COMPUTER NETWORKS

AY2022-2023 Spring Semester

COMP1047 Systems & Architecture

Ying Weng

Computer Networks Part-5. Network Security

Question

Are we hackers or crackers?

Hackers vs. Crackers

- Hackers were originally ‘tinkerers’, putting systems or devices to novel uses.
- Driven by the search of knowledge or status.
- When vulnerabilities are found, normally warn the manufacturer to allow it to be fixed.
- Term co-opted by mainstream media to mean Cracker.

- Crackers always compromise systems for malicious purposes.
- Normally do not care about the consequences of their actions.
- Driven by financial gain or notoriety.
- Almost universally disliked by the rest of the security community.

Hackers vs. Crackers

- This can get very confusing!
- Legitimate programmers and enthusiasts will often refer to themselves as ‘hackers’
  - Often to a concerned reaction!
- So be aware of the differences

Hackers vs. Crackers

–We are Hackers, not Crackers

Glossary

- Security Cracker
  - Aims to break passwords and authentication with brute force or other common attacks
- Software Cracker
  - Breaks software copy protection or restrictions

Discussion

Question:

Which hat do you wear?

Fill the "Coloured Hats" chart with

(a) 'Employed Hackers' or Paid Good Guys

(b) 'Cracker' or Bad Guys

(c) 'Ethical Hackers' or Good Guys

(d) 'Undecided'

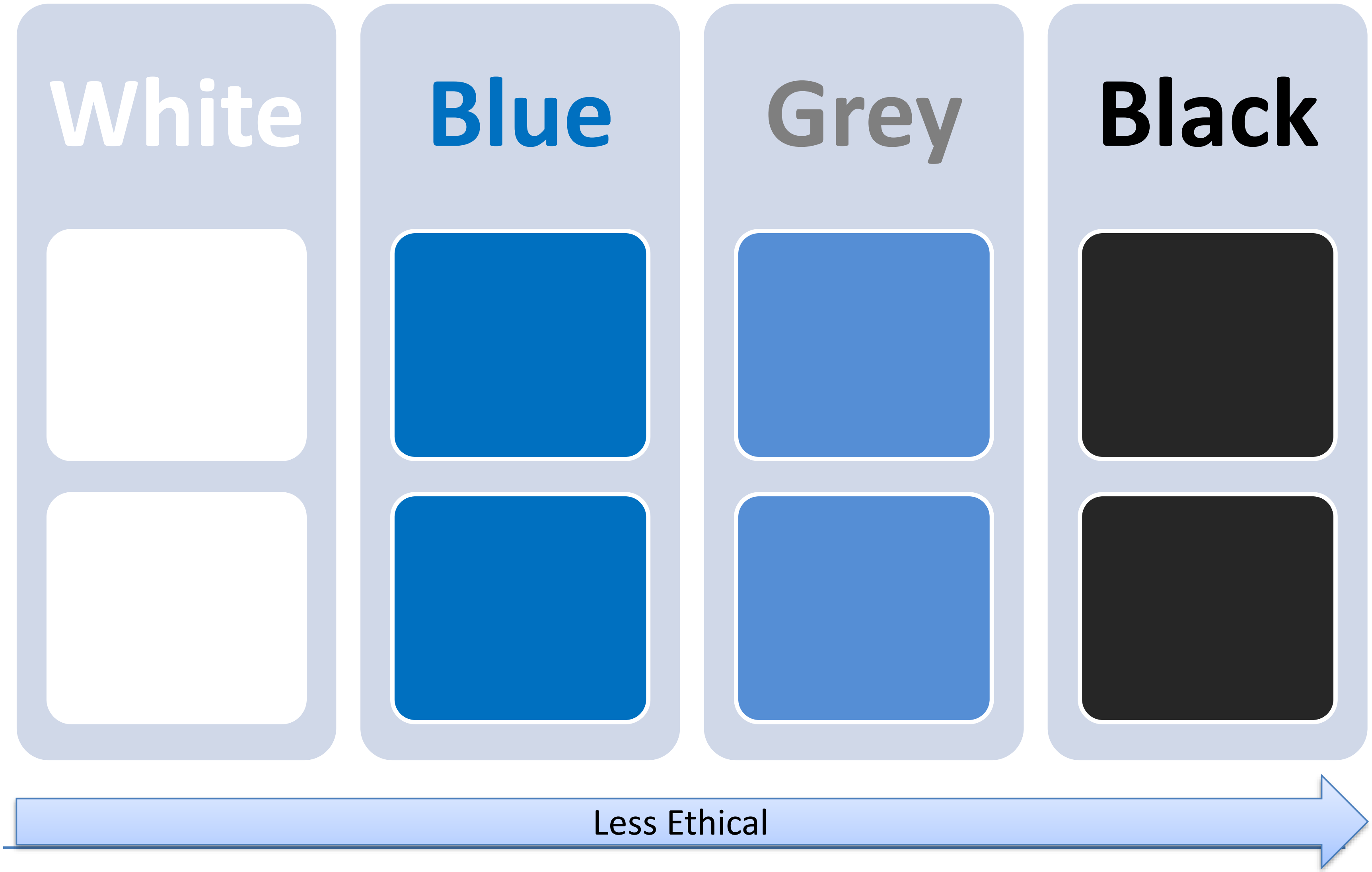
(e) Find Flaws to Improve Security

(f) Normally Hackers with 'Questionable' Ethics

(g) Compromise Systems for Financial or Other Gain

(h) New Term for Experts Employed to Evaluate Security

Coloured Hats



White

Blue

Grey

Black

Less Ethical

More Colours

- Originally evolved from Cold War military planning
- Red Team
  - Simulated attackers, designed to improve responses by thinking ‘creatively’
- Blue Team
  - Defenders, responding to attacks and threats from the Red Team

Other Characters

Script Kiddie

- A cracker without the skills. Uses pre-built attacks simply to crack systems.

Social Engineer

- A special form of cracker that does not attack the technology. Instead targets the weakest element, humans.

Hacktivist

- A hacker who uses their skills to advance a social or political agenda. Usually does not wish to cause damage, but seeks publicity.

The 3 “A”s of Security

- AAA (or Triple A): an acronym
- Stands for:
  - Authentication
  - Authorisation
  - Auditing (or Accounting)

- Roughly equivalent to the **Identification**, **Technical Controls** and **Policy** elements of the layered defences pyramid

The 3 “A”s of Security

- Authentication
  - i.e. use of passwords
  - Biometrics
- Authorisation
  - After verifying the user’s identity we still need to check their level of access
  - Which computers are they allowed to access?
  - Which actions are they allowed to perform?
- Auditing
  - We should record a user’s access to data – this can be an effective deterrent to mischievous behaviour

Authentication

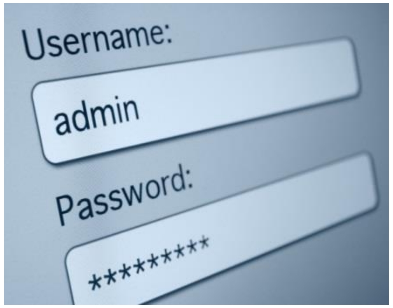
- “Are you who you say you are?”
- Direct analogue to the ‘Identification’ layer
- Can be established using simple mechanisms, password or cryptographic keys

- Better approach is Two-factor Authentication
  - Something you have **and** something you know…

Authentication Process

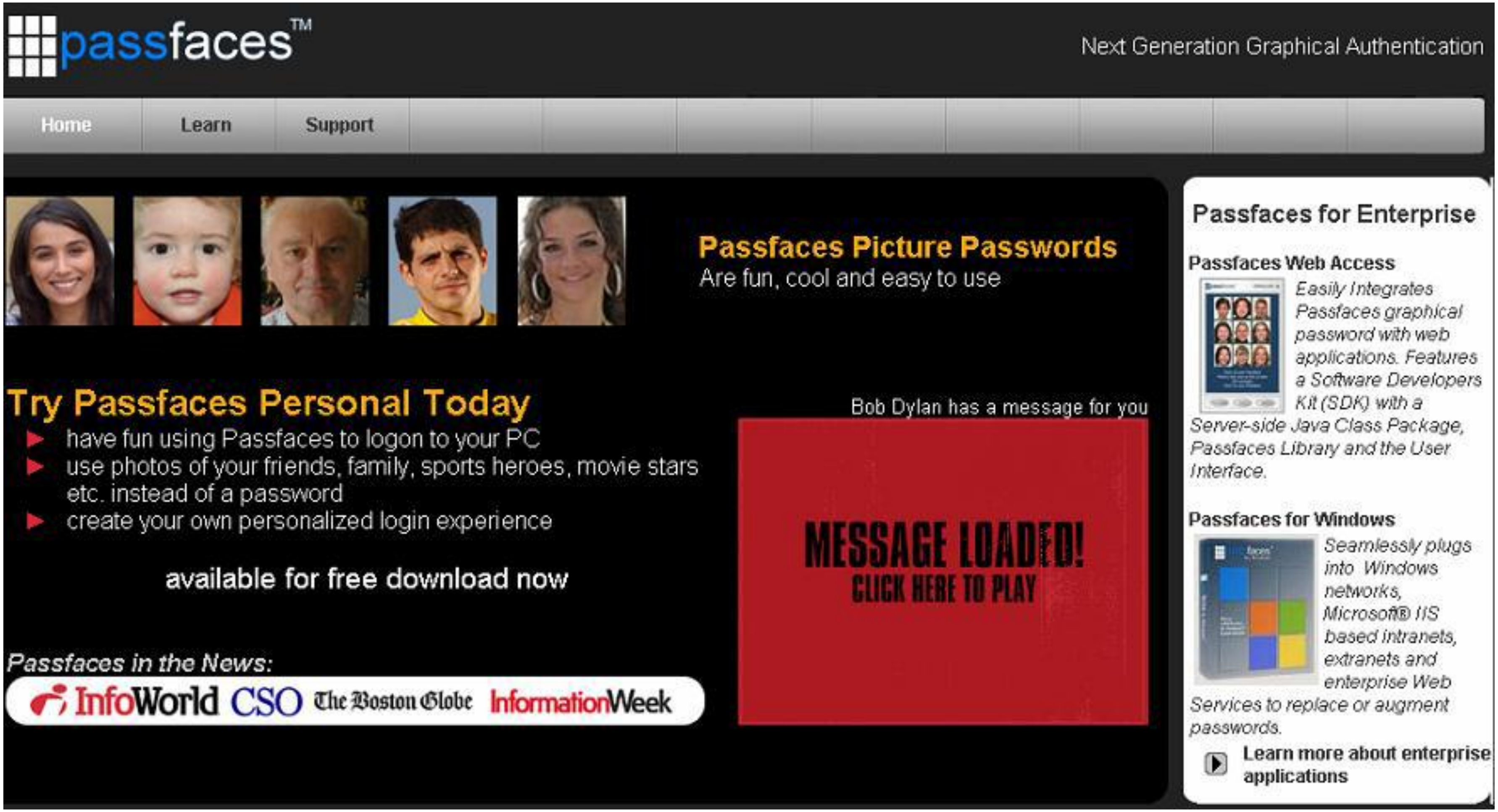
Authentication process is based on

- User knowledge
  - e.g. user name & password
- User possession
  - e.g. key card, dongle
- User attribute
  - i.e. biometrics – retina, palm, fingerprint


Username:
admin
Password:
****

User Knowledge

- *We can use information that the brain is designed to remember*



Next Generation Graphical Authentication

Passfaces Picture Passwords
Are fun, cool and easy to use

Try Passfaces Personal Today

- have fun using Passfaces to logon to your PC
- use photos of your friends, family, sports heroes, movie stars etc. instead of a password
- create your own personalized login experience

available for free download now

Passfaces in the News:

Bob Dylan has a message for you

Passfaces for Enterprise

Passfaces Web Access

Easily Integrates Passfaces graphical password with web applications. Features a Software Developers Kit (SDK) with a Server-side Java Class Package, Passfaces Library and the User Interface.

Passfaces for Windows

Seamlessly plugs into Windows networks, Microsoft® IIS based intranets, extranets and enterprise Web Services to replace or augment passwords.

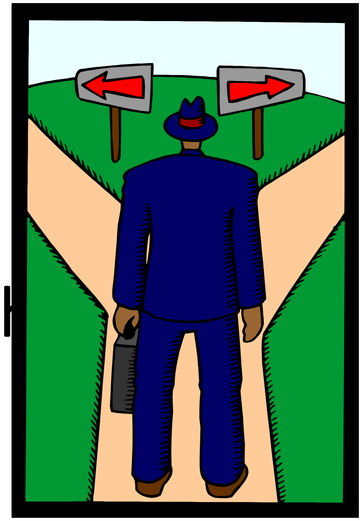
Learn more about enterprise applications

Humans are the Weakest Link

- The 'Wetware' (humans) are the weakest link in any security system
  - Make poor choices
  - Are easily coerced to reveal details
  - Forget details relatively easily
  - Do not fully understand the method of securing a system

Two Factor Authentication

- One of the best defences against brute forcing and poor credentials is Two Factor Authentication
- Requires two elements, in addition to the identification
  - A ‘known’ portion: a password, PIN or other credential
  - A ‘physical’ portion: a token or device with a temporally unique code



Two Factor Authentication

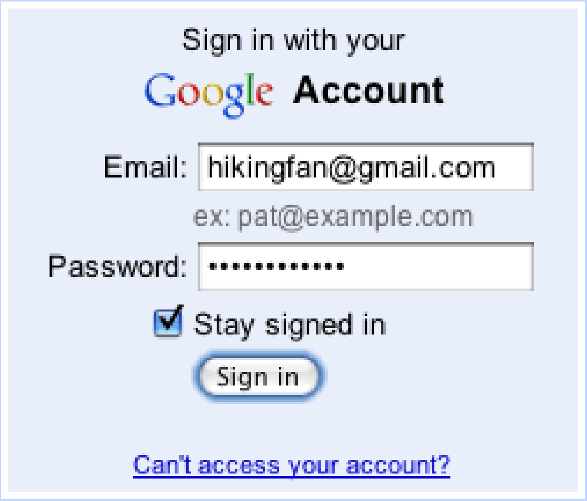
Live examples

- Google 2-Step Verification
- Location Aware Login
- One Time Password (OTP) Security Device

Google 2-Step Verification

- Uses the user’s own mobile phone or pager
- Site generates a request using Google’s API
- User signs in with normal credentials
- User enters the code shown on their device or received via SMS

1.



Sign in with your Google Account

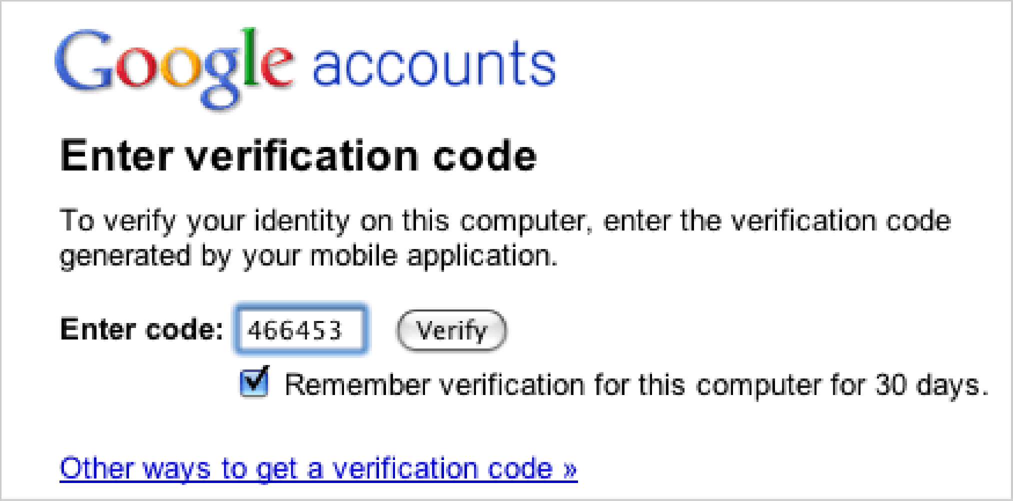
Email: hikingfan@gmail.com

ex: pat@example.com

Password: •••••••••••••

☑ Stay signed in

2.



Google accounts

Enter verification code

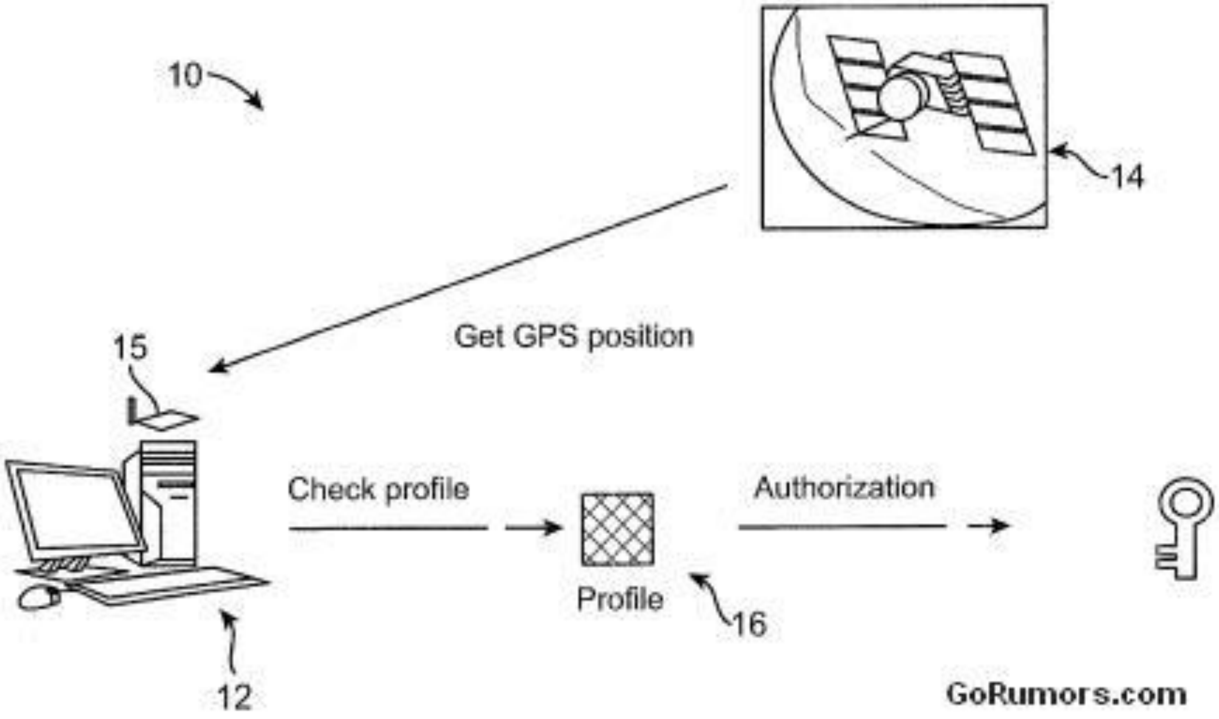
To verify your identity on this computer, enter the verification code generated by your mobile application.

Enter code: 466453

☑ Remember verification for this computer for 30 days.

Location Aware Login

- Either network geography, known as NLA – Network Location Aware
- Or, regular geography where the device must be detectable within range of a beacon



GoRumors.com

One Time Password (OTP) Security Device

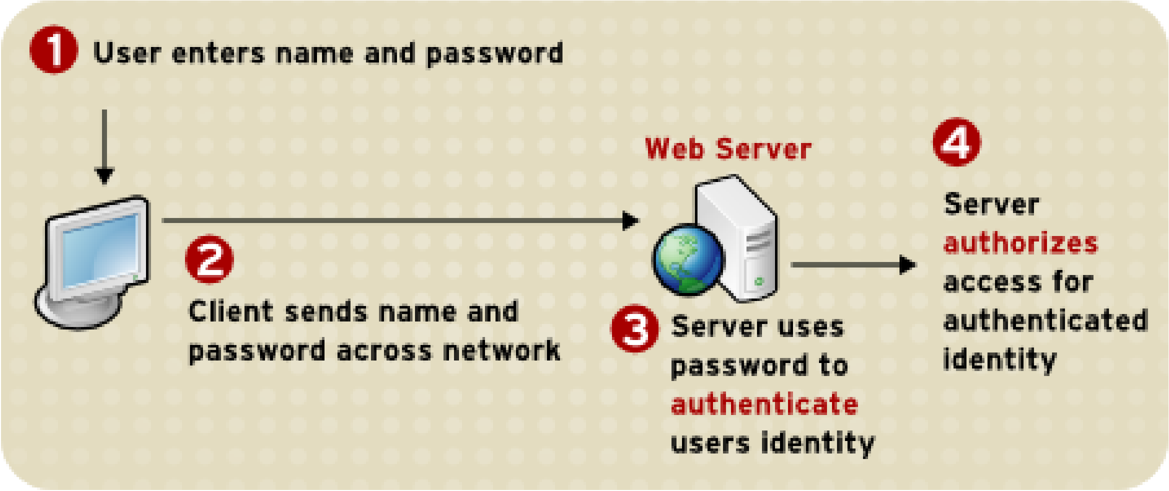
- OTP is a password valid for either one session or transaction
- After use, it is immediately invalidated
- Security of these schemes are only as good as the delivery mechanism
  - If the password is shown on screen, then potentially anyone could request and obtain a password
  - If the password is delivered via SMS, then short of a in-depth compromise of the network or device – a reset is secure

1st generation OPT security device

2nd generation OPT security device

Authorisation

- “Are you allowed to do that action to that object?”
- Analogous to the ‘Technical Controls’ layer. This doesn’t mean that the ‘rules’ are not backed by a Policy as well
- Could be File Permissions, Firewall Rules, Database Grants or a custom application control



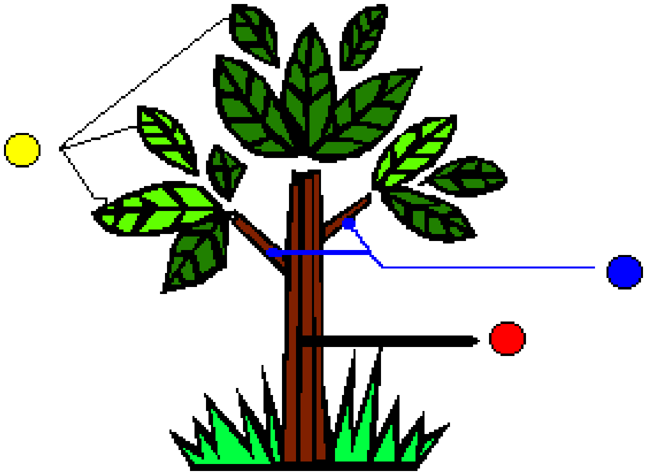
1 User enters name and password
2 Client sends name and password across network
Web Server
3 Server uses password to authenticate users identity
4 Server authorizes access for authenticated identity

Linux Filesystem

🟡 Files

🔵 Subdirectories
(branches of Tree)

🔴 Root



Linux File System is just like a tree

Filesystem Access Control

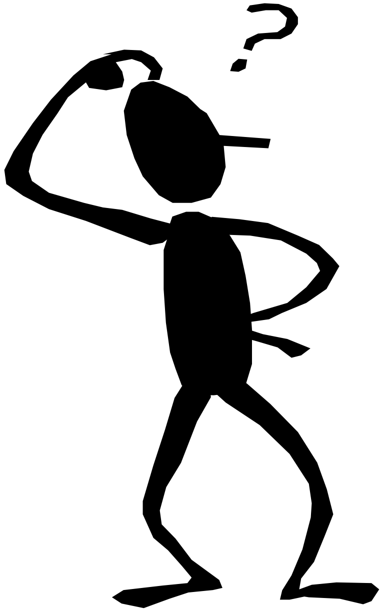
- Filesystem implements it's own access control system
- Only the filesystem implements user groups
- “everything is a file (descriptor)”

Filesystem Groups

- Every file has owner and a group
- Owners set permissions
- Can decide what owner, group owners, others can do with files
- e.g. permission bits: rwx

Question

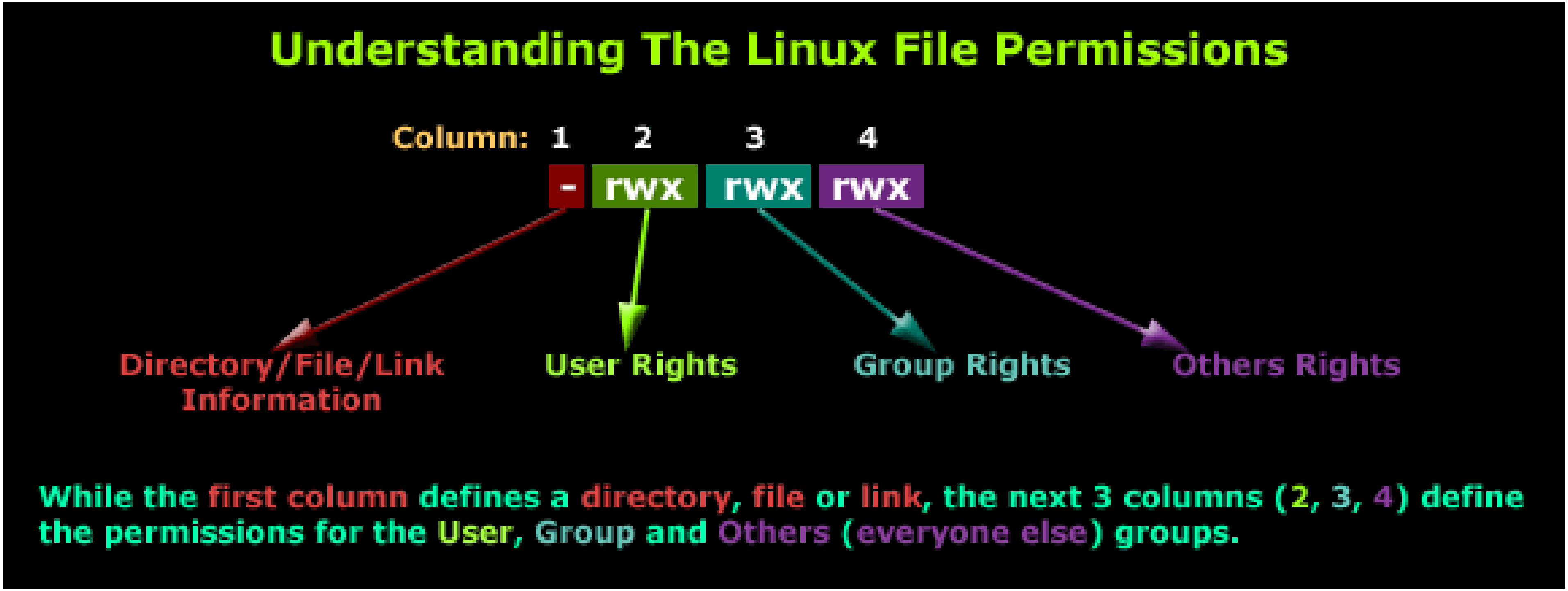
- r?
- w?
- x?



Pemission bits

- r: the file owner has read privilege of this file
- w: the file owner has write privilege of this file
- x: the file owner has execution privilege of this file

Filesystem Groups



Understanding The Linux File Permissions

While the first column defines a directory, file or link, the next 3 columns (2, 3, 4) define the permissions for the User, Group and Others (everyone else) groups.

DMZ (De-Militarized Zone)

- In computer security, DMZ is named after the military usage of the term
- Also known as
  - Data Management Zone
  - Demarcation Zone
  - Perimeter Network
- A physical or logical subnetwork within which all servers hosting publicly accessible services are placed
- Contains and exposes an organization’s external services to a larger, untrusted network, usually the Internet

DMZ (De-Militarized Zone)

- The purpose
  - To add an additional layer of security to an organization’s LAN
  - An external attacker only has access to equipment in the DMZ, rather than the whole of the network

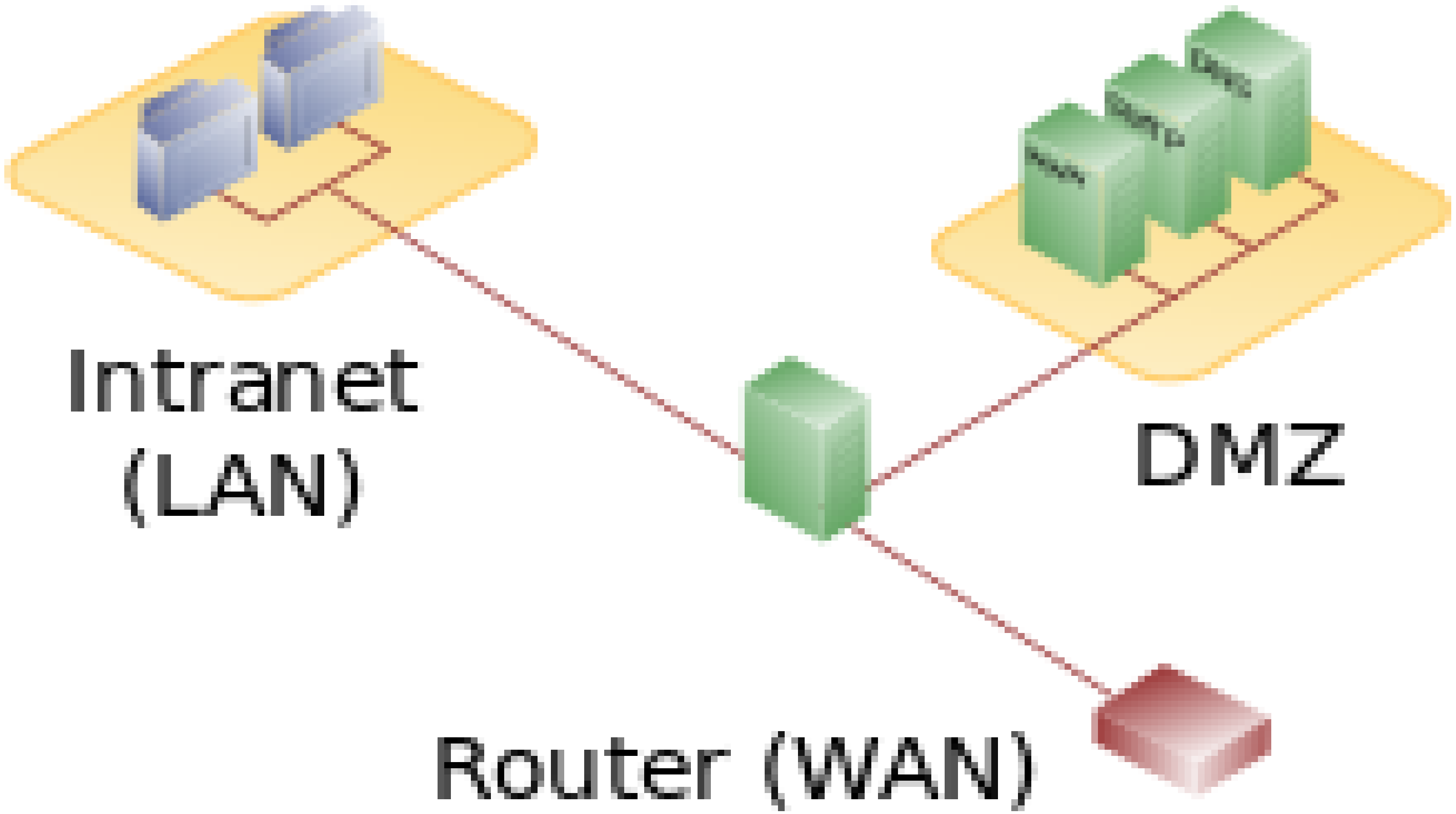
Question:

Do you know “ What is an additional layer of security”?

Firewall

- A part of a computer system or network
- Designed to block unauthorised access while permitting authorised communications
- A device or a set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria
- Can be implemented in either hardware or software, or a combination of both
- All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria

Single Firewall Architecture



Group Discussion

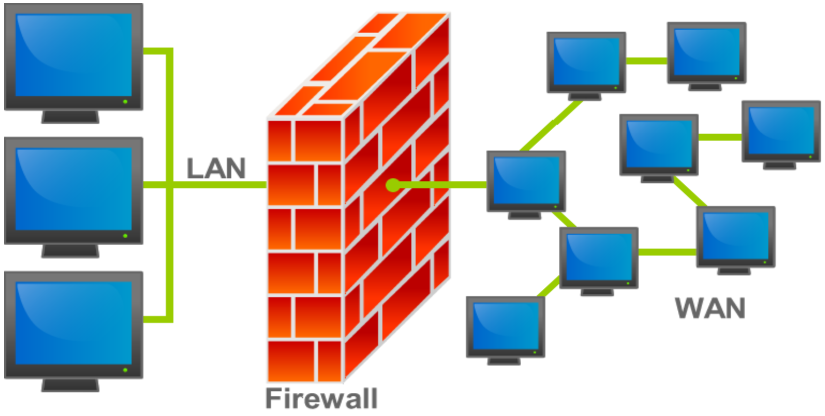
Question:

Can you draw the “Dual Firewall Architecture”?

Evolution of the firewall

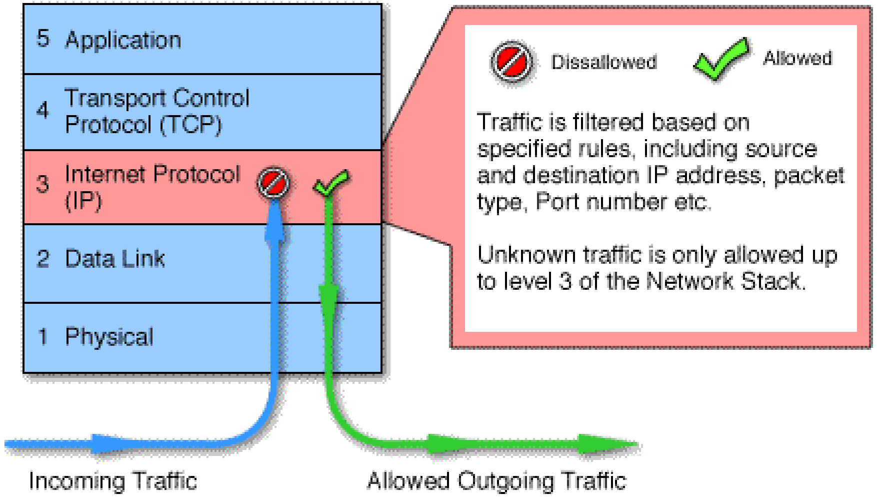
First paper referencing ‘firewalls’ published in 1988 by DEC.

- 1st Generation: Packet Filter
- 2nd Generation: Stateful Filter
- 3rd Generation: Application Layer



1st Generation: Packet Filter

- 1st Gen Firewalls intercept network traffic and inspect packets
- Filter packets based on a set of simple rules
- Can filter on packet's source and destination address, its protocol, the port number
- Packets are allow to pass or dropped/blocked

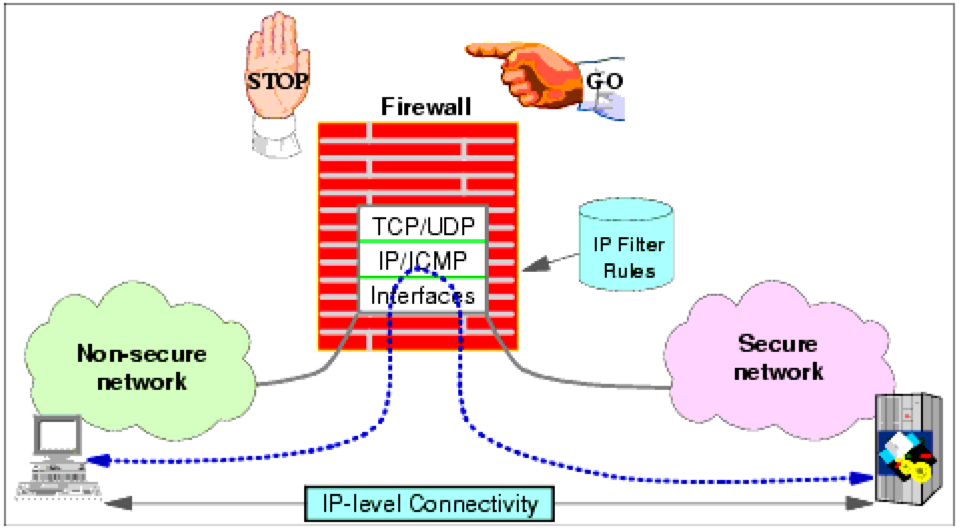


Traffic is filtered based on specified rules, including source and destination IP address, packet type, Port number etc.

Unknown traffic is only allowed up to level 3 of the Network Stack.

2nd Generation: Stateful Filter

- 1st Generation filters have no memory of connections and do not know whether a packet is part of an ongoing network connection or a new packet
- 2nd Generation Filters perform stateful packet inspection and keep track of ongoing connections



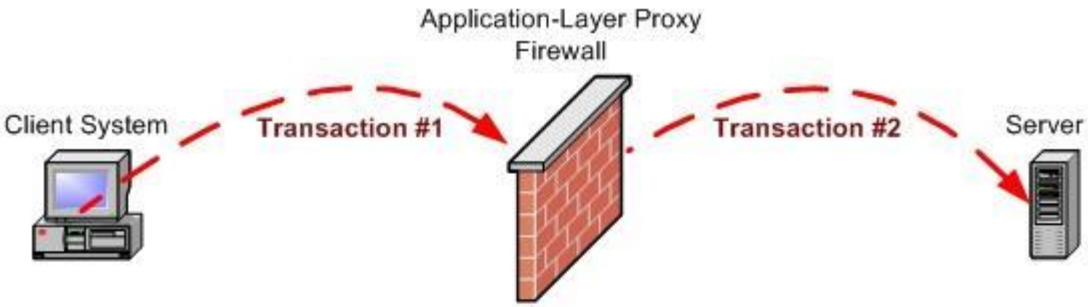
2nd Generation: Stateful Filter

- Knowing whether a packet is part of an established connection means it’s possible to only allow packet where the connection was established from inside the firewall
- Can be vulnerable to Denial of Service by bombardment

3rd Generation: Application Layer

- Filter at the application Layer
- Understands Application Protocol

e.g can tell the difference between HTTP traffic used to access a Web page and HTTP traffic used for file sharing, firewall that is only performing packet filtering would treat all HTTP traffic equally



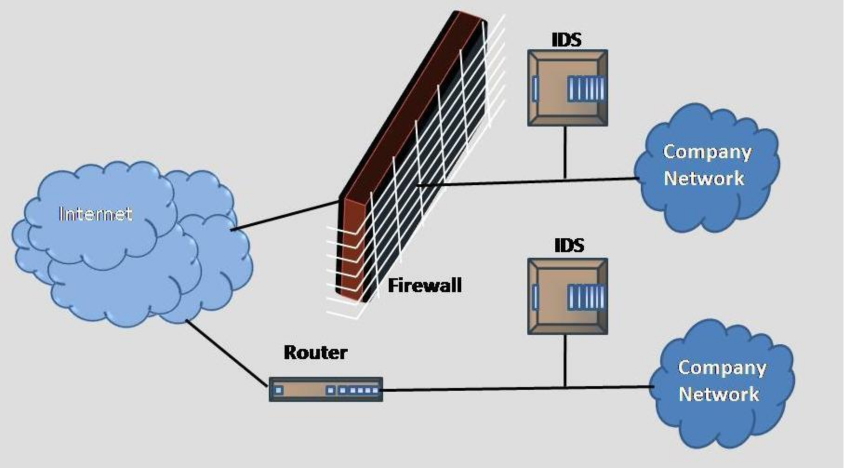
Transaction is split in two: to client, firewall appears to be the server (transaction #1); to server, firewall appears to be the client (transaction #2)

Auditing (Accounting)

- “There is a record of you doing this action to this object at this time from this location.”

- Potentially the most persuasive portion to discourage threats
- Allows enforcement of Policy elements, by providing evidence of wrong doing

What is an IDS?



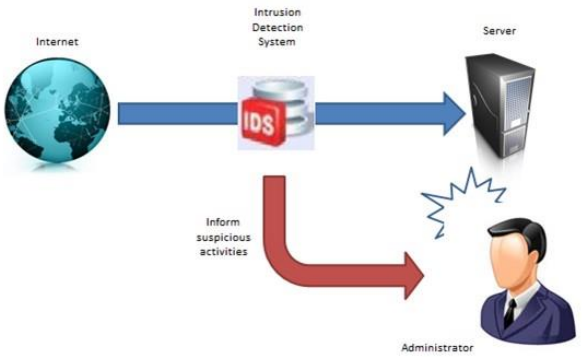
- Intrusion Detection System
- Monitors
  - Network traffic
  - Unauthorised access
  - Suspicious activities
- Alerts the system or network administrator
- A last line of defence in the network security

Authentication, Authorisation, Auditing

- Responds to anomalous or malicious traffic by
  - Blocking the user
  - Source IP address from accessing to the network

Why use an IDS?

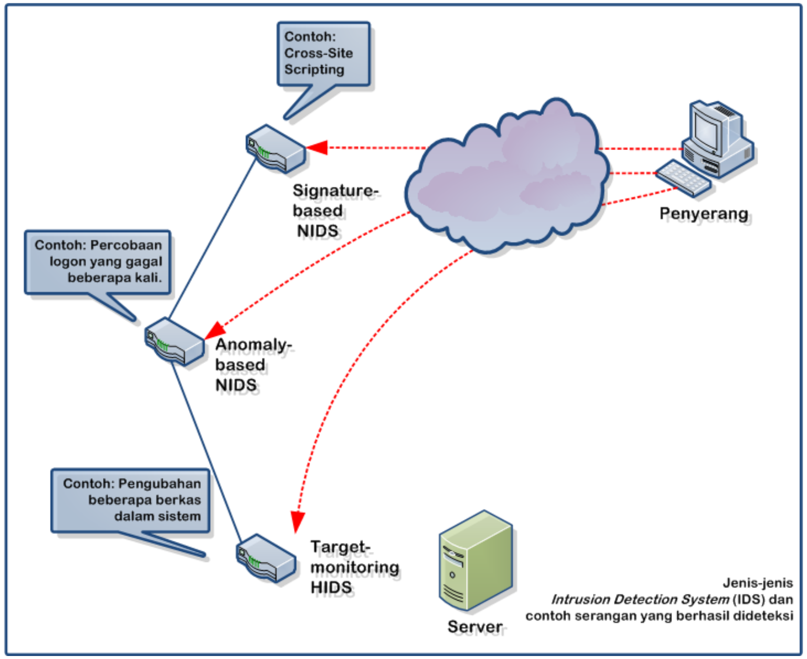
- Prevent problem behaviour by increasing attackers' perceived risk of discovery
- Document threats to an organisation and provide information about attacks that do take place
- Can help both learning and providing evidence
  - Detect and deal with precursors to attacks (scans & probes)
  - Detect / deflect / deter attacks not prevented by other mechanisms



Types of IDS

Based on the sources of the audit information used by each IDS, the IDS may be classified into

- Host-base IDS (HIDS)
- Network-based IDS (NIDS)


Contoh: Cross-Site Scripting
Signature-based NIDS
Penyerang
Contoh: Percobaan logon yang gagal beberapa kali.
Anomaly-based NIDS
Contoh: Pengubahan beberapa berkas dalam sistem
Target-monitoring HIDS
Server

Jenis-jenis *Intrusion Detection System* (IDS) dan contoh serangan yang berhasil dideteksi

Types of IDS

- HIDS
  - Get audit data from host audit trails
  - Detect attacks against a single host
- NIDS
  - Use network traffic as the audit data source
  - Relieve the burden on the hosts that usually provide normal computing services
  - Detect attacks from networks

Thank you