Lecture 01
Introduction

CMPU-4008

Advanced Security 2

Module Contents

- Authentication Applications
- Electronic Mail Security
- Internet Protocol Security
- Web security
- Intruders, Crimeware, Firewalls
- Security Policies, Standards, Compliance

Module Contents

- Security Metrics and Auditing
- Penetration Testing
- Social Engineering
- Defences to security attacks
- The impact of Technological developments on Security
- Disaster Recovery, Business Continuity

Assessment Methods

- Written examination – 50%

- Continuous assessment – 50%

Continuous assessment – 50%

- Quiz 1 - 10%.
  - Theory Test in week 6.
- Quiz 2 - 10%.
  - Theory Test in week 12 (All lecture material).
- Assignment 1 - 15% (Week7).
  - Research on the skills, certifications and training for security expert.
  - Google hacking, Vulnerabilities and Exploits
- Assignment 2 - 15% (Week13).
  - Security Tools

Submission guidelines

- Submission guidelines
  - Use Brightspace, no email submission
  - naming files (Full-Name_Student-Number_Assignment-Name)

- Optional Report guidelines
  - Cover page, introduction, body, discussion, conclusion and references

- Marks will be deducted for late submission

Penetration Testing Tools

- **Resources**
- http://www.darknet.org.uk/
- http://www.livehacking.com/
- http://www.hiren.info/
- http://holisticinfosec.org/

Tools used for security training

- Seed - http://www.cis.syr.edu/~wedu/seed/
- Sweet - http://csis.pace.edu/~lchen/sweet/
- Security Shepherd - https://www.owasp.org/index.php/OWASP_Security_Shepherd
- There are a lot of Security Gaming software

Essential Reading

- Computer Security: Principles and Practice, 3rd edition, William Stallings and Lawrie Brown (2015), Pearson.

Supplemental Reading

- Cryptography and Network Security : Principles and Practices, 6th Ed, Williams Stallings (2014) Prentice Hall.

- Network Security Essentials: Applications and Standards, 4th Ed, William Stallings (2011), Prentice Hall

References

- Seymour Bosworth and M.E. Kabay, 2009, Computer Security Handbook, John Wiley & Sons. Inc.
- Andrew Lockhart, 2004, Network Security Hacks 100 Industrial-Strength Tips & Tools, O'Reilly
- Markus Jakobsson, Zulfikar Ramzan, 2008, Crimeware: Understanding New Attacks and Defences,Symantec Press.
- Ed Skoudis and Tom Liston, 2006, Counter Hack Reloaded: A step-by-step Guide to Computer Attacks and Effective Defences, Prentice hall
- Bruce Schneier, 2012, Liars and Outliers: Enabling the Trust that Society Needs to Thrive, John Wiley & Sons ISBN: 978-1118143308

Software license

- This software is provided “as is” and any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the contributor be liable for any direct, indirect, accidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, or tort (including negligence or otherwise) arising in any way out of use of this software, even if advised of the possibility of such damage.

- In plain English what does the above information mean.

Software license

- We don’t claim this software is good for anything– if you think it is, great, but it’s up to you to decide.

- If this software doesn’t work: tough. If you lose a million dollars because this software messes up, it’s you that’s out of million, not us.

- If you don’t like this disclaimer: tough. We reserve the right to do the absolute minimum provided by law, up to and including nothing.

Software characteristics

- We interact with software on daily basis.
- How and when we touch software and how and when it touches us is less our choice everyday.
- The quality of software matters greatly.
- Software is insecure.
- Insecure software is everywhere interconnected and woven tightly into the fabric of civilisation.

Why Software is insecure

- Software is not necessarily designed and constructed with security in mind.
- Internet Explorer is one of many examples of insecure software.
- Lack of security training:
  - Many software developers do not understand the risks that they are exposing their users to by creating poorly written code.

Costs of Insecure Software

- Maintenance :
  - Network administrator has to spend a reasonable amount of his time installing security patches on the company's machines.

- Lack of productivity:
  - When a piece of software is compromised at work, everyone suffers.

- Reduce Bandwidth

Ongoing Platform Battlegrounds

- Web Search
  - Google vs. Bing/Yahoo, foreign engines
- Smart Phone
  - OS Apple vs. RIM, Nokia/Symbian, Android, Microsoft, Palm, Linux, ARM, Intel Atom)
- Digital Media
  - Apple (iPod, iPad & iTunes) vs. Microsoft (Media Player, Zune) vs. Real?
- Social Networking
  - Facebook, Twitter, LinkedIn, etc.

Ongoing Platform Battlegrounds

- Video Games
  - Sony, Nintendo, Microsoft
- Enterprise software
  - SAP vs. Oracle/Sun, Microsoft, IBM
- Micropayments
  - Sony Felica vs. PayPal, credit cards, Apple Pay,
  - Google Wallet, Softcard, CurrentC etc.
- Displays
  - Oled, 4k, Plasma vs. LCD (Sharp, Sony, Samsung, others)

The future of Security threats

- Cyberwar declared – Stuxnet a politically motivated attack (weaponized malware) :

  Duqu, Flame, and Shamoon

- Advanced Persistent Threat (APT) – advanced malware attack

- VoIP attacks – brute force and directory traversal class attacks against VoIP servers

The future of Security threats

- Car hacking – cars are more connected with built-in Bluetooth, 3G internet, GPS, Onstar, and dashboard computers
- The Facebook challenge - users trust of web (Web 2.0, API etc)
- Manufactured-delivered malware – products arriving with infections out of the box

The future of Security threats

- Fighting internet crime does not come cheap.

  For example, Inga Beale, the CEO of Lloyd's said that Lloyd's estimates that cyber attacks cost businesses as much as $400 billion a year, including the damage itself and subsequent disruption to the normal course of business.

Cybercrime Knows No Borders

- Prosecuting cybercrime is no easy task.

One of the biggest problems lies with the scope of legislation within a particular country. “There is a tremendous range in the laws – with many countries not having laws covering such simple concepts as unauthorized access to a computer system or installation of malicious software”.

Cloud apps a click away

- Dropbox – http://www.dropbox.com/
- Google Docs- https://docs.google.com/
- Microsoft OneDrive https://onedrive.live.com
- Evernote - http://www.evernote.com/
- GoToMyPC - http://www.gotomypc.co.uk/
- And many more …

Cloud Security Mechanism

- Take responsibility for your own security
- Ring fence your data
- Think about encryption
- Strong passwords for cloud services

Common Sense Security

- Security is not a specialist subject – it's everyone's responsibility
- The attackers only have to get lucky once and the defenders have to get it right 100% of the time

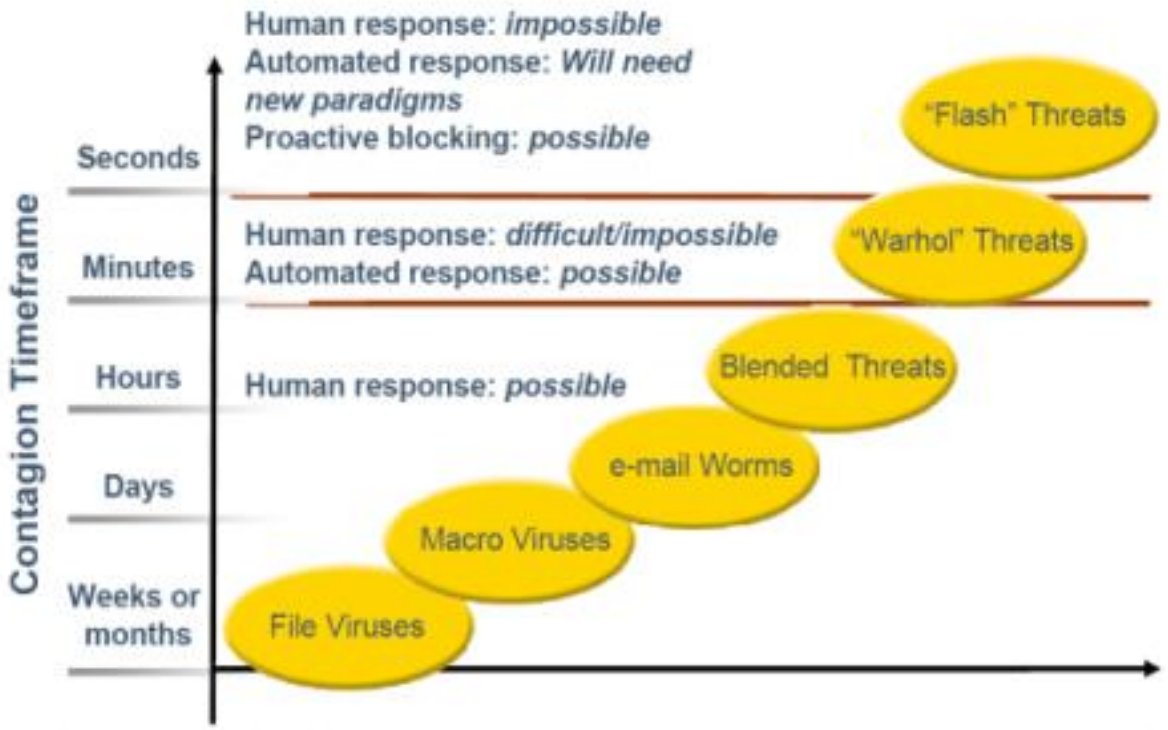
Some Resources on Cloud Security

1. Top Threats to Cloud Computing V1.0, Cloud Security Alliance, March, 2010.
2. Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance,2011.
3. Guidelines on Security and Privacy in Public Cloud Computing, Wayne Jansen and Timothy Grance, NIST, January 2011.
4. Cloud Computing Security: A Survey, Issa M. Khalil , Abdallah Khreishah,Muhammad Azeem, Computers 2014.
5. Overview of Attacks on Cloud Computing, Ajey Singh, Maneesh Shrivastava, IJEIT,2012
6. The Management of Security in Cloud Computing, Ramgovind S, Eloff MM, Smith E, IEEE, 2010

Intruders

- An Intruder is a person who attempts to gain unauthorized access to a system, to damage that system, or to disturb data on that system.
- Building technical knowledge and skills
- Gaining leverage through automation
- Exploiting network interconnections and moving easily through the infrastructure
- Becoming more skilled at masking their behaviour

Response Time



Vulnerability Trends

- Flaws can be found without source code
  - common: system call trace
  - new: subroutine call trace
  - protocols can be examined for vulnerabilities
  - program instabilities (buffer overflow, etc.)

- Good news — the public & vendors becoming
  - more security conscious
  - Patches now being released via Internet

I am a Developer

- 10 lines of code = 10 issues.

  500 lines of code = "looks fine."

- Code reviews.
  Recent source lines of code (SLOC) reviews and estimates suggest that a very conservative guess would place the number of bugs in most modern software at the rate of about one per 1000 lines of extremely well-written source code with great attention to security detail.
  1000 SLOC = 1 bug (error)

- Source: http://www.techrepublic.com/blog/it-security/thedanger-of-complexity-more-code-more-bugs

Windows: Source Lines of Code (Sloc)

Year	Operating System	Sloc (Million)
1993	Windows 3.1	6
1994	Windows NT 3.5	10
1996	Windows NT 4.0	16
2000	Windows 2000	29
2001	Windows XP	40
2005	Windows Vista Beta 2	50

Linux: Source Lines of Code (Sloc)

Operating System	Sloc (Million)
Red Hat Linux 6.2	17
Red Hat Linux 7.1	30
Debian 2.2	55-59
Debian 3.0	104
Debian 3.1	215
Debian 4.0	283
OpenSolaris	9.

Graphics Programs: Source Lines of Code (Sloc)

Operating System	Sloc (Million)
Mac OS X	86
Linux Kernel 2.6.0	5.2
Graphics Programs	
OpenOffice.org	10
Blender 2.42	1
GIMP v2.3.8	0.65
Paint.NET 3.0	0.13

Air Domain Strategic Context

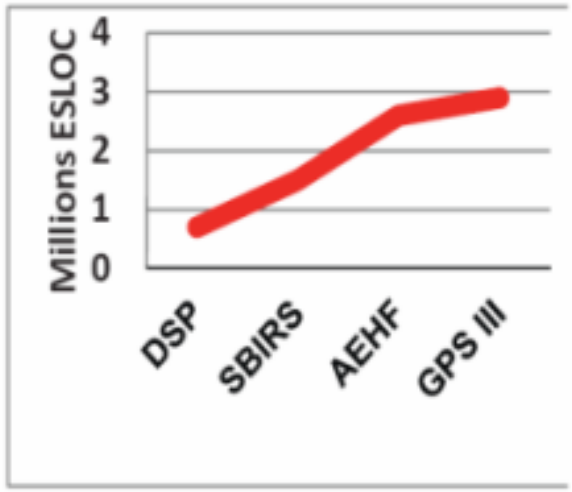


Figure 1b:

Space Systems Software Growth

Source: CMU/SEI

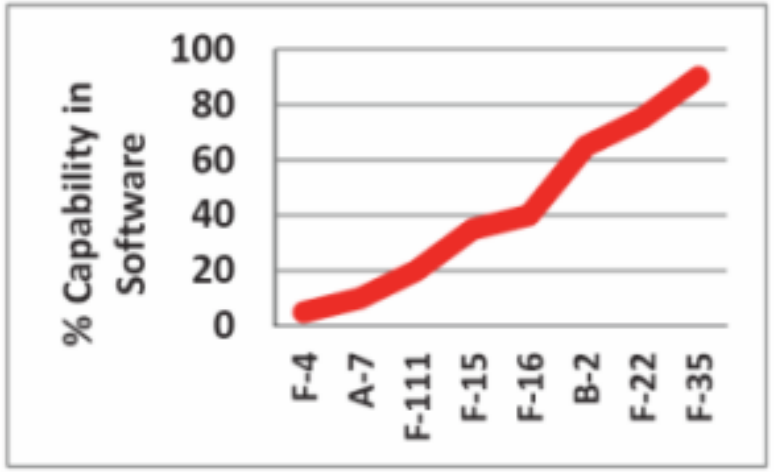


Figure 1a:

Air Platform Software Growth

Source: CMU/SEI and Lockheed Martin

Modernisation Centred Software

- Approximately ninety percent of the functionality in the Joint Strike Fighter (F-35) is dependent upon software (approximately 10 million lines of embedded code on the platform)

- 15 million on the ground-based Autonomic Logistics Information System (ALIS)).

- This contrasts with only five percent in a 1960-era F-4 fighter

Security Threats

- Spyware and Ad ware
- Viruses
- Phishing and Pharming
- Worms, Bots
- SQL injection
- Sophisticated targeted attacks
- Politically motivated attacks (Weaponized malware) - Stuxnet

Security Certification

- Certified Information System Security Professional (CISSP)

  https://www.isc2.org/Certifications/CISSP

- Cisco Certified Security Professional (CCSP)

  https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/security.html#~security-certifications

- Certified Ethical Hacking (CEH)

  https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

It’s going to get worse - 1

- Explosive growth of the Internet continues
  - continues to double in size every 10-12 months
  - where will all the capable system administrators come from?

- Market growth will drive vendors
  - time to market, features, performance, cost are primary
  - “invisible” quality features such as security are secondary

It’s going to get worse - 1

- The death of the firewall
  - traditional approaches depend on complete administrative control and strong perimeter controls
  - today’s business practices and wide area networks violate these basic principles
    - no central point of network control
    - more interconnections with customers, suppliers, partners
    - more network applications

It’s going to get worse - 1

- Beware of snake-oil
  - the market for security products and services is growing faster than the supply of *quality* product and service providers
  - sometimes the suppliers don’t understand Consumer needs

Before it gets better - 1

- Strong market for security professionals will eventually drive graduate and certificate programs.
- Increased understanding by technology users will build demand for quality security products; vendors will pay attention to the market.
- Insurance industry will provide incentives for improved business security practices.

Before it gets better - 1

- Technology will continue to improve and we will figure out how to use it
  - Encryption
  - strong authentication
  - survivable systems
- Increased collaboration across government and industry.

Sensible Security

- All security involves trade-offs
- Security trade-offs depend on power and agenda
- Security is a process and not a product
- Security is a game a never ending one

How Security Works

- You need to know systems and how they fail.
- Know the attackers
- Attackers never change their tunes, just their instruments
- Technology creates security imbalances
- Security is a weakest-link problem
- Security evolves around people
- Detection is useless without response
- Identification, authentication and authorization
- All countermeasures have some value, but no countermeasure is perfect

Computer Security

- The process of preventing and detecting unauthorized use of your computer.
- Attain the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

Key Security Concepts

- Confidentiality
- Integrity
- Availability

Level of Impact

- can define 3 levels of impact from a security breach
- Low
- Moderate
- High

Examples of Security Requirements

- Confidentiality – Student grades, Student enrolment, Staff Directory
- Integrity – patient information, Website Forum, Online poll.
- Availability – Bank authentication service, University Website, telephone directory

Computer Security Challenges

- Not simple
- Must consider potential attacks
- Involve algorithms and secret info
- Must decide where to deploy mechanisms
- Battle of wits between attacker / admin
- Requires regular monitoring

Security Areas

- Consumerization :
  - consumer devices will become trendier, cheaper, and more integrated
- Decentralization
  - increase use of cloud computing
- Deconcetration
  - special purpose hardware like iPhone
- Decustomerization:
  - get more IT function without any business relationship: free Google, Bing, Social, Networking sites etc

Vulnerabilities of the Internet

- The addressing system that finds out where to go on the internet for a specific address DNS
- The routing among ISPs, a systems known as the Border Gateway Protocol
- Almost everything that makes it work is open, unencrypted
- Its ability to propagate intentionally malicious traffic designed to attack computers
- It is one big network with a decentralised design

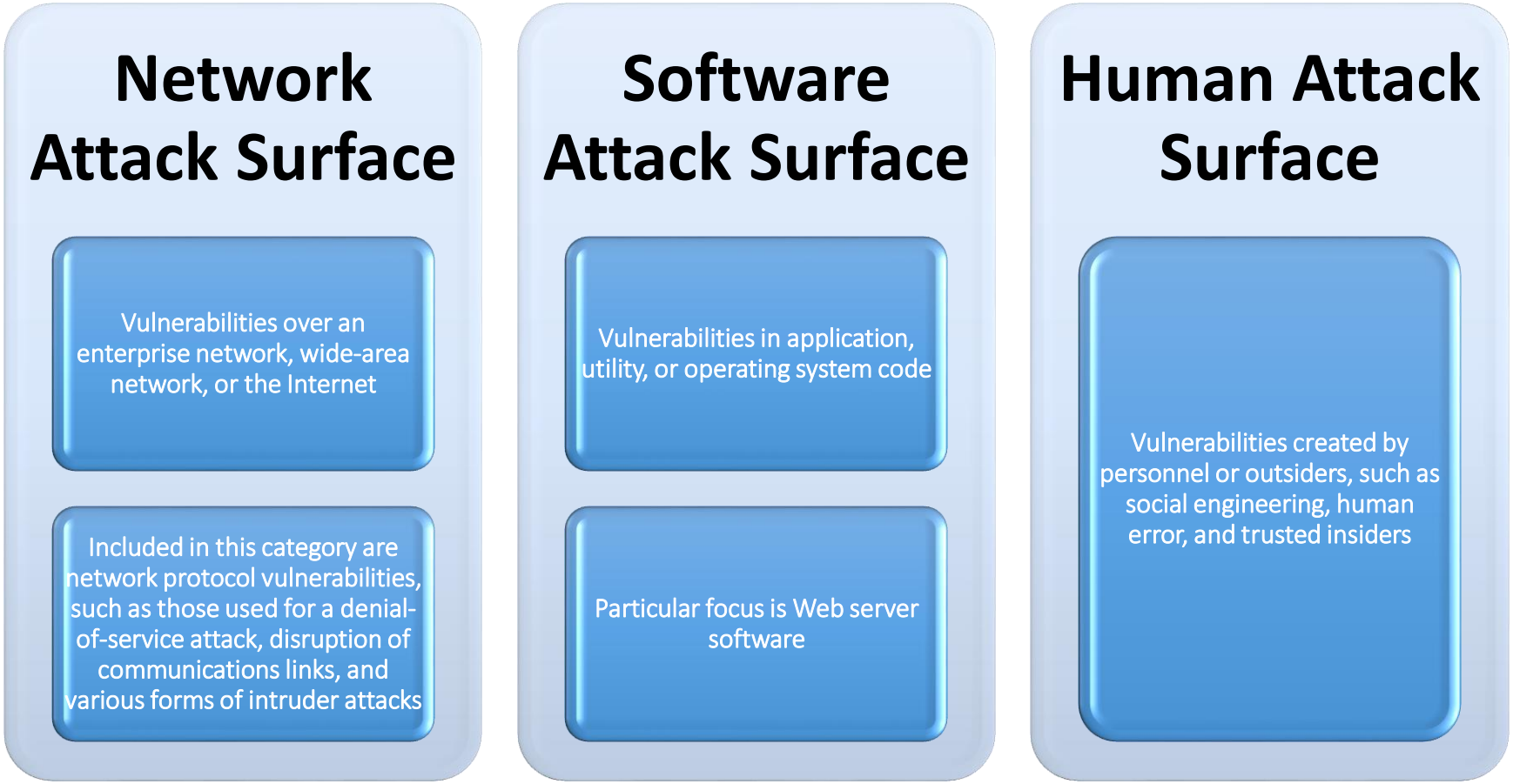
Attack Surfaces

Consist of the reachable and exploitable vulnerabilities in a system

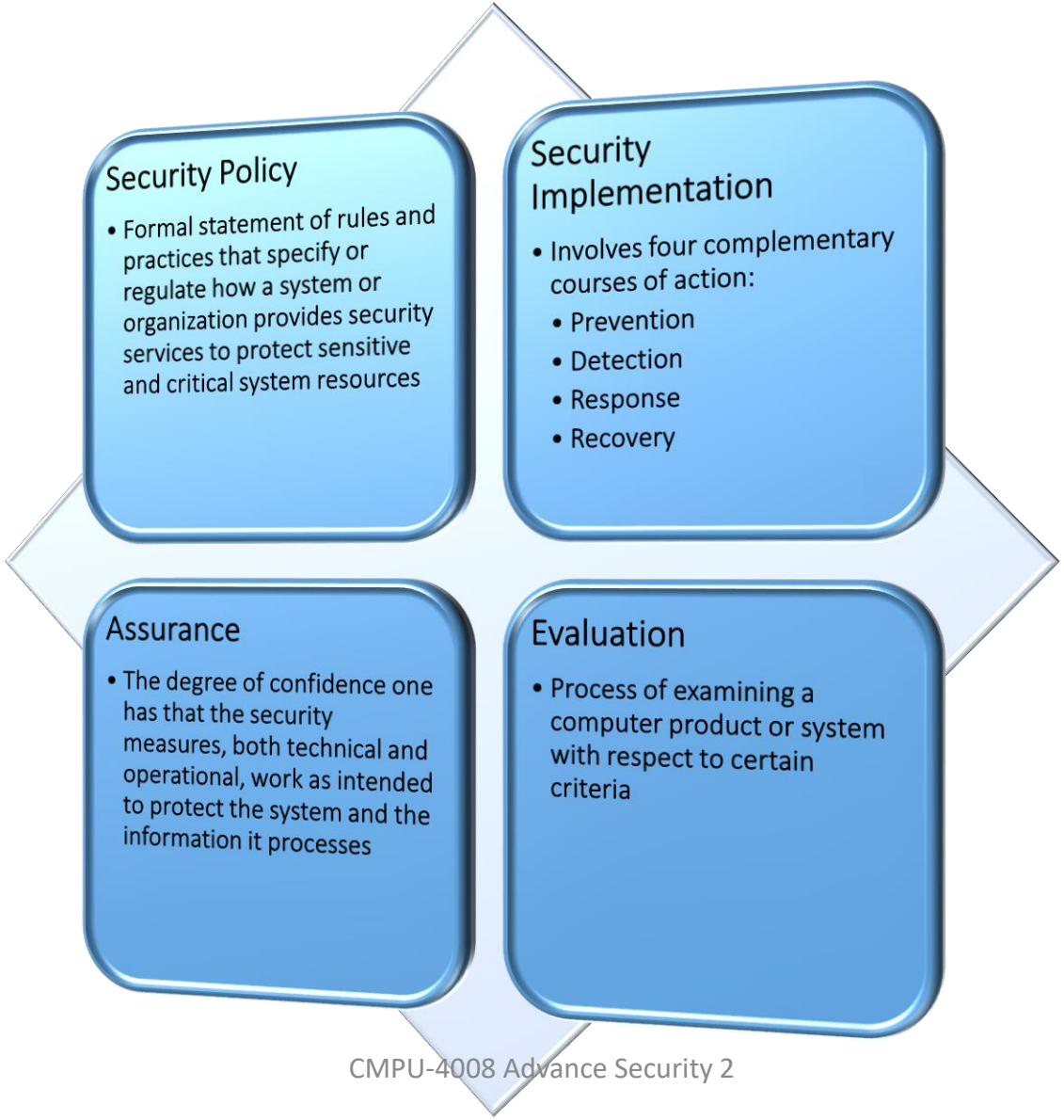
Examples:

- Open ports on outward facing Web and other servers, and code listening on those ports
- Services available on the inside of a firewall
- Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats
- Interfaces, SQL, and Web forms
- An employee with access to sensitive information vulnerable to a social engineering attack

Attack Surface Categories



Computer Security Strategy



Lecture 02
Google Hacking for Penetration Tester

CMPU-4008

Advance Security 2

Outline

- Google Introduction & Features
- Google Search Technique
- Google Basic Operators
- Google Advanced Operators

Google Hacking

- Google Search Technique
  - Just put the word and run the search
- You need to audit your Internet presence
  - One database, Google almost has it all!
- One of the most powerful databases in the world
- Usage:
  - Business …
  - One stop shop for attack, maps, addresses, photos, technical information

Google Hacking

- Google Advance Search
  - A little more sophisticated ……

- Google hacking is the term used when a hacker tries to find vulnerable targets or sensitive data by using the Google search engine.


Google
Advanced Search
Advanced Search Tips | About Google
Find results
with all of the words
with the exact phrase
with at least one of the words
without the words
10 results
Google Search
Language
Return pages written in
any language
File Format
Only
return results of the file format
any format
Date
Return web pages first seen in the
anytime
Occurrences
Return results where my terms occur
anywhere in the page
Domain
Only
return results from the site or domain
e.g. google.com, .org More info
Usage Rights
Return results that are
not filtered by license
More info
SafeSearch
No filtering
Filter using SafeSearch

Google Operators

- Operators are used to refine the results and to maximize the search value.

  They are your tools as well as hackers' weapons.

- Basic Operators:
  - +, -, ~ , ., *, "", |, OR
- Advanced Operators:
  - allintext:, allintitle:, allinurl:, bphonebook:, cache:, define:, filetype:, info:, intext:, intitle:, inurl:, link:, phonebook:, related:, rphonebook:, site:, numrange:, daterange

Basic Operators

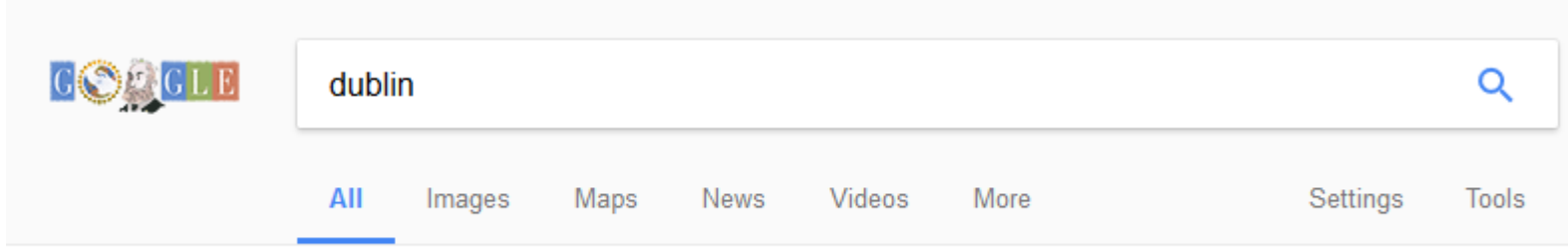
- (+) force inclusion of something common
- Google ignores common words (where, how, digit, single letters) by default:
  - Example: StarStar Wars Episode +I
- (-) exclude a search term
  - Example: apple -red
- (“) use quotes around a search term to search exact phrases:
  - Example: “Aneel Rahim”
  - Aneel Rahim without “” has the 35,900 results, but “Aneel Rahim” only has 742 results. Reduce the 99% irrelevant results

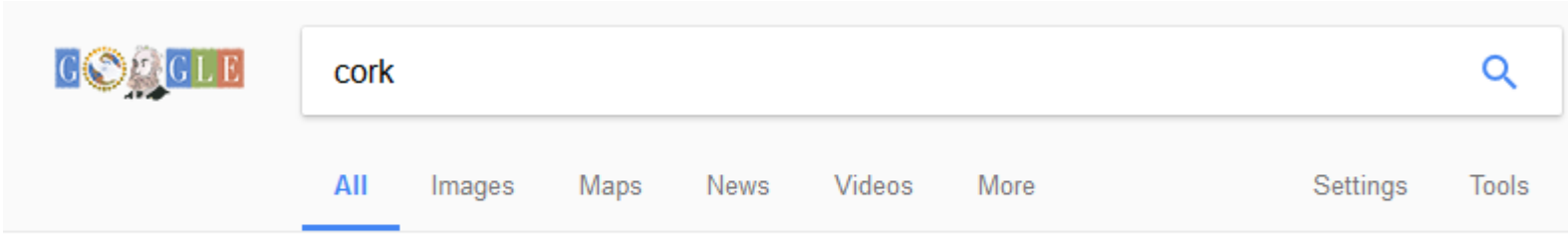
Basic Operators

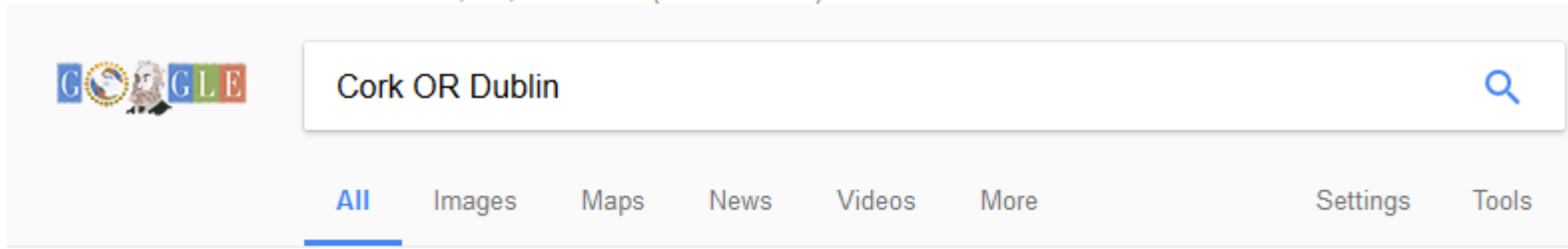
- **(~) search synonym:**
  - Example: ~food
- Return the results about food as well as recipe, nutrition and cooking
- **(.) a single-character wildcard:**
  - Example: m.trix
- Return the results of M@trix, matrix, metrix…….

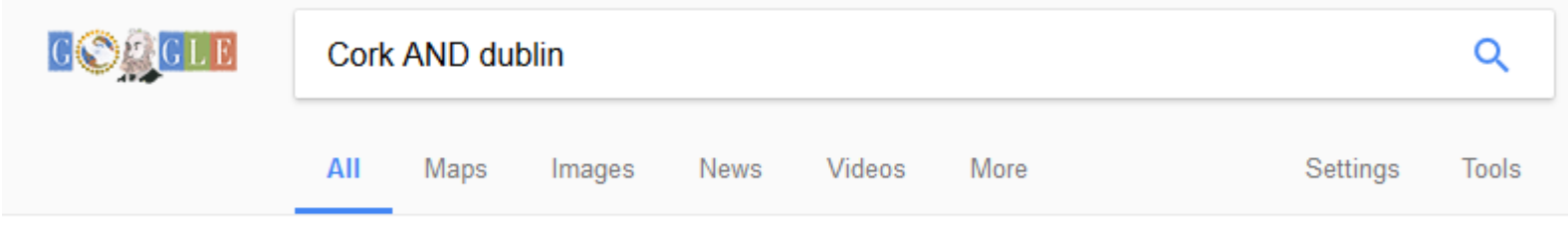
Basic Operators

- **(*) any word wildcard**
  - For example, **invit*** returns both invitation and invite
- **(AND)** Searches for results that include both the term before and the term after the operator.
- **(OR)** Searches for results that include either the term before or the term after the operator (or both).


dublin
All
Images
Maps
News
Videos
More
Settings
Tools
About 217,000,000 results (0.97 seconds)


cork
All
Images
Maps
News
Videos
More
Settings
Tools
About 128,000,000 results (0.80 seconds)


Cork OR Dublin
All
Images
Maps
News
Videos
More
Settings
Tools
About 343,000,000 results (0.54 seconds)


Cork AND dublin
All
Maps
Images
News
Videos
More
Settings
Tools
About 42,500,000 results (0.57 seconds)

Advanced Operators at a Glance

Advanced operators can be combined in some cases.

In other cases, mixing should be avoided.

Some operators can only be used to search specific areas of Google, as these columns show.

Operator	Purpose	Mixes with other operators?	Can be used alone?	Does search work in			
				Web	Images	Groups	News
intitle	Search page title	yes	yes	yes	yes	yes	yes
allintitle	Search page title	no	yes	yes	yes	yes	yes
inurl	Search URL	yes	yes	yes	yes	not really	like intitle
allinurl	Search URL	no	yes	yes	yes	yes	like intitle
filetype	Search specific files	yes	no	yes	yes	no	not really
allintext	Search text of page only	not really	yes	yes	yes	yes	yes
site	Search specific site	yes	yes	yes	yes	no	not really
link	Search for links to pages	no	yes	yes	no	no	not really
inanchor	Search link anchor text	yes	yes	yes	yes	not really	yes
numrange	Locate number	yes	yes	yes	no	no	not really
daterange	Search in date range	yes	no	yes	not really	not really	not really
author	Group author search	yes	yes	no	no	yes	not really
group	Group name search	not really	yes	no	no	yes	not really
insubject	Group subject search	yes	yes	like intitle	like intitle	yes	like intitle
msgid	Group msgid search	no	yes	not really	not really	yes	not really

Advance Operators

- **Advance Operator: “Site:”**
- Get results from certain sites or domains.
  - Example: **olympics site:nbc.com**
- To get results from multiple sites or domains, combine with **OR**
  - Example: **Olympics site:nbc.com OR site:.gov**

Olympics site:nbc.com

All Images Videos News Maps More Settings Tools

About 3,420 results (0.30 seconds)

2016 Rio Olympics - NBC.com
www.nbc.com/**olympics**
Commonly known as Rio 2016, the Games of the XXXI Olympiad in Rio de Janeiro, Brazil, mark a historic first time that the **Olympics** are held in South America, ...

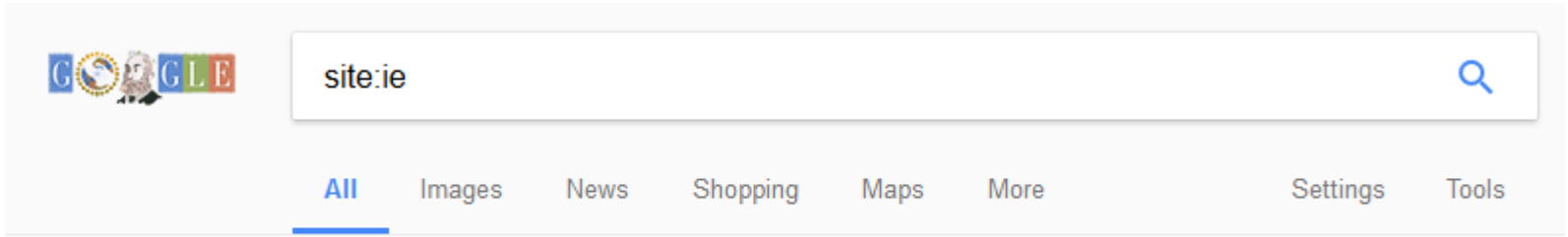
2016 Rio Olympics: 2016 Olympic Trials Photo: 2908958 - NBC.com
www.nbc.com/**olympics**/photos/2016-**olympic**-trials/2908958
Aug 8, 2016 - View photos from 2016 Rio **Olympics** 2016 **Olympic** Trials on NBC.com.

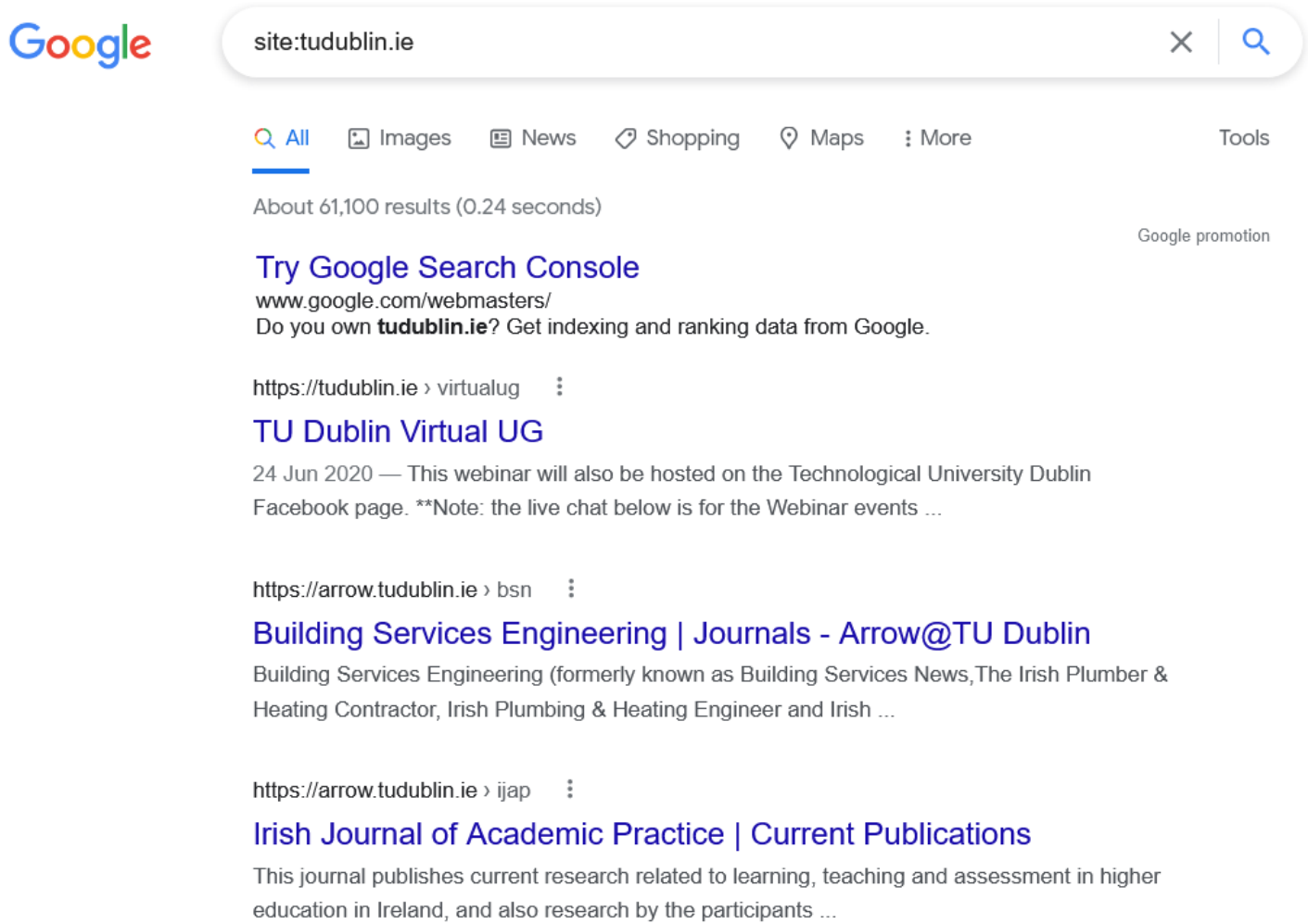
Monologue Image: 2016 Olympics - The Tonight Show - NBC.com
www.nbc.com/the-tonight-show/photo/monologue-image-2016-**olympics**/5871
The International **Olympic** Committee is now considering London as a backup host city for the 2016 **Olympics** if Rio isn't ready. So I'd like to officially congratulate ...

Superstore: Olympics Photo: 2908360 - NBC.com
www.nbc.com/superstore/photos/**olympics**/2908360
View photos from Superstore **Olympics** on NBC.com.

Advance Operators

- Advance Operator: “Site:”
- Examples:
  - site:ie
  - site:tudublin.ie


site:ie
All
Images
News
Shopping
Maps
More
Settings
Tools
About 469,000,000 results (0.31 seconds)


Google
site:tudublin.ie
All
Images
News
Shopping
Maps
More
Tools
About 61,100 results (0.24 seconds)
Google promotion
Try Google Search Console
www.google.com/webmasters/
Do you own tudublin.ie? Get indexing and ranking data from Google.
https://tudublin.ie › virtualug
TU Dublin Virtual UG
24 Jun 2020 — This webinar will also be hosted on the Technological University Dublin Facebook page. **Note: the live chat below is for the Webinar events ...
https://arrow.tudublin.ie › bsn
Building Services Engineering | Journals - Arrow@TU Dublin
Building Services Engineering (formerly known as Building Services News,The Irish Plumber & Heating Contractor, Irish Plumbing & Heating Engineer and Irish ...
https://arrow.tudublin.ie › ijap
Irish Journal of Academic Practice | Current Publications
This journal publishes current research related to learning, teaching and assessment in higher education in Ireland, and also research by the participants ...

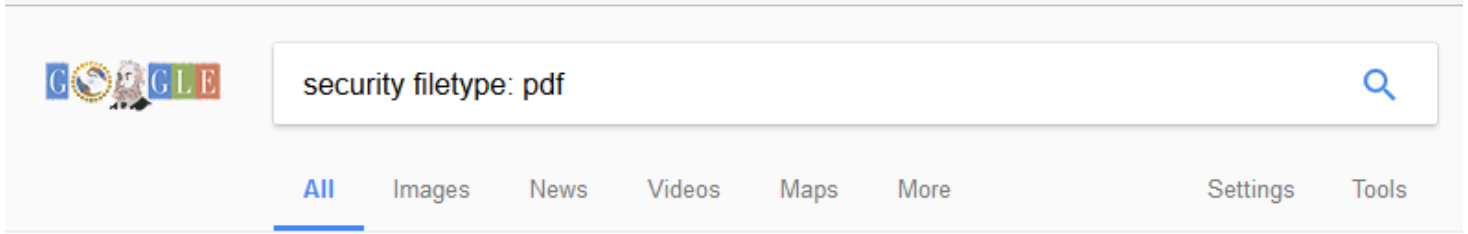
Advance Operators

- **Advanced Operators: “Filetype:”**
- Google searches more than just Web pages.
- Google can search many different types of files, including PDF (Adobe Portable Document Format) and Microsoft Office documents
- Filetype: extension_type

Advance Operators

The Main File Types Google Searches

File Type	File Extension
Adobe Portable Document Format	Pdf
Adobe PostScript	Ps
Lotus 1-2-3	wk1, wk2, wk3, wk4, wk5, wki, wks, wku
Lotus WordPro	Lwp
MacWrite	Mw
Microsoft Excel	Xls
Microsoft PowerPoint	Ppt
Microsoft Word	Doc
Microsoft Works	wks, wps, wdb
Microsoft Write	Wri
Rich Text Format	Rtf
Shockwave Flash	Swf
Text	ans, txt


security filetype: pdf
All
Images
News
Videos
Maps
More
Settings
Tools
About 638,000 results (0.29 seconds)
[PDF] Introduction to Network Security - Interhack
www.interhack.net/pubs/network-security.pdf
by M Curtin - 1997 - Cited by 47 - Related articles
Introduction to Network Security. Matt Curtin". March 1997. Reprinted with the permission of Kent Information Services, Inc. Abstract. Network security is a ...
[PDF] Introduction to Computer Security
its.ucsc.edu/security/training/docs/intro.pdf
4. Why is Computer Security. Important? Computer Security allows the. University to carry out its mission by: ○ Enabling people to carry out their jobs, education ...
[PDF] Network Security: History, Importance, and Future - MIT
web.mit.edu/~bdaya/www/Network%20Security.pdf
by B Daya - Cited by 27 - Related articles
The entire field of network security is vast and in an evolutionary stage. ..... www. infosecwriters.com/text_resources/pdf/IPv6_SSot illo.pdf. [6] Andress J., "IPv6: ...
[PDF] the NIST Handbook - NIST Computer Security Resource Center
csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
by A User - 1995 - Related articles
nist special Publication 800-12. An Introduction to Computer. Security: The NIST Handbook. U.S. DEPARTMENT OF. COMMERCE. Technology Administration.
[PDF] security in-a-box
https://securityinabox.org/sites/securitybkp.ngoinabox.org/security/booklet-en.pdf
Remembering and recording secure passwords 35. 4. How to protect ... Advocates are increasingly concerned about their digital security, and with good reason.

Advance Operators

- *filetype:xls username password email*
- Microsoft Excel spreadsheets containing the words *username, password*, and *email.*
- Read Criminal Justice (Offences Relating to Information Systems) Bill 2016 (http://www.oireachtas.ie/documents/bills28/bills/2016/1016/b1016d.pdf)
- Please do not practice this one, This is just for learning purpose.

filetype:xls username password email

All News Images Videos Maps More Settings Tools

About 4,950 results (0.22 seconds)

[XLS] **Using the Social Media Account Tracker**
cdn2.hubspot.net/hub/215313/file-499131210-xls
For a lot of social media accounts the **login** is the **email** address. ... Why wouldnt you just give them the primary **email** and **password** to access your Facebook ...

[XLS] **GUCCIFER-2016-cycle-passwords**
https://guccifer2.files.wordpress.com/2016/08/2016-cycle-**passwords**.xls
7, **Login**, **Password**, GO TO: www.tveyes.com. 8, Matsdorf@dccc.org ... 1, Customer ID, **Login**, **Password**. 2, 623040 ... 1, **Email**, **Password**. 2, padilla@dccc.org ...

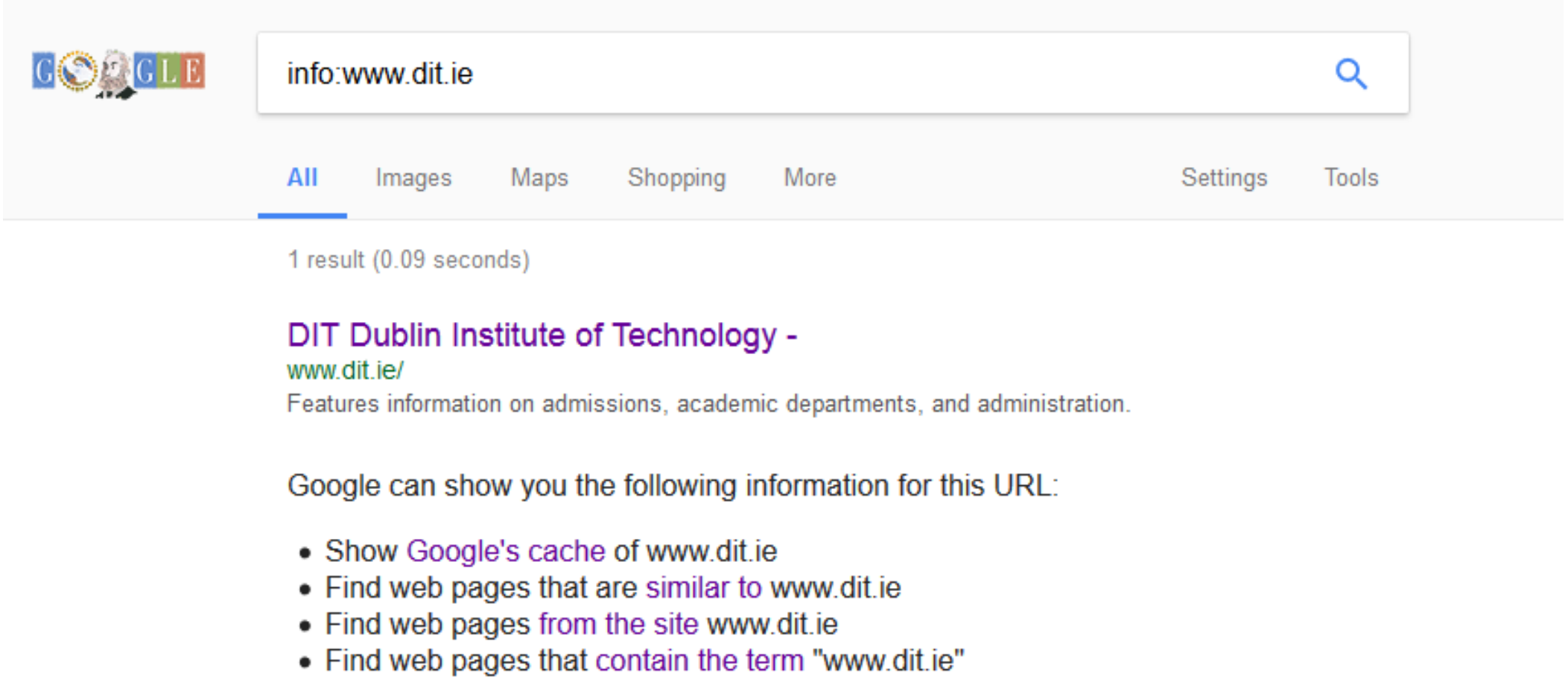
[XLS] **email address from username - Moodle**
https://moodle.org/pluginfile.php/183/mod_forum/.../**user**-account-creation_2.xls
1, **username**, **password**, firstname, lastname, **email**. 2, 0000111, changeme, john, smith, 0000111@citycol.com. 3. **username** from fname-lname. A, B, C, D, E.

[XLS] **17651_Copy of All Paid Accounts 07232007.xls - WikiLeaks**
https://wikileaks.org/.../17651_Copy%20of%20All%20Paid%20Accounts%20072320...
1, **username**, **password**, first_name, last_name, **email**, email_format, daily_email, address1, address2, city, state, province, country, postal_code, telephone ...

Advance Operators

- **Advanced Operators: “info:website”**
- Using this operator will tell Google to bring back information about a certain domain. It reveals:
  - Google’s cache of the site
  - Pages that are similar to the one you searched for
  - Pages that link to the domain you searched for
  - Other pages on the same domain
  - Pages that contain the domain text on their page

Advance Operators



Advance Operators

- Advanced Operators “Intitle:”
- Intitle: search_term
  - Find search term within the title of a Webpage
- Allintitle: search_term1 search_term2 search_term3
  - Find multiple search terms in the Web pages with the title that includes all these words
- These operators are specifically useful to find the directory lists
- Example:
  - **intitle:Google** This query will return pages that have the word Google in their title
  - **Intitle: Index.of “parent directory”** It find the directory list

Intitle: Index.of “parent directory”

All Images News Videos Shopping More Tools

About 189,000 results (0.29 seconds)

https://www.ieee802.org › files › public

Index of /1/files/public - IEEE 802

Index of /1/files/public. Icon Name Last modified Size Description. [PARENTDIR] **Parent Directory** - [DIR] 802-1-assigned-numbers/ 2021-07-20 14:34 - [DIR] ...

https://www.ucd.ie › phps

Index of /phps

Index of /phps. [ICO], Name · Last modified · Size · Description. [PARENTDIR], **Parent Directory**, -. [DIR], CVM 1 PMC Cardiovascular Disease (1) Session 1 ...

intitle index of "parent directory" games

All Images News Videos Maps More Settings Tools

About 79,600 results (0.36 seconds)

Index of /~archive/atari/Games
umich.edu/~archive/atari/Games/
Parent Directory - 0index 16-Mar-1997 01:30 32K Adventure/ 27-Nov-1995 15:49 - Arcade/ 28-Jan-1996 18:15 - Board/ 27-Jul-1995 12:43 - Cards/ 20-Jul-1995 ...

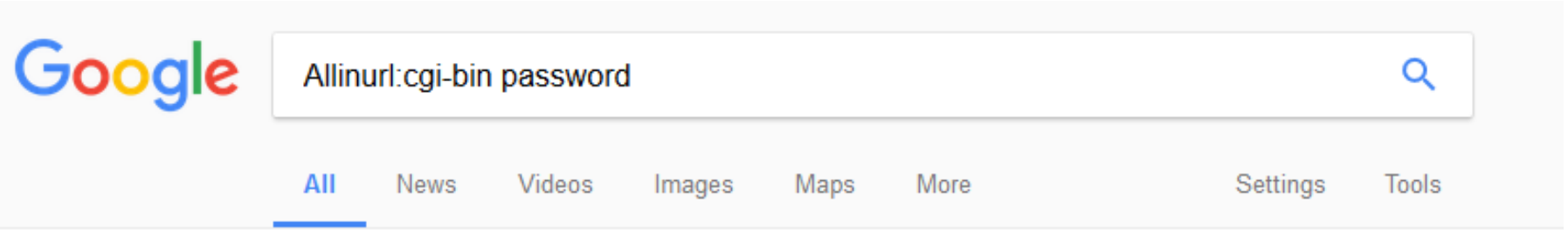
Index of /Shareware/Games/ - Pacsteam.org
pacsteam.org/Shareware/Games/
Index of /Shareware/**Games**/ ... up **Parent Directory** 01-Nov-2017 11:05 - directory ... Farm Frenzy - Four **Games** In One Pack 18-Sep-2013 02:19 - directory ...

Index of /games/
dl3.freegames.ir/games/
Parent directory/, -, -. 100ft-Robot-Golf-CODEX-www.FreeGames.iR.part1.rar, 1.0 GiB, 2017-Mar-30 01:01. 100ft-Robot-Golf-CODEX-www.FreeGames.iR.part2.

Index of /pub4/sourceforge/a/ah/ahmedateeqzia/games - Last modified
download2.nust.na/pub4/sourceforge/a/ah/ahmedateeqzia/games/
[PARENTDIR], **Parent Directory**, -. [ ], Age of Empires 2 setup.exe, 2014-06-05 02:50, 185M. [ ], Age of Mythology Gold Edition setup.exe, 2014-07-14 05:44 ...

Advance Operators

- Advanced Operators “Inurl:”
  - Inurl: search_term
- Find search term in a Web address
  - Allinurl: search_term1 search_term2 search_term3
- Find multiple search terms in a Web address
- Examples:
  - Inurl:cgi-bin
  - Allinurl:cgi-bin password (It provides access of password file of web applications)


Google
Allinurl:cgi-bin password
All
News
Videos
Images
Maps
More
Settings
Tools
About 9,800 results (0.46 seconds)
Index of /staff/tydesjo/physics/workarea/cgi-password/cgi-bin
www.hep.lu.se/staff/tydesjo/physics/workarea/cgi-password/cgi-bin/
Index of /staff/tydesjo/physics/workarea/cgi-password/cgi-bin. Icon Name Last modified Size Description. [DIR] Parent Directory - [ ] password.pl 09-Dec-2003 14:20 1.7K. Apache/2.2.15 (Linux/SUSE) Server at www.hep.lu.se Port 80.
The definitive super list for "Google Hacking". · GitHub
https://gist.github.com/cmartinbaughman/5877945
inurl:/wwwboard. inurl:/yabb/Members/Admin.dat. inurl:ccbill filetype:log. inurl:cgi-bin inurl:calendar.cfg. inurl:chap-secrets -cvs. inurl:config.php dbuname dbpass. inurl:filezilla.xml -cvs. inurl:lilo.conf filetype:conf password -tatercounter2000 -bootpwd -man. inurl:nuke filetype:sql. inurl:ospfd.conf intext:password -sample -test ...
[PDF] Google Hacking (Kind of)
fleming0.flemingc.on.ca/~blbrown/Google%20Hacking%20Lesson.pdf
Advanced Operators "Inurl:". – Inurl: search_term. – Find search term in a Web address. – Allinurl: search_term1 search_term2 search_term3. – Find multiple search terms in a Web address. – Examples: Inurl: cgi-bin. Allinurl: cgi-bin password. •. •Google Hacking ...

Advance Operators

- Advanced Operators “Intext;”
- Intext: search_term
  - Find search term in the text body of a document.
- Allintext: search_term1 search_term2 search_term3
  - Find multiple search terms in the text body of a document.
- Examples:
  - Intext: Administrator login

Google

Intext:Administrator login

All Images Videos News Shopping More Settings Tools

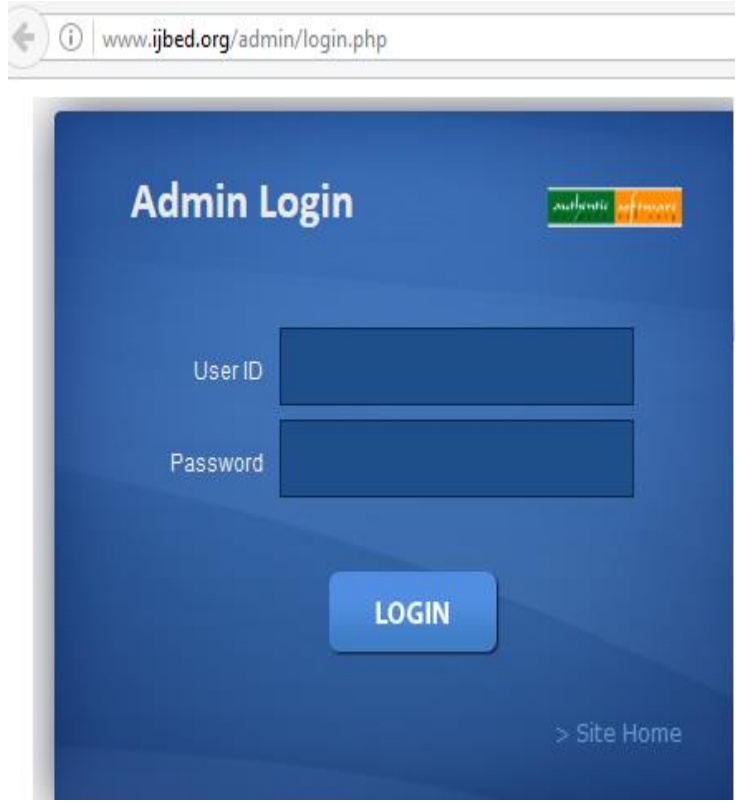
About 1,170,000 results (0.37 seconds)

Admin Login
https://admin.lavu.com/ ▾
Forgot Password? | Terms of Service By continuing, you are agree to our Terms of Service. Forgot Password. Username. Back to **Login** | Terms of Service By continuing, you are agree to our Terms of Service. Reset Password. Username. New Password. Confirm Password. Back to **Login** | Terms of Service By continuing ...

Administration Login - Adobe Business Catalyst
https://www.businesscatalyst.com/adminconsole/ ▾
Email Address: Password: Lost your password?

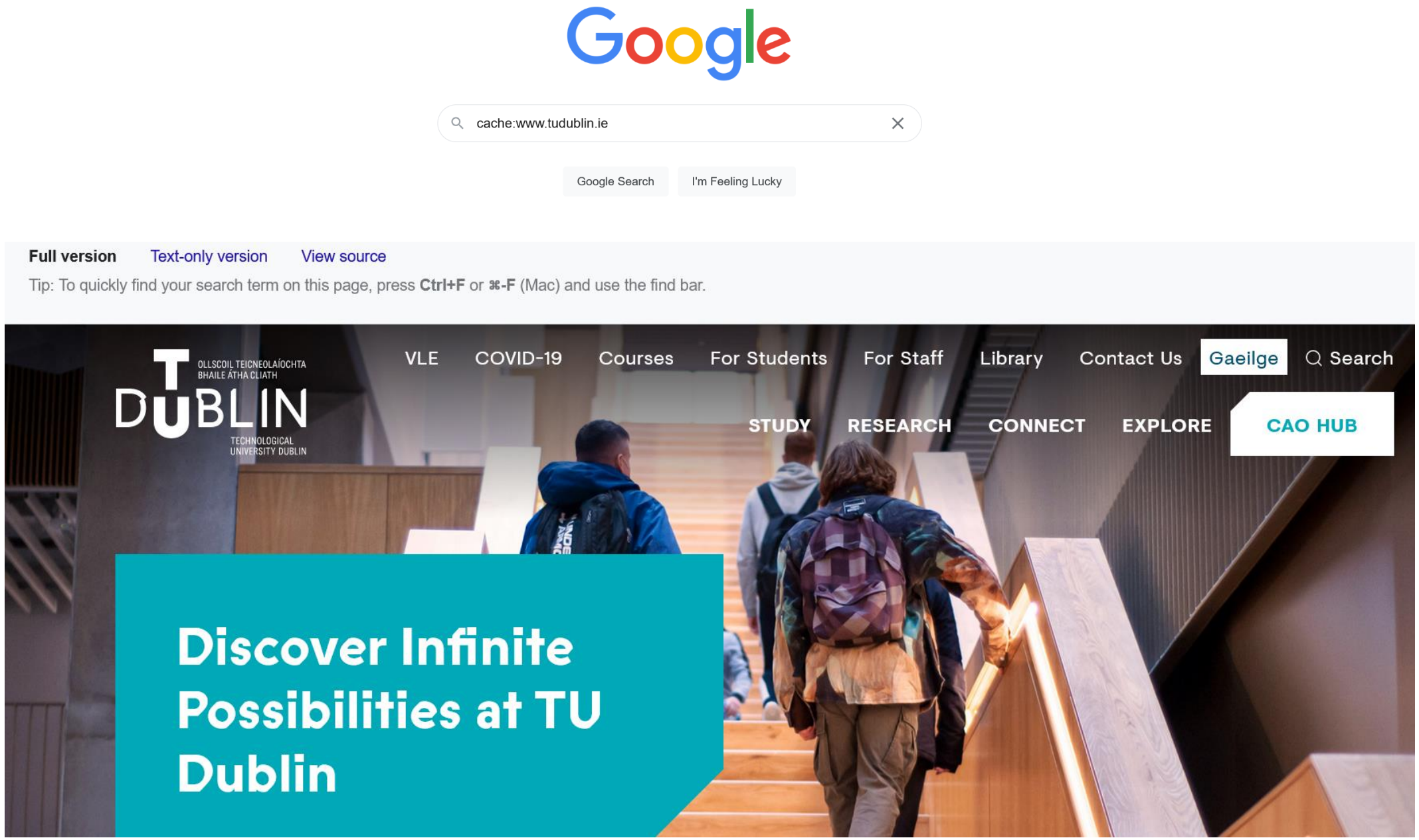
Admin Login
https://www.iitk.ac.in/hall7/admin.php ▾
Home · About Hall7; HEC. Wardens · Student HEC · Hall Office Staff · Hall Residents; Facilities. Mess · Canteen · Reading Room · TV Room · Computer Room · Games And Sports · Music Room · Gymnasium · Garden · Guest Room · Hall ShopC · Hall Bicycles. Events. Hall Day · Saraswati Puja · Diwali · Rush'08.

Admin - Login - phpSocial
https://phpsocial.com/demo/index.php?a=admin ▾
Admin Login. Username. Type in your **Admin** Username. Password. Type in your **Admin** Password. username: **admin** password: password (Note: no changes will be saved, this is just a demo). Share.



Advance Operators

- Advanced Operators: “Cache:”
- cache: URL
- Find the old version of Website in Google cache
- Sometimes, even the site has already been updated, the old information might be found in cache
- Examples:
  - cache:www.tudublin.ie


Google
cache:www.tudublin.ie
Google Search
I'm Feeling Lucky
Full version
Text-only version
View source
Tip: To quickly find your search term on this page, press Ctrl+F or ⌘-F (Mac) and use the find bar.
OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN
VLE
COVID-19
Courses
For Students
For Staff
Library
Contact Us
Gaeilge
Search
STUDY
RESEARCH
CONNECT
EXPLORE
CAO HUB
Discover Infinite Possibilities at TU Dublin

Advance Operators

- Advanced Operators
- <number1>..<number2>
- Conduct a number range search by specifying two numbers, separated by two periods, with no spaces. Be sure to specify a unit of measure or some other indicator of what the number range represents
- Examples:
  - Computer $500..1000
  - DVD player $250..350
  - boys clothes 2y..10

Computer $500..1000

All | Images | Maps | News | Videos | More | Settings | Tools

Inspiron

For home and home office

Micro desktops, small desktops and desktops featuring Intel® Core™ processors and AMD processors and plenty of storage space for the latest entertainment and productivity features.

Learn more

Desktops
Starting at $279.99

Small Desktop | Desktops

With the large hard drives and expandability of the Inspiron Desktop, you'll never be pressed for storage space. Space-saving desktop design perfect for small spaces and ideal for expandability.

3000 Series All-in-One
Starting at $349.99

20" | New 22" | 24"

Space-saving all-in-one desktops with easy, all-in-one set-up. Featuring AMD or Intel® processors and wide-screen viewing.

5000 Series All-in-One
Starting at $699.99

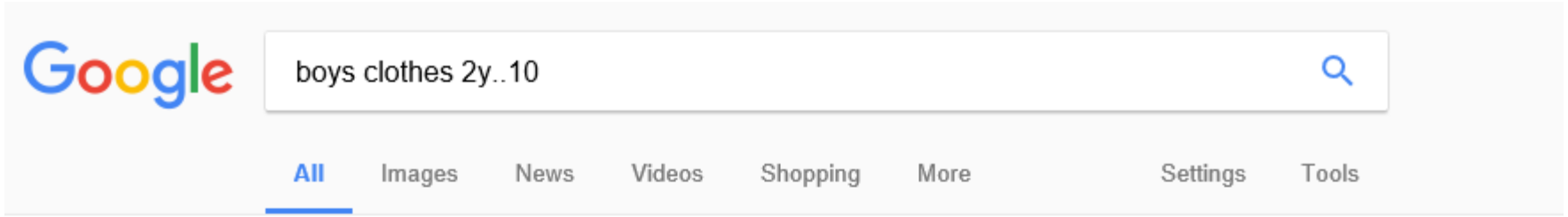
24"

Powerful, 24-inch all-in-one desktop with rich multimedia features.

7000 Series All-in-One
Starting at $799.99

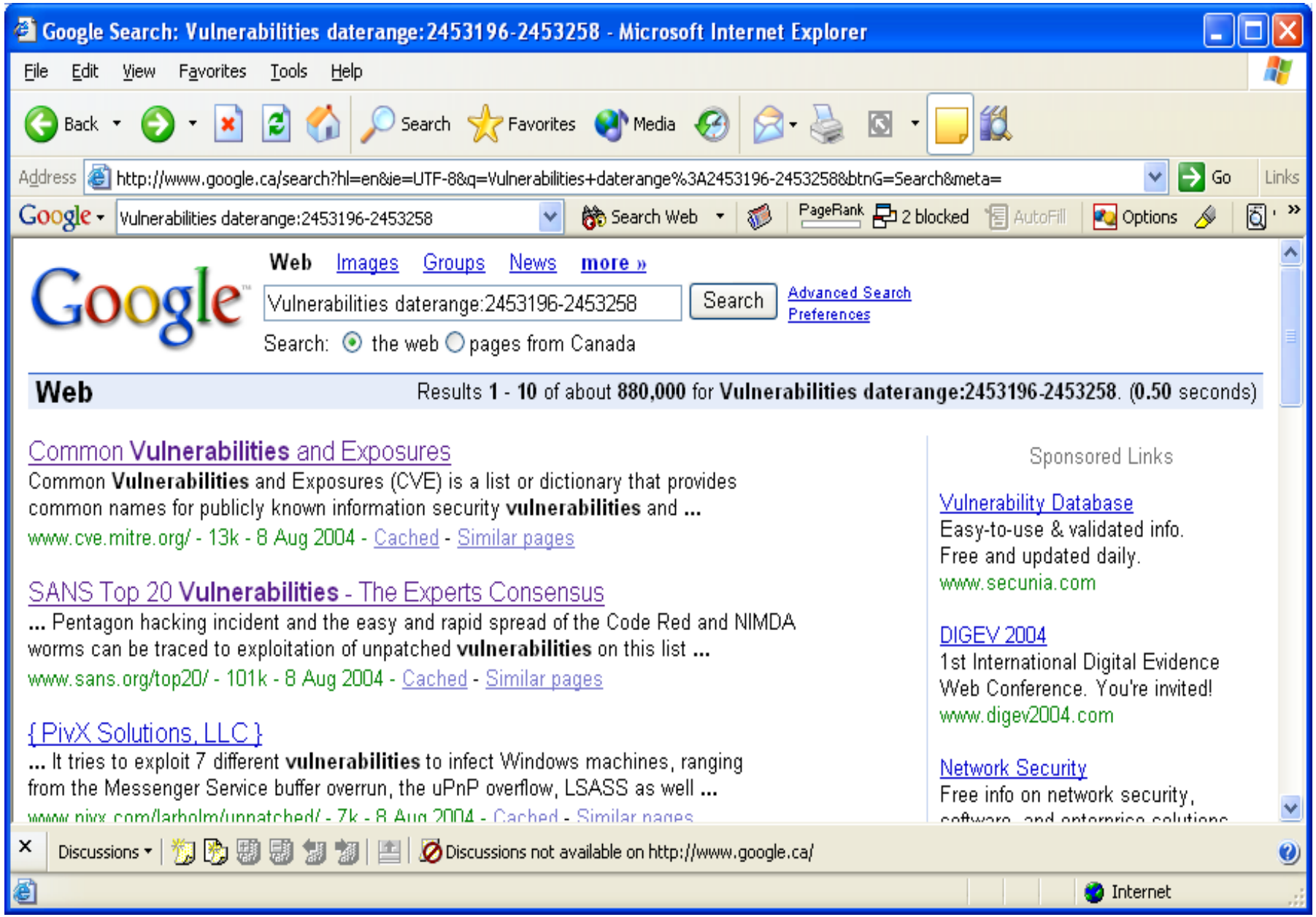
24"

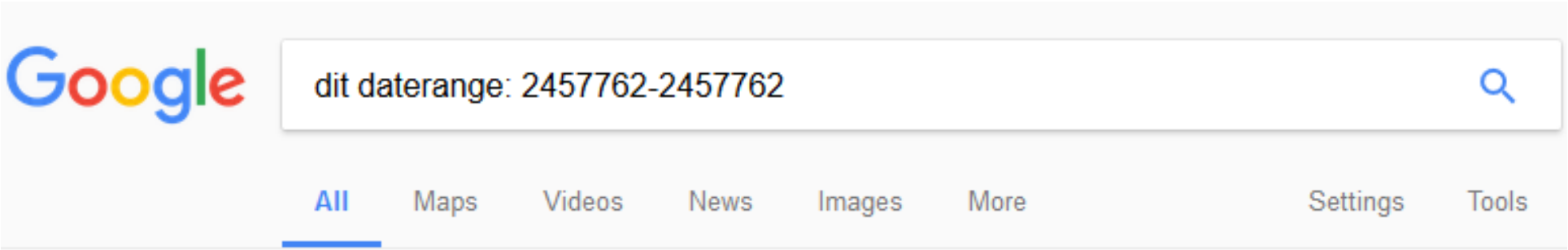
Ultrathin 24-inch all-in-one is designed to impress with an Intel® RealSense™ Camera and Windows Hello.


Google
boys clothes 2y..10
All
Images
News
Videos
Shopping
More
Settings
Tools
About 9,080,000 results (0.66 seconds)
Boys Clothes - 1½ - 10 years - Shop online | H&M
www2.hm.com/en_ie/kids/shop-by-product/boys-size-18m-8y.html
Comfy, practical and bursting with vibrant colours and charming prints – we have clothes and accessories for your boy's every need.
Boys Clothes - 1½ - 10 years - Shop online
www2.hm.com/en_ie/kids/shop-by.../boys-size-18m-8y.mobileapp.html?offset...
Boys 1½-10 years. Back to top Back to start. Category. Boys 1½-10 years (). All. Accessories. Best Basics. Blazers & Waistcoats. Cartoons & Comics. Fancy dress.
Children Pajamas Cotton Dinosaur Kids Clothes Boys Size 2Y-10Y ...
amazin-movers-and-shakers.com/.../children-pajamas-cotton-dinosaur-kids-clothes-bo...
Children Pajamas Cotton Dinosaur Kids Clothes Boys Size 2Y-10Y. $27.99 (as of December 12, 2016, 2:49 pm). 100% cotton,soft and comfortable. Long sleeve ...
Boys 2y-10y | Lola and the Boys
https://lolaandtheboys.com/product-category/boys/
Boys Ballin Paris Shirt. $18.00 Select options · Boys Patchwork Jeans ... BOYS SHIRTS SIZE 8-10 · CUSTOM BOY CLOTHES · Custom Dresses · Featured Back ...

Advance Operators

- Advanced Operators: “Daterange:”
- Daterange: <start_date>-<end date>
- Find the Web pages between start date and end date
- Note: start_date and end date use the Julian date
- The Julian date is calculated by the number of days since January 1, 4713 BC. For example, the Julian date for August 1, 2001 is 2452122
- Examples:
  2004.07.10=2453196
  2004.08.10=2453258
- Vulnerabilities date range: 2453196-2453258


Google Search: Vulnerabilities daterange:2453196-2453258 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?hl=en&ie=UTF-8&q=Vulnerabilities+daterange%3A2453196-2453258&btnG=Search&meta=
Go Links
Google Vulnerabilities daterange:2453196-2453258
Search Web PageRank 2 blocked AutoFill Options
Web Images Groups News more »
Google
Vulnerabilities daterange:2453196-2453258
Search
Advanced Search
Preferences
Search: the web pages from Canada
Web
Results 1 - 10 of about 880,000 for Vulnerabilities daterange:2453196-2453258. (0.50 seconds)
Common Vulnerabilities and Exposures
Common Vulnerabilities and Exposures (CVE) is a list or dictionary that provides common names for publicly known information security vulnerabilities and ...
www.cve.mitre.org/ - 13k - 8 Aug 2004 - Cached - Similar pages
SANS Top 20 Vulnerabilities - The Experts Consensus
... Pentagon hacking incident and the easy and rapid spread of the Code Red and NIMDA worms can be traced to exploitation of unpatched vulnerabilities on this list ...
www.sans.org/top20/ - 101k - 8 Aug 2004 - Cached - Similar pages
{ PivX Solutions, LLC }
... It tries to exploit 7 different vulnerabilities to infect Windows machines, ranging from the Messenger Service buffer overrun, the uPnP overflow, LSASS as well ...
Sponsored Links
Vulnerability Database
Easy-to-use & validated info.
Free and updated daily.
www.secunia.com
DIGEV 2004
1st International Digital Evidence Web Conference. You're invited!
www.digev2004.com
Network Security
Free info on network security,
Discussions
Discussions not available on http://www.google.ca/
Internet



Your search - **dit daterange: 2457762-2457762** - did not match any documents.

Suggestions:

- Make sure that all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

Advance Operators

- Advanced Operators “Link:”
- Link: URL
  - Find the Web pages having a link to the specified URL
- Related: URL
  - Find the Web pages that are “similar” to the specified Web page
- Define: search_term
  - Provide a definition of the words gathered from various online sources
- Examples:
  - Link:tudublin.ie
  - Related:dit.ie
  - Define:network security

https://tudublin.ie › for-students › student-login

Student Login | TU Dublin

As a student of **TU Dublin** you are entitled to the use of a wide range of services including email, Wi-Fi, print services, data storage, software and much ...

https://tudublin.ie › for-students › starting-at-tu-dublin › g...

Getting Online | TU Dublin

For access to Moodle, Tallaght students should use this **link** https://elearning-ta.**tudublin.ie** while those in Blanchardstown can visit the LMS here ...

6 Sept 2021 · Uploaded by IS Support

https://tudublin.ie › for-staff › city-centre

City Centre Login | TU Dublin

Staff Login · Username: firstname.lastname@**tudublin.ie** · Username: staffnumber · Business Apps · Useful **Links** · Privacy Preference Center.

https://tudublin.ie › how-to-apply › entry-pathways › a...

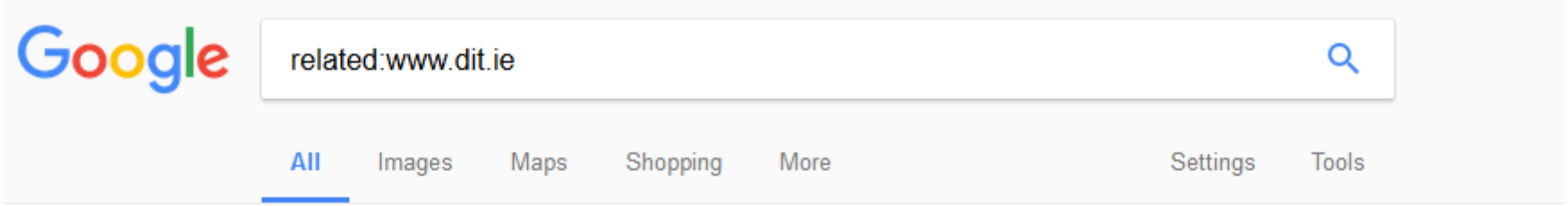
Access TU Dublin

Application Support from **TU Dublin** Access Service staff; Reduced points CAO ... The information in the **link** below is correct as of the 17th August 2021:.

https://www.tudublin.ie › student-services-and-support

Registration | TU Dublin

Welcome to Registration for **TU Dublin**. We manage the registration and fee payment process for students on your programme and modules. Useful **Links**.



About 46 results (0.13 seconds)

University College Dublin
www.ucd.ie/
This website uses cookies, by continuing you agree to their use. Learn more about cookies and how to manage them on cookie policy. Close. It appears JavaScript is disabled. To get the most out of the website we recommend enabling JavaScript in your browser. Home · Current Students · Alumni · Community · News and ...

Waterford Institute of Technology
https://www.wit.ie/
Waterford Institute of Technology (WIT) is a university-level institution in the South-East of Ireland with over 10000 students and 1000 staff. WIT offers tuition and research programmes in various areas from Higher Certificate to Degree to PhD.

Trinity College Dublin, the University of Dublin, Ireland
https://www.tcd.ie/
Cookies on the Trinity College Dublin website. By using this website you consent to the use of cookies in accordance with the Trinity cookie policy. OK. Skip to main content. Trinity College Dublin, The University of Dublin. Menu Search. Trinity Search. Your query. Search collection. All Trinity, Undergraduate Courses ...

NUI Galway - NUI Galway
www.nuigalway.ie/
Dr Elaine Toomey and Dr David Mothersill from the School of Psychology at NUI Galway, have both

Google

Define:network security

All Images News Videos Shopping More Settings Tools

About 2,760,000 results (0.45 seconds)

Network security is protection of the access to files and directories in a computer **network** against hacking, misuse and unauthorized changes to the system. An example of **network security** is an anti virus system.

Network security dictionary definition | network security defined
www.yourdictionary.com/network-security

About this result Feedback

People also ask

What do you mean by network security?

What are the different types of network security?

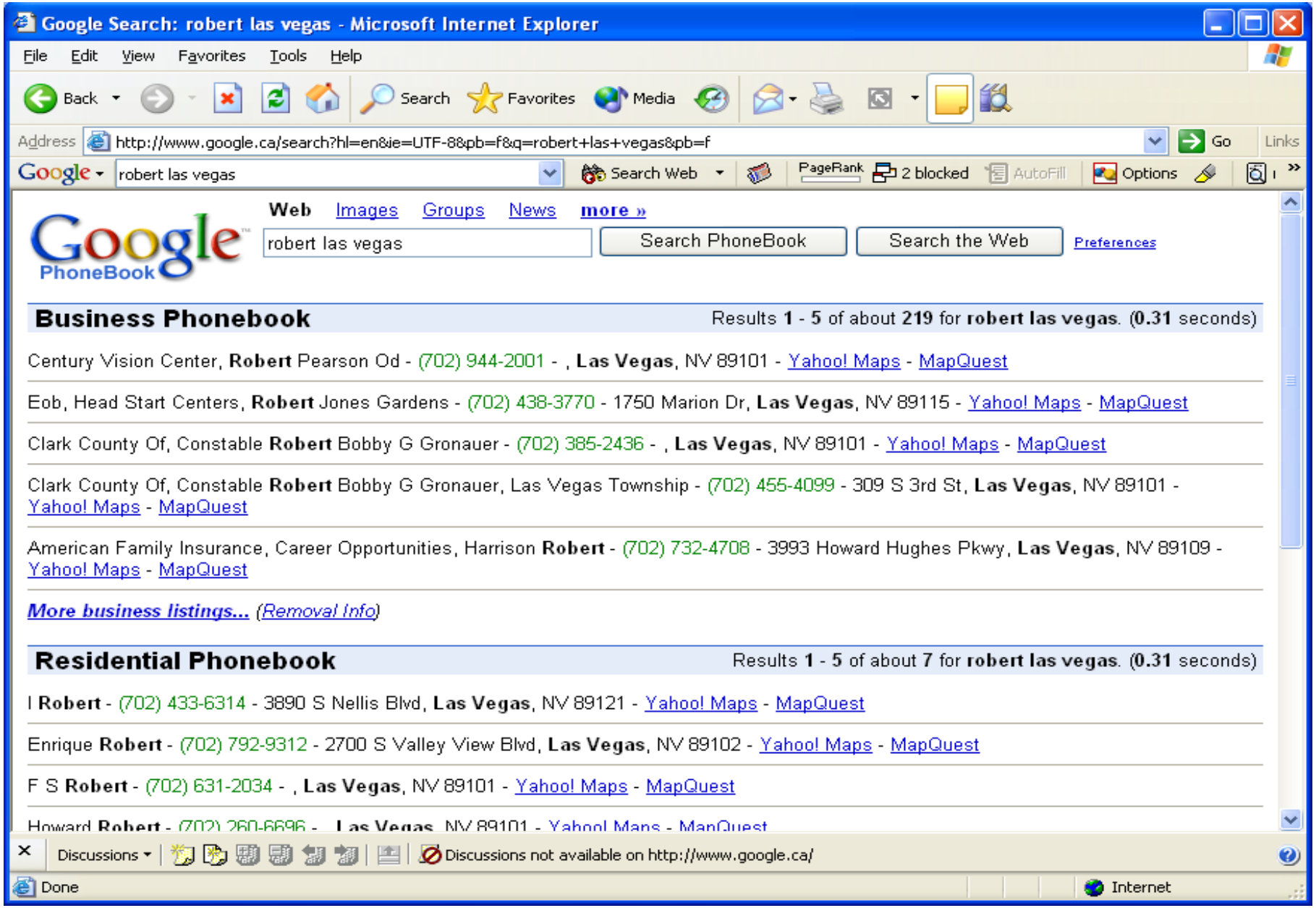
What is the job of network security engineer?

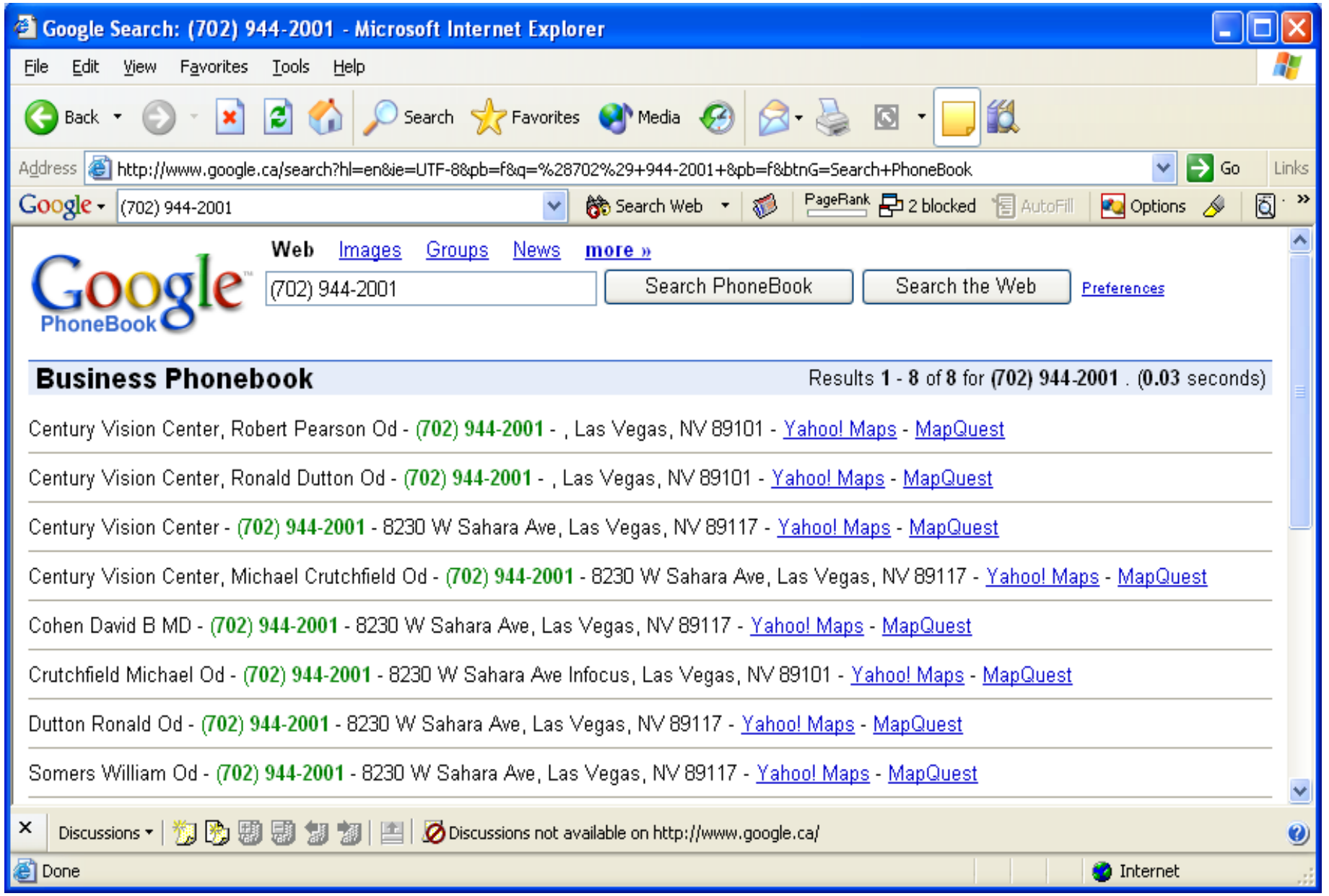
Why is Network Security?

Feedback

Advance Operators

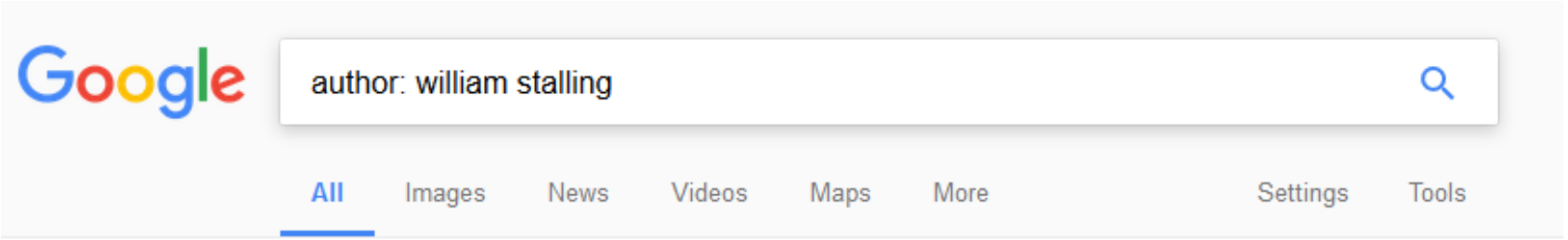
- Advanced Operators “phonebook:”
- Phonebook
  - Search the entire Google phonebook
- rphonebook
  - Search residential listings only
- bphonebook
  - Search business listings only
- Examples:
  - Phonebook: robert las vegas (robert in Las Vegas)
  - Phonebook: (702) 944-2001 (reverse search, not always work)
  - The phonebook is quite limited to U.S.A

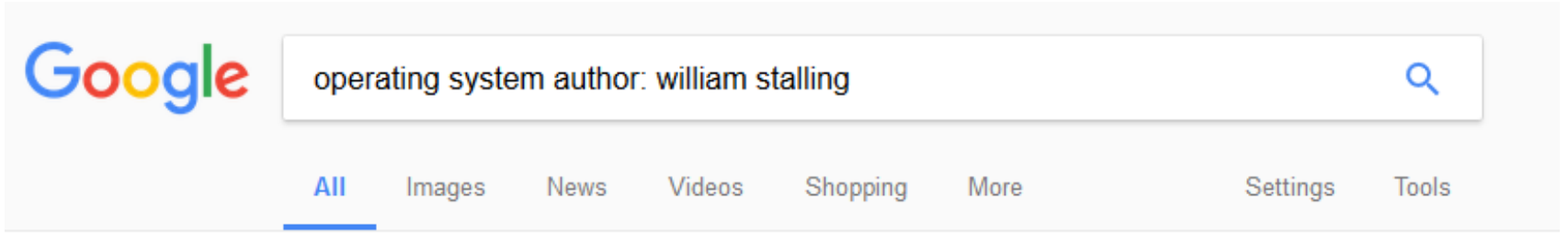

Google Search: robert las vegas - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?hl=en&ie=UTF-8&pb=f&q=robert+las+vegas&pb=f
Go Links
Google robert las vegas
Search Web PageRank 2 blocked AutoFill Options
Web Images Groups News more »
Google PhoneBook
robert las vegas
Search PhoneBook
Search the Web
Preferences
Business Phonebook
Results 1 - 5 of about 219 for robert las vegas. (0.31 seconds)
Century Vision Center, Robert Pearson Od - (702) 944-2001 - , Las Vegas, NV 89101 - Yahoo! Maps - MapQuest
Eob, Head Start Centers, Robert Jones Gardens - (702) 438-3770 - 1750 Marion Dr, Las Vegas, NV 89115 - Yahoo! Maps - MapQuest
Clark County Of, Constable Robert Bobby G Gronauer - (702) 385-2436 - , Las Vegas, NV 89101 - Yahoo! Maps - MapQuest
Clark County Of, Constable Robert Bobby G Gronauer, Las Vegas Township - (702) 455-4099 - 309 S 3rd St, Las Vegas, NV 89101 - Yahoo! Maps - MapQuest
American Family Insurance, Career Opportunities, Harrison Robert - (702) 732-4708 - 3993 Howard Hughes Pkwy, Las Vegas, NV 89109 - Yahoo! Maps - MapQuest
More business listings... (Removal Info)
Residential Phonebook
Results 1 - 5 of about 7 for robert las vegas. (0.31 seconds)
I Robert - (702) 433-6314 - 3890 S Nellis Blvd, Las Vegas, NV 89121 - Yahoo! Maps - MapQuest
Enrique Robert - (702) 792-9312 - 2700 S Valley View Blvd, Las Vegas, NV 89102 - Yahoo! Maps - MapQuest
F S Robert - (702) 631-2034 - , Las Vegas, NV 89101 - Yahoo! Maps - MapQuest
Howard Robert - (702) 260-6696 - Las Vegas, NV 89101 - Yahoo! Maps - MapQuest
Discussions Discussions not available on http://www.google.ca/
Done
Internet

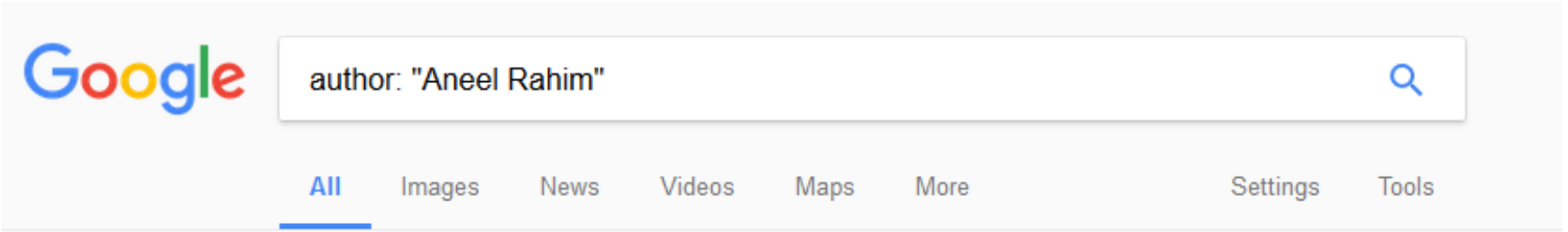

Google Search: (702) 944-2001 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.google.ca/search?hl=en&ie=UTF-8&pb=f&q=%28702%29+944-2001+&pb=f&btnG=Search+PhoneBook
Go Links
Google (702) 944-2001
Search Web PageRank 2 blocked AutoFill Options
Web Images Groups News more »
Google PhoneBook
(702) 944-2001
Search PhoneBook
Search the Web
Preferences
Business Phonebook
Results 1 - 8 of 8 for (702) 944-2001 . (0.03 seconds)
Century Vision Center, Robert Pearson Od - (702) 944-2001 - , Las Vegas, NV 89101 - Yahoo! Maps - MapQuest
Century Vision Center, Ronald Dutton Od - (702) 944-2001 - , Las Vegas, NV 89101 - Yahoo! Maps - MapQuest
Century Vision Center - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - Yahoo! Maps - MapQuest
Century Vision Center, Michael Crutchfield Od - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - Yahoo! Maps - MapQuest
Cohen David B MD - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - Yahoo! Maps - MapQuest
Crutchfield Michael Od - (702) 944-2001 - 8230 W Sahara Ave Infocus, Las Vegas, NV 89101 - Yahoo! Maps - MapQuest
Dutton Ronald Od - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - Yahoo! Maps - MapQuest
Somers William Od - (702) 944-2001 - 8230 W Sahara Ave, Las Vegas, NV 89117 - Yahoo! Maps - MapQuest
Discussions
Discussions not available on http://www.google.ca/
Done
Internet

Advance Operators

- Advanced Operators “author:”
- author : name
  - It restrict the Google search results to show pages only about the author you specify.
- Examples:
  - author: william stalling
  - operating system author: william stalling
  - author: “aneel rahim”


Google
author: william stalling
All
Images
News
Videos
Maps
More
Settings
Tools
About 457,000 results (0.72 seconds)
William Stallings
williamstallings.com/
BOOKS BY WILLIAM STALLINGS ... Welcome to the Web site for the computer science textbooks of William Stallings. He is an 12-time winner of the Texty Award ...
ComputerOrganization · Cryptography · OperatingSystems · NetworkSecurity
Amazon.com: William Stallings: Books, Biography, Blog, Audiobooks ...
https://www.amazon.com/William-Stallings/e/B000APXR9Q
Dr. William Stallings is an American author. He has written textbooks on computer science topics such as operating systems, computer networks, computer ...
William Stallings - Wikipedia
https://en.wikipedia.org/wiki/William_Stallings
Dr. William Stallings is an American author. He has written textbooks on computer science topics such as operating systems, computer networks, computer ...
Books by William Stallings (Author of Computer Organization and ...
https://www.goodreads.com/author/list/47971.William_Stallings
William Stallings has 77 books on Goodreads with 6203 ratings. William Stallings's most popular book is Computer Organization and Architecture: Designing...


Google
operating system author: william stalling
All
Images
News
Videos
Shopping
More
Settings
Tools
About 382,000 results (0.61 seconds)
OperatingSystems - William Stallings
williamstallings.com/OperatingSystems/
BOOKS BY WILLIAM STALLINGS. OPERATING ... A state-of-the art survey of operating system principles. Covers ... OPERATING SYSTEMS, EIGHTH EDITION.
OS8e-Student · OS8e-Instructor · OS7e-Instructor · OS7e-Student
Operating Systems, Sixth Edition - William Stallings
williamstallings.com/OS/OS6e.html
Student Resources Operating Systems: Internals and Design Principles, Sixth Edition. Last updated: Thursday, November 11, 2010 ...
Operating Systems - William Stalling 6th edition.pdf - Google Drive
https://docs.google.com/file/d/0ByWx.../edit
Sign in. Loading... Whoops! There was a problem loading more pages. Retrying... Whoops! There was a problem previewing this document. Retrying.
Operating Systems: Internals and Design Principles (8th Edition ...
https://www.amazon.com/Operating-Systems-Internals-Design.../dp/0133805913
Operating Systems: Internals and Design Principles (8th Edition) [William ... Data and Computer Communications (10th Edition) (William Stallings Books on ...


Google
author: "Aneel Rahim"
All
Images
News
Videos
Maps
More
Settings
Tools
About 1,430 results (0.50 seconds)
Aneel Rahim - Semantic Scholar
https://www.semanticscholar.org/author/Aneel-Rahim/2548533
Semantic Scholar profile for Aneel Rahim, with fewer than 50 highly influential citations, fewer than 50 est. total ... Authors who most influenced Aneel Rahim:.
STR member: Aneel Rahim publishes two papers: Intrusion Detection ...
str.tssg.org/2013/12/27/str-member-aneel-rahim-publishes-two-papers/
Dec 27, 2013 - Paper Title:Intrusion Detection System for Wireless Nano Sensor Networks. Authors:Aneel Rahim, Paul Malone. Conference:The 8th ...
Aneel Rahim - Articles - Scientific Research Publishing
www.scirp.org › Journals
Aneel Rahim. ... Information for Authors · Paper Submission · Manuscript Tracking System · Join Peer-Review Program · Free SCIRP Newsletter · Call for Special ...
Aneel Rahim, Fahad Bin Muhaya - جامعة الملك سعود
search.ksu.edu.sa/ar/search?num=10&q=aneel+rahim+fahad+bin...site...
http://pmc.ksu.edu.sa/ar/journals-papers ... Authors: Aneel Rahim, Fahad Bin Muhaya, Zeeshan Shafi , MA Ansari, Muhammad Sher. Journal: Informatica.

Google Hacking

- What can google can do for a hacker?
  - Search sensitive information like payroll, even personal email box
  - Vulnerabilities scanner
  - Transparency proxy

Google Hacking

- Financial Information
  - sales filetype: xls site: ie

Sales Value	Jan-13	Feb-13	Mar-13	Apr-13	May-13	Jun-13	Jul-13	Aug-13	Sep-13	Oct-13	Nov-13	Dec-13
Rooms	40,797	40,797	67,995	122,391	135,990	135,990	176,788	176,788	135,990	122,391	40,797	163,188
Events	2,588	2,588	7,764	7,764	15,528	15,528	15,528	15,528	15,528	15,528	2,588	12,940
Bar	10,000	10,000	30,000	30,000	60,000	60,000	60,000	60,000	60,000	60,000	10,000	50,000
Restaurant	15,000	15,000	45,000	45,000	90,000	90,000	90,000	90,000	90,000	90,000	15,000	75,000
Sales	**68,385**	**68,385**	**150,759**	**205,156**	**301,519**	**301,519**	**342,316**	**342,316**	**301,519**	**287,920**	**68,385**	**301,129**
Cost of Sales												
Rooms	4,080	4,080	6,800	12,239	13,599	13,599	17,679	17,679	13,599	12,239	4,080	16,319
Events	1,812	1,812	5,435	5,435	10,870	10,870	10,870	10,870	10,870	10,870	1,812	9,058
Bar	6,500	6,500	19,500	19,500	39,000	39,000	39,000	39,000	39,000	39,000	6,500	32,500
Restaurant	9,000	9,000	27,000	27,000	54,000	54,000	54,000	54,000	54,000	54,000	9,000	45,000
CoS	**21,391**	**21,391**	**58,734**	**64,174**	**117,469**	**117,469**	**121,549**	**121,549**	**117,469**	**116,109**	**21,391**	**102,877**

Sales Value	Jan-14	Feb-14	Mar-14	Apr-14	May-14	Jun-14	Jul-14	Aug-14	Sep-14	Oct-14	Nov-14	Dec-14
Rooms	44,877	44,877	74,795	134,630	149,589	149,589	194,466	194,466	149,589	134,630	44,877	179,507
Events	2,847	2,847	8,541	8,541	17,081	17,081	17,081	17,081	17,081	17,081	2,847	14,234
Bar	11,000	11,000	33,000	33,000	66,000	66,000	66,000	66,000	66,000	66,000	11,000	55,000
Restaurant	15,000	15,000	45,000	45,000	90,000	90,000	90,000	90,000	90,000	90,000	15,000	75,000
Sales	**73,724**	**73,724**	**161,335**	**221,171**	**322,671**	**322,671**	**367,547**	**367,547**	**322,671**	**307,712**	**73,724**	**323,742**
Cost of Sales												
Rooms	4,488	4,488	7,479	13,463	14,959	14,959	19,447	19,447	14,959	13,463	4,488	17,951
Events	1,993	1,993	5,978	5,978	11,957	11,957	11,957	11,957	11,957	11,957	1,993	9,964
Bar	7,150	7,150	21,450	21,450	42,900	42,900	42,900	42,900	42,900	42,900	7,150	35,750
Restaurant	9,000	9,000	27,000	27,000	54,000	54,000	54,000	54,000	54,000	54,000	9,000	45,000
CoS	**22,630**	**22,630**	**61,908**	**67,891**	**123,816**	**123,816**	**128,303**	**128,303**	**123,816**	**122,320**	**22,630**	**108,665**

Google Hacking

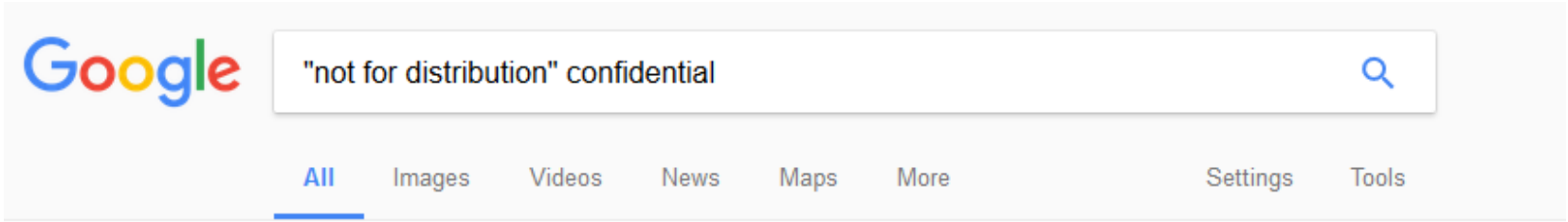
- Personal Mailbox
  - intitle: index.of inurl:inbox

Index of /INBOX

Name	Last modified	Size	Description
Parent Directory		-	
OLD/	05-Jan-2017 17:21	-	
archivo.tar.gz	12-May-2009 10:58	1.4M	
msg0000.WAV	05-Jan-2017 18:05	2.2K	
msg0000.gsm	05-Jan-2017 18:05	2.2K	
msg0000.txt	05-Jan-2017 18:05	249	
msg0000.wav	05-Jan-2017 18:05	22K	
msg0001.WAV	06-Jan-2017 11:26	34K	
msg0001.gsm	06-Jan-2017 11:26	35K	
msg0001.txt	06-Jan-2017 11:26	255	
msg0001.wav	06-Jan-2017 11:26	337K	
msg0002.WAV	06-Jan-2017 20:10	29K	
msg0002.gsm	06-Jan-2017 20:10	29K	
msg0002.txt	06-Jan-2017 20:10	250	
msg0002.wav	06-Jan-2017 20:10	283K	
msg0003.WAV	06-Jan-2017 20:12	23K	
msg0003.gsm	06-Jan-2017 20:12	23K	
msg0003.txt	06-Jan-2017 20:12	250	
msg0003.wav	06-Jan-2017 20:12	223K	

Google Hacking

- Confidential Files
  - "not for distribution" confidential



CONFIDENTIAL

SIRIUS DISCLOSURE

NOT FOR DISTRIBUTION

DOCUMENTARY SYNOPSIS:

UNACKNOWLEDGED: AN EXPOSE OF THE GREATEST SECRET IN HUMAN HISTORY

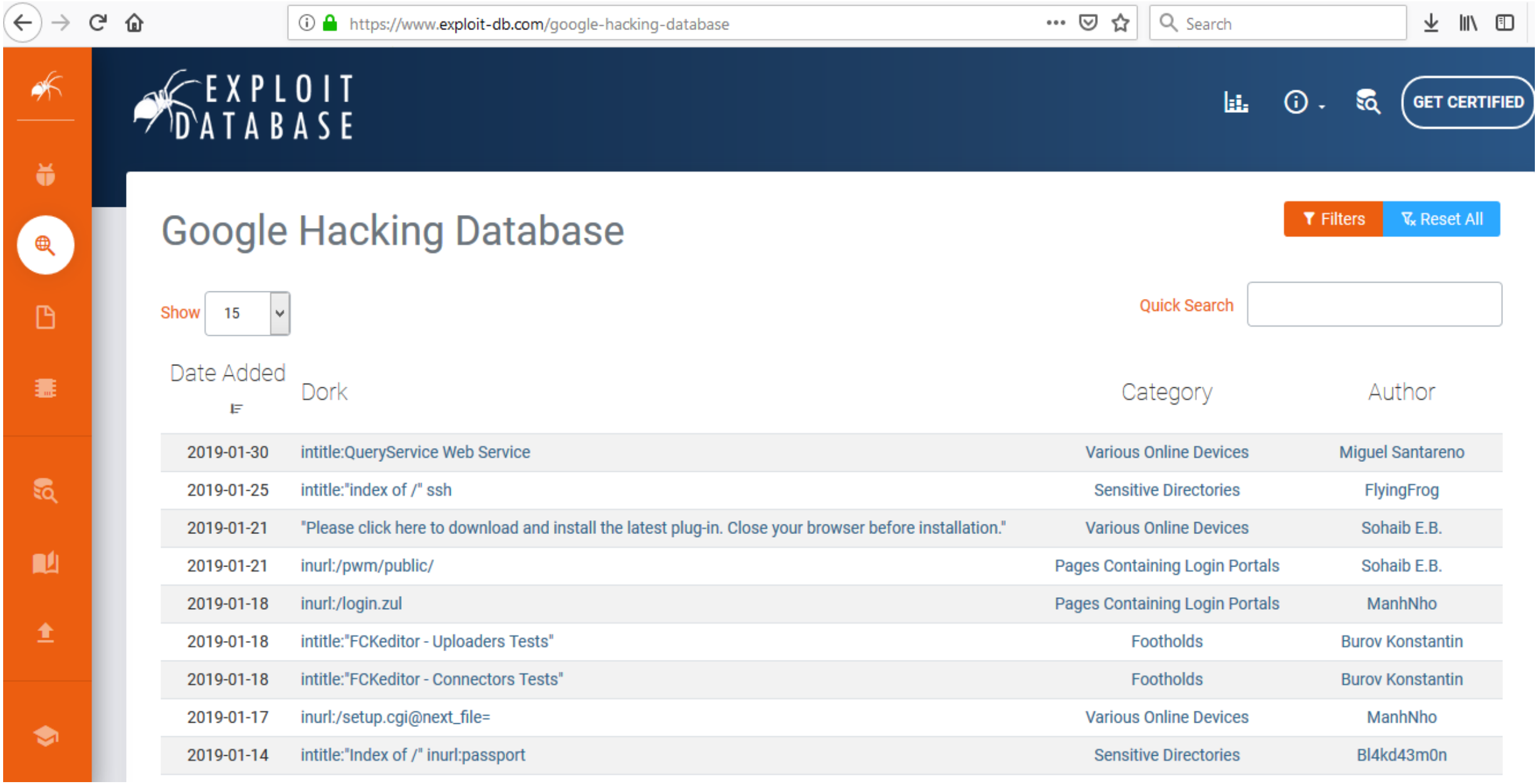
Created by: Steven M. Greer MD Release Date: Fall 2016
Director: TBA Produced by: SiriusDisclosure.com

In the aftermath of the most successful crowd-funded documentary in history, Sirius, Dr. Greer and his team are producing "Unacknowledged : An Expose of the Greatest Secret in Human History".

Sirius reached number 1 on Netflix for documentaries and was acclaimed throughout the world. With virtually no marketing or P & A budget, Sirius reached millions of people and has had over $1 million in revenue.

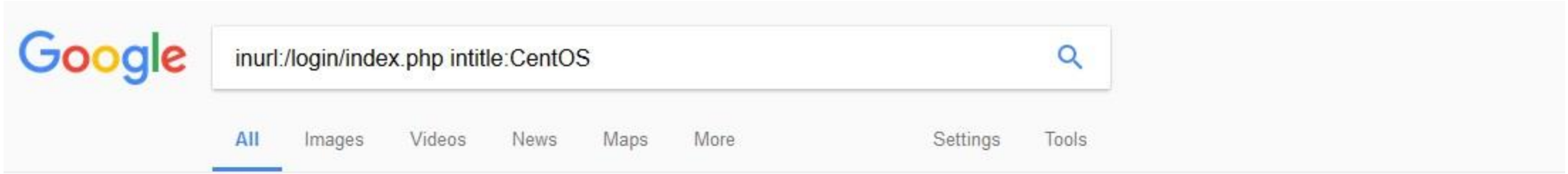
"Unacknowledged" will focus on the historic files of the Disclosure Project and how UFO secrecy has been ruthlessly enforced - and why. The best evidence for Extraterrestrial contact, dating back decades, will be presented with direct top-secret witness testimony, documents and UFO footage.

The behind-the-scenes research and high level meetings convened by Dr. Steven Greer will expose the degree of illegal, covert operations at the core of UFO secrecy. From meetings with Laurance Rockefeller and the Clintons, to briefings with the CIA Director, top Pentagon Generals and Admirals, to the briefing of President Obama via senior advisor John Podesta, current chairman of the Hillary Clinton Campaign - we will take the viewer behind the veil of secrecy and into the


https://www.exploit-db.com/google-hacking-database
Search
EXPLOIT DATABASE
GET CERTIFIED
Google Hacking Database
Filters
Reset All
Show 15
Quick Search
Date Added
Dork
Category
Author
2019-01-30 intitle:QueryService Web Service Various Online Devices Miguel Santareno
2019-01-25 intitle:"index of /" ssh Sensitive Directories FlyingFrog
2019-01-21 "Please click here to download and install the latest plug-in. Close your browser before installation." Various Online Devices Sohaib E.B.
2019-01-21 inurl:/pwm/public/ Pages Containing Login Portals Sohaib E.B.
2019-01-18 inurl:/login.zul Pages Containing Login Portals ManhNho
2019-01-18 intitle:"FCKeditor - Uploaders Tests" Footholds Burov Konstantin
2019-01-18 intitle:"FCKeditor - Connectors Tests" Footholds Burov Konstantin
2019-01-17 inurl:/setup.cgi@next_file= Various Online Devices ManhNho
2019-01-14 intitle:"Index of /" inurl:passport Sensitive Directories Bl4kd43m0n

Latest Google Vulnerabilities 2018

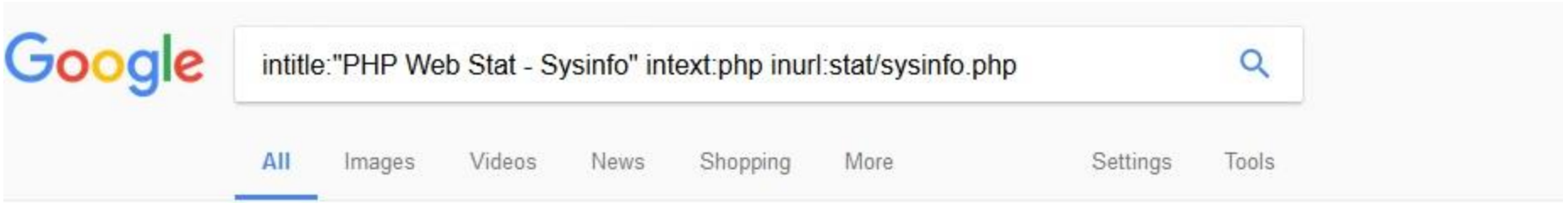
- Finds Login Pages of CentOS
  - inurl:/login/index.php intitle:CentOS


Google
inurl:/login/index.php intitle:CentOS
All
Images
Videos
News
Maps
More
Settings
Tools
4 results (0.20 seconds)
Server CentOS powered by HTTP Test Page Apache -www ...
www.microfin360.com/login/index.php/g700chorographical-cbrachymetropia17996/
This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page it means that the Apache HTTP server installed at this site is working properly. If you are a member of the general public: The fact that you are seeing this page indicates that the website you just ...
SSL login
https://128.199.170.195:2031/login/index.php
Login to CentOS WebPanel. Fast Login (no stats and checks). You are using SSL login. Visit Website How to Install. © 2017 CentOS WebPanel control panel for linux.
Login | CentOS WebPanel
dishut.kaltimprov.go.id:2030/login/index.php
Login to CentOS WebPanel. Fast Login (no stats and checks). Please use SSL login Click here for SSL login. Visit Website How to Install. © 2017 CentOS WebPanel control panel for linux.
Login | CentOS WebPanel - Web Site Satpol PP Prov.Kaltim
satpolpp.kaltimprov.go.id:2030/login/index.php
Login to CentOS WebPanel. Fast Login (no stats and checks). Please use SSL login Click here for SSL login. Visit Website How to Install. © 2017 CentOS WebPanel control panel for linux.


dishut.kaltimprov.go.id:2030/login/index.php
CWP CONTROL
WEB PANEL
Login to CentOS WebPanel
Admin Username
Admin Password
Fast Login (no stats and checks)
Login
Please use SSL login Click here for SSL login.

Latest Google Vulnerabilities 2018

- List all server statistics , hardware and software details
  - intitle:"PHP Web Stat - Sysinfo" intext:php inurl:stat/sysinfo.php



About 27 results (0.40 seconds)

PHP Web Stat - Sysinfo - Haus Martin
hausmartin.org/stat/sysinfo.php ▾
Server Info. Server Host, alfa3011.alfahosting-server.de. Server OS, Apache. **PHP** Version, 5.2.17. Max Execution T. 30 sec. Memory Limit, 16MB. Session Support, enabled. Cookie Support, disabled ...

PHP Web Stat - Sysinfo
www.sorenm.com/stat/sysinfo.php ▾
Server Info. Server Host, dd39220.kasserver.com. Server OS, Apache. **PHP** Version, 5.5.38-nmm3. Max Execution T. 30 sec. Memory Limit, 128MB. Session Support, enabled. Cookie Support, disabled ...

PHP Web Stat - Sysinfo - Meteo Gouda
www.meteo-gouda.nl/stat/sysinfo.php
Stat Info. Script Version, 4.9.15. Script Activitiy, enabled. DB Active, OFF. Script Domain, http://www.meteo-gouda.nl. Script Path, stat/. Starting Page, index.**php**. Domain(s), weerstation-gouda-bloemendaal.nl meteo-gouda.nl. URL Parameter. Frames, enabled. IP Recount Time, 10 min. Update Check, enabled.

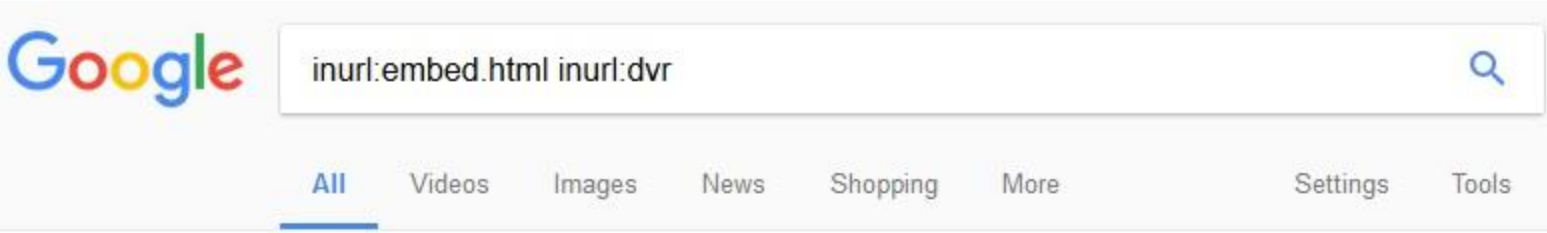
PHP Web Stat - Sysinfo
www.fv-dresden-sw.de/stat/sysinfo.php ▾
Stat Info. Script Version, 4.9.15. Script Activitiy, enabled. DB Active, OFF. Script Domain, http://www.fv-dresden-sw.de. Script Path, stat/. Starting Page, index.**php**. Domain(s), fv-dresden-sw.de. URL Parameter. Frames, OFF. IP Recount Time, 60 min. Update Check, enabled. Error Reporting, OFF. Log htaccess, enabled.

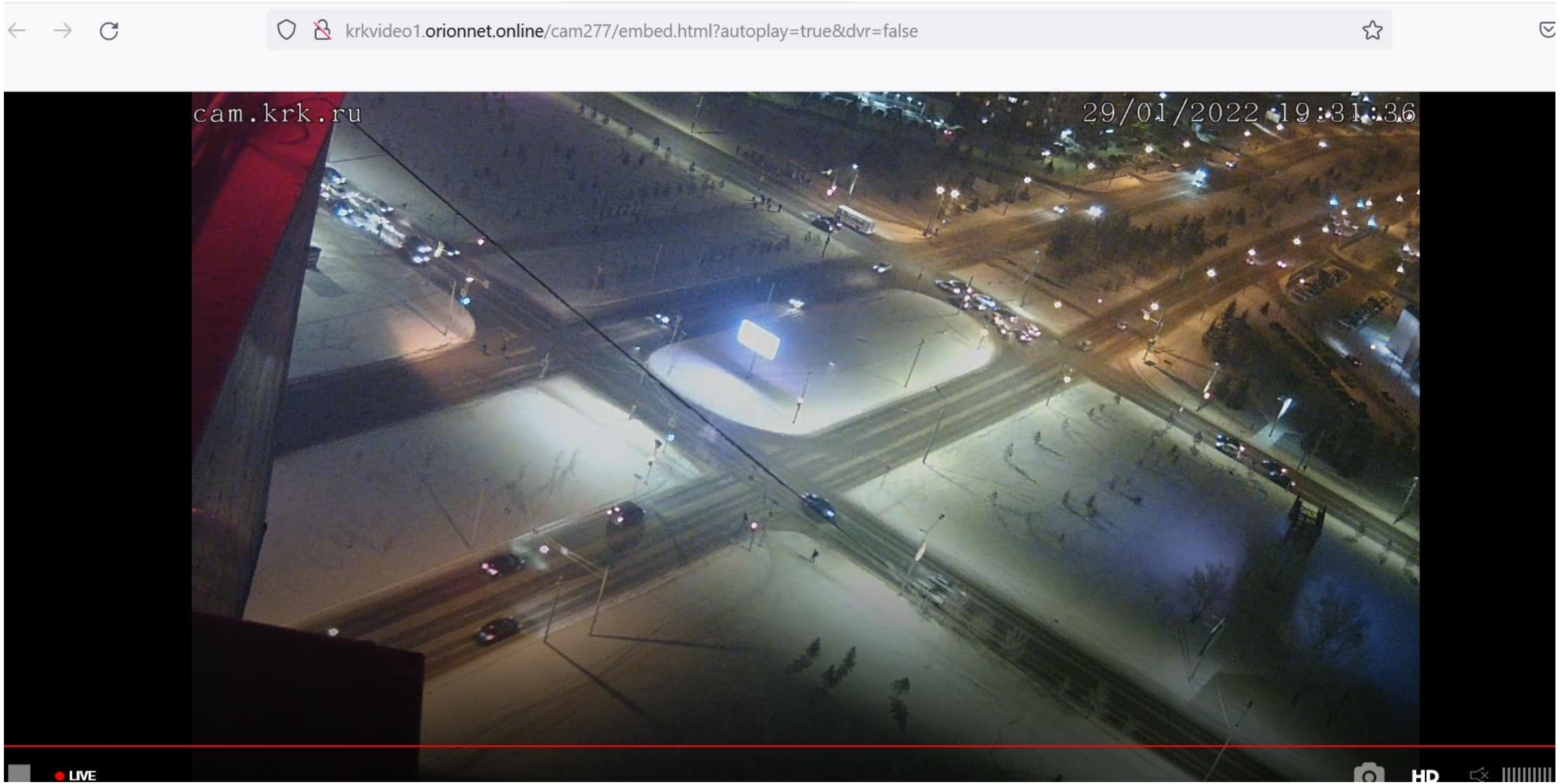

hausmartin.org/stat/sysinfo.php
Search
PHP Web Stat
SysInfo v2.4
Stat
Counter
File Version
Admin-Center
Stat Info
Script Version 4.9.15
Script Activitiy
DB Active OFF
Script Domain http://www.hausmartin.org
Script Path stat/
Starting Page index.html
Domain(s) hausmartin.org
URL Parameter
Frames OFF
IP Recount Time 5 min.
Update Check
Error Reporting
Log htaccess OFF
Creator Number 5.000
Referer Cut 0
Index Number 30.000
Cache Update OFF
Country detection 08/2014
Last log entry 27.01.2018 08:44:24
Server Info
Server Host alfa3011.alfahosting-server.de
Server OS Apache
PHP Version 5.2.17
Max Execution T. 30 sec.
Memory Limit 16MB
Session Support
Cookie Support
File Check
File
Version
config/admin.php
config/backup.php
config/reset.php
config/setup.php
func/func_browser.php
func/func_cache_write.php
func/func_display.php
func/func_load_creator.php
func/func_operating_system.php
func/func_pattern_matching.php
func/func_pattern_reverse.php
func/html_header.php
./archive.php
./cache_creator.php
./cache_panel.php
./cookie.php
./counter.php
./index.php
./last_hits.php
./plugin_loader.php
./syscheck.php
./sysinfo.php
./track.php
./track_file.php


www.sorenm.com/stat/sysinfo.php
Search
Server Info
Server Host dd39220.kasserver.com
Server OS Apache
PHP Version 5.5.38-nmm3
Max Execution T. 30 sec.
Memory Limit 128MB
Session Support
Cookie Support
./syscheck.php
./sysinfo.php
./track.php
./track_file.php
File CHMOD Status
File Size Rows CHMOD Status
backup/ 755
log/ 777
log/archive/ 777
config/config.php 666
config/config_db.php 666
config/pattern_site_name.inc 222,88 KB 2685 666
config/pattern_string_replace.inc 0,00 KB 0 666
config/tracking_code.php 0,49 KB 15 666
cache_time_stamp.php 0,04 KB 1 666
cache_time_stamp_archive.php 0,04 KB 1 666
cache_visitors.php 2.091,00 KB 20.961 666
cache_visitors_archive.php 28,24 KB 1.604 666
logdb.dta 27,53 KB 605 666
logdb_backup.dta 24.403,25 KB 534.909 666
logdb_temp.dta 26,44 KB 580 666
logdb_track_file.dta 0,28 KB 1 666
pattern_browser.dta 7,13 KB 342 666
pattern_operating_system.dta 0,27 KB 21 666
pattern_referer.dta 2.165,20 KB 11.870 666
pattern_resolution.dta 8,19 KB 659 666
pattern_site_name.dta 375,58 KB 7.941 666
Copyright © 2015 PHP Web Stat

Latest Google Vulnerabilities 2018

- Show live cams and tv
  - inurl:embed.html inurl:dvr


Google
inurl:embed.html inurl:dvr
All
Videos
Images
News
Shopping
More
Settings
Tools
About 3,480 results (0.20 seconds)
d4fee077-1a44-47fb-a367-d15cad794a2a
langate.tv/d4fee077-1a44-47fb-a367-d15cad794a2a/embed.html?dvr=false
braxer - AirMAX
https://streaming.airmax.pl/braxer/embed.html?dvr=false
Dvorkino_1
5.189.243.162:8082/Dvorkino_1/embed.html?dvr=false
Video is not available.
rysianka2
91.224.104.112:8181/rysianka2/embed.html?dvr=false
Video is not available.
dvoracky-panorama
79.98.156.78:8080/dvoracky-panorama/embed.html?dvr=false&proto=hls
live. back to live. Disabled.
BishopsLydeard_59234
mirlees.railcam.co.uk:8080/BishopsLydeard_59234/embed.html?dvr=false...rtmp
live. back to live. Disabled.


krkvideo1.orionnet.online/cam277/embed.html?autoplay=true&dvr=false
cam.krk.ru
29/01/2022 19:31:36
LIVE
HD

Latest Google Vulnerabilities 2018

- list of FTP/SFTP passwords from the text.
  - intitle:"Index Of" intext:sftp-config.json

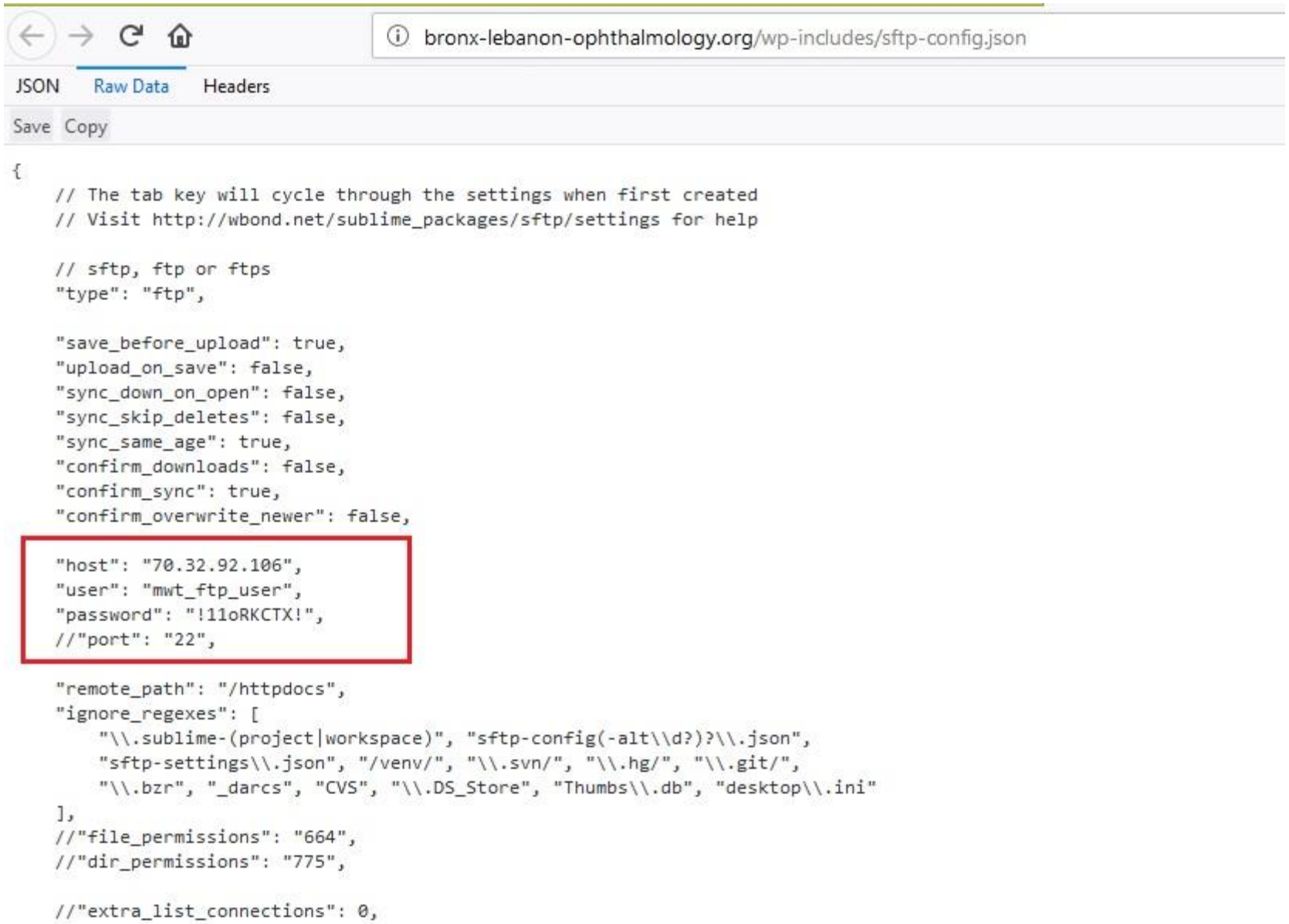
About 160 results (0.23 seconds)

Index of /kitnes/cache.old/pages2/sftp/config.json - GBC Ghana
www.gbcghana.com/kitnes/cache.old/pages2/sftp/config.json/
Index of /kitnes/cache.old/pages2/**sftp/config.json**. Name · Last modified · Size · Description · Parent Directory, -. 1.htm, 2015-07-11 18:30, 0.

Index of /wp-includes - Bronx Lebanon Ophthalmology
bronx-lebanon-ophthalmology.org/wp-includes/
... post-template.php · post-thumbnail-template.php · post.php · query.php · random_compat/ · registration-functions.php · registration.php · rest-api.php · rest-api/ · revision.php · rewrite.php · rss-functions.php · rss.php · script-loader.php · session.php · **sftp-config.json** · shortcodes.php · taxonomy.php · template-loader.php ...

Index of /assets - PintaSuper
pintasuper.com/assets/
Name · Last modified · Size · Description · Parent Directory, -. cache/, 2015-04-02 13:20, -. css/, 2016-04-30 14:47, -. docs/, 2015-04-02 13:20, -. fonts/, 2016-04-30 14:47, -. images/, 2016-04-30 14:48, -. js/, 2016-04-30 14:49, -. pdf/, 2015-04-02 13:20, -. **sftp-config.json**, 2016-04-30 13:20, 1.4K. svg/, 2016-04-30 14:48, -.

intitle:"Index Of" intext:sftp-config.json - Exploit-DB
https://www.exploit-db.com/ghdb/4657/
Jan 12, 2018 - 1. 2. 3. 4. 5. 6. 7. 8. Description : This dork returns list of FTP/SFTP passwords from sublime text. Dork : intitle:"Index Of" intext:**sftp-config.json**. Author : Vipin Joshi (@vocuzi) ...


bronx-lebanon-ophthalmology.org/wp-includes/sftp-config.json
JSON
Raw Data
Headers
Save
Copy
{
// The tab key will cycle through the settings when first created
// Visit http://wbond.net/sublime_packages/sftp/settings for help
// sftp, ftp or ftps
"type": "ftp",
"save_before_upload": true,
"upload_on_save": false,
"sync_down_on_open": false,
"sync_skip_deletes": false,
"sync_same_age": true,
"confirm_downloads": false,
"confirm_sync": true,
"confirm_overwrite_newer": false,
"host": "70.32.92.106",
"user": "mwt_ftp_user",
"password": "!11oRKCTX!",
//"port": "22",
"remote_path": "/httpdocs",
"ignore_regexes": [
"\\.sublime-(project|workspace)", "sftp-config(-alt\\d?)?\\.json",
"sftp-settings\\.json", "/venv/", "\\.svn/", "\\.hg/", "\\.git/",
"\\.bzr", "_darcs", "CVS", "\\.DS_Store", "Thumbs\\.db", "desktop\\.ini"
],
//"file_permissions": "664",
//"dir_permissions": "775",
//"extra_list_connections": 0,


```
{
    // The tab key will cycle through the settings when first created
    // Visit http://wbond.net/sublime_packages/sftp/settings for help

    // sftp, ftp or ftps
    "type": "sftp",

    "save_before_upload": true,
    "upload_on_save": false,
    "sync_down_on_open": false,
    "sync_skip_deletes": false,
    "sync_same_age": false,
    "confirm_downloads": false,
    "confirm_sync": true,
    "confirm_overwrite_newer": false,

    "host": "ftp.pintasuper.com",
    "user": "pintasuper",
    "password": "KXRD00wjr9",
    "port": "22",

    //"remote_path": "/home/pintasuper/public_html/prueba",
    "remote_path": "/home/pintasuper/public_html/",
    "ignore_regexes": [
```

Latest Google Vulnerabilities 2018

- Finds vulnerable printers
  - inurl:"/websys/webArch/mainFrame.cgi" -hatana


Google
inurl:"/websys/webArch/mainFrame.cgi" -hatana
All
Maps
Images
News
Shopping
More
Settings
Tools
About 60 results (0.36 seconds)
RNP002673A96CBA - Web Image Monitor - PRINTER-HACKED
impsecfyp.us.es/web/guest/en/websys/webArch/mainFrame.cgi
Status. System: Status OK. Toner: Status OK. Waste Toner Bottle: Status OK. Input Tray: Status OK. Output Tray: Status OK. Check Details. Skip menu and go to the main content. Status/Information. Device Info · Status · Counter · Job · Inquiry. Device Management. Configuration · Device Home Management. Print Job/Stored ...
Web Image Monitor
62.93.36.200/web/user/en/websys/webArch/mainFrame.cgi
SMB · System Log · Webpage. Top Page. Click [Refresh] to display current status. Help. Refresh. Web Image Monitor. Device Name, : RNP802EE8. Comment, : DRUKARKA-FIZYKA. Status. Printer, : Alert. Copier, : Alert. Scanner, : Energy Saver Mode. Detail. Point to each function with mouse pointer to display details.
192.168.1.101 /web/guest/en/websys/webarch ... - IPAddress.com
https://www.ipaddress.com/search/192.168.1.../en/websys/webarch/mainframe.cgi
Your search for 192.168.1.101 /web/guest/en/websys/webarch/mainframe.cgi would give you better results when you put the query in the form of a domain name or IP address format. The term 192.168.1.101 /web/guest/en/websys/webarch/mainframe.cgi can be used in domains. Our suggested articles will help you put ...

impsecfyp.us.es/web/guest/en/websys/webArch/mainFrame.cgi

Search

RICOH MP C3003 Web Image Monitor

Home

English Switch Refresh

- Status/Information
- Device Management
- Print Job/Stored File
- Convenient Links

Device Name	: Ricoh MPC 3003	Comment	:
Location	:	Host Name	: RNP002673A96CBA

Alert

- Alert
- Messages (0item(s))

Status

System	Status OK
Toner	Status OK
Waste Toner Bottle	Status OK
Input Tray	Almost Out of Paper
Output Tray	Status OK

Latest Google Vulnerabilities 2019

- Access SAP Crystal report
- inurl:apspassword

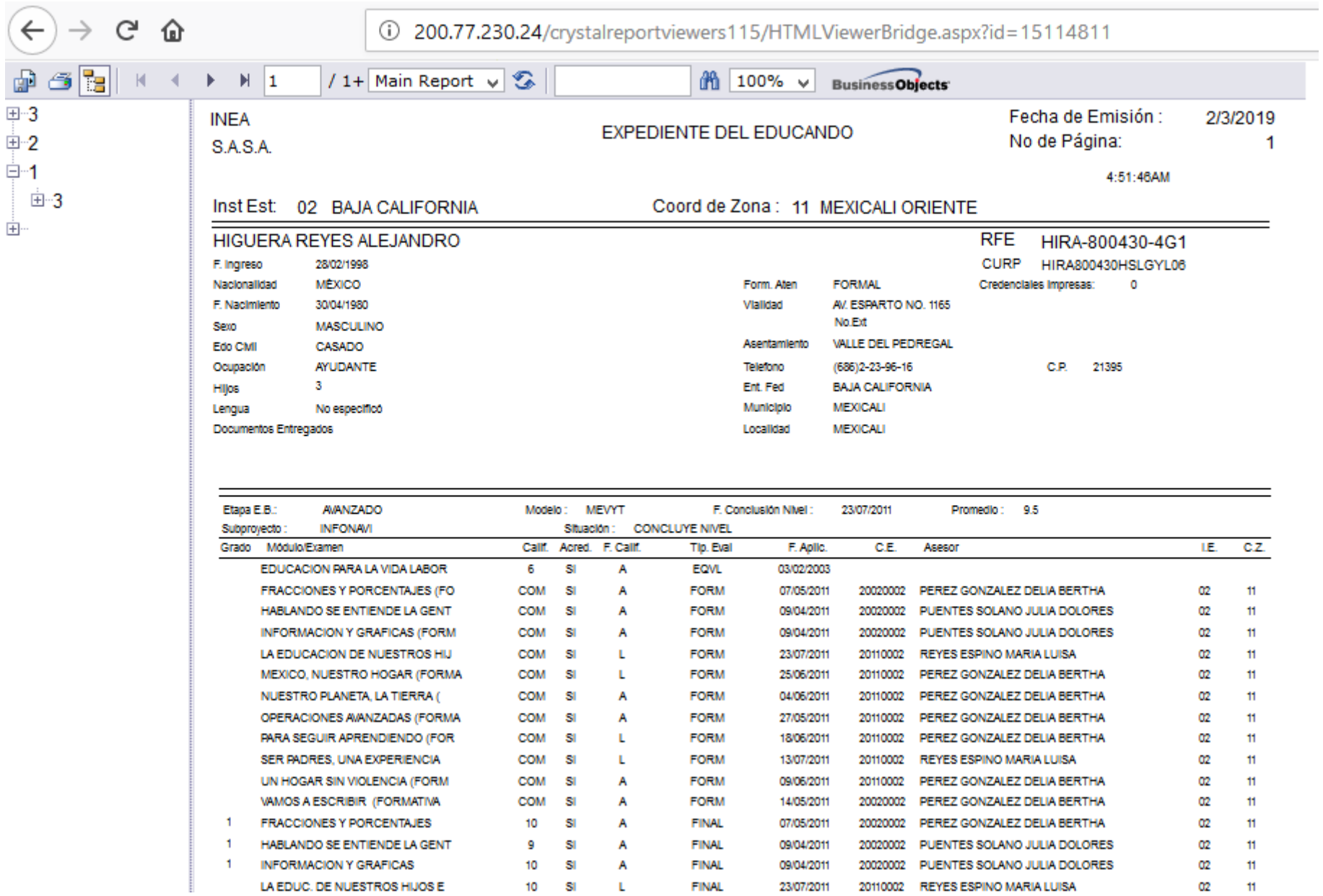
About 36 results (0.22 seconds)

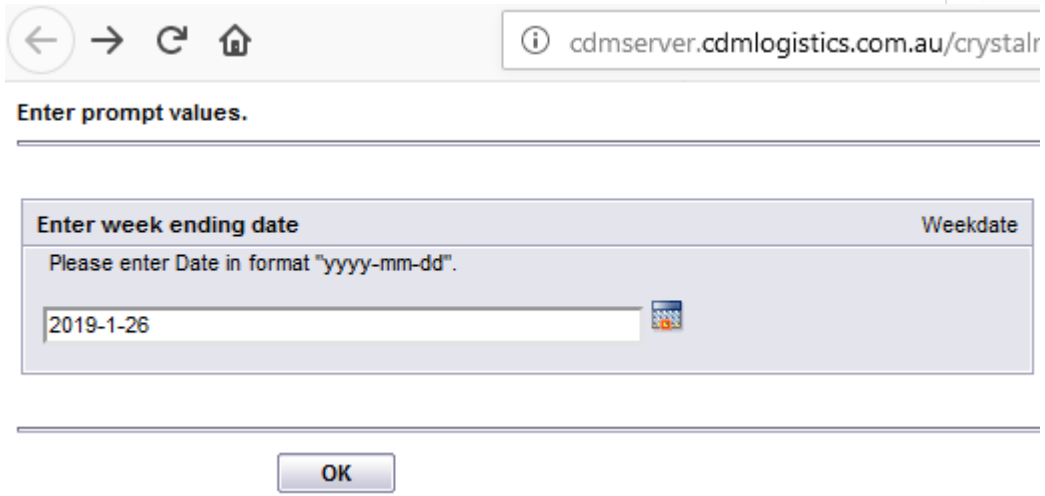
Crystal Reports Viewer
rz3.cubeserv.com:49000/BOE/OpenDocument/.../viewrpt.cwr?...apspassword...
The viewer could not process an event. The object with ID 326660 does not exist in the CMS or you do not have the right to access it. [CRSDK00001182] ...

Crystal Reports Viewer
200.77.230.24/.../viewrpt.aspx?...apspassword... Translate this page
AV. ESPARTO NO. 1165. VALLE DEL PEDREGAL. (686)2-23-96-16. HIGUERA REYES ALEJANDRO. HIRA-800430-4G1. HIRA800430HSLGYL06. 0. MÉXICO.

Crystal Reports Viewer
200.77.230.24/crystalreportviewers115/viewrpt.aspx?id...apspassword...
@Annio, @Annio. Set to Null. @Mes, @Mes. Set to Null. @icveie, @icveie. Set to Null. @quincena, @quincena. Set to Null. OK.

Crystal Reports Viewer - ncdenr.org
https://reports.ncdenr.org/BOE/.../viewrpt.cwr?id...U&apspassword...
Enter prompt values. Please enter Animal Operations Permit Number (must include NC or NCG prefix):, prm00_Permit_Number. OK.


200.77.230.24/crystalreportviewers115/HTMLViewerBridge.aspx?id=15114811
1
/ 1+
Main Report
100%
BusinessObjects
3
2
1
3
INEA
S.A.S.A.
EXPEDIENTE DEL EDUCANDO
Fecha de Emisión : 2/3/2019
No de Página: 1
4:51:46AM
Inst Est: 02 BAJA CALIFORNIA
Coord de Zona : 11 MEXICALI ORIENTE
HIGUERA REYES ALEJANDRO
RFE HIRA-800430-4G1
CURP HIRA800430HSLGYL06
F. Ingreso 28/02/1998
Nacionalidad MÉXICO
F. Nacimiento 30/04/1980
Sexo MASCULINO
Edo Civil CASADO
Ocupación AYUDANTE
Hijos 3
Lengua No especificó
Documentos Entregados
Form. Aten FORMAL
Vialidad AV. ESPARTO NO. 1165
No.Ext
Asentamiento VALLE DEL PEDREGAL
Telefono (686)2-23-96-16
C.P. 21395
Ent. Fed BAJA CALIFORNIA
Municipio MEXICALI
Localidad MEXICALI
Credenciales Impresas: 0
Etapa E.B.: AVANZADO
Modelo : MEVYT
F. Conclusión Nivel : 23/07/2011
Promedio : 9.5
Subproyecto : INFONAVI
Situación : CONCLUYE NIVEL
Grado Módulo/Examen Calif. Acred. F. Calif. Tip. Eval F. Aplic. C.E. Asesor I.E. C.Z.
EDUCACION PARA LA VIDA LABOR 6 SI A EQIVL 03/02/2003
FRACCIONES Y PORCENTAJES (FO COM SI A FORM 07/05/2011 20020002 PEREZ GONZALEZ DELIA BERTHA 02 11
HABLANDO SE ENTIENDE LA GENT COM SI A FORM 09/04/2011 20020002 PUENTES SOLANO JULIA DOLORES 02 11
INFORMACION Y GRAFICAS (FORM COM SI A FORM 09/04/2011 20020002 PUENTES SOLANO JULIA DOLORES 02 11
LA EDUCACION DE NUESTROS HIJ COM SI L FORM 23/07/2011 20110002 REYES ESPINO MARIA LUISA 02 11
MEXICO, NUESTRO HOGAR (FORMA COM SI L FORM 25/06/2011 20110002 PEREZ GONZALEZ DELIA BERTHA 02 11
NUESTRO PLANETA, LA TIERRA (COM SI A FORM 04/06/2011 20110002 PEREZ GONZALEZ DELIA BERTHA 02 11
OPERACIONES AVANZADAS (FORMA COM SI A FORM 27/05/2011 20110002 PEREZ GONZALEZ DELIA BERTHA 02 11
PARA SEGUIR APRENDIENDO (FOR COM SI L FORM 18/06/2011 20110002 PEREZ GONZALEZ DELIA BERTHA 02 11
SER PADRES, UNA EXPERIENCIA COM SI L FORM 13/07/2011 20110002 REYES ESPINO MARIA LUISA 02 11
UN HOGAR SIN VIOLENCIA (FORM COM SI A FORM 09/06/2011 20110002 PEREZ GONZALEZ DELIA BERTHA 02 11
VAMOS A ESCRIBIR (FORMATIVA COM SI A FORM 14/05/2011 20020002 PEREZ GONZALEZ DELIA BERTHA 02 11
1 FRACCIONES Y PORCENTAJES 10 SI A FINAL 07/05/2011 20020002 PEREZ GONZALEZ DELIA BERTHA 02 11
1 HABLANDO SE ENTIENDE LA GENT 9 SI A FINAL 09/04/2011 20020002 PUENTES SOLANO JULIA DOLORES 02 11
1 INFORMACION Y GRAFICAS 10 SI A FINAL 09/04/2011 20020002 PUENTES SOLANO JULIA DOLORES 02 11
LA EDUC. DE NUESTROS HIJOS E 10 SI L FINAL 23/07/2011 20110002 REYES ESPINO MARIA LUISA 02 11



Combined Distribution Management Pty Ltd

T/AS **CDM LOGISTICS**

ACN: 072 045 802 **ABN: 50 072 045 802**

Admin Office - PO Box 6264 Wetherill Park NSW 2164
Phone: 02 9773 2400 Fax: 02 9773 2440
email: accounts@cdmlogistics.com.au

WEEKLY TAX INVOICE - 45054 - 1/20/2019 to 1/26/2019

Customer - **INTA**

INTERTRADING AUSTRALIA P/L
PO BOX 256

NARELLAN NSW 2561

TAX INVOICE

Consignment No.	SY03060225	Invoice Date	1/21/2019
Origin: SMEATON GRANGE	INTERTRADING AUSTRALIA 157 HARTLEY RD SMEATON GRANGE	Pick Up Date	1/21/2019
Destination: KEYSBOROUGH	IMS 4 FIVEWAYS BOULEVARD		

Customer References 224874+

Rate type	Quantity	Description	Rate	Amount
Q	3.00	STANDARD PALLETS	109.0210	$327.06
L		FUEL LEVY 6.85% 6.85%	327.0600	$22.40

Net Invoice Amount $317.69 GST Amount $31.77 **Invoice Total (incl GST) $349.46**

Latest Google Vulnerabilities 2019

- Find Answer Keys
- filetype:doc "Answer Key"

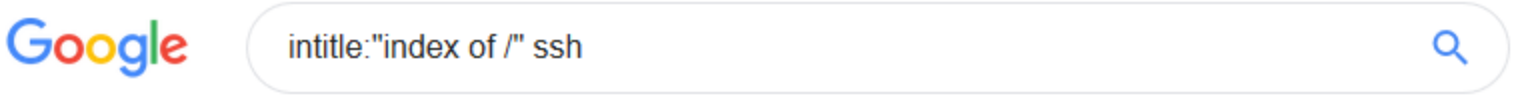

Google
filetype:doc "Answer Key"
All
Images
News
Maps
Books
More
Settings
Tools
About 158,000 results (0.30 seconds)
[DOC] Answer Key - Schoolnet
https://cleveland.schoolnet.com/Outreach/Content/ServeAttachment.aspx?...id...
Answer Key. Day 1. 1. C. 2. "The square root of a number is 15" can be represented by the equation . To find x, students should realize that the inverse operation ...
[DOC] Answer Key for Exercises
https://www.uvm.edu/~dhowell/.../SPSSAnswer%20Key%20for%20Exercises.doc
Answer Key for Exercises. Exercises-Chapter 1. 1.1 A variety of topics appear under ANOVA. A summary is below. You should look at some of the topics in more ...
[DOC] Answer Key:
https://mars.nasa.gov/mer/classroom/marsdial/downloads/Marsdial1_answers.doc
Answer Key: Will the curve be the same throughout the year? Why or why not? The shape of the curve will be the same, but the exact positioning of the curve on ...
[DOC] answer key - Cengage
www.cengage.com/resource_uploads/downloads/elt.../0618789677_34117.DOC
ANSWER KEY. TOP 20 STUDENT .... No answer key required for this exercise. 3. 1 ... NOTE: Answer key applicable only for first part of each question. 1 ...

Latest Google Vulnerabilities 2019

- I found a lot of servers using SSH .
- intitle:"index of /" ssh

Data you find:

- Webserver Version
- SSH Version
- SSH Keys
- SSH Logins



About 38,300 results (0.33 seconds)

Index of /ssh/ccc

www.cs.tau.ac.il/ssh/ccc/

Index of /**ssh**/ccc. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [DIR], META-INF/, 2001-06-12 11:59, -. [DIR], mindbright ...

Index of /~edmund/materials/ssh

enos.itcollege.ee/~edmund/materials/ssh/

Index of /~edmund/materials/**ssh** ... **ssh**-fingerprint-server-bbd-**oldssh**.sh, 2018-01-24 12:02, 1.5K. [TXT] ... **ssh**-fingerprint-server.sh, 2018-01-21 06:37, 1.1K.

Index of /.ssh - Auberge d'Eygliers

auberge-eygliers.com/.ssh/

Index of /.**ssh**. Icon Name Last modified Size Description. [PARENTDIR] Parent Directory - [ ] authorized_keys2 2014-08-04 15:16 397.

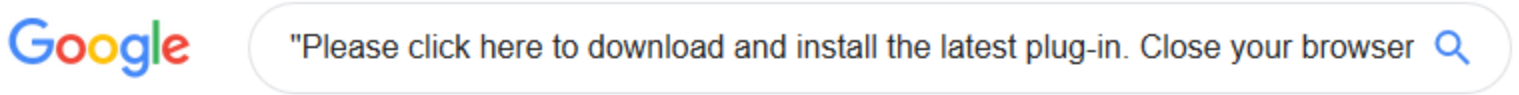
Index of /.ssh - Weave Conference 2018

weaveconference.com/.ssh/

Index of /.**ssh**. Parent Directory. Apache Server at weaveconference.com Port 80.

Latest Google Vulnerabilities 2019

- Find NVR (Network Video Recorder) login portals.
- "Please click here to download and install the latest plug-in. Close your browser before installation."



10 results (0.35 seconds)

"Please click here to download and install the latest plug-in. Close ...
https://www.exploit-db.com/ghdb/5082
Jan 21, 2019 - Google Dork: "**Please click here to download and install the latest plug-in. Close your browser before installation**." # Description: Find NVR ...

NVR-ADM4P4
remote.cetechnology.net/
Please click here to download and install the latest plug-in. Close your browser before installation. Language. 简体中文, English, 繁體中文, にほんご, 한국의 ...

NVR304-32E
212.3.204.54/
Please click here to download and install the latest plug-in. Close your browser before installation. Language. 简体中文, English, 繁體中文, にほんご, 한국의 ...

NVR-ADM8P8
www.cgfaucher.com/
Please click here to download and install the latest plug-in. Close your browser before installation. Language. 简体中文, English, 繁體中文, にほんご, 한국의 ...

Latest Google Vulnerabilities 2020

- **allintext:"Index Of" "cookies.txt“**
  - Show Valuable cookie information

- **inurl:check_mk/login.py**
  - Show the login pages of admin

- **intitle:"index of" "ftp.log"**
  - Show files that contains FTP logs

Latest Google Vulnerabilities 2021

- **allintext:@gmail.com filetype:log**
- Show log files that contains emails and passwords

- **"password 7" ext:txt | ext:log | ext:cfg**
  - Show files containing passwords

- **inurl:authorization.ping**
  - Pages containing portals for login or employee account recovery

Google, Friend or Enemy?

- Google, Friend or Enemy?
- Google is everyone's best friend (yours or hackers)
- Information gathering and vulnerability identification are the tasks in the first phase of a typical hacking scenario
- Google can do more than search
- Have you used Google to audit your organization today?

Lecture 3
User Authentication

CMPU-4008

Advance Security 2

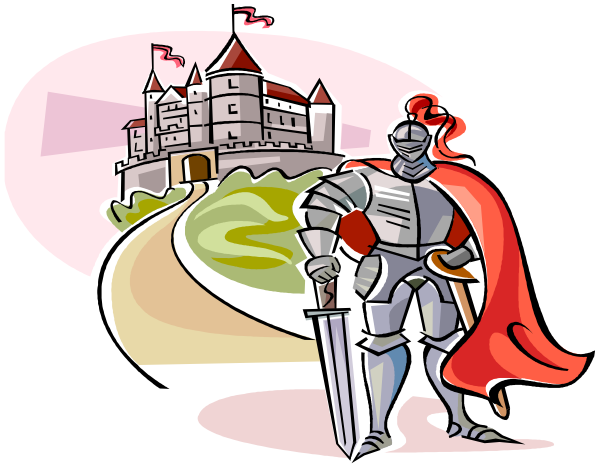
RFC 4949

RFC 4949 defines user authentication as:

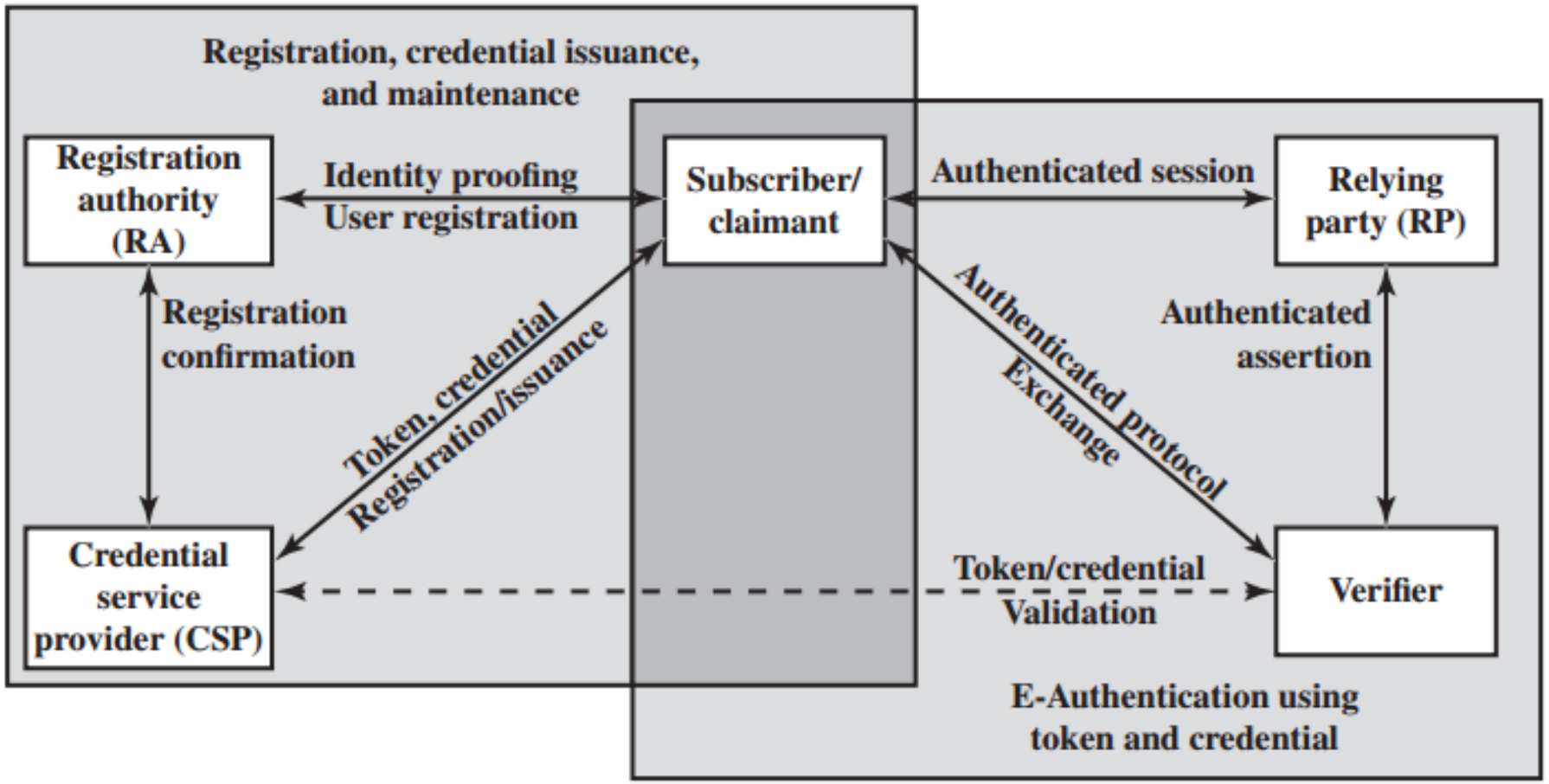
"The process of verifying an identity claimed by or for a system entity."

Authentication Process

- Fundamental building block and primary line of defense
- Basis for access control and user accountability



- Identification step
  - Presenting an identifier to the security system
- Verification step
  - Presenting or generating authentication information that corroborates the binding between the entity and the identifier



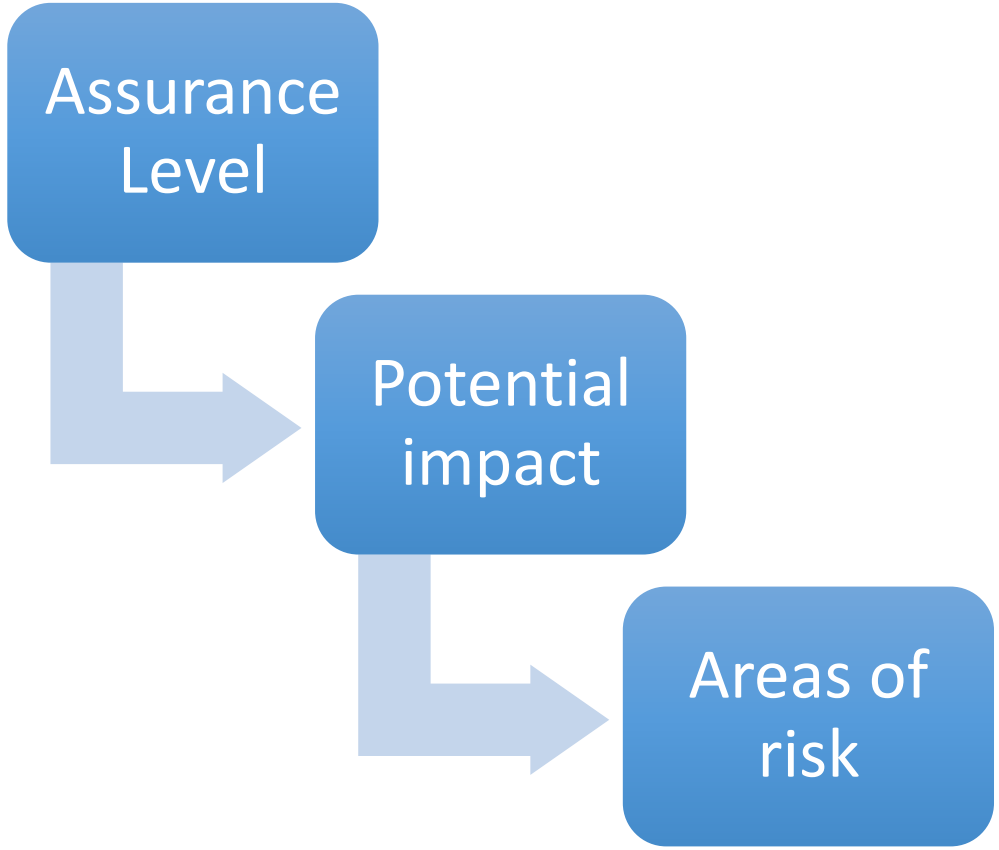
The NIST SP 800-63-2 E-Authentication Architectural Model

The four means of authenticating user identity are based on:

Something the individual knows	Something the individual possesses (token)	Something the individual is (static biometrics)	Something the individual does (dynamic biometrics)
• Password, PIN, answers to prearranged questions	• Smartcard, electronic keycard, physical key	• Fingerprint, retina, face	• Voice pattern, handwriting, typing rhythm

Risk Assessment for User Authentication

- There are three separate concepts:



Assurance Level

Describes an organization's degree of certainty that a user has presented a credential that refers to his or her identity

More specifically is defined as:

The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued

The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued

Four levels of assurance

Level 1
- Little or no confidence in the asserted identity's validity

Level 2
- Some confidence in the asserted identity's validity

Level 3
- High confidence in the asserted identity's validity

Level 4
- Very high confidence in the asserted identity's validity

Potential Impact

- FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security:
  - Low
    - An authentication error could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
  - Moderate
    - An authentication error could be expected to have a serious adverse effect
  - High
    - An authentication error could be expected to have a severe or catastrophic adverse effect

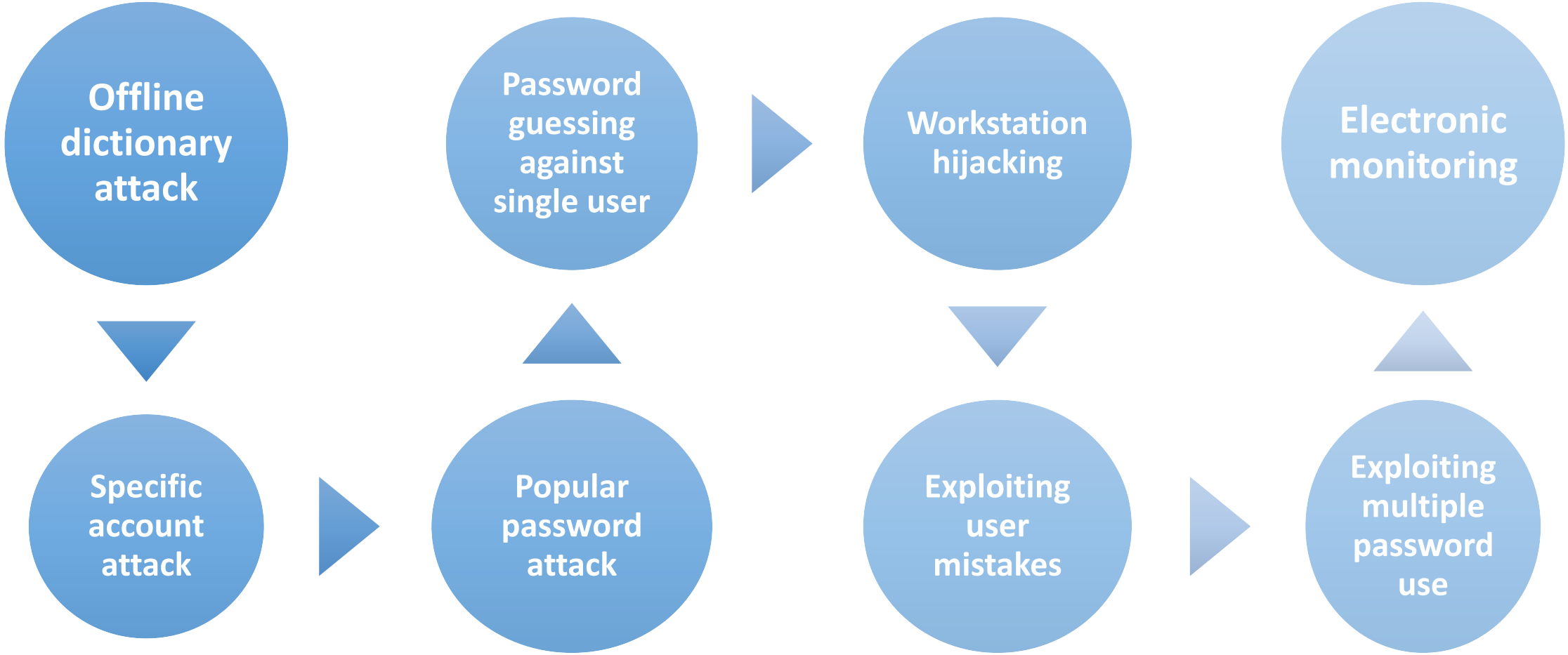
Maximum Potential Impacts for Each Assurance Level

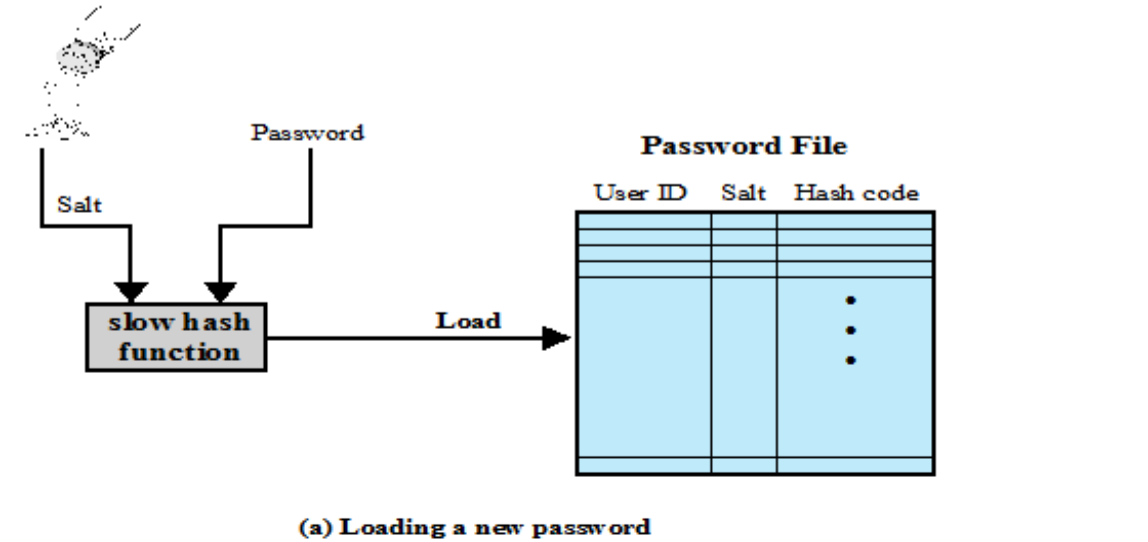
	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or organization liability	Low	Mod	Mod	High
Harm to organization programs or interests	None	Low	Mod	High
Unauthorized release of sensitive information	None	Low	Mod	High
Personal safety	None	None	Low	Mod/ High
Civil or criminal violations	None	Low	Mod	High

Password Authentication

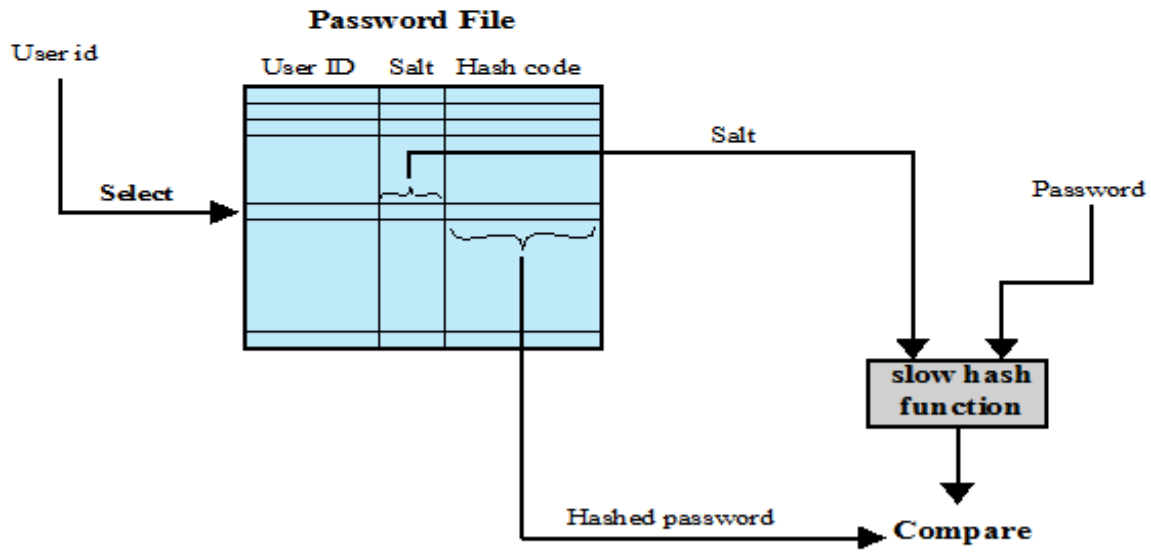
- Widely used line of defense against intruders
  - User provides name/login and password
  - System compares password with the one stored for that specified login
- The user ID:
  - Determines that the user is authorized to access the system
  - Determines the user's privileges
  - Is used in discretionary access control

Password Vulnerabilities





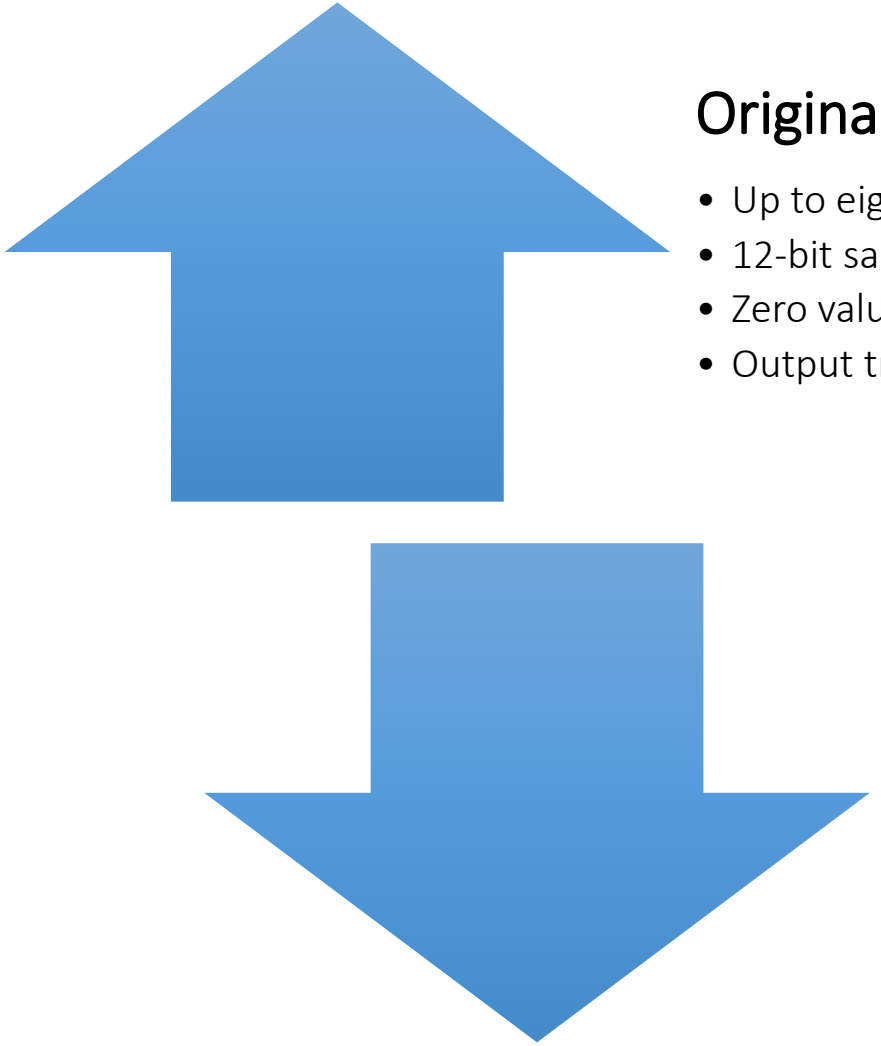
(a) Loading a new password



(b) Verifying a password

UNIX Password Scheme

UNIX Implementation



Original scheme

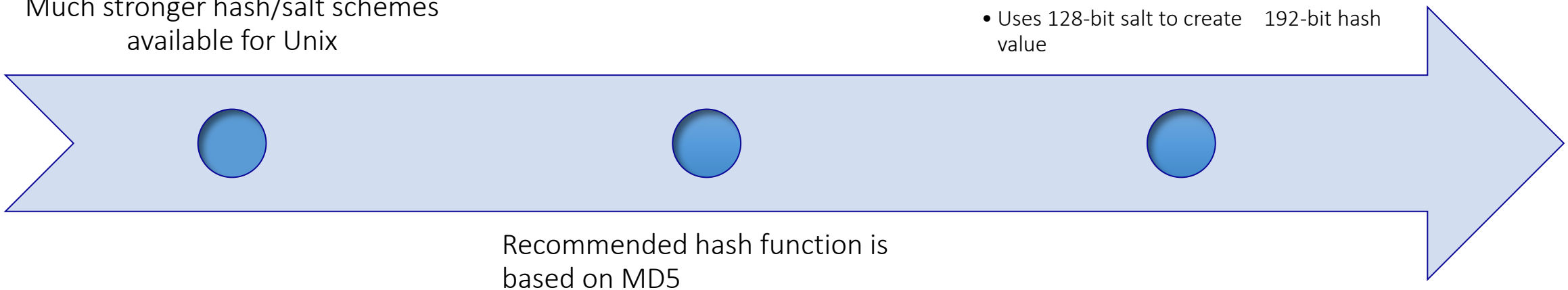
- Up to eight printable characters in length
- 12-bit salt used to modify DES encryption into a one-way hash function
- Zero value repeatedly encrypted 25 times
- Output translated to 11 character sequence

Now regarded as inadequate

- Still often required for compatibility with existing account management software or multivendor environments

Improved Implementations

Much stronger hash/salt schemes available for Unix



Recommended hash function is based on MD5

- Salt of up to 48-bits
- Password length is unlimited
- Produces 128-bit hash
- Uses an inner loop with 1000 iterations to achieve slowdown

OpenBSD uses Blowfish block cipher based hash algorithm called Bcrypt

- Most secure version of Unix hash/salt scheme
- Uses 128-bit salt to create 192-bit hash value

Password Cracking

Dictionary attacks

- Develop a large dictionary of possible passwords and try each against the password file
- Each password must be hashed using each salt value and then compared to stored hash values

Rainbow table attacks

- Pre-compute tables of hash values for all salts
- A mammoth table of hash values
- Can be countered by using a sufficiently large salt value and a sufficiently large hash length

Password crackers exploit the fact that people choose easily guessable passwords

- Shorter password lengths are also easier to crack

John the Ripper

- Open-source password cracker first developed in in 1996
- Uses a combination of brute-force and dictionary techniques

Modern Approaches

- Complex password policy
  - Forcing users to pick stronger passwords
- However password-cracking techniques have also improved
  - The processing capacity available for password cracking has increased dramatically
  - The use of sophisticated algorithms to generate potential passwords
  - Studying examples and structures of actual passwords in use

Password File Access Control

Can block offline guessing attacks by denying access to encrypted passwords

- Make available only to privileged users
- Shadow password file

Vulnerabilities

- Weakness in the OS that allows access to the file
- Accident with permissions making it readable
- Users with same password on other systems
- Access from backup media
- Sniff passwords in network traffic

Password Selection Strategies

User education

Users can be told the importance of using hard to guess passwords and can be provided with guidelines for selecting strong passwords

Computer generated passwords

Users have trouble remembering them

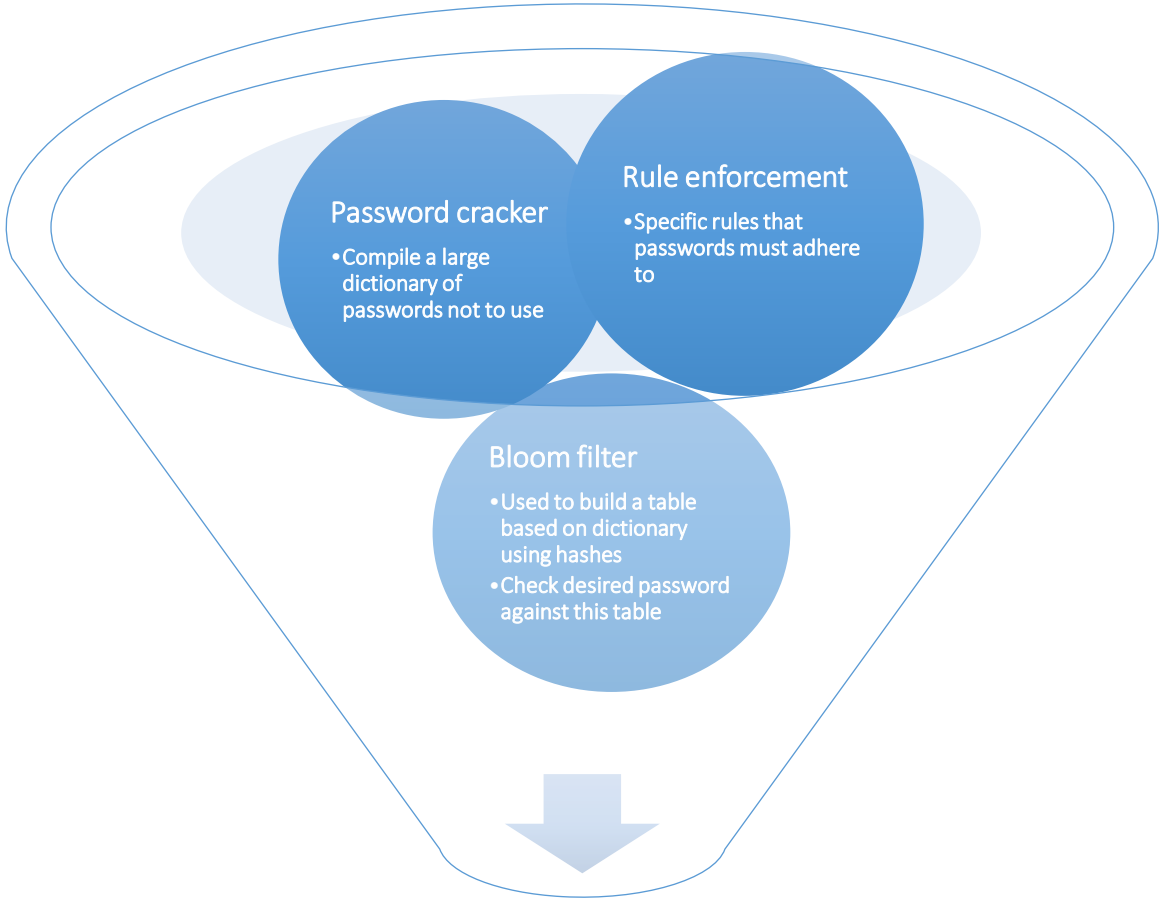
Reactive password checking

System periodically runs its own password cracker to find guessable passwords

Complex password policy

User is allowed to select their own password, however the system checks to see if the password is allowable, and if not, rejects it	Goal is to eliminate guessable passwords while allowing the user to select a password that is memorable

Proactive Password Checking



Token Based Authetication

Types of Cards Used as Tokens

Card Type	Defining Feature	Example
Embossed	Raised characters only, on front	Old credit card
Magnetic stripe	Magnetic bar on back, characters on front	Bank card
Memory	Electronic memory inside	Prepaid phone card
Smart Contact Contactless	Electronic memory and processor inside Electrical contacts exposed on surface Radio antenna embedded inside	Biometric ID card

Memory Cards

- Can store but do not process data
- The most common is the magnetic stripe card
- Can include an internal electronic memory
- Can be used alone for physical access
  - Hotel room
  - ATM
- Provides significantly greater security when combined with a password or PIN
- Drawbacks of memory cards include:
  - Requires a special reader
  - Loss of token
  - User dissatisfaction

Smart Tokens

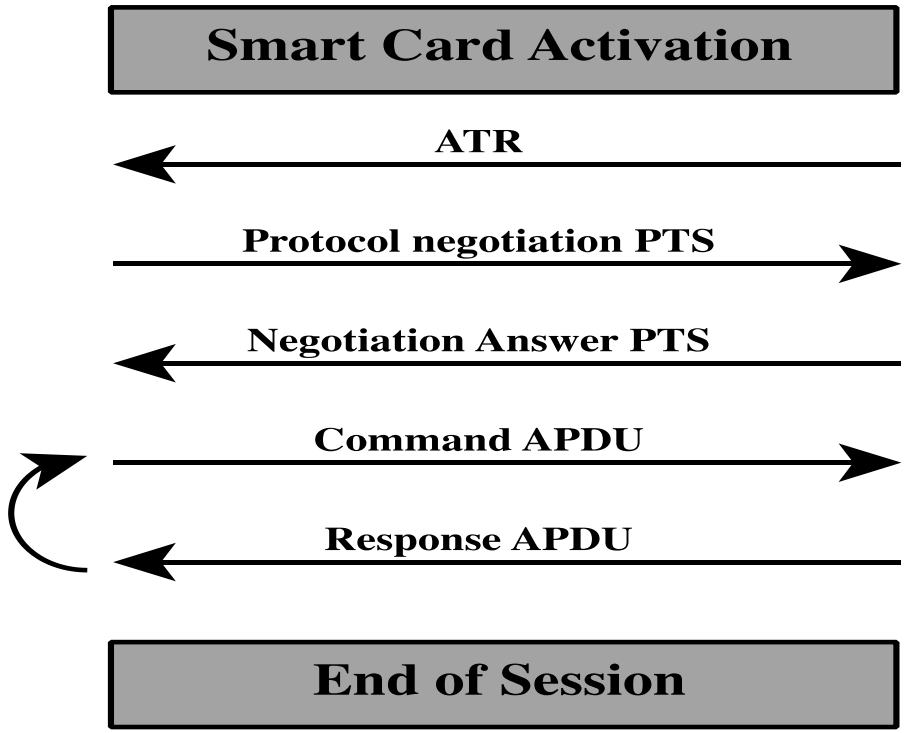
- Physical characteristics:
  - Include an embedded microprocessor
  - A smart token that looks like a bank card
  - Can look like calculators, keys, small portable objects
- Interface:
  - Manual interfaces include a keypad and display for interaction
  - Electronic interfaces communicate with a compatible reader/writer
- Authentication protocol:
  - Classified into three categories:
    - Static
    - Dynamic password generator
    - Challenge-response

Smart Cards

- Most important category of smart token
  - Has the appearance of a credit card
  - Has an electronic interface
  - May use any of the smart token protocols
- **Contain:**
  - An entire microprocessor
    - Processor
    - Memory
    - I/O ports
- **Typically include three types of memory:**
  - Read-only memory (ROM)
    - Stores data that does not change during the card's life
  - Electrically erasable programmable ROM (EEPROM)
    - Holds application data and programs
  - Random access memory (RAM)
    - Holds temporary data generated when applications are executed

Smart card

Card reader



APDU = application protocol data unit
ATR = Answer to reset
PTS = Protocol type selection

Figure 3.5 Smart Card/Reader Exchange

Electronic Identity Cards (eID)

Use of a smart card as a national identity card for citizens

Can serve the same purposes as other national ID cards, and similar cards such as a driver's license, for access to government and commercial services

Can provide stronger proof of identity and can be used in a wider variety of applications

In effect, is a smart card that has been verified by the national government as valid and authentic

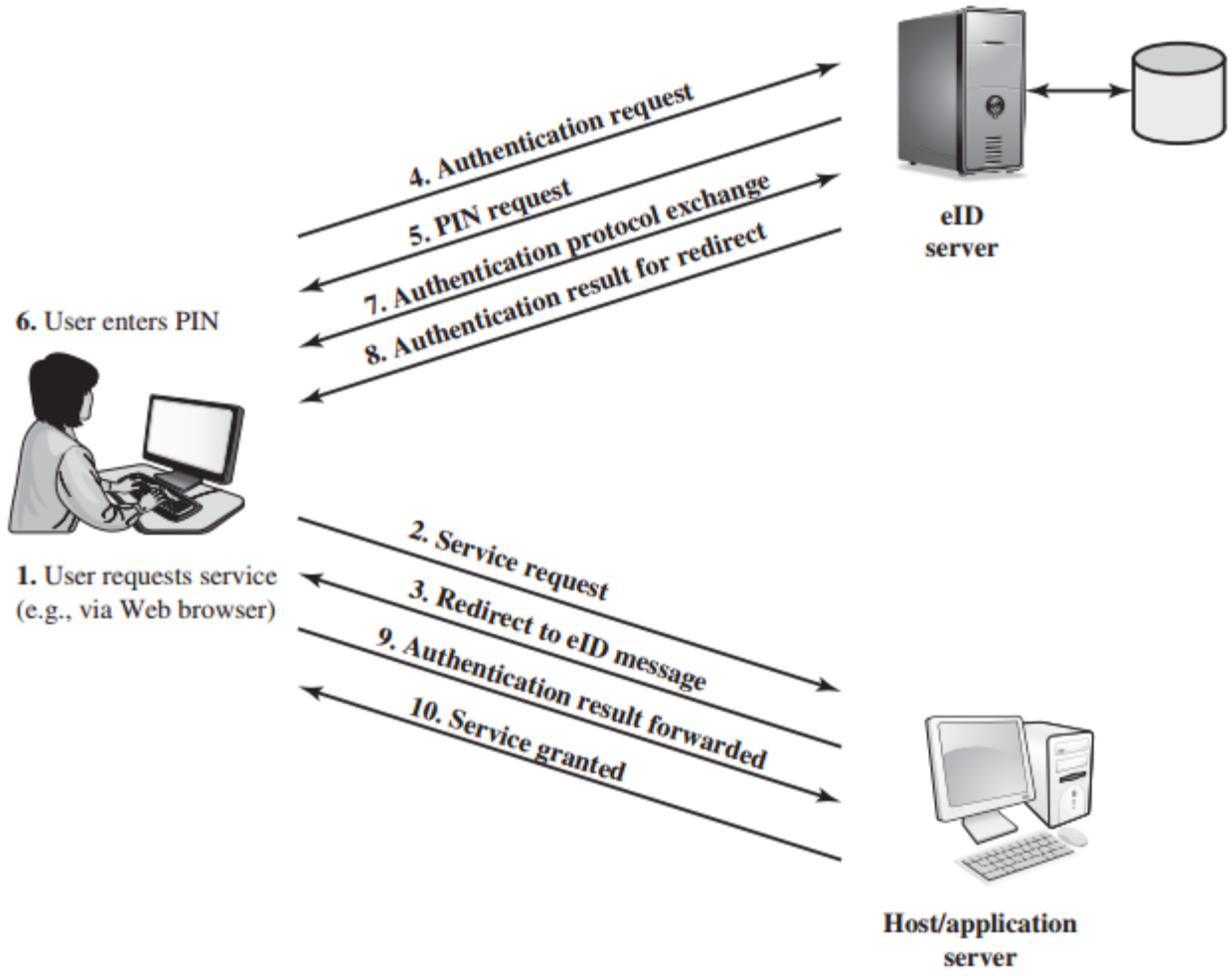
Most advanced deployment is the German card *neuer Personalausweis*

Has human-readable data printed on its surface

- Personal data
- Document number
- Card access number (CAN)
- Machine readable zone (MRZ)

Function	Purpose	PACE Password	Data	Uses
ePass (mandatory)	Authorized offline inspection systems read the data	CAN or MRZ	Face image; two fingerprint images (optional), MRZ data	Offline biometric identity verification reserved for government access
eID (activation optional	Online applications read the data or acess functions as authorized	eID PIN	Family and given names; artistic name and doctoral degree: date and place of birth; address and community ID; expiration date	Identification; age verification; community ID verification; restricted identification (pseudonym); revocation query
	Offline inspection systems read the data and update the address and community ID	CAN or MRZ		
eSign (certificate optional	A certification authority installs the signature certificate online	eID PIN	Signature key; X.509 certificate	Electronic signature creation
	Citizens make electronic signature with eSign PIN	CAN		

CAN = card access number
MRZ = machine readable zone
PACE = password authenticated connection establishment
PIN = personal identification number



User Authentication with eID

Password Authenticated Connection Establishment (PACE)

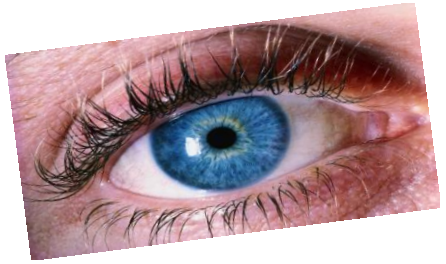
Ensures that the contactless RF chip in the eID card cannot be read without explicit access control

For online applications, access is established by the user entering the 6-digit PIN (which should only be known to the holder of the card)

For offline applications, either the MRZ printed on the back of the card or the six-digit card access number (CAN) printed on the front is used

Biometric Authentication

- Attempts to authenticate an individual based on unique physical characteristics
- Based on pattern recognition
- Is technically complex and expensive when compared to passwords and tokens
- Physical characteristics used include:
  - Facial characteristics
  - Fingerprints
  - Hand geometry
  - Retinal pattern
  - Iris
  - Signature
  - Voice



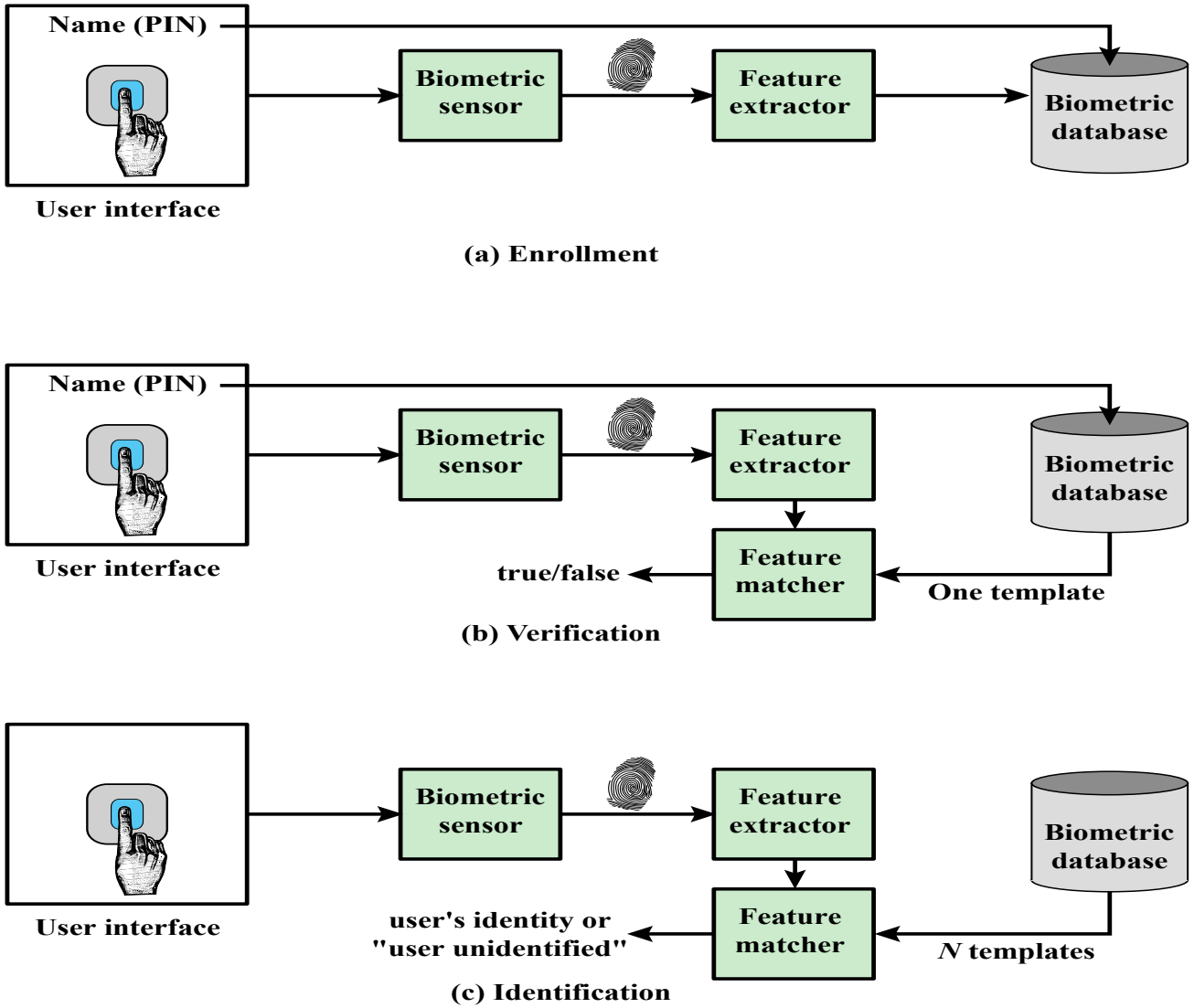


Figure 3.8 A Generic Biometric System. Enrollment creates an association between a user and the user's biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user.

Remote User Authentication

- Authentication over a network, the Internet, or a communications link is more complex
- Additional security threats such as:
  - Eavesdropping, capturing a password, replaying an authentication sequence that has been observed
- Generally rely on some form of a challenge-response protocol to counter threats

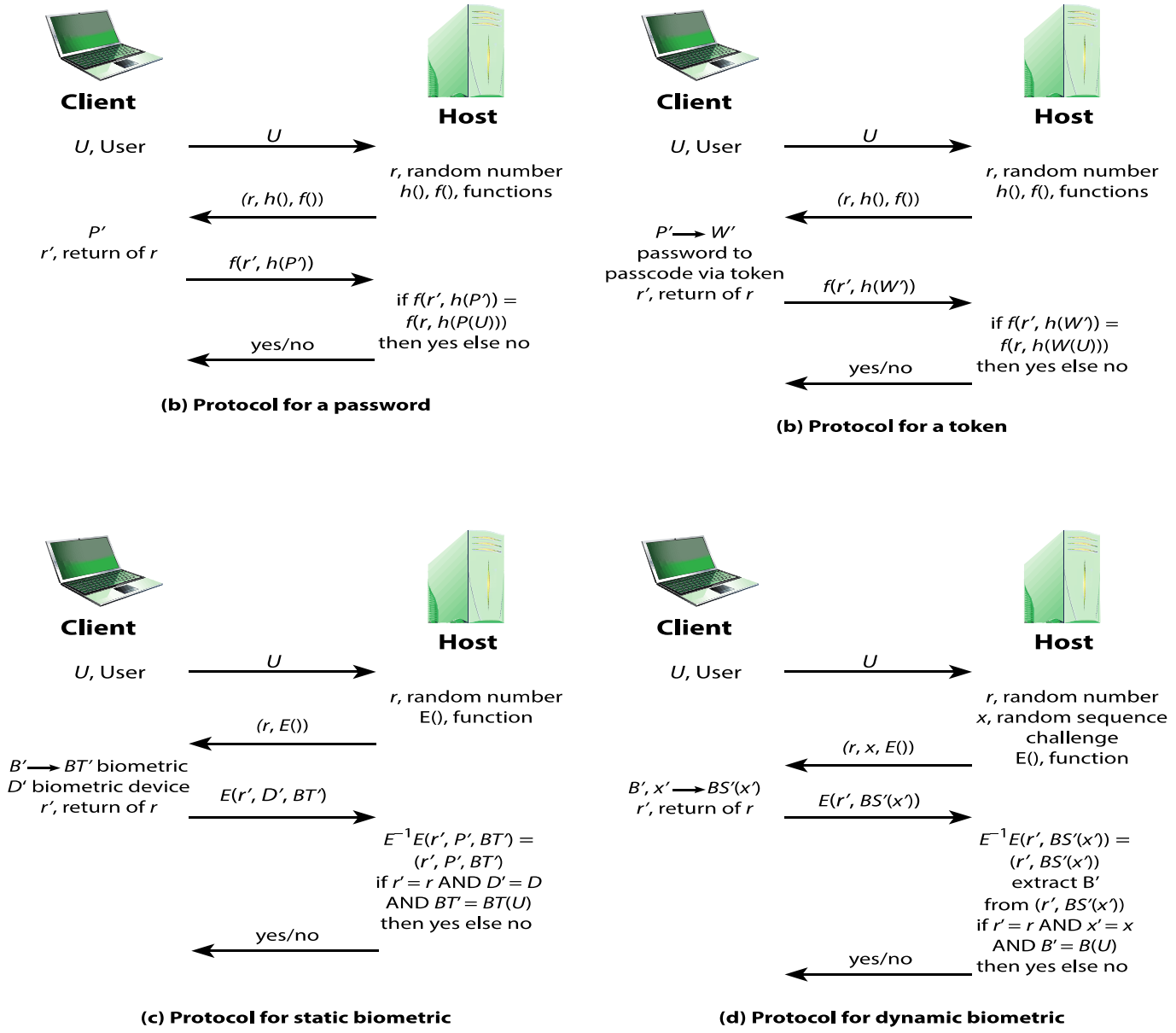
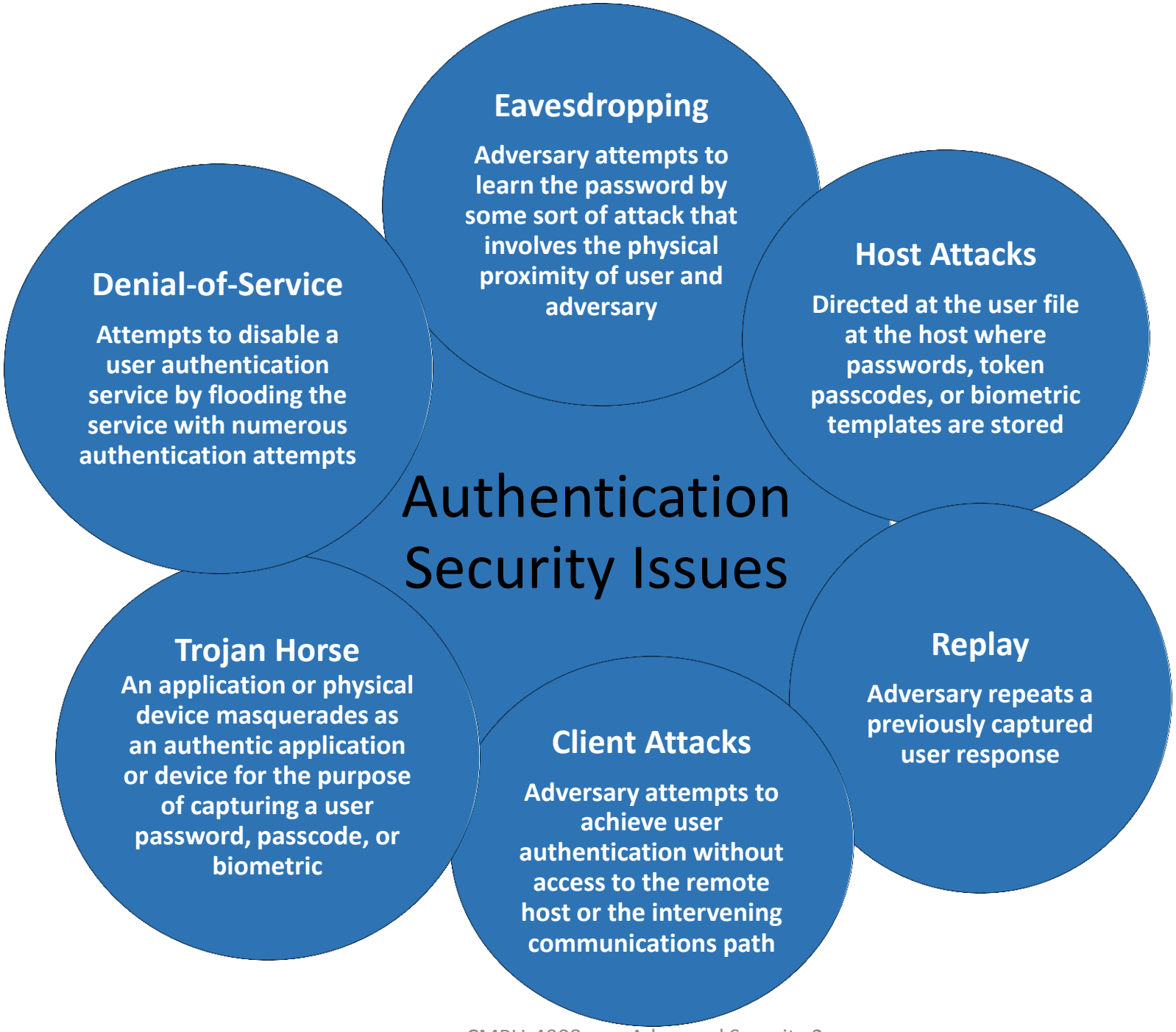


Figure 3.12 Basic Challenge-Response Protocols for Remote User Authentication

Attacks	Authenticators	Examples	Typical defenses
Client attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts, theft of object requires presence
	Biometric	False match	Large entropy; limited attempts
Host attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection of password database
	Token	Passcode theft	Same as password; 1-time passcode
	Biometric	Template theft	Capture device authentication; challenge response
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode
	Biometric	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge-response protocol
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of client or capture device within trusted security perimeter


Authentication Security Issues
Eavesdropping
Adversary attempts to learn the password by some sort of attack that involves the physical proximity of user and adversary
Host Attacks
Directed at the user file at the host where passwords, token passcodes, or biometric templates are stored
Denial-of-Service
Attempts to disable a user authentication service by flooding the service with numerous authentication attempts
Replay
Adversary repeats a previously captured user response
Trojan Horse
An application or physical device masquerades as an authentic application or device for the purpose of capturing a user password, passcode, or biometric
Client Attacks
Adversary attempts to achieve user authentication without access to the remote host or the intervening communications path

Lecture 4
Access Control

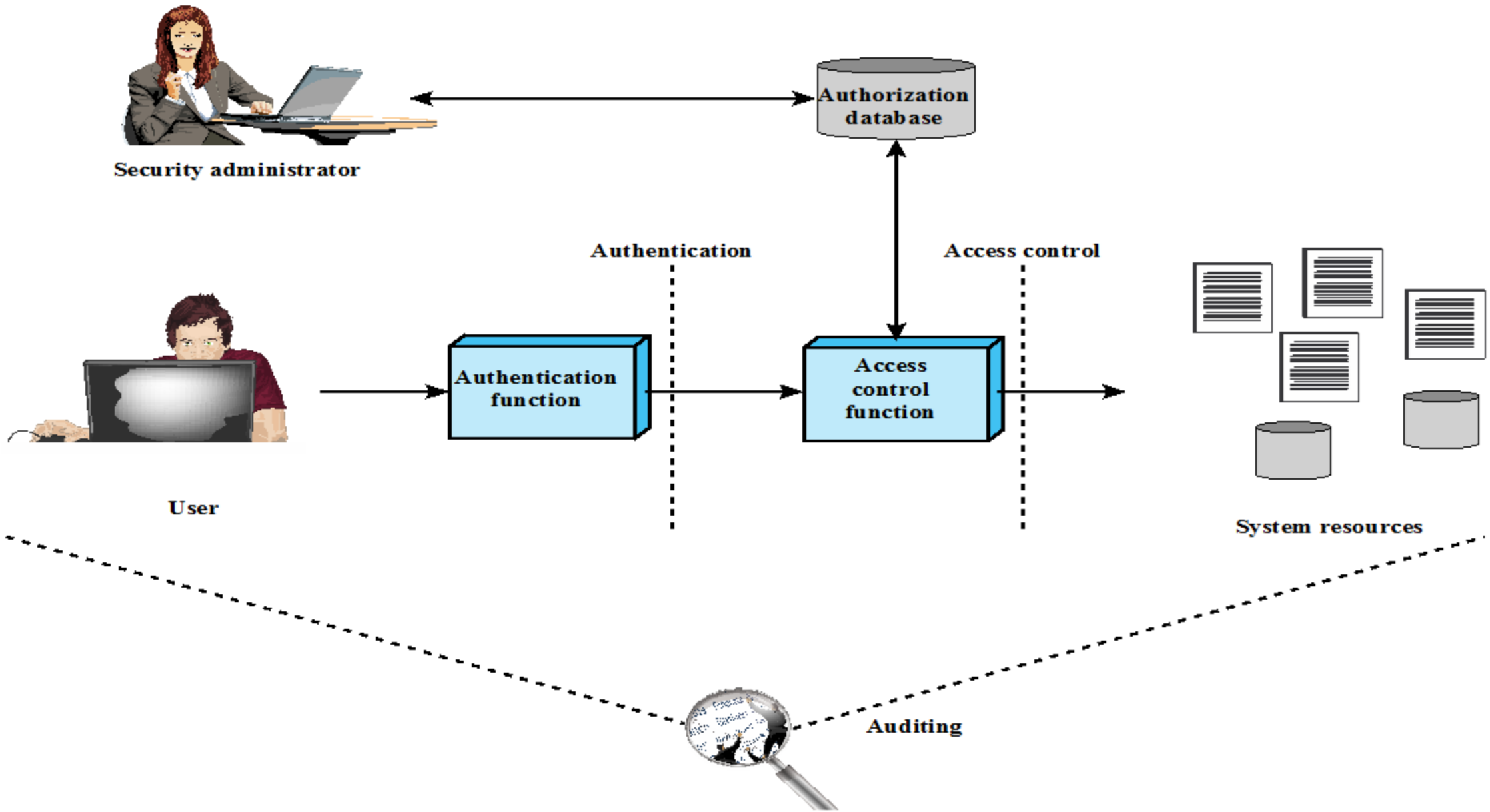
CMPU-4008

Advance Security 2

Access Control Principles

RFC 4949 defines computer security as:

"Measures that implement and assure security services in a computer system, particularly those that assure access control service."



Relationship Among Access Control and Other Security Functions

Access Control Policies

- Discretionary access control (DAC)
  - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do
- Mandatory access control (MAC)
  - Controls access based on comparing security labels with security clearances
- Role-based access control (RBAC)
  - Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles
- Attribute-based access control (ABAC)
  - Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions

Subjects, Objects, and Access Rights

Subject

An entity capable of accessing objects

Three classes
- Owner
- Group
- World

Object

A resource to which access is controlled

Entity used to contain and/or receive information

Access right

Describes the way in which a subject may access an object

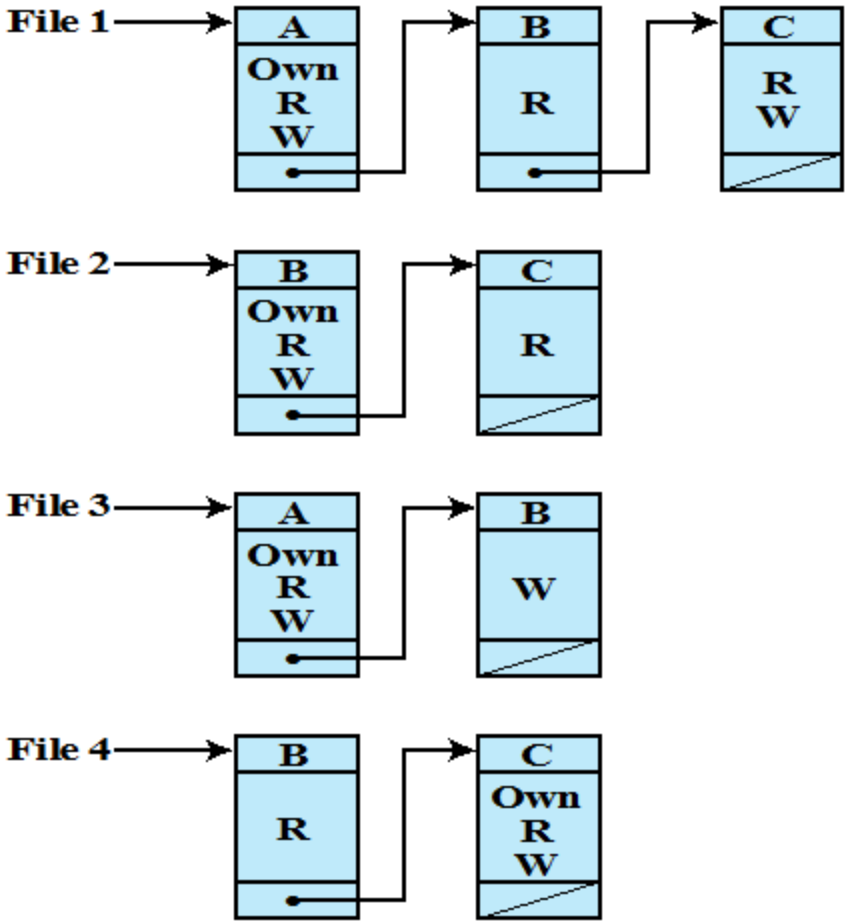
Could include:
- Read
- Write
- Execute
- Delete
- Create
- Search

Discretionary Access Control (DAC)

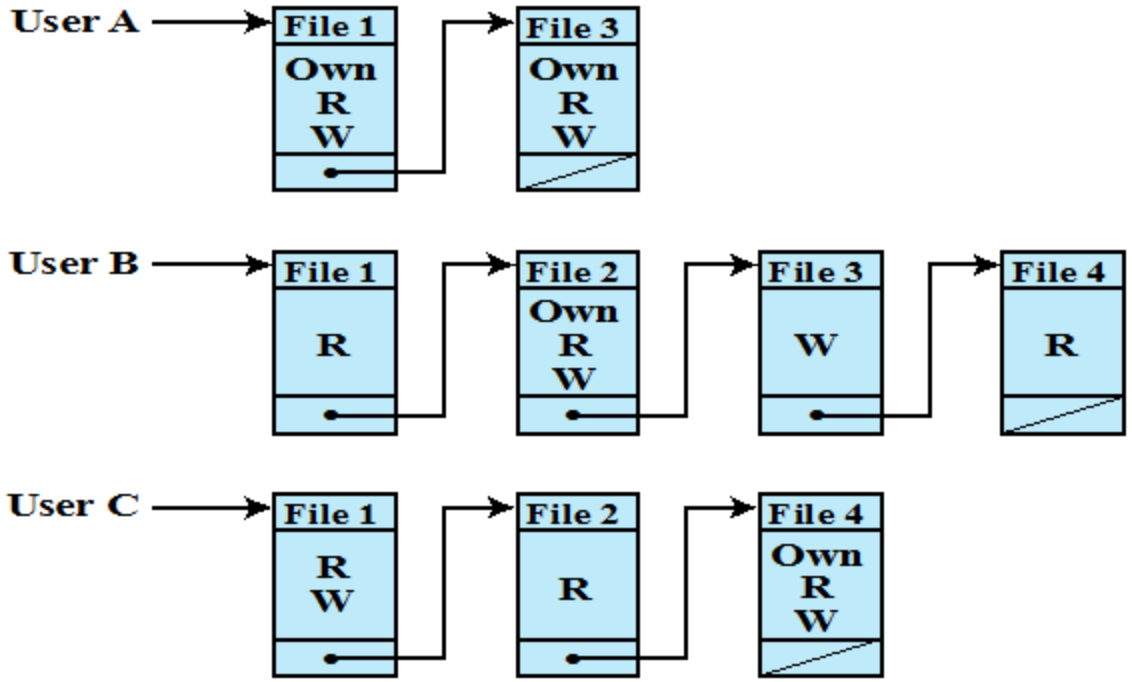
- Scheme in which an entity may enable another entity to access some resource
- Often provided using an access matrix
  - One dimension consists of identified subjects that may attempt data access to the resources
  - The other dimension lists the objects that may be accessed
- Each entry in the matrix indicates the access rights of a particular subject for a particular object

		OBJECTS			
		File 1	File 2	File 3	File 4
SUBJECTS	User A	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

(a) Access matrix



(b) Access control lists for files of part (a)



(c) Capability lists for files of part (a)

Example of Access Control Structures

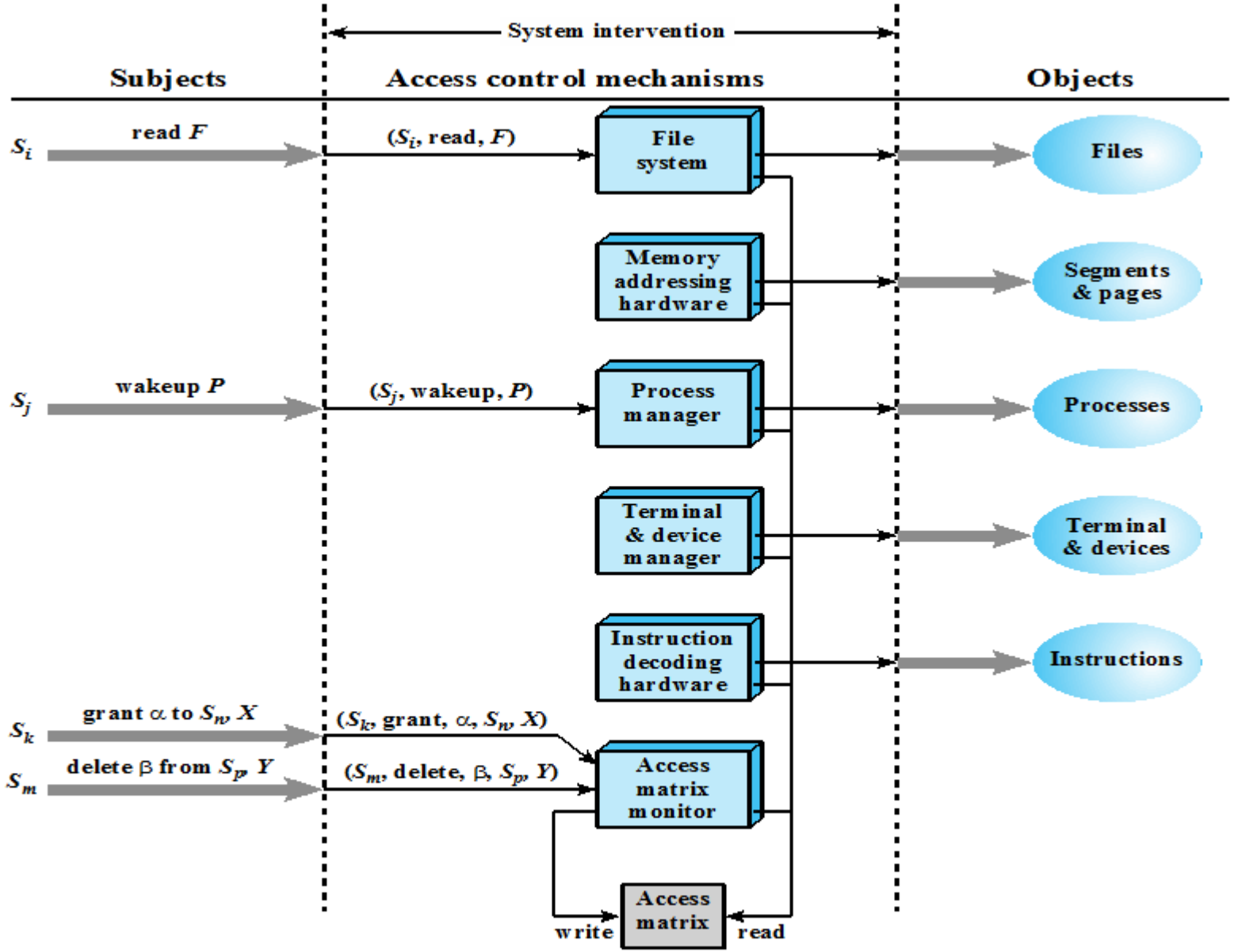
Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

Authorization Table for Files

		OBJECTS								
		subjects			files		processes		disk drives	
		S_1	S_2	S_3	F_1	F_2	P_1	P_2	D_1	D_2
SUBJECTS	S_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S_2		control		write *	execute			owner	seek *
	S_3			control		write	stop			

* – copy flag set

Extended Access Control Matrix



An Organization of the Access Control Function

UNIX File Access Control

UNIX files are administered using inodes (index nodes)

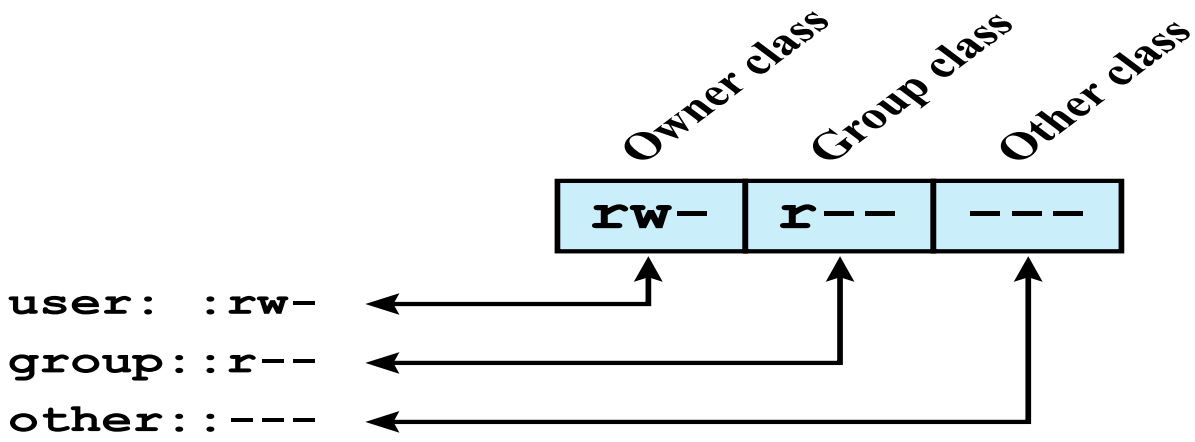
- Control structures with key information needed for a particular file
- Several file names may be associated with a single inode
- An active inode is associated with exactly one file
- File attributes, permissions and control information are sorted in the inode
- On the disk there is an inode table, or inode list, that contains the inodes of all the files in the file system
- When a file is opened its inode is brought into main memory and stored in a memory resident inode table

Directories are structured in a hierarchical tree

- May contain files and/or other directories
- Contains file names plus pointers to associated inodes

UNIX File Access Control

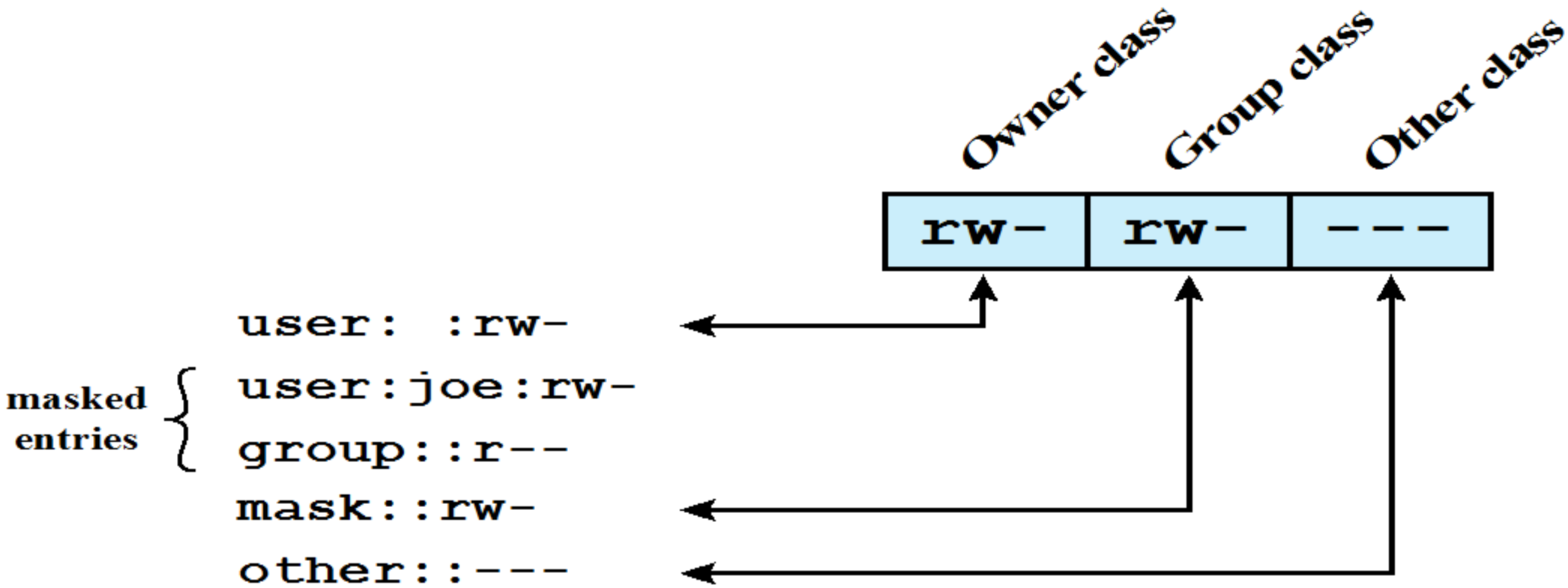
- Unique user identification number (user ID)
- Member of a primary group identified by a group ID
- Belongs to a specific group
- 12 protection bits
  - Specify read, write, and execute permission for the owner of the file, members of the group and all other users
- The owner ID, group ID, and protection bits are part of the file's inode



(a) Traditional UNIX approach (minimal access control list)

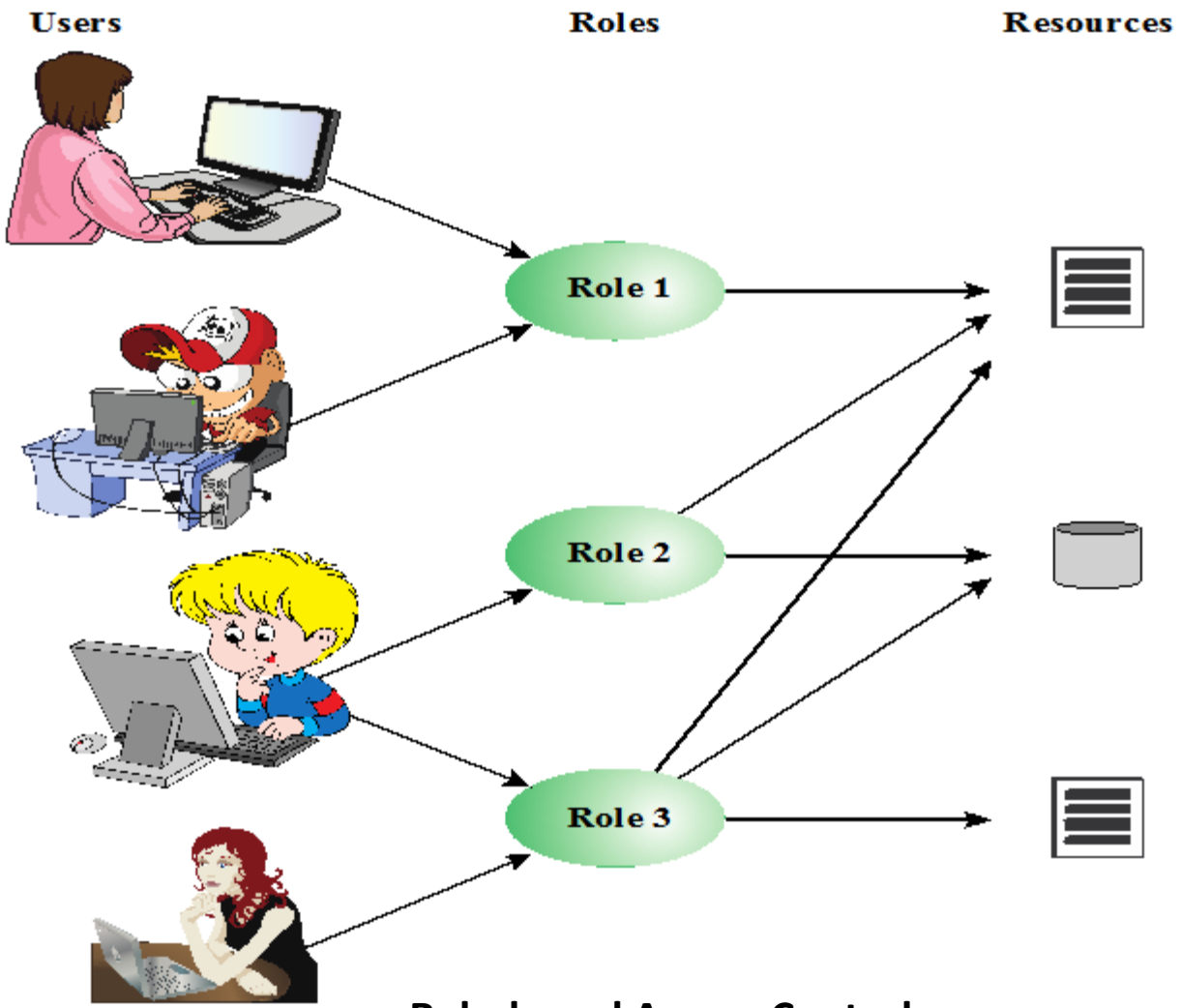
Traditional UNIX File Access Control

- "Set user ID"(SetUID)
- "Set group ID"(SetGID)
  - System temporarily uses rights of the file owner/group in addition to the real user's rights when making access control decisions
  - Enables privileged programs to access files/resources not generally accessible
- Sticky bit
  - When applied to a directory it specifies that only the owner of any file in the directory can rename, move, or delete that file
- Superuser
  - Is exempt from usual access control restrictions
  - Has system-wide access



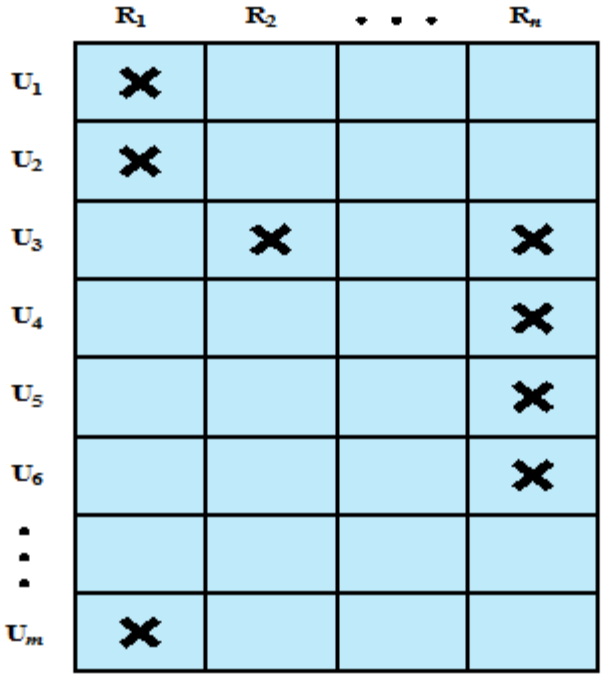
(b) Extended access control list

UNIX File Access Control



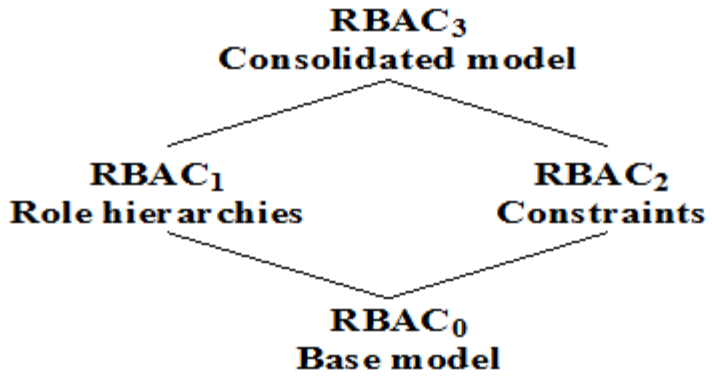
Role-based Access Control

Users, Roles, and Resources

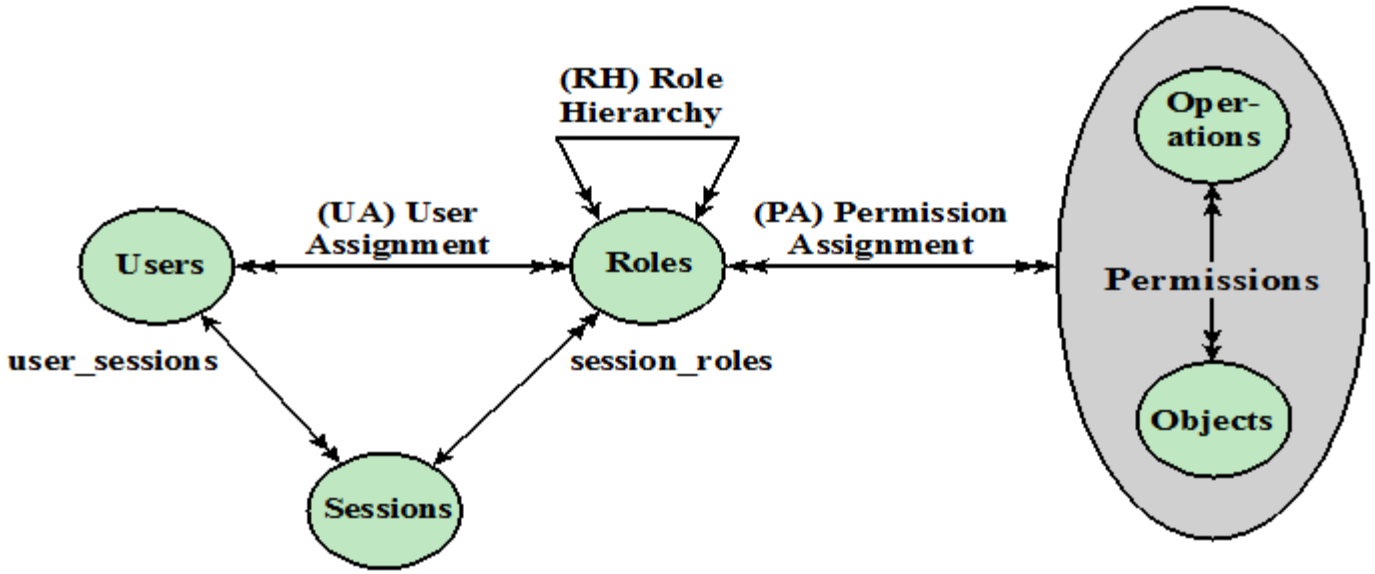


	OBJECTS								
ROLES	R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
...									
R_n			control		write	stop			

Access Control Matrix Representation of RBAC



(a) Relationship among RBAC models

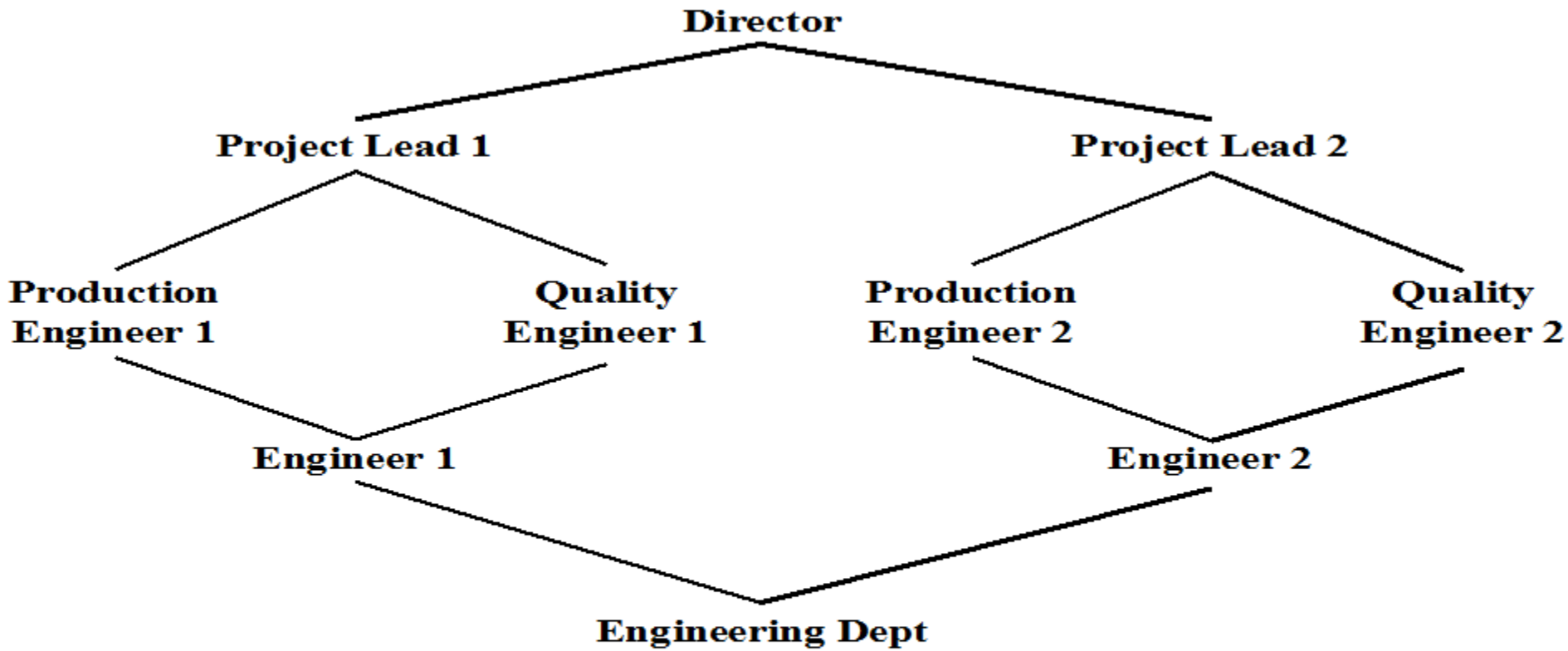


(b) RBAC models

A Family of Role-Based Access Control Models.

Scope RBAC Models

Models	Hierarchies	Constraints
$RBAC_0$	No	No
$RBAC_1$	Yes	No
$RBAC_2$	No	Yes
$RBAC_3$	Yes	Yes



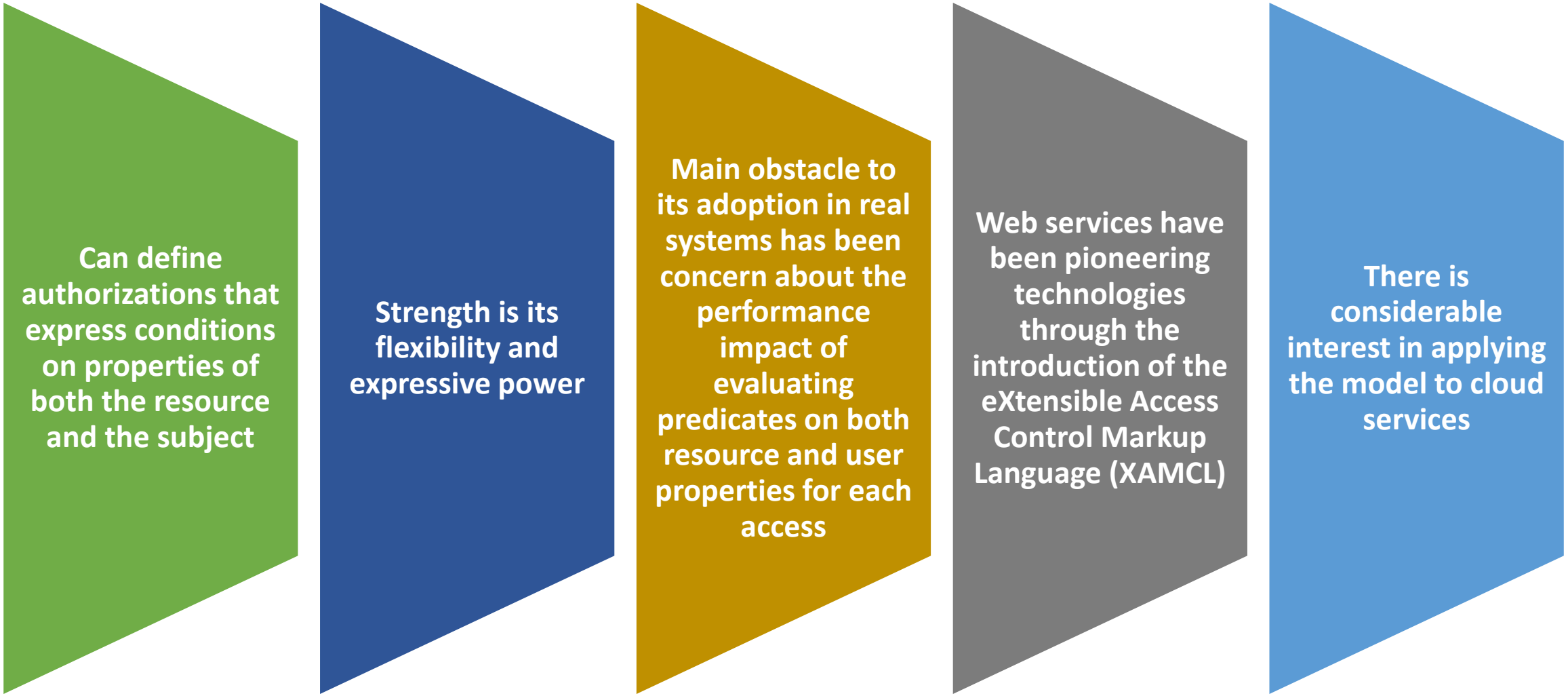
Example of Role Hierarchy

Constraints - RBAC

- Provide a means of adapting RBAC to the specifics of administrative and security policies of an organization
- A defined relationship among roles or a condition related to roles
- Types:

Mutually exclusive roles	Cardinality	Prerequisite roles
• A user can only be assigned to one role in the set (either during a session or statically) • Any permission (access right) can be granted to only one role in the set	• Setting a maximum number with respect to roles	• Dictates that a user can only be assigned to a particular role if it is already assigned to some other specified role

Attribute-Based Access Control (ABAC)



ABAC Model: Attributes

Subject attributes

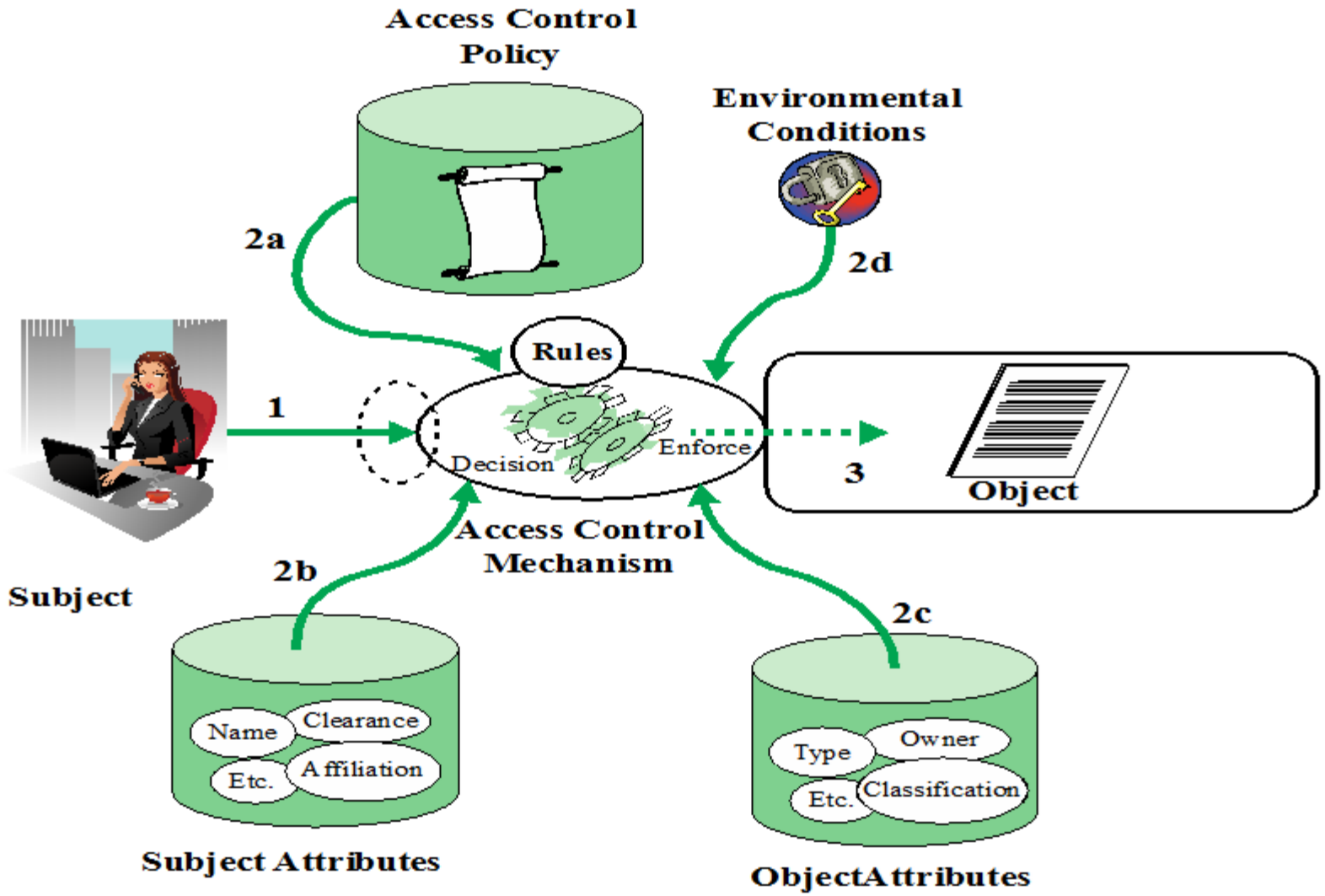
- A subject is an active entity that causes information to flow among objects or changes the system state
- Attributes define the identity and characteristics of the subject

Object attributes

- An object (or resource) is a passive information system-related entity containing or receiving information
- Objects have attributes that can be leverages to make access control decisions

Environment attributes

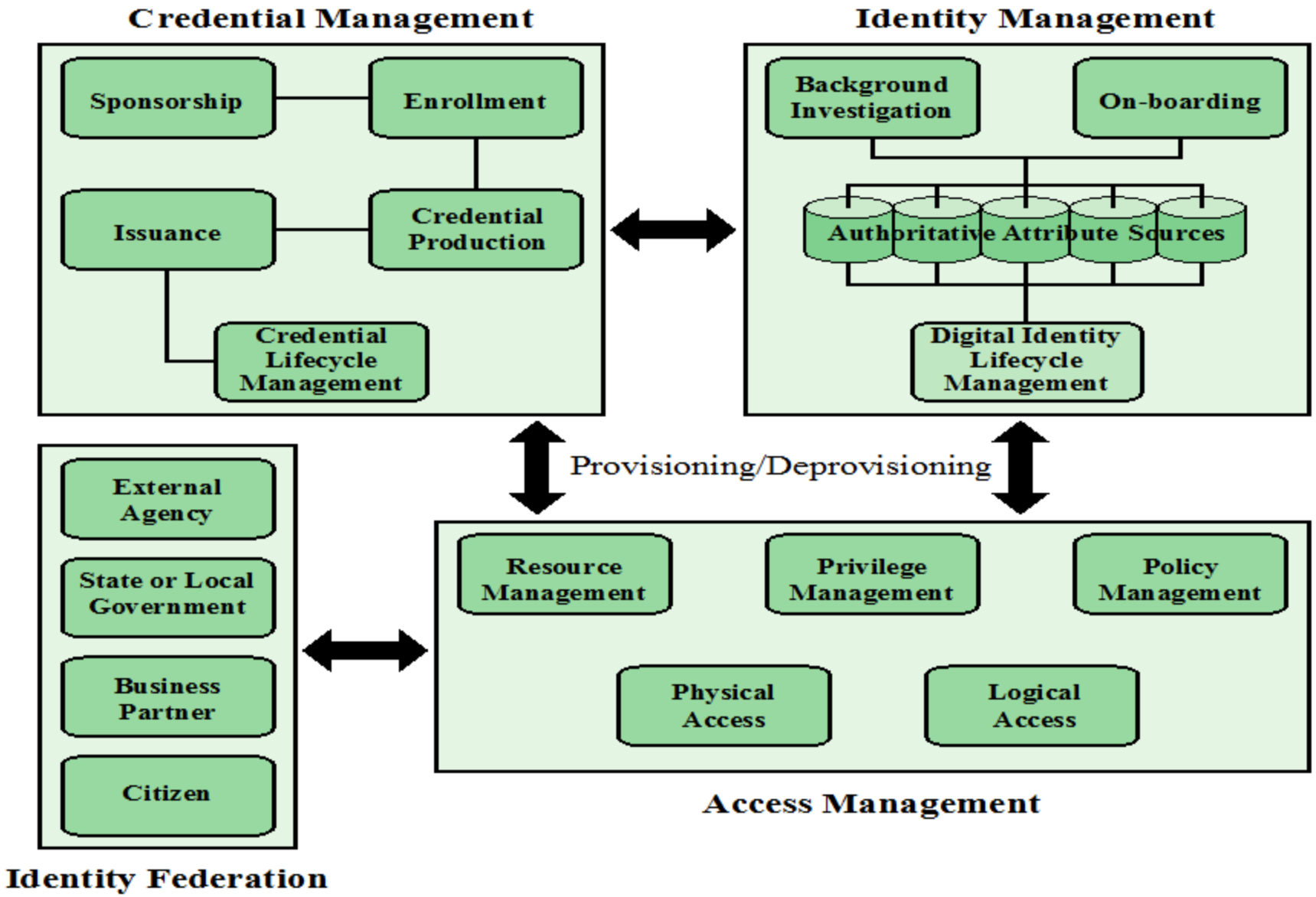
- Describe the operational, technical, and even situational environment or context in which the information access occurs
- These attributes have so far been largely ignored in most access control policies



ABAC Logical Architecture

Identity, Credential, and Access Management (ICAM)

- A comprehensive approach to managing and implementing digital identities, credentials, and access control
- Developed by the U.S. government
- Designed to:
  - Create trusted digital identity representations of individuals and nonperson entities (NPEs)
  - Bind those identities to credentials that may serve as a proxy for the individual of NPE in access transactions
    - A credential is an object or data structure that authoritatively binds an identity to a token possessed and controlled by a subscriber
  - Use the credentials to provide authorized access to an agency's resources



Identity, Credential, and Access Management (ICAM)

Identity Management

Concerned with assigning attributes to a digital identity and connecting that digital identity to an individual or NPE

Goal is to establish a trustworthy digital identity that is independent of a specific application or context

Most common approach to access control for applications and programs is to create a digital representation of an identity for the specific use of the application or program

Maintenance and protection of the identity itself is treated as secondary to the mission associated with the application

Final element is lifecycle management which includes:

- Mechanisms, policies, and procedures for protecting personal identity information
- Controlling access to identity data
- Techniques for sharing authoritative identity data with applications that need it
- Revocation of an enterprise identity

Credential Management

The management of the life cycle of the credential

Examples of credentials are smart cards, private/public cryptographic keys, and digital certificates

Encompasses five logical components:

An authorized individual sponsors an individual or entity for a credential to establish the need for the credential

The sponsored individual enrolls for the credential

- Process typically consists of identity proofing and the capture of biographic and biometric data
- This step may also involve incorporating authoritative attribute data, maintained by the identity management component

A credential is produced

- Depending on the credential type, production may involve encryption, the use of a digital signature, the production of a smart card or other functions

The credential is issued to the individual or NPE

A credential must be maintained over its life cycle

- Might include revocation, reissuance/replacement, reenrollment, expiration, personal identification number (PIN) reset, suspension, or reinstatement

Access Management

Deals with the management and control of the ways entities are granted access to resources

Covers both logical and physical access

May be internal to a system or an external element

Purpose is to ensure that the proper identity verification is made when an individual attempts to access a security sensitive building, computer systems, or data

Three support elements are needed for an enterprise-wide access control facility:

- **Resource management**
- **Privilege management**
- **Policy management**

Three support elements are needed for an enterprise-wide access control facility:

Resource management

- Concerned with defining rules for a resource that requires access control
- Rules would include credential requirements and what user attributes, resource attributes, and environmental conditions are required for access of a given resource for a given function

Privilege management

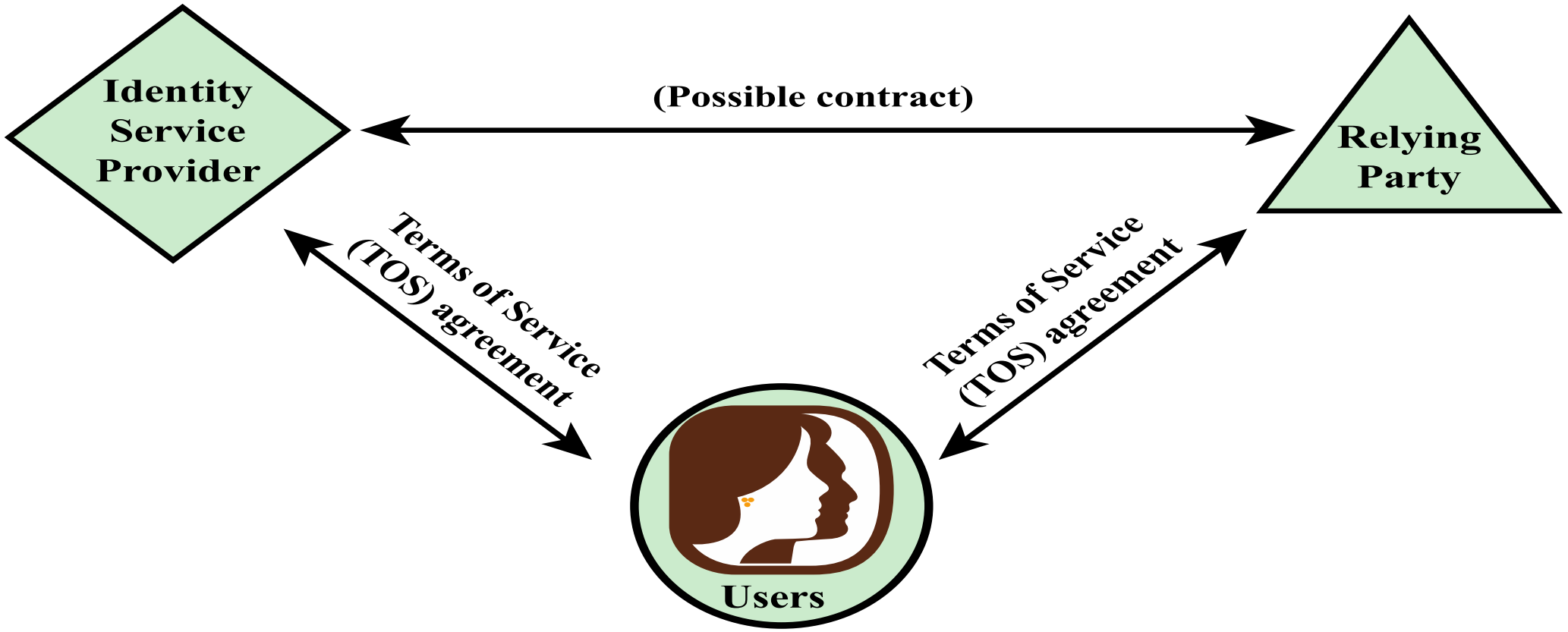
- Concerned with establishing and maintaining the entitlement or privilege attributes that comprise an individual's access profile
- These attributes represent features of an individual that can be used as the basis for determining access decisions to both physical and logical resources
- Privileges are considered attributes that can be linked to a digital identity

Policy management

- Governs what is allowable and unallowable in an access transaction

Identity Federation

- Term used to describe the technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization
- Addresses two questions:
  - How do you trust identities of individuals from external organizations who need access to your systems
  - How do you vouch for identities of individuals in your organization when they need to collaborate with external organizations



(a) Traditional triangle of parties involved in an exchange of identity information

Identity Information Exchange Approaches

Open Identity Trust Framework

OpenID

- An open standard that allows users to be authenticated by certain cooperating sites using a third party service

OIDF

- OpenID Foundation is an international nonprofit organization of individuals and companies committed to enabling, promoting, and protecting OpenID technologies

ICF

- Information Card Foundation is a nonprofit community of companies and individuals working together to evolve the Information Card ecosystem

OITF

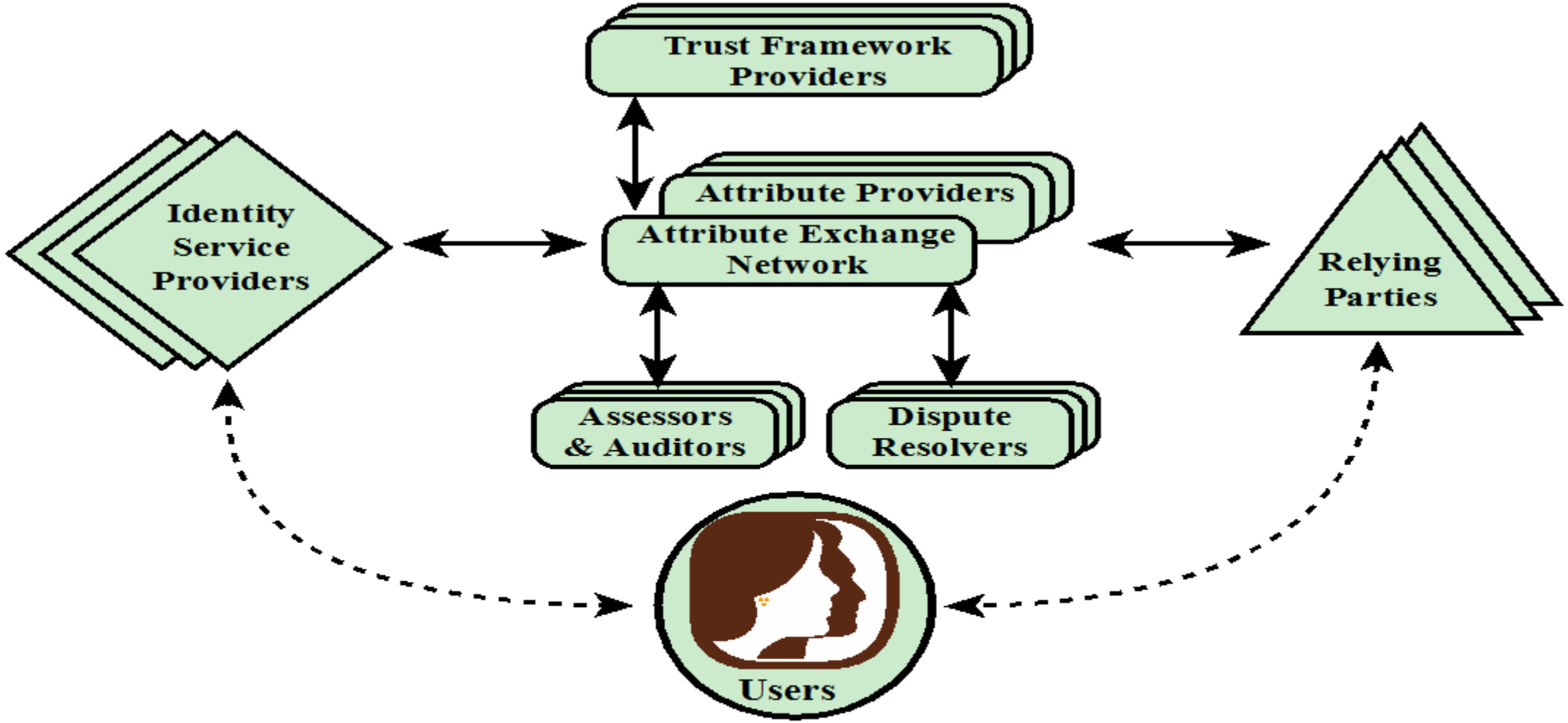
- Open Identity Trust Framework is a standardized, open specification of a trust framework for identity and attribute exchange, developed jointly by OIDF and ICF

OIX

- Open Identity Exchange Corporation is an independent, neutral, international provider of certification trust frameworks conforming to the OITF model

AXN

- Attribute Exchange Network is an online Internet-scale gateway for identity service providers and relying parties to efficiently access user asserted, permissioned, and verified online identity attributes in high volumes at affordable costs



(B) Identity attribute exchange elements

Identity Information Exchange Approaches

Lecture 5
Database and Cloud security

CMPU-4008

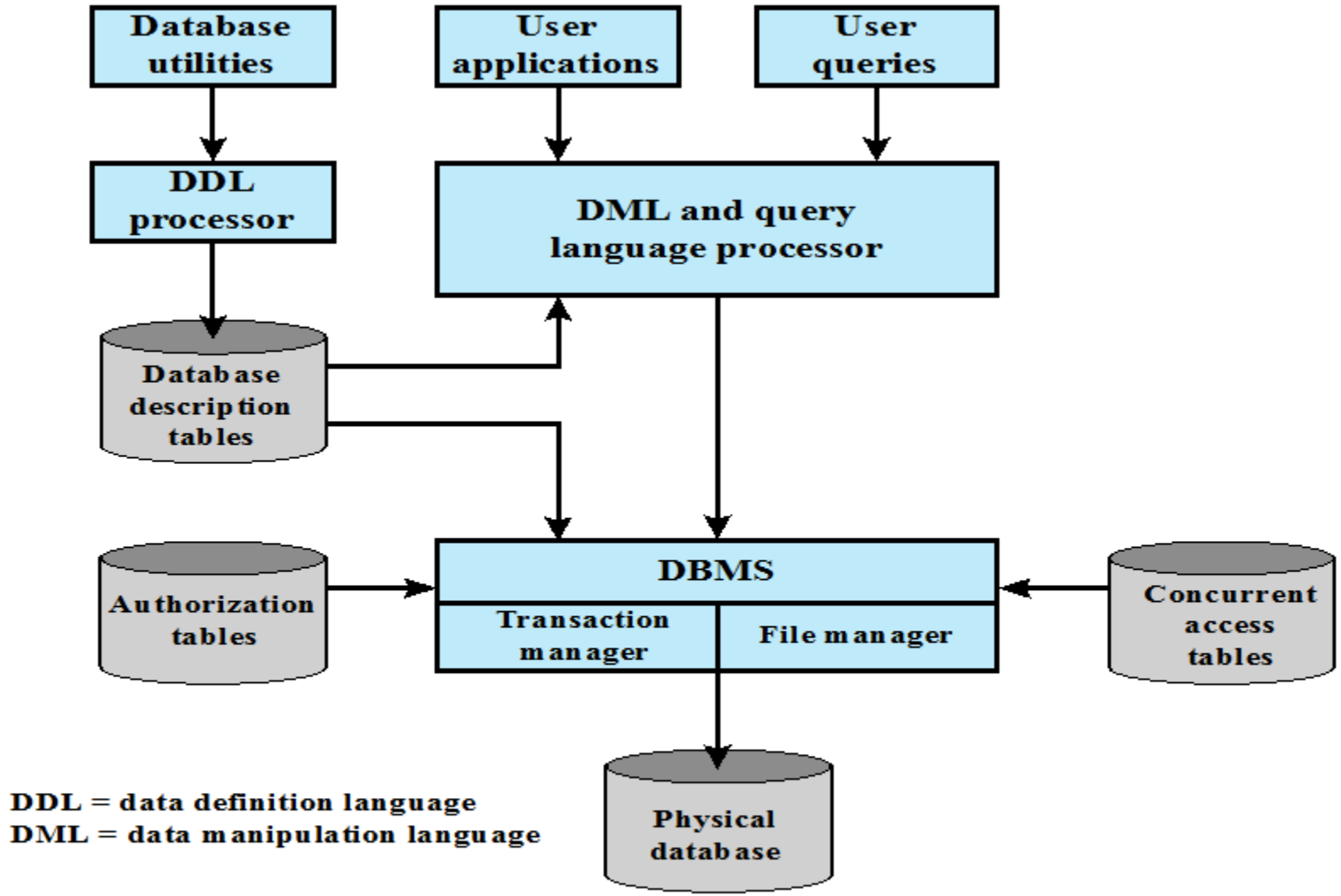
Advance Security 2

Databases

- Structured collection of data stored for use by one or more applications
- Contains the relationships between data items and groups of data items
- Can sometimes contain sensitive data that needs to be secured
- Query language
  - Provides a uniform interface to the database

Database management system (DBMS)

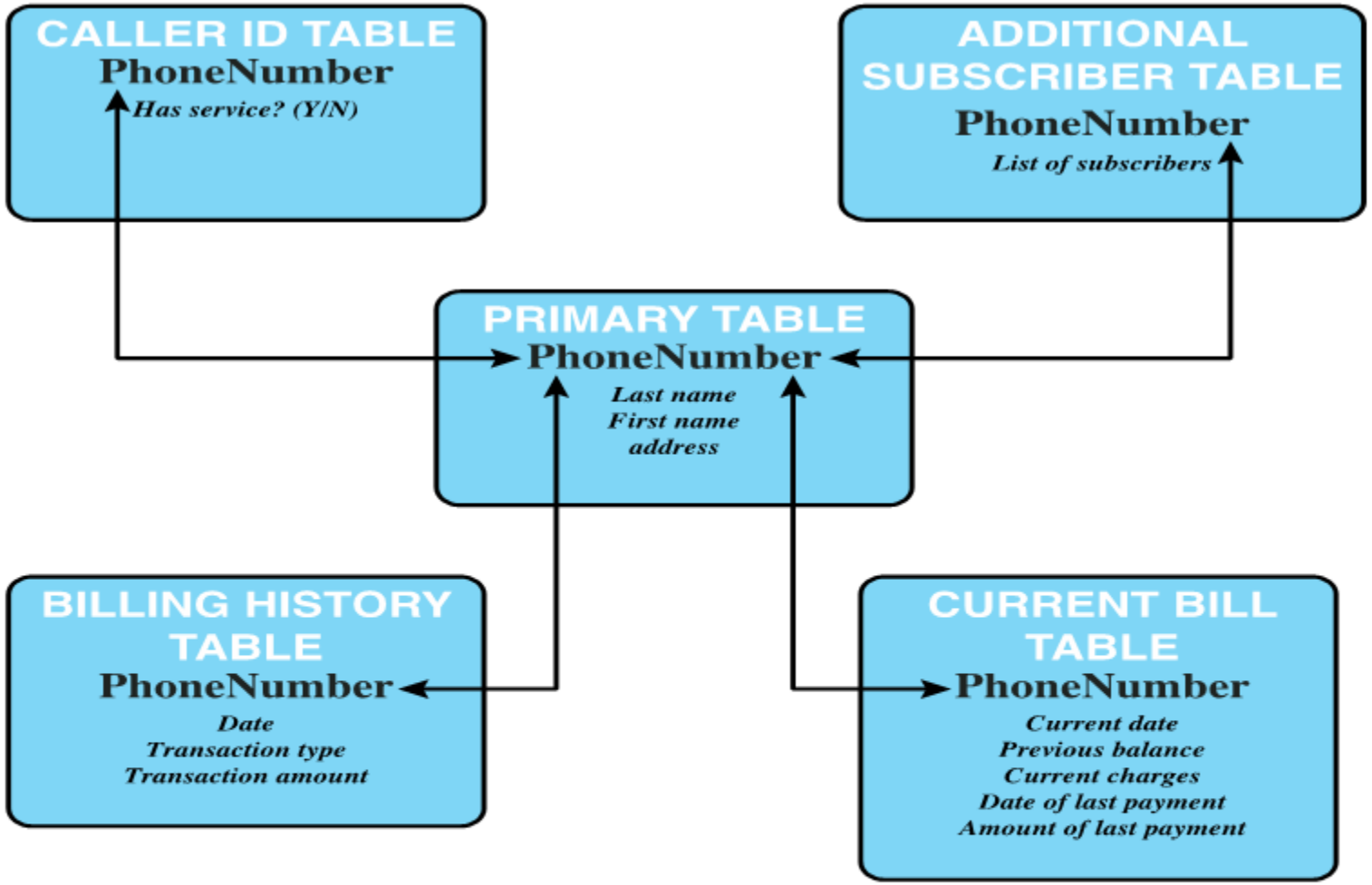
- Suite of programs for constructing and maintaining the database
- Offers ad hoc query facilities to multiple users and applications



DBMS Architecture

Relational Databases

- Table of data consisting of rows and columns
  - Each column holds a particular type of data
  - Each row contains a specific value for each column
  - Ideally has one column where all values are unique, forming an identifier/key for that row
- Enables the creation of multiple tables linked together by a unique identifier that is present in all tables
- Use a relational query language to access the database
  - Allows the user to request data that fit a given set of criteria



Example Relational Database Model. A relational database uses multiple tables related to one another by a designated key; in this case the key is the PhoneNumber field.

Relational Database Elements

- Relation/table/file
- Tuple/row/record
- Attribute/column/field

Primary key

- Uniquely identifies a row
- Consists of one or more column names

Foreign key

- Links one table to attributes in another

View/virtual table

- Result of a query that returns selected rows and columns from one or more tables

Basic Terminology for Relational Databases

Formal Name	Common Name	Also Known As
Relation	Table	File
Tuple	Row	Record
Attribute	Column	Field

Department Table

Did	Dname	Dacctno
4	human resources	528221
8	education	202035
9	accounts	709257
13	public relations	755827
15	services	223945

primary key

Employee Table

Ename	Did	Salarycode	Eid	Ephone
Robin	15	23	2345	6127092485
Neil	13	12	5088	6127092246
Jasmine	4	26	7712	6127099348
Cody	15	22	9664	6127093148
Holly	8	23	3054	6127092729
Robin	8	24	2976	6127091945
Smith	9	21	4490	6127099380

foreign key

primary key

(a) Two tables in a relational database

Dname	Ename	Eid	Ephone
human resources	Jasmine	7712	6127099348
education	Holly	3054	6127092729
education	Robin	2976	6127091945
accounts	Smith	4490	6127099380
public relations	Neil	5088	6127092246
services	Robin	2345	6127092485
services	Cody	9664	6127093148

(b) A view derived from the database

Relational Database Example

Structured Query Language (SQL)

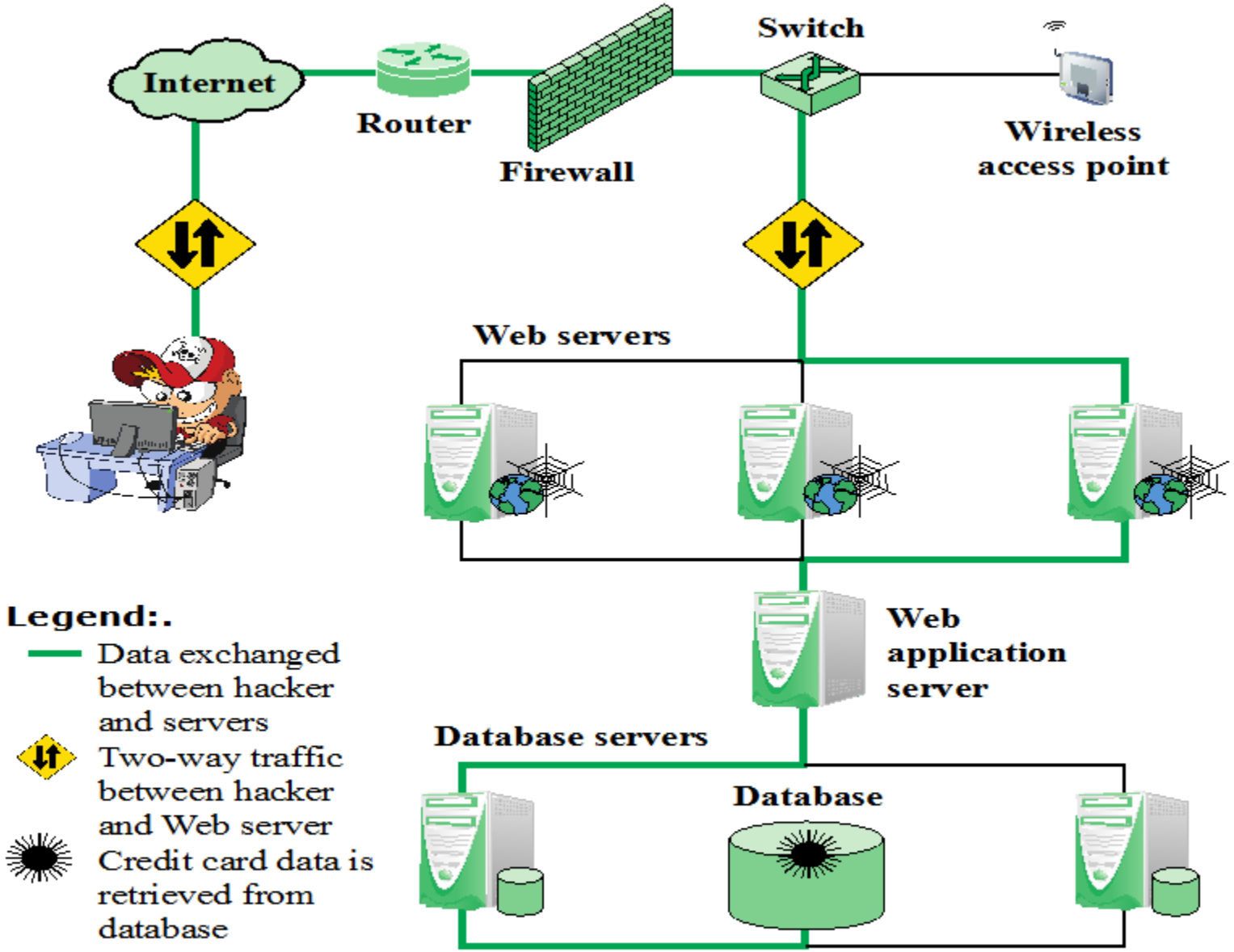
- Standardized language to define schema, manipulate, and query data in a relational database
- Several similar versions of ANSI/ISO standard
- All follow the same basic syntax and semantics

SQL statements can be used to:

- Create tables
- Insert and delete data in tables
- Create views
- Retrieve data with query statements

SQL Injection Attacks (SQLi)

- One of the most prevalent and dangerous network-based security threats
- Designed to exploit the nature of Web application pages
- Sends malicious SQL commands to the database server
- Most common attack goal is bulk extraction of data
- Depending on the environment SQL injection can also be exploited to:
  - Modify or delete data
  - Execute arbitrary operating system commands
  - Launch denial-of-service (DoS) attacks



Typical SQL Injection Attack

Injection Technique

The SQLi attack typically works by prematurely terminating a text string and appending a new command

Because the inserted command may have additional strings appended to it before it is executed the attacker terminates the injected string with a comment mark “- -”

Subsequent text is ignored at execution time

SQLi Attack Avenues

User input

- Attackers inject SQL commands by providing suitable crafted user input

Server variables

- Attackers can forge the values that are placed in HTTP and network headers and exploit this vulnerability by placing data directly into the headers

Second-order injection

- A malicious user could rely on data already present in the system or database to trigger an SQL injection attack, so when the attack occurs, the input that modifies the query to cause an attack does not come from the user, but from within the system itself

Cookies

- An attacker could alter cookies such that when the application server builds an SQL query based on the cookie's content, the structure and function of the query is modified

Physical user input

- Applying user input that constructs an attack outside the realm of web requests

Inband Attacks

- Uses the same communication channel for injecting SQL code and retrieving results
- The retrieved data are presented directly in application Web page
- Include:

Tautology

This form of attack injects code in one or more conditional statements so that they always evaluate to true

End-of-line comment

After injecting code into a particular field, legitimate code that follows are nullified through usage of end of line comments

Piggybacked queries

The attacker adds additional queries beyond the intended query, piggy-backing the attack on top of a legitimate request

Inferential Attack

- There is no actual transfer of data, but the attacker is able to reconstruct the information by sending particular requests and observing the resulting behavior of the Website/database server
- Include:
  - Illegal/logically incorrect queries
    - This attack lets an attacker gather important information about the type and structure of the backend database of a Web application
    - The attack is considered a preliminary, information-gathering step for other attacks
  - Blind SQL injection
    - Allows attackers to infer the data present in a database system even when the system is sufficiently secure to not display any erroneous information back to the attacker

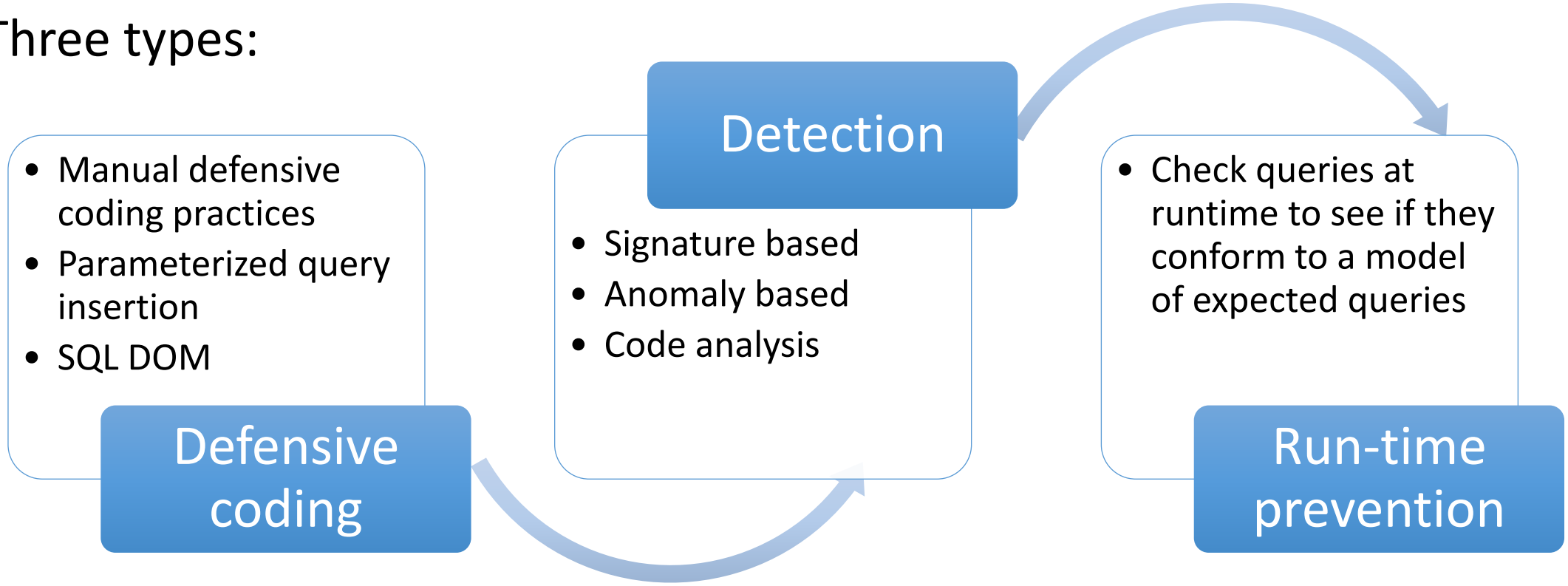
Out-of-Band Attack

- Data are retrieved using a different channel

- This can be used when there are limitations on information retrieval, but outbound connectivity from the database server is lax

SQLi Countermeasures

- Three types:



Database Access Control

Database access control system determines:

If the user has access to the entire database or just portions of it

What access rights the user has (create, insert, delete, update, read, write)

Can support a range of administrative policies

Centralized administration

- Small number of privileged users may grant and revoke access rights

Ownership-based administration

- The creator of a table may grant and revoke access rights to the table

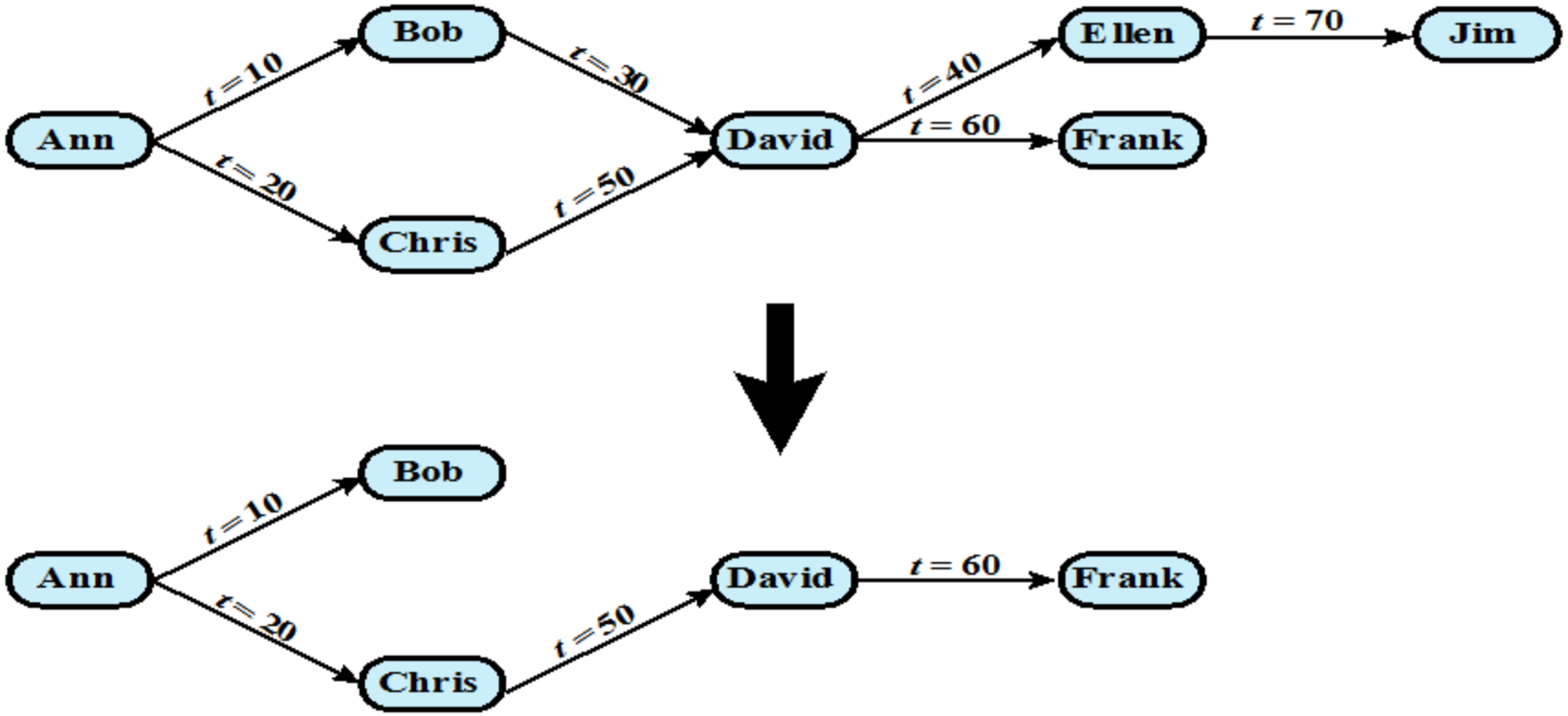
Decentralized administration

- The owner of the table may grant and revoke authorization rights to other users, allowing them to grant and revoke access rights to the table

SQL Access Controls

- Two commands for managing access rights:
  - Grant
    - Used to grant one or more access rights or can be used to assign a user to a role
  - Revoke
    - Revokes the access rights
- Typical access rights are:
  - Select
  - Insert
  - Update
  - Delete
  - References

Example of Cascading Authorizations



Bob Revokes Privilege from David

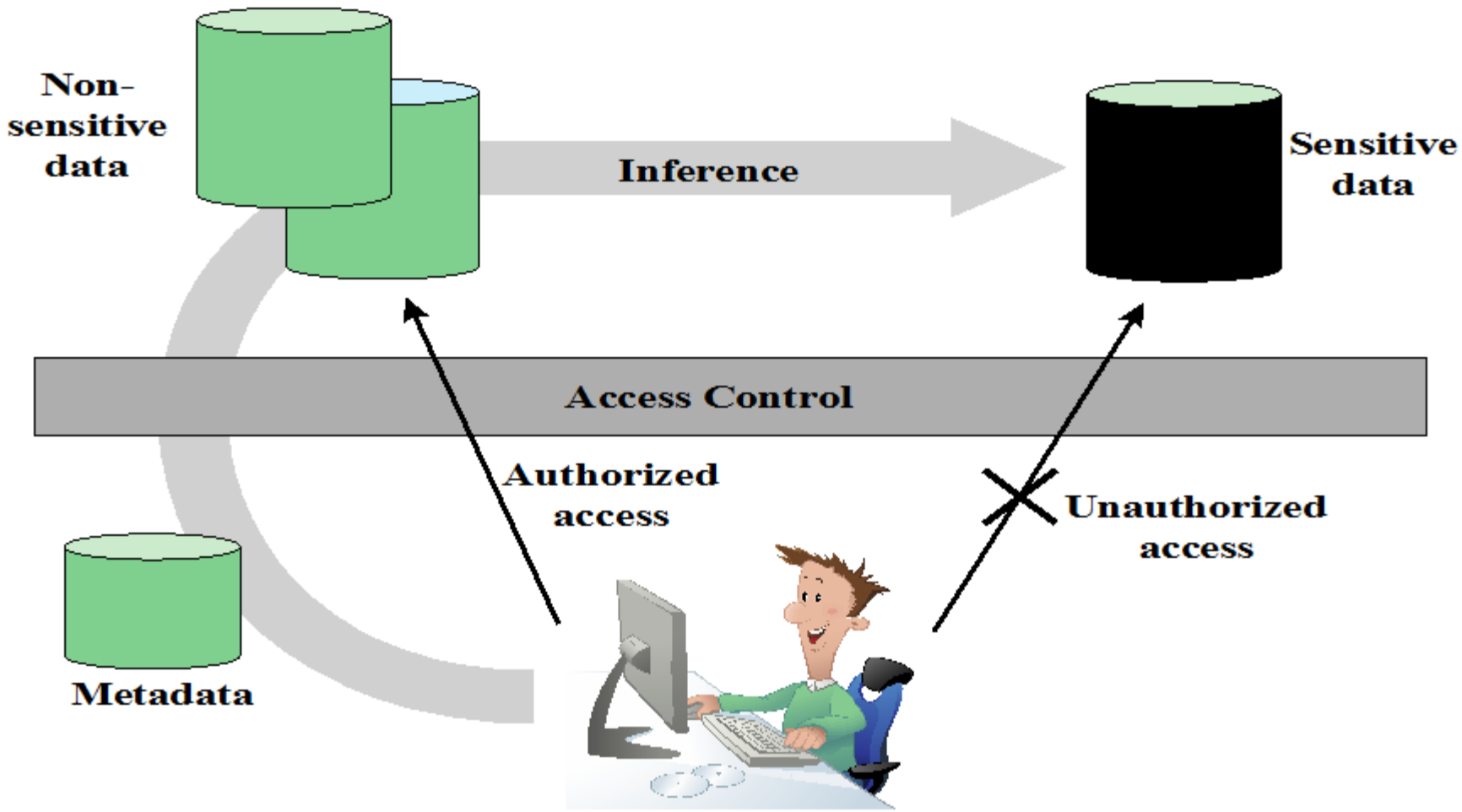
Role-Based Access Control (RBAC)

- Role-based access control eases administrative burden and improves security
- A database RBAC needs to provide the following capabilities:
  - Create and delete roles
  - Define permissions for a role
  - Assign and cancel assignment of users to roles
- Categories of database users:

Application owner	End user	Administrator
• An end user who owns database objects as part of an application	• An end user who operates on database objects via a particular application but does not own any of the database objects	• User who has administrative responsibility for part or all of the database

Fixed Roles in Microsoft SQL Server

Role	Permissions
Fixed Server Roles	
sysadmin	Can perform any activity in SQL Server and have complete control over all database functions
serveradmin	Can set server-wide configuration options, shut down the server
setupadmin	Can manage linked servers and startup procedures
securityadmin	Can manage logins and CREATE DATABASE permissions, also read error logs and change passwords
processadmin	Can manage processes running in SQL Server
dbcreator	Can create, alter, and drop databases
diskadmin	Can manage disk files
bulkadmin	Can execute BULK INSERT statements
Fixed Database Roles	
db_owner	Has all permissions in the database
db_accessadmin	Can add or remove user IDs
db_datareader	Can select all data from any user table in the database
db_datawriter	Can modify any data in any user table in the database
db_ddladmin	Can issue all Data Definition Language (DDL) statements
db_securityadmin	Can manage all permissions, object ownerships, roles and role memberships
db_backupoperator	Can issue DBCC, CHECKPOINT, and BACKUP statements
db_denydatareader	Can deny permission to select data in the database
db_denydatawriter	Can deny permission to change data in the database



Indirect Information Access Via Inference Channel

Item	Availability	Cost ($)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware
Cake pan	online only	12.99	housewares
Shower/tub cleaner	in-store/online	11.99	housewares
Rolling pin	in-store/online	10.99	housewares

(a) Inventory table

Availability	Cost ($)
in-store/online	7.99
online only	5.49
in-store/online	104.99

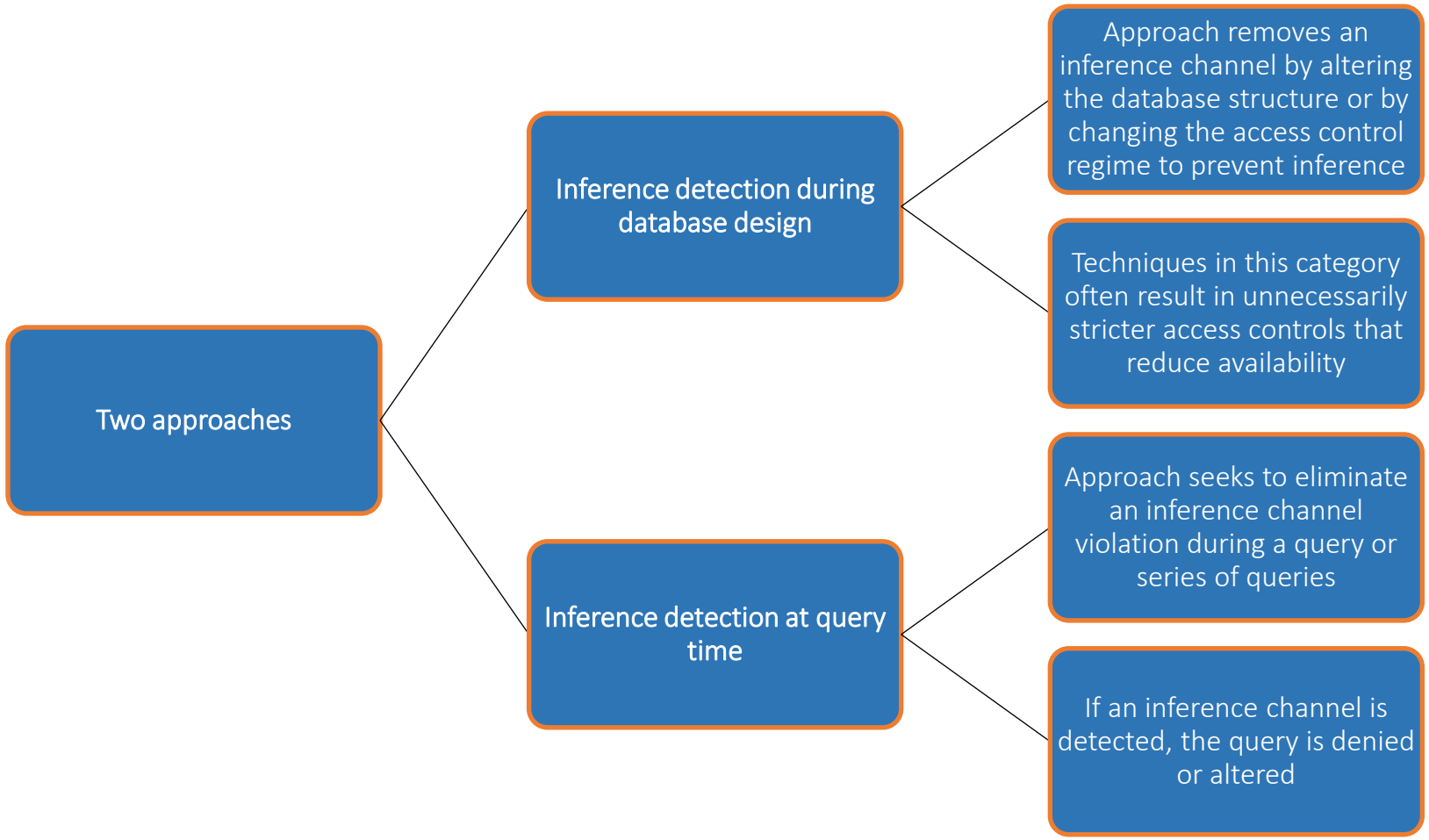
Item	Department
Shelf support	hardware
Lid support	hardware
Decorative chain	hardware

(b) Two views

Item	Availability	Cost ($)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware

(c) Table derived from combining query answers

Inference Detection



- Some inference detection algorithm is needed for either of these approaches
- Progress has been made in devising specific inference detection techniques for multilevel secure databases and statistical databases

Database Encryption

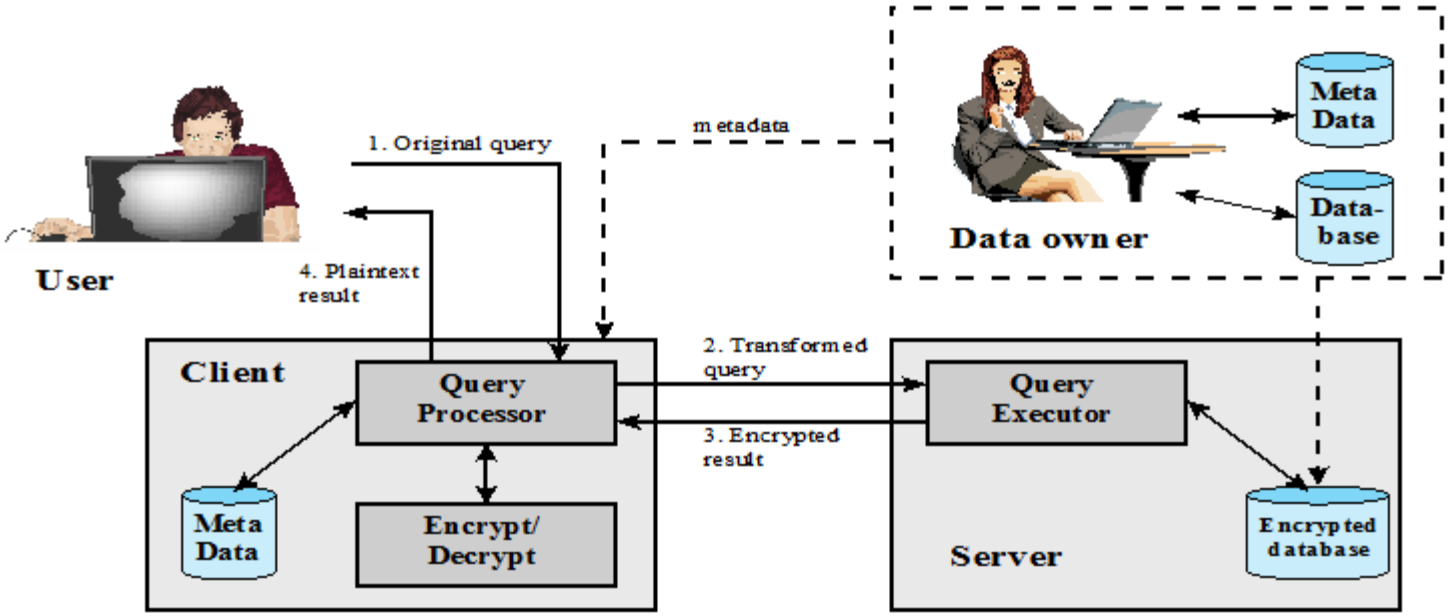
- The database is typically the most valuable information resource for any organization
  - Protected by multiple layers of security
    - Firewalls, authentication, general access control systems, DB access control systems, database encryption
    - Encryption becomes the last line of defense in database security
  - Can be applied to the entire database, at the record level, the attribute level, or level of the individual field
- Disadvantages to encryption:
  - Key management
    - Authorized users must have access to the decryption key for the data for which they have access
  - Inflexibility
    - When part or all of the database is encrypted it becomes more difficult to perform record searching

Data owner – organization that produces data to be made available for controlled release

User – human entity that presents queries to the system

Client – frontend that transforms user queries into queries on the encrypted data stored on the server

Server – an organization that receives the encrypted data from a data owner and makes them available for distribution to clients

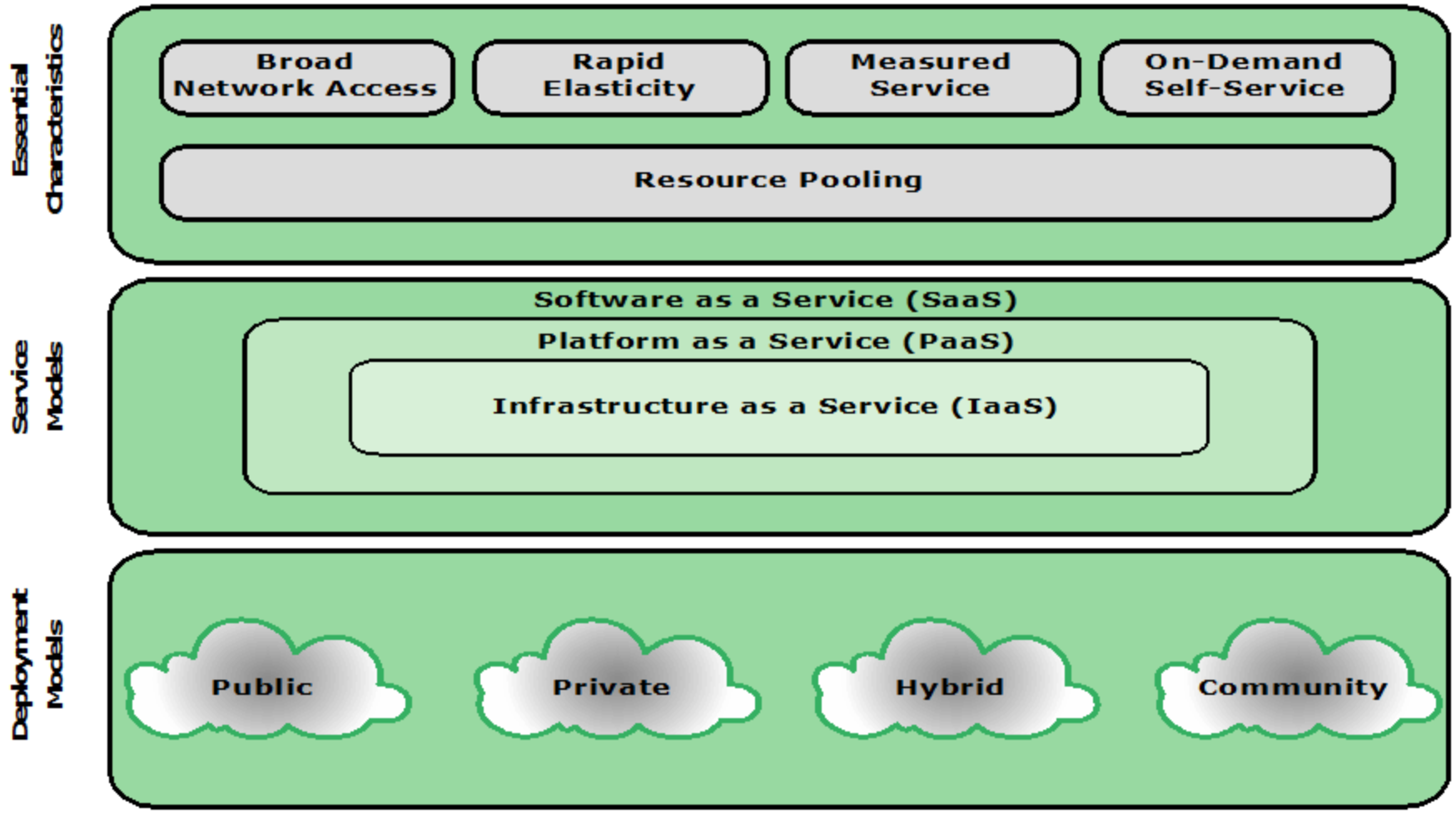


A Database Encryption Scheme

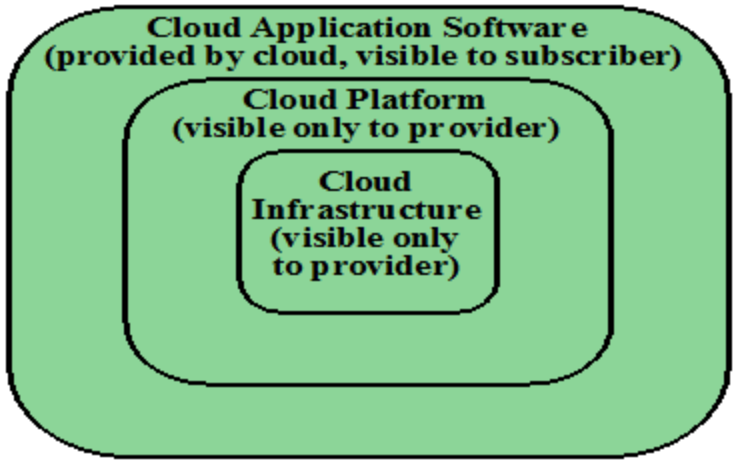
Cloud Security

NIST SP-800-145 defines cloud computing as:

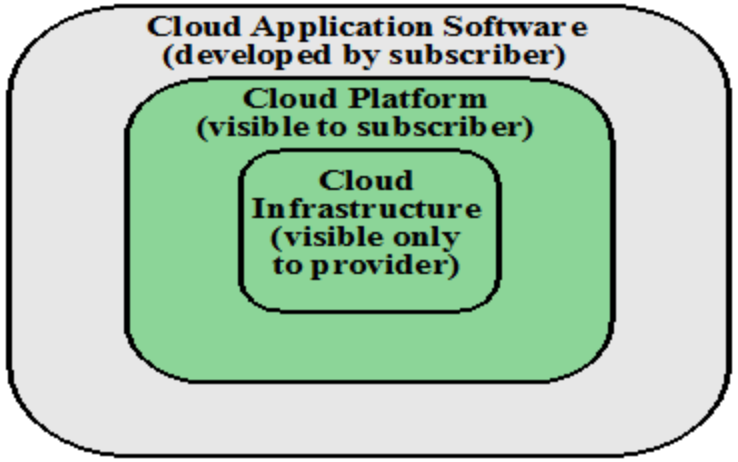
"A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."



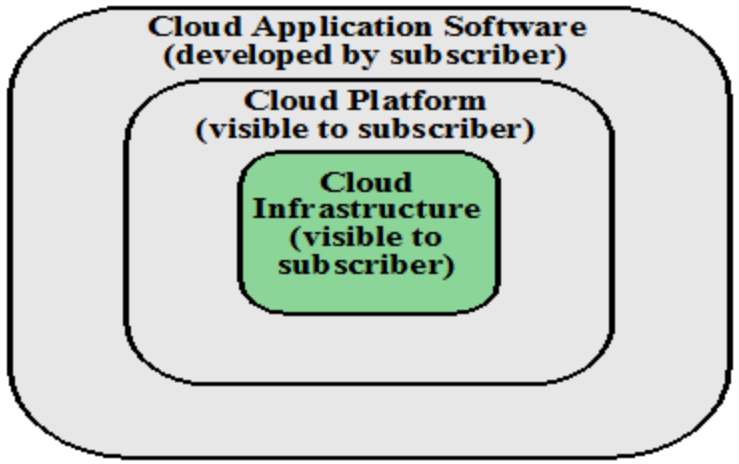
Cloud Computing Elements



(a) SaaS



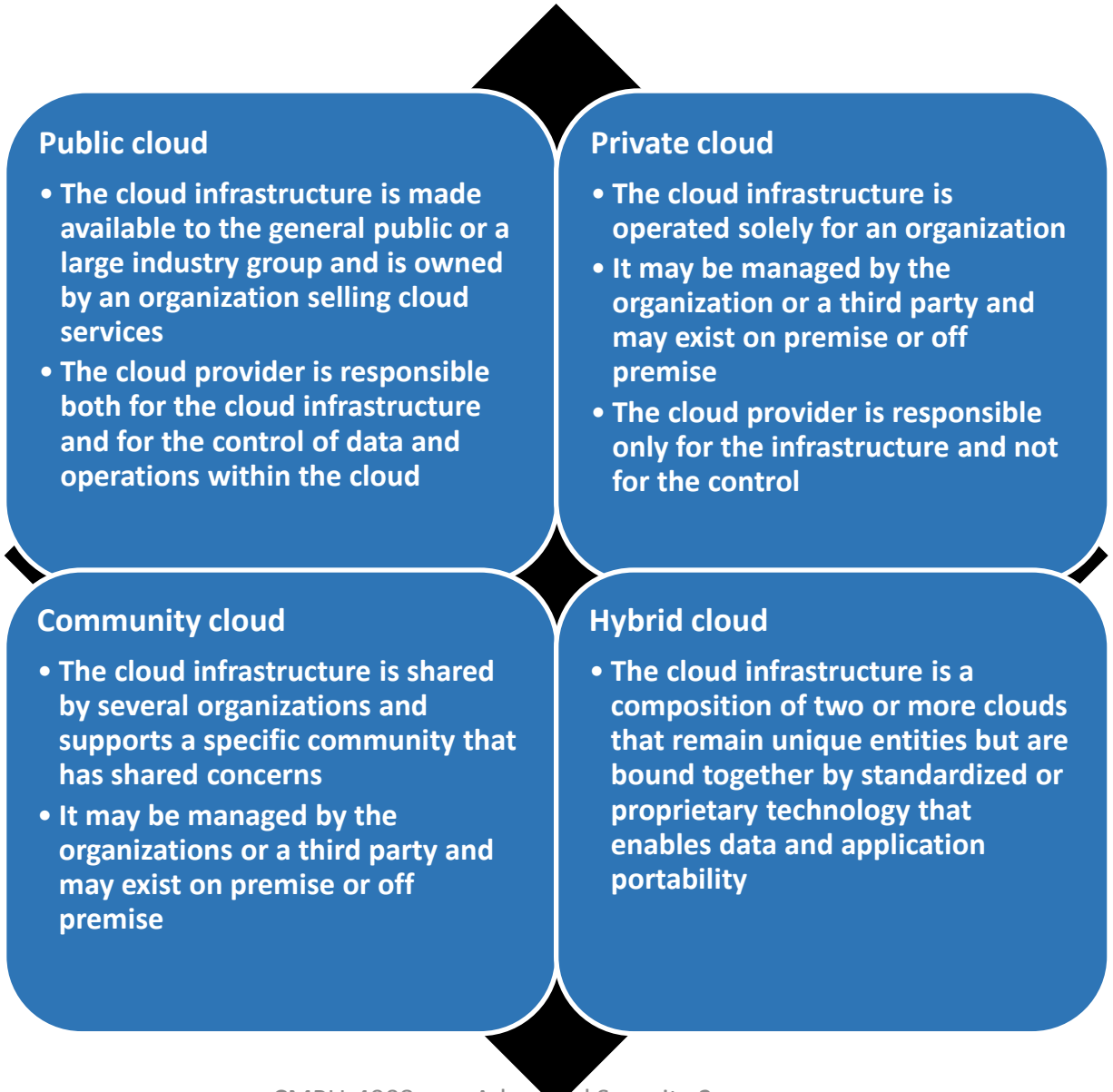
(b) PaaS

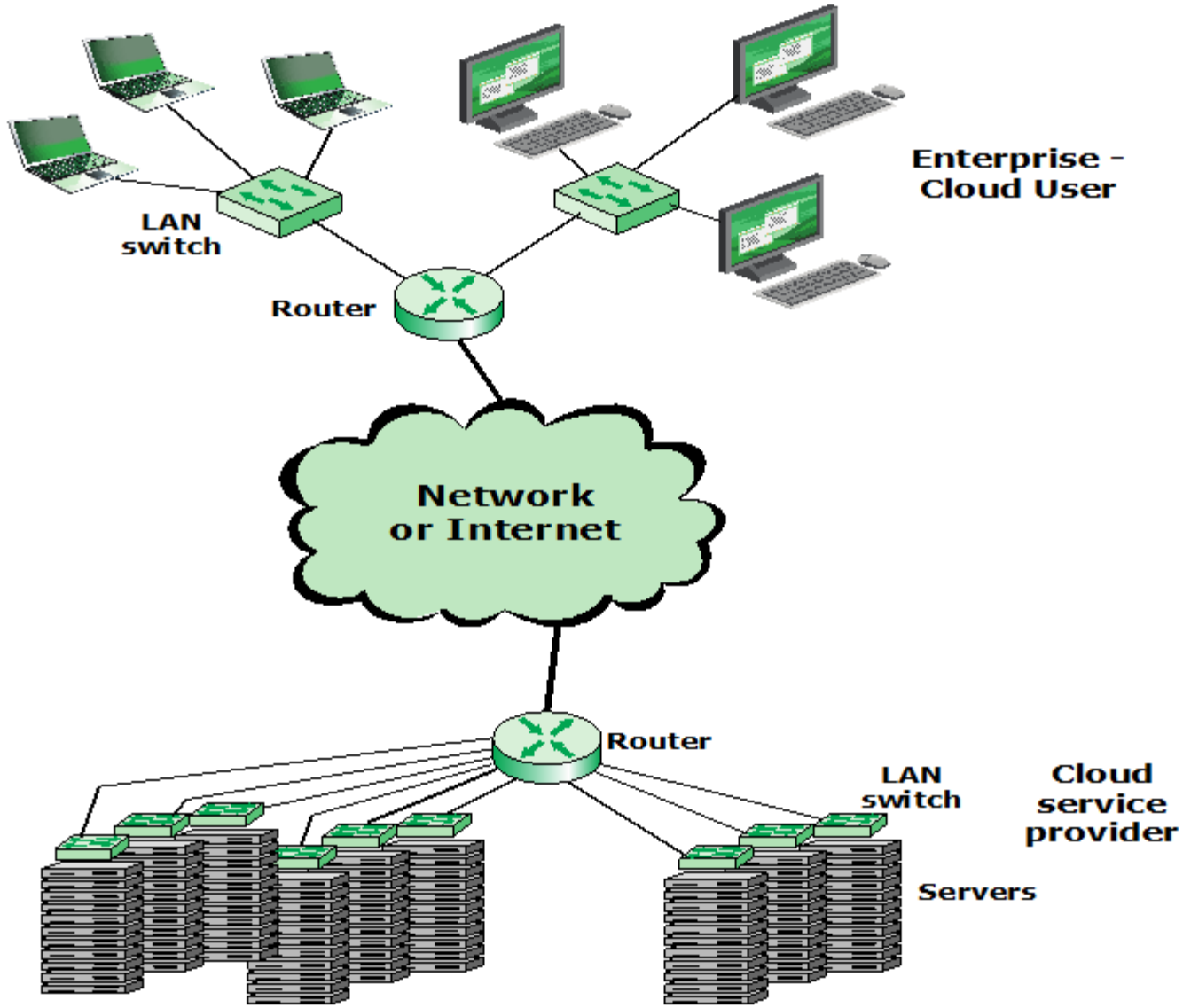


(c) IaaS

Cloud Service Models

NIST Deployment Models

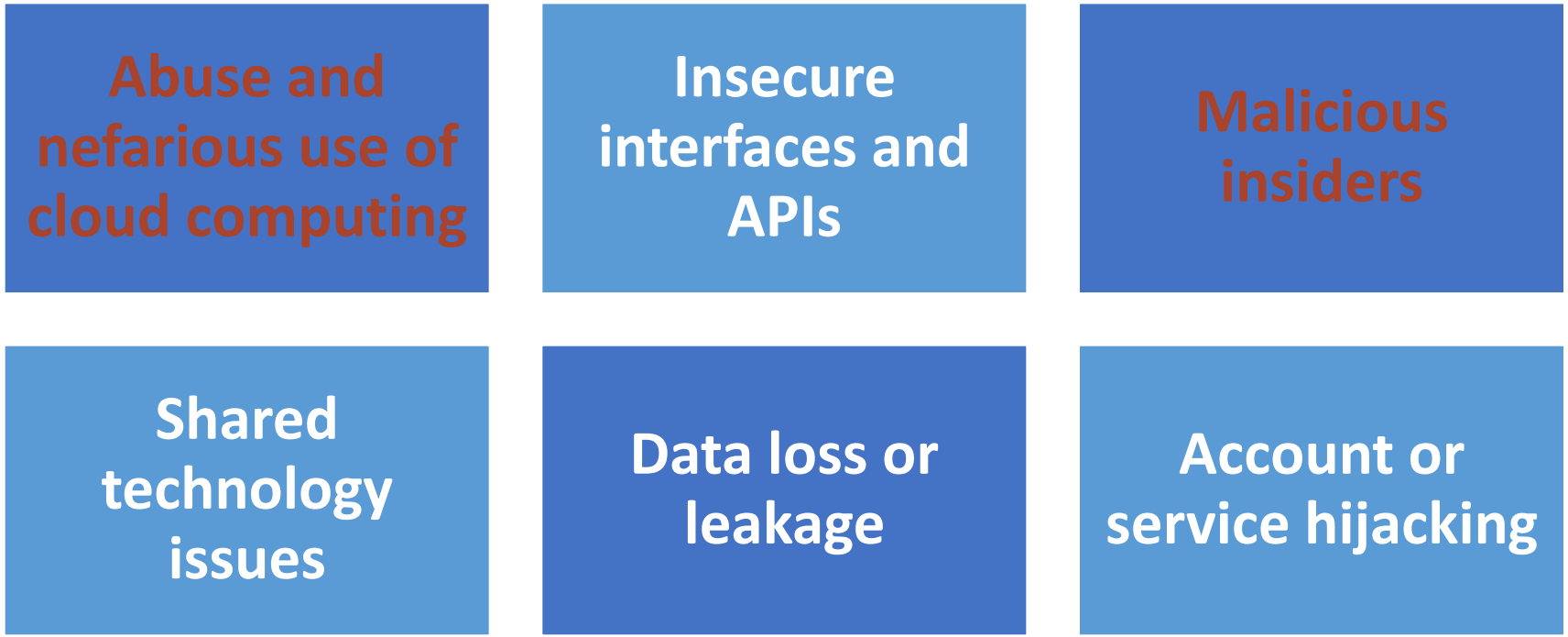




Cloud Computing Context

Cloud Security Threats

The Cloud Security Alliance lists the following as the top cloud specific security threats:



Cloud Security As A Service

- SecaaS
- Is a segment of the SaaS offering of a CP
- Defined by The Cloud Security Alliance as the provision of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers' on-premise systems

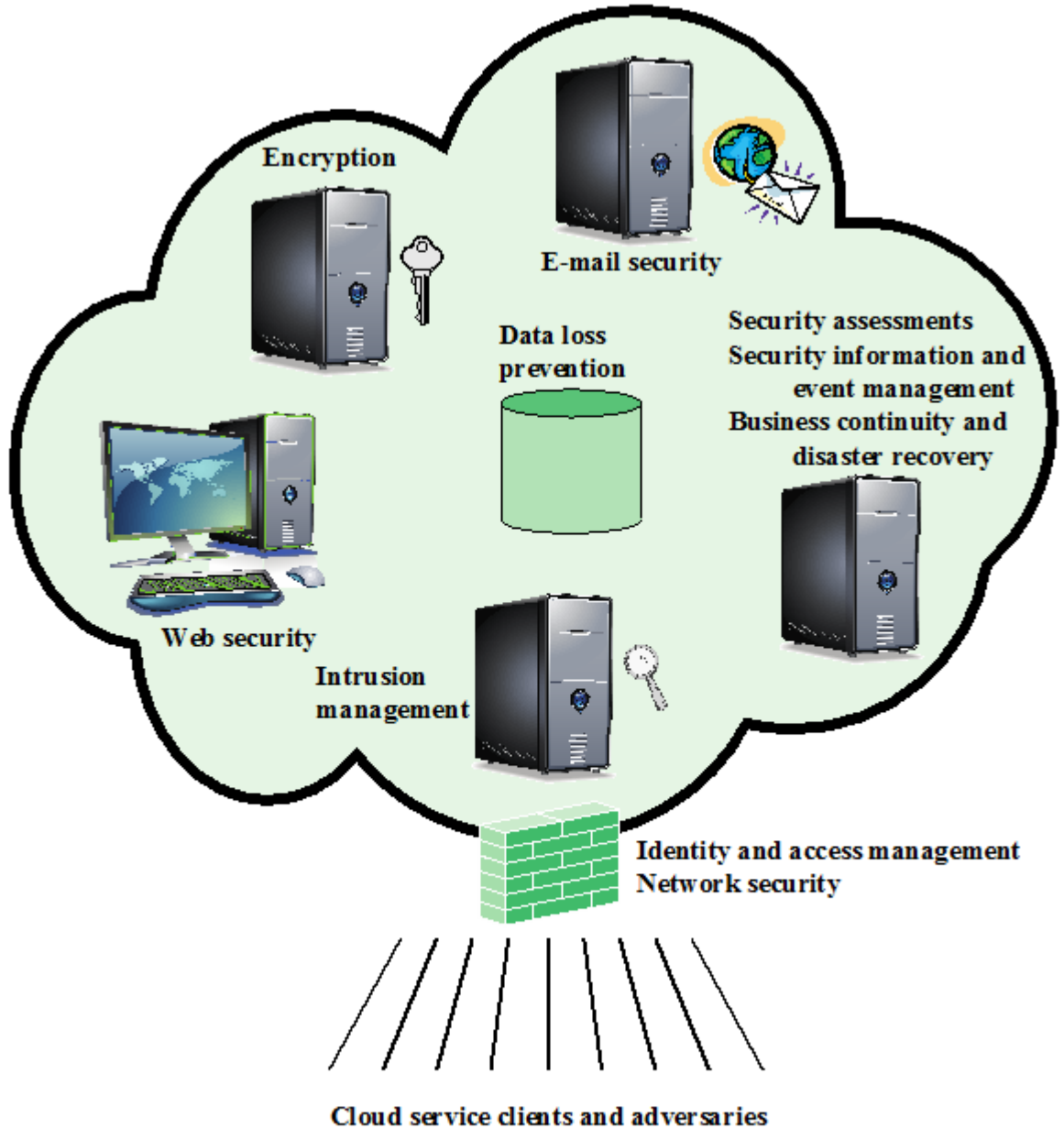


Figure Elements of Cloud Security as a Service

Cloud Security Attacks

- Denial of Service (DoS) attacks
- Malware Injection Attack
- Authentication Attacks
- Man In The Middle Attacks

Cloud Security Mechanisms

- Secure Operating System
- Strong Authentication
- Encrypt Store Data
- Intrusion Detection System

Cloud Security References

1. Top Threats to Cloud Computing V1.0, Cloud Security Alliance, March, 2010.
2. Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, Cloud Security Alliance,2011.
3. Guidelines on Security and Privacy in Public Cloud Computing, Wayne Jansen and Timothy Grance, NIST, January 2011.
4. Cloud Computing Security: A Survey, Issa M. Khalil , Abdallah Khreishah,Muhammad Azeem, Computers 2014.
5. Overview of Attacks on Cloud Computing, Ajey Singh, Maneesh Shrivastava, IJEIT,2012
6. The Management of Security in Cloud Computing, Ramgovind S, Eloff MM, Smith E, IEEE, 2010.