CSF 432: Intro to Network and System Security

Week 06 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020

Cloud Services and Delivery Models

Cloud Services and Delivery Models

Software as a service (SaaS)

- On-demand software
  - No local installation
  - Why manage your own email distribution? Or payroll?
- Central management of data and applications
  - Your data is out there
- A complete application offering
  - No development work required
  - Google Mail

Cloud Services and Delivery Models

Infrastructure as a service (IaaS)

- Sometimes called Hardware as a Service (HaaS)
  - Outsource your equipment
- You're still responsible for the management
  - And for the security
- Your data is out there, but more within your control
- Web server providers

Cloud Services and Delivery Models

Platform as a service (PaaS)

- No servers, no software, no maintenance team, no HVAC
  - Someone else handles the platform, you handle the development
- You don't have direct control of the data, people, or infrastructure
  - Trained security professionals are watching your stuff
  - Choose carefully
- Put the building blocks together
  - Develop your app from what's available on the platform
  - SalesForce.com

Cloud Services and Delivery Models

Cloud deployment models

- Private - Your own virtualized local data center
- Public - Available to everyone over the Internet
- Hybrid - A mix of public and private
- Community - Several organizations share the same resources

Cloud Services and Delivery Models

Local and cloud resources

- On-premise
  - Your applications are on local hardware
  - Your servers are in your data center in your building
- Hosted
  - Your servers are not in your building
  - They may not even be running on your hardware
  - Usually a specialized computing environment
- Cloud
  - Entire application instances can be created and torn down on-demand
  - Resources are available as needed

Cloud Services and Delivery Models

Connecting to the cloud

- Existing Internet connection
  - Browser-based, SSL encryption
- VPN (Virtual Private Network)
  - Encrypted tunnel for all traffic between you and the cloud
  - Will probably require some additional hardware on both ends
- Direct connection
  - Co-location, same shared data center
  - High speed 10 Gigabit connection
  - No external traffic (added security)

Cloud Services and Delivery Models

Managing cloud security policies

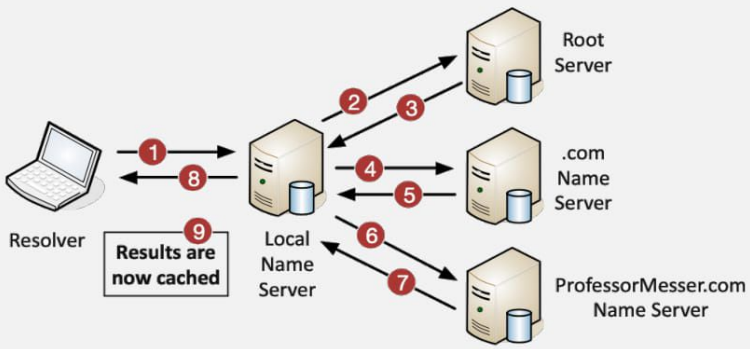
- Clients are at work, data is in the cloud
  - How do you keep everything secure?
  - The organization already has well-defined security policies
- How do you make your security policies work in the cloud?
  - Integrate a CASB (Cloud Access Security Broker)
  - Implemented as client software, local security appliances, or cloud-based security solutions

Cloud Services and Delivery Models

Cloud access security broker (CASB)

- Visibility
  - Determine what apps are in use
  - Are they authorized to use the apps?
- Compliance
  - Are users complying with HIPAA? PCI?
- Threat prevention
  - Allow access by authorized users, prevent attacks
- Data security
  - Ensure that all data transfers are encrypted
  - Protect the transfer of PII with DLP

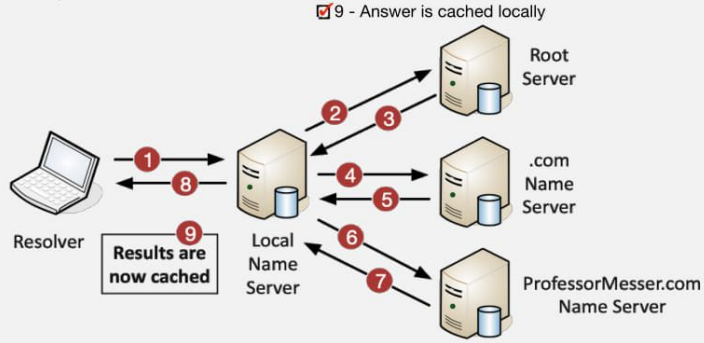
An Overview of DNS



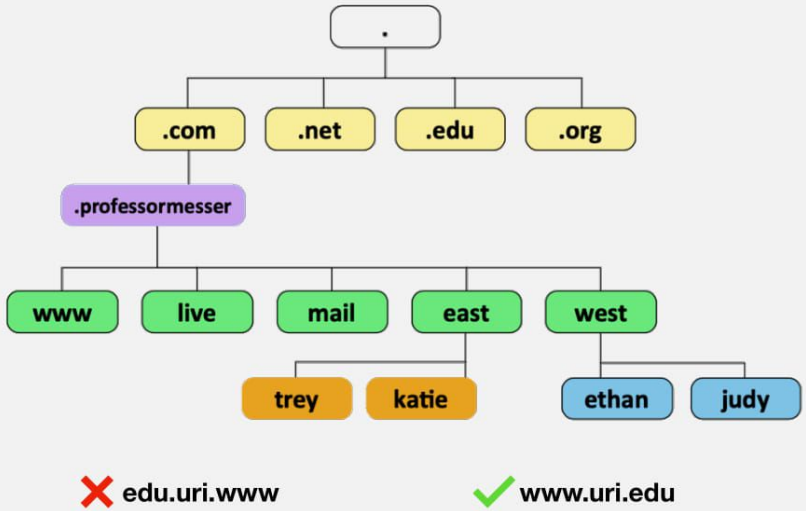
An Overview of DNS

The DNS Resolution Process

- 1 - Request sent to local name server
- 2 - Name server queries root server
- 3 - Root response sent to local name server
- 4 - Name server queries .com name server
- 5 - .com Response sent to local name server
- 6 - Name server queries specific domain server
- 7 - Domain server responds to name server
- 8 - Name server provides result to local device
- 9 - Answer is cached locally



An Overview of DNS



An Overview of DNS

Internal vs. External DNS

- Internal DNS - Managed on internal servers
  - Configured and maintained by the local team
  - Contains DNS information about internal devices
  - DNS service on Windows Server
- External DNS - Managed by a third-party
  - Does not have internal device information
  - Google DNS, Quad9

An Overview of DNS

Third-party DNS

- Managing DNS can be challenging
  - Especially in large environments
- Outsource the DNS
  - Cloud-based DNS services
- Features not available on a privately-hosted DNS server
  - High-availability, low latency, and scaling options

DNS Record Types

DNS Record Types

Resource Records (RR)

- The database records of domain name services
- Over 30 record types - IP addresses, certificates, host alias names, etc.

Address Records (A) (AAAA)

- Defines the IP address of a host
- This is the most popular query
- A records are for IPv4 addresses
- Modify the A record to change the host name to IP address resolution
- AAAA records are for IPv6 addresses
- The same DNS server, different records

```
www.professormesser.com.    IN A    162.159.246.164  ; Professor Messer
```


DNS Record Types

Canonical name records (CNAME)

- A name is an alias of another, canonical name
- One physical server, multiple services

```
; Alias (canonical) names
    gopher  IN CNAME    mail.mydomain.name.
    ftp     IN CNAME    mail.mydomain.name.
    www     IN CNAME    mail.mydomain.name.
```

Canonical name records (CNAME)

- Find a specific service
  - Where is the Windows Domain Controller? Where is the instant messaging server? Where is the VoIP controller?

```
;Service records
; _service._proto.name.  TTL   class SRV priority weight port target.
 _ldap._tcp.domain.com.  300   IN    SRV 10       60     389  s1.domain.com.
```


DNS Record Types

Mail exchanger record (MX)

- Determines the host name for the mail server - this isn't an IP address; it's a name

```
; This is the mail-exchanger.  You can list more than one (if
; applicable), with the integer field indicating priority (lowest
; being a higher priority)
      IN MX       mail.mydomain.name.

; Provides optional information on the machine type & operating system
; used for the server
      IN HINFO    Pentium/350 LINUX

; A list of machine names & addresses
    spock.mydomain.name.    IN A    123.12.41.40   ; OpenVMS Alpha
    mail.mydomain.name.     IN A    123.12.41.41   ; Linux (main server)
    kirk.mydomain.name.     IN A    123.12.41.42   ; Windows NT (blech!)
```


DNS Record Types

Name server records (NS)

- List the name servers for a domain - NS records point to the name of the server

```
; main domain name servers
                IN      NS      ns1.example.com.
                IN      NS      ns2.example.com.
; mail domain mail servers
                IN      MX       mail.example.com.
; A records for name servers above
ns1             IN      A       192.168.0.3
ns2             IN      A       192.168.0.4
; A record for mail server above
mail            IN      A       192.168.0.5
```

DNS Record Types

Pointer record (PTR)

- The reverse of an A or AAAA record
- Added to a reverse map zone file

```
2               IN      PTR     joe.example.com. ; FDQN
....
15              IN      PTR     www.example.com.
....
17              IN      PTR     bill.example.com.
```


DNS Record Types

Text records (TXT)

- Human-readable text information
  - Useful public information
- SPF protocol (Sender Policy Framework)
  - Prevent mail spoofing
  - Mail servers check that incoming mail really did come from an authorized host
- DKIM (Domain Keys Identified Mail)
  - Digitally sign your outgoing mail
  - Validated by the mail server, not usually seen by the end user
  - Put your public key in the DKIM TXT record

DHCP Addressing Overview

DHCP Addressing Overview

DHCP

- IPv4 address configuration used to be manual
  - IP address, subnet mask, gateway, DNS servers, NTP servers, etc.
- October 1993 - The bootstrap protocol - BOOTP
- BOOTP didn't automatically define everything
  - Some manual configurations were still required
  - BOOTP also didn't know when an IP address might be available again
- Dynamic Host Configuration Protocol
  - Initially released in 1997, updated through the years
  - Provides automatic address / IP configuration for almost all devices

DHCP Addressing Overview

The DHCP Process

- Step 1: Discover - Client to DHCP Server
  - Find all of the available DHCP Servers
- Step 2: Offer - DHCP Server to client
  - Send some IP address options to the client
- Step 3: Request - Client to DHCP Server
  - Client chooses an offer and makes a formal request
- Step 4: Acknowledgement - DHCP Server to client
  - DHCP server sends an acknowledgement to the client

DHCP Addressing Overview

Managing DHCP in the enterprise

- Limited Communication range
  - Uses the IPv4 broadcast domain
  - Stops at a router
- Multiple servers needed for redundancy
  - Across different locations
- Scalability is always an issue
  - May not want (or need) to manage DHCP servers at every remote location
- You're going to need a little help(er)
  - Send DHCP request across broadcast domains

DHCP Addressing Overview

IP Address Management (IPAM)

- Manage IP addressing
  - Plan, track, configure DHCP
- Report on IP address usage
  - Time of day, user-to-IP mapping
- Control DHCP reservations
  - Identify problems and shortages
- Manage IPv4 and IPv6
  - One console

Configuring DHCP

Configuring DHCP

Scope properties

- IP address range
  - And excluded addresses
- Subnet mask
- Lease durations
- Other scope options
  - DNS server, default gateway, WINS server

Configuring DHCP

DHCP pools

- Grouping of IP addresses
  - Each subnet has its own scope
  - 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24, etc.
- A scope is generally a single contiguous pool of IP addresses
  - DHCP exceptions can be made inside of the scope

Configuring DHCP

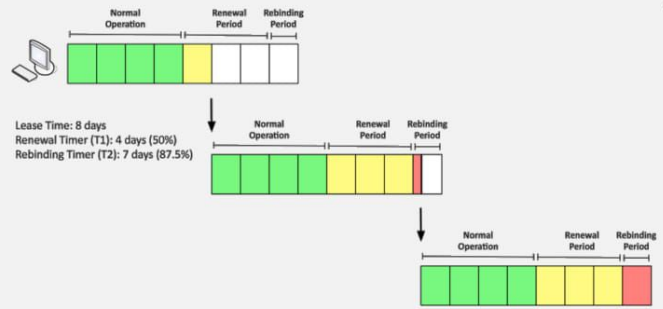
DHCP address allocation

- Dynamic allocation
  - DHCP server has a big pool of addresses to give out
  - Addresses are reclaimed after a lease period
- Automatic allocation
  - Similar to dynamic allocation
  - DHCP server keeps a list of past assignments
  - You'll always get the same IP address
- Static allocation
  - Administratively configured table of MAC addresses
  - Each MAC address has a matching IP address
  - Other names - Static DHCP Assignment, Static DHCP, Address Reservation, IP Reservation

Configuring DHCP

DHCP address allocation

- T1 timer
  - Check in with the lending DHCP server to renew the IP address
  - 50% of the lease time (by default)
- T2 timer
  - If the original DHCP server is down, try rebinding with any DHCP server
  - 87.5% of the lease time (7/8ths)



An Overview of NTP

An Overview of NTP

NTP (Network Time Protocol)

- Switches, routers, firewalls, servers, workstations
  - Every device has its own clock
- Synchronizing the clocks becomes critical
  - Log files, authentication information, outage details
- Automatic updates
  - No flashing 12:00 lights
- Flexible
  - You control how clocks are updated
- Very accurate
  - Accuracy is better than 1 millisecond on a local network

An Overview of NTP

NTP clients and servers

- NTP server
  - Respond to time requests from NTP clients
  - Does not modify their own time
- NTP client
  - Requests time updates from NTP server
- NTP client/server
  - Requests time updates from an NTP server
  - Responds to time requests from other NTP clients
- Important to plan your NTP strategy
  - Which devices are clients, servers, and client/servers?

An Overview of NTP

NTP stratum layers

- Some clocks are better than others
  - Your distance from the original reference clock is a stratum
- Stratum 0
  - Atomic clock, GPS clock
  - Very accurate
- Stratum 1
  - Synchronized to stratum 0 servers
  - Primary time servers
- Stratum 2
  - Sync'd to stratum 1 servers

An Overview of NTP

Configuring NTP

- NTP client
  - Specify the NTP server address (IP or hostname)
  - Use multiple NTP servers (if available) for redundancy
- NTP server
  - You need at least one clock source
  - Specify the stratum level of the clock
  - If there's a choice, the lower stratum level wins

CSF 432: Intro to Network and System Security

Week 06 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes