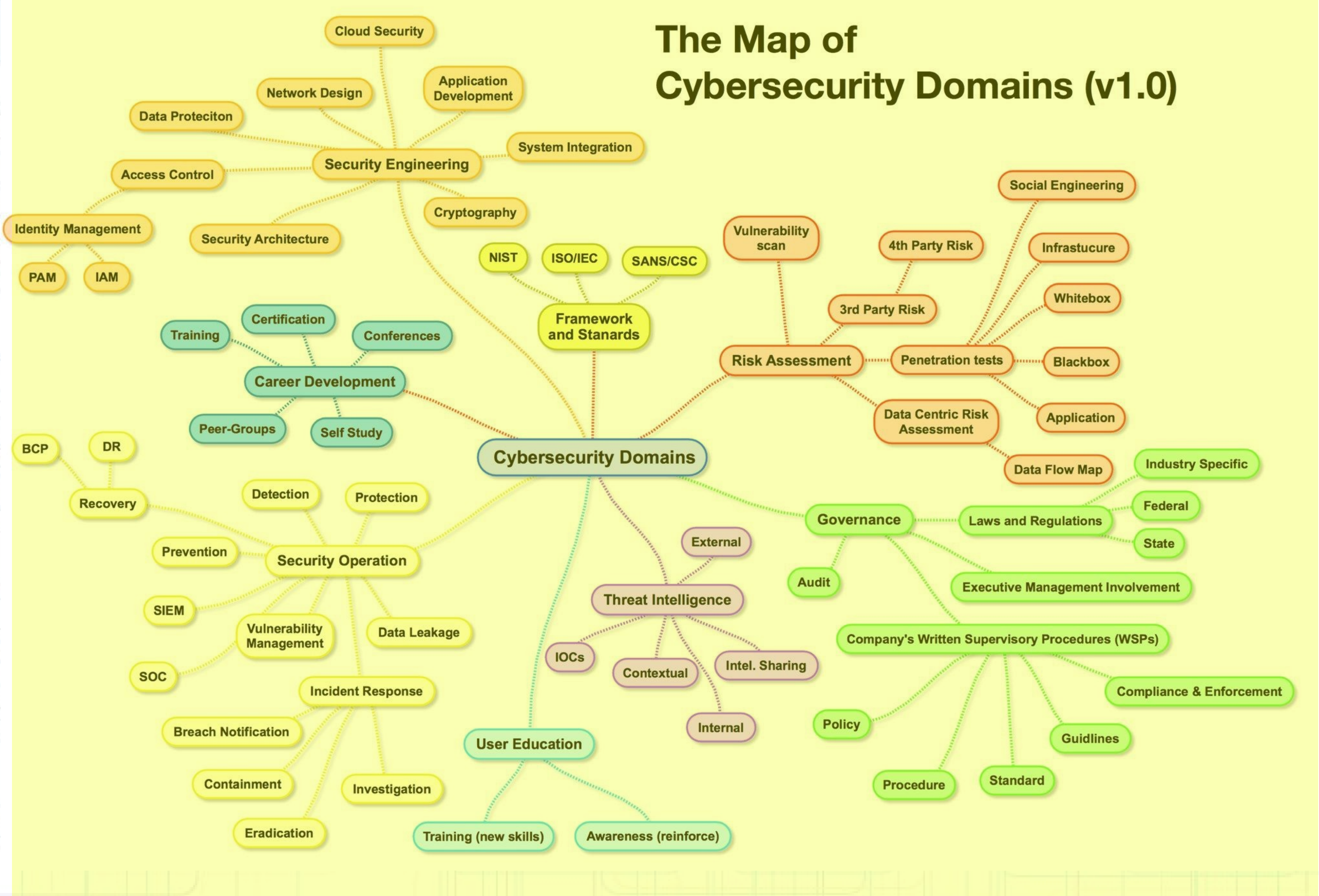
Introduction to IT Security

Renaud Dubois – December 2017

Introduction to IT Security

- Conceptual approach.. Don't go in bits and bytes.
- Straight to the goal & “keep in mind”
- Avoid to repeat what you know already

Introduction to IT Security



Introduction to IT Security

- 10 chapters of the CISSP (Certified Information Systems Security Professional)

1. Risk Management & Security Management Practices
2. Access Control Systems & Methodology
3. Cryptography
4. Physical Security
5. Security Architecture & Models
6. Telecommunications & Network Security
7. Law, Investigation & Ethics
8. Business Continuity & Disaster Recovery Planning
9. Application & Systems Development
10. Operations Security

The strength of the chain is in the weakest link

Risk Management & Security Management Practices

Risk Management & Security Management Practices

The 3 goals of any information security program:

CIA Triad: Confidentiality, Integrity, Availability

- Confidentiality: prevent unauthorized disclosure
- Integrity: prevent unauthorized modification,

  keep data consistent
- Availability: reliable and timely accessible

Risk Management & Security Management Practices

- Vulnerability: Weakness in a mechanism that can threaten the confidentiality, integrity or availability of an asset. Defines also the lack of countermeasure (example: un-patched application, lack of way to detect fraud, default password, concentration of responsibilities,..)
- Threat: Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. (sabotage, fraud & theft, loss of infrastructure, fire, hurricane,..)
- Risk: Probability of a threat becoming real and the corresponding potential damage
- Exposure: a vulnerability has been exploited by a threat agent (database hacked through an open port on the firewall)
- Countermeasure: A measure to mitigate potential losses
- $\text{Risk} = \frac{\text{Threat x Vulnerability}}{\text{Countermeasure}}$

Risk Management & Security Management Practices

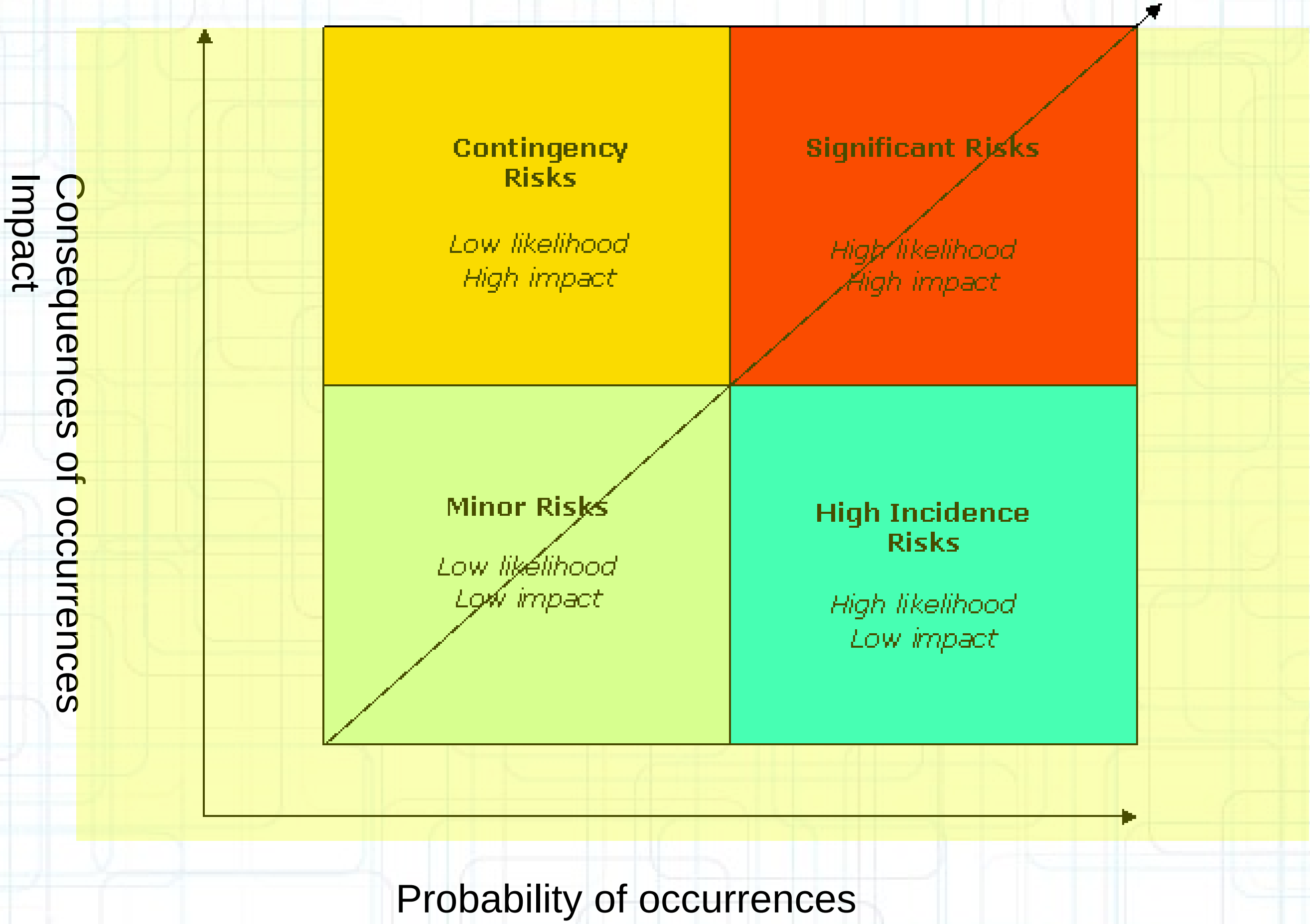
- Risk management is a systematic process for the controlled taking of known risks to attain approved objectives
- Goal of the “Risk Management” = Optimal security at minimal cost
- Who is dealing with the risks ? → Senior Management, Board
- Who is ultimately responsible for risk? → Management
- Management may delegate to departments and business units that shoulder some of the risk but ultimately the senior management is responsible for the companies health and risks.
- Risk Management Process

Plan → Collect information → Define recommendations → Management

- Risk Mitigation (implement countermeasures)
- Risk Transference (third party involvement, purchase insurance)
- Risk Acceptance (informed decision – no action taken)
- Risk Avoidance (decide to stop activity)

Risk Management & Security Management Practices

- Risk Approach



Contingency Risks

Low likelihood
High impact

Significant Risks

High likelihood
High impact

Minor Risks

Low likelihood
Low impact

High Incidence Risks

High likelihood
Low impact

Consequences of occurrences
Impact

Probability of occurrences

Risk Management & Security Management Practices

- How to calculate the risks ?

EF: Exposure Factor

ARO: Annual Rate of Occurrence

SLE: Single Loss of Expectancy

ALE: Annualized Loss Expectancy

Asset Value x EF = SLE

SLE x ARO = ALE

Risk Management & Security Management Practices

- An e-commerce website has a value of 300.000$. In case of attack on the website, the estimated damage to the company is 40% (loss revenue, liability, costs, confidentiality data corrupted,..)

Asset Value x EF = SLE

300.000$ x 0,4 = 120.000$

- Based on the current safeguards, this threat is estimated to happen once in 12 months

SLE x ARO = ALE

120.000$ x 1,0 = 120.000$

Risk Management & Security Management Practices

- The goal of the countermeasure is to reduce the potential loss (ALE value after implementation of countermeasure < ALE value before implementation)
- ALE for a specific asset is 78.000$ and after implementation of the control, the new ALE is 20.000$ and the annual cost of the control is 60.000$. What is the value of the control to the company ?

78.000$ - 20.000$ = 58.000$

58.000$ - 60.000$ = -2000$ → Not cost beneficial

Risk Management & Security Management Practices

Concept of Defense-in-depth

- Never rely upon just one control !
- Provide multiple layers of defense that an attacker must compromise before accessing an asset
- Compensate the weakness of one layer

Risk Management & Security Management Practices

Concept of Defense-in-depth

- Never rely upon just one control !
- Provide multiple layers of defense that an attacker must compromise before accessing an asset
- Compensate the weakness of one layer

Risk Management & Security Management Practices

Reactive – Alerts that occur at failure

Proactive – Alerts that occur before failure

Predictive – Alerts that trend on a possible failure

Risk Management & Security Management Practices

Concept of Defense-in-depth

- Never rely upon just one control !
- Provide multiple layers of defense that an attacker must compromise before accessing an asset
- Compensate the weakness of one layer

Access Control Systems & Methodology

Access Control Systems & Methodology

Access controls are security features that control how people can interact with systems and resources

Goal is to protect from un-authorized access

- Subject is a person, process or program
- Object is a resource (file, printer, database,..)
- Access is the data flow between an subject and an object

Access Control Systems & Methodology

- Identification: Who am I ? (user id)
- Authentication: Prove that I'm who I say I'm
- Authorization: What am I allowed to access
- Auditing/Accountability: audit logs and monitoring to track the user activity

Access Control Systems & Methodology

- Identification identifies an user uniquely (username, UID, email address,..)
- Don't share! No group account ! Must be unique for the accountability and responsibility purpose
- Standard naming

Access Control Systems & Methodology

- Authentication: proving who you say you are:
  - Something you know (password)
  - Something you have (smart card, token)
  - Something you are (biometrics)

  → Strong authentication is a combination of at least 2 factors

  → One factor authentication = username + password

  - Sometime also adding “Somewhere you are” (location)

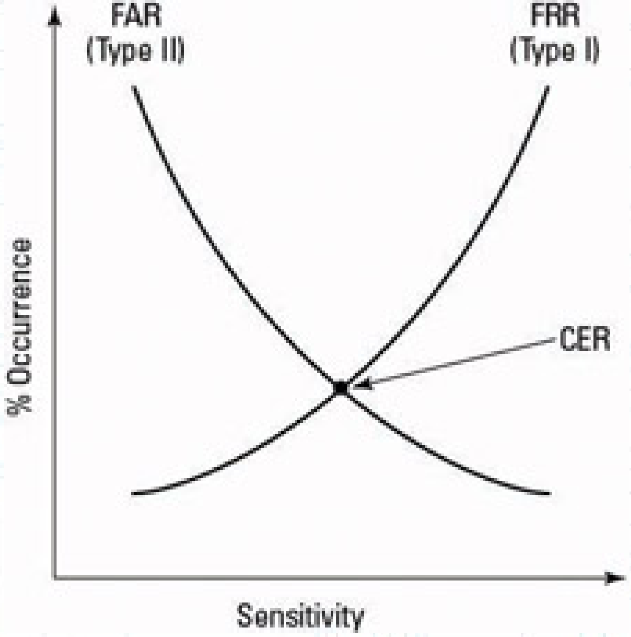
Access Control Systems & Methodology

Biometrics

- Unique personal attribute for authentication (1:1) or identification (1:N)
- Most expensive
- Sophisticated
- Enrollment time
- Can be based on
  - Behavior (signature dynamics) – might change over time
  - Physical attribute (fingerprints, iris, retina scans)

Access Control Systems & Methodology

- FRR: False Reject Rate (reject authorized individual)
- FAR: False Acceptance Rate (accepts impostor)
- CER: Cross Error Rate (FRR = FAR); % value – lowest % is the most accurate



Source: http://flylib.com/books/en/2.930.1.46/1/

Access Control Systems & Methodology

Some examples of biometric types

- Fingerprint
- Palm Scan
- Hand Geometry
- Retina Scan
- Iris Scan
- Keyboard Dynamics
- Voice Print
- Facial Scan

- RFID chips are not biometry !

Access Control Systems & Methodology

Attacks on password

- Sniffing
- Brute force attacks
- Dictionary Attack
- Social Engineering
- Rainbow tables → defense: hash(password+salt)

Access Control Systems & Methodology

One time password

- Only valid once
- Secure
- Not vulnerable to eavesdropping
- Require a token device to generate password
- 2 types: synchronous or asynchronous

Access Control Systems & Methodology

Memory card

- NOT a smart card
- Holds information, does not process
- Easily copied, not secure

Access Control Systems & Methodology

Smart card

- Holds and process information
- Can destroyed itself after a threshold of failed login
- Can provide two factor authentication

Access Control Systems & Methodology

Attacks on smart card

- Fault generation: manipulate environment controls and measure errors (change clock, change electrical signal,..)
- Software attack
- Side channel: non-intrusive such as measuring the electromagnetic field, the power,..
- Microprobing: advanced techniques to remote the protection on the cards circuits (laser, chemical, ultrasonic vibration..)

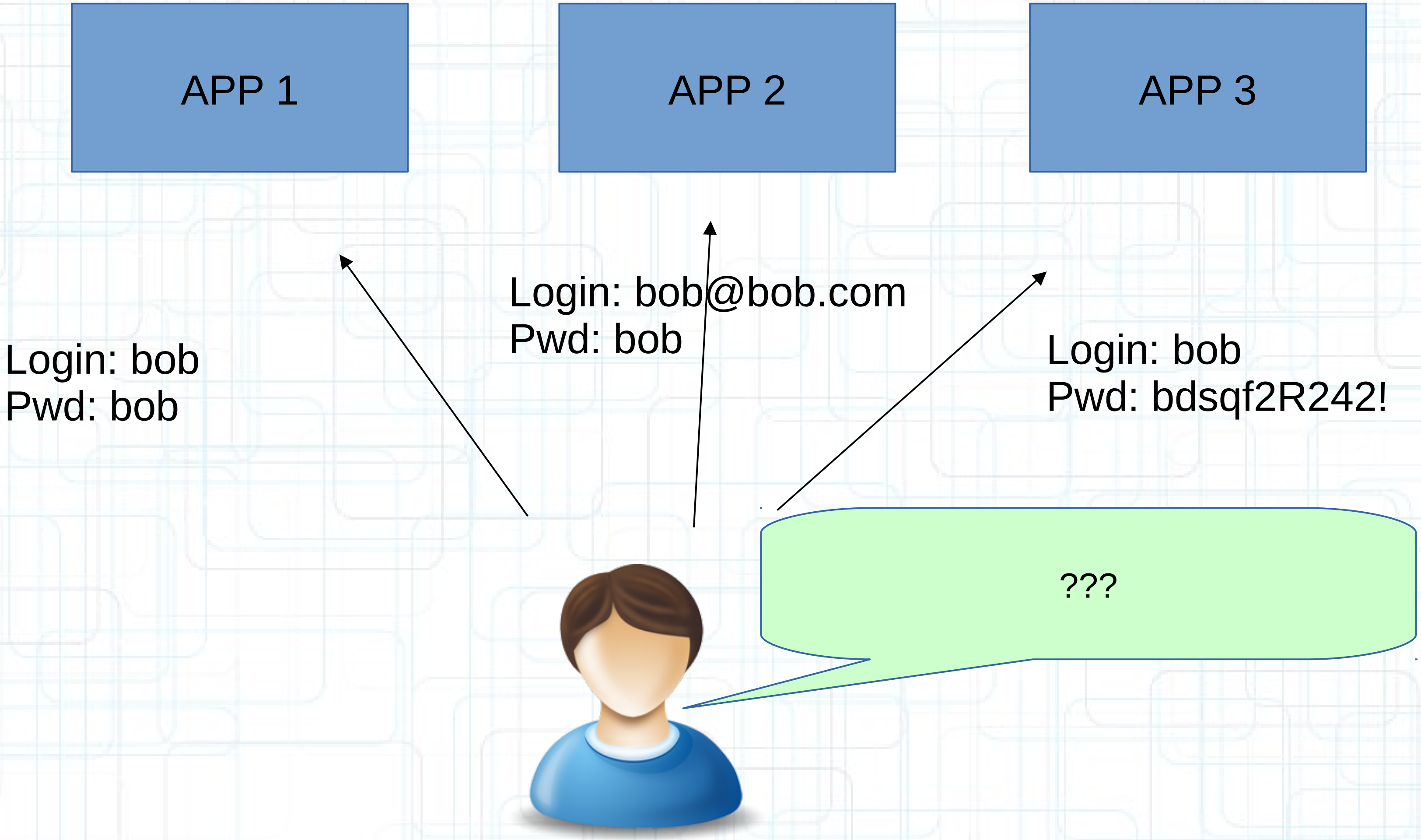
Access Control Systems & Methodology

Authorization

- Default NO access → principle “Need to know”
- SSO
  - Kerberos: use symetric key cryptology
  - SESAME: similar to Kerberos but asymetric key
  - SAML & Federation: newer on the market and XML based

Access Control Systems & Methodology

Why do we need federation ?



APP 1

APP 2

APP 3

Login: bob
Pwd: bob

Login: bob@bob.com
Pwd: bob

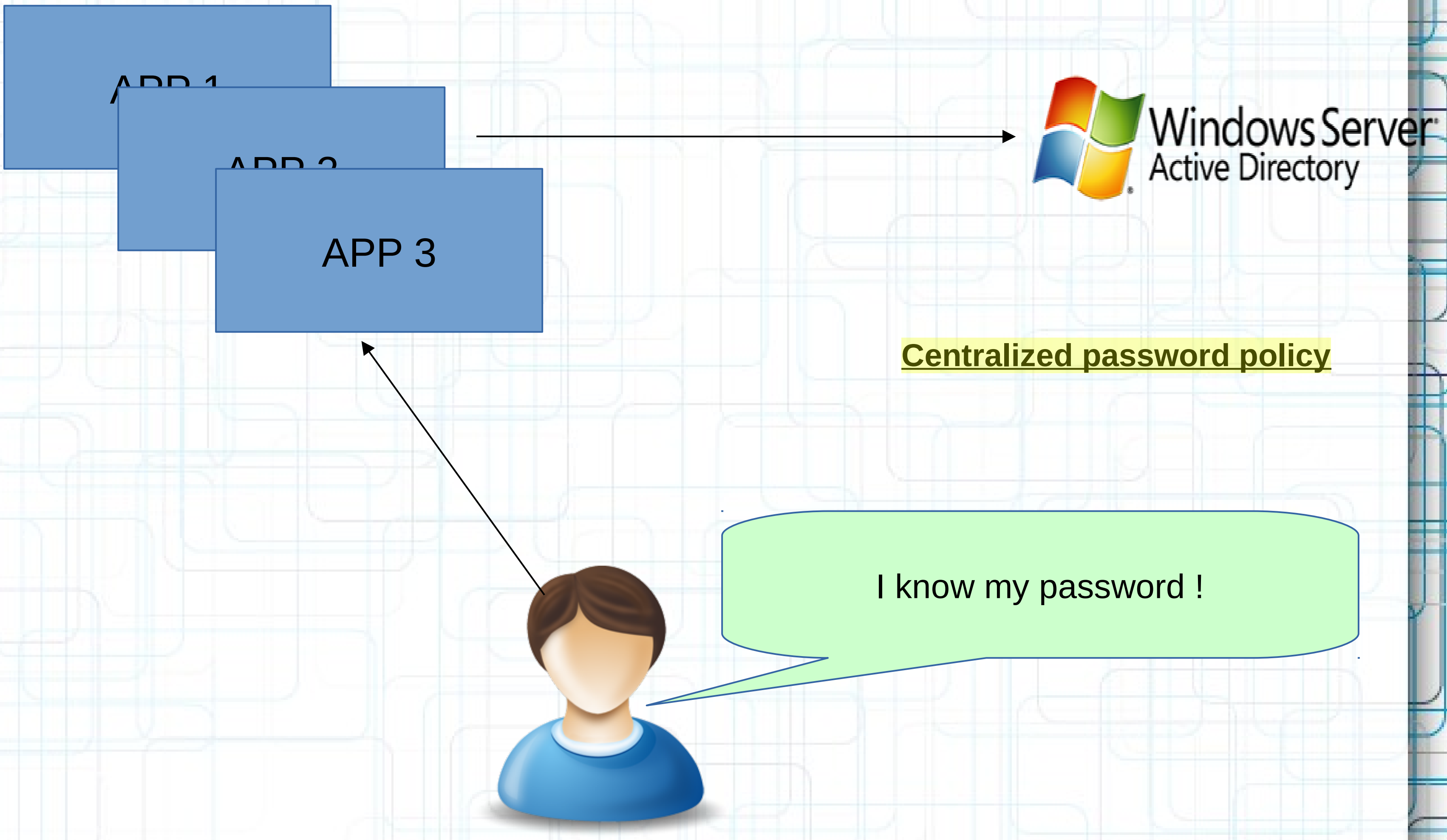
Login: bob
Pwd: bdsqf2R242!

???

Access Control Systems & Methodology

Then came Active Directory

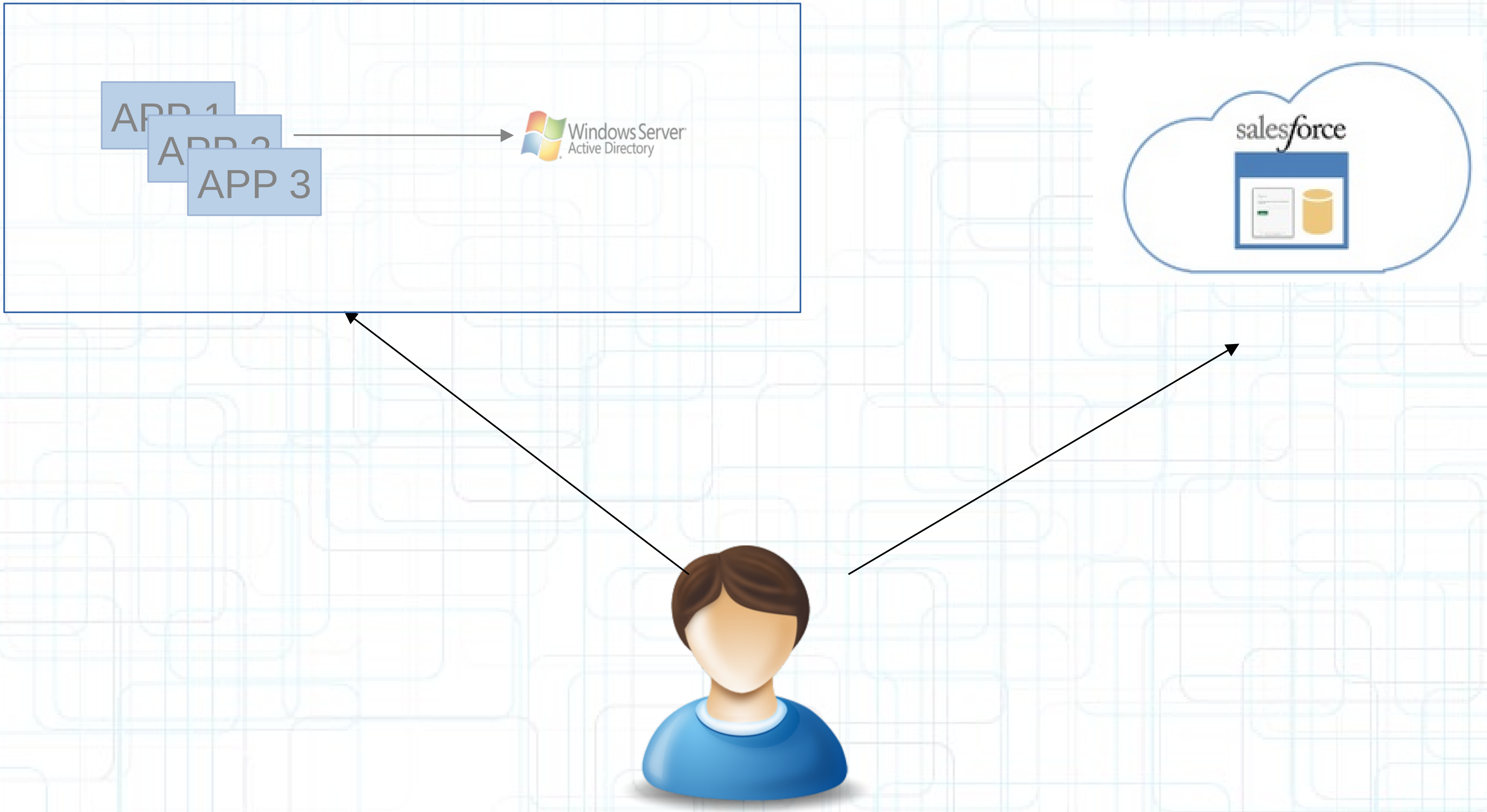
Login: bob
Pwd: bob!2”4oP)_3



Centralized password policy

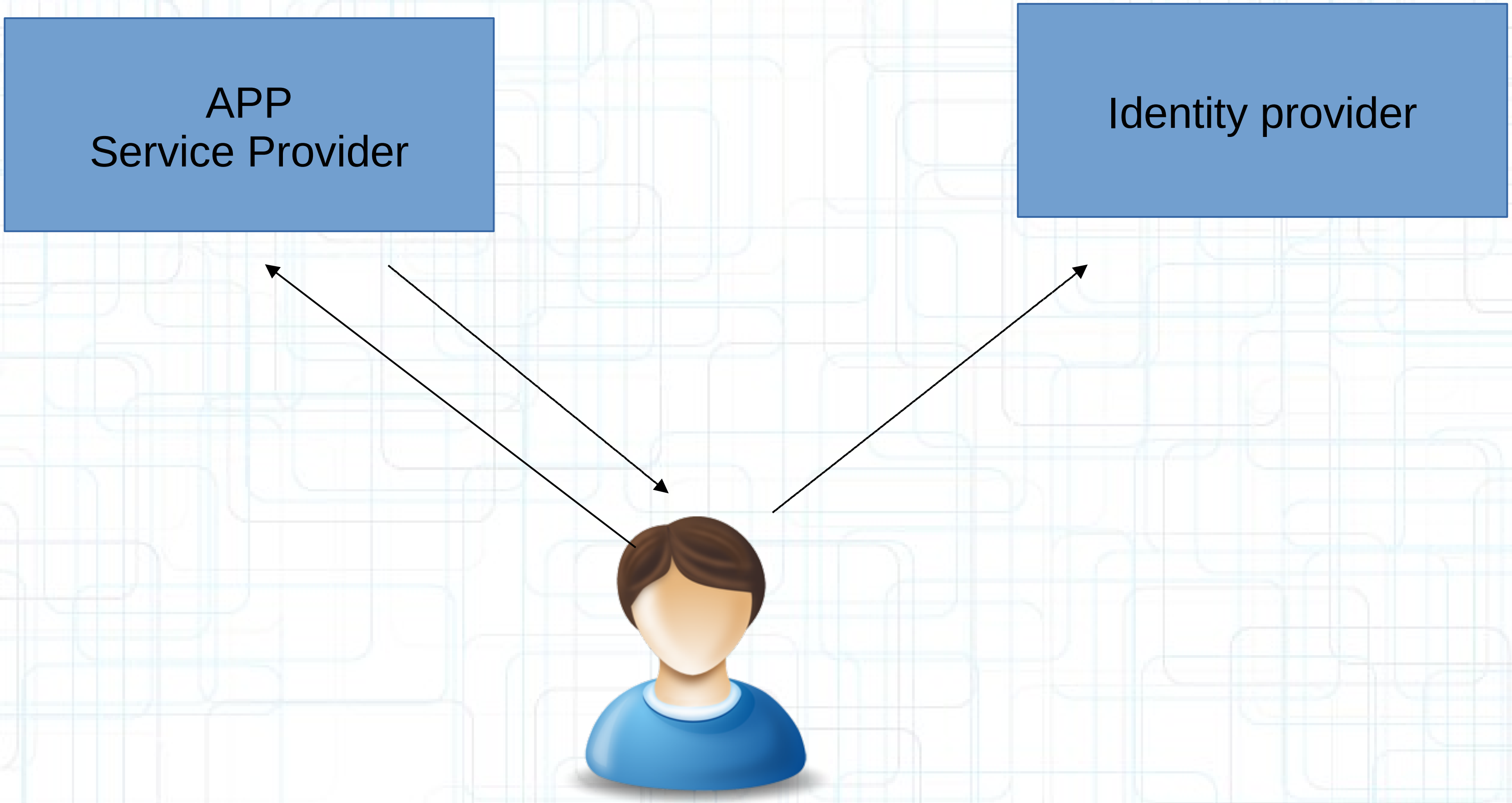
Access Control Systems & Methodology

Then came the cloud apps...



Access Control Systems & Methodology

Centralized identity provider



Access Control Systems & Methodology

IDS allows to detect intrusion and unauthorized access

Different types:

- NIDS Network based IDS
- HIDS Host IDS

Access Control Systems & Methodology

Network Based IDS

- Monitor network traffic ONLY
- Watch out for switches (use mirroring) or network tap
- Computer or network appliance with NIC in promiscuous mode
- Sensors communicate with a central management console
- Able to detect botnets on the network segment

Access Control Systems & Methodology

Host Based IDS

- Installed on computers
- Monitor logs or configuration files
- Agent that resides on individual computer
- Detect suspicious activities on a system, not a the network

Access Control Systems & Methodology

IDS types

- Signature based:
  - pattern matching, look for known signature
  - Must be updated with new signatures
  - Cannot stop 0-day attacks
- Anomaly based
  - Protocol based
  - Statistical anomaly based
  - Can detect 0-day attacks
  - Very subjective and could have higher rate of false positives

Physical Security

Physical Security

The 5 goals of the Physical Security

1)Deterrence (prevent)

2)Delaying

3)Detection

4)Assessment

5)Response

Physical Security

The 4 threats categories

1)Natural environment (flood, storm,..)

2)Supply system (power distribution outage, communication interruption,..)

3)Man-made (unauthorized access, explosion, fraud, vandalism,..)

4)Political events (strike, bombs, terrorist attack,..)

Telecommunications & Network Security

Telecommunications & Network Security

OSI Model:

- Application
- Presentation
- Session
- Transport
- Network
- Data link
- Physical

Telecommunications & Network Security

TCP/IP Model:

- Application
- Transport (Host to Host)
- Internet
- Link

Telecommunications & Network Security

Network Security services

- Firewall
- IDS/IPS
- SSL VPN
- IPsec VPN
- DDoS Defense
- Forward Proxy
- Reverse Proxy
- Authentication
- Session Border Controller
- SIEM - Security Information & Event Management

Telecommunications & Network Security

Firewall

- Enforce network policy
- Used to create DMZ
- Installed at the perimeter of the network to protect against the external threats
- Installed internally to segregate the network into different zones according to the risk profiles of the assets

Telecommunications & Network Security

Stateful firewall

- Keeps track of the connections in a table
- Allows dynamically the traffic to comeback
- Dynamic inspection (ALG) allows complex communications that require dynamic ports to be opened (such as FTP, RSH,..)
- Able to define NAT rules
- Able to setup VPN tunnels
- Redundant firewalls to avoid SPOF

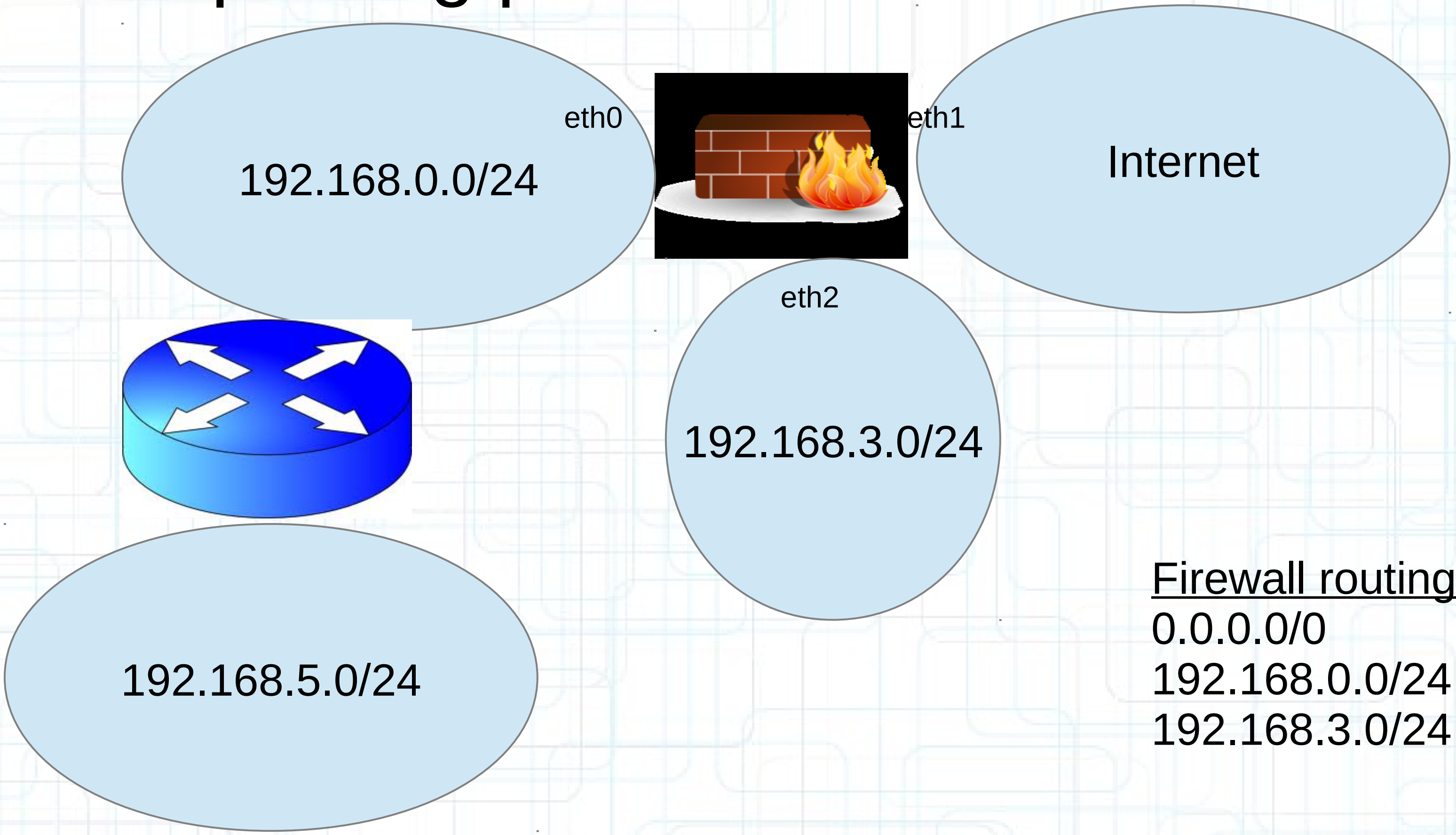
Telecommunications & Network Security

Redundant firewall

- Active/passive or active/active
- Stateful Synchronisation (ARP cache, session table, fib)
- Configuration synchronisation
- Exchange of heartbeats
- HA link
- Link monitoring
- Path monitoring (watchdog)

Telecommunications & Network Security

Antispoofing protection



Firewall routing table:
0.0.0.0/0 via eth1
192.168.0.0/24 via eth0
192.168.3.0/24 via eth2

Firewall rule:
From 192.168.3.1 to 192.168.5.5, allow HTTP

Telecommunications & Network Security

Firewall best practices

- Keep the rules simple
- Group the rules by category
- Avoid the multiplications of “exceptions”
- Enable anti-spoofing protection
- Avoid to use “ANY” keyword
- Use least privilege principles
- Enable logging
- Regular review of the rules is needed (obsolete, shadowing,..)
- Be careful with tunnels or tunneling protocol

Telecommunications & Network Security

Security zones

- Segregate the assets of different security levels into security zones or areas
- Each zone has its own level of trust (e.g. PCI)
- Protect the data center against the outside world, but also against the internal users
- Use firewalls to separate the security zones
- Use a frontend gateway, located in DMZ, to protect the assets
- Intra-zone traffic is typically allowed by default

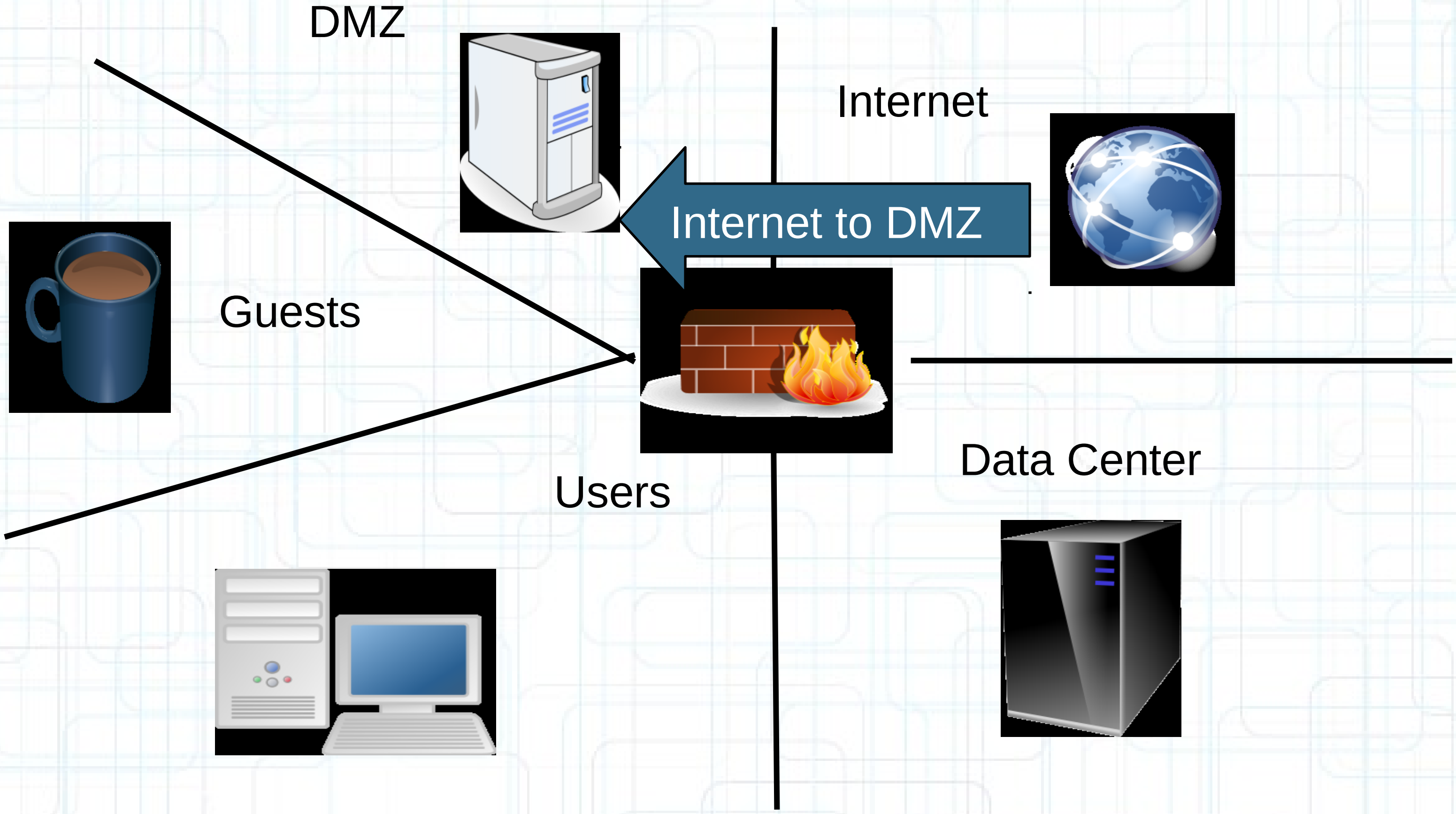
Telecommunications & Network Security

DMZ

- A buffer zone between an unprotected network and a protected network that allows the regulation and the monitoring of the traffic between the two
- Hardening of the servers placed in DMZ
- Group the servers into different DMZ's following the business needs
- Authenticate the users in DMZ

Telecommunications & Network Security

Security zones



Telecommunications & Network Security

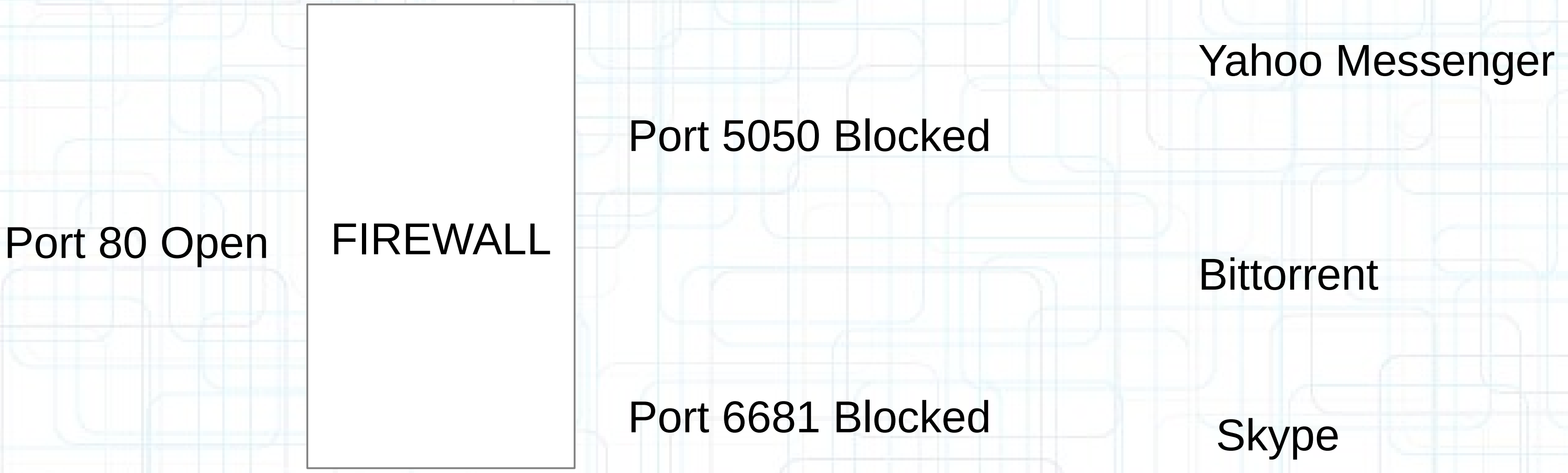
Next generation firewalls (NGFWs)

- Standard firewall features (NAT, stateful inspection, VPN,..)
- IDS/IPS integrated in the firewall
- Application awareness
- Threat detection and application vulnerability lists
- Integrated with AD or captive portal: “user based” and not only “ip based”. Users are now mobile and have multiple workplaces.
- SSL decryption

Telecommunications & Network Security

Next generation firewalls (NGFWs)

Evasive applications are able to detect the blocked ports and use port-hopping techniques to bypass the security rules



Yahoo Messenger

Port 5050 Blocked

Port 80 Open

FIREWALL

Bittorrent

Port 6681 Blocked

Skype

Telecommunications & Network Security

Next generation firewalls (NGFWs)

In the past, port 80/443 traffic was clearly classified as web browsing traffic.

Today, it could be:

Salesforce.com → Business application

Gmail → Web Mail

Meebo → instant messaging

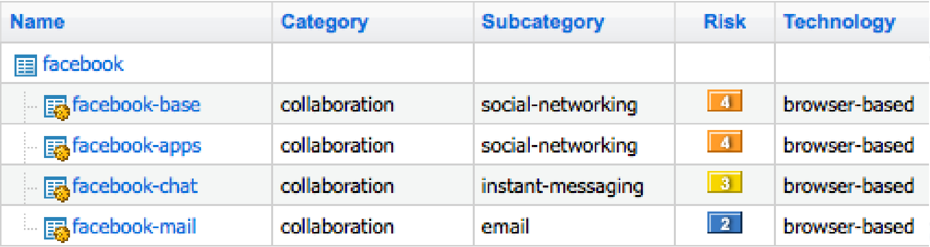
Youtube → Media

Conclusion: we need visibility at application (L7) level

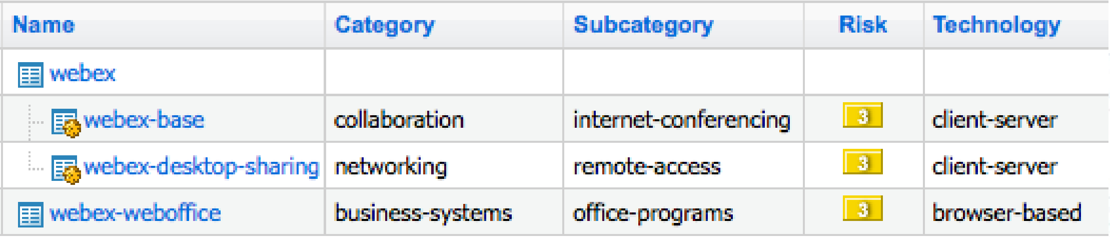
Telecommunications & Network Security

Next generation firewalls (NGFWs)

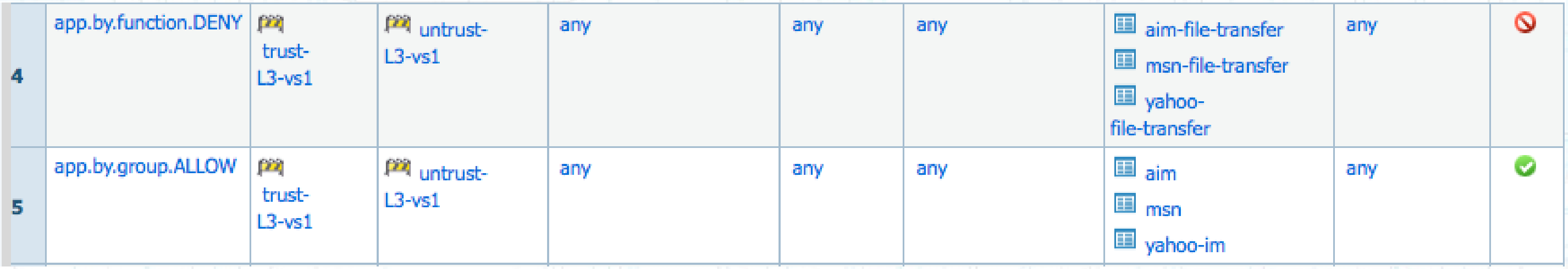
“Application awareness”



Name	Category	Subcategory	Risk	Technology
facebook				
facebook-base	collaboration	social-networking	4	browser-based
facebook-apps	collaboration	social-networking	4	browser-based
facebook-chat	collaboration	instant-messaging	3	browser-based
facebook-mail	collaboration	email	2	browser-based



Name	Category	Subcategory	Risk	Technology
webex				
webex-base	collaboration	internet-conferencing	3	client-server
webex-desktop-sharing	networking	remote-access	3	client-server
webex-weboffice	business-systems	office-programs	3	browser-based



4	app.by.function.DENY	trust-L3-vs1	untrust-L3-vs1	any	any	any	aim-file-transfer msn-file-transfer yahoo-file-transfer	any	⊘
5	app.by.group.ALLOW	trust-L3-vs1	untrust-L3-vs1	any	any	any	aim msn yahoo-im	any	✓

Telecommunications & Network Security

Next generation firewalls (NGFWs)

Able to decode the stream and apply contextual signatures to detect the application

If the traffic is encrypted (e.g. SSL), the firewall must be the SSL endpoint to be able to decrypt the SSL traffic and then detect the encapsulated protocol (e.g. HTTP) and finally the application

Heuristics engine, based on patterns to identify application (used for proprietary end-to-end encryption such as Skype or BitTorrent)

Telecommunications & Network Security

Next generation firewalls (NGFWs)

Reminder about HTTPS connectivity:

1) Browser downloads the server certificate. The certificate is signed with the private key of a trusted CA.

2) The browser uses the public key of the trusted certificate (installed by default in the browser) to verify that the server certificate is indeed signed by the trusted CA

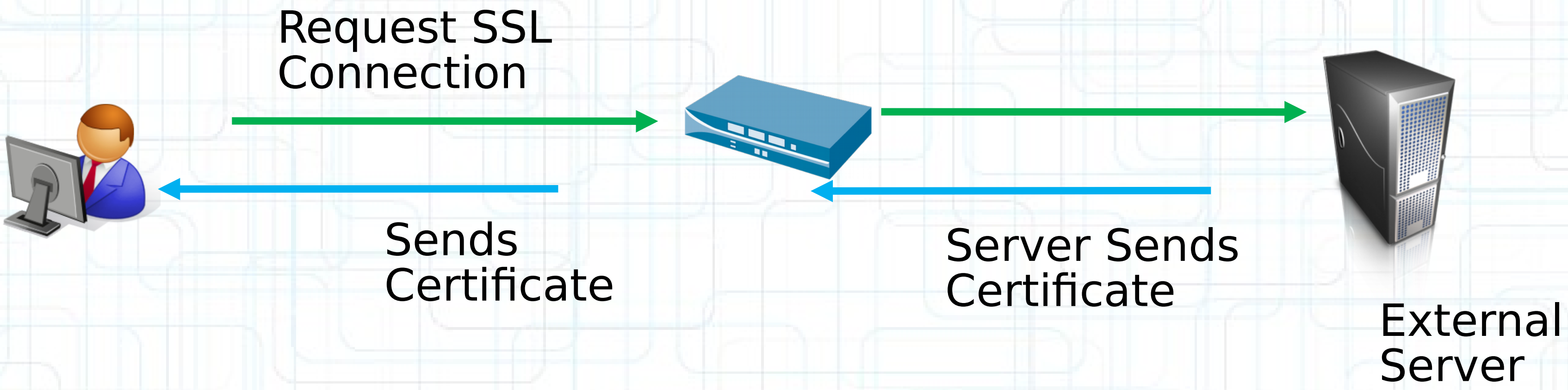
3) The browser verifies the URL presents in the certificate is indeed the one to which a connection has been opened

4) The browser generates a symmetric key that is being used to encrypt the HTTP traffic

Telecommunications & Network Security

Next generation firewalls (NGFWs)

SSL decryption



Request SSL Connection

Sends Certificate

Server Sends Certificate

External Server

Telecommunications & Network Security

Next generation firewalls (NGFWs)

Not a solution to every problem

- Use WAF for web application attacks (XSS, SQL injection, etc) → Don't confuse “application aware” with Web Application Security
- Use dedicated email security solution for advanced spam filtering

Telecommunications & Network Security

Next generation firewalls (NGFWs) - bots detection

Bots steal sensitive info

Bots send spam, act as a proxy

Execute DDos & distributed attacks

Telecommunications & Network Security

Example of real attack

- An email containing is link to a phishing website is sent
- The user accesses the phishing website, enters its credentials
- The phishing website sends a malware to the user disguised as a “Security Update”
- The user executes the applications. All the data are compromised and the computer is now part of a botnet sending spam and phishing emails

Telecommunications & Network Security

Example of countermeasure on this attack

- An email containing is link to a phishing website is sent → The message can be detected as a spam before the user reads the email
- The user accesses the phishing website, enters its credentials→ The access to the phishing website can be blocked by a proxy
- The phishing website sends a malware to the user disguised as a “Security Update” → The content scanning can prevent malicious content to be downloaded. Moreover, the local antivirus can detect the malware
- The user executes the applications. All the data are compromised and the computer is now part of a botnet sending spam and phishing → The bonet can be detected by the IDS/IPS functionality and the flows can be blocked by the firewalls

→ In each case, security administrators are able to be alerted

Telecommunications & Network Security

Network based attacks:

- Network as a channel for attacks (viruses, worms, spam,...)
- Network as the target of the attack
  - Reconnaissance attack (gain info about the network): scanning, sniffing,..
  - Unauthorized access (social engineering, clear text password, weak password, misconfiguration,..)
  - Session Layer attack (spoofing, session replay, session hijacking,..)
  - Denial of Service (Switch MAC address table flooding, STP flapping, TCP SYN flood,...)
  - Network service attacks (DNS cache poisoning, Rogue DHCP server,..)

Telecommunications & Network Security

“I will do my home-made encryption algorithm, so I'm sure nobody can decrypt it”

“I will upload this confidential file on a hidden folder of my web server so nobody can find it”

→ YOU ARE WRONG

- Security by obscurity is a weak security control
- Not a bad idea to keep secrets but nearly always fails when it's the only control
- E.g. alternate port binding, hidden folder on a website containing secret information,..

Telecommunications & Network Security

“*I'm not in financial or governmental activities, security doesn't concern me*”

→ YOU ARE WRONG

- Manual attacks
- Automated attacks
- Servers attack (Internet but also Intranet !)
- Clients attack

Telecommunications & Network Security

Principles and “keep in mind”

- Defense in Depth
- Network segmentation
- Least Privilege
- Mediated access through gateways and control points
- Accountability and traceability
- Separation of duties
- Industrialized solutions
- Out of band management
- Strong separation between Production and Non-Production
- Encryption is needed but can be maliciously used to bypass network security controls

END