ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

User management

COM-402: Information Security and Privacy

(slide credits: Cristina Basescu)

Users vs company resources

- **Company resources**
  - Located on premises or in the cloud
  - Servers, workstations, data, applications
- **Users access company resources**
  - On premises through corporate-owned / personal devices
  - From outside the company's network through corporate-owned / personal devices

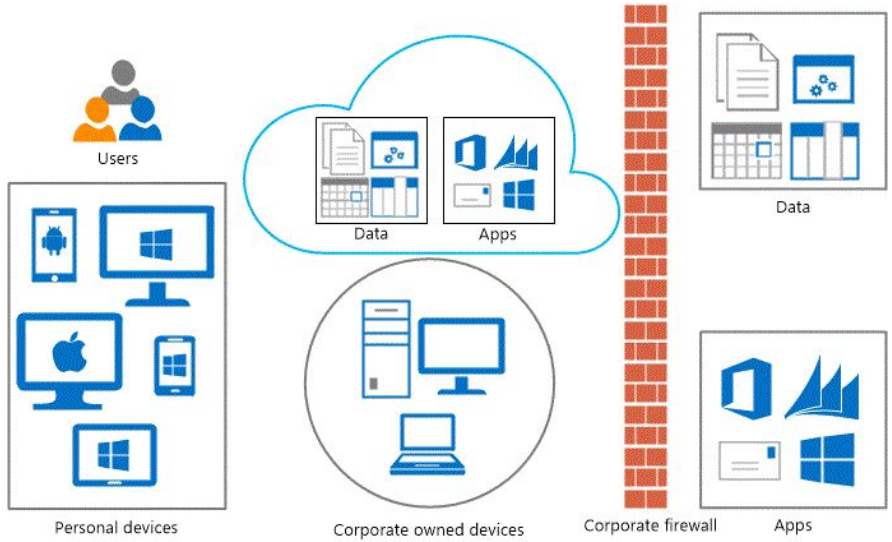
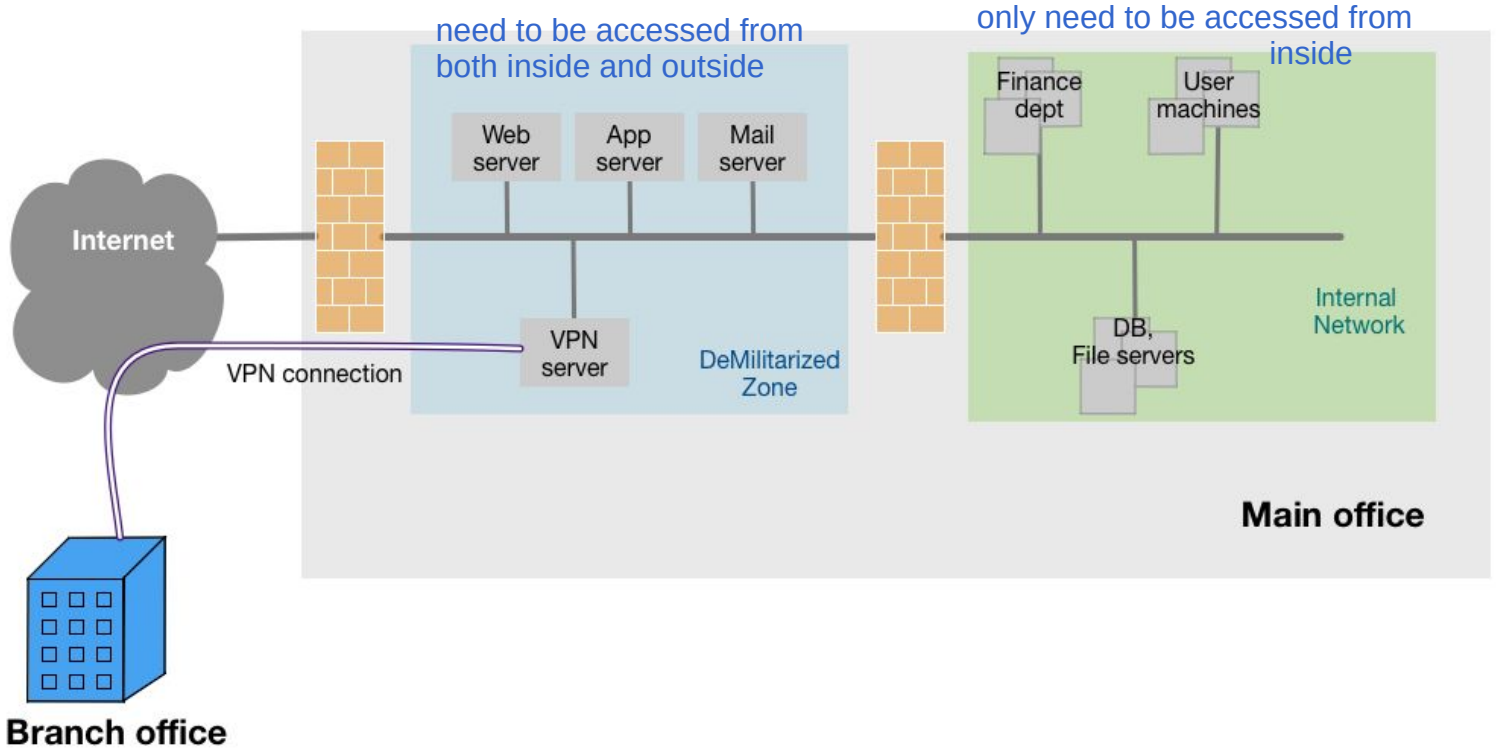
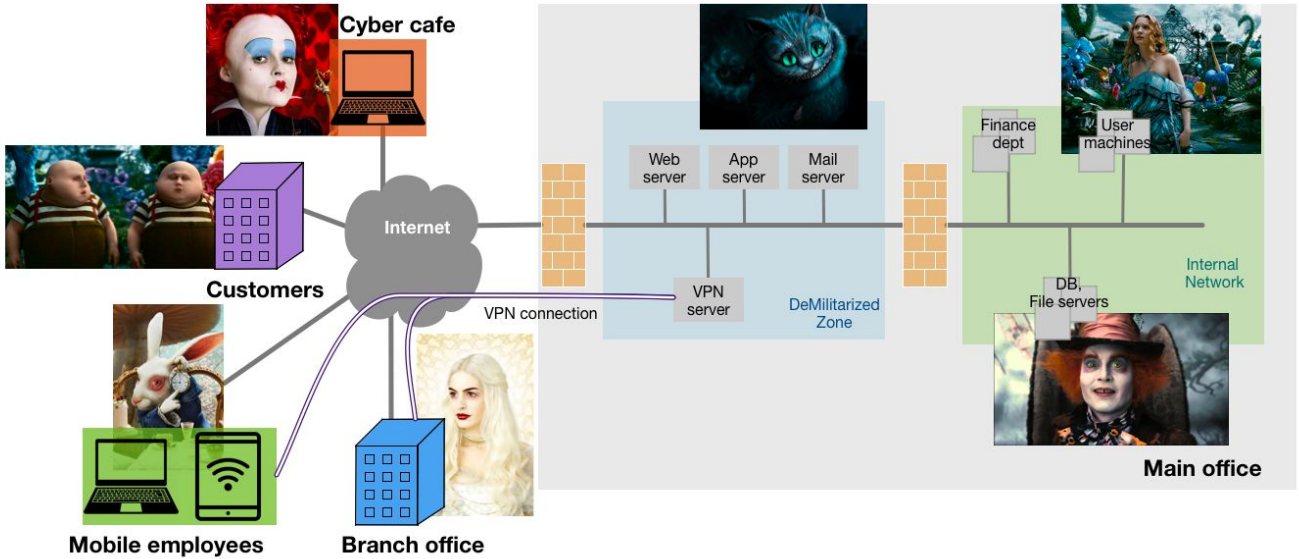


Image from https://technet.microsoft.com/en-us/library/dn550982(v=ws.11).aspx

Typical enterprise infrastructure



User interaction with company resources



- **Wonderland is complicated**
  - Who can install software on user machines?
  - Who can read files from the mail server?
  - How to authenticate users?

Which user is the weakest link?

Image from http://jennybrice.com.au/wp-content/uploads/2016/02/full-list-of-weakest-link-episodes-u1.jpg

Outline

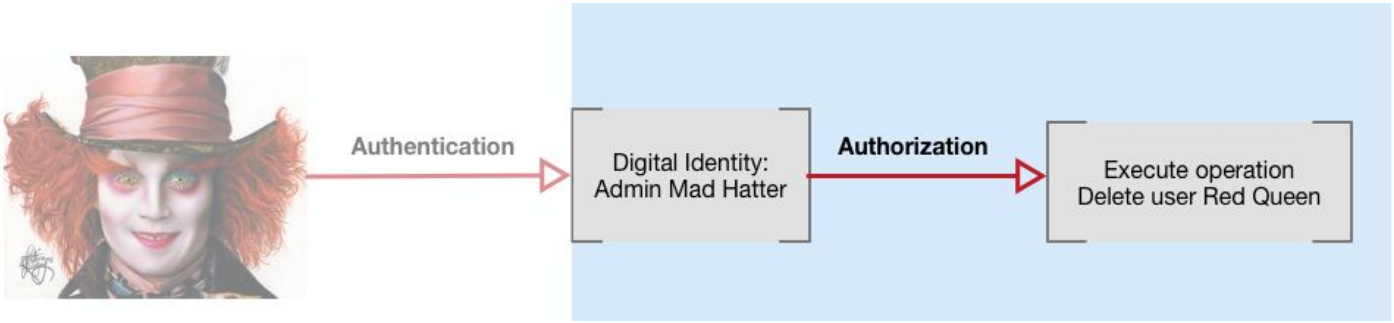
- **Access control**
- User authentication using passwords
- Kerberos
- Multi-factor authentication
- LDAP
- User training

Access control

- **Define and enforce users' restricted access to resources**
  - Subject S (e.g., user, process) attempts to perform operation O (e.g., read, write) on resource R (e.g., file, socket)

rows are users, processes... (entities that need access), cols may be the targets that'd need to be accessed. Such a matrix would have the info on who can access what. You can have several matrices, one for each operation (read, write...)

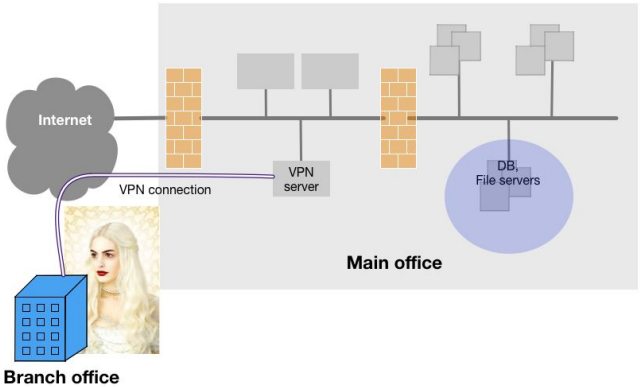
- **Subject already logged in the system under a digital identity (later today)**
- **Principle of least privilege**
  - Access granted only to resources required to fulfill duties

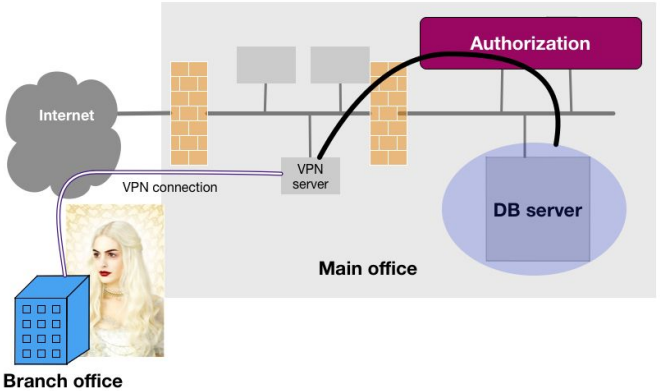


Multiple levels of access control

if a machine is allowed to connect to another machine, firewall configs..

- **Network-level access control to reach the dst machine (next week) (left fig)**
  - E.g., Can messages from White Queen's network reach the DB server?
- **User management within the enterprise (right fig)**
  - E.g., Is the White Queen herself allowed to connect to the DB server?
- **Operating System-level access control (right fig)** usernames, pwds, ...
  - E.g., Can the DB engine be executed by the user she logged in as within the OS?
- **Access control of the application itself**
  - E.g., access control of the DB engine (previous lecture)





Multiple approaches to access control

Three common varieties:

1. Role-Based Access Control (RBAC)
2. Discretionary Access Control (DAC)
3. Mandatory Access Control (MAC)

1 Role-based access control (RBAC) (1)

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- **Standardized by NIST since 1992 (latest in 2012: INCITS 359-2012)**
- **Centered on user roles** you sort users into roles, and take decisions for the roles
  - A role can contain multiple permissions
  - A user can be assigned multiple roles
  - This reduces the number of decisions per user

Subjects

Many to many mapping

	Navigate Pages	Draw / Markup	Import Content Sync Rights	Delete Pages & other user's content	Permission Controls	Vyew Room Settings
Owner	✓	✓	✓	✓	✓	✓
Moderator	✓	✓	✓	✓	✓	
Collaborator	✓	✓	✓			
Reviewer	✓	✓				
Viewer	✓*					

* A viewer can only navigate pages if Sync Mode is OFF.

Roles

for each role, there's a set of permissions that the role is associated with

1 Role-based access control (RBAC) (2)

- **RBAC for user management within the company**

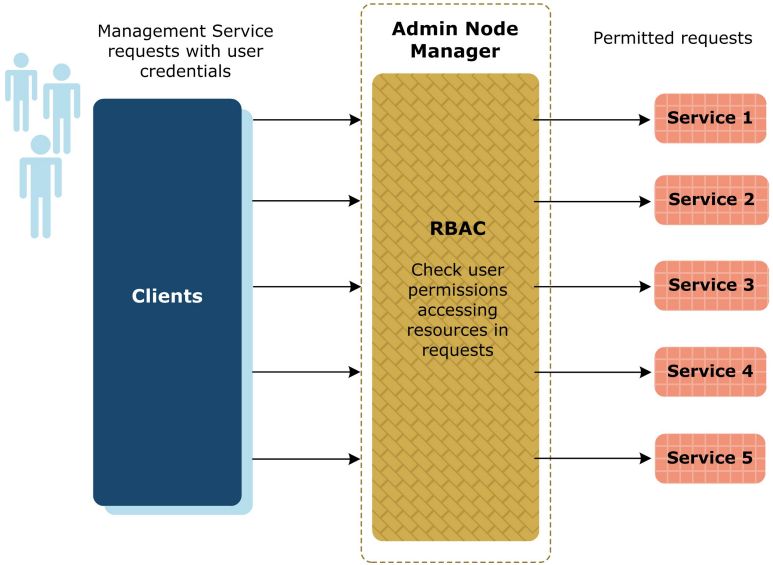


Image from https://docs.axway.com/u/documentation/api_gateway/7.5.2/webhelp_portal_admin/Content/Resources/Images/docbook/images/admin/rbac/rbac_overview.png

RBAC in Windows

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- **Windows Authorization Manager (AzMan)**
  - Administrative Tools for users to manage authorization policies
  - Runtime Executives for applications to perform access checks against policies
- **Available in:**
  - Windows Server (2012 / 2008 R2 / 2008 / 2003), Windows 8, 7, Vista, XP
  - Deprecated as of Windows Server 2012 R2, replaced with Dynamic Access Control
- **Azman components:**
  - Authorization Store - stores policies
  - Application
  - Scope - resources with the same policy
  - Role - in the sense of RBAC role
  - Operation - RBAC action
  - Task - RBAC action set

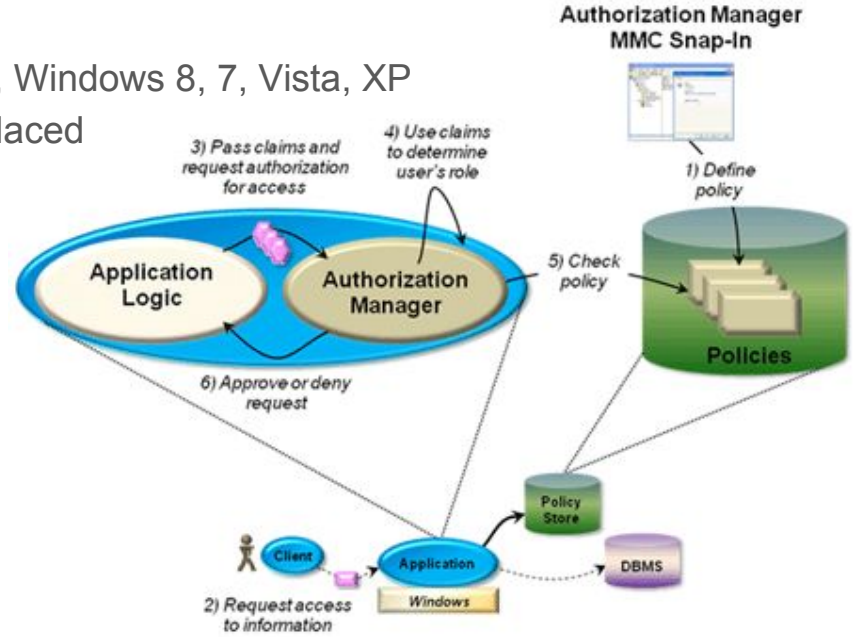


Image from https://i-msdn.sec.s-msft.com/dynimg/IC159391.gif

1 Advantages of RBAC

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- ✓ **Easy to grasp the idea of roles**
- ✓ **Easy to manage in principle**
  - Roles decouple digital identities from permissions
  - Simply assign roles to a new subject, instead of deciding on access for each resource
  - Easy to revoke authorization for a subject by removing roles
- ✓ **Easy to tell through roles which permissions a subject has, and why**
  - Typically centrally managed

1 Disadvantages of RBAC

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- ✖ **Difficult to decide on the granularity of roles**
  - Should we create separate roles for modifying client information and for deleting a client, or not?
  - Is authorization too broad / still up-to-date for all subjects having this role?
- ✖ **Role meaning is fuzzy**
  - Employee position in company may be different from RBAC roles (think of developers in the same team working on different projects)
  - Source of misunderstanding between admins and managers, for instance who assign them
- ✖ **Unclear if roles can be shared between different departments**

2 Discretionary access control (DAC)

this one is often the default

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- **Access control is at the discretion of the object owner** "discretionary access control"
  - Object owner specifies policies to access resources it owns
- **Access control matrix to represent rules**

(a)
  - Stored by column: access control list (ACL) stored with resource

	/stud1/grades.txt	/hw1/grade.sh	/sensitive
Stud1	r--	--x	---
TA1	rw-	rwx	r-x

(b)
  - Stored by row: access rights (capability) of a given process or user

	/stud1/grades.txt	/hw1/grade.sh	/sensitive
Stud1	r--	--x	---
TA1	rw-	rwx	r-x

"row oriented"
capability approach
for each user, what they can do

ACL vs Capabilities

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Capability (b)	ACL (a)
× Instant revocation hard you'd need to go through the list of all users	✓ Instant revocation possible, especially for single object
✓ Eventual revocation easy (create no more capabilities)	× Revocation requires changing many objects
✓ Easy to give access to new subjects	× Giving access to new subjects requires updating objects
✓ Enables delegation	× Difficult to delegate
✓ Easy to enumerate accessible objects per user	× Hard to enumerate accessible objects per user
× Hard to enumerate users that can access object	✓ Easy to enumerate users that can access object

Slide adapted from System Security course at ETH, ©David Barrera

DAC in Unix (1)

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- **Definition of capability**
  - In Unix it refers to access rights of a subject on an object
  - Generally it denotes an unforgeable token that grants access rights and that can be passed around
- **ACLs**
  - Store rights with the target object
  - Group subjects in three accessor categories
  - Representation compressed to 9 bits
    - 3 groups of R,W,X bits, each group then converted to octal
    - Example: 754 means `rwx|r-x|r`

Accessor	Access to descriptor
owner	Read, write, execute
group	Read, execute
others	Read

DAC in Unix (2)

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- **Setuid / setgid**
  - Set user / group id upon execution
  - User executing file with setuid bit set gets permissions of user or group owning the file
- **Use setuid / setgid responsibly**
  - Why do we need setuid on `/usr/bin/passwd` (see below)
  - What could go wrong if executable with setuid bit set has a vulnerability?

```
-rwsr-xr-x 1 root root 42856 2009-07-31 19:29 /usr/bin/passwd
```

DAC pros and cons

✓ Advantages

- Flexible - the main reason of its popularity in OSes
- Easy to implement
- Intuitive
- Flexibility

✗ Disadvantages

- Rely on resource owner's judgement to modify the protection state of the resource
- DAC works if all processes are benign, and users make no mistakes (impossible)
- Vulnerability to trojans: users A, B, data D only readable by A. B sends trojan to A that, when run by A, reads D and writes it under D', readable by B

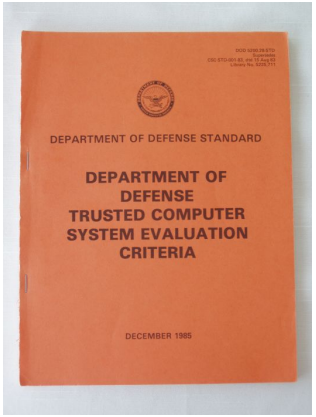
Mandatory access control (MAC)

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

tries to ensure that even someone with access cannot leak the data

- **Historically associated with the military to protect information**
  - Multi-level security: unclassified, confidential, secret, top secret
- **The system labels both subject and objects with security labels**
  - Can only be modified by trusted administrators via trusted software
  - ~~Labels are immutable during system execution~~
- **Security policy:**
  - Subject can access object if subject's label has a higher or equal label compared to object's label

only
v



- **Can be used in conjunction with DAC or RBAC**

! **(Do not confuse with message authentication codes)**

MAC security labels

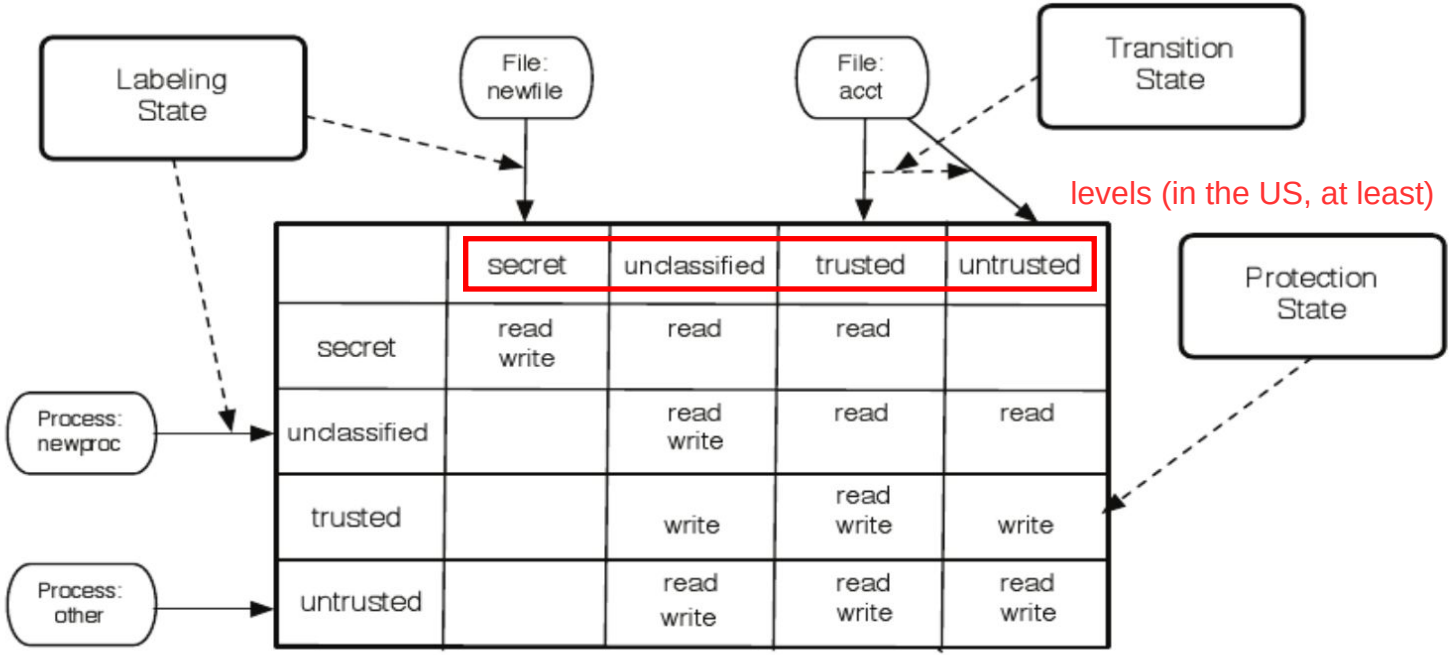
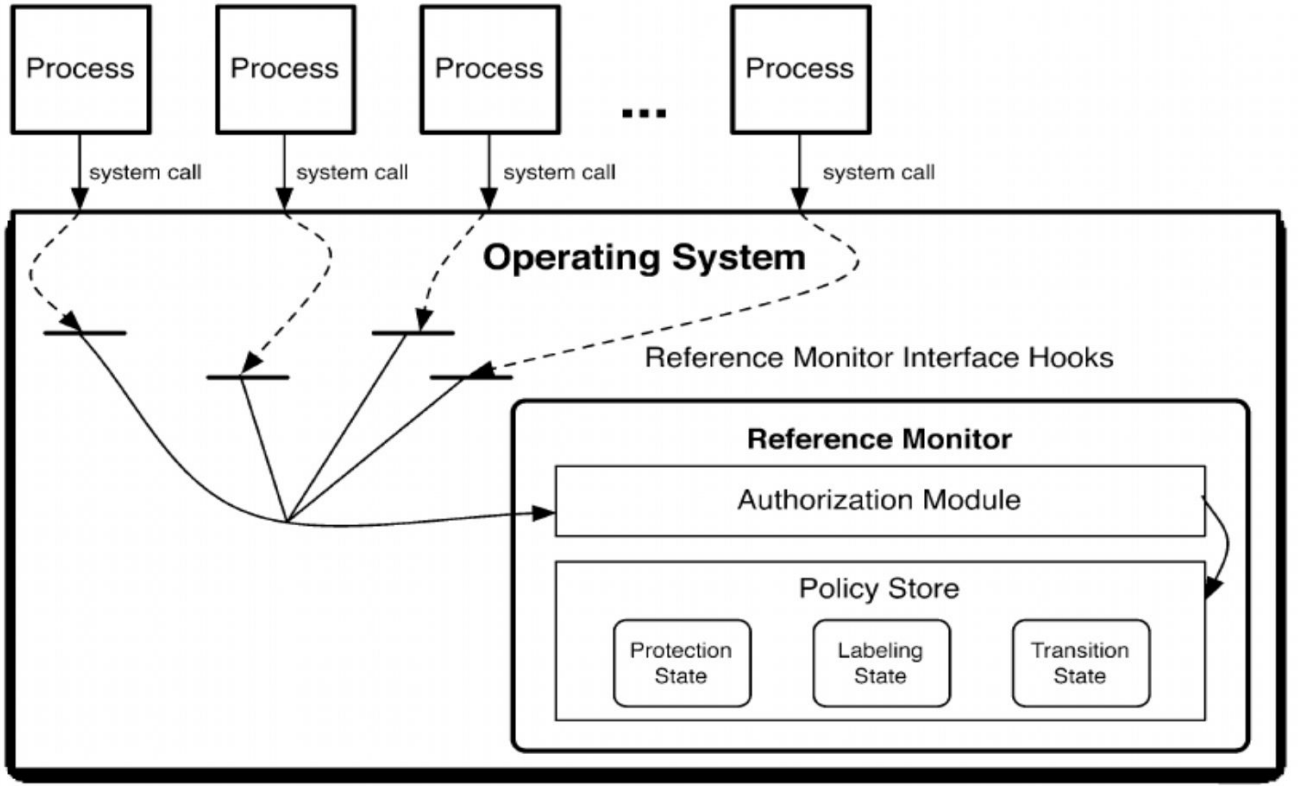


Figure 2.2: A Mandatory Protection System: The *protection state* is defined in terms of labels and is immutable. The immutable *labeling state* and *transition state* enable the definition and management of labels for system subjects and objects.

MAC in Operating Systems

- **Arguably wider audience after Linux Security Modules (LSM)**
  - Part of Linux kernel since Linux 2.6
  - Makes it possible to add a MAC security module to the OS
  - Currently accepted modules: AppArmor, SELinux, Smack, TOMOYO Linux, Yama
- **Trusted Solaris also implements MAC**
- **Implemented using a Reference Monitor**
  - Input: request to perform operation
  - Output: binary response indicating whether request is authorized by the policy

Reference Monitor (1)



Slide adapted from System Security course at ETH, ©David Barrera

Reference Monitor (2)

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- **Reference monitor interface**
  - Intercepts all security-sensitive operations
  - OS must be designed such that sensitive system calls use this interface
- **Authorization module**
  - The brain
  - Converts request into query that can be looked up in the policy store
- **Policy store**
  - Database containing protection state, labelling state, transition state

Linux Security Modules (LSM) (1)

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

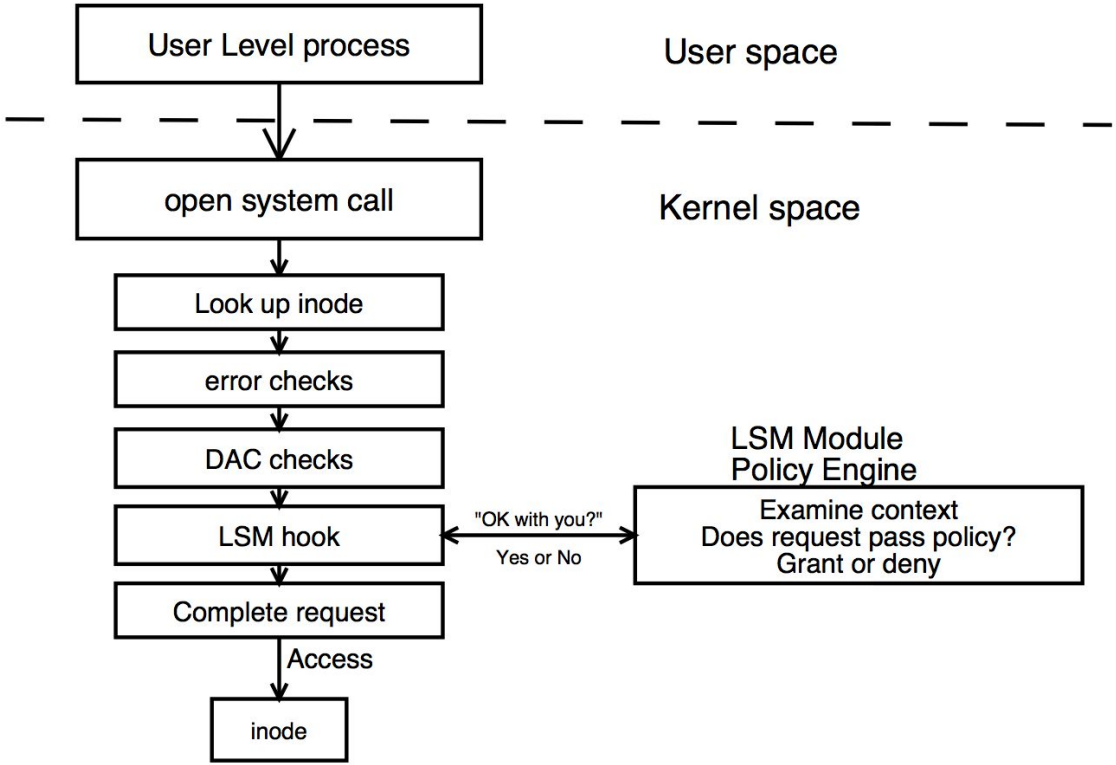
- **Functions for modules to register / unregister as security modules**
- **Opaque security fields associated with kernel objects**
  - Must handle pre-existent objects, which do not have security fields associated
  - Either ignore pre-existent objects or set security fields during module initialization
- **Security hooks for function calls inserted in the kernel**
  - Implemented by security modules
  - Hooks are called after DAC checks

Table: Kernel data structures modified by the LSM kernel patch and the corresponding abstract objects.

STRUCTURE	OBJECT
task_struct	Task (Process)
linux_binprm	Program
super_block	Filesystem
inode	Pipe, File, or Socket
file	Open File
sk_buff	Network Buffer (Packet)
net_device	Network Device
kern_ipc_perm	Semaphore, Shared Memory Segment,
	or Message Queue
msg_msg	Individual Message

Image from https://www.usenix.org/legacy/event/sec02/full_papers/wright/wright_html/node6.html

Linux Security Modules (LSM) (2)



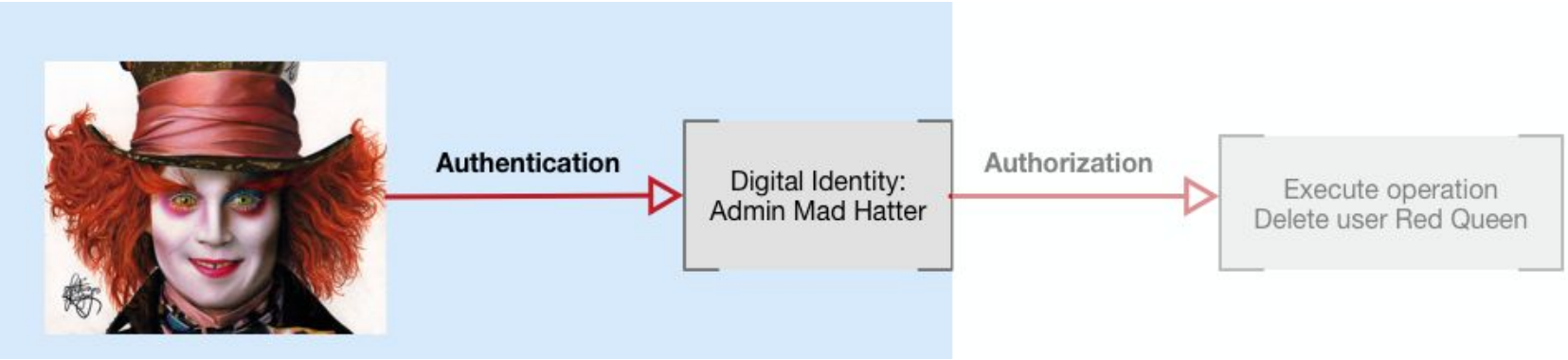
MAC pros and cons

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- ✓ **Addresses key vulnerability issues of DAC**
- ✗ **Too restrictive**
  - Prevent people from achieving legitimate tasks
  - Arguably does not apply to SELinux's targeted mode
- ✗ **Information leakage still possible via covert channels (timing, storage, …)**
  - MAC restricted usability without getting the benefit
  - Example: database files storing tables have the clearance *secret*, but the meta-data about these files is *unclassified*, because it does not contain real confidential information. User A with label unclassified can infer a **pattern** of changes to data, even though it cannot read the actual data
- ● **MAC tried to evolve to information flow control (IFC)**
  - Generalization for commercial purposes - to be covered later in course

Outline

- Access control
- **User authentication using passwords**
- Kerberos
- Multi-factor authentication
- LDAP
- User training



Authentication

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

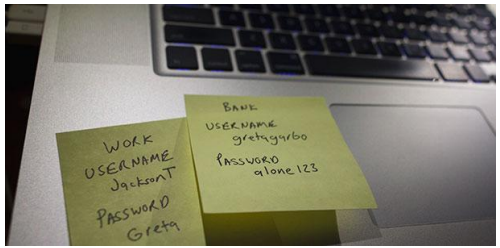
- **Procedure by which an entity establishes claimed relationship property to another entity**
  - User authentication
  - Server authentication
  - Mutual authentication

“The password is dead”...

- “*They just don’t meet the challenge for anything you really want to secure*” (B. Gates, 2004)
- Within 5 years “*You’ll never need a password again*” (IBM, 2011)
- “*Passwords are done at Google*” (H. Adkins, manager of Information Security at Google, 2013)
- **Arguably passwords still the main form of authentication on the web**
- “*No other single technology matches their combination of cost, immediacy and convenience*” (C. Herley, P. van Oorschot, 2015)

Password habits (1)

- **Users are difficult to model**
  - Use same / similar passwords for different accounts
  - Prefer passwords with low entropy, because they are easier to remember
  - What are the dangers of the two points above? (hint: previous lecture)
- **Typically at least one uppercase and one non-alphabetic character**
  - But users may insert these characters in predictable places: (e.g., F1rst)
- **Users reuse passwords when prompted to periodically change them**
  - Predictable changes (s becomes $, add sequences at the end 1, 2, 3)
- **Users write them down**



BRIAN BARRETT SECURITY 03.10.16 7:00 AM

WANT SAFER PASSWORDS? DON'T CHANGE THEM SO OFTEN

Figures from D. Florêncio and C. Herley. A large-scale study of web password habits. 16th International Conference on the World Wide Web (WWW), 2007.

Password habits (2)

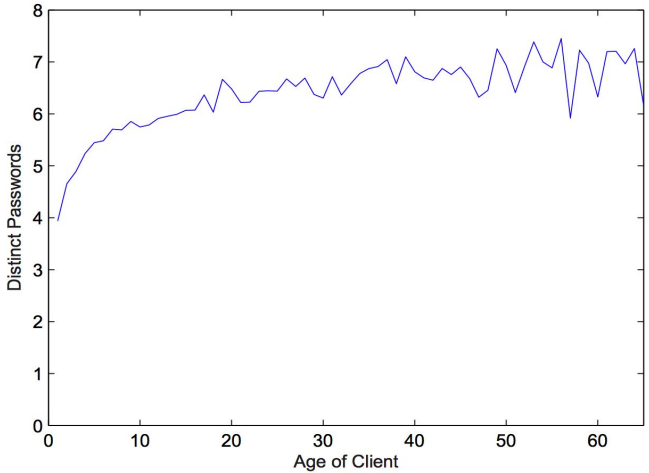


Figure 2: Number of distinct passwords used by a client *vs.* age of client in days. The average client appears to have about 7 passwords that are shared, and 5 of them have been re-used at least once within 3 days of installing the client.

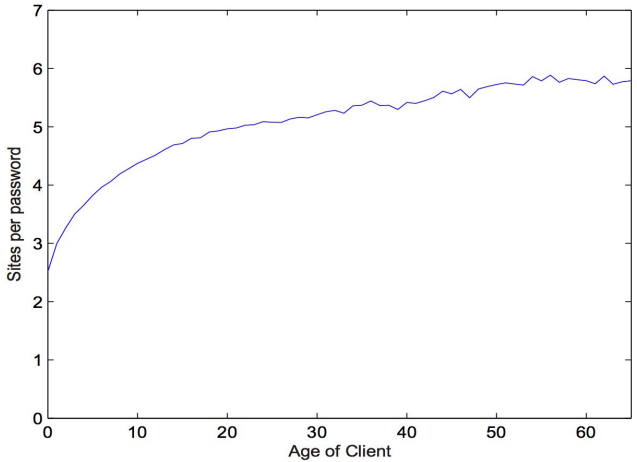


Figure 3: Number of sites per password *vs.* age of client in days. The average password appears to be used at about 6 different sites.

Figures from D. Florêncio and C. Herley. A large-scale study of web password habits. 16th International Conference on the World Wide Web (WWW), 2007.

Password habits (3)

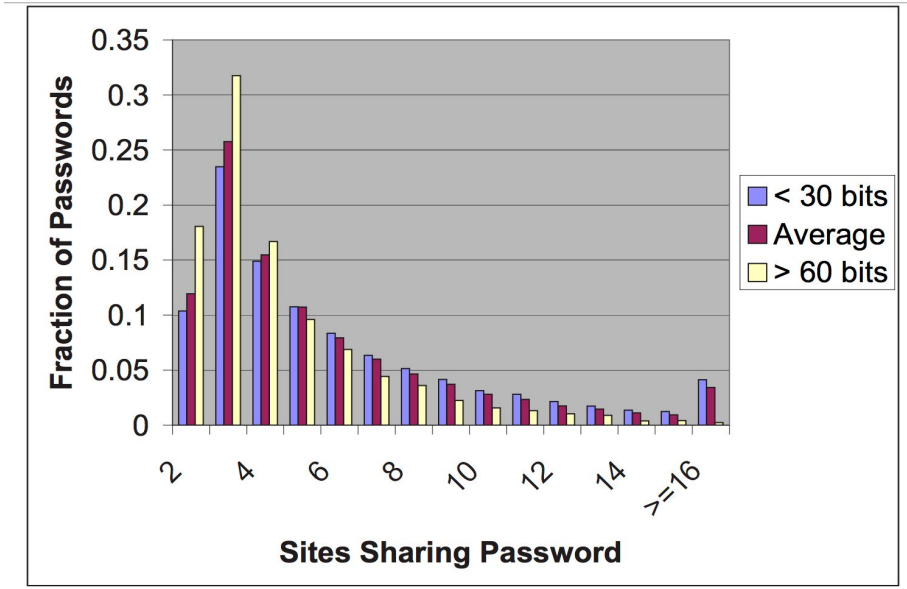
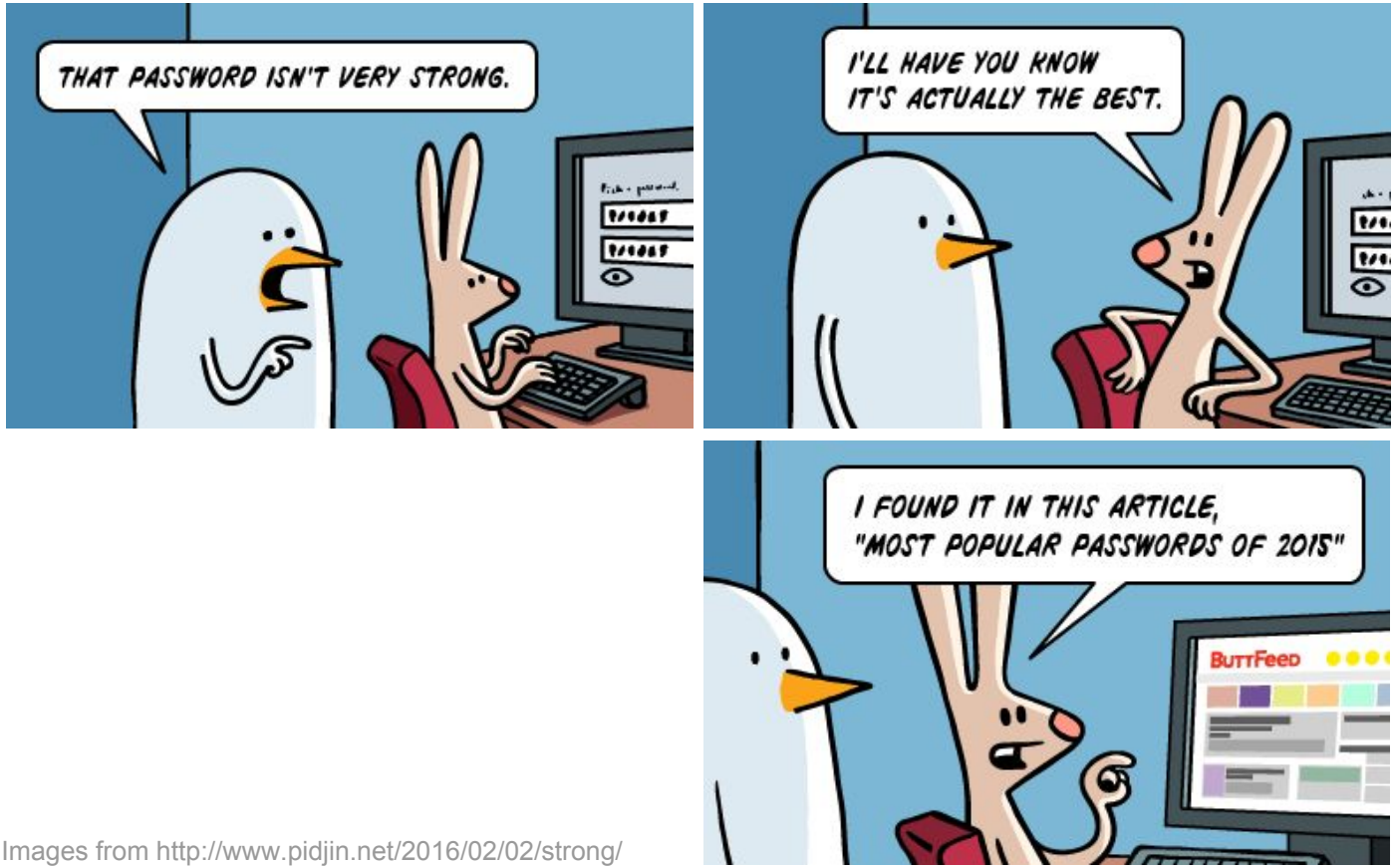


Figure 4: Fraction of the number of sites that share a password for weak passwords (bitstrength < 30 bits), strong passwords (> 60 bits) and the overall average. Observe that weaker passwords tend to be shared at more sites, and stronger ones at fewer.

Figures from D. Florêncio and C. Herley. A large-scale study of web password habits. 16th International Conference on the World Wide Web (WWW), 2007.

A good password



Images from http://www.pidjin.net/2016/02/02/strong/

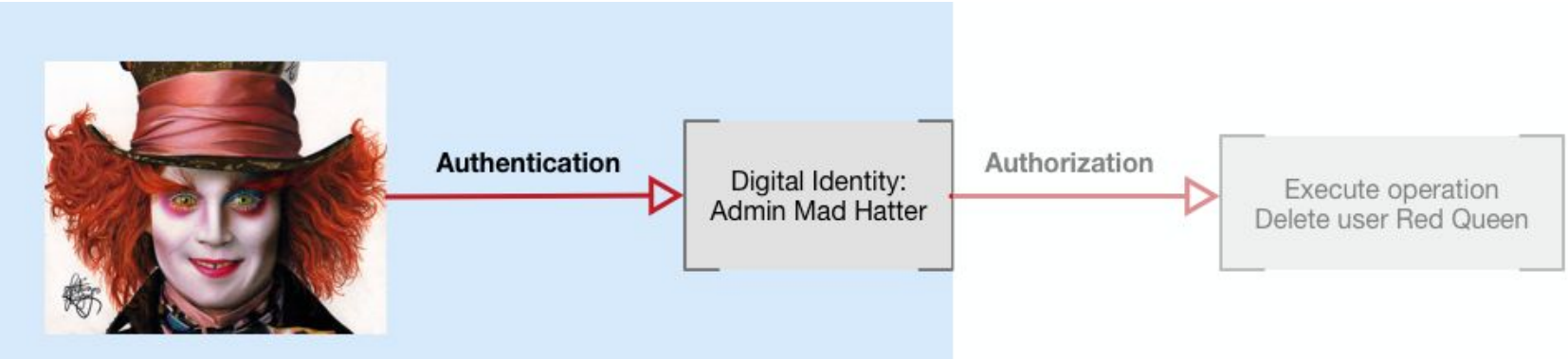
Even very strong passwords are at risk

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- **Passwords are essentially login tokens that can be replayed**
- **An attacker can:**
  - Steal passwords using client-side malware
  - Password-crack a stolen server-side database (covered earlier)
  - Phish passwords using a spoofed site
  - Eavesdrop the password

Outline

- Access control
- User authentication using passwords
- **Kerberos**
- Multi-factor authentication
- LDAP
- User training



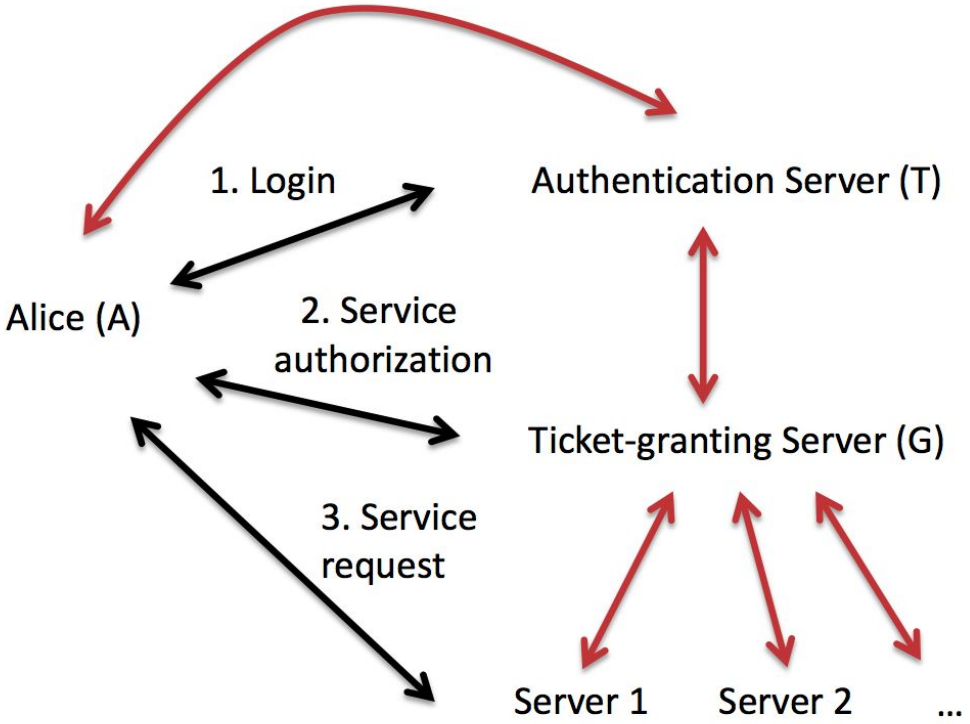
Kerberos

created before public key crypto was so used, hence uses symmetric key only

- **MIT late 80's**
- **Clients use session tickets to access services**
- **Authentication server (T)**
  - Shares keys with users, e.g., based on user's password
- **Ticket-granting server (G)**
  - Issues tickets to clients, which clients show to the server when requesting service
  - Tickets prove the client is authenticated
  - Tickets carry a client-server session key

Both servers can be the same, but often two different servers are used. It's more of an architectural separation.

Kerberos architecture



msg exchange

shared key

1. Alice contacts (T) and proves that it's really Alice

2. Alice is granted a ticket (based on a symmetric secret key). Both authentication server and ticket-granting server know the symm secret key. This ticket granted is the ticket-granting ticket (sort of a meta-ticket)

3. Alice uses the meta-ticket to ask for service authorization. (T) checks if somebody is really Alice, while (G) believes that that's Alice and decides whether to grant service authorization or not (and gives a ticket when granting the service).

4. After Alice gets the ticket for a service,it can access the server with that service (server 1, server 2, ...)

Kerberos advantages

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- **Distributed access control**
  - No password communicated in cleartext over the network (earlier protocols did)
- **Cryptographic protection against spoofing**
  - All accesses mediated by ticket-granting service
- **Limited period of validity**
  - Tickets have a validity period, which servers check
  - Limits window of vulnerability
  - Timestamp prevents replay attacks
- **Mutual authentication**
  - User sends nonces as challenges

Kerberos disadvantages

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

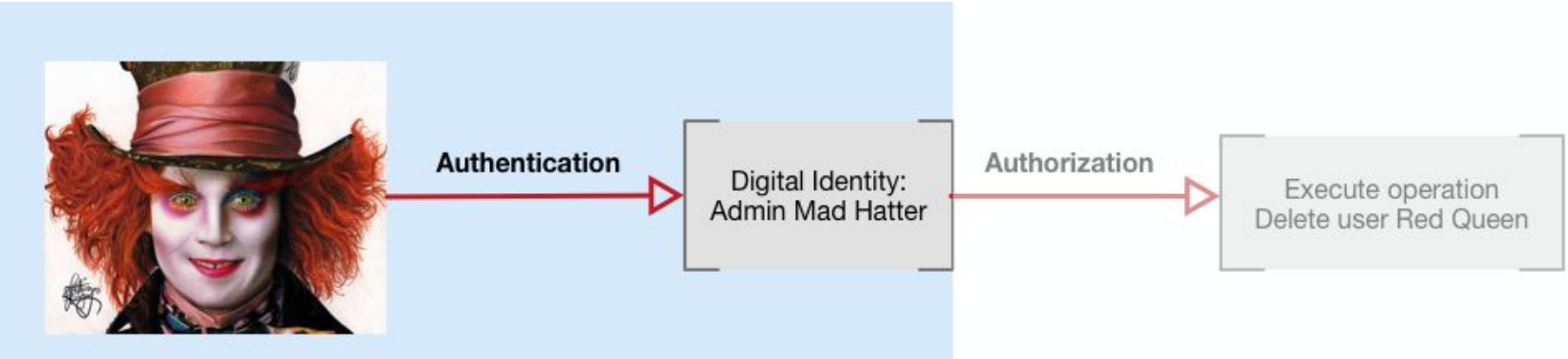
- **Ticket-granting server**
  - Single point of failure or compromise
  - Performance bottleneck
- **Requires at least roughly-synchronized clocks**
  - All accesses mediated by ticket-granting service

otherw. you can have problemd due to tickets having "expired"

- **Ticket replay possible during validity period**
- **Password used at the beginning is a weak spot**
  - User host can save it and then replay it

Outline

- Access control
- User authentication using passwords
- Kerberos
- **Multi-factor authentication**
- LDAP
- User training



Multi-factor authentication (MFA)

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- **User granted access after presenting several separate pieces of information to authentication mechanism**


Knowledge (smth you know)


Biometrics (smth you are)


Possession (smth you have)

- **Two-factor authentication (2FA)**
  - Use two of the three classes above

Scenarios

- **What authentication factors are used in the following?**

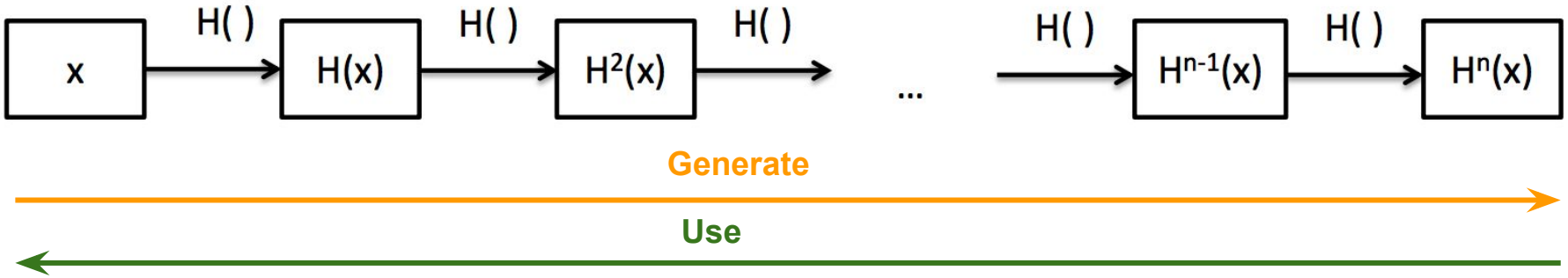
Right figure: Quick and easy boarding at Schiphol airport (https://www.internationalairportreview.com/news/31734/amsterdam-schiphol-facial-recognition/)

Authentication factors

- **Something you know**
  - PIN, Password, passphrase - as discussed earlier
- **Something you have**
  - Secure token (or similar) to generate a one-time password
  - Key embedded in a secure area on host machine, browser software
  - Smartcard

One-time password - Lamport (1)

- **Cannot impersonate user through eavesdropping or server compromise**
- **Based on hash chains**



One-time password - Lamport (2)

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- **Client stores x, server stores $t = H^n(x)$**
- **Authentication**
  - Server sends n
  - Client computes $y = H^{n-1}(x)$ and sends it to server
  - Server check that $H(y) == t$
- **Eavesdropping ineffective**
  - Eve observes $H^{n-i}(x)$ in round i
  - Round i+1 requires $H^{n-i11}(x)$, which Eve cannot compute from $H^{n-i}(x)$
  - What property of hash chains do we use?
- **Small n attack**
  - Eve impersonates server, sends small n = 100
  - Alice replies $H^{99}(x)$. Eve can impersonate Alice for $m \geq 100$

Biometrics

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- **Motivation**
  - Something you know could be guessed
  - Something you own could be stolen
  - Nothing to remember, nothing to share
- **Behavioral**
  - Speech
  - Keystroke timing
- **Physiological**
  - Iris
  - Fingerprint
  - Face / voice recognition

Slide adapted from Information Security course at ETH, ©Srdjan Capkun

Biometrics authentication process

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

- **Registration**
  - Acquisition
  - Creation of master characteristics
  - Storage of master characteristics
- **Authentication**
  - Acquisition
  - Comparison
  - Decision

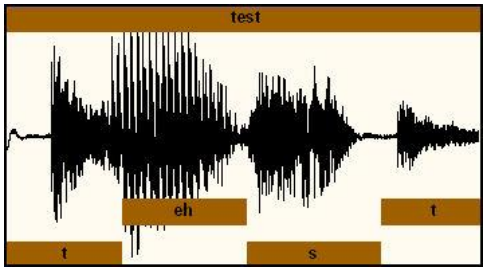
Fingerprint recognition

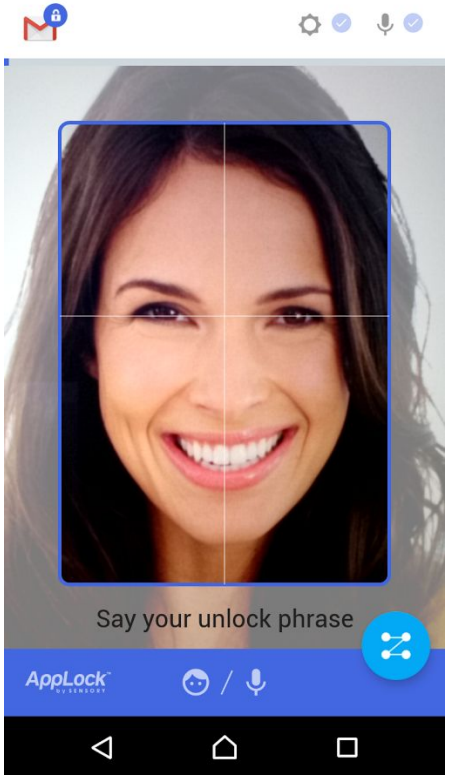
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- **Through contact**
- **Inaccuracies**
  - Dirt
  - Wounds
  - Moisture
- **Issues**
  - Can be cloned
  - Play-Doh fingers can fool fingerprint scanners

Voice recognition

- **Speech input**
  - Cadence
  - Frequency
  - Duration
- **Issues**
  - Environmental noise
  - Having a cold
  - Lossy transformation from analog to digital
  - Same person has different accents in different languages

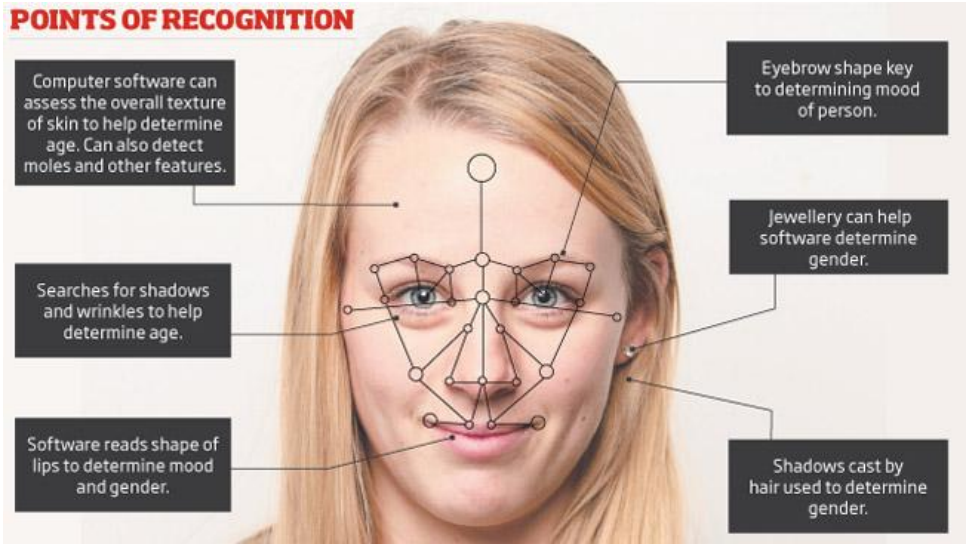




Slide adapted from Information Security course at ETH, ©Srdjan Capkun

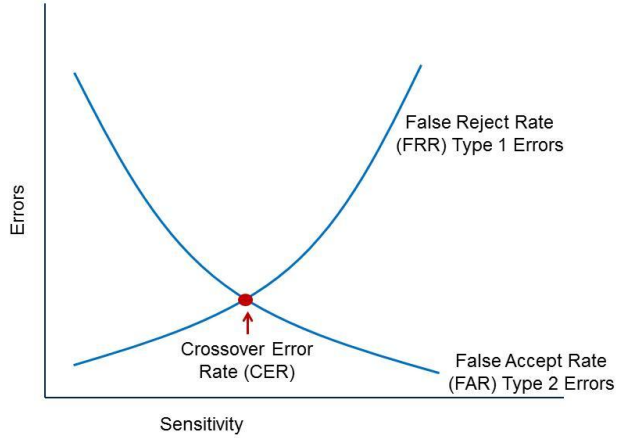
Face recognition

- **Software assesses**
  - Age
  - Gender
  - Mood
- **Software identifies**
  - Special features, e.g., moles



Biometrics errors

- **False accept rate (FAR)**
- **False reject rate (FRR)**
- **Higher sensitivity is not always better**
  - **Company needs to decide what makes most sense for its scenarios**



Outline

- Access control
- User authentication using passwords
- Kerberos
- Multi-factor authentication
- **LDAP**
- User training

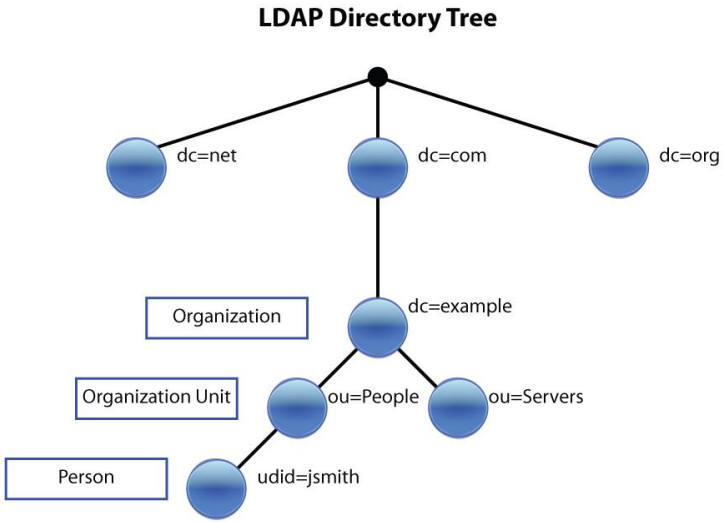
Lightweight directory access protocol (LDAP)

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

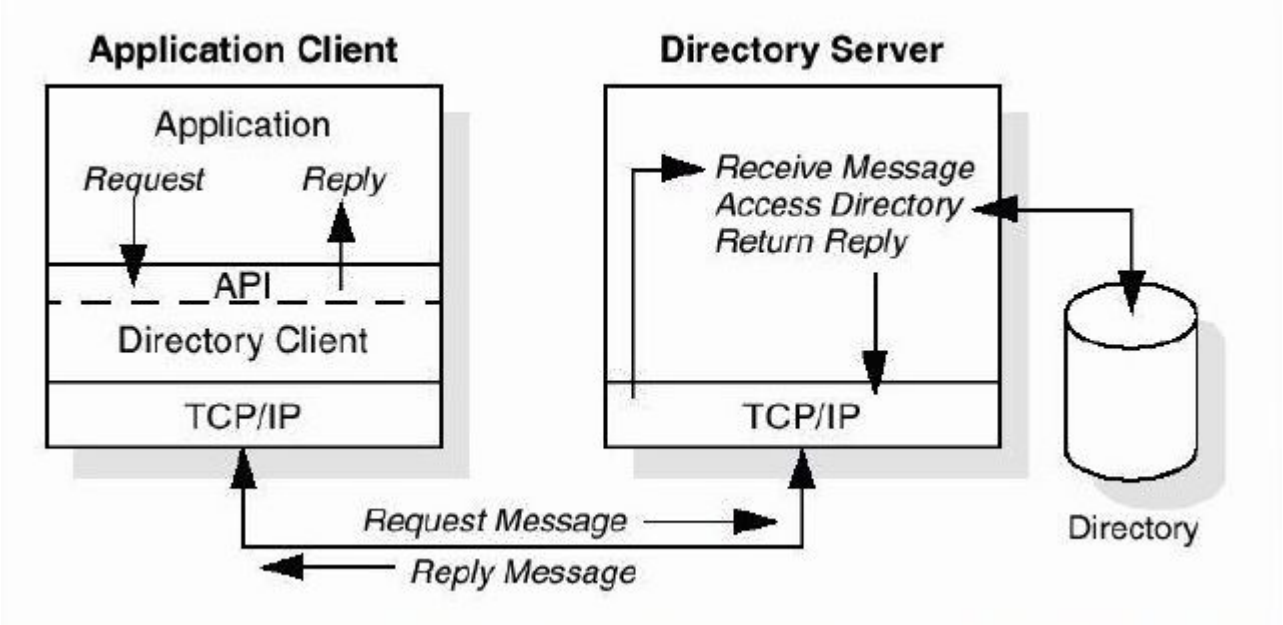
- **Standard for accessing a corporate repository for commonly-used information**
  - Many RFCs specify parts of LDAP
  - Information stored hierarchically
  - Allows to represent objects (users, groups, organizational units, network objects, printers, etc)
  - Allows representation of object attributes (text, binary data, lists, etc)
- **Optimized for reads and searches**
  - Allows queries to find resources, e.g., find server that has access to employee records
- **Runs on top of TCP/IP**
- **Secure communication using TLS and X.509 certificates**

LDAP information storage

- **Data stored in entries that are tree nodes**
  - Format compatible with X.500
  - Information accessed through LDAP URL: `ldap://ds.example.com:389 (scheme://url:port)`

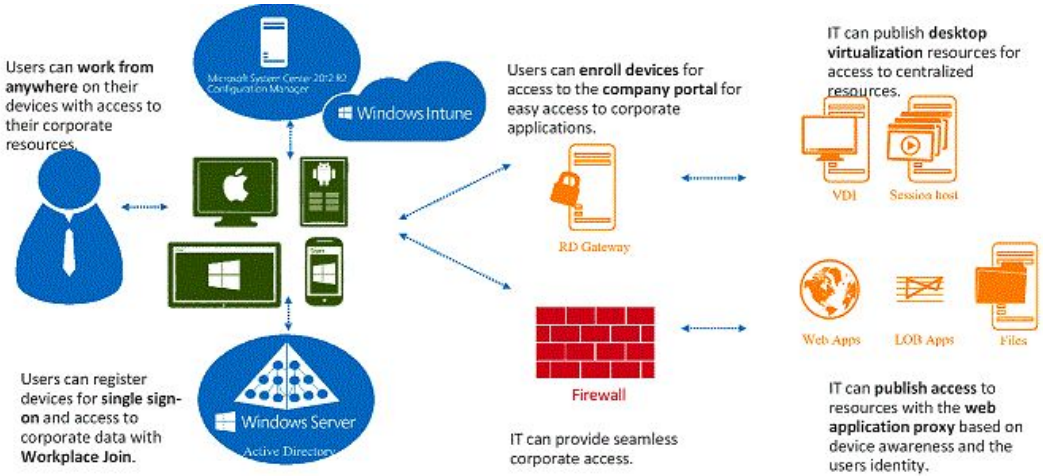


LDAP client-server interaction



LDAP usage (1)

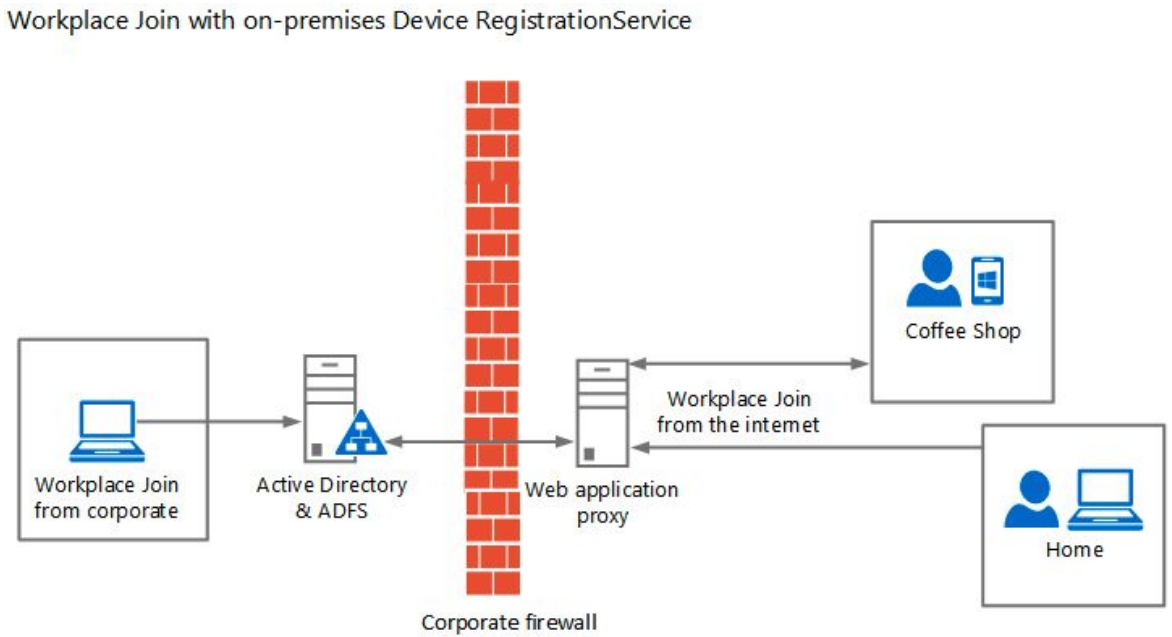
- **Store users and access authorization (e.g., use for RBAC)**
- **Implementation example:** Microsoft Active Directory
- **Scenario**
  - Medium-sized banking firm, >5000 employes who bring their own devices (PC and mobile)
  - Goal: users can access corporate apps and data on these devices, according to their needs
  - Company can identify and manage devices



Scenario (and subscenarios) and images from https://technet.microsoft.com/en-us/library/dn550982(v=ws.11).aspx

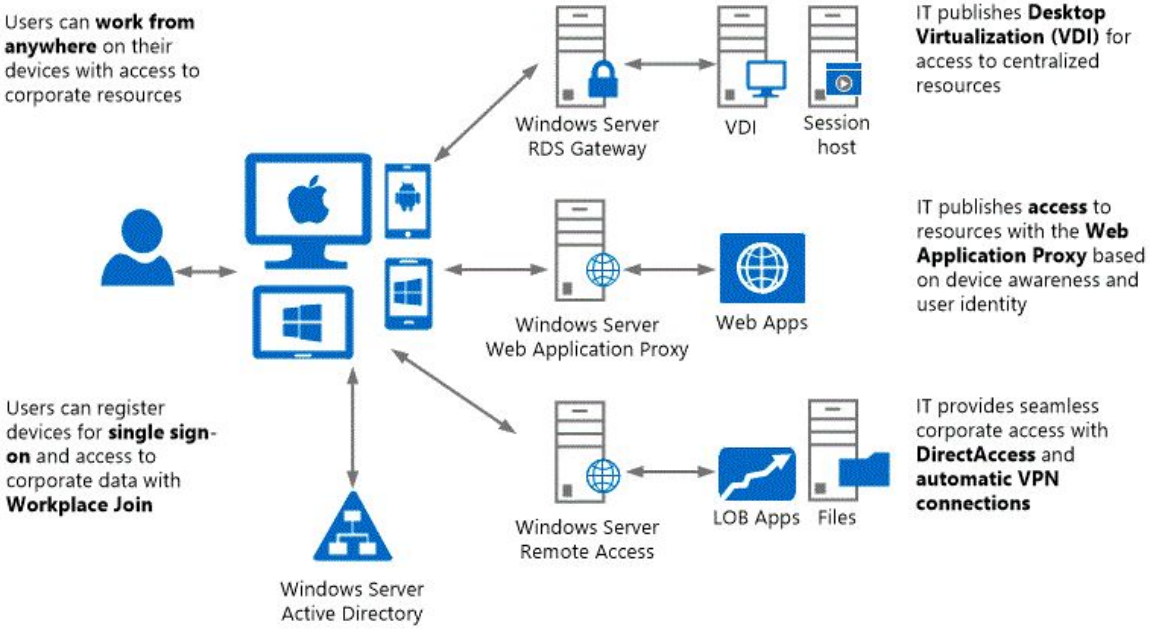
LDAP usage (2)

- **Sub-scenario 1**
  - Enable users to register devices
  - Enable users to have a single sign-on experience



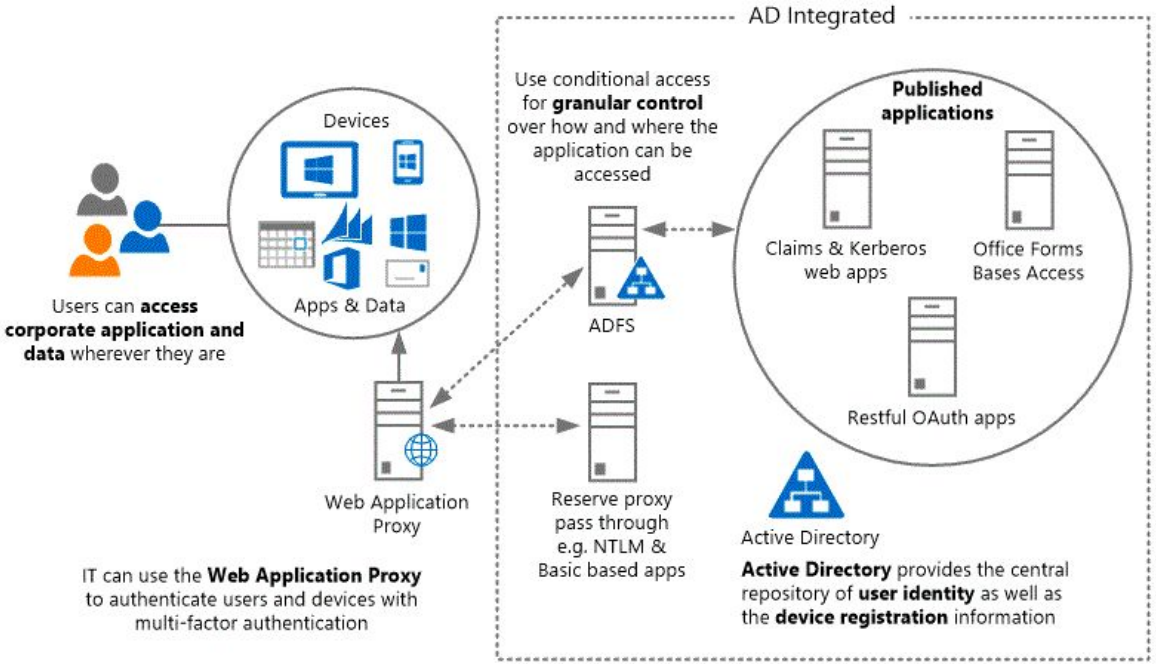
LDAP usage (3)

- **Sub-scenario 2**
  - Enable users to set up seamless access to corporate resources



LDAP usage (4)

- **Sub-scenario 3**
  - Active Directory enhancements for improving access control risk mitigation



LDAP food for thought

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

- **Where should the LDAP server be located inside the company network?**
- **Where should each component in the scenarios be located and why?**

Outline

- Access control
- User authentication using passwords
- Kerberos
- Multi-factor authentication
- LDAP
- **User training**

Staying safe online: experts vs non-experts

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- **Common: careful password management**
  - 24% of non-experts use password managers for some of their accounts vs 73% of experts
  - “I try to remember my password because no one can hack my mind” (non-expert)
- **Software updates**
  - 35% of experts vs 2% of non-experts
  - “Patch, patch, patch,” (expert)
  - “What if I download malicious update?” (non-expert)
- **Antivirus software**
  - 42% of non-experts vs. 7% of experts
  - “Gives false sense of bulletproof security” (expert)

Src https://security.googleblog.com/2015/07/new-research-comparing-how-security.html

Best practices

- **BYOD training**
  - Data ownership: personal vs corporate e-mail / contacts / data
  - Define BYOD for the organisation
  - Supported devices
  - Security policies: device loss / theft, passwords
- **Do not connect random devices to company network**

Security

Half of people plug in USB drives they find in the parking lot

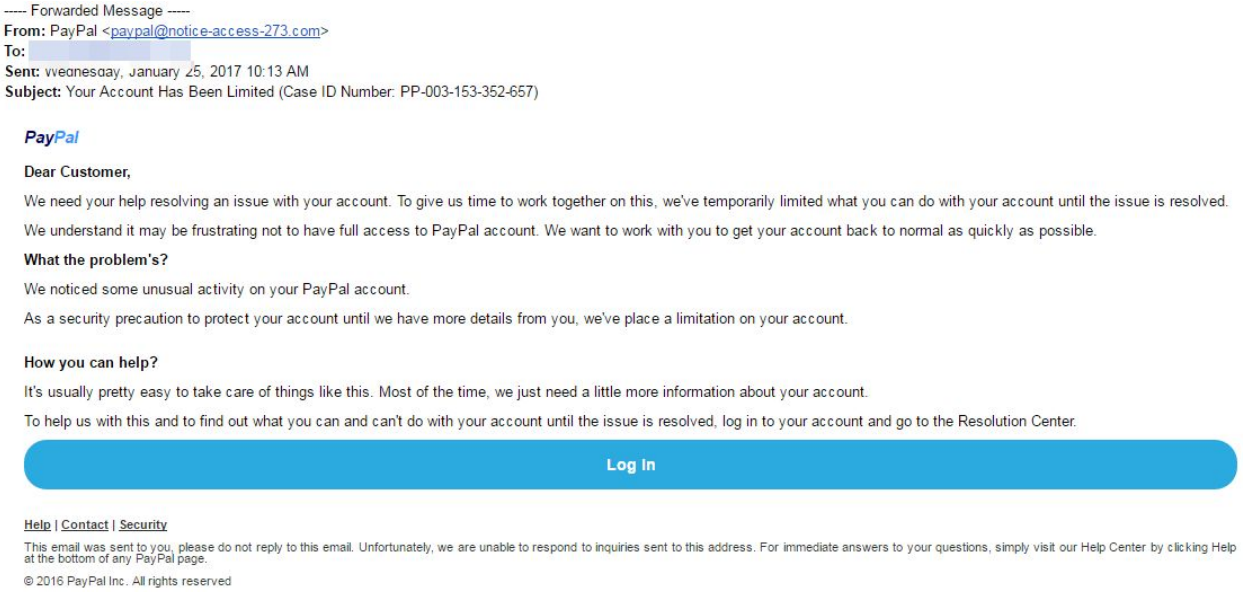
Why do we even bother with security software?

11 Apr 2016 at 21:09, Shaun Nichols

Phishing

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

- **Over the phone**
- **Over e-mail (attachment, link) - some are very sophisticated**



----- Forwarded Message -----
From: PayPal <paypal@notice-access-273.com>
To:
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Log In

Help | Contact | Security

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

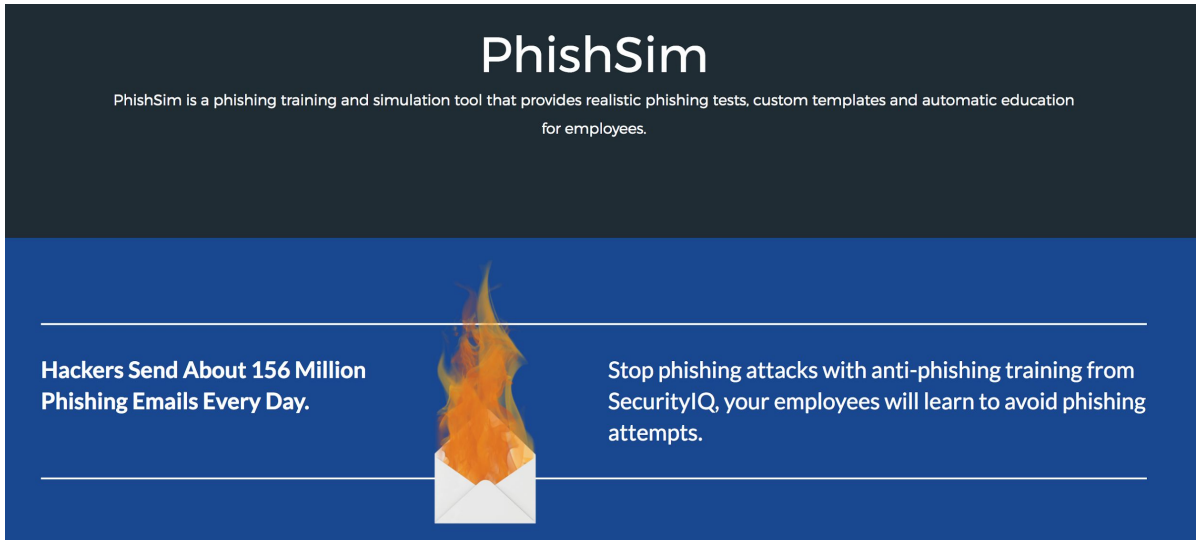
An example of phishing attack

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

- **Goal: Stealing bank credentials of users**
- **Steps**
  - Hijack the DNS server the users connect to
  - Change the IP address the URL of the bank resolves to
  - Built a website clone
  - Send phishing e-mail with a legitimate looking link, but which will resolve to attacker's IP address

Employee training

- **Companies periodically run employee training**
- **Services for employee training**



Conclusion

Important to understand how users interact with security-critical systems

- Tradeoffs in access control mechanisms: RBAC, DAC, MAC
- Authentication versus authorization
- Common network access technologies: Kerberos, LDAP, Active Directory