Key Security Tools

10 August 2020 16:38

Firewalls

isolates organization's internal net from larger Internet
- some packets can pass through, others blocked

- Prevent DoS: SYN flooding, attacker establishes many fake TCP connections
- Prevent illegal access of internal data
- Allow only authorized access to inside network (authenticated users)

2 types of firewall: Application-level (also XML gateway)
Packet-filtering

Packet filtering

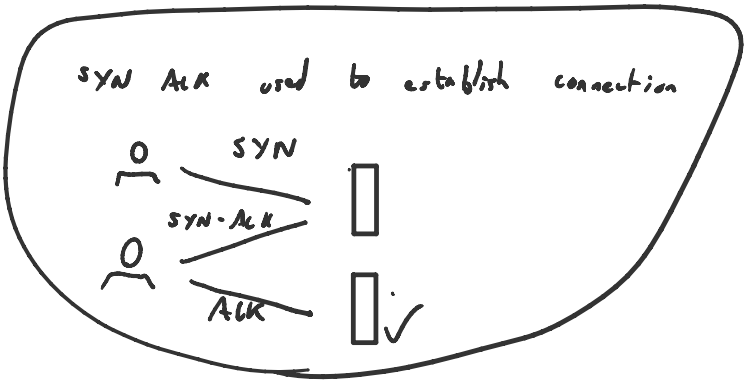
Decision to filter based on:
- source/destination IP
- TCP/UDP source + destination Port numbers
- ICMP message type
- TCP SYN and ACK bits

router firewall

should packet be allowed in/out?

ACK bit: acknowledge bit

Internet Control Message Protocol
- normally generated in response to errors in IP operations



Application Gateways

Filters packets on application data as well as IP/TCP/UDP

Example: only allow telephone network use to certain internal users
external

limitations of firewalls/gateways:
- IP spoofing, router can't really know claimed source
- each app needs own gateway
- filters often use all or nothing policy for UDP
- tradeoff = communication with outside world Vs security
- many highly protected sites still suffer from attacks

User Datagram Protocol
- can send messages to other IPs without prior communications to setup

XML Gateway

XML traffic passes through conventional firewall without inspection
- it passes through port 80 - generally left open

... traffic passes through conventional firewall without inspection
↳ it passes through port 80 - generally left open

Gateway examines XML payload, looking for:
- well formed payload
- no executable code
- source ID is known

Firewall State

Stateless - no concept of state
"packet filter" - less secure
- filters based on Layers 3 and 4 (IP, Port)

Stateful - have state tables to compare current packets with previous packets
- maybe slower than stateless
- Application firewalls can use Layer 7 information

Proxy firewalls - intermediary server
- terminate connections and initiate new ones
- two 3-way handshakes between 2 devices
↳ one with each device and firewall

Cryptography

Data in motion and data at rest - both need to be secure

Modern ciphers used modular math - XOR (exclusive or) is common

Stream cipher - bit by bit decryption/encryption

Block cipher - decrypt/encrypt many bits at a time i.e. 64-bit depends on algorithm

3 primary types

Symmetric - same key to encrypt and decrypt
- security depends on keeping key safe
- fast and key generally strong (bigger = stronger)
- Key needs to be shared using secure, out-of-band method
- examples: DES, Triples DES, AES

Asymmetric - 2 keys public and private
- one to encrypt one to decrypt
- uses "one way" algorithms to generate the two keys
↳ factoring prime numbers and discrete logarithm
- slower
- example: HTTPS uses asymetric encryption when first visiting site

Hash function - one way algorithm, no key
- variable-length "plaintext" $\xrightarrow{\text{hashed}}$ fixed length hash
- provides integrity verification

- variable-length "plaintext" → (hashed) fixed length hash
- provides integrity verification
- older algorithms prone to collisions - SHA-1, MD5
- SHA-2 is newer and recommended

Attacks

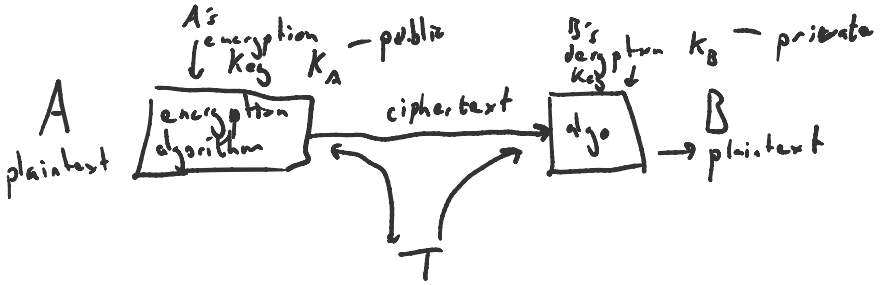
Brute force - trial and error

Rainbow tables - similar (faster) but using previously tried and known passes

Social engineering - non-technical methods to acquire from human

Known Plaintext - having plaintext and analysing to understand cipher

Known ciphertext - ↑ same but with only ciphertext



symmetric $K_A = K_B$

asymmetric $K_A \neq K_B$

A uses B's public key to encrypt and B uses their private key to decrypt

monoalphabetic cipher, replace one letter with another e.g. Caesar cipher

Foundational problem with symmetric cryptography is distribution of key

DES - Data encryption standard
- 56-bit symmetric key, 64 plaintext input
- how secure?
  - brute force decrypted in 4 months (could change every 3 months)
  - no known "backdoor" decryption approach
- make more secure?
  - use 3 DES sequentially
  - use cipher-block chaining

DES operation

16 identical permutations of applying function to different 48 bits of 64 bits

AES = Advanced encryption standard

replaced DES in 2011 - 64 → 128 bit blocks

256-bit key

brute force taking 1 sec for DES = 149 trillion years for DES

256-bit key
brute force taking 1 sec for DES = 149 trillion years for DES

Penetration Testing

White hat - ethical
- under contract and authorized

Gray hat - ethically motivated
- not authorized

Black hat - unethical
- money, politically, socially motivated

Threat actors (malicious actor)
- organization responsible for incident
- script kiddies (use available tools)
- hacktivists
- organized crime
- insiders (ex-employee)
- competitors
- Nation states - Fancy Bears aka APT28 (sophisticated highly funded)
  - Lazarus Group
  - Scarecrft aka Group 123
  - APT29

Methodologies:

OSSTMM
NIST - network security testing
FFIEC - financial
ISSAF
p-test - simple methodology

Vulnerability Assessment:

Vulnerability { Identify indicators
Exposure
Sensitivity
Adaptive capacity
Potential Impacts

automated process run on a regular basis

Digital Forensics:

Identification, recovery, investigation, validation of facts

Digital Forensics

Identification, recovery, investigation, validation of facts

Digital evidence found on computers, phones, servers, hard drives

Locard's exchange principal
Criminal will take something but also leave something
↳ both = evidence

chain of custody: chronological documentation of custody of evidence
is required for evidence to be used legally in court

Tools: Faraday cage - blocks signals
Forensic laptops, cameras, power supply toolkit etc. } hardware

Volatility (opensource)
FTK
EnCase } paid
dd - bit by bit copier on Linux
Autopsy (the sleuth kit)
Bulk extractor
} software