



Secure Software Development Design Principles

Objectives

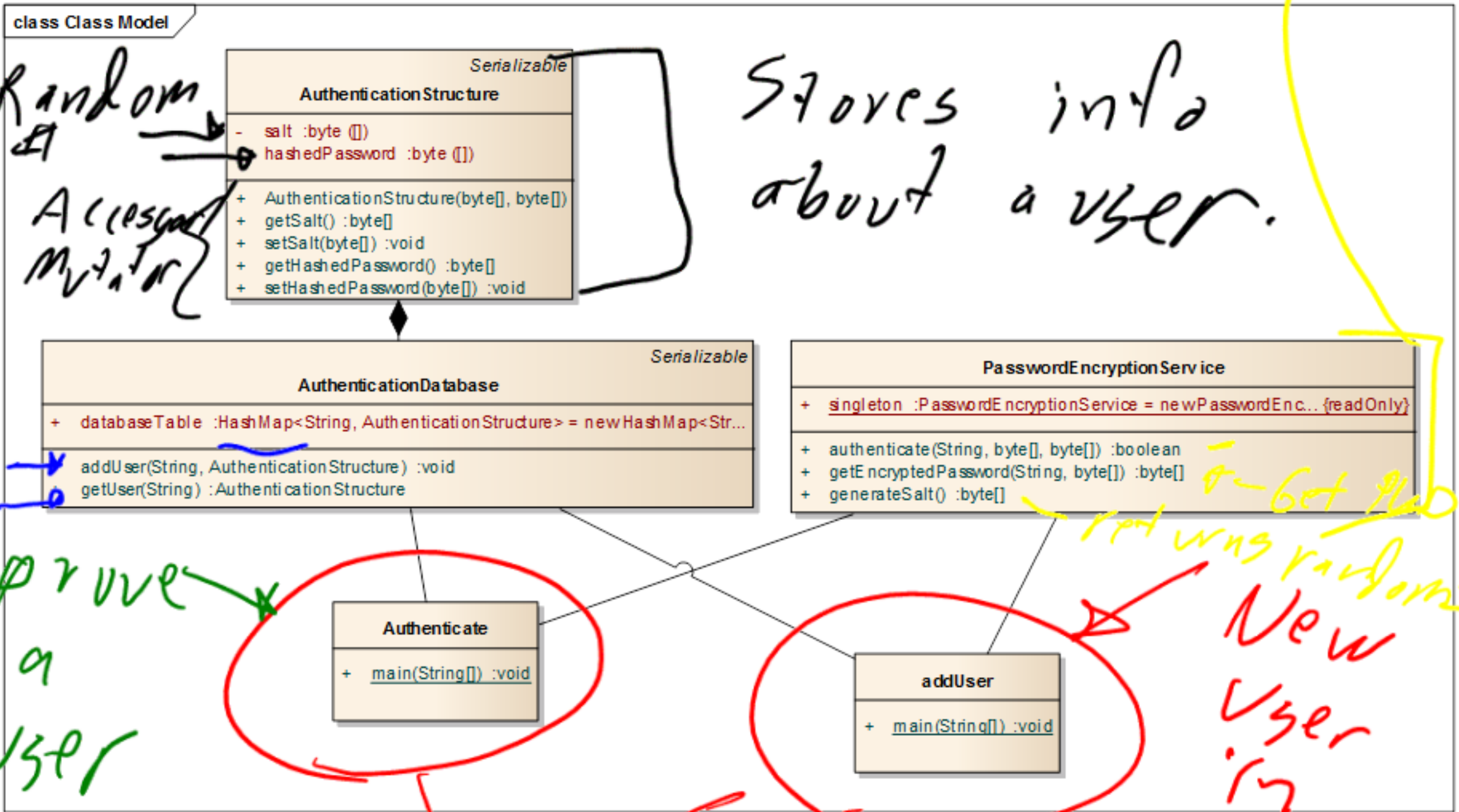
- Explain the design for an appropriate mechanism for encrypting and storing passwords
- List and explain the Secure Design Principles
- Describe the concept of trust domains and trust boundaries
- Critique architectures based on trust allocations
- Critique a modern software application from a security standpoint

Find problems/risks

A Yeah, probably not setting here.

AN Encryption Example

Service



Random Access Mutator

Stores info about a user.

prove a user

get salt
return was random
New User in System

Main programs



Design Case Study

- A system is setup on campus at MSOE to log failed login attempts
 - Logs entered user name
 - Logs attempted password

⇒ Discloses a lot about passwords

What flaws do we see in design?

tiger \Rightarrow tgierr

User name tiger
password bob



Design Flaws

- Not following coding standards —
- Improper implementation of least privilege — *shortly talk about*
- Software fails insecurely —
- Authentication methods easily bypassed \Rightarrow *AKA Microsoft + Bob*
- Security through obscurity —
- Improper error handling — *Fails unsecure*
- Weak input validation —

Cross Scripting

Secure Design Principles

- Principle of Least Privilege
- Separation of Duties
- Defense in Depth
- Fail Secure
- Economy of Mechanisms
- Complete Mediation
- Open design
- Least Common Mechanisms
- Psychological Acceptability
- Leveraging Existing Components

Reuse what others have done.

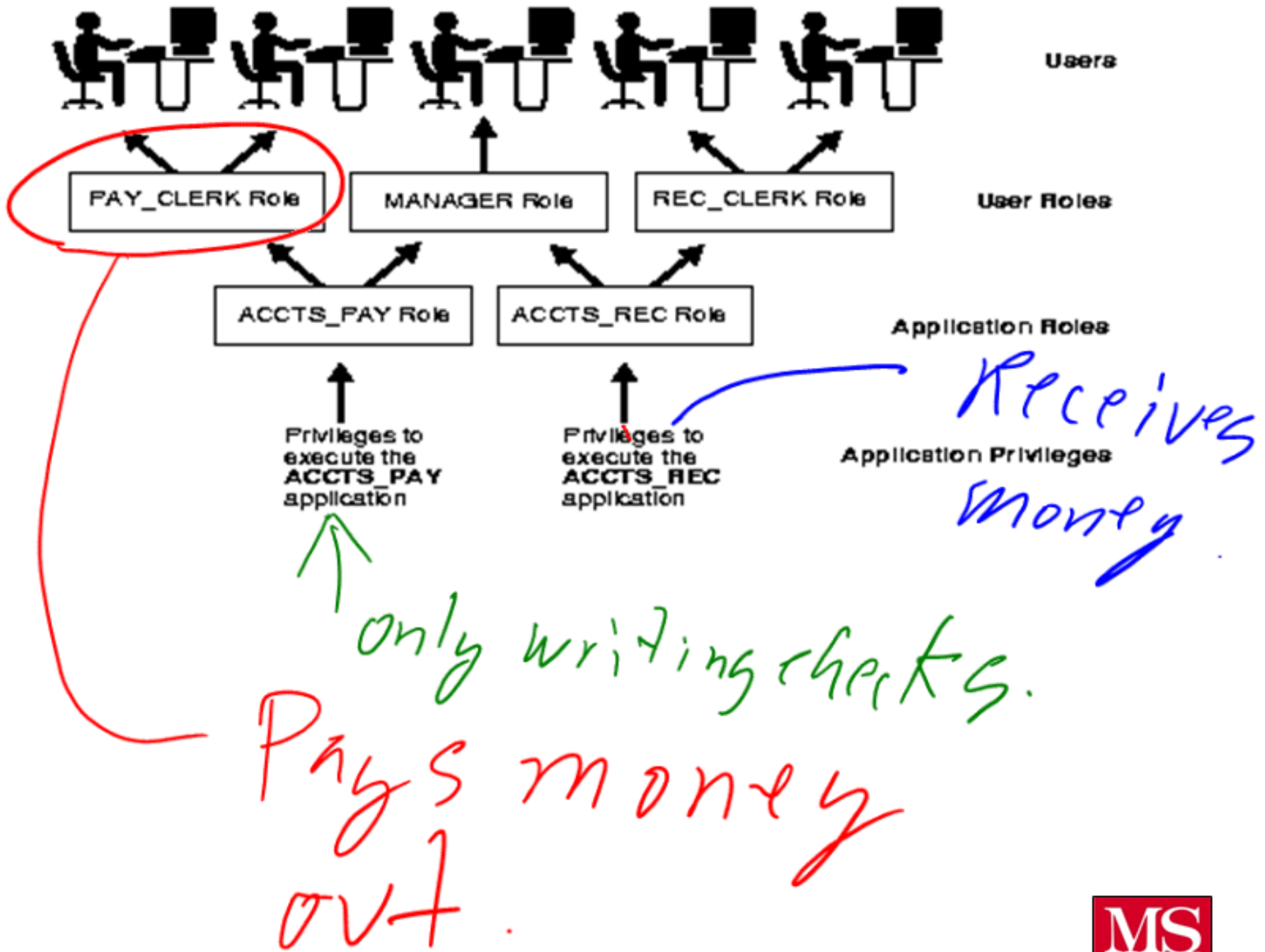


The Principle of Least Privilege

The Principle of Least Privilege

- “[The Principle of Least Privilege] requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.”
 - Department of Defense (DOD-5200.28-STD), also known as the orange book

What does this mean to us in software?



Unix Security Levels and

Sudo

Separation of Duties

- Design is compartmentalized — Split; +
 - Split keys for cryptographic functions
- Development roles
 - Programmer does not review his own code —
 - Programmer does not deploy code onto production system —

only have a component do what it needs to do.

Defense in Depth

- Layered defense towards security
 - The breach of a single vulnerability does not result in complete or total system compromise
- Deters curious hacker / nondetermined hacker

- Use of input validation prepared statements / stored prog.

Security Zones

Zone Access Separated based on person is in.



Fail Secure

- Software reliably functions when attacked
- Is rapidly recoverable in the event of a failure
- Fails to a secure state if a failure occurs

True Crypt and fail secure

Economy of Mechanism

- The more complex the design of the software, the more likelihood for a security failure there is
 - Unnecessary functionality or unneeded security mechanisms should be avoided
 - Strive for operational ease of use

Complete Mediation

- Every access to every object must be checked for authority every time the object is accessed.
- **Example 1**
 - When a UNIX process tries to read a file, the operating system determines if the process is allowed to read the file. If so, the process receives a file descriptor encoding the allowed access. Whenever the process wants to read the file, it presents the file descriptor to the kernel. The kernel then allows the access. If the owner of the file disallows the process permission to read the file after the file descriptor is issued, the kernel still allows access. This scheme violates the principle of complete mediation, because the second access is not checked. The cached value is used, resulting in the denial of access being ineffective.

Index of /

https://myweb.msoe.edu/?user=sebern&path=msoe/Winter2011/ce2800/ce2800.shtml

Suggested Sites Web Slice Gallery Church Sound System LXR linux/include/li... Professional Audio ... Other bookmarks









Index of /

Index of /

https://myweb.msoe.edu/?user=schilling&path=msoe/Winter2011/ce2800/ce2800.shtml

Suggested Sites Web Slice Gallery Church Sound System LXR linux/include/li... Professional Audio ... Other bookmarks

Index of /

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 favicon.ico	08-Jun-2004 17:12	766	
 graphics/	01-Nov-2004 10:37	-	
 index.html	18-Nov-2010 10:17	1.9K	
 local/	08-Apr-2009 13:56	-	
 msoe.ico	08-Jun-2004 17:12	766	
 robots	06-Jul-2007 16:12	0	
 test.cgi	25-Feb-2008 14:22	65	
 test.py	25-Feb-2008 14:22	65	

Apache/2.2.8 (Ubuntu) mod_auth_kerb/5.3 DAV/2 SVN/1.4.6 mod_jk/1.2.25 mod_ldap_userdir/1.1.12-20070601 PHP/5.2.4-2ubuntu5.12 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g mod_perl/2.0.3 Perl/v5.8.8 Server at myweb.msoe.edu Port 443

Credit Card's Billing Name & Address:

First Name:

Last Name:

Address:

City:

State/Province:

Zip/Postal Code:

Country:

Process Now

(do not click more than once)

Open Design

- All information about crypto systems is public knowledge except the key, and the security of the system against cryptanalysis attacks is dependent on the secrecy of the key
- Not Security through obscurity

Least common mechanisms

- Mechanisms common to more than one user or process should not be shared
 - Design should compartmentalize or isolate the functions by user roles

Psychological Acceptability

- The security principle should be designed to maximize usage, adoption, and automatic application
- Discuss strong passwords as an example

Leverage Existing Components

- Use existing components when possible

Trust Relationship

- Every communication between parties must have some degree of trust associated with it
 - Trust relationship
- For simply communications systems, each system has full trust and allows the other complete access to its communication facilities
 - Not very secure

Trust Boundaries

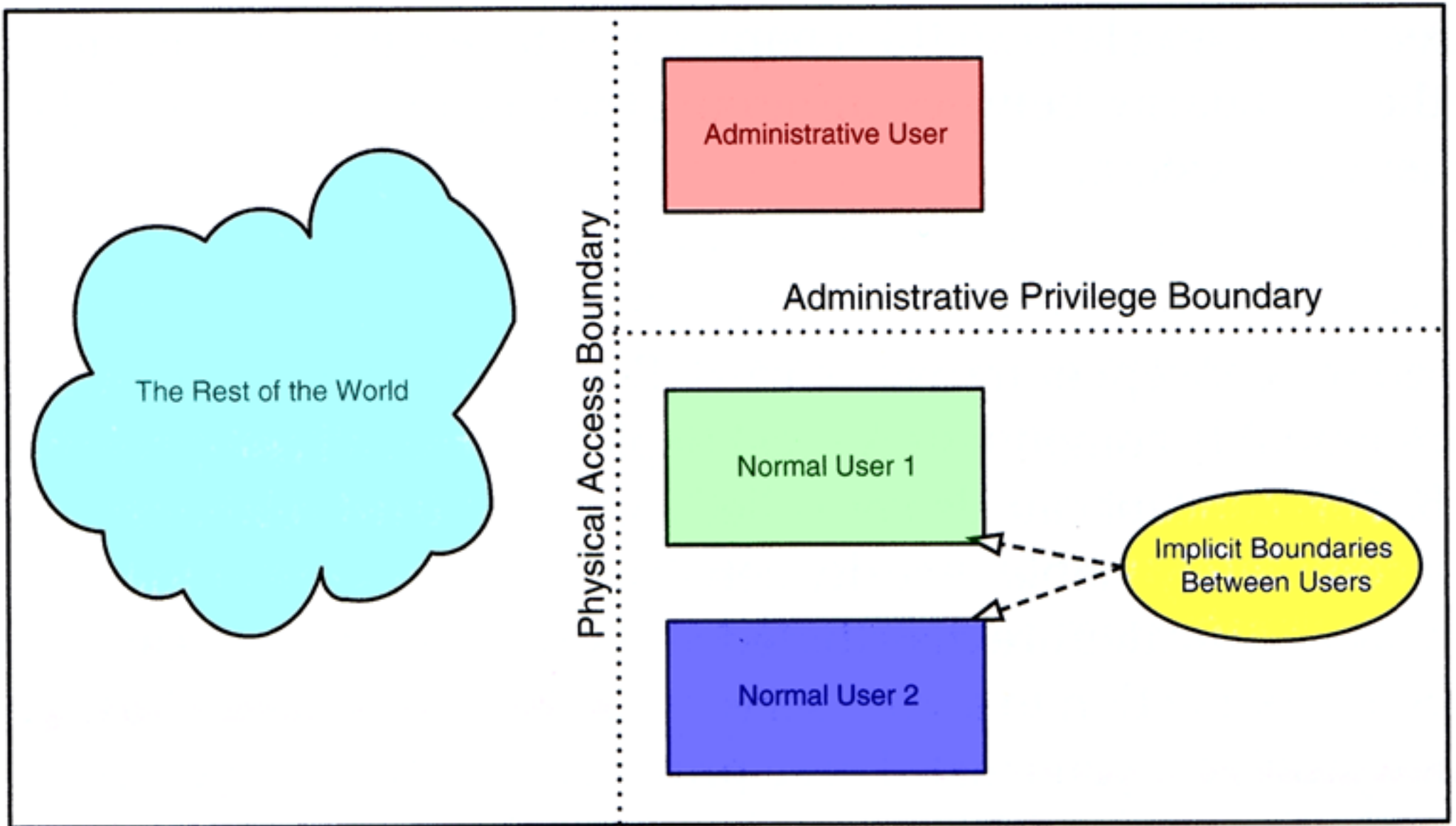
- Distinguishes between regions of shared trust
 - Region of shared trust is a trust domain

Windows 98 Trust Boundary

Example



Simple trust relationships



Security Trust – Defense in

Depth

- Layering protections so that the compromise of one is mitigated
- Running services and daemons as low privileged accounts
- Isolating different functions to different pieces of hardware
- Demilitarized zones
- Stack and heap guards

- Strong coupling
 - Strong coupling indicates a high level of trust amongst components
 - High exposure of internal interfaces
 - High risk of problems
 - Data validation error prone and difficult
- Strong cohesion
 - Strong cohesion indicates module handles only one specific task

- Modules which cross trust boundaries
 - Design decomposition which fail to decompose modules along trust boundaries

Strong coupling exploit

- Shatter class of vulnerabilities

Google Chrome

The screenshot shows the Wikipedia Main Page in a Google Chrome browser window. The address bar displays the URL http://en.wikipedia.org/wiki/Main_Page. The page layout includes a navigation sidebar on the left with sections for navigation, search, interaction, toolbox, and languages. The main content area features a 'Today's featured article' section about the Battle of Dyrrhachium, a 'Did you know...' section with several trivia items, and a 'Recently featured' section. On the right side, there are sections for 'In the news' and 'On this day...', each containing a list of recent events and a small image.

Wikipedia, the free encyclo... x

← → ↻ ☆ http://en.wikipedia.org/wiki/Main_Page ▶ ⌵ ⌵ ⌵

navigation

- Main page
- Contents
- Featured content
- Current events
- Random article
- Advanced search

search

Go Search

interaction

- About Wikipedia
- Community portal
- Recent changes
- Contact Wikipedia
- Donate to Wikipedia
- Help

toolbox

- What links here
- Related changes
- Upload file
- Special pages
- Printable version
- Permanent link

languages

- Simple English
- العربية
- Bahasa Indonesia
- Bahasa Melayu
- বাংলা
- Brezhoneg
- Bosanski
- Български
- Català
- Český
- Dansk
- Deutsch

Today's featured article

The **Battle of Dyrrhachium** took place on 18 October 1081 between the Byzantine Empire, led by the Emperor Alexius I, and the Normans of Southern Italy under Robert Guiscard, Duke of Apulia & Calabria. The battle was fought outside the city of Dyrrhachium, the Byzantine capital of Illyria, and ended in a Norman victory. Following the Norman conquest of Byzantine Italy and Saracen Sicily, the Byzantine Emperor, Michael VII betrothed his son to Robert Guiscard's daughter. When Michael was deposed, Robert took this as an excuse to invade the Byzantine Empire in 1081. His army laid siege to Dyrrhachium but his fleet was defeated by the Venetians. On 18 October, the Normans engaged a Byzantine army under Alexius I Comnenus outside Dyrrhachium. The battle began with the Byzantine right wing routing the Norman left wing which broke and fled. Varangian mercenaries joined in the pursuit of the fleeing Normans but became separated from the main force and were massacred. Norman knights in the centre attacked the Byzantine centre and routed it, causing the Byzantines to flee. After the capture of Dyrrhachium in February 1082, the Normans advanced inland capturing most of Macedonia and Thessaly. [\(more...\)](#)


Recently featured: [Leo Ornstein](#) – [Dartmouth College](#) – [Local Government Commission for England](#)

[Archive](#) – [By email](#) – [More featured articles...](#)


Did you know...

From Wikipedia's newest articles:

- ... that 19th-century American actor and playwright **Steele MacKaye** [\(pictured\)](#) invented a variety of theatrical devices, including folding theatre seats?
- ... that 16th century noblewoman **Marguerite de La Rocque** was marooned on an island in the [Gulf of St Lawrence](#) by her relative, the privateer de Roberval, as punishment for an affair?
- ... that **Charles Van Riper**, a severe stammerer, was a pioneer in the development of speech pathology?
- ... that **Lexie Fyfe** became a professional wrestler while working in the billing department of a clinical laboratory firm at the invitation of a co-worker? [August 2008 \(UTC\)](#)
- ... that the book *[Help at Any Cost](#)* triggered hearings by the United States House Committee on Education and Labor into behavior modification techniques used by the tough love teen industry?
- ... that the 19th century Mexican soprano **Ángela Peralta** once sang Donizetti's opera *Maria di Rohan* in a theatre improvised from a disused coal pit in [La Paz, Baja California](#)?




In the news

- Japanese Prime Minister **Yasuo Fukuda** [\(pictured\)](#) resigns less than a year after taking office following Shinzo Abe's resignation. 
- **Hurricane Gustav** makes landfall on the U.S. Gulf Coast in Louisiana after causing at least 66 deaths in Haiti, 8 more in the Dominican Republic, and 11 in Jamaica.
- John McCain chooses **Sarah Palin**, the Republican Governor of Alaska, as his vice-presidential running mate in the 2008 U.S. presidential election.
- **Russia officially recognizes** the independence of Abkhazia and South Ossetia; the latter announces it will become part of Russia.
- Over 1.2 million people in Bihar, India are affected by **flooding** as the Koshi River changes its course.

[Wikinews](#) – [Recent deaths](#) – [More current events...](#)

On this day...

September 2: National Day for Vietnam (1945)

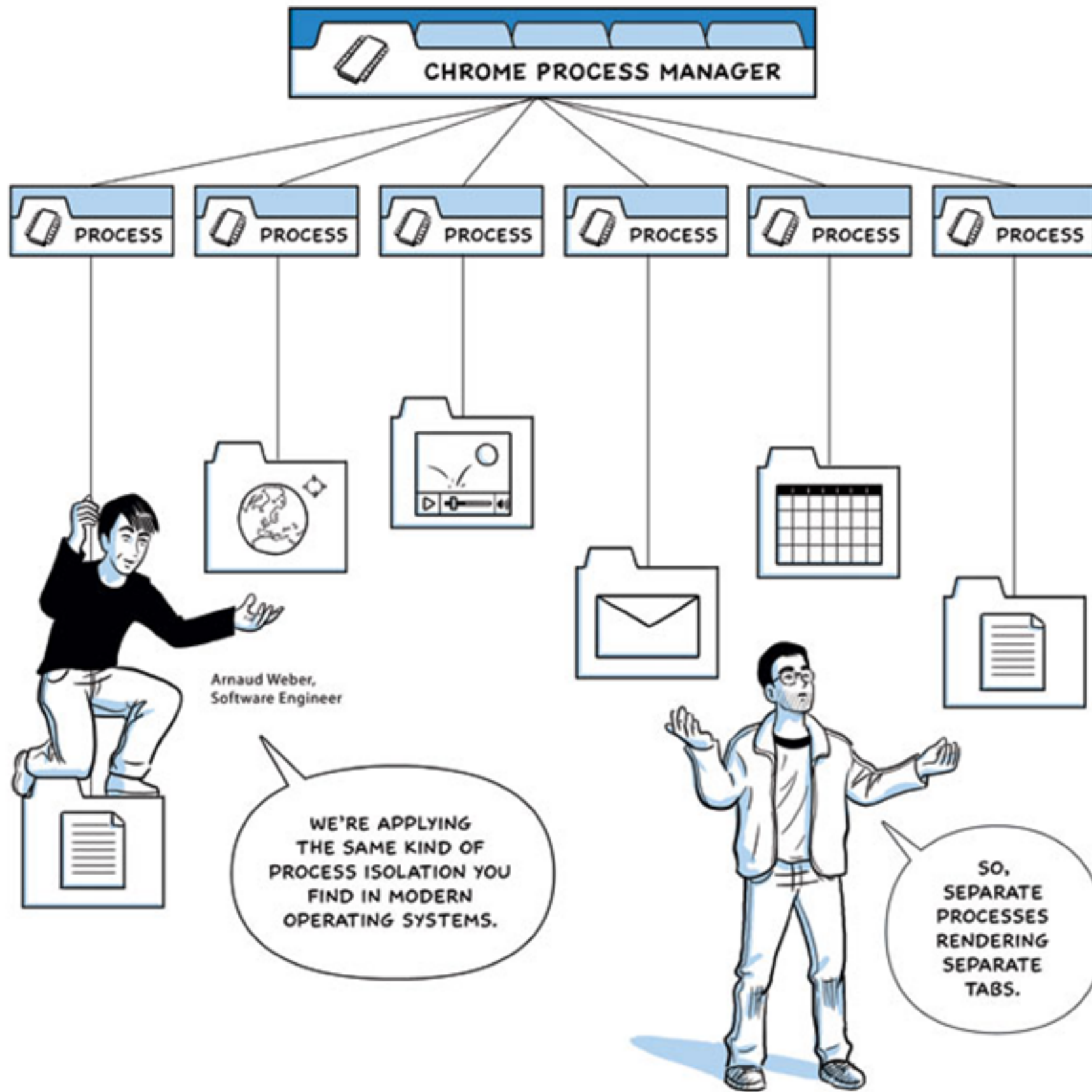
- 31 BC – Final War of the Roman Republic: Troops supporting Octavian defeated the forces of Mark Antony and Cleopatra in the naval **Battle of Actium** on the Ionian Sea near Actium in Greece. 
- 1666 – A large fire began on London's Pudding Lane and **burned the city** for three days [\(pictured\)](#), destroying St Paul's Cathedral and the homes of 70,000 of the city's 80,000 inhabitants.
- 1898 – Mahdist War: Forces led by Horatio Kitchener defeated Sudanese tribesmen at the **Battle of Omdurman** in Omdurman, Khartoum, Sudan, establishing British dominance in northeastern Africa.
- 1945 – On the deck of the United States Navy battleship USS *Missouri* in Tokyo Bay, representatives from the Empire of Japan and several Allied Powers signed the **Japanese Instrument of Surrender**, formally ending World War II.
- 1998 – Swissair **Flight 111** en route from New York City to Geneva crashed into the Atlantic Ocean, killing all 229 on board.

[More events: September 1](#) – [September 2](#) – [September 3](#)

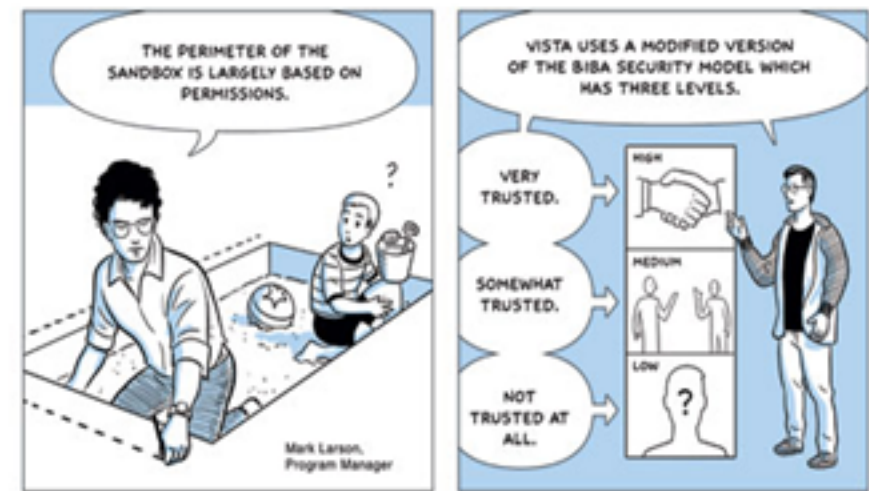
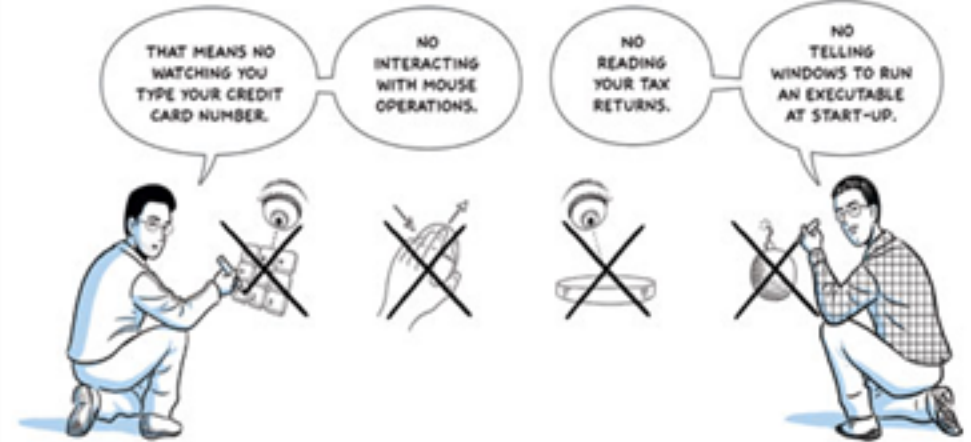
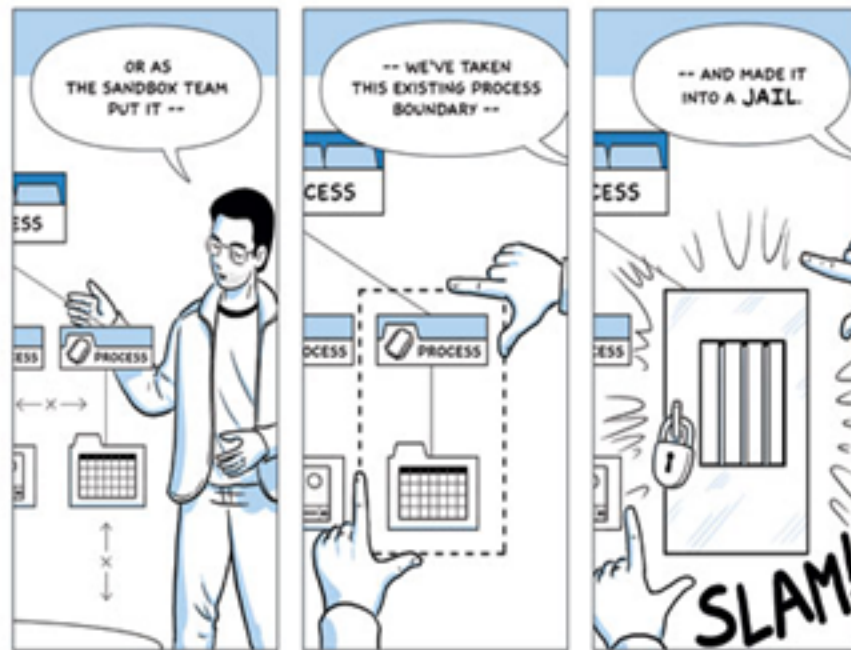
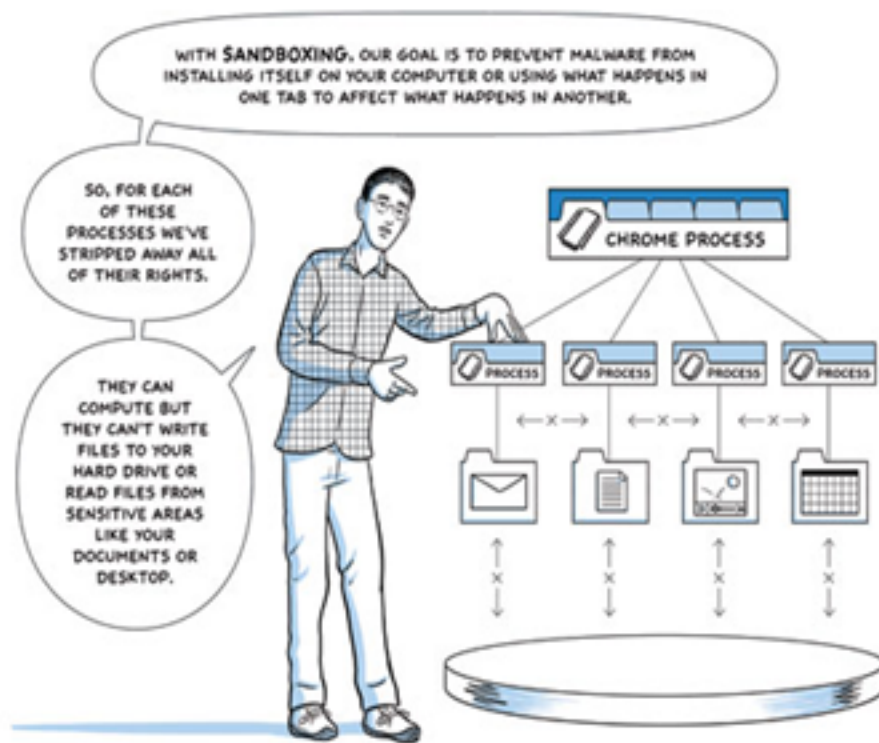
Google Chrome

Why is Google
Building a Browser?

Google Chrome



Google Chrome





Online Banking

En Español

Sign In

Enter Online ID:

(6 - 32 characters)

Save this Online ID [How does this work?](#)

[Sign In](#)

[Where do I enter my Passcode](#)
[Forgot or need help with your ID?](#)

Not using Online Banking?

[Enroll now for Online Banking](#)

[Learn more about Online Banking](#)

[Service Agreement](#)

[Go to Online Banking for a state other than Wisconsin](#)

Secure Area

[Home](#) . [Locations](#) . [Contact Us](#) . [Help](#) . [Sign in](#) . [Site Map](#)
[Personal Finance](#) . [Small Business](#) . [Corporate & Institutional](#)
[About the Bank](#) . [In the Community](#) . [Finance Tools & Planning](#) . [Privacy & Security](#)



Bank of America, N.A. Member FDIC. Equal Housing Lender
©2009 Bank of America Corporation. All rights reserved.



Bank of America | Onli... x 2009 Sports Illustrated... x Google Chrome - W... x

http://sportsillustrated.ann.com/2009_swimsuit/

MODELS NBA DANCERS TENNIS STARS ON LOCATION VIDEO SWIMSUIT GOODIES

VIDEO LINEUP ALL VIDEO

ARIEL MEREDITH CHENEY LARSCHIED MELISSA HARO ALISON PRESTON DANIELA HANTUCHOVA

Brooklyn DECKER

VIDEO PHOTOS

ALL MODELS

Brooklyn Decker was photographed by Raphael Mazzucco in Carriacou Island, The Grenadines. Swimsuit by Sugarwater.

SWEETSTAKES Sports Illustrated Rolvinic

start Firefox Windows Task... Presentation1 LectureArchit... Jax Paint Sho... 2009 Sports IL... 12:02 PM

Google Chrome

- Each tab is its own process
 - Not thread
 - "prevent malware from installing itself" or "using what happens in one tab to affect what happens in another",
- Can not write files or read from sensitive areas (e.g. documents, desktop)
- two levels of security, user and sandbox
 - *sandbox* can only respond to communication requests initiated by the *user*.[\[34\]](#)
- Plugins are run in separate processes
 - communicate with the renderer in dedicated per-tab processes.¹
- *Incognito* mode prevents the browser from storing any history information or [cookies](#)
 - Referred to as a [porn mode](#)