Week7 Review Notes

ELEC0099: Introduce to Internet Protocol Networks 21/22

RUFENG DING

Contents

1 DNS **1**

1.1 DNS implementation 1

1.2 DNS lookups 2

1.2.1 2 method of performing a query 2

1.2.2 answers 2

1.3 Main types of DNS records 3

2 SNMP **3**

2.1 History 3

2.2 information to manage 3

2.3 Monitoring applications 3

2.3.1 Manager function 4

2.3.2 Agent function 4

2.3.3 Manage objects 4

2.3.4 Monitoring Agent 4

2.4 Monitoring Methods 4

2.4.1 Polling 4

2.4.2 Traps 5

2.5 MIB (and SNMP) 5

2.5.1 Extensibility 5

2.5.2 SMI 5

2.6 MIB-II 6

2.7 Private MIBs . . . 6
2.8 Limitations of MIB Objects . . . 6
2.9 SNMP Operations . . . 7
2.10 SNMP interactins . . . 7
2.11 SNMP over UDP . . . 7
2.12 More on TRAPS . . . 8
2.13 SNMPv2 . . . 8
2.14 SNMPv3 . . . 8

3 Network Security **8**

3.1 Policies . . . 9
3.2 Physical Security . . . 9
3.3 Virus and Worms . . . 9
3.4 Bot Nets . . . 9

4 Cryptography **10**

4.1 Encryption . . . 10
4.2 Key . . . 10
4.3 Public Key Cryptography . . . 10
4.4 Encrypting and Decrypting . . . 11
4.5 Authentication . . . 11
4.6 SSL/TLS . . . 11
4.6.1 SSL/TLS characters . . . 11
4.7 Certificate . . . 12
4.8 Secure shell . . . 12
4.9 IPSec and VPNs . . . 13
4.10 DNS security . . . 13

5 Firewalls **13**

5.1 Define 13

5.2 Methods of Access control 13

5.3 Next generation Firewall Features 14

6 Denial-of-Service **14**

6.1 Source Spoofing 14

6.2 SYN cookies 14

6.3 BotNets 15

6.4 SPAM 15

6.5 Fighting SPAM 15

1 DNS

Domain Name System

- solution to the directory problem for hosts.
- Characters:
  - Distributed
  - Local control and update
  - Replicable
  - Consistent
- translate host names to IP addresses
- support IPv6 addresses

The DNS specification defines a Name Space:

- name space is **hierarchical** (Tree like)
- extensible
- branches called **Domains** leaves are **Hosts**

Domains can be groups into Zones of control:

- administrator of zones has full control to everything
- administrator of upper branches can delegate control of lower ones and create a separate zone.

1.1 DNS implementation

Each zone has a Primary server

- it is the authority of the information about the zone
- it makes updates
- should have one or more secondary servers(for performance and availability)
- invalid the data after a time-to-live period if no update

1.2 DNS lookups

name resolution $->$ query

- client in a library called a *resolver*
- configuration files contains address of local DNS server and domain of the client
- supplied by DHCP for desktop machines

The resolution process client $--$ ask $->$ dns name server $--$ refers to $->$ root server $--$ according to the name ask name server $->$ [name server (continue asking according to the name hierachy)]

Caching DNS cache the address so no need to ask again
(Caching) Time to Live: time a record be cache
trade-off

- too small TTL the system will be queried a lot
- too big TTL the system cannot change the addresses efficiently
- one week TTLs are common

1.2.1 2 method of performing a query

- iterative mode
- recursive mode (the Root server do the ask part and let to target name server directly send the address to you)

1.2.2 answers

- from domain server (authoritative answer)
- from cache at local server (Non-authoritative answer)

1.3 Main types of DNS records

- A IPv4
- AAAA IPv6
- CNAME redirects a domain to another domains
- PTR maps a IP address to a domain name
- NS returns the name servers for a given domain

2 SNMP

simple network management protocol

2.1 History

ICMP - SGMP - SNMP (CMOT long term) - SNMPv2 - SNMPv3

2.2 information to manage

- static
- dynamic
- statistical

functional architecture:

- manager-agent model
- a model for summarisation

2.3 Monitoring applications

these components include the functions that are visible to the users/manager
main tasks:

- performance monitoring
- fault monitoring
- security monitoring
- accounting monitoring

2.3.1 Manager function

retrieving information from other elements of the configuration. Usually this consists of library code linked with the monitoring applications.

2.3.2 Agent function

gather and records management information for network elements and communicates info to them. Agent function usually runs in elements and listen/reply to info request.

2.3.3 Manage objects

the info represent resources and their activities.eg: queue sizes/numbers of packets with errors...

2.3.4 Monitoring Agent

- generates summaries and statistical analysis of management information
- usually separate from the manager and reports to it periodically
- very useful in a heterogeneous environment

2.4 Monitoring Methods

decide when to use polling or traps is often a crucial for network efficiency

2.4.1 Polling

management station periodically ask for the info

Polling frequency because not many TRAPs are defined most problems will be detected by sequential polling.

$$N \leq \frac{T}{\Delta} \tag{1}$$

N number of agents
T desired polling interval
Δ average time for a poll

Δ depends of many factors

- processing time for the request at the management station
- network delay
- processing time for the request at the agent
- numbers of request/responses

2.4.2 Traps

when somethings abnormal happened, a device send a trap to management station

2.5 MIB (and SNMP)

MIB: database each objects represent a resource

- structured in the form of Tree
- each system maintains one for its managed resources

2.5.1 Extensibility

- allows new equipment with new features to be added without significant changes to the infrastructures
- allows private MIBs

2.5.2 SMI

structure of management information

- define the general framework in which a MIB can be defined
- identified the data types that can be used in the MIB
- defined in RFC 1155

SMI defined types:

- networkaddress
- ipaddress
- counter
- gauge
- timeticks
- opaques

2.6 MIB-II

MIB-II is the part of MIB that deals with the management of internet based protocols. It contains:

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- egp
- dot3
- snmp

2.7 Private MIBs

companies can register private MIBs for experimental testing and research.companies can register with IANA.

2.8 Limitations of MIB Objects

lack of granularity in the information limit the identification of problems.SNMP is designed to minimise the impact in the network.

2.9 SNMP Operations

- GET : *GetRequest* message to get a value of a managed object
- SET : *SetRequest* message to set a value in a object
- TRAP : agent send *Trap* message to inform the manager of events

GetNextRequest: (bacause the MIB info is structured in a tree, we can ask for the next one.) will allow us to traverse the MIB tree without knowing its structure

Generic-trap field

- coldStart(0)
- warmStart(1)
- linkDown(2)
- linkUp(3)
- authenticationFailure(4)
- egpNeighbourLoss(5)
- enterpriseSpecific(6)

2.10 SNMP interactins

- get values: manager $--$ get request PDU $->$ Agent $--$ get response PDU $->$ manager
- get next values: manager $--$ get next request PDU $->$ Agent $--$ get response PDU $->$ manager
- set values: manager $--$ set request PDU $->$ Agent $--$ get response PDU $->$ manager
- send trap:Agent $--$ trap PDU $->$ manager

2.11 SNMP over UDP

SNMP is designed to be transported by any protocols. In practice UDP is used.

- uses ports 161 for gets/sets and 162 for traps
- TRAPs should be used as soon a problems arises and before becoming critical
- SNMP traffic should be prioritized

2.12 More on TRAPS

- traps are not acknowledged by the monitoring station. May leed to problem
- Threshold values configured with a **Set** command
- a trap is usually packed with information in the form of MIB object and its values

2.13 SNMPv2

- No security mechanisms
- new structure of management information (SMI)
- manager-to-manager capabilities
- new protocol operations

2.14 SNMPv3

SNMPv2 + administration and security

security issues address

- modification of information
- masquerade
- message stream modification
- disclosure
- NOT denial of Service
- NOT traffic analysis

3 Network Security

- **confidentiality** man-in-the-middle attack: intercept the packets or messages between two. eg: using a packet sniffer
- **Authentication** fake email address/DNS poisoning/Phishing
- **Non Repudiation** sends message to someone and claims not send it/similar problem to authentication
- **Unauthorized Access** pretends to be one and access her/his resources: password capture/inadequate firewall
- **Denial-of Service** sends a huge amount of traffic disabling ones server. /Distributed:Botnets. /Source Spoofing. /SYN floods. /Email SPAM.

3.1 Policies

a security policy is first step.

- What to be protected?
- Who is it to be protected from?
- Is it affordable?

3.2 Physical Security

protect he quipment.(Theft for eg.)
Insurance.

3.3 Virus and Worms

- virus are attached to other files.
- Worms propagate by themselves.
- both are Exponential attacks as each program can infect many hosts and then proceed to search for and infect more.
- The mathematics and epidemiology is the same as that in biology.

3.4 Bot Nets

- commonly, virus/trojan infected machines to form a remotely controlled large networks
- these are commonly rented out
- used to launch distributed denial os services (DDoS) attacks (usually for Blackmail)
- used to accept and relay SPAM

4 Cryptography

4.1 Encryption

- standard encryption is symmetric. Same key to encrypted and decrypted message.
- AlgorithmsL: Data Encryption Standard (DES) and Advanced Encryption Standard (AES)
- same text encrypted with the same key will result in the same cipher text.
- use an random initialization vector and XOR the message

Main problem is key distribution.

4.2 Key

- Key exchange method:
  - exchange key through another method: telephone / letter etc.
  - Diffie-Hellman key exchange.
- Numbers of Key is proportional to N^2 for an N party network
  - use a Key Distribution Center
- Solution: Asymmetric Cryptography (Public Key Cryptography)

4.3 Public Key Cryptography

Encryption key : public key
Decryption key : private key
private key is never communicated and can not be eavesdropped.

one way function use large prime numbers and modular arithmetic

- a one way function is where it is very computationally expensive to reverse the calculation

The process:

1. choose 2 very large prime numbmers p and q
2. n = pq and $m = LCM\{p-1, q-1\}$(lowest common multiple)
3. choose r where r > 1 and coprime with m
4. find s such that $rs- > 1(mod\ m)$
5. n and r are the public key
6. p q s are the private key

4.4 Encrypting and Decrypting

- To encrypt a message M:
  $M_c = M_r(mod\ n)$ [$0 < M < n$ and M and n are coprime]
- To decrypt a message M:
  $(M_c)^s == M(mod\ n)$

4.5 Authentication

the same public key system can be used for authentication

4.6 SSL/TLS

- ACK
- using asymmetric to certificate
- transfer data normally

4.6.1 SSL/TLS characters

- Secure Sockets Layers/Transport Layer Security
- Widely used for web applications
- Overview of the protocols:

- server must have pub/pri key pair
- should have a certificate
- connects to server use https
- client and server should negotiate a cryptographic algorithm to use for session and the server assign a sessionID.
- allows the same keys to be used for a period instead of using new ones for each connection.

process:

1. server sends the certificate to the client
2. client checks the certificate using the root certification authority's key(supplied with the browser)
3. checks the names of the server
4. self generated key warn (unless the pseudo root certificate is installed on the client browser)
5. the client generate the key material for encrypting the traffic
6. material signed using the server's public key and sent
7. server and client then exchange a message authentication code(MAC) to ensure that both agree with the key exchanges up to that point

Now all data is encrypted and has a MACs added.(If the client stop and comeback to the session, client can still use the same key as long as the session is still valid).
Caveats with SSL/TLS: all you know is that you are communicate with the server in an encrypted channel.

4.7 Certificate

- web server manager creates a pub/pri key
- web server signs the request (required by signing CA) with private key and send to CAs
- Responsible CAs then go through a great deal of efforts to check the request is valid
- CAs added its pertinent information to the certificate and signs the request using **CAs private key**
- then CAs send the certificate back to webserver and I install it on my webserver

4.8 Secure shell

- use public key cryptography
- do not use certificate
- main purpsoe is to encrypt telnet/rlogin and ftp sessions
- on connection the client downloads the server's public key and displays it to the user
- symmetric encryption key exchange is performed
- session secured using 3DES or IDEA
- SSH used to tunnel many other protocols:X11

4.9 IPSec and VPNs

IPSec 3 protocols:

- Encapsulating Security Protocol (ESP)
- Authentication Headers (AH)
- Internet Key Exchange (IKE)

4.10 DNS security

DNS Security Extensions (DNSSEC)
sign zone data with a private key
use TCP for transport(Instead of UDP)
use TSIG for authenticated updates

5 Firewalls

- provide second line of defence
- could be circumvented for other hosts you trust may become compromised

5.1 Define

- an entity on the network used to perform access control on the network traffic
- software running on a host : dependent on the host kernel being free of vulnerability
- a dedicate piece of hardware : more secure
- a dedicate virtual machine

5.2 Methods of Access control

- static filtering
- dynamic fitering
- content based access control (CISCO)

Static Fltering TCP and UDP packet will be identifiable by the 4-tuple of: source of IP address/source Port/Destination of IP address/Destination Port(allow combination)

Have to remember to allow traffic in the other direction as well.

Dynamic Filtering static + make a note of addresses and port numbers and dynamically installs a rule to allow the reverse traffic.

May have problem when the control channel and data channel negotiated dynamically whithin the application.
Also problematic with asymetric routing

Content Based Access Control look inside of the command stream and set up rules to enable the protocol to work

5.3 Next generation Firewall Features

- content inspection
- email attachment sandbox
- machine learning

6 Denial-of-Service

Dos:

- Internet is designed to lower transmission costs
- Default ON
- Increased by BotNets

6.1 Source Spoofing

- ISP/AS should check
- Other ASes can do Reverse Path Check
- (Big problem is asymetric)

6.2 SYN cookies

encode the client initial sequence number in the server sequence number

6.3 BotNets

- many computers are controlled by the Botnet Herder
- hard to detect
- traffic comes with the right source address
- attackers can return the right ACK to SYN-ACK

the solution:

- Cloud Computing helps
- Machine Learning helps

6.4 SPAM

sending identical messages to thousands of recipients.

Perpetrators often harvest addresses of prospective recipients from Usenet postings or from web pages, obtain them from databases or simply guess them by using common names and domains. By definition SPAM occurs without the permission of the recipients. Represents 95% of the mail sent in the Internet. Major problems for ISPs.

6.5 Fighting SPAM

- Bayesian filtering
- Governments have legal options...
- 'electronic stamps'(proposed)
- ISPs have several technologies

SPF sender policy framework.
SPF works by domains publishing ”reverse MX”records. only receive message from specified list.(domain/server)