Protecting the infrastructure
Introduction

CSCI E 45b: The Cyber World – part B

1

Introduction: learning goals

- Understand the types of threats that use the Internet for connectivity
- Understand some of the threats to the Internet and some of the approaches the US government has used to try to reduce them
- Understand denial of service types of attacks

2

Introduction: learning goals, contd.

- Understand the vulnerabilities in the Internet routing system, the the threats to it and ways to mitigate the threats
- Understand the vulnerabilities in the domain name system, the the threats to it and ways to mitigate the threats

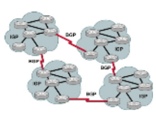
3

Introduction: learning goals, contd.

- Understand the difficulties presented by emergency communications using the Internet

4

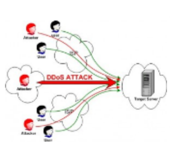
Topics

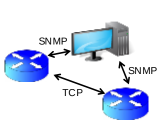


- Threats via the Internet - R
  - Espionage, theft, disruption & extortion
  - Some contributing factors
- Threats to the Internet – R
  - Threat mitigation approach used in the telephone network
  - The different types of threats to the Internet itself
  - U.S. government efforts to mitigate threats to the Internet

5

Topics, contd.





- Denial of service attacks - R
  - The technology behind a DoS attack
  - DoS targets
- Internet Addressing 101, Routing 101 – O
  - Review of Internet routing and addressing
- Threats to routing – R
  - Disruption, Falsification, stress
  - Mitigation approaches

6

Topics, contd.

- Threats to DNS - R
  - DoS threats to root servers & mitigation design
  - Threats to DNS resolving process & mitigation technology
- Emergency communications - R
  - Citizen to government
  - Government to citizen
  - Government to government

7

Image credits

Slide#	credit
5	https://en.wikipedia.org/wiki/Nuclear_power_plant
	http://ciscorouterswitch.over-blog.com/article-bgp-protocol-is-essential-in-your-ip-network-115059468.html
6	https://kshitiz25.wordpress.com/2012/04/12/denialof-service-dos-attack/
7	http://www.prweb.com/releases/2009/03/prweb2199054.htm

8

Protecting the infrastructure

Threats via the Internet

CSCI E 45b: The Cyber World – part B

1

Threat via the Internet

- Internet provides an attack path
  - From anywhere to anywhere
- Threats
  - Espionage & theft
    - e.g., NSA, industrial, political & military secrets
    - e.g., personal information
  - Disruption
    - e.g., reprogram industrial controllers
  - Extortion
    - e.g., threat to do the above
    - For monetary or other reason

2

Threats via the Internet, contd.

- We cover a lot of threats over the Internet in other modules
- Beyond phishing, DDoS, hacking banks, and other Internet-y things, the Internet also provides a control path for many industrial, physical control systems
  - SCADA (Supervisory control and data acquisition) controllers particularly vulnerable

3

Power System as an Example

'The System has been designed to perform all power plant automation tasks: turbine control, boiler control including boiler protection, balance of plant (BOP) and integration of third party systems, such as gasification islands in IGCC applications.'

SIEMENS

- Power plant controllers (e.g., SCADA) are connected to the Internet
  - Makes management "easier"
- e.g. Siemens Power Plant Automation
  - Web-based interface
    - Can control from "virtually anywhere"
- A major risk, even if the security was good
  - Which it is not

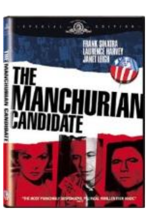
4

Power Plant Controllers, contd.

- A controller can be reprogrammed to cause a controlled device to self destruct
  - e.g. Stuxnet
- The Aurora Project showed that power generators could be made to self destruct
  - Note: big power generators are no longer made in the US – they are made in China & India
    - And can take years to be delivered

5

Power Plant Controllers, contd.



- Chinese hackers are attacking US infrastructure
  - What if: these hackers reprogrammed controllers to wait for a signal to destroy the generators
    - *"Manchurian controllers"*

6

Power Plant Controllers, contd.

Joel Brenner

- *America the Vulnerable* (Brenner) paints such a scenario
- Brenner recommended (in Sept. 2011):
  - Creating industry standards blocking connecting infrastructure controllers directly or indirectly to the Internet
  - And federal regulations requiring power companies disclose any connections in their SEC filings

7

Power Plant Controllers, contd.

- Note: it is likely far too late to prevent compromising the controllers
  - But it may not be too late to prevent the activation

8

Data

- Far too much data is accessible to far too many people
  - e.g., Manning & Snowden - Why should they have had the access to all the information?
    - (Why was there no alarm for large downloads?)

9

Data

- e.g., corporate America
  - A: Too much data
    - Why store millions of SSNs or credit card numbers?
  - B: Too little compartmentalization
    - Company president & mail room clerk do not need direct access to corporate secret data
    - How was the RSA attacker able to leverage access of an admin assistant to find and steal customer seed files?

10

Data, contd.

- All major industries under relentless attack
- To find & steal industrial secrets
  - e.g., Chinese hackers
    - Against Google & 33 other companies
    - Against RSA and 760 other companies
  - e.g. Russian hackers
    - Against Citibank
  - e.g., French espionage
    - Provided discovered secrets to French companies
  - e.g., NSA

11

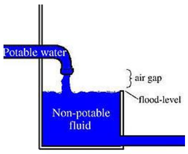
Lessons

- If the data or control is accessible via the Internet, it will be accessed
  - It is only a matter of time & perseverance
  - The hackers are getting very, very good
  - Software is not getting much better
- Compartmentalize!
  - Needs-based access

12

Lessons, contd.

- Isolate!
  - An air gap helps
    - But does not cure people (e.g., Stuxnet)



13

Image credits

Slide#	credit
2	https://en.wikipedia.org/wiki/National_Security_Agency
3	https://en.wikipedia.org/wiki/Nuclear_power_plant
4	http://www.energy.siemens.com/us/en/automation/power-generation/sppa-products/sppa-t3000.htm
5	http://therunagatesclub.blogspot.com/2007/09/aurora-cyber-attack-destroyed-million.html
6	http://www.amazon.com/The-Manchurian-Candidate-Special-Edition/dp/B00020X88Y
7	http://www.streetnewsservice.org/news/2011/may/feed-278/in-cyberspy-vs-cyberspy,-china-has-the-edge.aspx
10	target - https://commons.wikimedia.org/wiki/File:Target_logo.svg
	jp morgan - http://www.brookstonelaw.com/cases/potter-vs-jp-morgan-chase/
	rsa - https://commons.wikimedia.org/wiki/File:RSA_Security_logo.svg
11	China - https://commons.wikimedia.org/wiki/File:China-outline.png
	Russia - http://andrewmonaghan.net/
	France - http://www.france-pub.com/emap3.htm
	nsa - https://en.wikipedia.org/wiki/National_Security_Agency
12	http://www.pivotaladvisors.com/blog/?p=168
13	http://www.mymcws.com/index.php/cross-connections

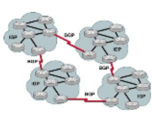
14

Protecting the infrastructure

Threats to the Internet

CSCI E 45b: The Cyber World – part B

Threats to the Internet



- Attack Internet infrastructure servers
  - e.g., DNS, whois
- Attack routers
- Attack routing
  - e.g., BGP
- Attack links
  - e.g., DoS attack on router ports

Old Phone System

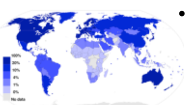
- Regulations and industry groups ensured reliable design and operation of old phone system
  - e.g., *Network Reliability and Interoperability Council (NRIC)*
- Multiple levels of redundancy
  - e.g., batteries and generators (and generators)
- Regulations ensured money to fund redundancy, etc.
  - But even that is not perfect
    - Human failure at Hinsdale, etc.

Old Phone System, contd.

- Future of reliability is uncertain as the phone system moves more to an unregulated model
  - no profit guarantee may impact design & operation
- Old phone system:
  - Assumed a closed & protected network
  - Almost no security in the protocols themselves
    - e.g., Signaling System 7 (SS7)
  - Now big security threat with Internet replacement

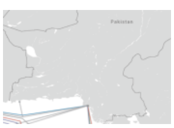
4 Copyright © Scott Bradner & Ben Gaucherin 2016

Internet



Fixed broadband Internet penetration - 2012

- Most developed countries are dependent on the proper functioning of the Internet
- But the Internet grew up unregulated
  - With no profit guarantees for extra cost of reliability
- Inherently redundant topological design
  - Except for tail circuits
  - e.g., single underwater cable for all of Pakistan in 2005



Pakistan cables - 2015

5 Copyright © Scott Bradner & Ben Gaucherin 2016

Internet, contd.

Security Considerations

Security issues are not discussed in this memo.

RFC 1654 BGP-4 1994

Security Considerations

BGP vulnerabilities analysis is discussed in [RFC4272].

RFC 4271 BGP-4 2006

- In-band controls can expose controls to attack
- Original infrastructure technologies not designed with security in mind
  - And in some cases, it was a conscious choice: e.g., IP
  - IETF standards since 1994 must address security

6 Copyright © Scott Bradner & Ben Gaucherin 2016

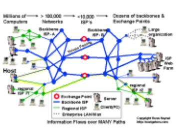
Internet, Pre 9/11

- General government concern but no real action
- NRIC started discussing Internet "best practices" for reliability

  But little participation by ISPs

7

Internet, Pre 9/11, contd.



Internet physical layer

- Big ISPs felt redundant topology would survive significant attacks

  They were right

- Small ISPs could not afford to worry about it

8

Internet, Post 9/11

- A push at the US Federal level to worry about terrorism just about everywhere
- Including the US cyber infrastructure

  Task force produced *"The National Strategy to Secure Cyberspace"* February 2003

  Directions but no teeth

9

Internet, Post 9/11, contd.

Richard Clarke

- Cybersecurity czar appointed
  - Richard Clarke - was president Bush's counterterrorism coordinator at the time of 9/11
  - Later resigned when DHS was formed and cybersecurity did not get as much attention as he wanted

10

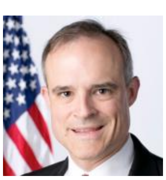
Internet, Post 9/11


Howard Schmidt

- President Obama named Howard Schmidt to be US Cybersecurity Czar on Dec 22, 2009
  - A number of people had turned down an offer of the job
    - 'responsibility without authority'
- Schmidt was an advisor to President Bush & chief security officer at Microsoft
- But little agreement on what the job actually means
- Schmidt resigned May 2012

11

Cybersecurity Czar, contd.


Michael Daniel

- Replaced by Michael Daniel
  - Special Assistant to the President and Cybersecurity Coordinator
  - *"leads the interagency development of national cybersecurity strategy and policy"*
  - *"ensures that the federal government is effectively partnering with the private sector, non-governmental organizations, other branches and levels of government, and other nations."*
- Role eliminated 2018

12

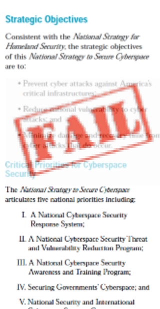
Cybersecurity Czar, contd.

Chris Inglis

replaced by Harry Coker, Jr in December 2023

- Chris Inglis confirmed June 2021 as National Cyber Director
  - Special Assistant to the President and Cybersecurity Coordinator
  - *"The National Cyber Director serves as a principal advisor to the President on cybersecurity policy and strategy, and cybersecurity engagement with industry and international stakeholders."*

Strategy to Secure Cyberspace - 2003



- Objectives
  - Prevent cyber attacks
  - Reduce vulnerability to attacks
  - Minimize damage and recovery time from an attack
- Priorities
  - Create cybersecurity response system
  - Create security threat and vulnerability reduction program
  - Create security awareness program
  - Secure government cyberspace
  - National and international cybersecurity cooperation

Vulnerability Reduction Program

- Secure Internet mechanisms
  - Improve security and resilience of key protocols
    - Use IPv6, secure DNS, secure BGP
  - Improve routing
    - Address verification, out of band management
  - Improve management
- Foster trusted control systems
- Reduce software vulnerabilities
- Understand infrastructure independence

Federal Efforts

- CMU CERT continuing
  - Paid for by US government
  - Formed in 1989 after Morris Worm
  - Now close relationship with DHS & US-CERT
- Mostly known for releasing information about software vulnerabilities
  - But not until vendors fix them

15

Federal Efforts, contd.

- Some work was done in NRIC
  - Network Reliability and Interoperability Council (NRIC) not renewed after 2005
- Replaced by *Communications Security, Reliability and Interoperability Council* (CSRIC) in 2007
  - Renewed every 2 years – current: CSRIC VIII
  - 6 working groups, e.g., NG 9-1-1
- FCC advisory group
- Industry led development of 'voluntary Best Practices'

16

Federal Efforts, contd.


President Joe Biden

- President Biden signed a Cybersecurity Executive Order 12 May 2021
  - EO 1428
  - many provisions including
  - improve security of US government systems
    - using government purchasing power
    - $70 B IT purchasing
  - improve incident response
    - IT providers must report issues
    - private sector share info with government confidentially
    - push security info on products

17

Federal Efforts, contd.

- Core agency: Cybersecurity & Infrastructure Security Agency (CISA)
  - Within Department of Homeland Security
  - Established Nov 2018
  - Current Director: Jen Easterly
  - Budget: $3.16 B
  - includes US-CERT & StopRansomware.gov

CISA works with partners to defend against today's threats and collaborates to build a more secure and resilient infrastructure for the future.

Jen Easterly

18

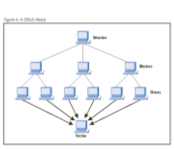
Federal Efforts, contd.

- Historically voluntary guidelines
  - developed in cooperation with industry
- Starting to become mandatory
  - e.g., July 2021 pipeline security regulations
  - announced but not made public
    - WaPO got a redacted copy via FOIA
  - pushback from some in Congress
    - wanted less direction
- **Revised & reissued a year later**

UPDATED

19

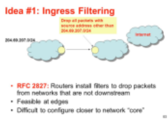
Protecting Network Infrastructure



- Threats
  - Brute force denial of service (DoS)
  - Disrupting core network services
    - Routing
    - Domain Name System (DNS)
  - Disrupting control systems
  - Disrupting network users
    - Emergency communications
    - Control systems for non-network infrastructures
- Threats apply to both enterprise and Internet

22

Clean Living



replaced by RFC 6890

UPDATED

- Ingress filtering at borders

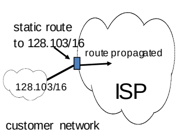
  ISP: discard incoming packets with source addresses outside of customer ranges

  Enterprise: discard packets with source addresses within customer ranges

  Filter out all packets using private addresses or other non-routed addresses (RFC 5735) (bogon addresses) going across the border

23 Copyright © Scott Bradner & Ben Gaucherin 2024

Clean Living, contd.



- ISP: use static routing where feasible

  (i.e., do not accept routing updates from customers)

24 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide# credit

2 http://ciscorouterswitch.over-blog.com/article-bgp-protocol-is-essential-in-your-ip-network-115059468.html

3 & 7 https://transition.fcc.gov/nric/nric-6/06022003/industry-collaboration-presentation.ppt

4 battery - http://apibattery.com/projects/telecom-lawrence-ks/

att logo- http://cfarthistory.blogspot.com/2013/12/graphic-design-at-history-and-logo.html

5 http://www.vox.com/a/internet-maps

http://www.submarinecablemap.com

6 http://www.ietf.org/rfc/rfc-1654.txt

http://www.ietf.org/rfc/rfc-4271.txt

8 http://navigators.com/sessphys.html

9 & 13 https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

10 https://raymondpronk.wordpress.com/tag/against-all-enemies/

11 http://www.securitysquared.com/2009/12/issa-president-howard-schmidt-named-cybersecurity-czar.html

25 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Slide#	credit
12	https://www.whitehouse.gov/blog/author/michael-daniel
15	https://www.cylab.cmu.edu/news_events/news/2009/square-tool-released.html
	https://www.southernstates.com/catalog/p-10701-black-flag-roach-motel-2pk.aspx
16	http://itlaw.wikia.com/wiki/Communications_Security,_Reliability_and_Interoperability_Council
17	https://www.whitehouse.gov/administration/president-biden
18	https://en.wikipedia.org/wiki/Cybersecurity_and_Infrastructure_Security_Agency
	https://en.wikipedia.org/wiki/Jen_Easterly
17	http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html
23	http://slideplayer.com/slide/697431/

Protecting the infrastructure
Denial of service (DoS) attacks

CSCI E 45b: The Cyber World – part B

Denial of Service (DoS)

201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH

. . .

17.04: **Computer System Security Requirements**

. . .

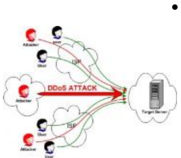
… a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following elements:

. . .

(e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

- Multiple attacks
  - Disrupt access
  - Overload network link
  - Overload service
  - …
- Aim of a DoS attack is to interrupt use
  - i.e., deny service to a user
  - Low effort example
    - Mount password guessing attack on account protected by an automatic lockout on bad guesses
    - User denied access to their account

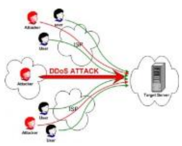
DoS, Overload Link



- Flood a network link with more traffic than it can handle
- For example, by a distributed DoS attack
  - Traffic from many sources (e.g., hijacked PCs) addressed to flow though a target link
  - e.g., Microsoft DNS servers in 2001

DoS, Overload Link

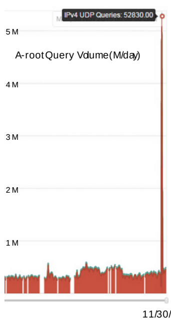
attack of 71 million requests per second Feb 2023



- Blocks all types of traffic on link
- Basic network functioning can be maintained if control traffic is set to have a higher priority
  - But that provides an attack opportunity
    - Be sure to strip any elevated priority bits on ingress to the network
- Business opportunity for mitigation services

4

Disrupting Support Services



- Some services must run for network to work correctly
  - e.g., routing, DNS, NTP
- Well planned disruption could (in theory) make Internet unusable
- Few determined attacks in the past
- Some protections have been added

5

Disrupting Support Services, contd.


Ways Terrorists May Use the Internet

There are some ways that terrorists use the internet, like publicity, that are common knowledge. There is strong evidence that terrorists use the internet in other ways, such as communication by email. There are other ways terrorists could use the internet that there is not evidence of, but since detection systems are recently developed technologies, there could be much terrorist activity that goes undetected. Lieutenant Colonel Timothy L. Thomas, an analyst with the U.S. Army Foreign Military Studies Office, suggests that there are nine ways that terrorists could use the internet. Some of them are probable, some of them are possible, but most of them are uncertain. In many of the suggested uses of the internet, the terrorist would wish to remain undetected.

The nine ways are:

- Note that the bad guys need the net to be working in order to be able to communicate
  - But that does not mean a rogue group will not attack

6

Image credits

Slide#	credit
2	http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf
3 & 4	https://kshitiz25.wordpress.com/2012/04/12/denial-of-service-dos-attack/
5	http://timesoracle.com/2015/12/attack-on-root-dns-servers-blasted-5-million-queries-eery.html
6	http://www.mtholyoke.edu/~lwpoole/politics116/ways.html

Protecting the infrastructure

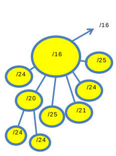
Internet Addressing 101, Routing 101

CSCI E 45b: The Cyber World – part B

Internet addressing 101

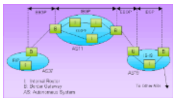
Internet Addressing 101

Internet Assigned Numbers Authority



- Top level: IANA
  - Allocate big blocks of addresses (address prefixes) to Regional Internet Registries (RIRs)
    - 5 RIRs, each with own geographic territory
- RIRs allocate smaller address prefixes to ISPs
  - And to some multi-homed end sites
- ISPs allocate address prefixes to customers
  - Some customers can be smaller ISPs

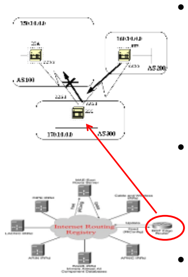
Autonomous System (AS)



- AS number used to indicate routing entity
- In BGP4, a routing entity is a BGP speaker
  - ISP or multi-homed enterprise
- Allocated by RIRs
- To BGP4, the Internet is a collection of interconnected ASs

4

Address Filtering



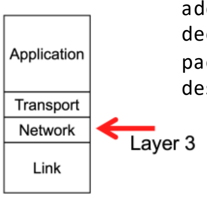
- Big ISPs filter incoming routing advertisements
  - Only accept prefixes that meet business, policy or security criteria
    - e.g., discard advertisements for non-legit (e.g. private) addresses
- Some use the routing registry
  - ISPs list their routing policies & prefix announcements
  - Volunteer effort
- No sure way to know if a routing advertisement is legitimate

5

Routing 101

6

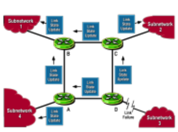
Internet Routing 101



- The Internet is a collection of networks interconnected with "routers"
- Routers use the "layer 3" addresses (IP addresses) to decide how to forward data packets towards a destination

7

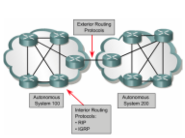
Internet Routing 101, contd.



- Routers exchange reachability and topology information using routing protocols
  - Information includes address "prefixes" - address ranges

8

Routing

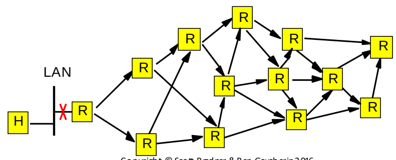


- Two basic types of routing protocols
  - Interior gateway protocols (IGP): within an organization
    - e.g., RIP, OSPF, IS-IS
  - Exterior gateway protocols (EGP): between organizations
    - e.g., BGP4
- Different trust and security environments
  - IGP: within single trust and security environment
  - EGP: between trust and security environments

9

Routing: Change Notification

- Router adjacent to change informs its neighbors of changes
- Information propagates throughout network
- Other routers adjust tables based on new information



Routing: Finding Routers

```
router rip
 version 2
 network 172.88.16.0
 default-information originate route-map condition
```

- RIP/OSPF/IS-IS (IGPs): auto discovery

  Finds other routers on the LAN or on direct links and starts exchanging routing information

```
router bgp 100
 neighbor external-peers peer-group
 neighbor external-peers route-map set-metric out
 neighbor external-peers filter-list 99 out
 neighbor external-peers filter-list 101 in
 neighbor 171.69.232.90 remote-as 200
 neighbor 171.69.232.90 peer-group external-peers
 neighbor 171.69.232.100 remote-as 300
 neighbor 171.69.232.100 peer-group external-peers
 neighbor 171.69.232.110 remote-as 400
 neighbor 171.69.232.110 peer-group external-peers
 neighbor 171.69.232.110 filter-list 400 in
```

- BGP4 (EGP): manual configuration

  Not restricted to same LAN or direct links

  Only interacts with other routers listed in configuration files

  - Security advantage

Image credits

Drawings by Scott Bradner unless noted

Slide#	credit
3	https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority
	https://www.nro.net/about-the-nro/regional-internet-registries
4	https://www.pinterest.com/pin/478437160389819582/
5	http://www.ittc.ku.edu/EECS/EECS_800.ira/bgp_tutorial/15.html
	http://www.assignmenthelp.net/analysis-of-the-internet-routing-registry
7	http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_13-1/131_aggregation.html
8	http://www.hill2dot0.com/wiki/index.php?title=Link_state_routing_protocol
9	http://studynet-work.blogspot.com/2011/09/igp-vs-egp.html
11	http://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfrip.html
	http://www.cisco.com/c/en/us/td/docs/ios/12_2/iproute/command/reference/fiprrp_r/1rfbgp2.html

Protecting the infrastructure

Threats to routing

CSCI E 45b: The Cyber World – part B

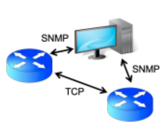
1

Routing: Threats

- Disruption
  - Disrupt routing protocol communication
    - e.g., kill BGP-4 inter-router sessions
- Falsification
  - Inject false information - e.g., Pakistan & YouTube
    - e.g., claim you own a prefix that you do not own
    - e.g., claim that you know how to reach a prefix that you do not
- Stress
  - Overload adjacent routers
    - e.g., send too many prefixes

2

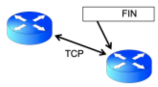
Routing: Weak Points



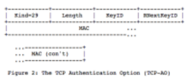
- For disruption
  - Router to router communications
  - Management station to router communication
- For falsification
  - Prefix origin authentication
    - Was prefix properly allocated to this site?
  - Prefix origin authorization
    - Is ISP authorized by owner to originate this prefix?
  - Router authorization
    - Is router authorized to forward prefix?

3

Routing: Protection From Disruption

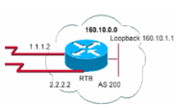


- Secure router-to-router communication
  - e.g., threat: send TCP packets with FIN bit on in them with forged source address - kills session
    - BGP forgets all routes learned through killed session
  - e.g., TCP Authentication Option - used with BGP4
    - TCP option that adds message authentication code to TCP packets
      - Usually keyed hash
    - Forged packets are discarded



Routing: Protection From Disruption, contd.

- Secure router-to-router communication, contd.
  - e.g., solution: make router interfaces externally unreachable
    - Use private addresses, add filters to permit known sources only
- Protect against interface failure
  - Use loopback address for management
  - An address for the router itself, rather than an address of a particular interface



Routing: Disruption, contd.

- Secure management station to router communication
  - Use SNMPv3 - secure SNMP
  - Use SSH - individual secure login
  - Use loopback address for management traffic
  - Filter in router for management station source address
  - Filter out at border any traffic to router loopback addresses

Routing: Disruption, contd.

RANCID
Really Awesome New Cisco conflg Differ

Number	Value	Name
0	0	EOOL - End of Options List
1	1	NOP - No Operation
2	130	SEC - Security
3	131	LSR - Loose Source Route
4	68	TS - Time Stamp
5	133	E-SEC - Extended Security
6	134	CIPSO - Commercial Security
7	7	RR - Record Route
8	136	SID - Stream ID
9	137	SSR - Strict Source Route
10	10	ZSU - Experimental Measurement
11	11	MTUP - MTU Probe
12	12	MTUR - MTU Reply
13	205	FINN - Experimental Flow Control
14	142	VISA - Experimental Access Control
15	15	ENCODE - ???
16	144	IMITD - IMI Traffic Descriptor
17	145	EIP - Extended Internet Protocol
18	82	TR - Traceroute
19	147	ADDEXT - Address Extension
20	148	RTRALT - Router Alert
21	149	SDB - Selective Directed Broadcast

- Verify router configuration files
  - Retrieve files nightly and compare to master copy in database
    - Check for technician-made or hacker-made changes
- Filter out packets which can cause high processing loads
  - e.g., packets with IP header options
- Rate control processing of management packets
  - e.g., pings to router ports

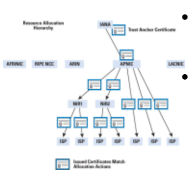
7

Secure Inter-Domain Routing

- IETF working group (sidr)
- Improve security for interdomain routing
- Provide assurance of legitimacy of routing information
  - (i.e., not securing communication channel between two routers)
- Making progress after many years of IETF stalemate

8

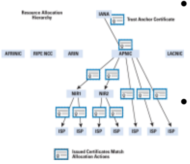
SIDR, parts



- Function-specific PKI
  - For routing infrastructure
- Signed routing objects
  - Entity can verifiably assert ownership of addresses or ASs
  - Owner of address prefix can authorize an AS to advertise the prefix
- Distributed repository system
  - Hold information to support PKI
  - Hold signed routing objects

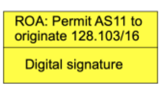
9

SIDR, RPKI



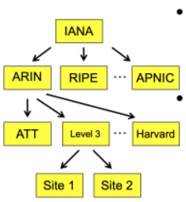
- Resource Public Key Infrastructure
  - PKI for Internet number resources - IP addresses or ASs
- Resource Certificates: attest to an allocation
  - Issued by allocator of resource
  - Bind public key to resource
  - *CA certificates*: allocating entity assertion of allocation
  - *End-Entity certificates*: public key used to validate ROAs and manifests

SIDR, RPKI, contd.



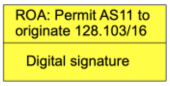
- Route Origin Authorization (ROA)
  - Resource holder authorization for AS to advertise prefix(s)
- Manifest
  - Signed list of published signed objects

SIDR, RPKI: CA Certificates



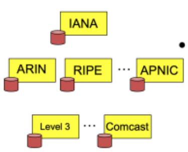
- IANA provides CA certificates for allocations to RIRs
- RIRs provide CA certificates for allocations to ...
  - Where "..." is ISP, end site or local Internet registry, etc.
- ISPs provide CA certificates for any allocations they do
- Subject name in certificate is unimportant
  - Must be locally unique

SIDR, RPKI: ROA



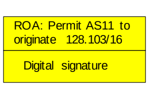
- Contains one AS and a list of address prefixes
  - Means that AS is authorized to advertise those prefixes
- Signed by private key corresponding to pubic key in a EE (*End-Entity)* certificate
- Only valid if EE certificate is valid
  - Revoking EE certificate revokes ROA
  - Validity time: several months

SIDR, RPKI: Repositories



- Made up of distributed databases
- Each registry will maintain database containing all CA and EE certificates associated with that registry
- Each ISP will maintain a database containing all CA, EE and ROA certificates associated with the ISP
- Public databases

SIDR, First Phase



- First phase only provides origin prefix authentications and authorizations
  - i.e., that a prefix was properly allocated & the origin AS is legit
  - Does not validate AS path
- Further work now underway

Routing Threats, Insider

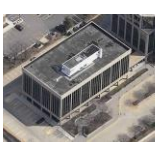
- Insiders can cause major problems
  - On purpose, or by accident
- e.g., AS 7007 case (04/97)
  - Deaggregated and re-advertised entire Internet routing table
  - Overloaded routing tables on peer routers
  - May have been "simple" misconfiguration or a bug
  - ISPs now filter for max number of prefixes from a peer

Routing threats - software

- Routers have large and complex software systems
- Thus, they are subject to software bugs
- E.g., vulnerabilities to malformed packets

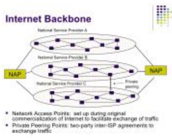

SECURITY WEEK
Cisco Routing Systems Vulnerable to Malformed IPv6 Packet Attacks
Cisco Fixes DoS Vulnerability in IOS XR Software
Cisco has released software updates to address a denial-of-service (DoS) vulnerability in IOS XR Software, a self-healing and fully distributed network operating system designed for service providers.

BGP Security, How Big a Problem?


MAE East

- Congressional testimony 'take down net in 30 min'
- Assumed using TCP resets on BGP sessions on public peering points between ISPs
  - Spoof packet must include correct src & dest addresses, src & dest port and sequence #
    - Can loop trying different combinations

BGP Security, How Big a Problem, contd.



- But most ISP peering is private
  - And packet filters ensure packets are coming from correct physical link
  - Use of TCP Authentication Option means attacker would have to know secret key
- Guessing would take enough time for attack to be seen and blocked

19 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Figures by Scott Bradner unless noted

Slide#	credit
2	https://www.youtube.com/yt/brand/downloads.html
3	http://iconbug.com/detail/icon/1809/windows-vista-workstation/
5	http://superuser.com/questions/611736/private-address-in-traceroute-results
	http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html
6	snmp - http://forumspain.net/thread/linux-snmpv3-snmpd.conf.html
7	http://www.iana.org/assignments/ip-param et ers/ip-para met ers. xhtml
8	https://www.ietf.org/logo/
9	https://www.nro.net/about-the-nro/regional-internet-registries
	http://www.cisco.com/web/about/ac123/ac147/archived_issu es/ip j_14-2/142_bgp.html
10 & 12	http://www.cisco.com/web/about/ac123/ac147/archived_issu es/ip j_14-2/142_bgp.html
16	http://www.mainet.com/
17	http://www.securityweek.com/cisco-routing-systems- vulner abl e-malform ed-ipv6-packet-attacks
18	https://cryptome.org/eyeball/m a e-e ast/m ae e-birdse ye .htm
19	http://www.slideshare.net/sangusajj an/unit-i-packet-switchin g-networks - slide 19

20 Copyright © Scott Bradner & Ben Gaucherin 2016

Protecting the infrastructure

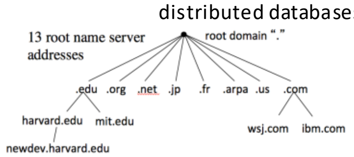
Threats to DNS

CSCI E 45b: The Cyber World – part B

1

Domain Name System (DNS) 101

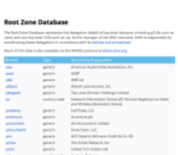
- DNS translates human friendly alphanumeric, case insensitive names into IP addresses
  - Long lived DNS names into short lived IP addresses
- DNS is a hierarchical set of distributed databases



name servers for each domain have a database of next lower level entries

2

DNS, Root Servers



- Contents of root name server database is pointers to servers for "top level domains" - e.g., .com
  - Database maintained by IANA

3

DNS, Root Servers

- Only space in DNS packet for 13 IP addresses of root name servers
  - But single IP address can be shared by many servers
    - Called "anycast"
  - Anycast address injected into routing system at multiple locations
    - Packets routed to "nearest" one
- Servers located all over the world
  - The 13 root servers are mirrored in more than 1754 actual servers

2023-09-27

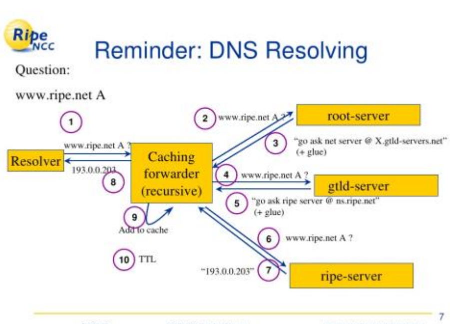
DNS, Anycast Root Servers

- DoS attacks mitigated
  - e.g., DDoS attack on roots November 30, 2015
- Some servers, not anycast, impacted

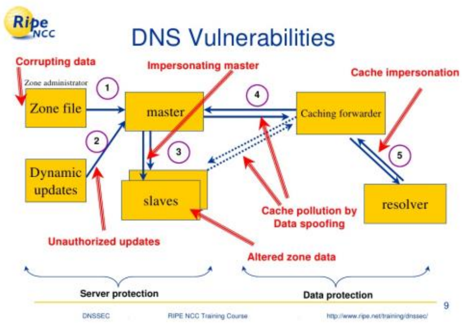
DNS query load

DNS server health during the attack

DNS, resolving sequence



DNS, Vulnerabilities



DNS, Threats

```
golem> dig qaws2.com

; <<>> DiG 9.8.3-P1 <<>> qaws2.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode QUERY, status: NXDOMAIN
id: 5588
;; flags: qr rd ra; QUERY: 1, ANSWER 0, AUTHORITY: 1,
ADDITIONAL: 0

;; QUESTION SECTION:
;qaws2.com.                     IN
            A

;; AUTHORITY SECTION:
com.                            900
            IN          SOA
            a.gtld-servers.net. nstld.verisign-
grs.com. 1451005688 1800 900 604800 86400

;; Query time: 23 msec
;; SERVER 127.0.0.1#53(127.0.01)
;; WHEN: Thu Dec 24 2008:24 2015
;; MSG SIZE  rcvd: 100
```

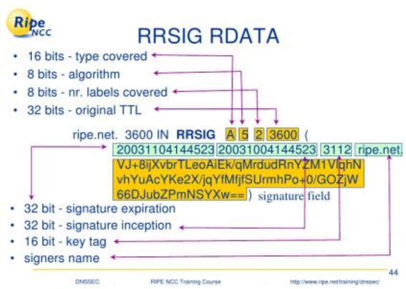
- How does client know that resolution came from correct server?
- How does client know that data was not modified in transit
- How does client know that NXDOMAIN is real

DNS message that says a domain does not exist

DNSSEC

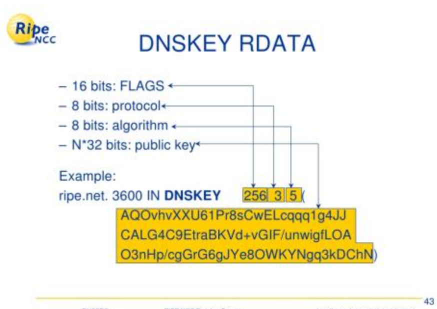
- Authenticates data exchanges in DNS system
- Provides for data integrity of DNS data
- Sign data in domain zones
- Describe gaps in zone (NXDOMAIN) and sign
- Sign resource records in zone

DNSSEC: signature for DNS entry



10

DNSSEC: public keys published in DNS



11

DNSSEC, political issue

Internet Assigned Numbers Authority

- Root signed in July 2010
  - Political issue: who manages the root private key?
    - Keyholder could, in theory, lock countries (ccTLDs) out of DNS

12

Image credits

Figures by Scott Bradner unless noted

Slide#	credit
3	http://www.iana.org/domains/root/db
4	http://www.root-servers.org/
5	http://www.ibtimes.co.uk/are-isis-hackers-trying-destroy-internet-1533332
	http://www.theregister.co.uk/2015/12/08/internet_root_servers_ddos/
6	http://www.slideshare.net/guest3131f85/dnssec – slide 7
7	http://www.slideshare.net/guest3131f85/dnssec – slide 9
9	http://www.prweb.com/releases/2009/03/prweb2199054.htm
10	http://www.slideshare.net/guest3131f85/dnssec – slide 44
11	http://www.slideshare.net/guest3131f85/dnssec – slide 43
12	https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority

Protecting the infrastructure
Emergency communications

CSCI E 45b: The Cyber World – part B

Emergency Communications 101

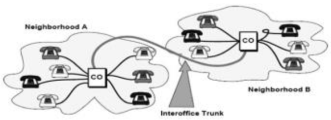
- Different situations
  - Citizen to government
    - e.g., 911 - request emergency help
  - Government to citizen
    - e.g., emergency broadcast system - warn of tornado
    - E.g., Amber alert
  - Government to government
    - e.g., GETS - emergency workers communicating

Emergency Communications, Contd.

- What to do in a congested network?
  - Citizen to government
    - Cannot authenticate citizens - so cannot give special treatment
    - DoS risk
  - Government to citizen -
    - Assume authentication - but how to interact with access networks?
    - i.e., how to pass authentication and authorization?
    - What kind of special handling?
  - Government to government
    - Same issues as government to citizen except authentication is harder

Emergency Communications, Contd.

- Big problem #1 - regulators assume that the Internet works like the PSTN
- PSTN admission control means calls only go through if there is enough capacity
  - Fast busy signal if not
  - No such function on the packet-based Internet



4

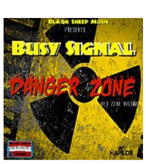
Emergency Communications, Contd.

- GETS provides for priority call placement
  - **G**overnment **E**mergency **T**elecommunications **S**ervice
  - Does not preempt existing calls
    - Preemption = terminate other calls
    - Preemption illegal in the US
- Too many regulators assume that per-packet prioritization gets the same results

5

Emergency Communications, Contd.

Action granularity = call



- With PSTN & preemption
  - Limit total # of calls at each priority
  - Calls are allowed to be placed only if there is capacity so that they will receive full quality

6

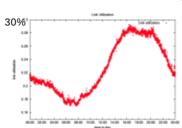
Emergency Communications, Contd.

Action granularity = packet

- With Internet and packet prioritization
  - No limit on # of calls
  - Packets lost from all calls if there is congestion
    - Lower priority calls lose more packets
  - Packet loss impacts call quality
    - Loss > 10% makes calls generally unintelligible
  - Simple prioritization of packets based on call value will mean that low-value calls will be useless
    - And high value calls will also if there are too many

7

Emergency Communications, Contd.



Google backbone link utilization

- Big problem #2 - regulators do not accept ISP's assertions that they have plenty of capacity
  - Insist on mandating QoS controls to support emergency communications
- ISPs are worried that any QoS controls would:
  - Make their networks more complex
  - Make their networks less secure
  - Make their networks more susceptible to DoS attacks

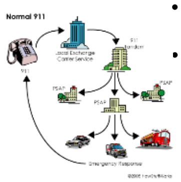
8

Citizen to government

- Enhanced 911 (E911)
- Need location to call, caller's location & call-back number
- Location to call: Public-safety answering point (PSAP) (U.S.)
  - Answers 911 calls
  - 5,748 PSAPs in U.S. (2023)
- Telephone company maps 911 call to number of PSAP that covers the area where the call is from
  - Not necessarily the closest PSAP
  - Usually use political boundaries

9

E911: wireline

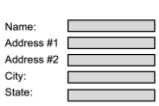


- Local phone company receives a call to 9-1-1
- Phone company needs to determine location of caller
  - Forwards call to special 911 telephone switch
  - 911 switch looks up calling number in a database to get location
    - Uses caller ID to get calling number
    - Maps calling number to location
      - Termination point of wire
      - Database usually maintained by local telephone company
- Looks up location in 2nd database to select PSAP

E911: cellular

- Local phone company receives call to 9-1-1
- Phone company needs to determine location of caller
  - Triangulation by multiple call towers
    - Signal strength, time difference, etc.
  - GPS in phones
- Looks up location in 2nd database to select PSAP

E911: VoIP



- Not supported by all vendors
- VoIP company receives call to 9-1-1
- Phone company needs to determine location of caller
  - Caller has recorded an address
    - Issue if customer moves phone and forgets to update location
  - Other options under development
- Looks up location in 2nd database to select PSAP

Next Generation 911 (NG9-1-1)

- North American Emergency Number Association developed an IP-based emergency calling system for North America
  - Slow deployment (started 2008)
- Based on IETF standards
  - *Geographic Location/Privacy (geopriv) WG*
    - 32 RFCs, including location object
  - *Emergency Context Resolution with Internet Technologies (ecrit) WG*
    - 22 RFCs, many defining LoST

13

E911: LoST

- Location-to-Service Translation Protocol (LoST)
- Select a PSAP based on real world location
  - Input: civic location or lat/long
- Replace telephone company location-to-PSAP database
  - Uses coverage polygons
- Device just needs to know its location
  - Programmed into device
  - Pick up from network
  - GPS

14

Image credits

Drawings by Scott Bradner unless noted

Slide#	credit
2 & 3	http://kosciusko.ms/city/e911
	http://www.nbcchicago.com/news/local/amber-alert-randle-el-241801961.html
	https://www.fcc.gov/help/public-safety-tech-topic-18-priority-telecommunications-services
4	http://gizmodo.com/5918715/13-tech-sounds-you-dont-hear-anymore
	http://slideplayer.com/slide/4159840/ - slide 78
5	https://www.cisa.gov/sites/default/files/2022-12/GETs-User-Guide-508.pdf
6 & 7	http://www.hulkshare.com/theegg507/busy-signal-danger-zone
8	http://static.googleusercontent.com/media/research.google.com/en//pubs/archive/41315.pdf – figure 1
9	http://kosciusko.ms/city/e911
10	http://electronics.howstuffworks.com/everyday-tech/location-tracking4.htm
11	http://henrycounty911.com/How911worksTennessee.pdf
12	http://www.marciliroff.com/new/the-secret-to-skype-auditions/
13	http://www.michigannena.org/
	https://www.ietf.org/logo/
14	http://www.tschofenig.priv.at/wp/?p=138

15

Protecting the infrastructure
Conclusion

CSCI E 45b: The Cyber World – part B

Threats via the Internet

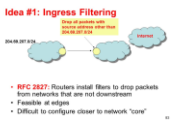
- Internet is a threat highway
  - Attacking individuals
  - Attacking "critical infrastructure"
    - SCADA controllers particularly vulnerable
  - Controllers may already be hacked
- Issue: too much accessible data
  - Compartmentalize & isolate

Threats to the Internet

- Attack middleware systems
  - DNS, routers & routing, time
- Reliability and protection were required in the old telephone system by regulation
  - Not in Internet
- Internet redundant topology helps a lot
- Since 1994 IETF protocol designers have to consider security

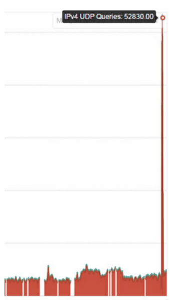
Pakistan cables - 2015

Threats to the Internet. Contd.



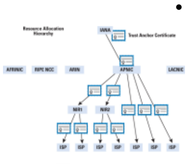
- Some voluntary U.S. federal initiatives
  - *The National Strategy to Secure Cyberspace*
  - *Framework for Improving Critical Infrastructure Cybersecurity*
- But little consistent direction or emphasis
- ISP ingress filtering can help limit spoofing
- ISP static routing can help limit impact of misconfigurations

Denial of Service (DoS) attacks



- DoS attacks on Internet services can be disruptive
  - E.g., DoS attacks on DNS root servers
  - Proper design can limit impact
- DoS attacks on user logins can block user access

Threats to routing



- Disruption
  - Block routing updates
  - Authentication of routing exchanges helps limit
- Falsification
  - Inject false routes to redirect or interfere with traffic
  - IETF sidr WG developing ways to secure interdomain routing
    - Can block forging of route origin information
    - More protections coming

Threats to routing, contd.

- Stress
  - Routing tables are big
    - Configuration errors can expand them and cause routers to crash
- How big an issue?
  - Few major outages
  - More a theoretical problem that a common one

7 Copyright © Scott Bradner & Ben Gaucherin 2016

Threats to DNS

- DoS threat to DNS servers mitigated by use of replicated servers accessed through anycast
  - Root & TLD servers
  - Some enterprise servers as well
- DNS resolving process vulnerable to the injection of incorrect data
  - Direct user to wrong server
  - DNS Security (DNSSEC) solves issues but is poorly deployed

DNSSEC SECURED by Afilias

This image is a service mark of Afilias

8 Copyright © Scott Bradner & Ben Gaucherin 2016

Emergency communications

CALL 911 EMERGENCY

- Packet-based Internet does not work in the same was as circuit-based telephone network
- Thus teleco systems emergency communications technologies do not work on the Internet
- Regulators still want same results
- Best-effort Internet works quite well in emergencies

9 Copyright © Scott Bradner & Ben Gaucherin 2016

Image credits

Drawings by Scott Bradner unless noted

Slide#	credit
2	https://en.wikipedia.org/wiki/Nuclear_power_plant
3	http://www.submarinecablemap.com
4	http://slideplayer.com/slide/697431/
5	http://timesoracle.com/2015/12/attack-on-root-dns-servers-blasted-5-million-queries-eery.html
6	https://www.nro.net/about-the-nro/regional-internet-registries
7	http://www.mainet.com/
8	http://blog.appriver.com/2013/09/security-concerns-on-the-new-gtlds/
	http://www.prweb.com/releases/2009/03/prweb2199054.htm
9	http://kosciusko.ms/city/e911
	http://www.nbcchicago.com/news/local/amber-alert-randle-el-241801961.html
	https://www.fcc.gov/help/public-safety-tech-topic-18-priority-telecommunications-services

10