmail provider, ProtonMail, has been fighting a wave of DDoS attacks since November 3 that, by last Friday, had taken its service offline for more than 24 hours. At the time of writing the attacks are still coming.

They have included what ProtonMail co-founder Andy Yen described as a "co-ordinated assault" on its ISP that exceeded 100Gbps and attacked not only the Swiss datacenter but routers in various locations where the ISP has nodes — taking multiple services offline, not just ProtonMail's email.

CrunchBase

ProtonMail

FOUNDED
2013

OVERVIEW
End-to-end encrypted email, based in Switzerland. ProtonMail is a new service that provides easy to use secure email. ProtonMail's secure email system is designed around the principle of zero access. This means user data cannot be read by ProtonMail and turned over to third parties because ProtonMail servers do not store user encryption keys. The service is backwards compatible with insecure email ...

LOCATION
Geneva, 07

CATEGORIES
Messaging, Email, Data Security, Security

FOUNDERS

Goals of this lecture

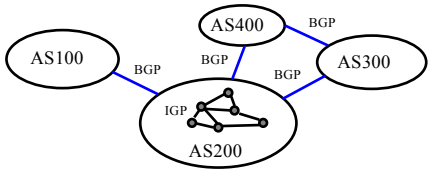
- Understand attacks on availability *in the network.*
  - Many attacks at the application layer — bugs in code — go take 18-487 to learn more about those.
  - This class focuses on attacks on availability in the network.

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

Carnegie Mellon

PITTSBURGH SUPERCOMPUTING CENTER

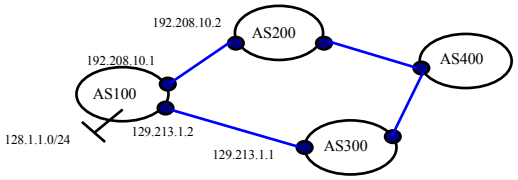
Abilene

cenic

Recap by doing!

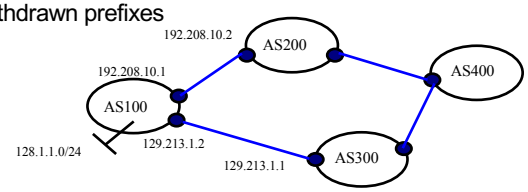
Principles of operation

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



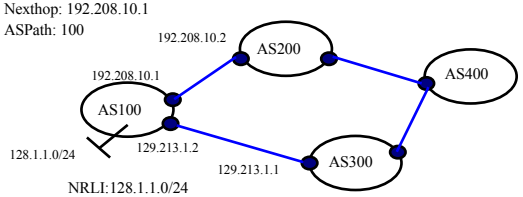
BGP UPDATE message

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



UPDATE message example

NLRI: 128.1.1.0/24
Nexthop: 192.208.10.1
ASPath: 100

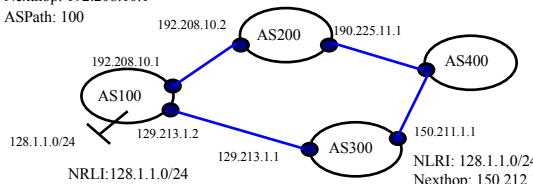


NRLI:128.1.1.0/24
Nexthop: 129.213.1.2
ASPath: 100

Route propagation

NLRI: 128.1.1.0/24
Nexthop: 192.208.10.1
ASPath: 100

NLRI: 128.1.1.0/24
Nexthop: 190.225.11.1
ASPath: 200 100



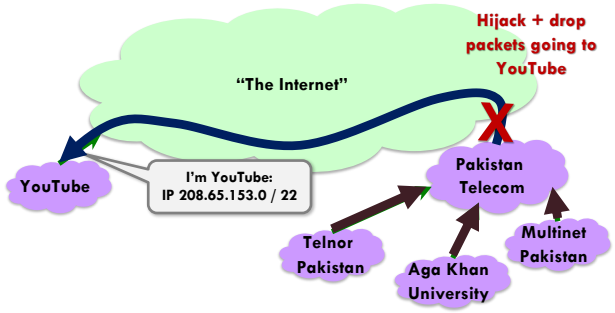
NRLI:128.1.1.0/24
Nexthop: 129.213.1.2
ASPath: 100

NLRI: 128.1.1.0/24
Nexthop: 150.212.1.1
ASPath: 300 100

Pakistan Telecom: Sub-prefix hijack

Pakistan Telecom: Sub-prefix hijack

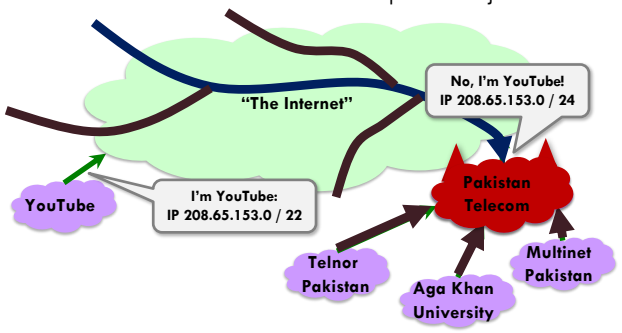
Here's what should have happened:



Block your own customers.

Pakistan Telecom: Sub-prefix hijack

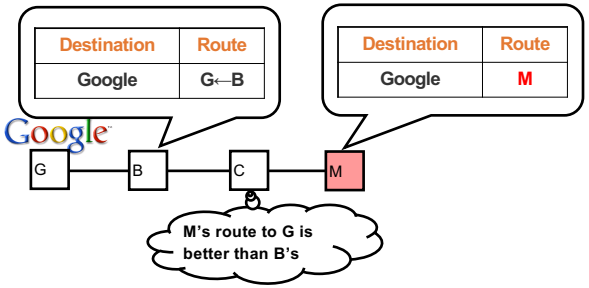
But here's what Pakistan ended up doing!



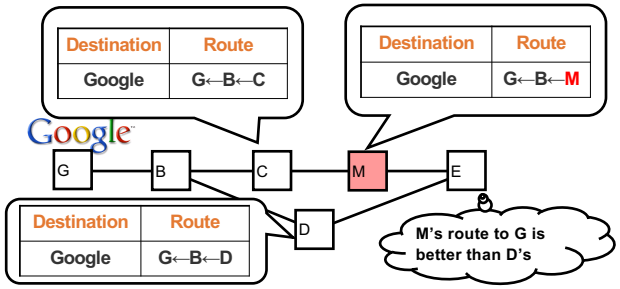
Potential attack objectives

- Blackholing – make something unreachable
- Redirection – e.g., congestion, eavesdropping
- Instability
- But more often than not, just a mistake!

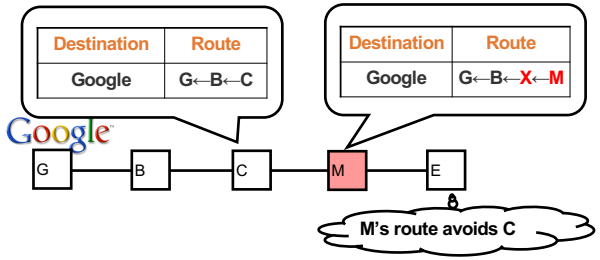
Unauthorized origin ISP (prefix theft)



AS-path truncation



AS path alteration



How can we fix this problem?

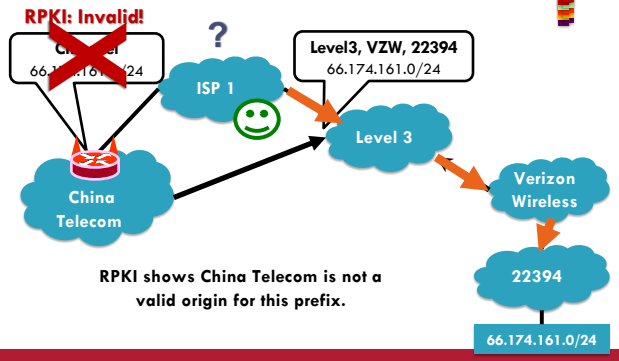
What tools from the last two lectures might we use?

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

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

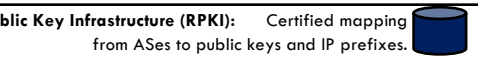
Securing the Internet: RPKI



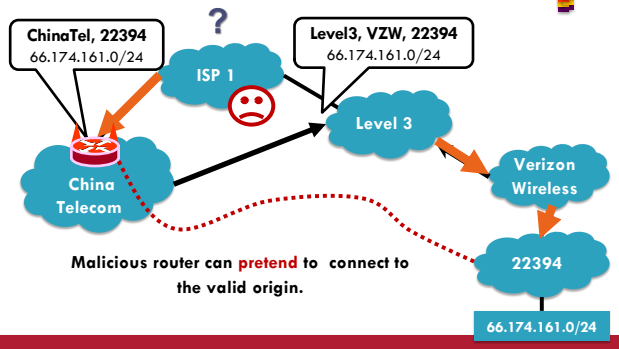
RPKI shows China Telecom is not a valid origin for this prefix.

Why is this solution insufficient?

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

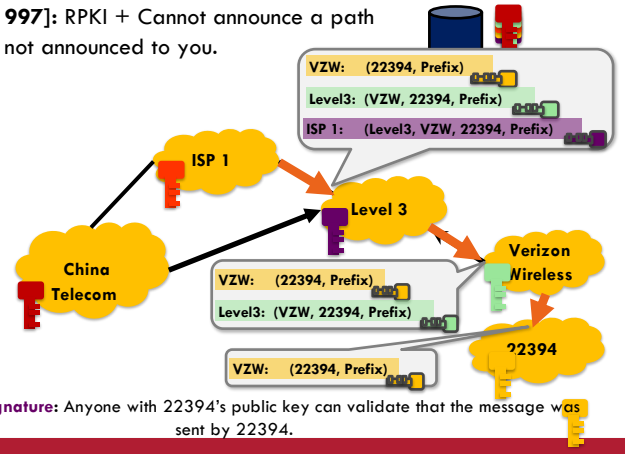


But **RPKI** alone is not enough!



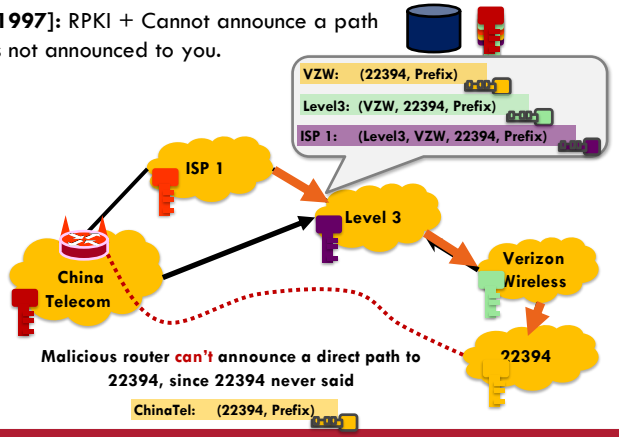
Malicious router can **pretend** to connect to the valid origin.

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



Public Key Signature: Anyone with 22394's public key can validate that the message was sent by 22394.

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



Malicious router **can't** announce a direct path to 22394, since 22394 never said

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"

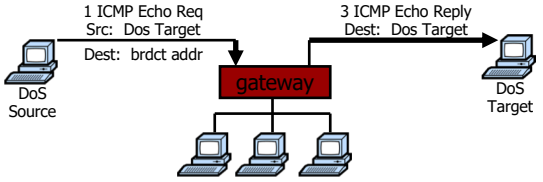
- One attacker with one server generating traffic probably cannot completely overwhelm the victim.
- Smurf and DNS attacks:
  - Attacker can harness arbitrary machines (lots of them!)
  - Receiver is just one server.
  - "Resource Asymmetry" is the problem.

Evolution of (D)DoS in history

Time

- 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

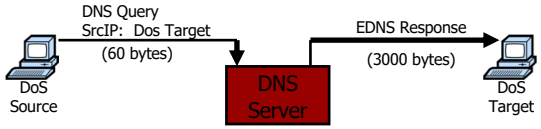


- Send ping request to broadcast addr (ICMP Echo Req)
- Lots of responses:
  - Every host on target network generates a ping reply (ICMP Echo Reply) to victim

Prevention: reject external packets to broadcast address

Modern day example (May '06)

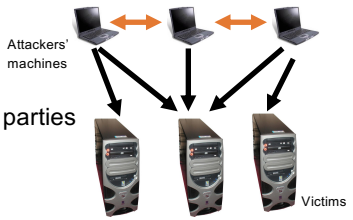
DNS Amplification attack: (×50 amplification)



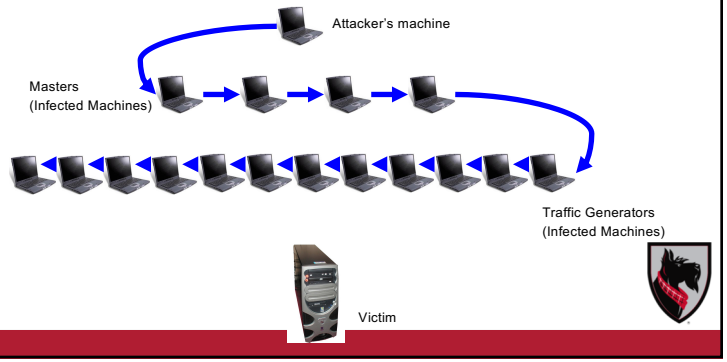
580,000 open resolvers on Internet (Kaminsky-Shiffman'06)

Coordinated DoS

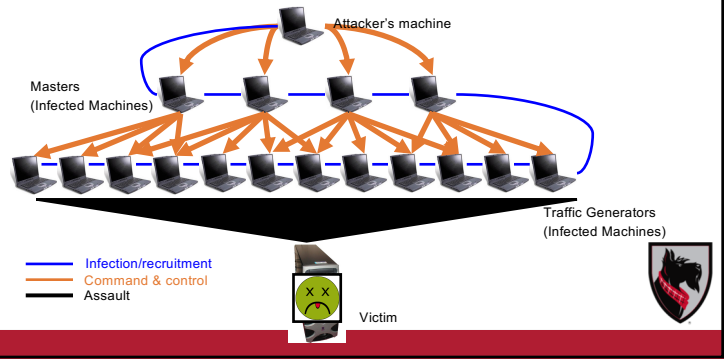
- Simple extension of DoS
- Coordination between multiple parties
  - Can be done off-band
  - IRC channels, email…



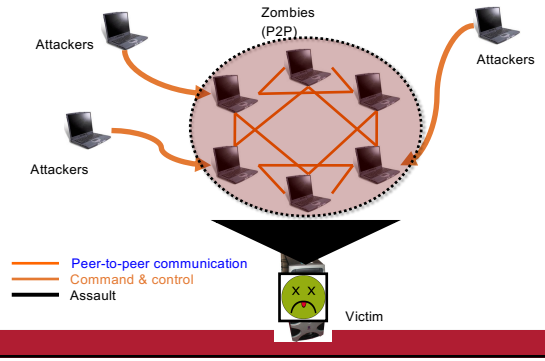
Typical DDoS setup circa 2005



Typical DDoS setup circa 2005



Modern Botnet setup



Goal: Overload the Host and Disable their Availability

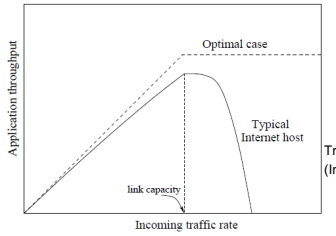
- Multiple ways to achieve overload!
  - Smurf and DNS amplification attacks overload the network link.
    - Botnets can do that too.

DoS Attacks Characteristics

- Link flooding causes high loss rates for incoming traffic
- TCPthroughput

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

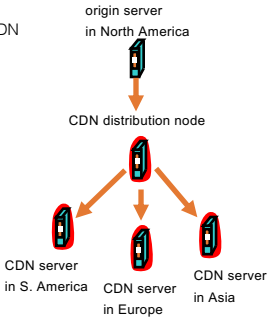
- During DoS few legitimate clients served



Traffic Generators (Infected Machines)

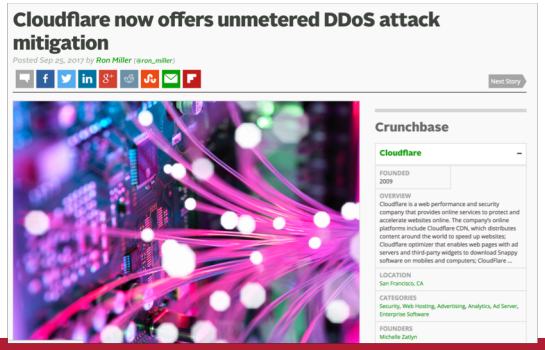
Content Distribution Networks (CDNs)

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

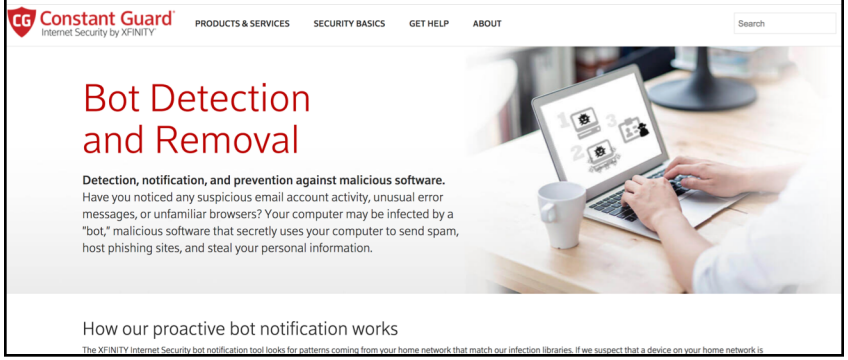


- How can this help DDoS?
- Legitimate requests can still go through
- Attack scale must be higher

Some CDNs even specialize in DDoS Defense!



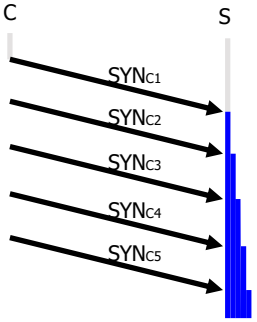
Finding the Zombies and Killing Them



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: low rate (DoS bug)



Single machine:

- SYN Packets with **random source IP addresses**
- Fills up backlog queue on server
- No further connections possible

SYN Floods (phrack 48, no 13, 1996)

OS	Backlog queue size
Linux 1.2.x	10
FreeBSD 2.1.5	128
WinNT 4.0	6

Backlog timeout: 3 minutes

⇒ 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 = MAC_{key} (SAddr, SPort, DAddr, DPort, SN_C, T) [24 bits]
    - key: picked at random during boot
  - SN_S = (T . mss . L) (|L| = 24 bits)
  - **Server does not save state** (other TCP options are lost)
- Honest client responds with ACK ($AN=SN_S$, $SN=SN_C+1$)
  - Server allocates space for socket only if valid SN_S.

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

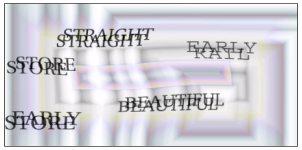
Client puzzles

- Idea: slow down attacker
- Moderately hard problem:
  - Given challenge C find X such that
    $LSB_n(SHA\text{-}1(C \,||\, X)) = 0^n$
  - 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 [Killbots '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:
- http://nabcop.org/index.php/DDoS-DoS-attack-BCOP
- 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