

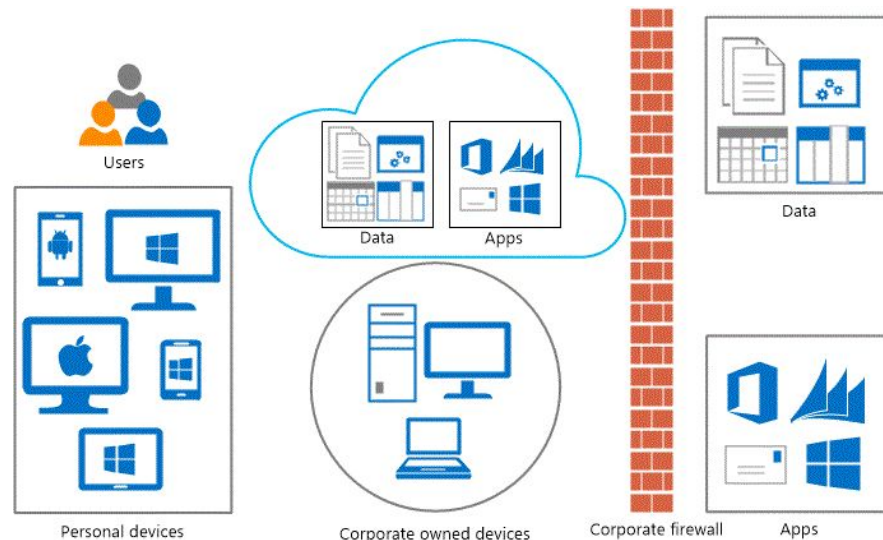
User and Access Management

COM-402: Information Security and Privacy

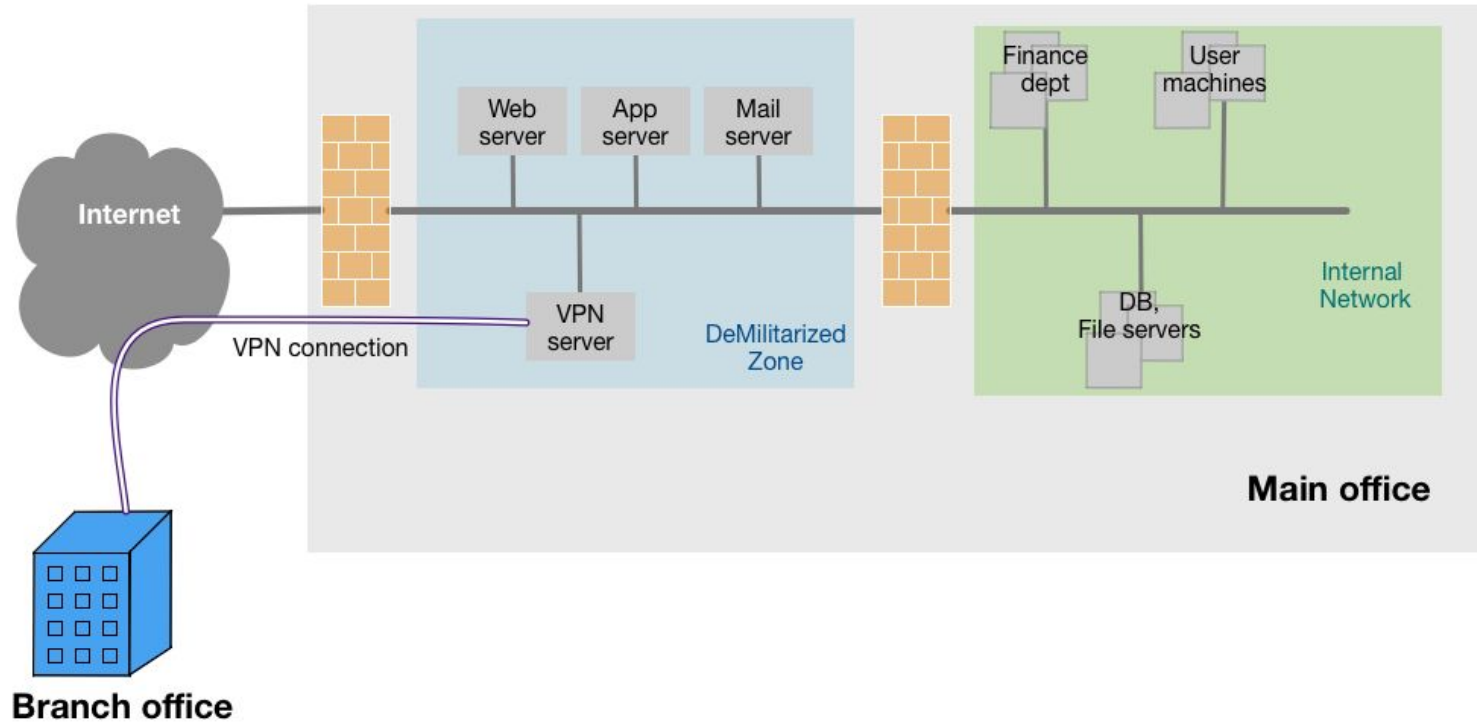
(slide credits: Cristina Basescu)

Users vs Company Resources

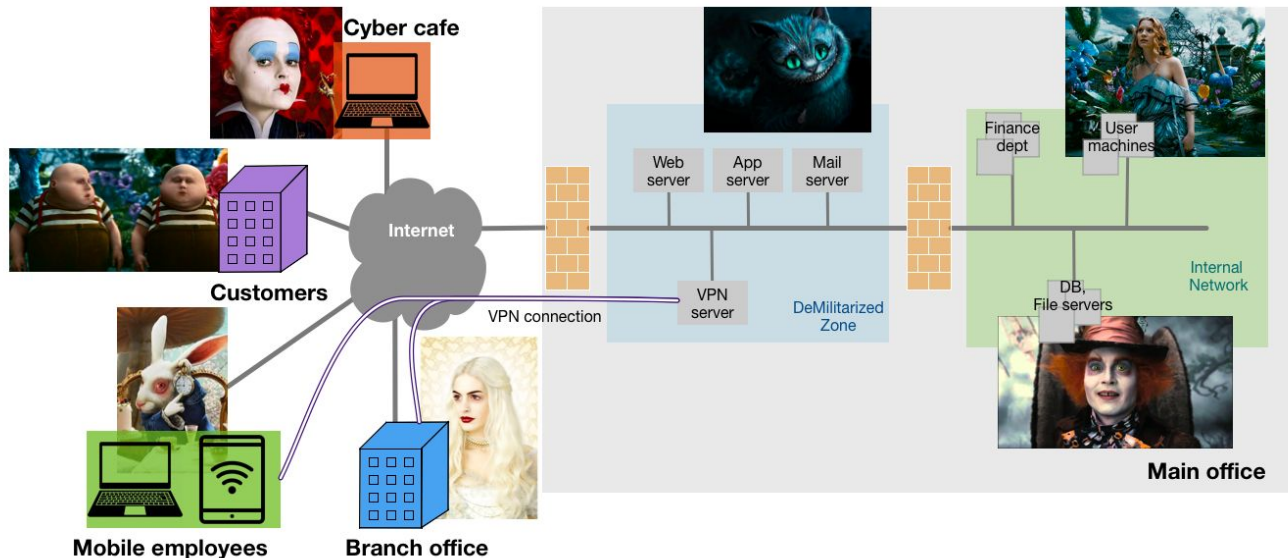
- Company resources
 - Located on premises or in the cloud
 - Servers, workstations, data, applications
- Users access company resources
 - On premises through corporate-owned / personal devices
 - From outside the company's network through corporate-owned / personal devices



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?



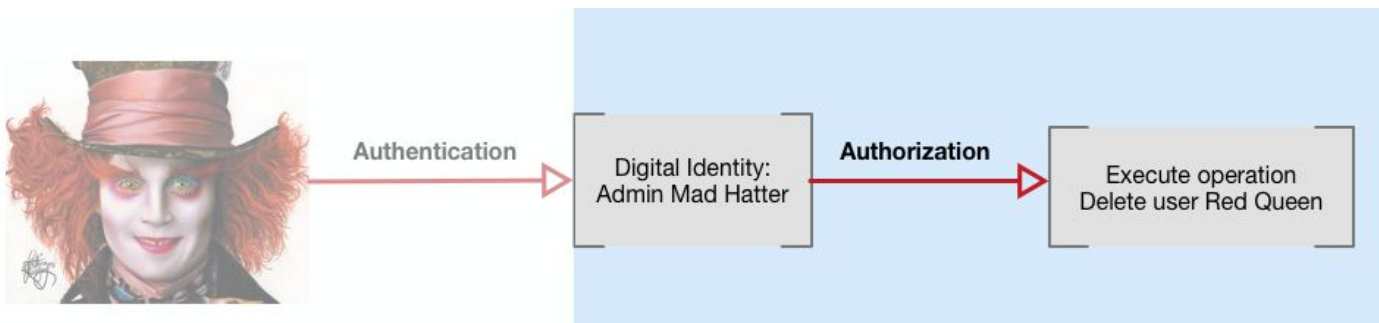
Outline

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



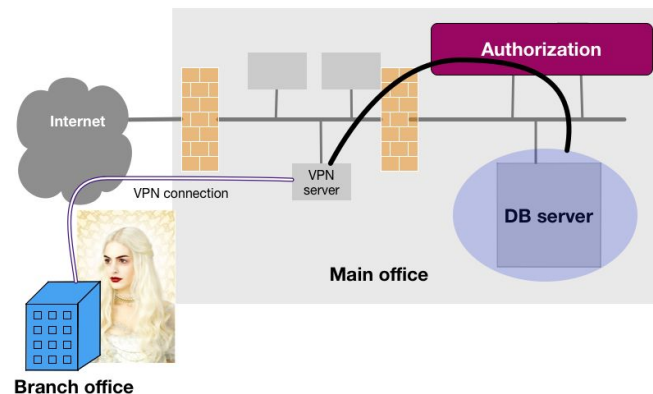
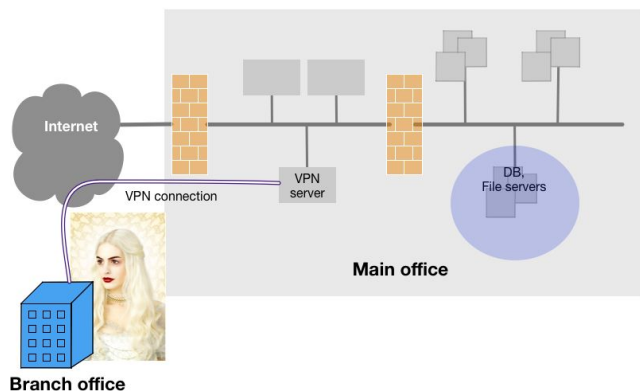
Access Control

- 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)
- 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

- 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)
 - 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:

- Role-based Access Control (RBAC)
- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)

Role-based Access Control (RBAC) (1)

- Standardized by NIST since 1992 (latest in 2012: INCITS 359-2012)
- Centered on **user roles**
 - A role can contain multiple permissions



Subjects

Many to many mapping

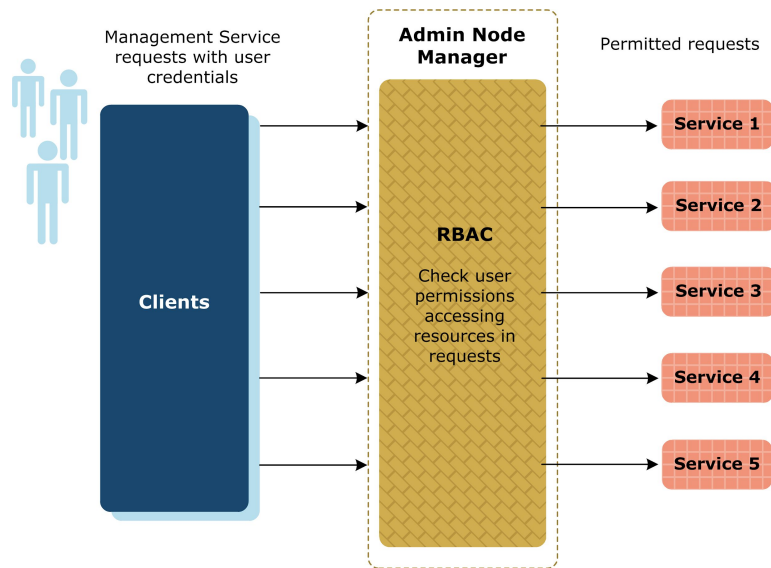
	Navigate Pages	Draw / Markup	Import Content Sync Rights	Delete Pages & other user's content	Permission Controls	View Room Settings
★ Owner	✓	✓	✓	✓	✓	✓
★ Moderator	✓	✓	✓	✓	✓	
✎ Collaborator	✓	✓	✓			
✎ Reviewer	✓	✓				
👁 Viewer	✓*					

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

Roles

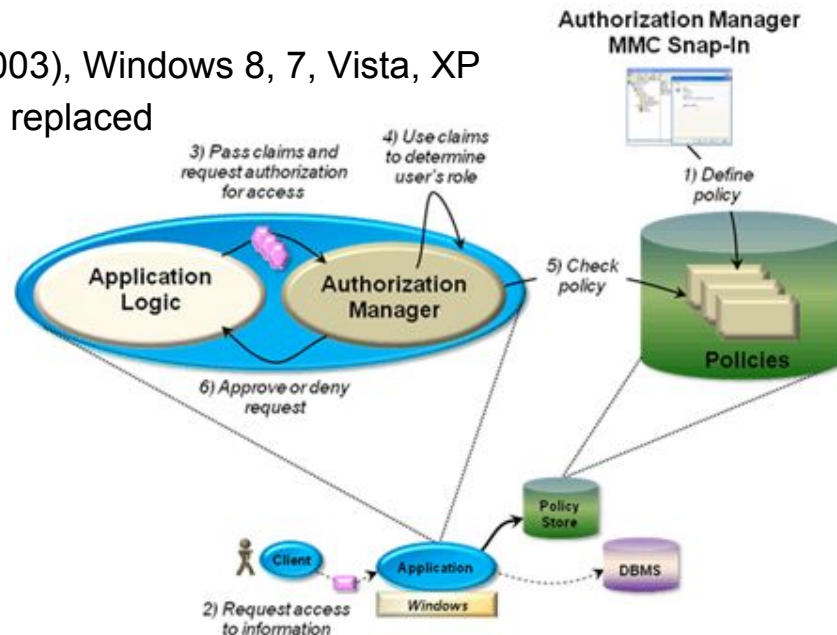
Role-based Access Control (RBAC) (2)

- RBAC for user management within the company



RBAC in Windows

- 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



Advantages of RBAC

- ✓ 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

Disadvantages of RBAC

- × 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

Discretionary Access Control (DAC)

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

- 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

ACL vs Capabilities

Capability	ACL
✗ Instant revocation hard	✓ 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

DAC in Unix (1)

- 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`
- ACL representation compressed to 9 bits
 - 3 groups of R,W,X bits, each group then converted to base 10
 - Example: 754 means `rwx | r-x | r`

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

DAC in Unix (2)

- 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

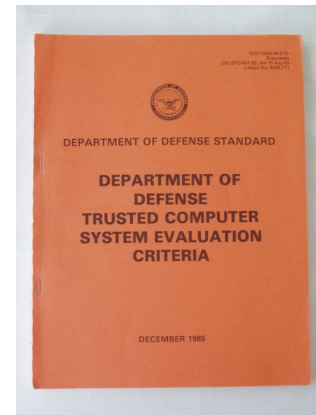
✗ Disadvantages

- 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:
 - D only readable by A
 - B sends trojan to A so when run by A, reads D and writes it under D'
 - D' is readable by B

Mandatory Access Control (MAC)

Tries to ensure that even someone with access **cannot leak the data**

- Historically associated with military-grade information security
 - **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
- Security policy:
 - Subject can access object only if subject's label has a higher or equal label compared to object's label
- Can be used in conjunction with DAC or RBAC
 - **DO NOT** confuse with message authentication codes!



MAC Security Labels

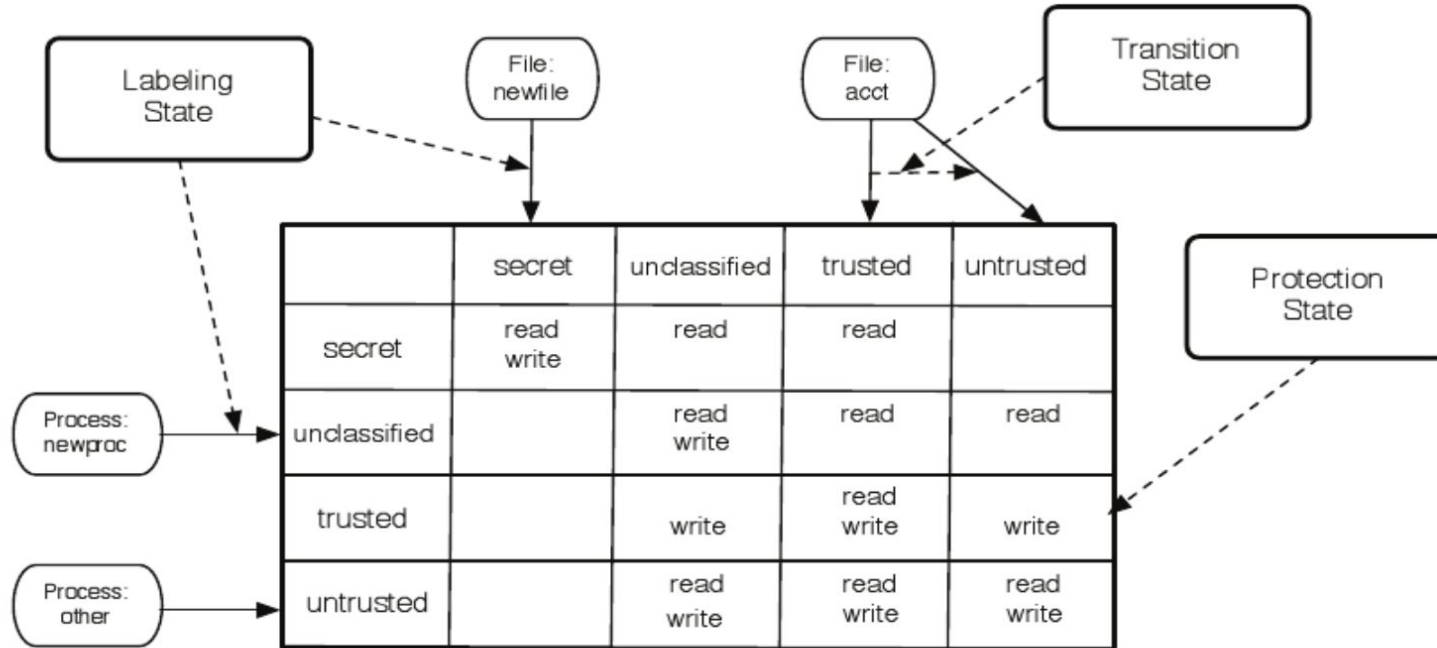
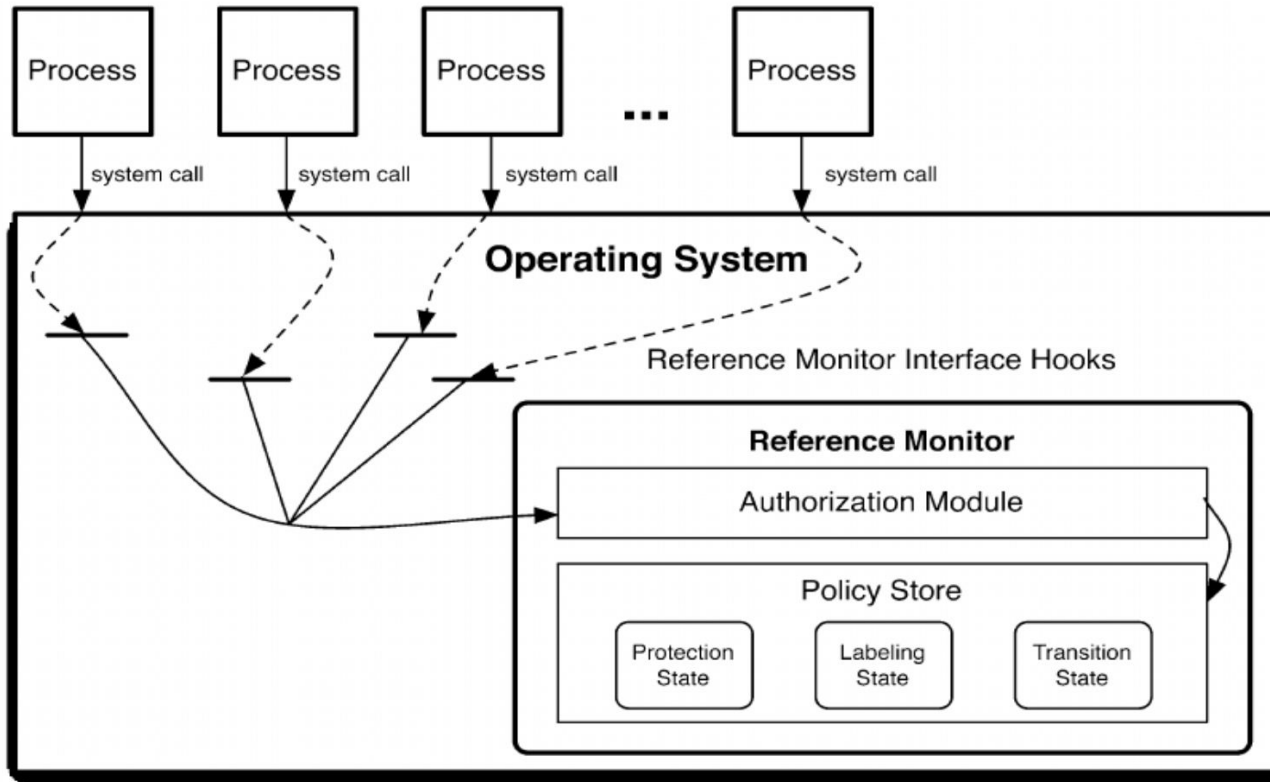


Figure 2.2: A Mandatory Protection System: The *protection state* is defined in terms of labels and is immutable. The immutable *labeling state* and *transition state* enable the definition and management of labels for system subjects and objects.

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)



Reference Monitor (2)

- 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

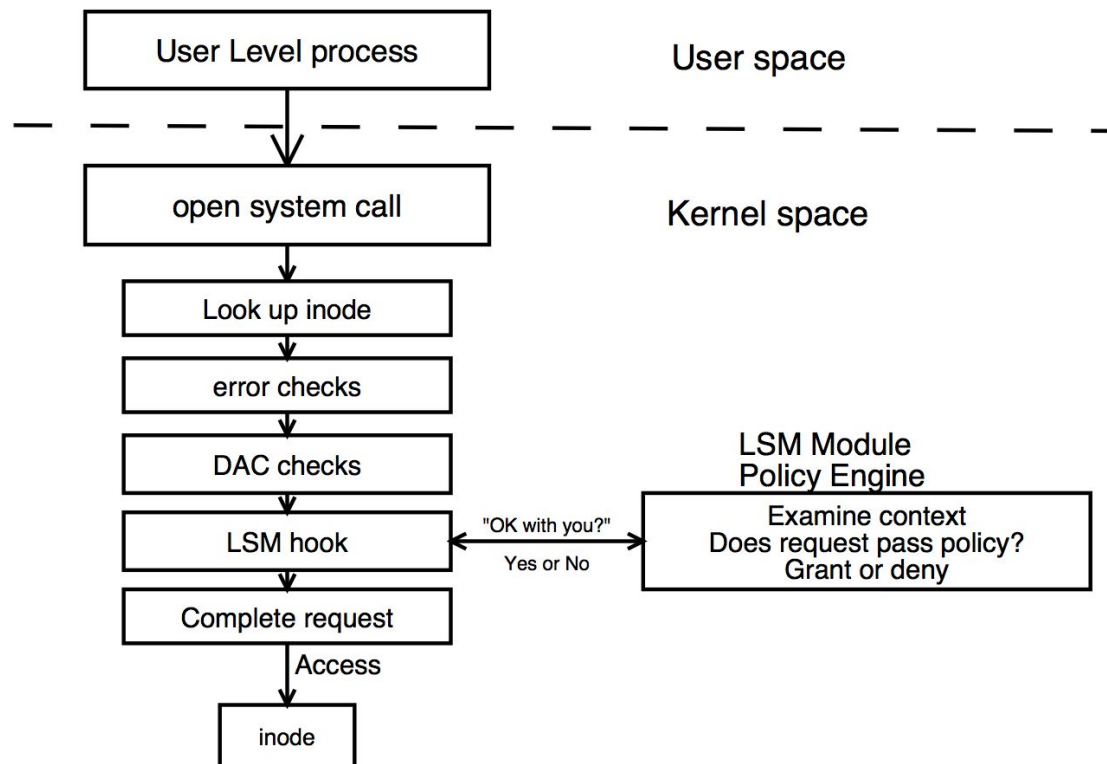
Linux Security Modules (LSM) (1)

- 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

Linux Security Modules (LSM) (2)

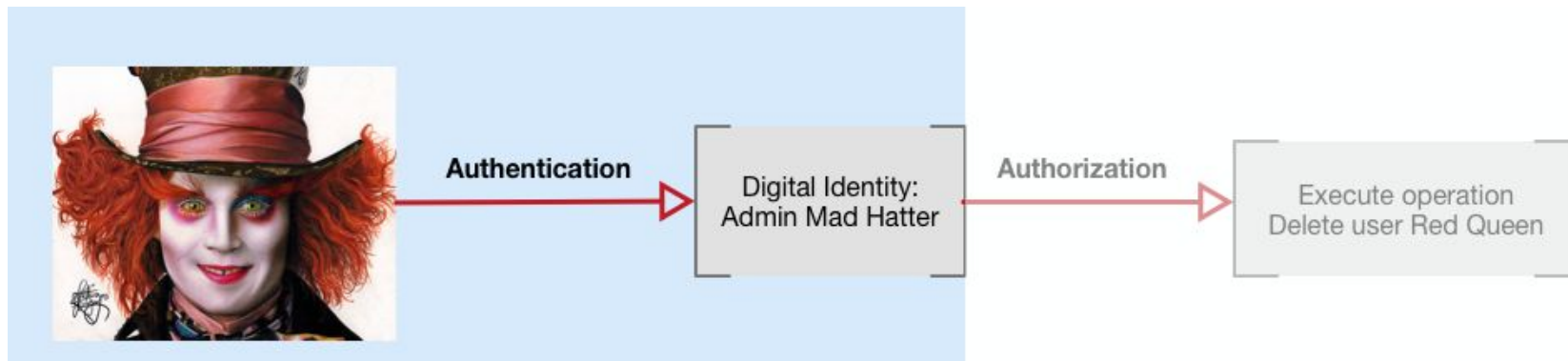


MAC Pros and Cons

- ✓ 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 metadata 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 has tried to evolve into **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

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

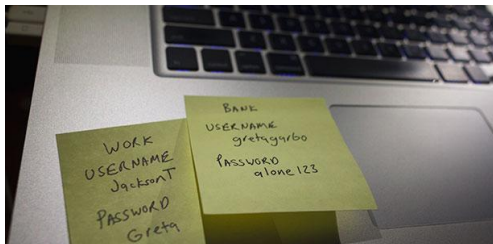
“The password is dead”...

- *“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**

Password Habits (2)

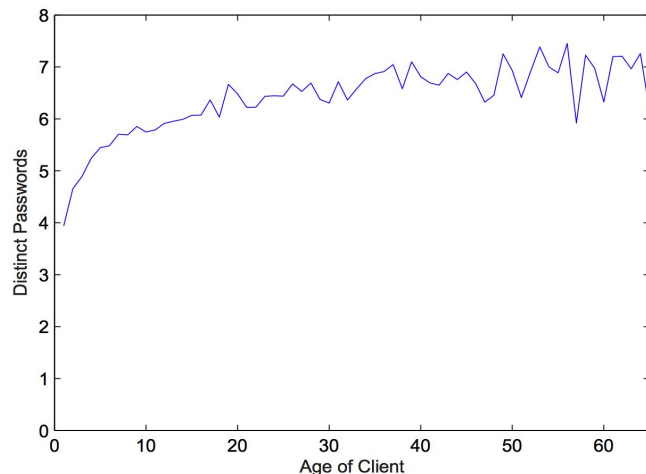


Figure 2: Number of distinct passwords used by a client *vs.* age of client in days. The average client appears to have about 7 passwords that are shared, and 5 of them have been re-used at least once within 3 days of installing the client.

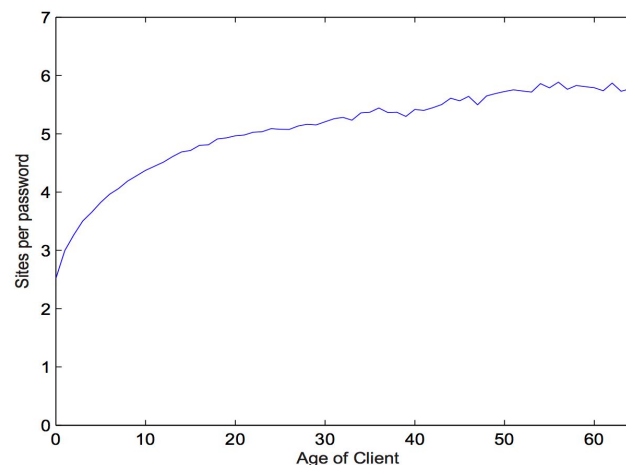


Figure 3: Number of sites per password *vs.* age of client in days. The average password appears to be used at about 6 different sites.

Password Habits (3)

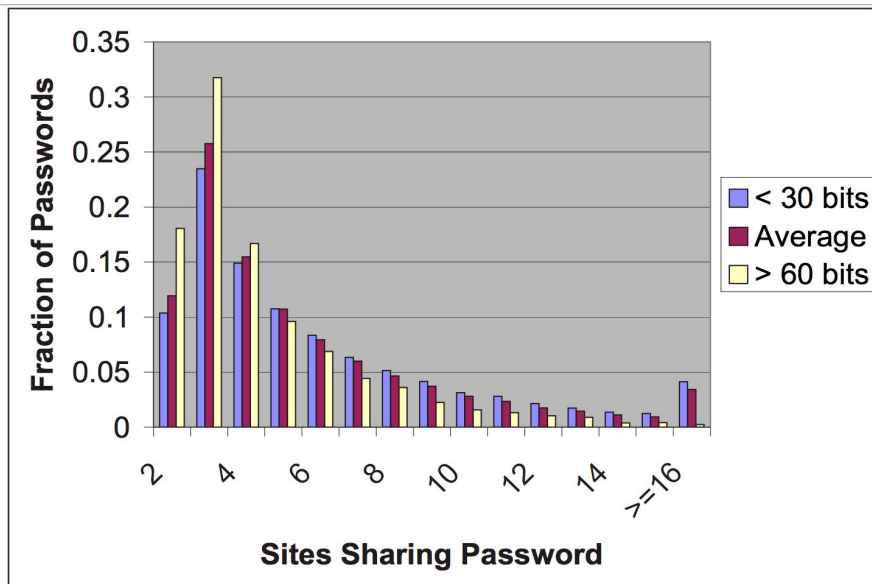
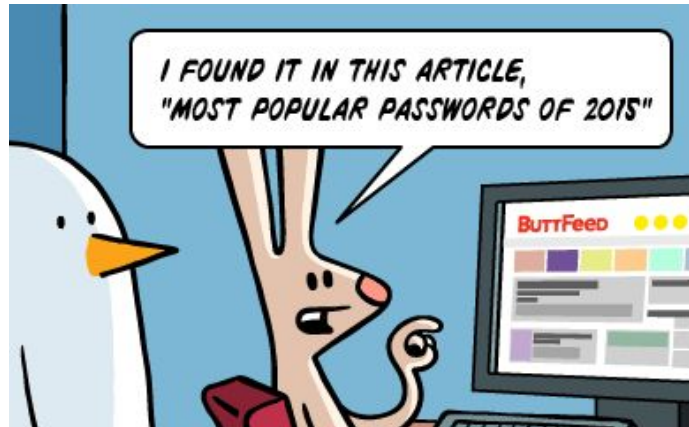


Figure 4: Fraction of the number of sites that share a password for weak passwords (bitstrength < 30 bits), strong passwords (> 60 bits) and the overall average. Observe that weaker passwords tend to be shared at more sites, and stronger ones at fewer.

A Good Password

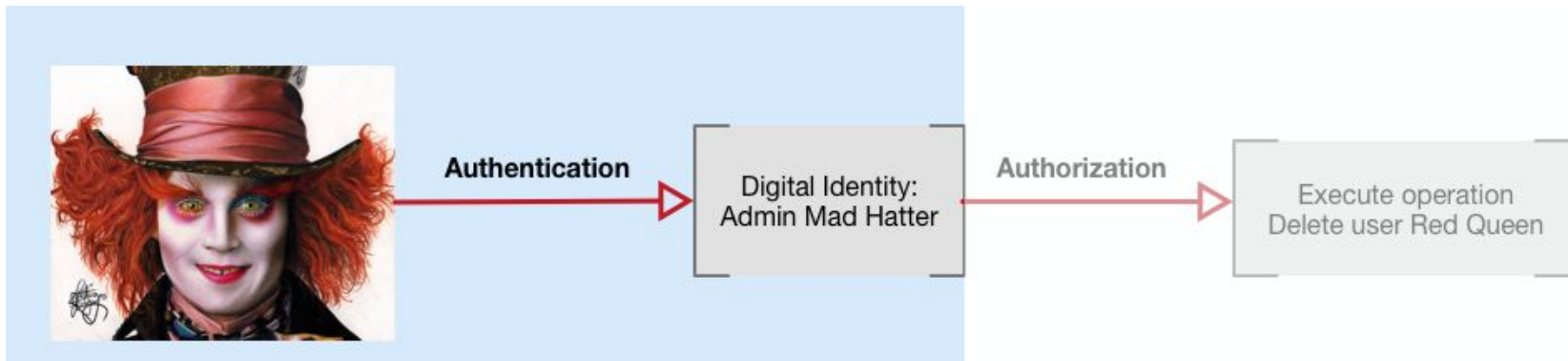


Even very strong passwords are at risk

- 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

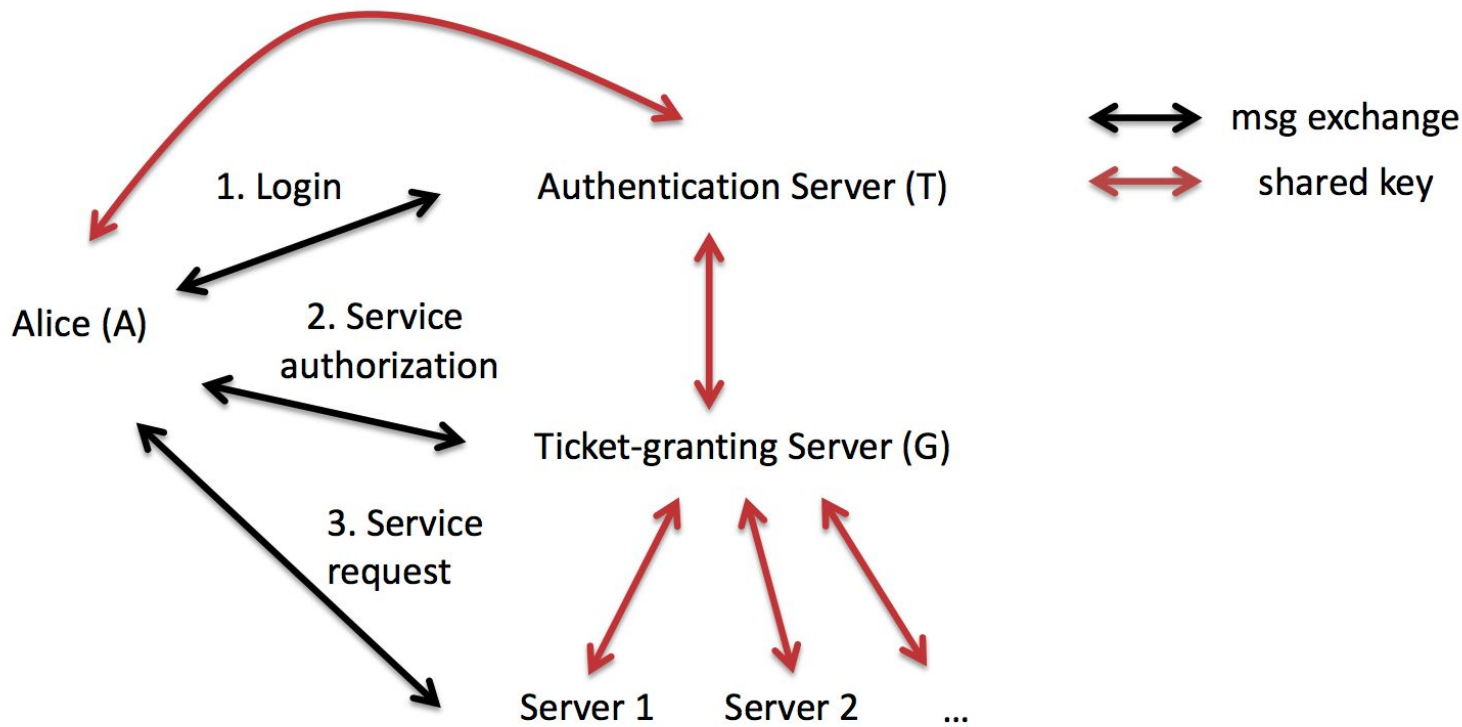
- Access control
- User authentication using passwords
- **Kerberos**
- Multi-factor authentication
- LDAP
- User training



Kerberos

- 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

Kerberos Architecture



Kerberos Advantages

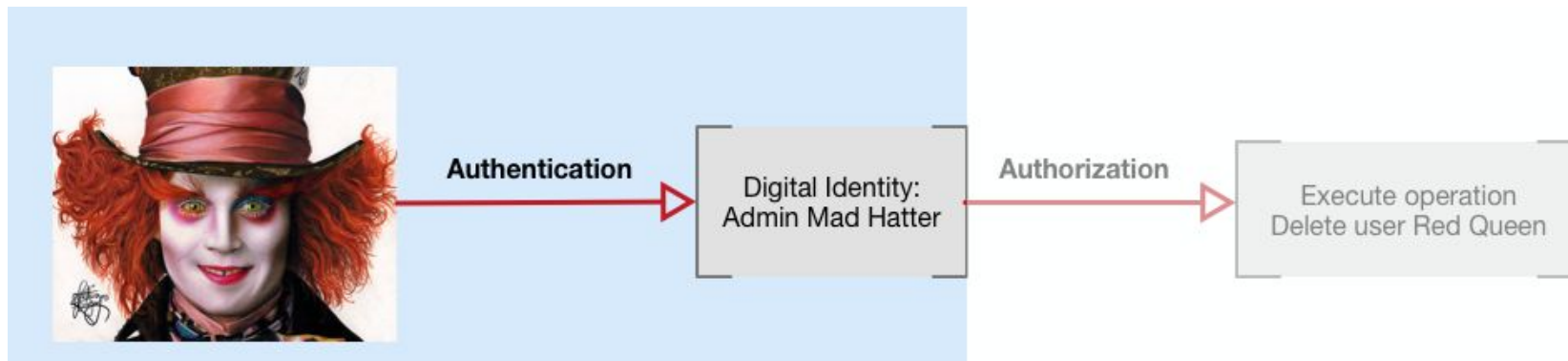
- Distributed access control
 - No password communicated in cleartext over the network
- Cryptographic protection against spoofing
 - All accesses mediated by ticket-granting service
- Limited period of validity
 - Tickets have a validity period, which servers check
 - Limits window of vulnerability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

Kerberos Disadvantages

- Ticket-granting server
 - Single point of failure or compromise
 - Performance bottleneck
- Requires at least roughly-synchronized clocks
 - All accesses mediated by ticket-granting service
- Ticket replay possible during validity period
- Password used at the beginning is a weak spot
 - User host can save it and then replay it

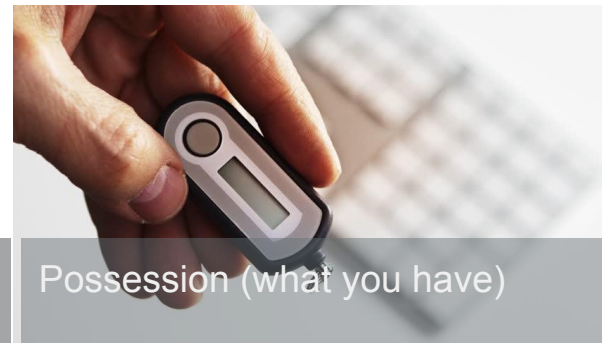
Outline

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



Multi-factor Authentication (MFA)

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



- **Two-factor authentication (2FA)**

- Use two of the three classes above

Scenarios

- What authentication factors are used in the following?



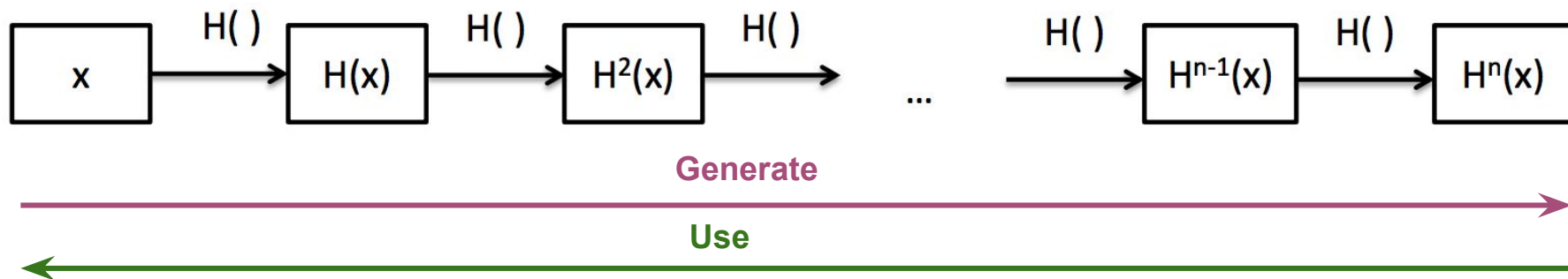
Authentication Factors

- 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)

- **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 $H^{n-i-1}(x)$, 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 $m \geq 100$

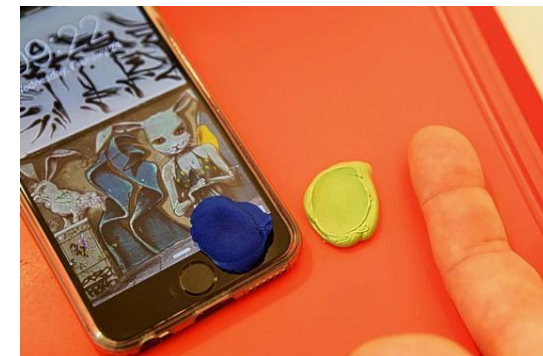
- Motivation
 - Something you know could be guessed
 - Something you own could be stolen
 - Nothing to remember, nothing to share
- Behavioral
 - Speech
 - Keystroke timing
- Physiological
 - Iris
 - Fingerprint
 - Face / voice recognition

Biometrics Authentication Process

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

Fingerprint Recognition

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



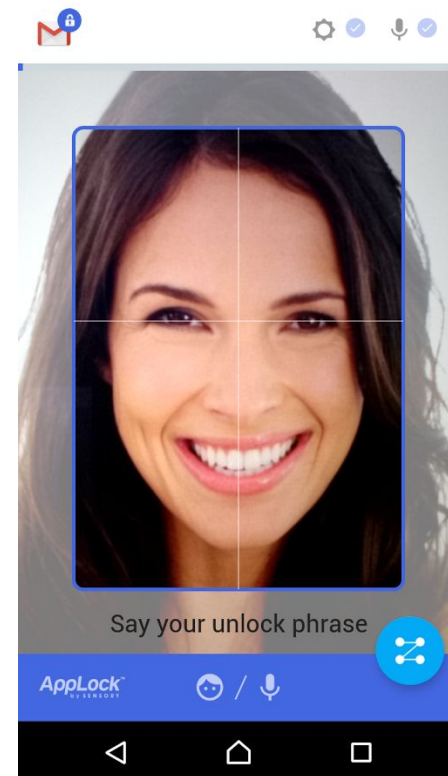
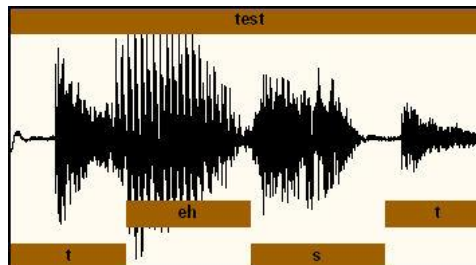
Voice Recognition

- Speech input

- Cadence
- Frequency
- Duration

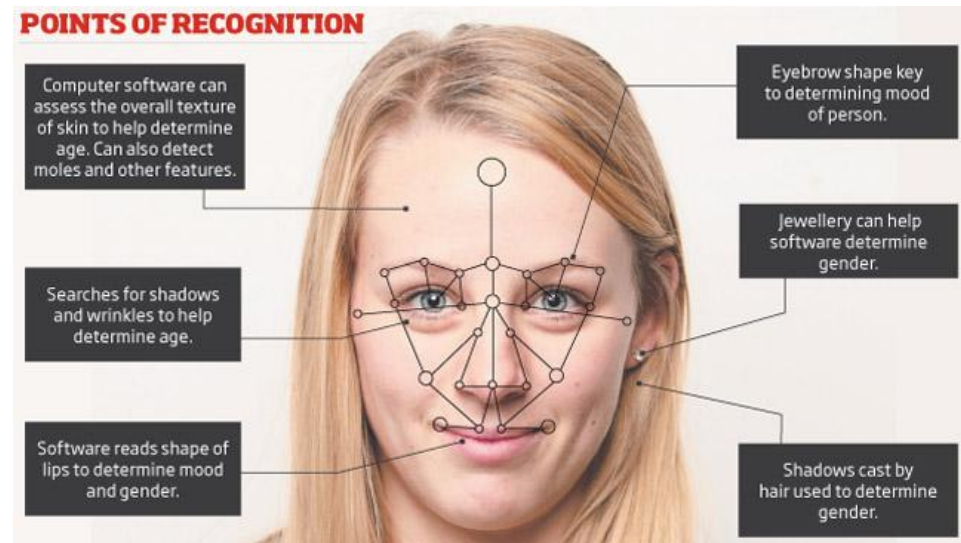
- Issues

- Environmental noise
- Having a cold
- Lossy transformation from analog to digital
- Same person has different accents in different languages



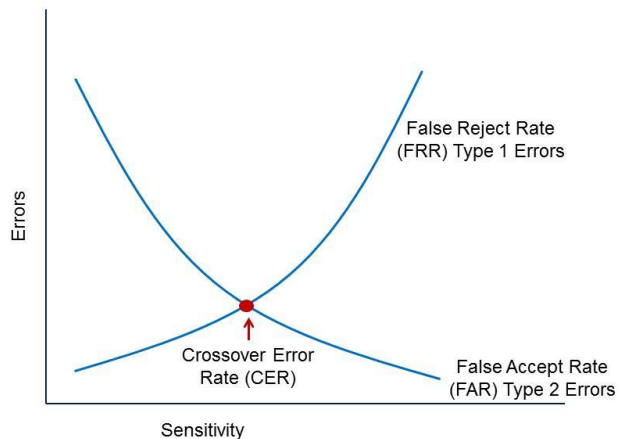
Face Recognition

- 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

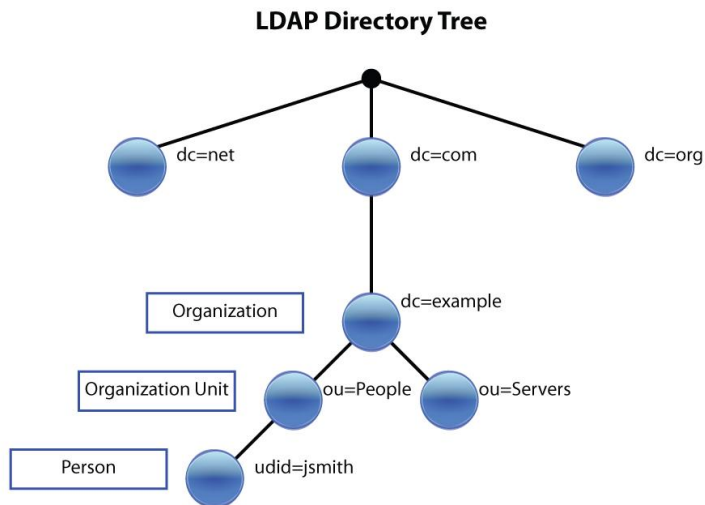
- Access control
- User authentication using passwords
- Kerberos
- Multi-factor authentication
- **LDAP**
- User training

Lightweight Directory Access Protocol (LDAP)

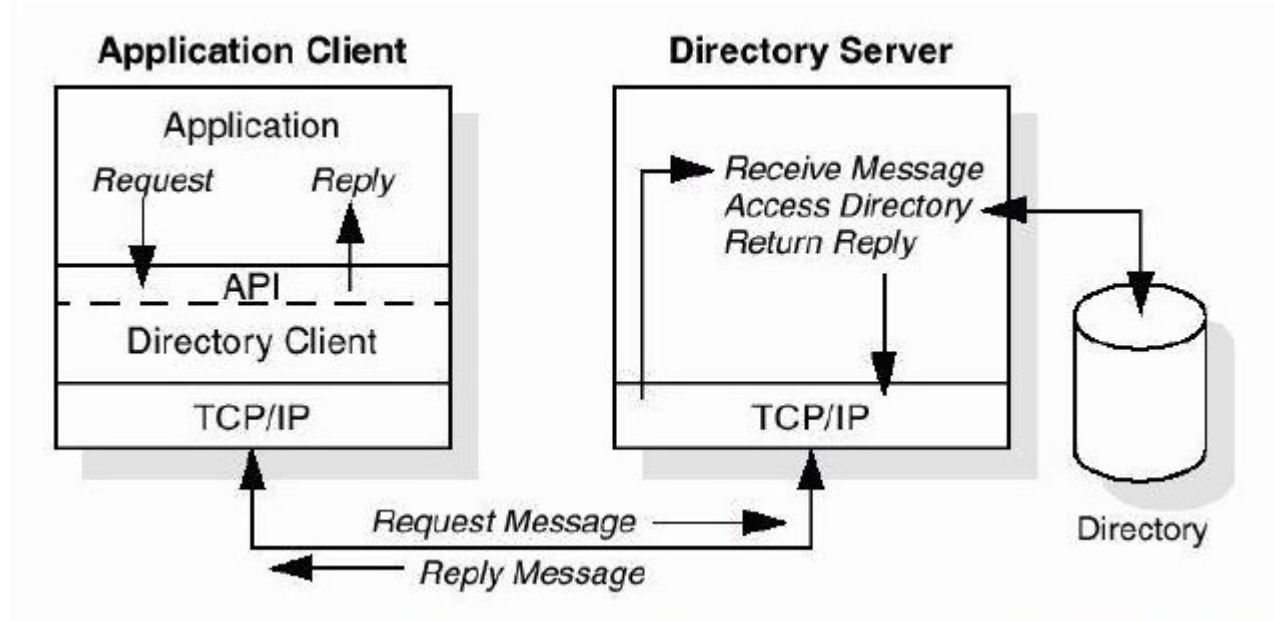
- Standard for accessing a corporate repository for commonly-used information
 - Many RFCs specify parts of LDAP
 - Information stored hierarchically
 - Allows to represent objects (users, groups, organizational units, network objects, printers, etc)
 - Allows representation of object attributes (text, 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)

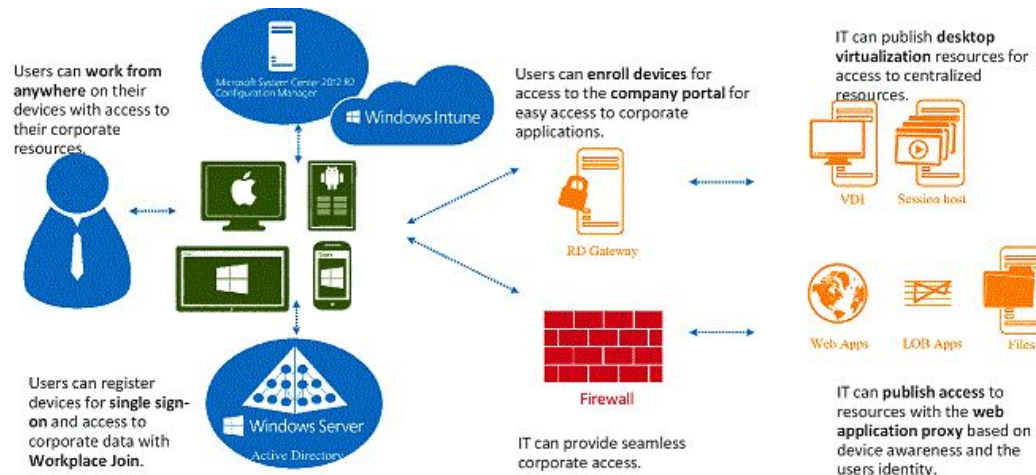


LDAP Client-Server Interaction



LDAP Usage (1)

- Store users and access authorization (e.g., use for RBAC)
- Implementation example: Microsoft Active Directory
- Scenario
 - Medium-sized banking firm, >5000 employees 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



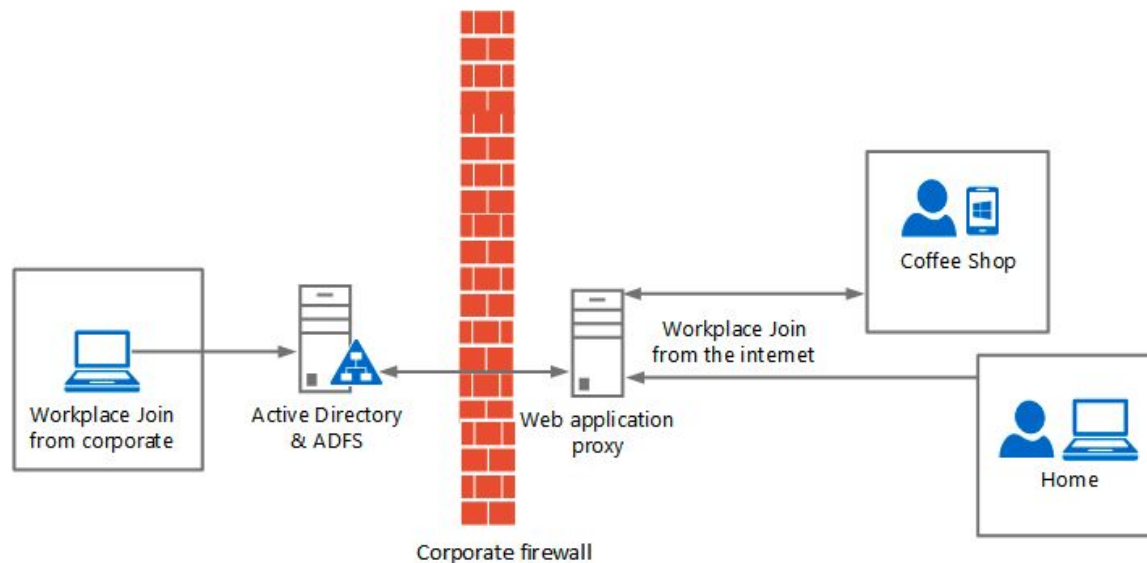
Scenario (and subscenarios) and images from
[https://technet.microsoft.com/en-us/library/dn550982\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn550982(v=ws.11).aspx)

LDAP Usage (2)

- **Sub-scenario #1**

- Enable users to register devices
- Enable users to have a single sign-on experience

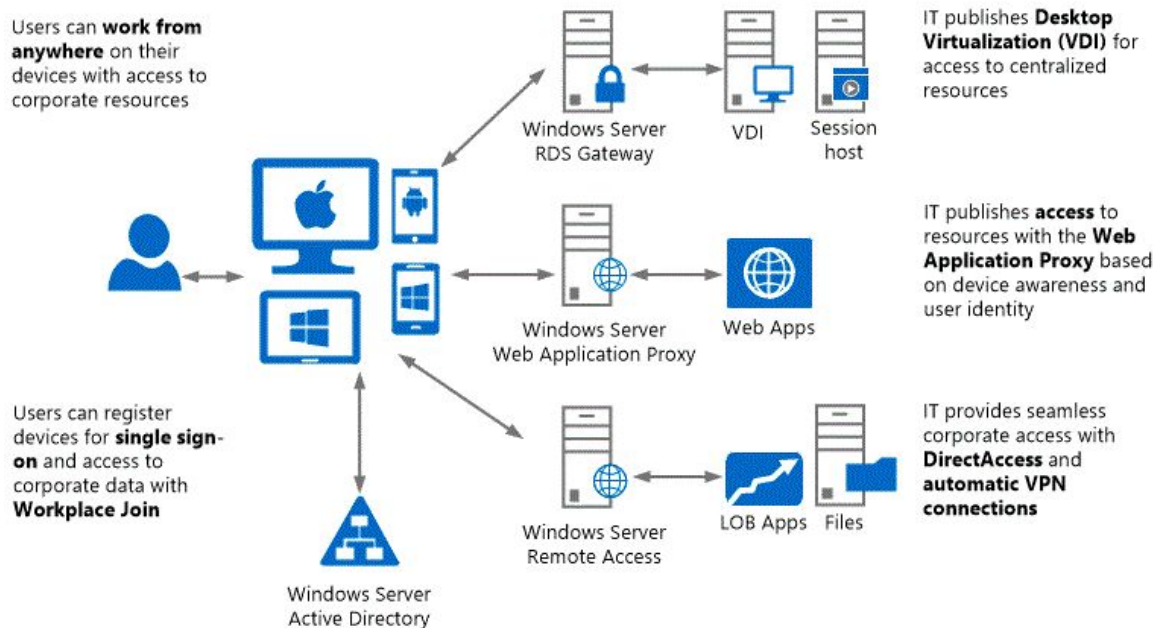
Workplace Join with on-premises Device RegistrationService



LDAP Usage (3)

- **Sub-scenario #2**

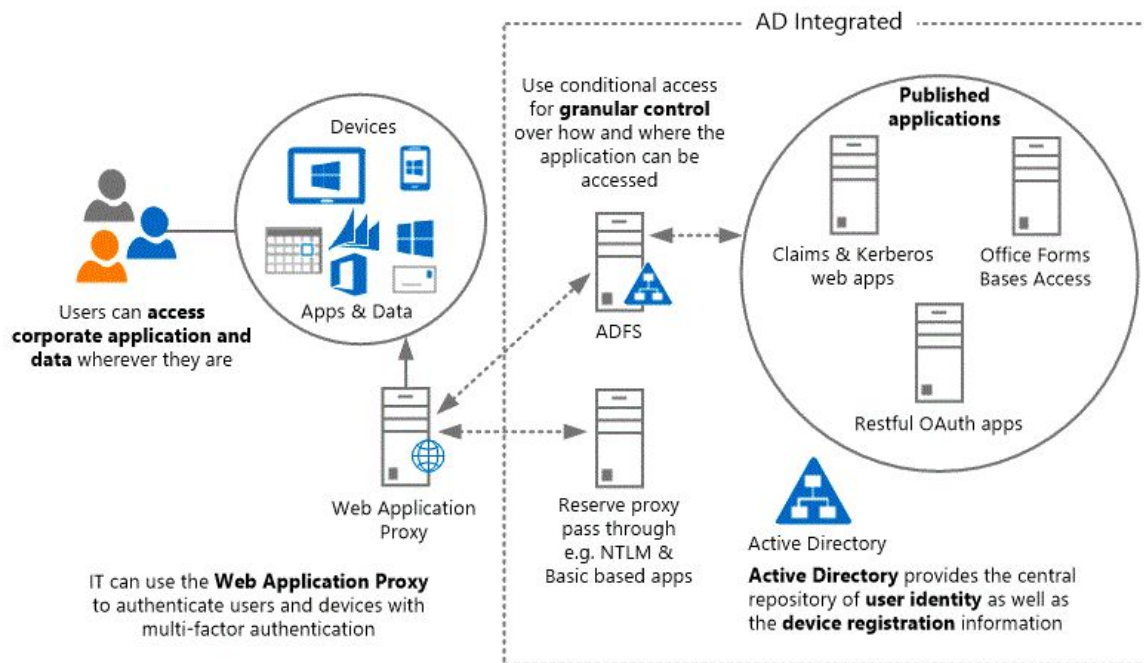
- Enable users to set up seamless access to corporate resources



LDAP Usage (4)

- **Sub-scenario #3**

- Active Directory enhancements for improving access control risk mitigation



LDAP - Food for Thought

- 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

- 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)

SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES		VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES	
1. USE ANTIVIRUS SOFTWARE				1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS				2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY				3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW				4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION				5. USE A PASSWORD MANAGER

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?

Phishing

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

----- Forwarded Message -----

From: PayPal <paypal@notice-access-273.com>

To: [REDACTED]

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 placed 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

- 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

PhishSim

PhishSim is a phishing training and simulation tool that provides realistic phishing tests, custom templates and automatic education for employees.

Hackers Send About 156 Million Phishing Emails Every Day.



Stop phishing attacks with anti-phishing training from SecurityIQ, your employees will learn to avoid phishing attempts.

Conclusion

Important to understand how users interact with security-critical systems

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

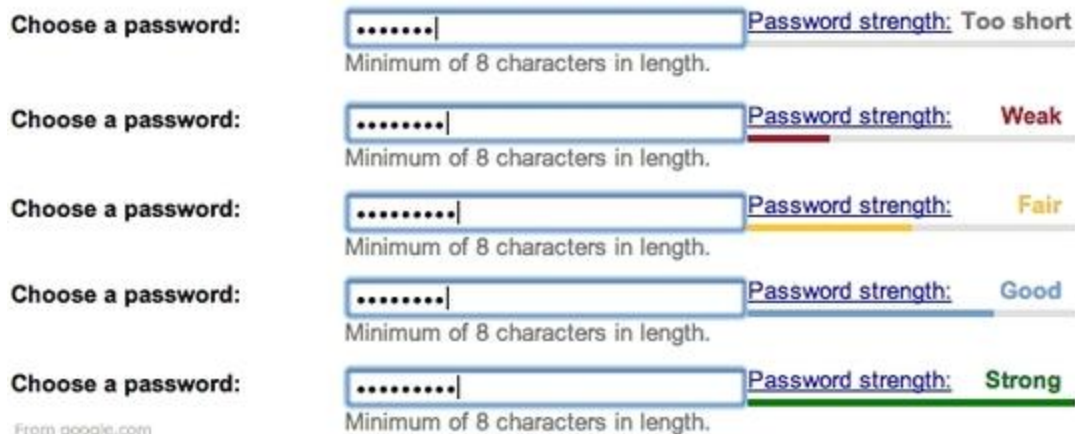
Backup slides

What makes a good password? (1)

- **Ideally passwords are random choices from a uniform distribution**
 - Green Book of US Defense Dept (1985) recommends machine-generated passwords
 - But these are difficult to remember, so the recommendation was abandoned
- **Password strength estimation through “entropy”**
 - NIST’s electronic guidelines: introduced heuristic measure of entropy
 - Run popular open-source password cracking library, evaluate average number of guesses to find a proportion of the passwords
- **NIST guidelines**
 - At least one uppercase and one non-alphabetic character
 - But users may insert these characters in predictable places: (e.g., F1rst)
 - Estimate increase in password guess difficulty by a factor of 64

Towards stronger passwords

- Advice to discourage simple dictionary passwords
- Strength meters



- Black lists to limit frequency of most common passwords

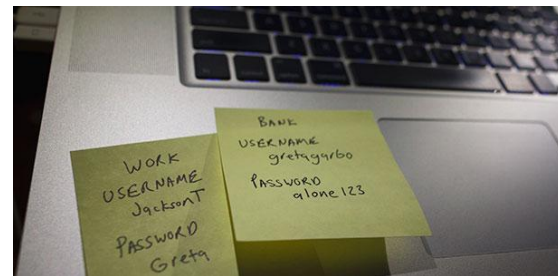
What makes a good password? (3)

- **Easy to remember, hard to guess**

- Otherwise users reuse passwords when prompted to periodically change them
- Otherwise users write them down

- **Tackling online attacks**

- How? Make attack costly for attacker
- Rate limiting (e.g., “three strikes”)
- Block IP addresses that send millions of failed attempts



- **Tackling offline attacks**

- Attacker has access to passwords file
- Offline attackers have unbounded nr of guesses; bounded only by computational capabilities
- Only proper hashing and salting of passwords make a real difference against such attacks
- If breach detected, admins could require users to reset passwords

RBAC in Solaris OS

- **Alternative to superuser-based model**
- **Rights profiles assigned to special user accounts called roles**
- **Users first log in, then assume a role**
- **Right profiles:**
 - Root
 - System Administrator - manages file system, mail, software installation. Cannot set passwords
 - Operator - backups, printer management
- **Security profiles:**
 - Three right profiles with supplementary profiles
 - Information Security (Network security as supplementary profile), User security, Zone security

