KANAZAWA UNIVERSITY | Emerging Media Initiative

GSCI1801A

Information Science

Lecture 7: Information Security, Ethics, and Emerging Topics

Asst. Prof. Chawanat NAKASAN | 2021-11-16

Note

- This presentation was prepared in 16:9 widescreen format.

Disclaimer: all content (after Security section) is the lecturer’s opinion presented under the principles of academic freedom and does not reflect the official position of Kanazawa University. We do not endorse, promote, or condone any of the brands or entities mentioned. All intellectual property including trademarks and technologies are mentioned for academic critique. Cryptocurrency, financial products, and investment in venture businesses have their inherent risks. Neither the lecturer nor Kanazawa University shall be held responsible for financial losses should you be inspired by this lecture to engage in financial or entrepreneurial pursuits after this presentation. The University is also not responsible for any other messages in this presentation.

Agenda

- Information Security
  - Principles of Information Security
  - Cryptography and Related Technologies
- Ethics
  - Computer Crimes
  - Privacy
- Selected Discussions on Emerging Topics:
  - How is your data being used?
  - Cryptocurrency: Future Digital Goldmine, or what?
  - The Meta Concern about Metaverse and Meta: Is it all an illusion?

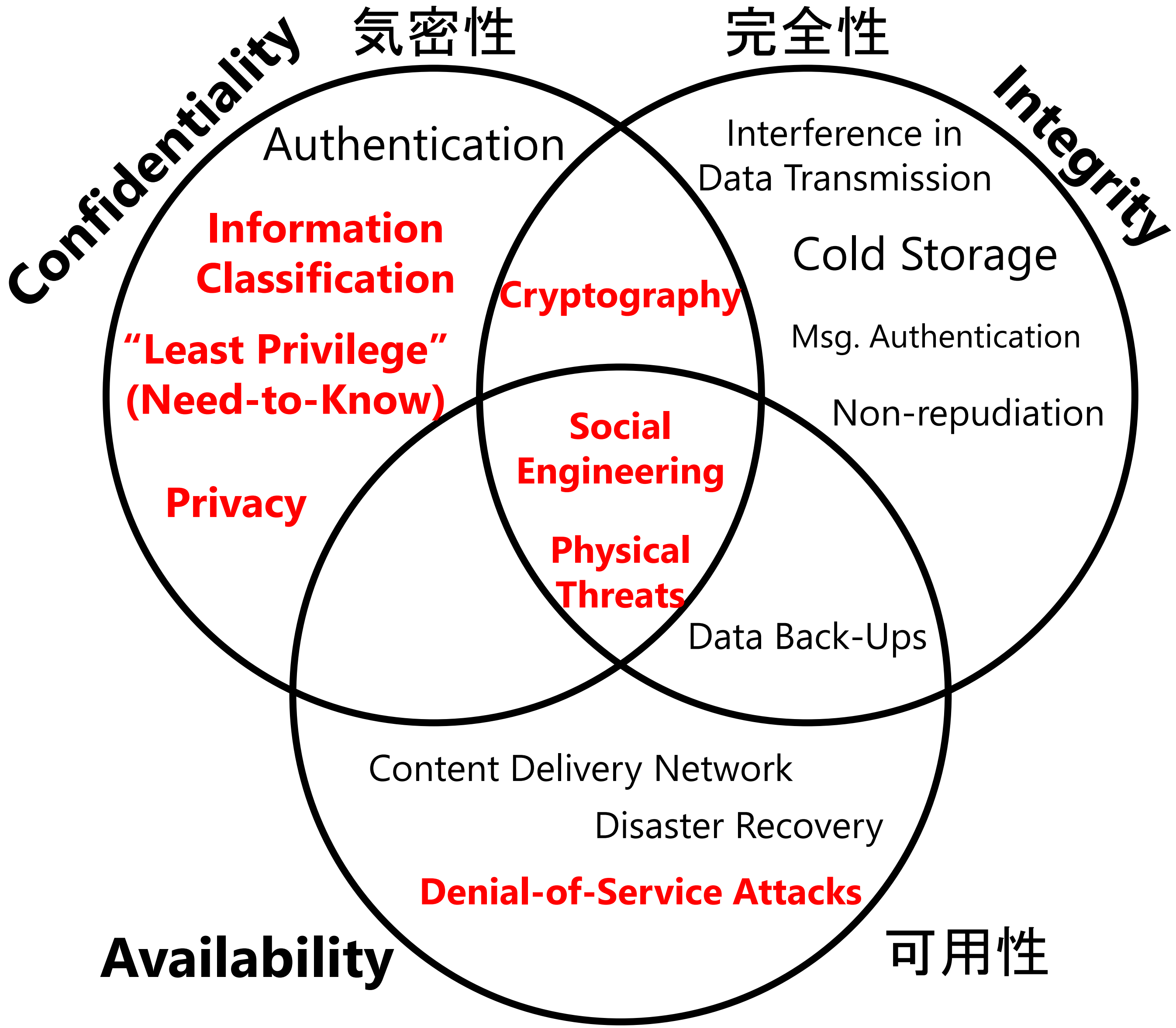
Fields in information security

- Application: Web, Database, specific CMS (WordPress, Joomla, etc.), mobile apps, etc.
- Infrastructure: Network, Cloud, OS, etc.
- Theory: Cryptography, etc.
- Policy and corporate implementation (CISSP, ISO 27001, etc.)

The CIA Triad

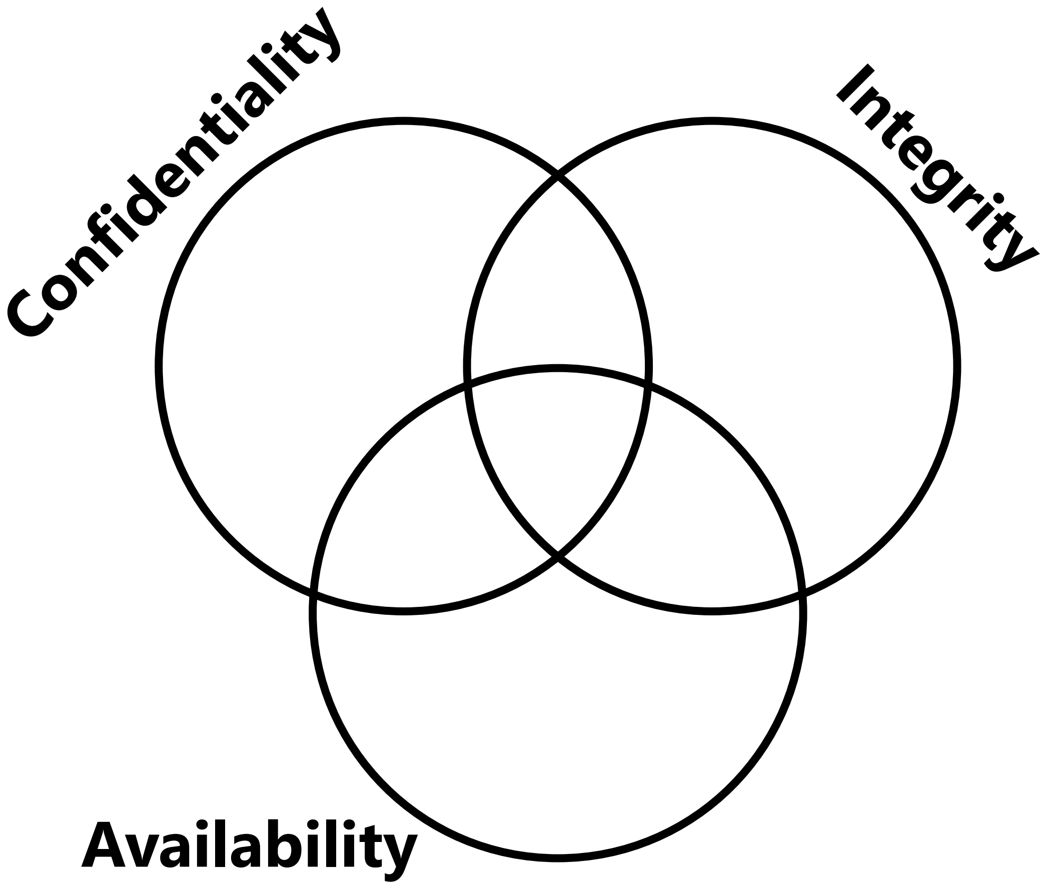
They are the three key components of information security. Notice that some elements may be related to multiple components.

Today I’ll discuss the highlighted topics.

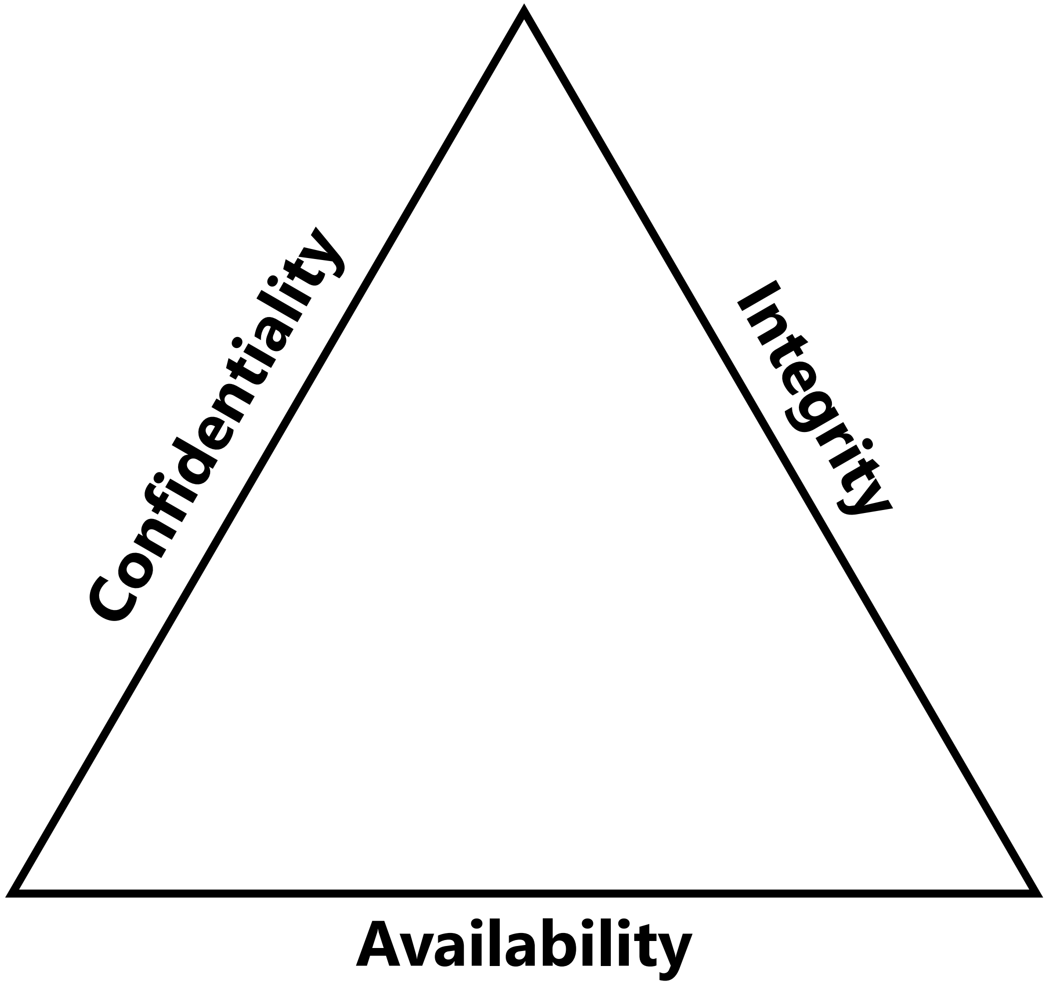


* The topics here are shown as examples only. This is not an exhaustive list.

Wait, which CIA Triad?



"Venn Diagram" design:
topics overlapping multiple domains



"Triangle of Fire" design:
all three elements are necessary for a secure system

Information Classification

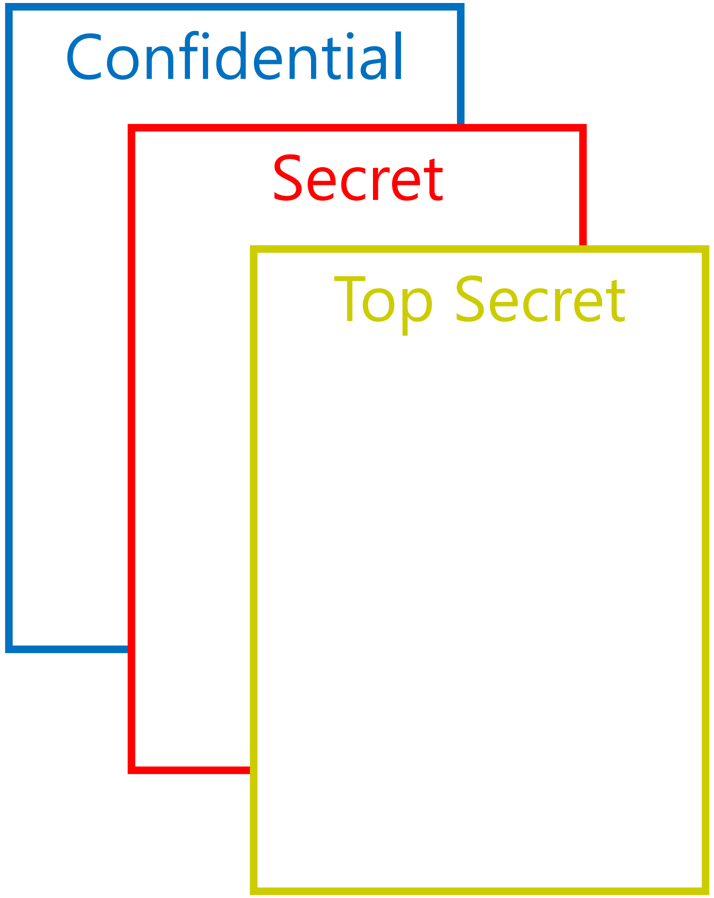
These two people work at two different levels of a company.
One is likely an engineer. Another looks like a CEO or maybe a president of a company.

Who should have better access to more sensitive data?

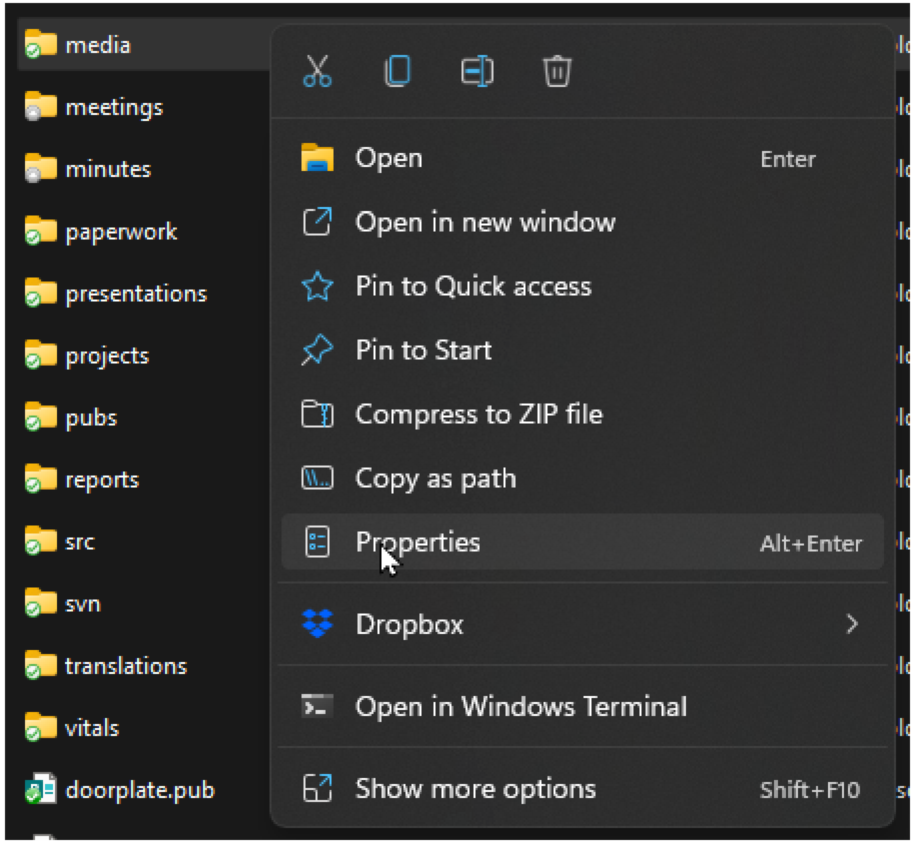
Graphics: GDJ / OpenClipart ; j4p4n / OpenClipart

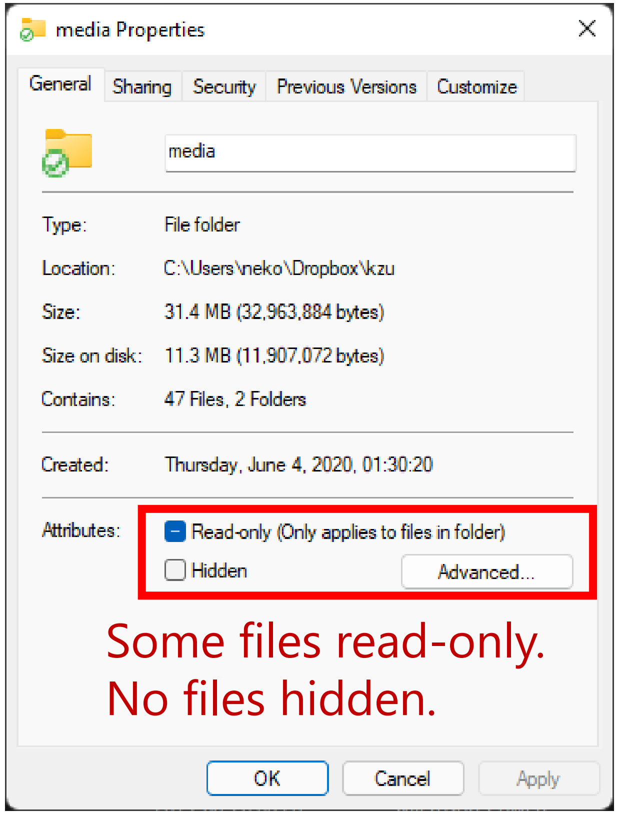
Information Classification

- Define how your document is to be handled by your organization.
- Most government organizations and large companies already have classification.
- How do you implement and integrate classification with IT?



File Permissions (Windows)





media

Type: File folder

Location: C:\Users\neko\Dropbox\kzu

Size: 31.4 MB (32,963,884 bytes)

Size on disk: 11.3 MB (11,907,072 bytes)

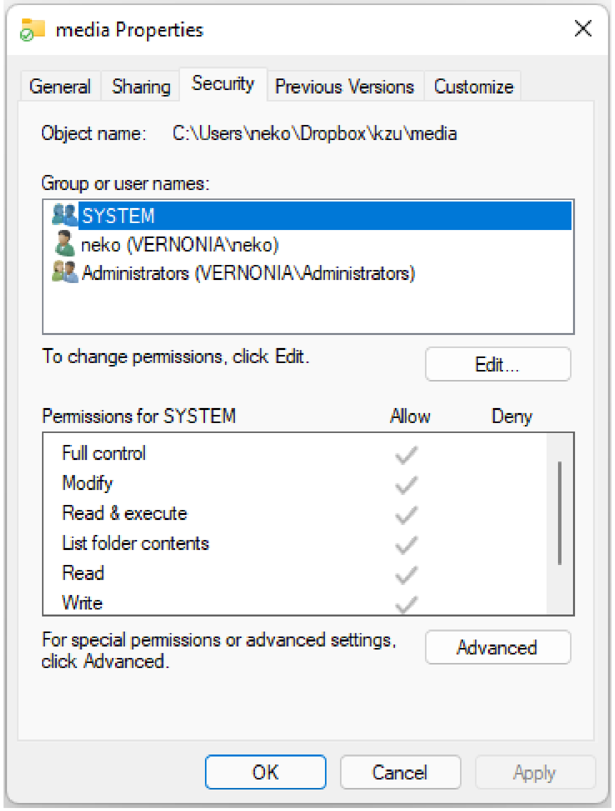
Contains: 47 Files, 2 Folders

Created: Thursday, June 4, 2020, 01:30:20

Attributes: ■ Read-only (Only applies to files in folder)

□ Hidden

Some files read-only.
No files hidden.



Object name: C:\Users\neko\Dropbox\kzu\media

Group or user names:

SYSTEM
neko (VERNONIA\neko)
Administrators (VERNONIA\Administrators)

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

If there are many users on a single computer, or you are using a server, this will be more complicated.

File Permissions (linux)

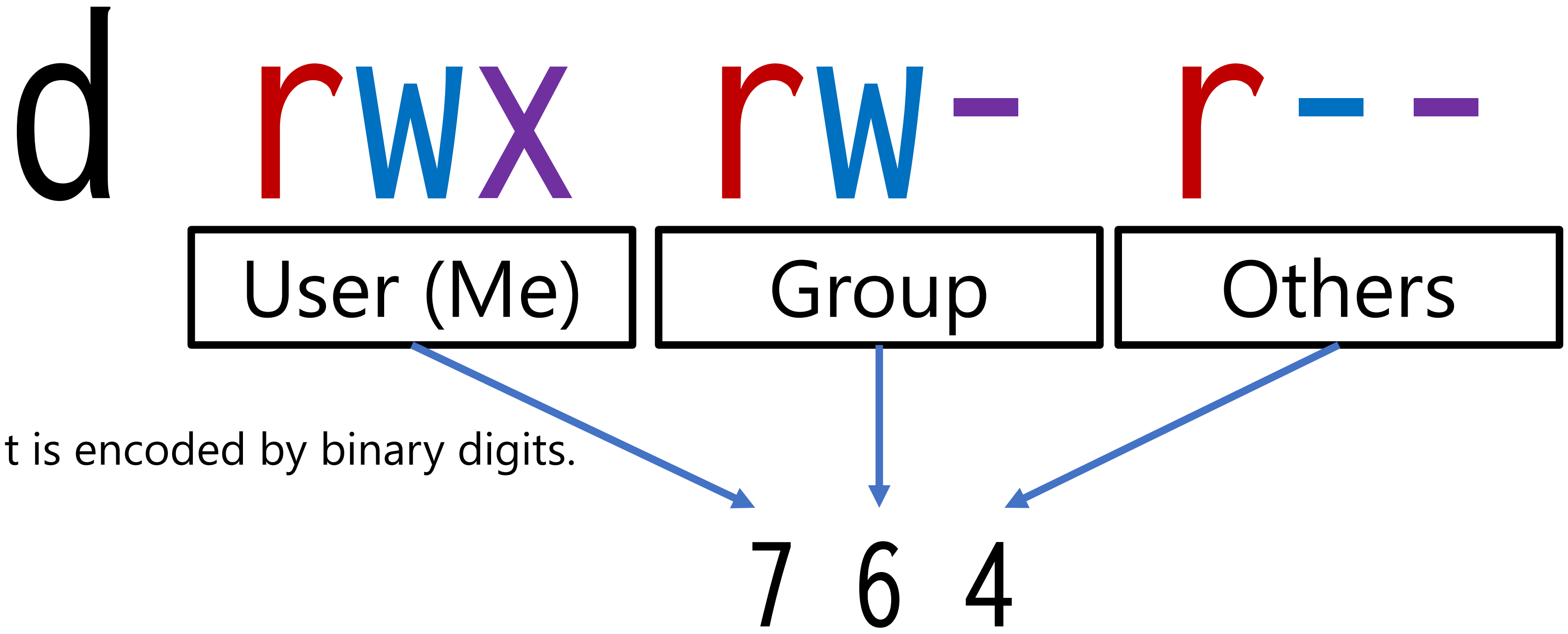
r = read

w = write

x = execute (run the file)

Letter means permission
Dash means no permission

d = it is a directory (folder)



d rwx rw- r--

User (Me)

Group

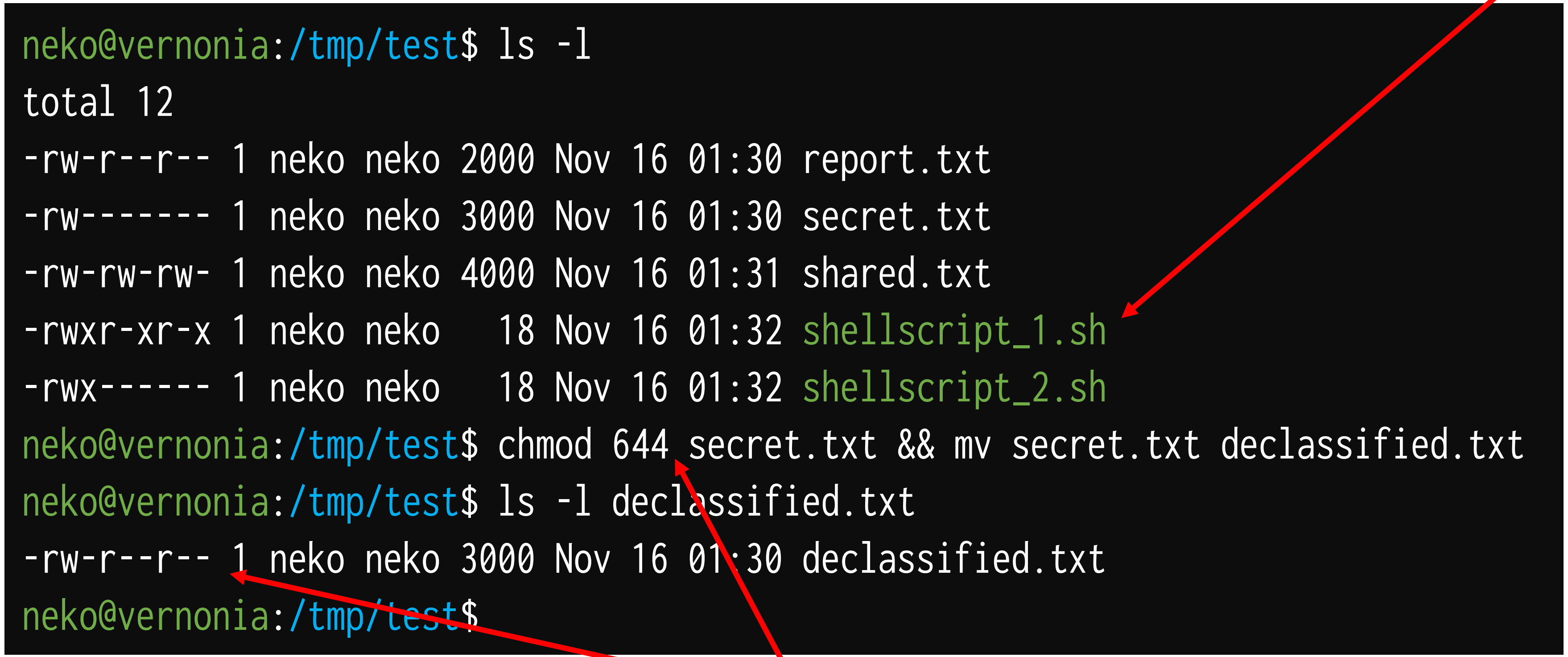
Others

It is encoded by binary digits.

7 6 4

File Permissions (linux)

Files in green can be executed.

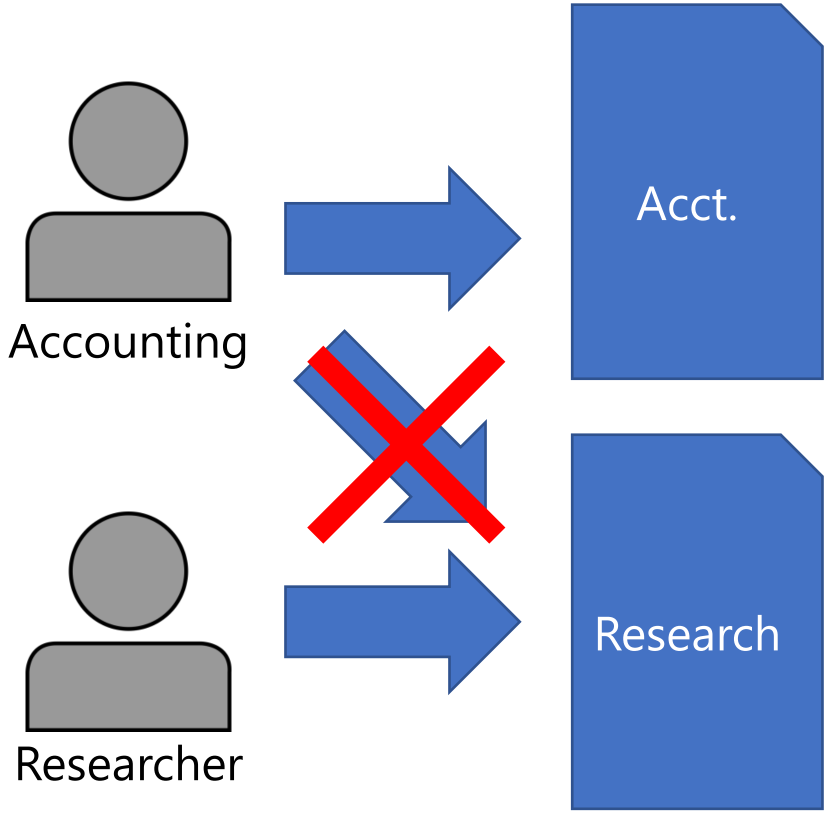


```
neko@vernonia:/tmp/test$ ls -l
total 12
-rw-r--r-- 1 neko neko 2000 Nov 16 01:30 report.txt
-rw------- 1 neko neko 3000 Nov 16 01:30 secret.txt
-rw-rw-rw- 1 neko neko 4000 Nov 16 01:31 shared.txt
-rwxr-xr-x 1 neko neko   18 Nov 16 01:32 shellscript_1.sh
-rwx------ 1 neko neko   18 Nov 16 01:32 shellscript_2.sh
neko@vernonia:/tmp/test$ chmod 644 secret.txt && mv secret.txt declassified.txt
neko@vernonia:/tmp/test$ ls -l declassified.txt
-rw-r--r-- 1 neko neko 3000 Nov 16 01:30 declassified.txt
neko@vernonia:/tmp/test$
```

Change file permissions to 644 or “rw-r--r--”
(Owner can read/write, group can read, others can read)

2. Least Privilege

- In addition to classification, organizations also require that you have a “need to know” to access specific information.
- For example, even if you have clearance, you cannot access information irrelevant to your work.

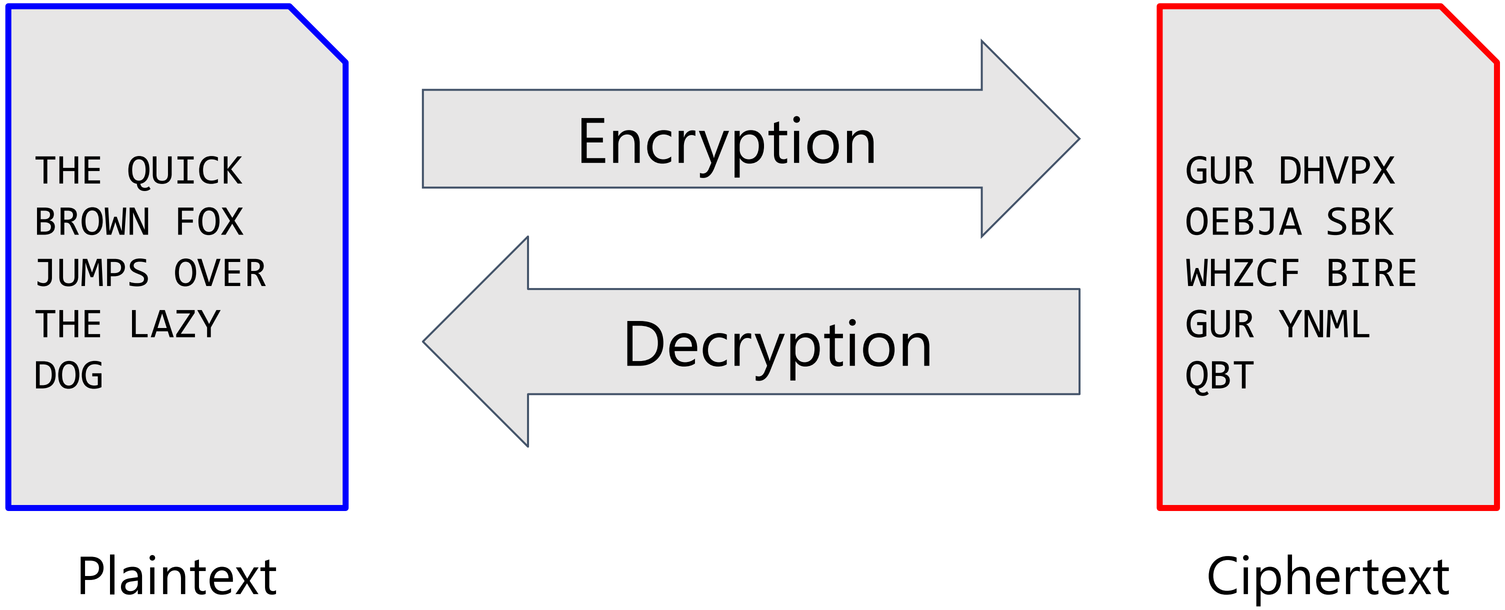


3. Cryptography

3.1. What is cryptography?

Cryptography is a mathematical method to transform your data so that it cannot be read or modified for unauthorized people.

This is usually done using mathematical methods.



THE QUICK
BROWN FOX
JUMPS OVER
THE LAZY
DOG

Encryption

Decryption

GUR DHVPX
OEBJA SBK
WHZCF BIRE
GUR YNML
QBT

Plaintext

Ciphertext

3.2. Where can we see cryptography?

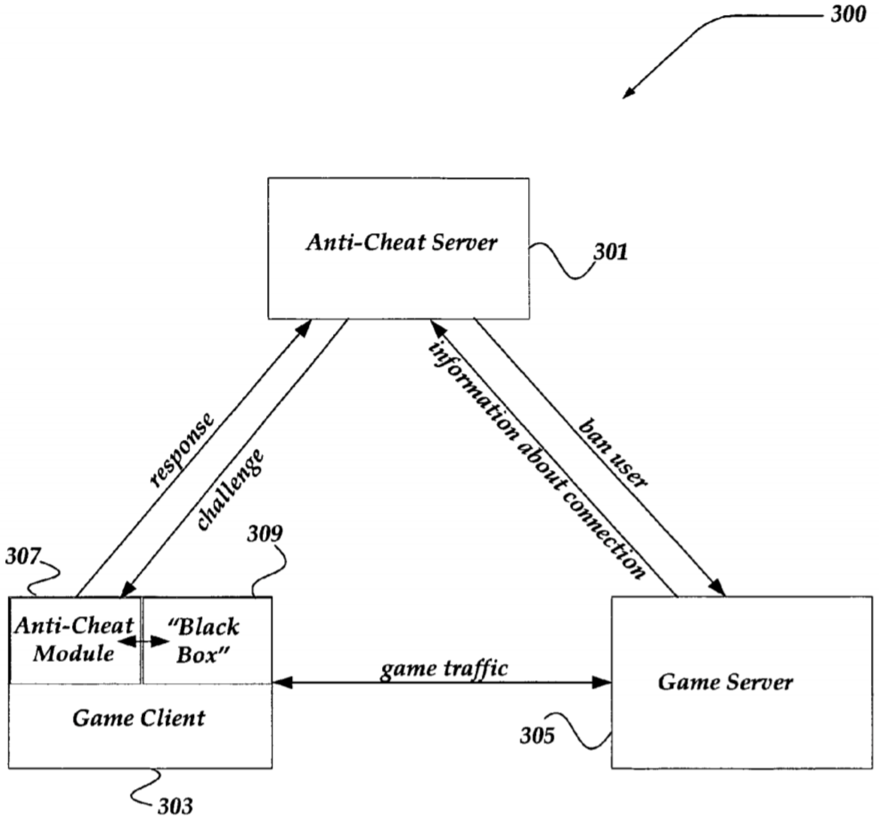
🔒 https:// ...

Secure Network Protocols

(there's more: TLS, IPSEC, etc.)

File & Disk Encryption Tools

(in order: Microsoft BitLocker, TrueCrypt, VeraCrypt)



Video Game Anti-cheat Facility

Bamberger et al. (2006), US Patent 2006/0247038 A1

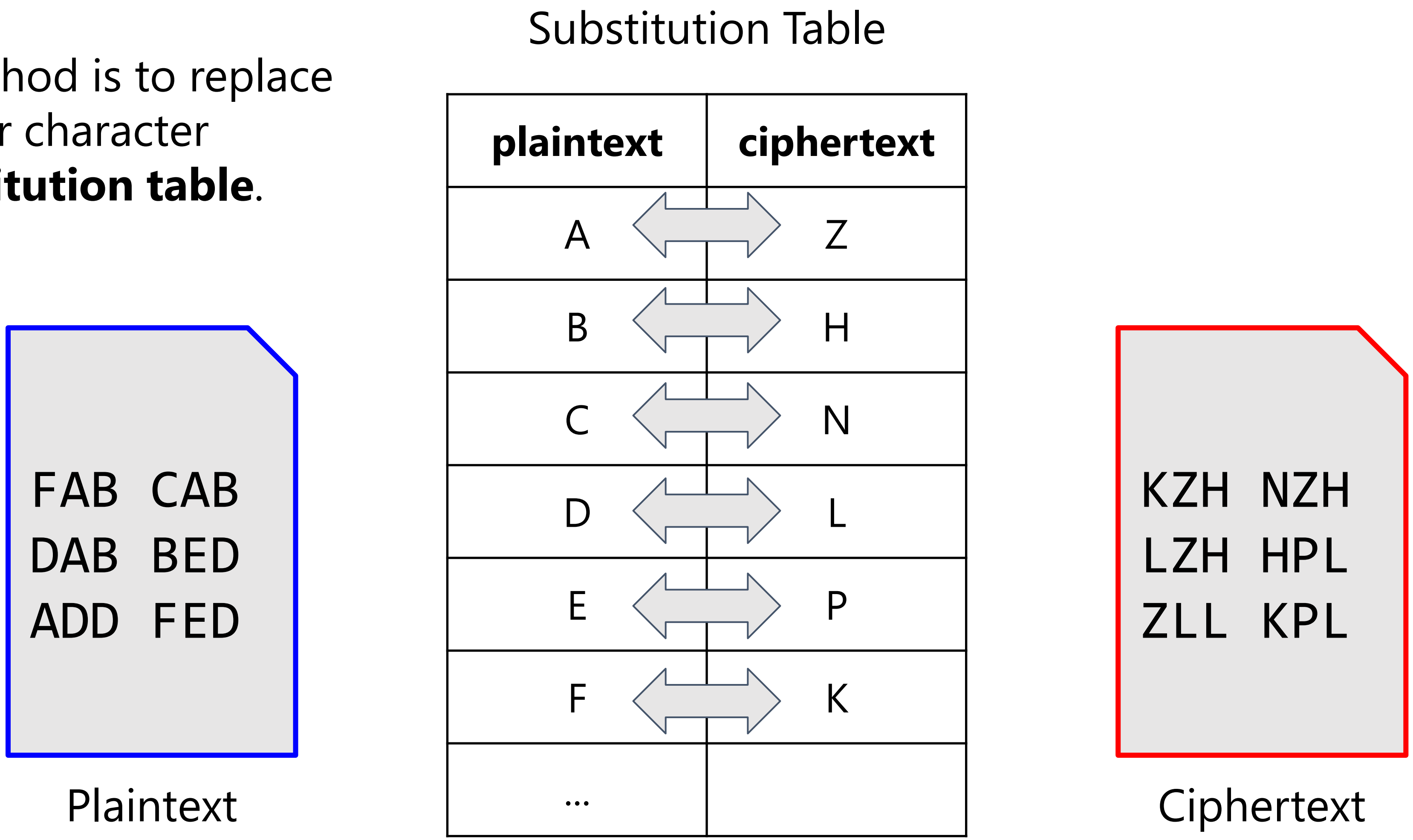
(assigned to Valve Corporation)

Military Communications

That's the Enigma Machine, so it's a little old, but the concept still stands.

3.3. Basic Substitution

A simple encryption method is to replace one character by another character based on a preset **substitution table**.



Substitution Table

plaintext	**ciphertext**
A	Z
B	H
C	N
D	L
E	P
F	K
…	

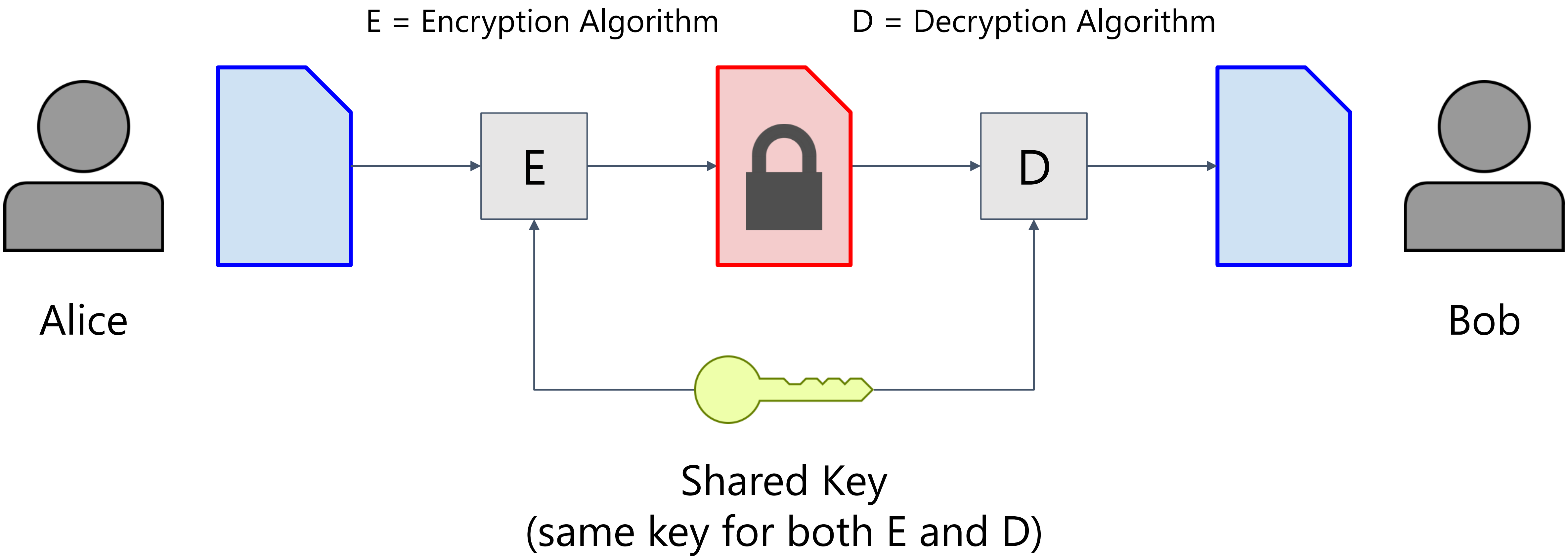
```
FAB  CAB
DAB  BED
ADD  FED
```

Plaintext

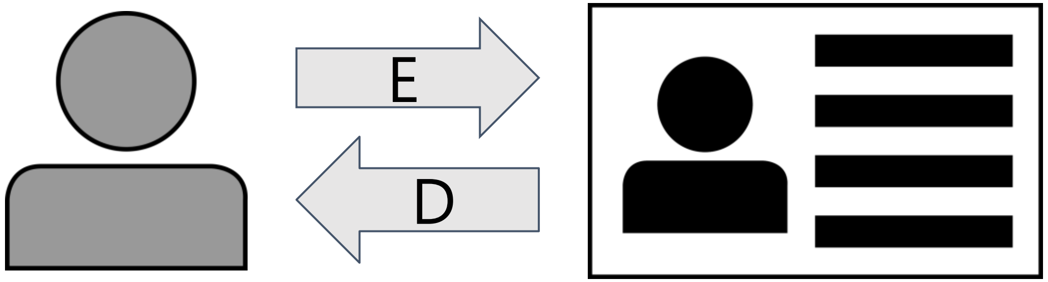
```
KZH  NZH
LZH  HPL
ZLL  KPL
```

Ciphertext

3.4. Symmetric Key Cryptography



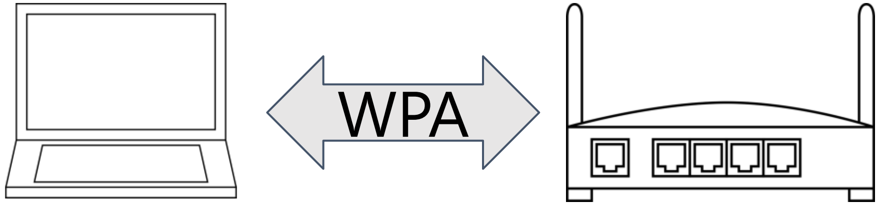
3.4. Symmetric Key Cryptography: Applications



Managing own user account

File storage

(Disk Encryption we mentioned earlier, etc.)



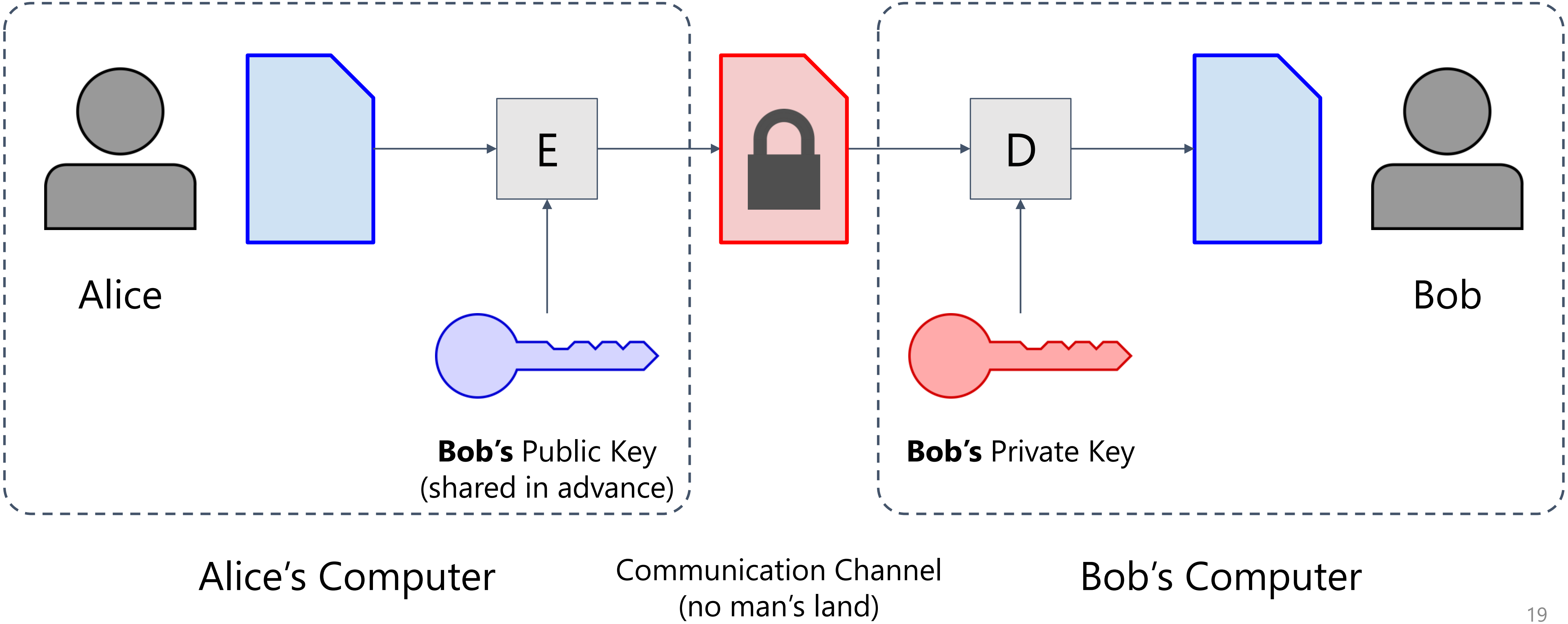
Secure Network Protocols

(WPA = Wifi Protected Access)

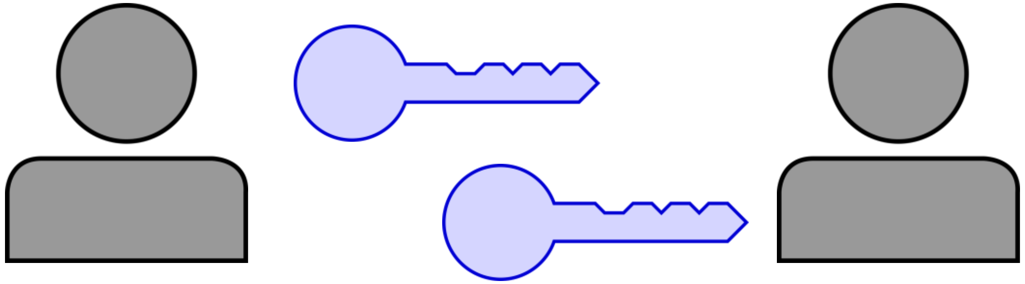
You can also read RFC4764 for more details about encryption.

P.S. That router *isn't* a LinkSys :P

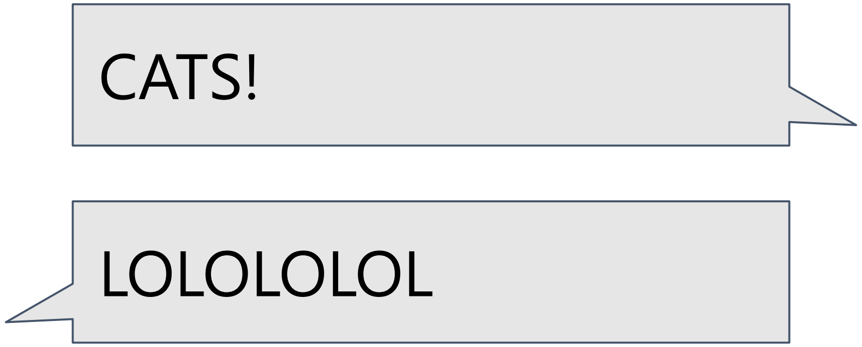
3.5. Asymmetric Key Cryptography



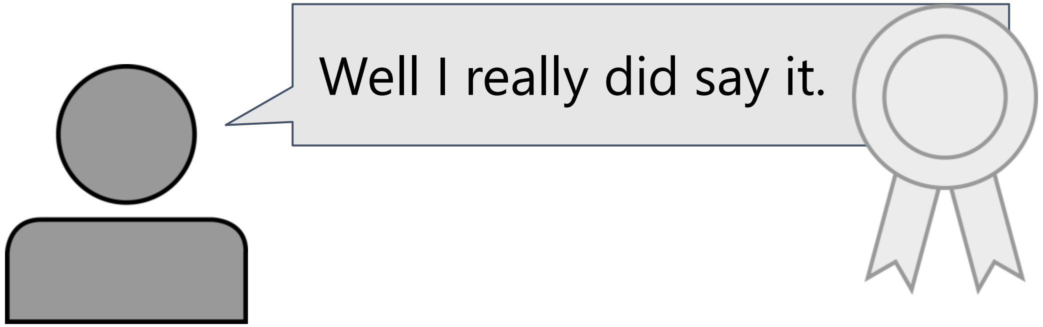
3.5. Applications of Asymmetric Key Cryptography



Secure Key Exchange and Authentication (to set up for future communication using symmetric key encryption)



Secure Messaging and Emails



Digital Signatures

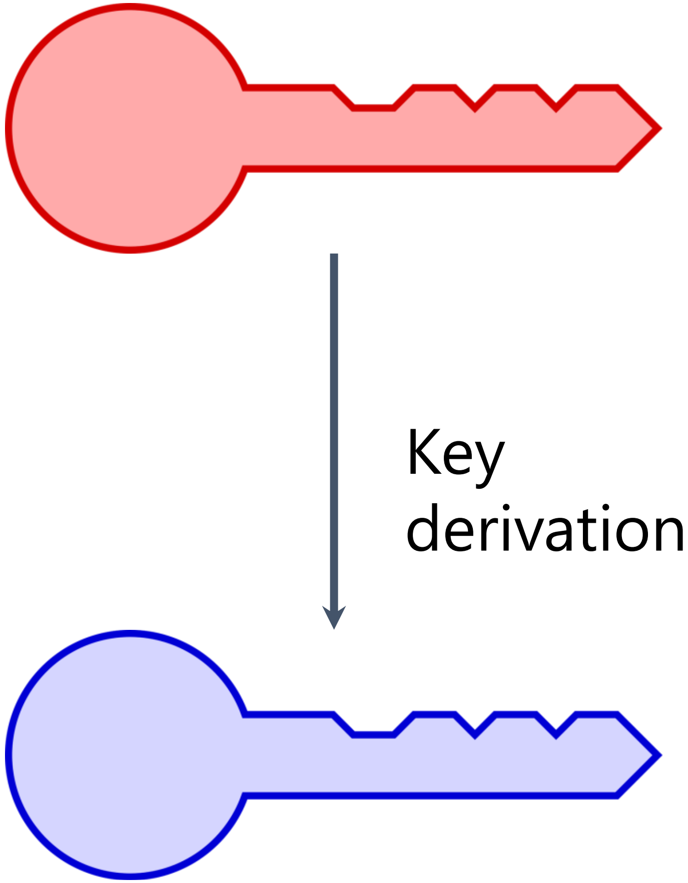
3.6. Asymmetric Key Cryptography: Public and Private Keys

There … are two keys per person?

Thus begins our discussion on asymmetric key cryptography.

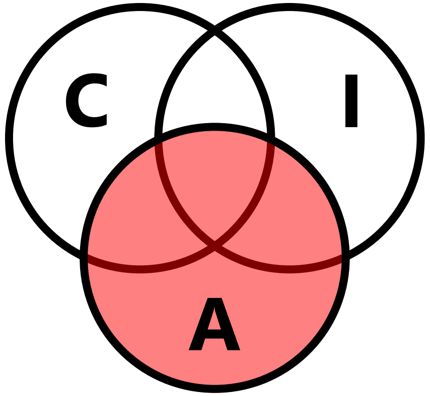
Rule #1*: The public and private keys are mathematically related pairs, but it must be “impossible” to find the private key based on the public key!

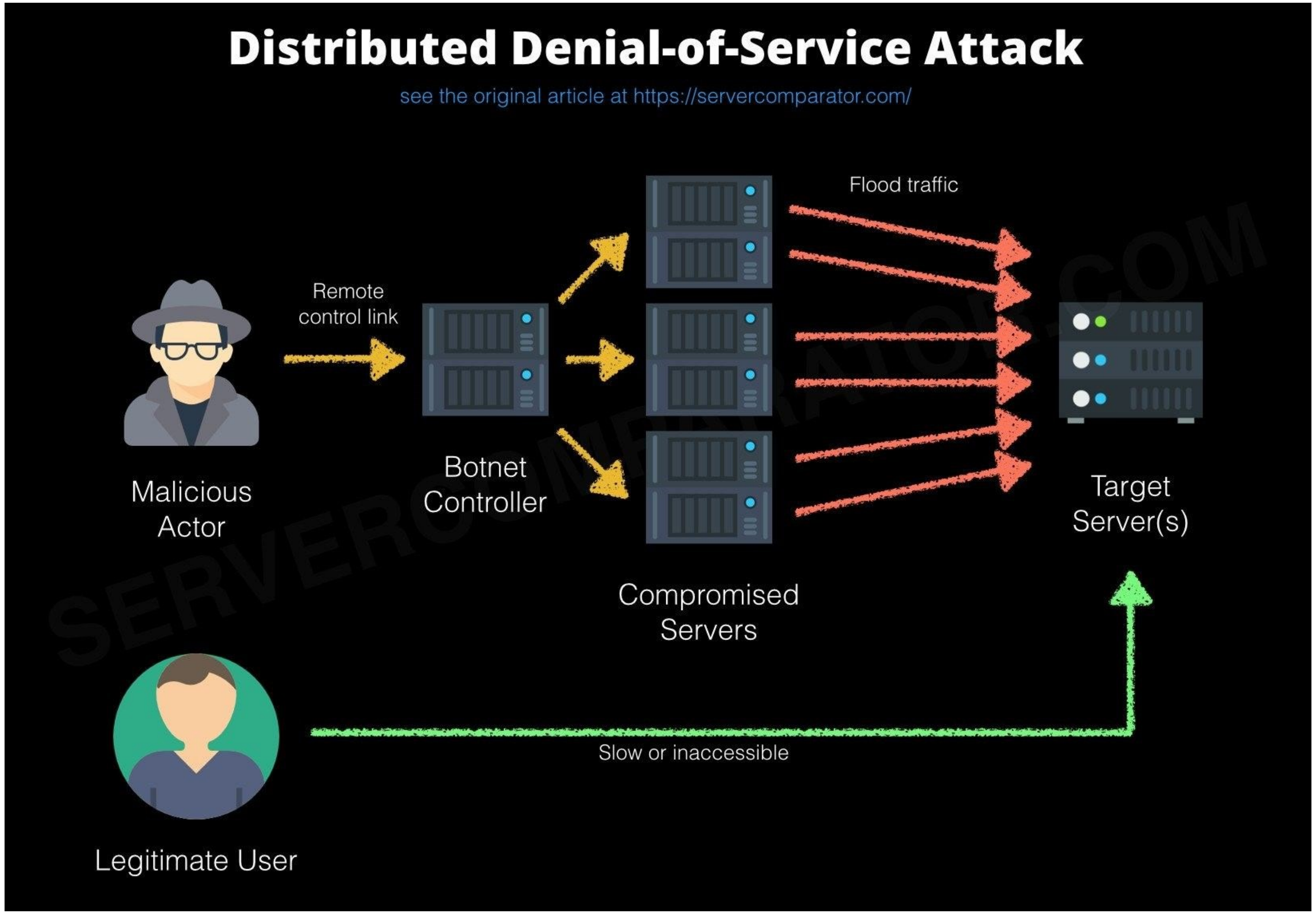
(*Not literally, but it’s still pretty important.)



4. Threats

4.1. Denial-of-Service (DoS) Attacks





Source: MSDN, https://techcommunity.microsoft.com/t5/sql-server/understanding-server-traffic-logs-and-detecting-denial-of/ba-p/385529

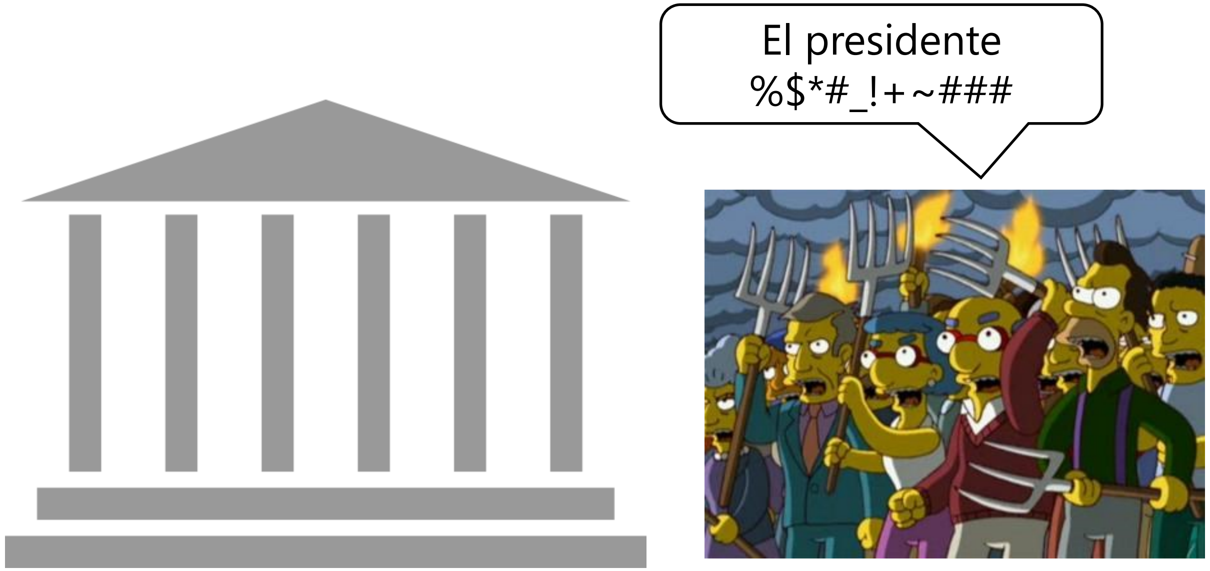
4.1. Importance of DoS attacks

- Cheap yet effective against government & large companies.
- They are seen in conjunction with zombie and mob attacks.
- Easily confused with legitimate traffic.
- Cat-and-mouse situation between ISPs and shady people.

Confusing Situation: Is it DoS or just happy hour?

Buy!
Buy!
Buy!
Buy!
Buy!
Buy!
Reserve Today!

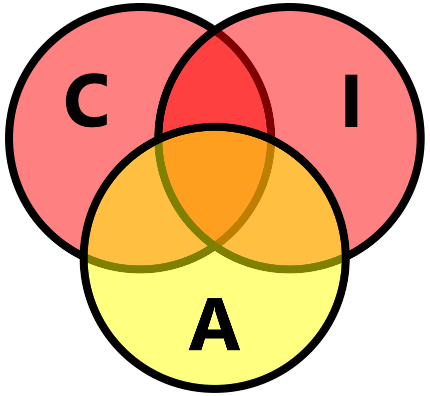
Designer shoes!
Online reservation only!
¥99,000

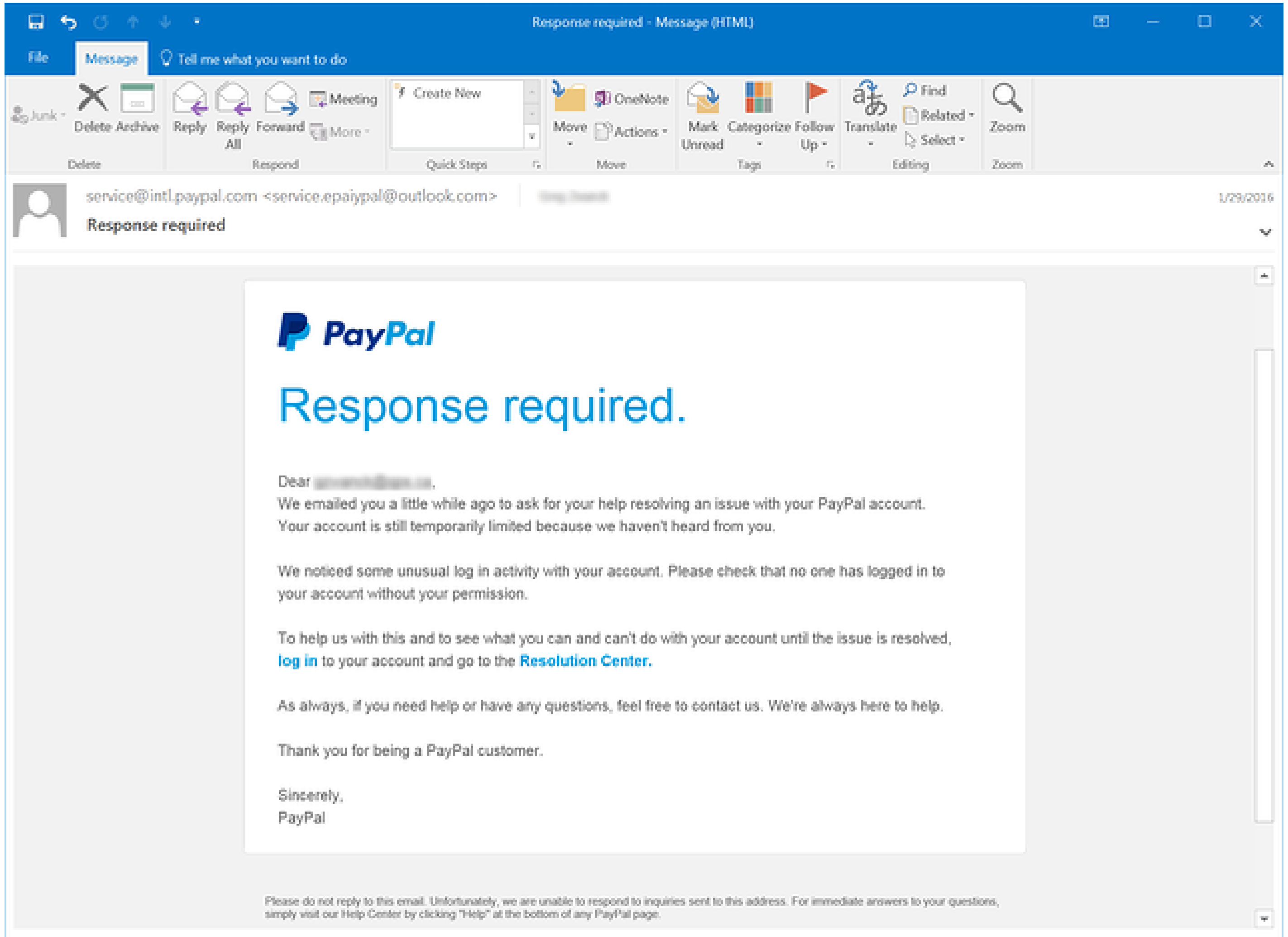


The Government did something wrong!
People are very angry!

Graphics: oksmith / OpenClipart; The Simpsons

4.2. Phishing (Social Engineering)





service@intl.paypal.com <service.epaiypal@outlook.com> [redacted] 1/29/2016

Response required

PayPal

Response required.

Dear [redacted],
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account.
Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

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

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

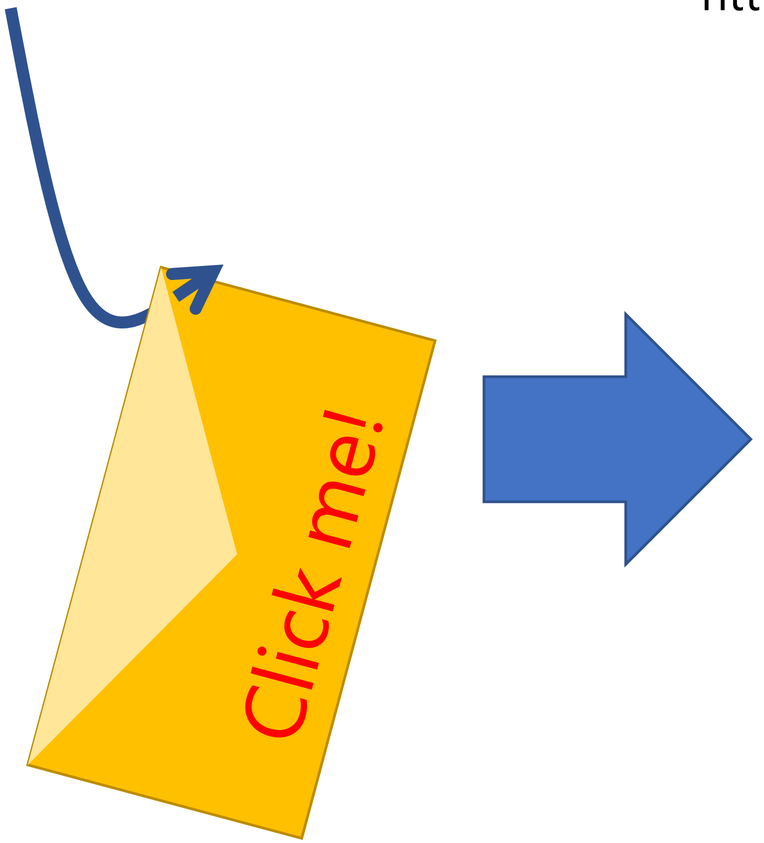
Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

Source: https://www.phishing.org/phishing-examples

4.2. Impacts of Phishing

- Leak of sensitive information (corporate secrets, customer data, etc.)
- Perpetrators gain access to our systems and may take control of them (leading to further attacks)
- Impacts against trust in our company

What phishing can lead to?



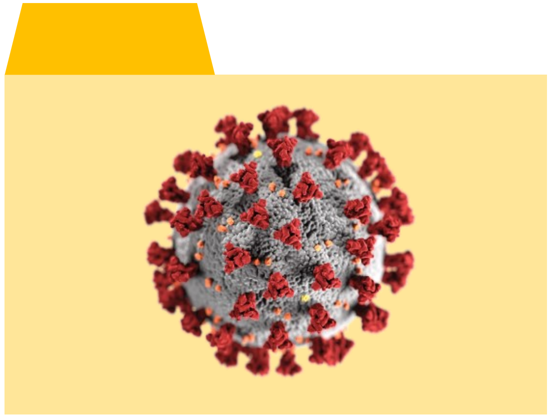
http://kanazawa-u.ac.jp.adasdsasd.com/login.php

Acanthos
Portal
Kanazawa University

USER	me@kanazawa-u.ac.jp
PASS	********

Connect to KUWIN

Password theft websites

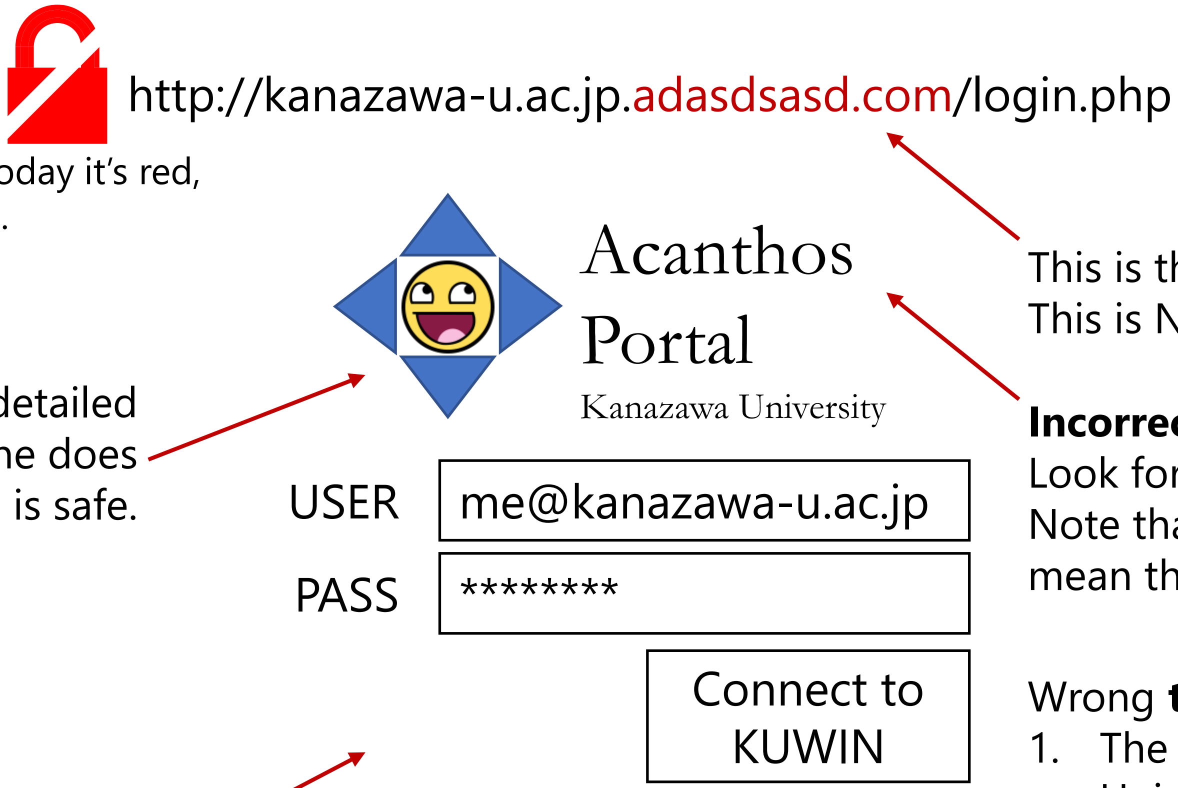


Virus or malware attachments!

(Fake website for illustration only.)

Graphics: APSF

Okay, how fake can a website get? What to look for?



http://kanazawa-u.ac.jp.adasdsasd.com/login.php

Acanthos Portal

Kanazawa University

USER me@kanazawa-u.ac.jp

PASS ********

Red or broken lock.
If it was usually green or gray but today it’s red, assume that it is unsafe.

Incorrect, outdated, or poorly detailed **logo**. Note that correct logo alone does not mean the website is safe.

Poor or incorrect **website design**. Acanthus Portal login page is blue.

This is the **main part of the URL**.
This is NOT Kanazawa University website.

Incorrect service name.
Look for small differences.
Note that correct name alone does not mean the website is safe.

Wrong **technical information**.

1. The official network for Kanazawa University is KAINS-WIFI, not KUWIN (it is operated by another university).
2. You connect to KAINS-WIFI directly using the Wi-Fi menu on your computer or phone, not by web.

Note that real phishing attempts are much more professional than this!

Example of a legitimate website (from textbook)

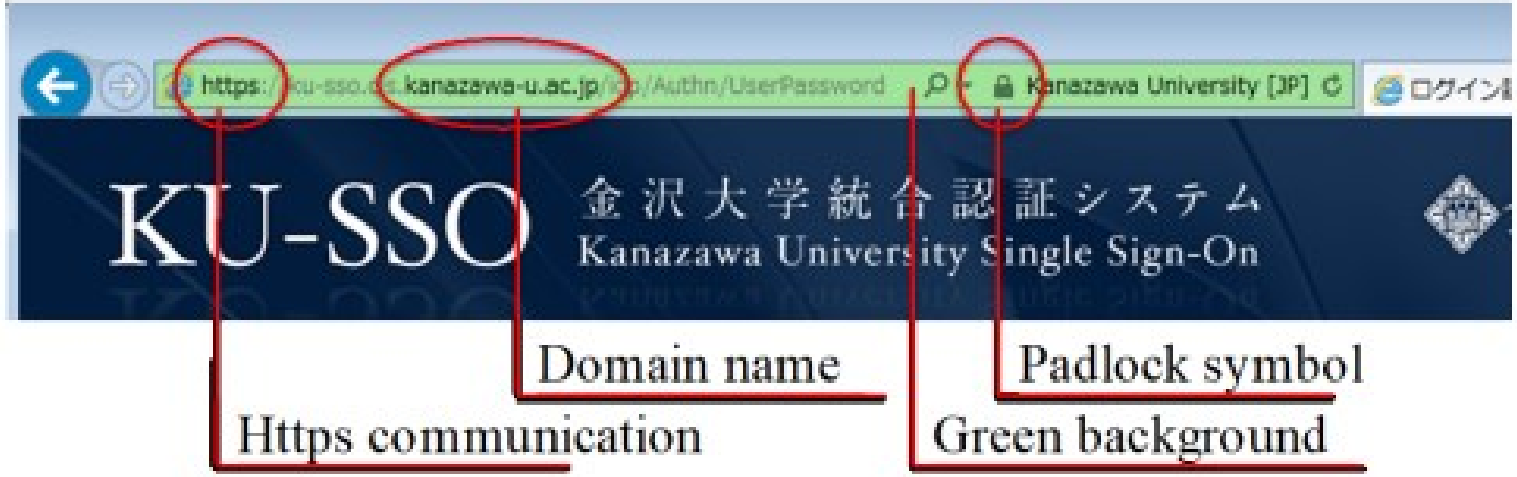
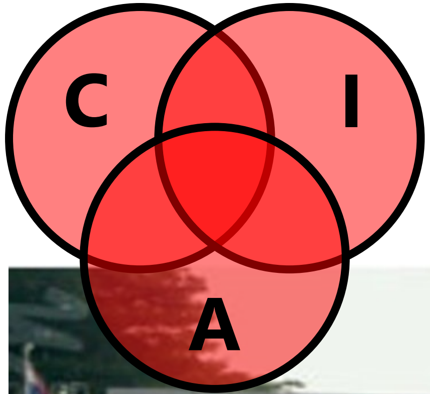


Figure 9-10: A website using HTTPS

4.3. Physical Threats



Never underestimate physical security!

Attacks on government centers and public corporations seriously disrupt important services. Physical assaults can occur together with attacks on information security.

Protests blocking CAT Telecom in Thailand

Photo: https://www.sanook.com/news/1334551/

US Capitol Assault

Laptops of US federal employees were also reported stolen.

https://abcnews.go.com/Politics/capitol-attack-conjures-american-legacy-racial-violence/story?id=75331177

Ethics

Definition of Ethics

- Principles, or rules of what’s good or bad.
- BBC: “a system of moral principles”.

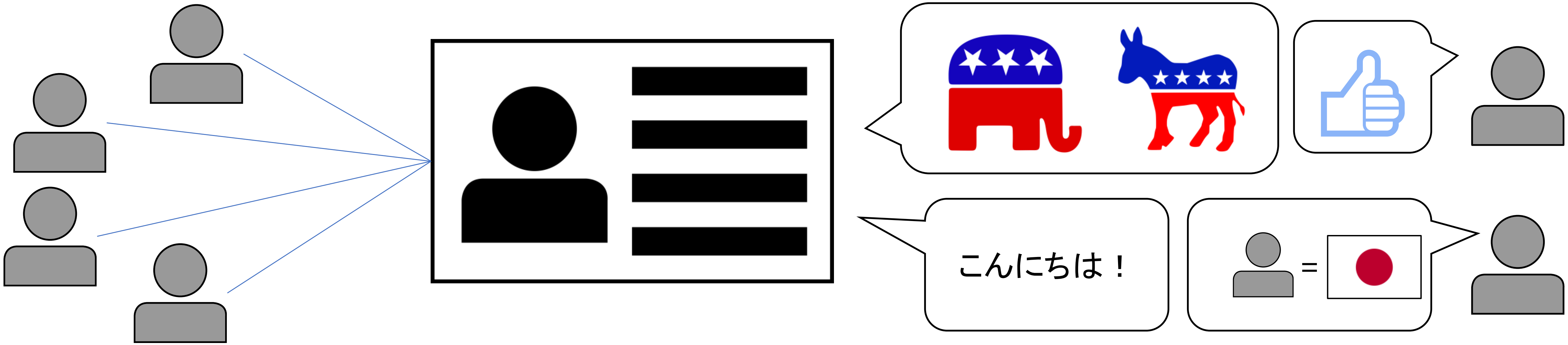
- Ethics come in many forms:
  - Law
  - Code of Ethics
  - Unwritten Rules
  - Gentlemen’s Agreements

Computer Crimes

- Modern laws in many countries have specific articles outlining computer crimes. Examples include:

- Unauthorized access (不正アクセス)
- Service disruption
- Data modification
- Data theft (leakage)
- Piracy

Privacy:
How much information do you give out online?



Your Contacts

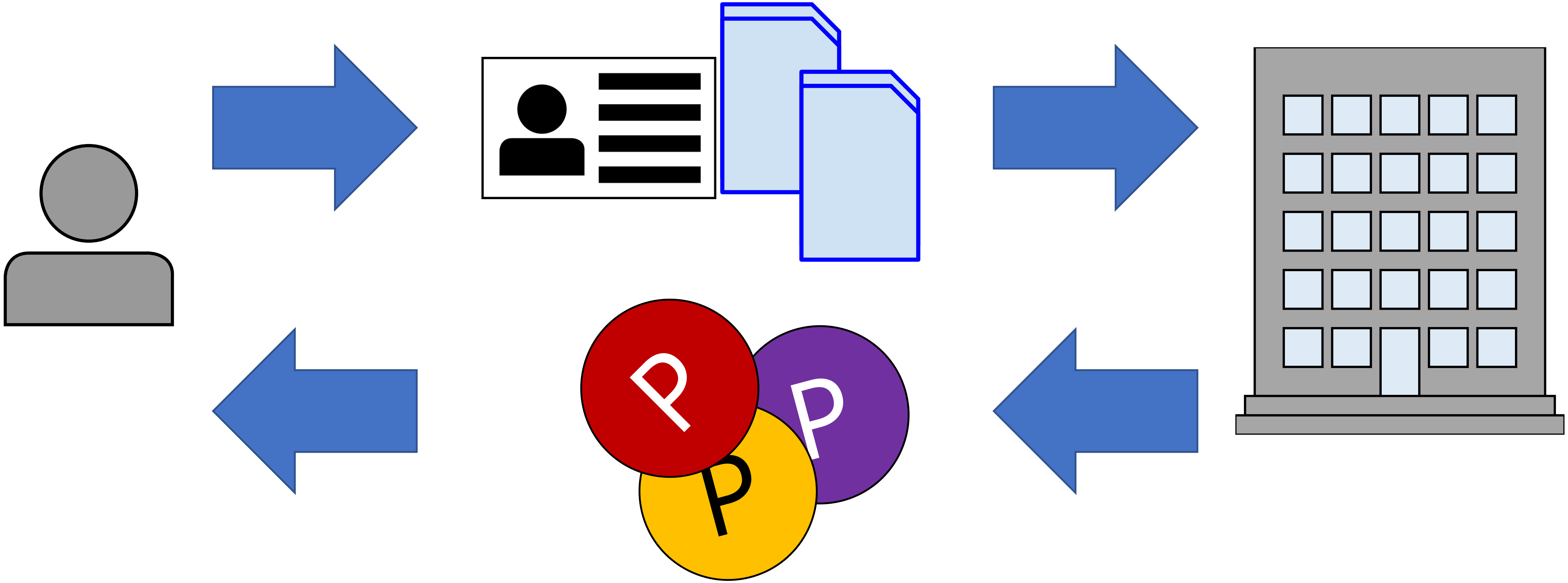
Your Identity

- Real name
- Email address
- Telephone number
- Address
- Credit cards and payment methods

Your Activities Reveal about You

- Discussions about politics and religions
- Your language may reveal your nationality or local accent.
- Complaining about your job may get you fired.

Are those "app points" worth enough for you to give your information?



“The question is what else is being done with that data? And who supervises it? Who regulates it?”

– Yuval Noah Harari (Author of Sapiens: A Brief History of Humankind)

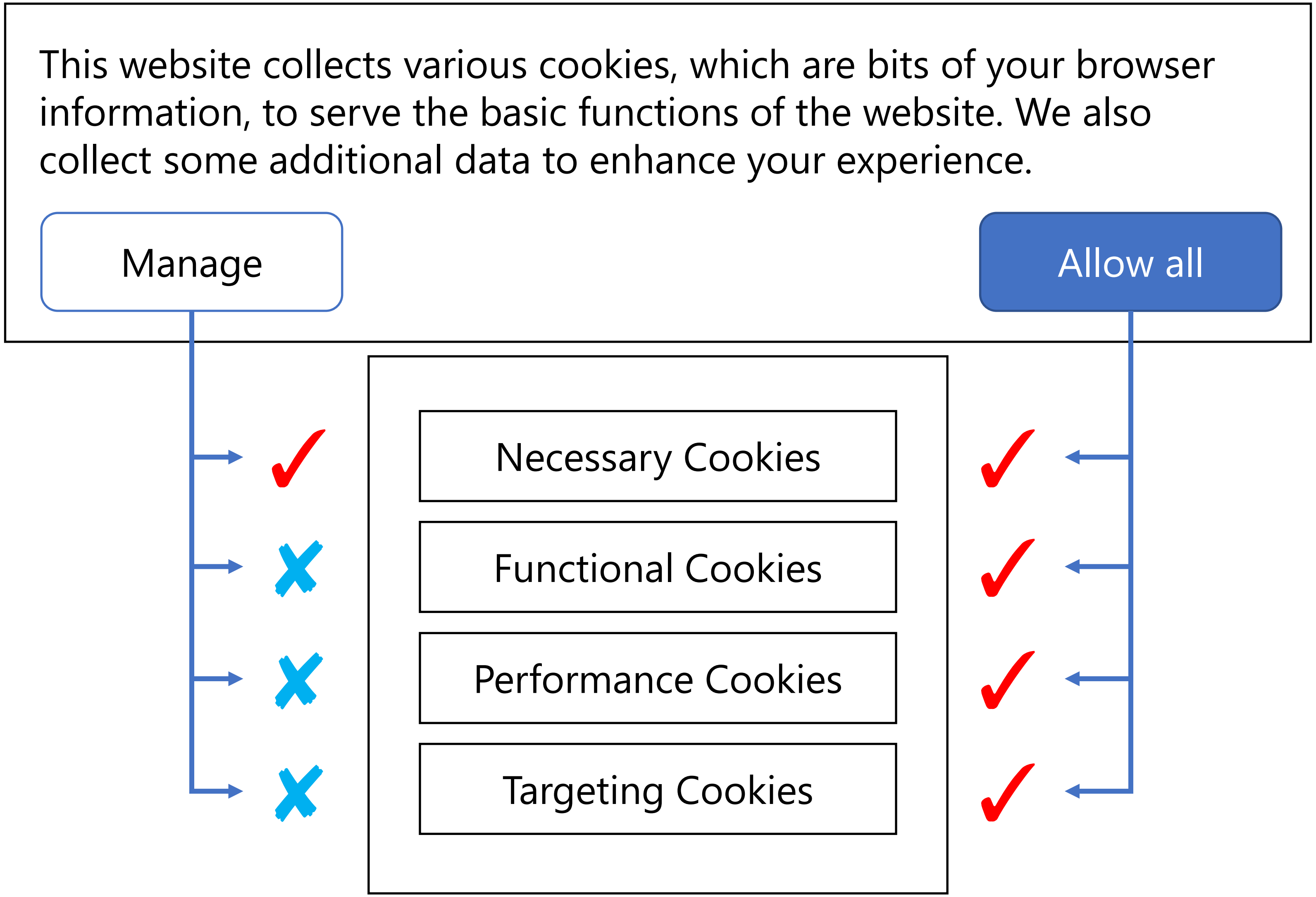
Selected Discussion on Emerging Topics

Opening a can of worms.

Here be dragons: Content following this slide will not be graded in exam. (May still be on exam for evaluation purposes but won’t affect your grade.)

1. How is your data being used?

Web tracking



This website collects various cookies, which are bits of your browser information, to serve the basic functions of the website. We also collect some additional data to enhance your experience.

Manage

Allow all

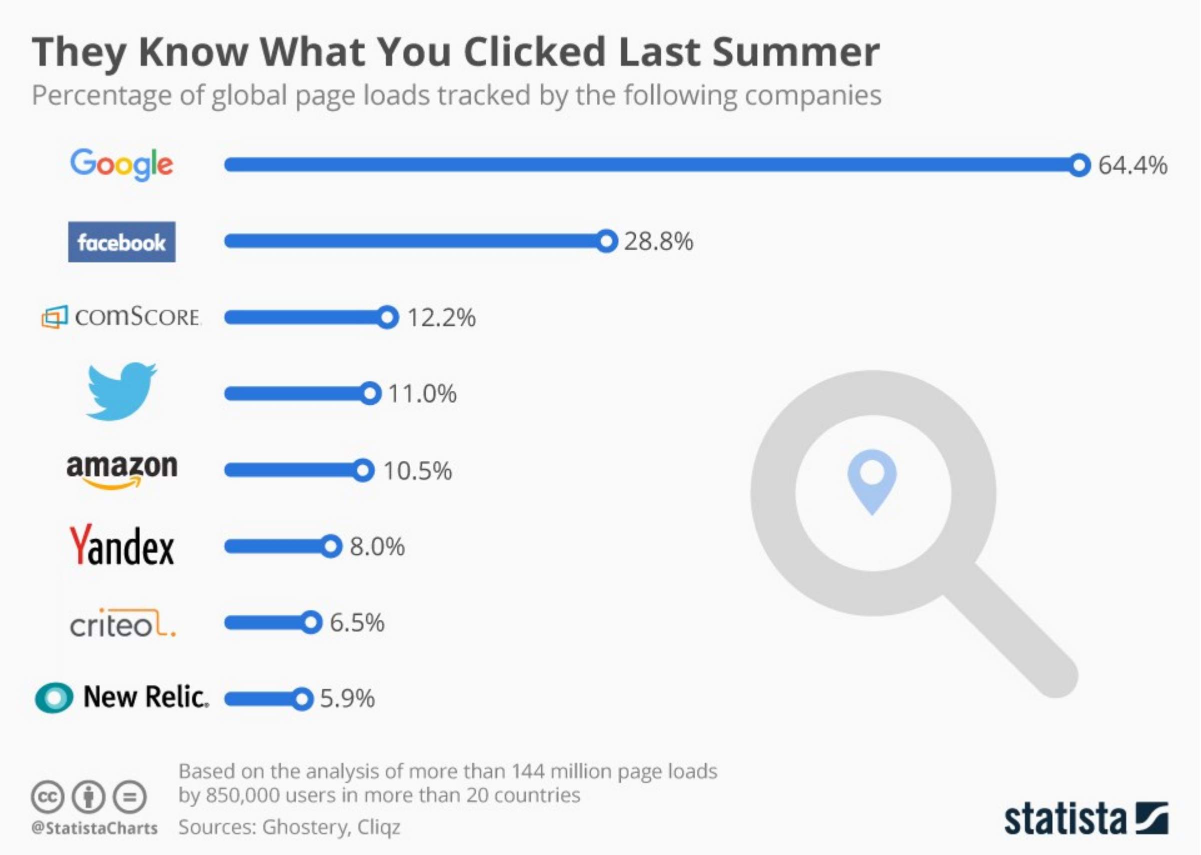
✓ Necessary Cookies ✓

✗ Functional Cookies ✓

✗ Performance Cookies ✓

✗ Targeting Cookies ✓

Who keeps your data?



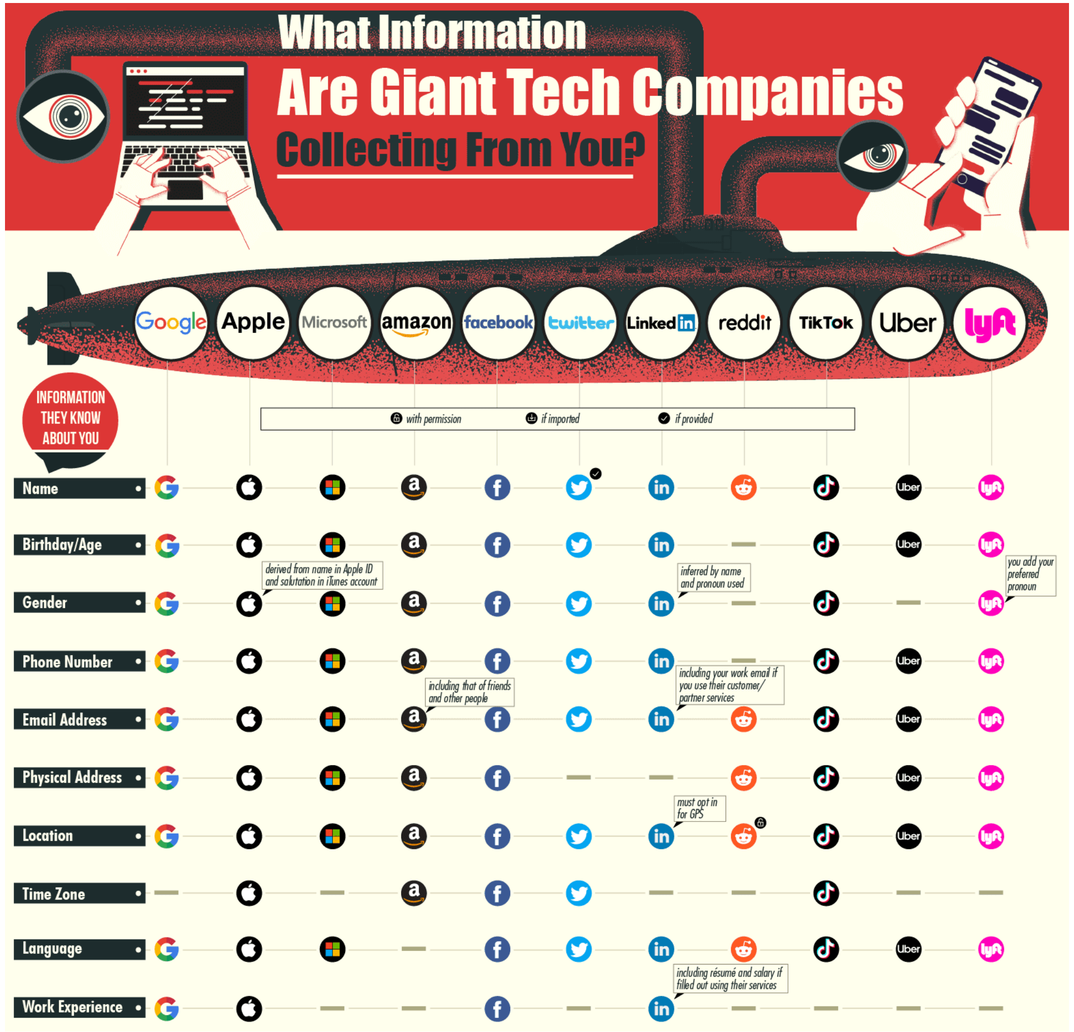
They Know What You Clicked Last Summer

Percentage of global page loads tracked by the following companies

Based on the analysis of more than 144 million page loads by 850,000 users in more than 20 countries

@StatistaCharts Sources: Ghostery, Cliqz

https://www.statista.com/chart/12236/reach-of-companies-tracking-online-behavior/



What Information Are Giant Tech Companies Collecting From You?

INFORMATION THEY KNOW ABOUT YOU

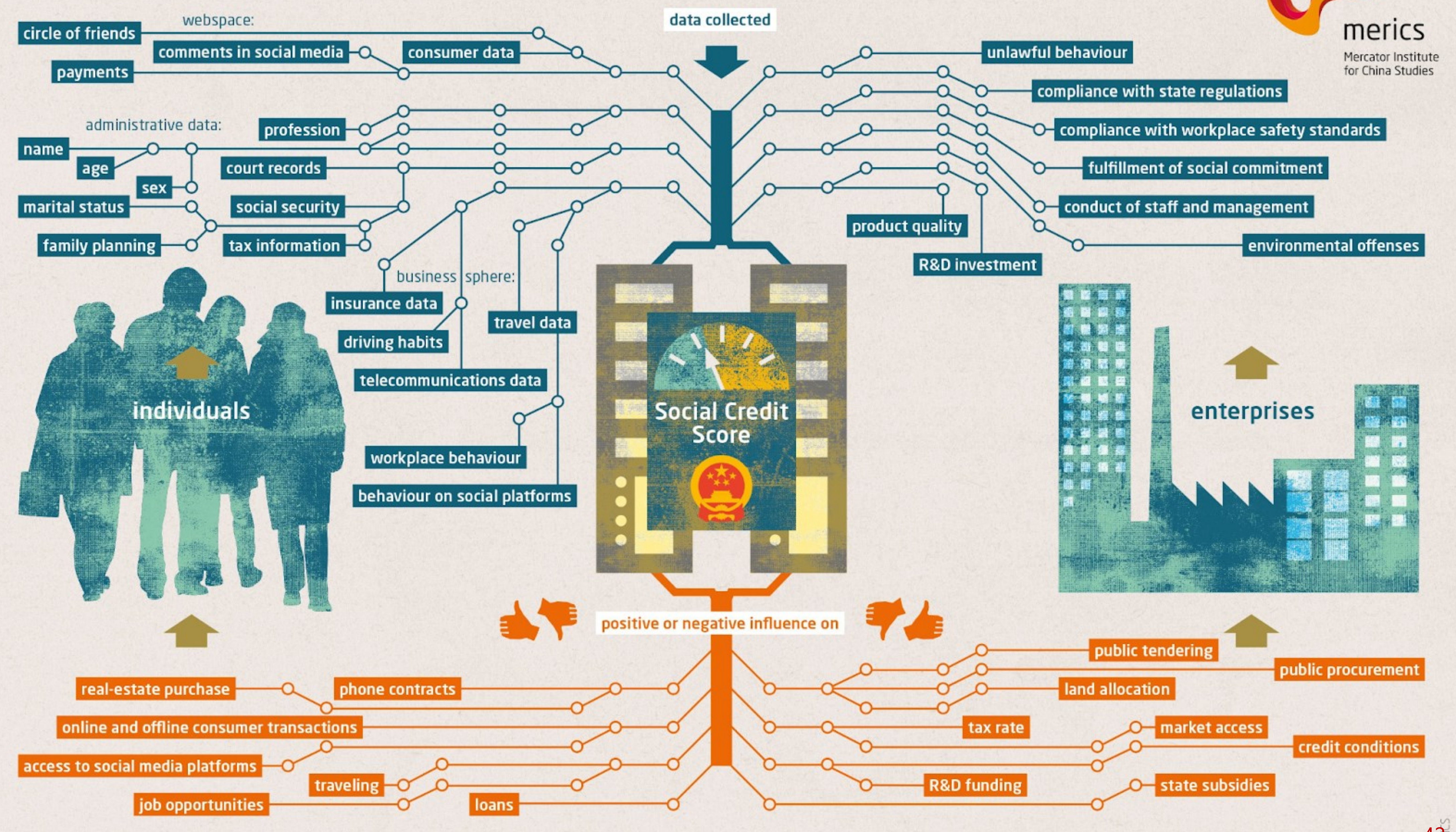
🔓 with permission ⊕ if imported ✓ if provided

	Google	Apple	Microsoft	amazon	facebook	twitter	LinkedIn	reddit	TikTok	Uber	lyft
Name	●	●	●	●	●	● ✓	●	●	●	●	●
Birthday/Age	●	●	●	●	●	●	●	—	●	●	●
Gender	●	● derived from name in Apple ID and salutation in iTunes account	●	●	●	●	● inferred by name and pronoun used	—	●	—	● you add your preferred pronoun
Phone Number	●	●	●	●	●	●	●	—	●	●	●
Email Address	●	●	●	● including that of friends and other people	●	●	● including your work email if you use their customer/ partner services	●	●	●	●
Physical Address	●	●	●	●	●	—	—	●	●	●	●
Location	●	●	●	●	●	●	● must opt in for GPS	● 🔓	●	●	●
Time Zone	—	●	—	●	●	●	—	—	●	—	—
Language	●	●	●	—	●	●	●	●	●	●	●
Work Experience	●	●	—	—	●	—	● including résumé and salary if filled out using their services	—	—	—	—

https://www.digitalinformationworld.com/2020/08/infographic-what-data-are-giant-tech-companies-collecting-from-you.html

The all-seeing state: China's plans for total data control

merics
Mercator Institute
for China Studies



data collected

webspace:
circle of friends
comments in social media
consumer data
payments

administrative data:
name
age
sex
marital status
family planning
profession
court records
social security
tax information

business sphere:
insurance data
driving habits
travel data
telecommunications data
workplace behaviour
behaviour on social platforms

individuals

unlawful behaviour
compliance with state regulations
compliance with workplace safety standards
fulfillment of social commitment
conduct of staff and management
environmental offenses
product quality
R&D investment

enterprises

Social Credit Score

positive or negative influence on

real-estate purchase
phone contracts
online and offline consumer transactions
access to social media platforms
traveling
job opportunities
loans

public tendering
public procurement
land allocation
tax rate
market access
credit conditions
R&D funding
state subsidies

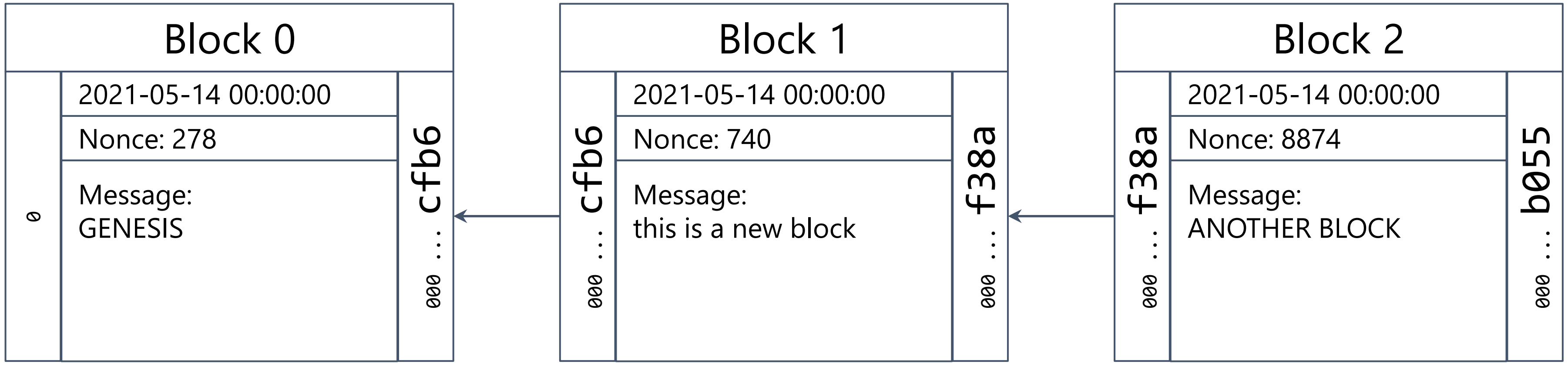
© MERICS

https://twitter.com/merics_eu/status/898220464090341377/photo/1

2. Cryptocurrency: Digital Goldmine, or What?

Blockchain in 1 minute

- Blockchain is a series of data structures (**blocks**) that cryptographically verify each other.
- Blocks are created by **mining**, a cryptographic process that **consumes processing power**.



Block 0

0

2021-05-14 00:00:00

Nonce: 278

Message:
GENESIS

000 ... cfb6

Block 1

000 ... cfb6

2021-05-14 00:00:00

Nonce: 740

Message:
this is a new block

000 ... f38a

Block 2

000 ... f38a

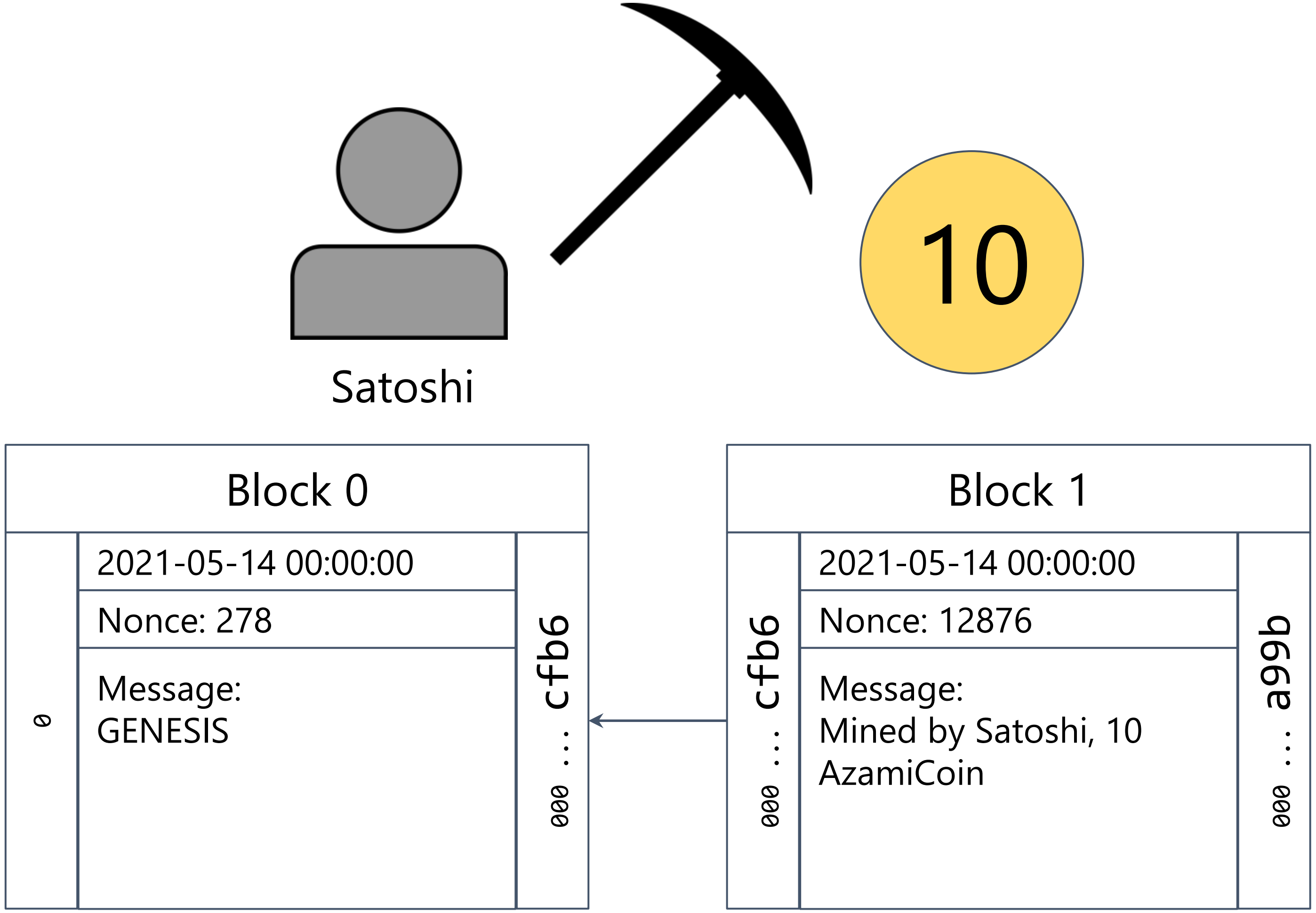
2021-05-14 00:00:00

Nonce: 8874

Message:
ANOTHER BLOCK

000 ... b055

Mining can be used to create **cryptocurrency.**



Block 0

0

2021-05-14 00:00:00

Nonce: 278

Message:
GENESIS

000 … cfb6

Block 1

000 … cfb6

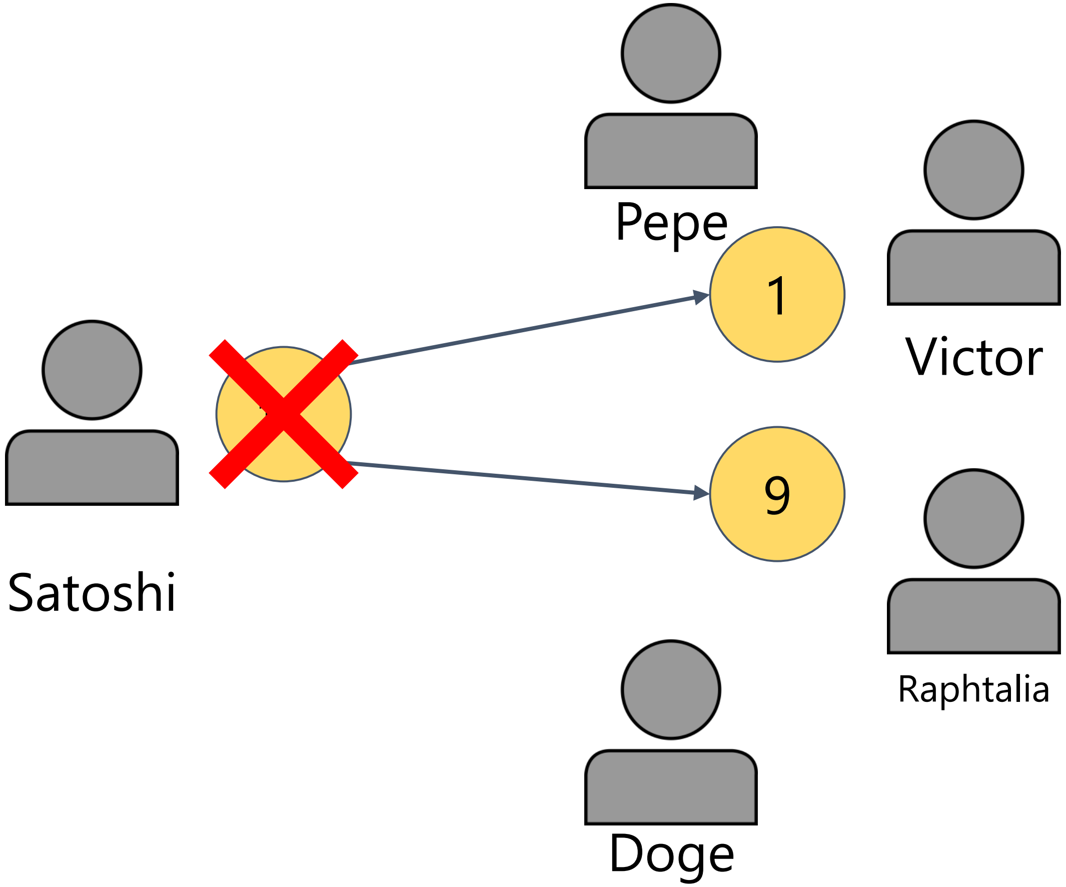
2021-05-14 00:00:00

Nonce: 12876

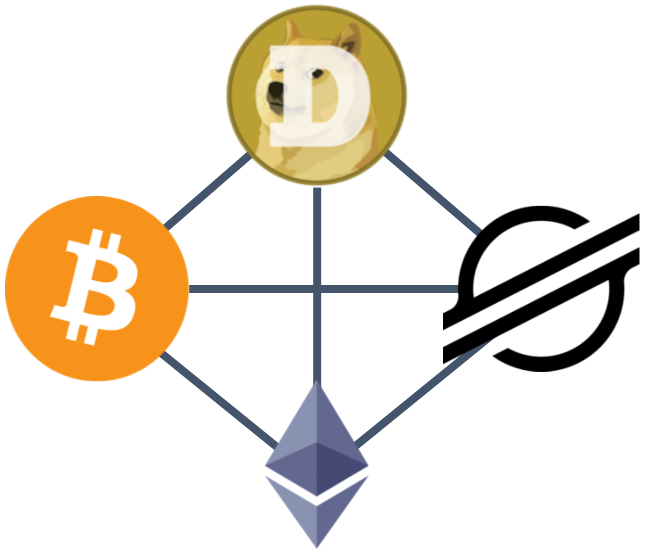
Message:
Mined by Satoshi, 10
AzamiCoin

000 … a99b

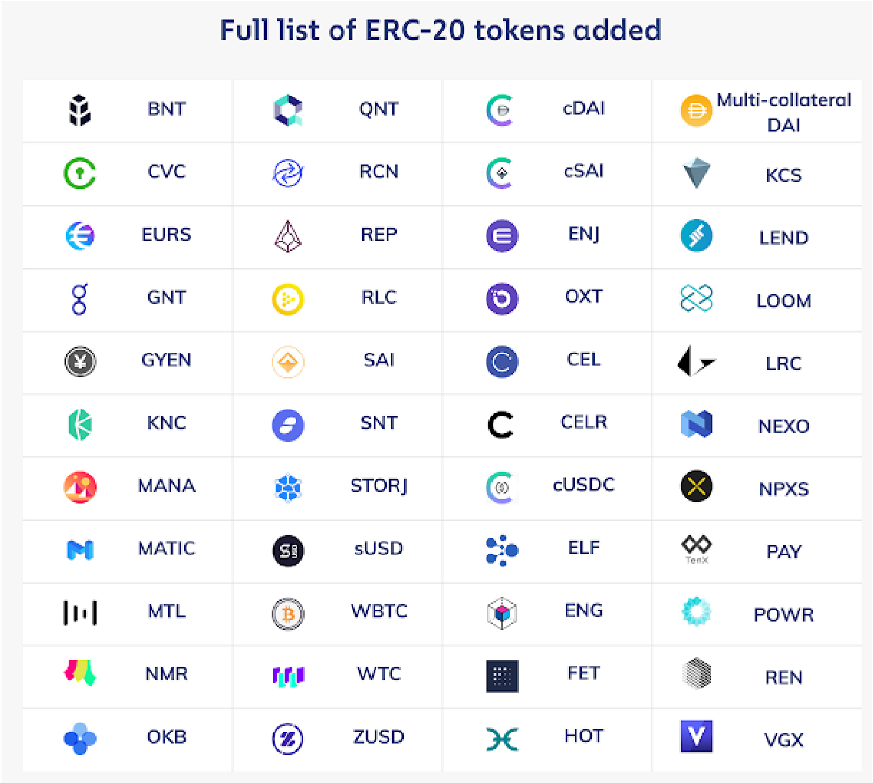
Transaction of cryptocurrency using cryptographic signatures forms the basis of cryptocurrency.



Many “tokens”, or “currencies” are now available worldwide.



Decentralized trading allows anyone to “become a bank”.

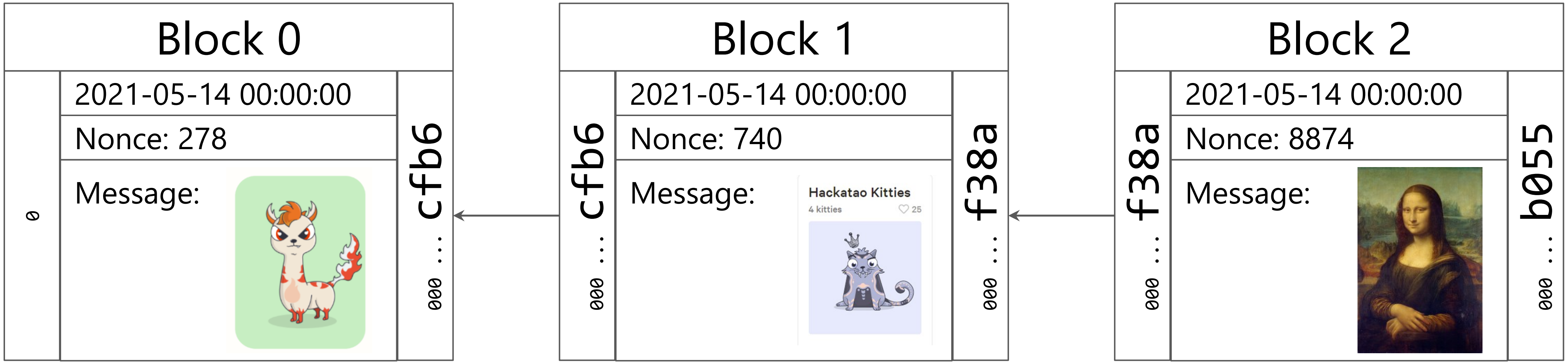


Full list of ERC-20 tokens added

BNT	QNT	cDAI	Multi-collateral DAI
CVC	RCN	cSAI	KCS
EURS	REP	ENJ	LEND
GNT	RLC	OXT	LOOM
GYEN	SAI	CEL	LRC
KNC	SNT	CELR	NEXO
MANA	STORJ	cUSDC	NPXS
MATIC	sUSD	ELF	PAY
MTL	WBTC	ENG	POWR
NMR	WTC	FET	REN
OKB	ZUSD	HOT	VGX

https://blog.chainalysis.com/reports/erc20-updates-march-2020

Specific, "unit" types of digital collectibles form the NFT (non-fungible token) economy.



Block 0

0

2021-05-14 00:00:00

Nonce: 278

Message:

000 ... cfb6

Block 1

000 ... cfb6

2021-05-14 00:00:00

Nonce: 740

Message:

000 ... f38a

Block 2

000 ... f38a

2021-05-14 00:00:00

Nonce: 8874

Message:

000 ... b055

Digital Investment Asset

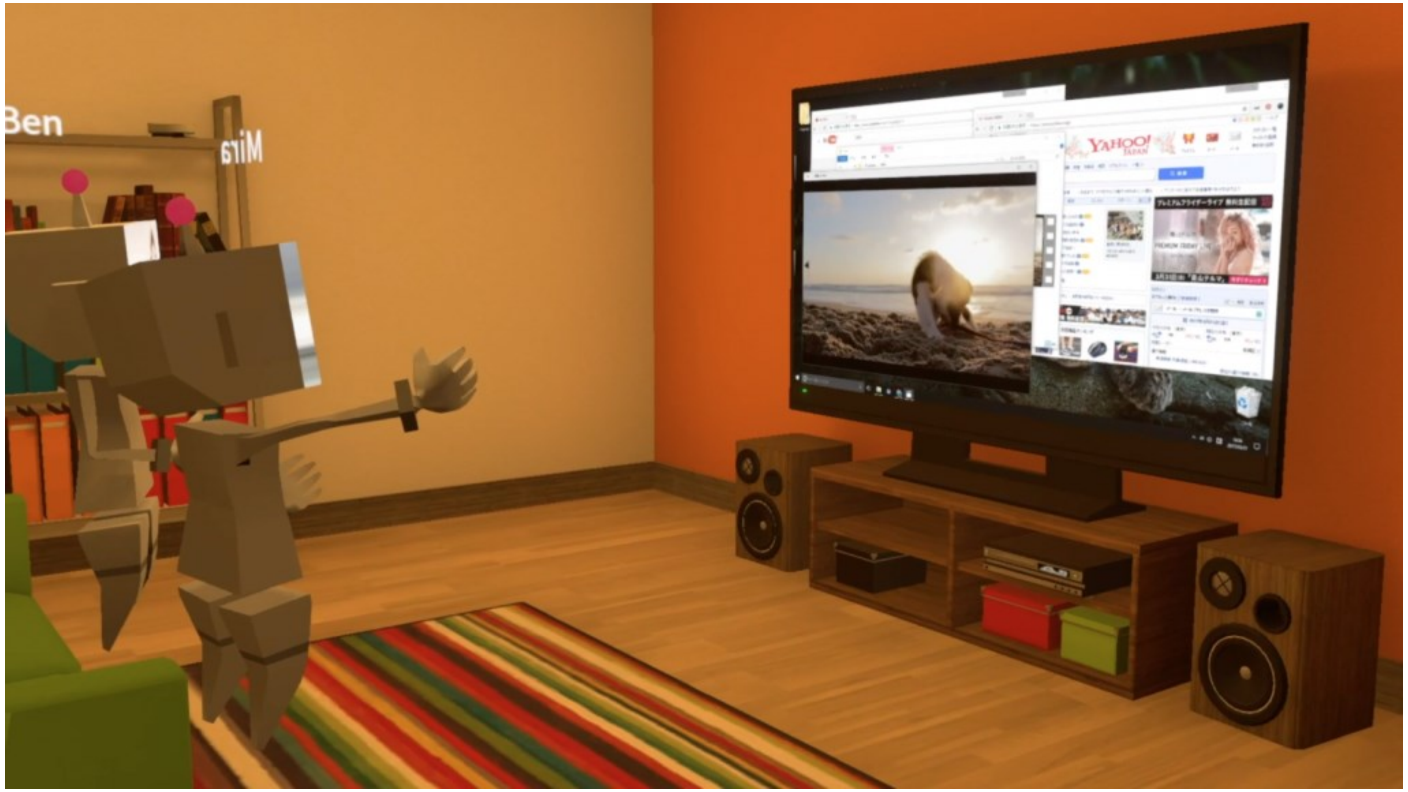
Game Token

Digital Artwork

3. Facebook’s Rebrand to Meta

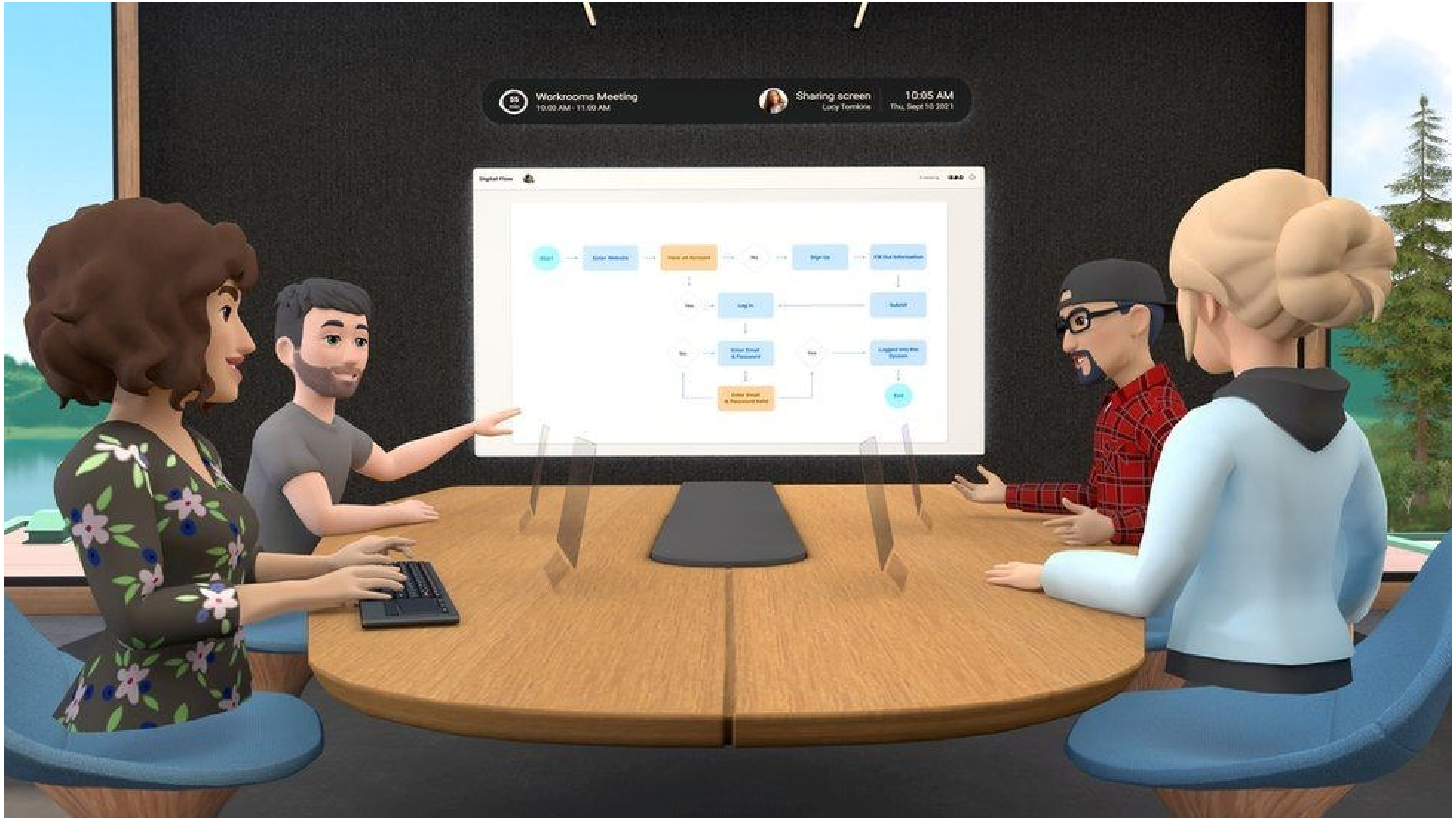
But what is the metaverse?

- What if we can live inside the Internet, 24/7/365?
- Does this *ring a bell*?



Both images via TechCrunch Japan

What about productivity use?



https://www.bbc.com/news/technology-58749529

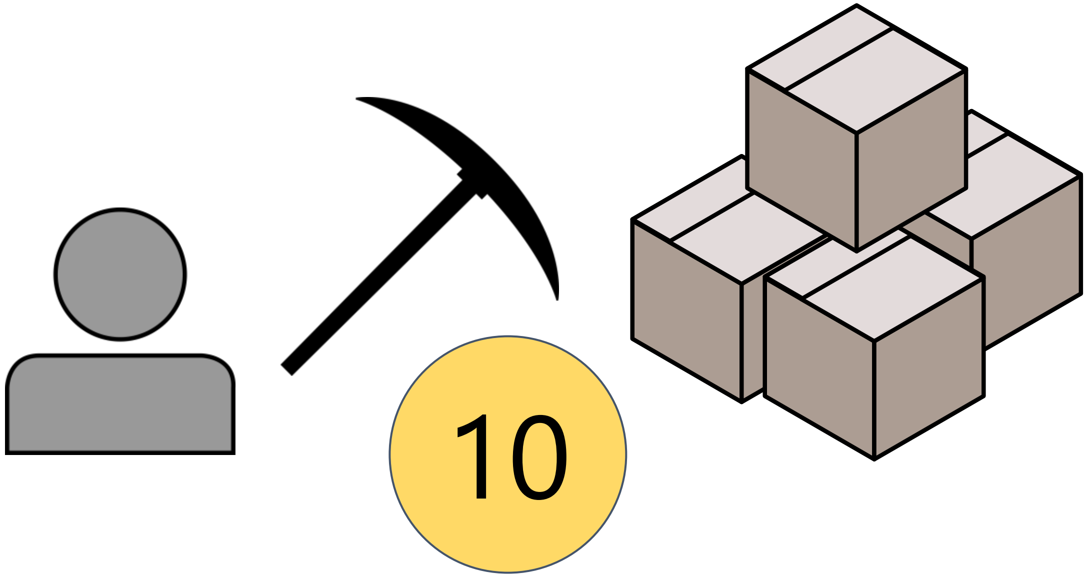
But can we trust these companies?

Zuckerberg testified last year before Congress that **[Facebook] removes 94 percent of the hate speech** it finds before a human reports it. But in internal documents, researchers estimated that the company was removing **less than 5 percent of all hate speech on Facebook**.

https://www.washingtonpost.com/technology/2021/10/25/what-are-the-facebook-papers/

Crypto-Metaverse: Another Player!

Cryptocurrency entrepreneurs are rapidly creating new services to build digital economies around metaverses.



https://www.rockpapershotgun.com/things-to-build-in-minecraft-building-ideas

Is the Government Helping?

Economy and Cryptocurrency

Ethical Use of Data

Psychological Manipulation of Users

Misinformation & Fake News

Graphics: j4p4n / OpenClipart