

# ECE458/ECE750T27: Computer Security

## Revision

Dr. Kami Vania,  
Electrical and Computer Engineering  
[kami.vania@uwaterloo.ca](mailto:kami.vania@uwaterloo.ca)



UNIVERSITY OF  
**WATERLOO**

FACULTY OF  
ENGINEERING



# First, the news...

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
  1. Some students show up late for various good reasons
  2. Reward students who show up on time
  3. Important to see real world examples

## Side-channel attack

Instead of tracking a Prime Minister, easier to just wait for his security detail to upload running data onto Strava.

## Swedish PM's private address revealed by Strava data shared by bodyguards

Data made public by Ulf Kristersson's security revealed his location, routes and movements over several years



📷 An Instagram post of Ulf Kristersson (right) running with Jonas Gahr Støre, the Norwegian prime minister (left), and Alexander Stubb (centre), the Finnish president, in Norway. Photograph: kristerssonulf / instagram

Secret service bodyguards have been accused of jeopardising the Swedish prime minister's safety over several years by sharing details of their running and cycling routes on the fitness app Strava.

Ulf Kristersson's bodyguards appear to have inadvertently revealed his location, routes and movements - including details of hotels and his private addresses - by uploading their workouts to the app, making them publicly available.

# We have covered...

- Basics of security
- Authentication
- Access control
- Cryptography
- Network
- Programming security
- Web security
- Privacy

## Not on exam

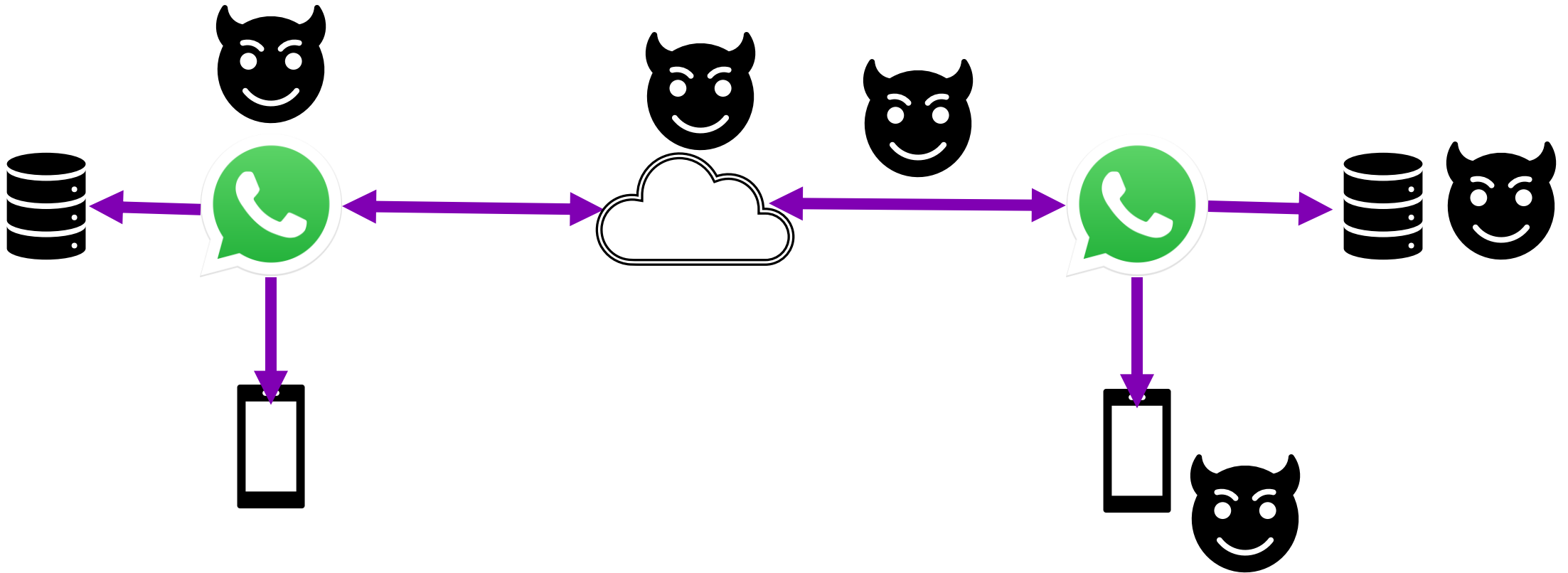
- ~~Phishing~~ – barely covered, will only show up on exams at a high level
- ~~STRIDE~~ – Threat modeling as a concept could be on the exam. But I do not expect you to know things like STRIDE
- ~~IPv6~~ – It exists and is the newer version of IPv4
- ~~Network Address Translation (NAT)~~

# CORE CONCEPTS

# Will very likely show up on an exam:

- CIAAA definition
- Privacy definition
- Man in the Middle attacks
- Reference monitor
- Key skills learned in activities (not all activities teach skills)
- Swiss Cheese Model
- Threat model – who is the attacker, what can they do?

**Data exists in different places, and the approaches to protect it differ depending on where it is.**



# TWO CASES



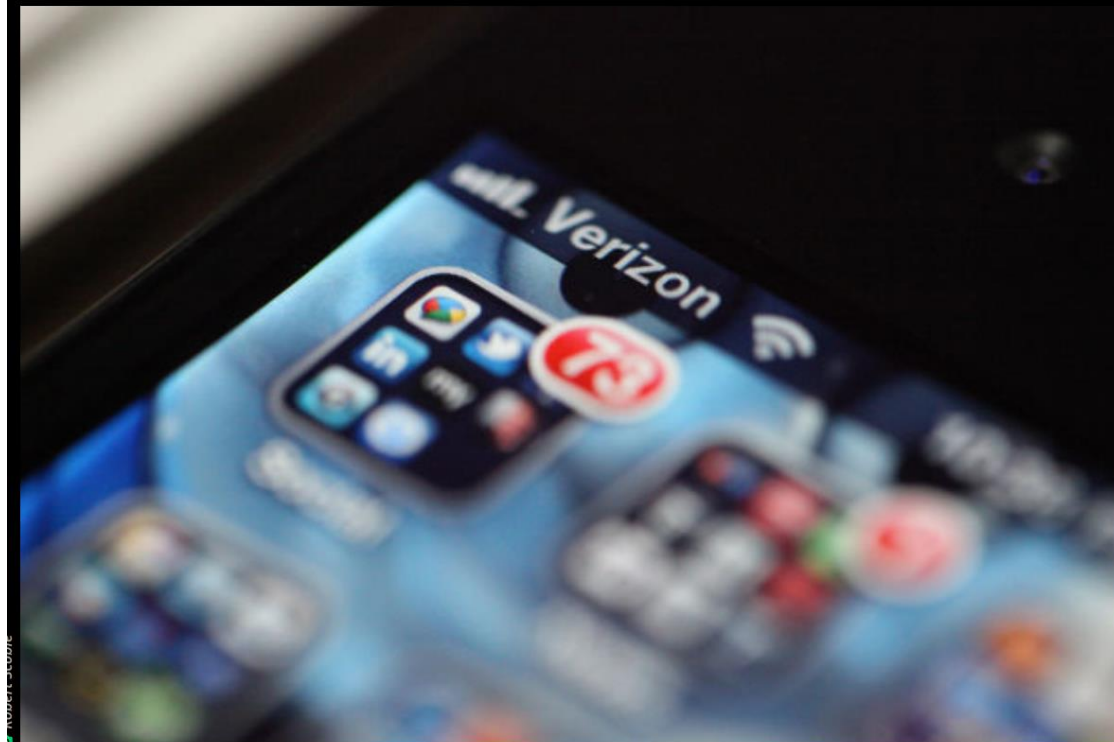
Verizon added cookies to all connections so that advertisers could track better and link data to demographics Verizon provided.

BIZ &amp; IT—

## Verizon's zombie cookie gets new life

Verizon's tracking supercookie joins up with AOL's ad tracking network.

JULIA ANGIN AND JEFF LARSON, PROPUBLICA - 10/7/2015, 8:00 AM



65

Verizon is giving a new mission to its controversial hidden identifier that tracks users of mobile devices. Verizon said in a little-noticed [announcement](#) that it will soon begin sharing the profiles with AOL's ad network, which in turn monitors users across a large swath of the Internet.



### FURTHER READING

Verizon will now let users kill previously indestructible tracking code

That means AOL's ad network will be able to match millions of Internet users to their real-world details gathered by Verizon, including "[your gender, age range and interests](#)." AOL's network is on 40 percent of websites, including on ProPublica.

AOL will also be able to use data from Verizon's identifier to track the apps that mobile users open, what sites they visit, and for how long. Verizon purchased AOL earlier this year.

# Verizon MITM to add a “perma-cookie”

- Verizon smartphone customer traffic was modified by Verizon to add a header with a unique identifier
- “Verizon Wireless does not use the [cookie] to track where customers go on the web.” @kennwhite (Verizon)
- Opt-out option was provided to customers two years after the header started being used.
  - “If a customer has not opted out [...] ad serving partners will receive demographic and third-party interest based segments” @kennwhite (Verizon)

# On-device MITM Attack

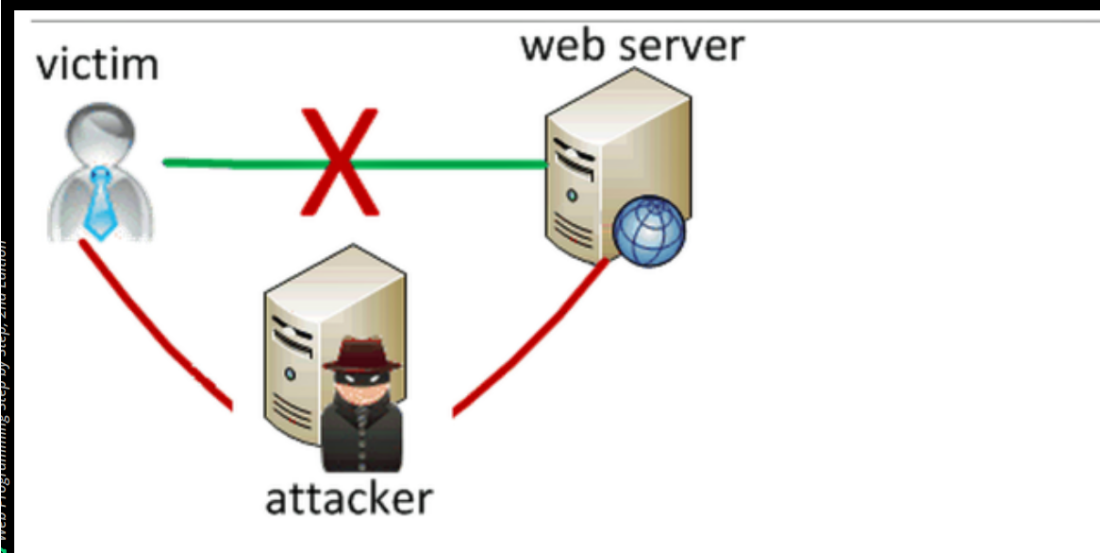
Lenovo shipped computers with software that used MITM to inject ads into all network traffic.

BIZ &amp; IT —

## Lenovo PCs ship with man-in-the-middle adware that breaks HTTPS connections [Updated]

Superfish may make it trivial for attackers to spoof any HTTPS website.

DAN GOODIN - 2/19/2015, 11:36 AM



333

Lenovo is selling computers that come preinstalled with adware that hijacks encrypted Web sessions and may make users vulnerable to HTTPS man-in-the-middle attacks that are trivial for attackers to carry out, security researchers said.

The critical threat is present on Lenovo PCs that have adware from a company called Superfish installed. As unsavory as many people find software that injects ads into Web pages, there's something much more nefarious about the Superfish package. It installs a self-signed root HTTPS certificate that can intercept encrypted traffic for every website a user visits. When a user visits an HTTPS site, the site certificate is signed and controlled by Superfish and falsely represents itself as the official website certificate.

Even worse, the private encryption key accompanying the Superfish-signed Transport Layer Security certificate appears to be the same for every Lenovo machine. Attackers may be able to use the key to certify imposter HTTPS websites that masquerade as Bank of America, Google, or any other secure destination on the Internet. Under such a scenario, PCs that have the Superfish root certificate installed will fail to flag the sites as forgeries—a failure that completely undermines the reason HTTPS protections exist in the first place.

# Lenovo, a laptop manufacturer

- Pre-installed Superfish
- Superfish Man-in-the-middle all traffic and added advertising
- Superfish/Lenovo pre-installed a single self-signed root certificate
- They used the same root certificate with a weak 1024-bit RSA key on ALL affected Lenovo PCs (1024-bit depreciated in 2013)

152 3134

## UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE COMMISSION

Commissioners: **Maureen K. Ohlhausen, Acting Chairman**  
**Terrell McSweeney**

In the Matter of

**LENOVO (UNITED STATES) INC.**  
**a corporation.**

**Docket No. C-**

### COMPLAINT

The Federal Trade Commission, having reason to believe that Lenovo (United States) Inc. has violated Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Lenovo (United States) Inc. (“Lenovo”) is a Delaware corporation with its principal office or place of business located at 1009 Think Place, Morrisville, North Carolina 27560-9002.
2. The acts and practices of Respondent alleged in the Complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

### **RESPONDENT’S BUSINESS PRACTICES**

3. Respondent is one of the world’s largest manufacturers of personal computers, including desktop computers, laptops, notebooks, and tablets. Respondent employs approximately 7,500 people in the United States.
4. In August 2014, Respondent began selling certain laptop models to U.S. consumers with a preinstalled ad-injecting software (commonly referred to as “adware”), known as VisualDiscovery. VisualDiscovery was developed by Superfish, Inc. , a Delaware corporation with its principal office or place of business located in Palo Alto, California.
5. VisualDiscovery delivered pop-up ads to consumers of similar-looking products sold by Superfish’s retail partners whenever a consumer’s cursor hovered over the image of a product on a shopping website. For example, if a consumer’s cursor hovered over a product image while the consumer viewed owl pendants on a shopping website like Amazon.com, VisualDiscovery would overlay pop-up ads onto that website of other similar-looking owl pendants sold by Superfish’s retail partners.

# DEFINITIONS



## Security is a whole system issue

- Software
- Hardware
- Physical environment
- Personnel
- Corporate and legal structures

## Security properties to ensure

**Confidentiality** No improper information gathering

**Integrity** Data has not been (maliciously) altered

**Availability** Data/services can be accessed as desired

**Accountability** Actions are traceable to those responsible

**Authentication** User or data origin accurately identifiable



# Defining privacy

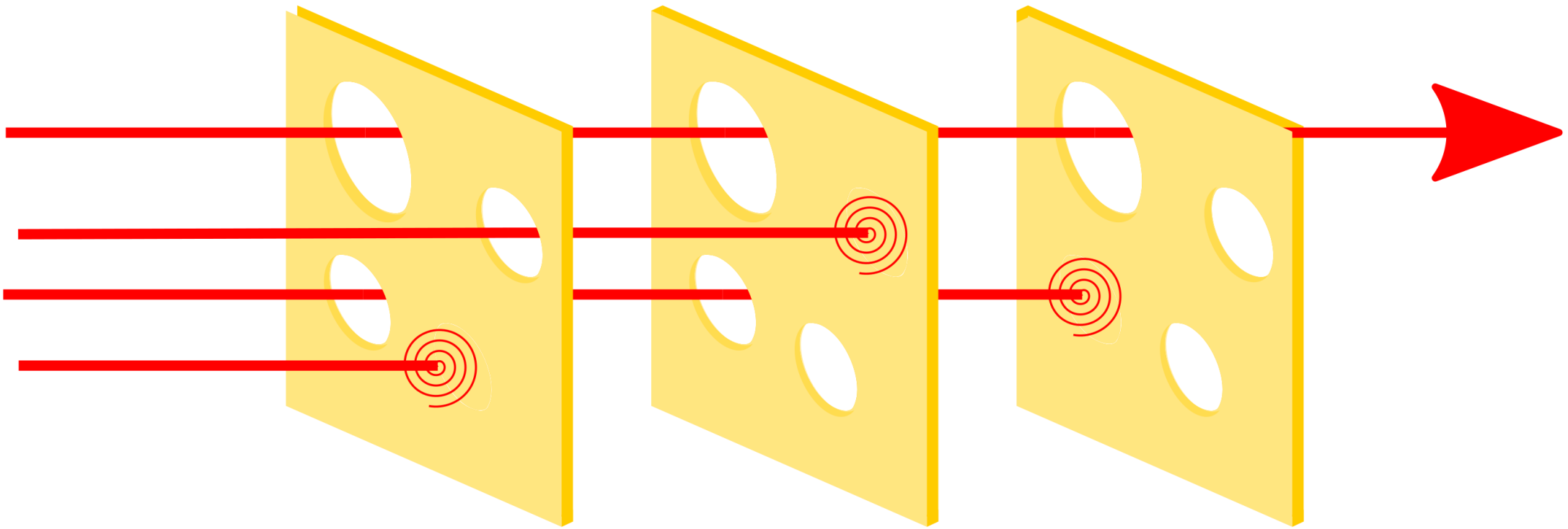
- The Cambridge Dictionary

- Someone's right to keep their personal matters and relationships secret
  - Right to control the disclosure and use of personal data
  - Right to not disclose information
- Be alone and control access to themselves
  - Right to be let alone
  - Right to control access to themselves
  - Right to have a space (physical, digital, mental) that is inaccessible to others





# Swiss Cheese Model



# BRUCE WAYNE/BATMAN'S THREAT MODEL



## ASSETS



BAT CAVE



ALFRED



EMAILS



TEXTS

## PROTECTION



SECURITY SYSTEM



HIDE LOCATION



ENCRYPTION

## THREATS



POLICE



THE JOKER



JOURNALISTS

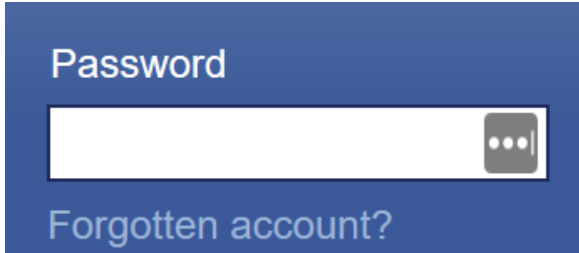
- - - LOW RISK  
— MED RISK  
= HIGH RISK

# AUTHENTICATION AND ACCESS CONTROL

# Authentication

- Verifying a fact about an entity before allowing it/them to perform an action
  - Entity could be a person or a computer or even an animal (think dog doors)
  - Action can include viewing, reading, writing, or interacting in any way (see access control)
- Authentication should happen every time an action is taken and there is no way to be certain that the authenticated entity has not changed.
  - Authentications do not have to be the same
  - Initial authentication can be:
    - person -> computer
    - person -> web server
    - Followed by computer -> web server for future transactions

# Authentication factors (for humans)



- Something you **know**
  - Password, mother's maiden name, your address
- Something you **have**
  - Student ID card, credit card chip, RSA key fob, Yubikey
- Something you **are**
  - Fingerprints, voice tones, iris, typing patterns



# Password protections

## Problems

- Stranger guessing
- Significant-other guessing
- Offline/online guessing
- Tricking the user into giving it away (phishing)
- Stealing from users or from servers

## Protections

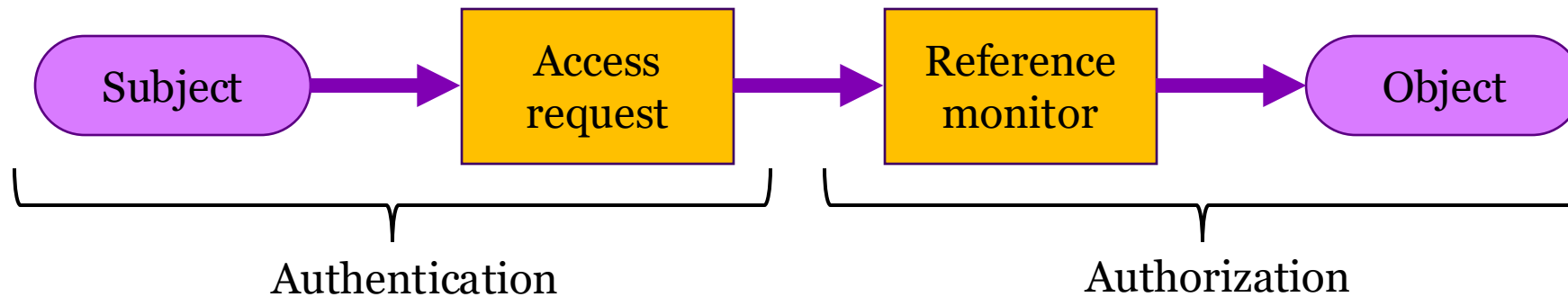
- Selecting passwords resistant to guessing
- Hashing with salt
- Lockout
- 2 factor authentication
  - SMS authentication
  - Authenticator app
- Backup authenticator (reset)

# Access Control

- Ensure that certain users can use a resource in one way (i.e. read-only), others in a different way (i.e. modify), and still others not at all.
- **Subjects** – human users who are often represented by surrogate programs running on behalf of the users
- **Objects** – things on which an action can be preformed. Such as files, database tables, programs, memory objects, hardware, network connections, and processors. User accounts can also be objects since they can be added to the system, removed, and modified.
- **Access modes** – any controllable actions of subjects on objects, including read, write, modify, delete, execute, create, destroy, copy export, and import.

# Access control

A guard controls whether a principal (the subject) is allowed to perform an action (access mode) on a resource (the object).





# Access Control Implementation

## Approaches

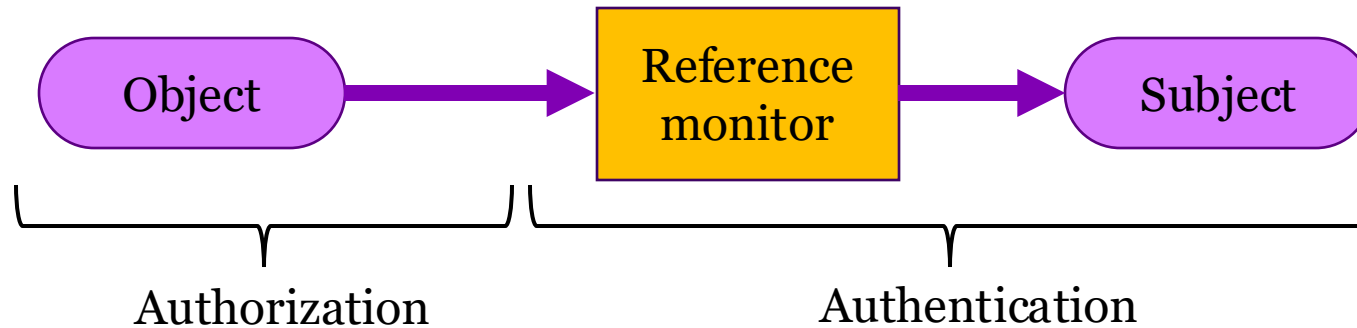
- Access Control Directory
- Access Control Matrix
- Access Control Triples
- Access Control Lists
  - Ordered with wildcards
- Capabilities

## Possible limitations

- Lookup time impacts file access time
- Revocation of permission accuracy and time
- Insertion time
- Conflicts – i.e. permission granted twice
- Delegation of permissions
  - Confused deputy problem

# Information flow control

A guard controls whether a principal (the subject) is allowed access to a resource (the object).



This is the dual notion, sometimes used when confidentiality is the primary concern.

# Information flow control

Document with top  
secret data



User



Email  
Server



Journalist

# Multi-level security

- **Multi-level security** (MLS) systems originated in the military. A **security level** is a label for subjects and objects to describe a policy.
- These are models or ways of thinking about the problem of access control logically and are not implementations
- Security levels are ordered

Unclassified  $\leq$  Confidential  $\leq$  Secret  $\leq$  Top Secret

- Ordering is important since it can express policies like “no write down” to prevent a subject with high-level clearance from writing secrets into a low-level document

# Bell-LaPadula

- Simple model of MLS designed to promote academic thought
  - **Simple Security Condition** – Subject  $S$  can read object  $O$  if and only if  $L(O) \leq L(S)$
  - **\*-Property (star property)** - Subject  $S$  can read object  $O$  if and only if  $L(S) \leq L(O)$
- In other words:
  - No read up
  - No write down

# Biba Integrity Model

- Focus on the integrity of the data rather than the confidentiality
  - Subjects S and Objects O have Integrity values
  - **Simple Integrity Property** – subjects at a given level of integrity must not read data at a lower integrity level (no read down)
  - \* **Integrity Property** – subjects at a given level of integrity must not write to data at a higher level of integrity (no write up)
  - **Invocation Property** – processes from below cannot request higher access; only with subjects at an equal or lower level
- In other words...
  - No read down
  - No write up

# PHISHING

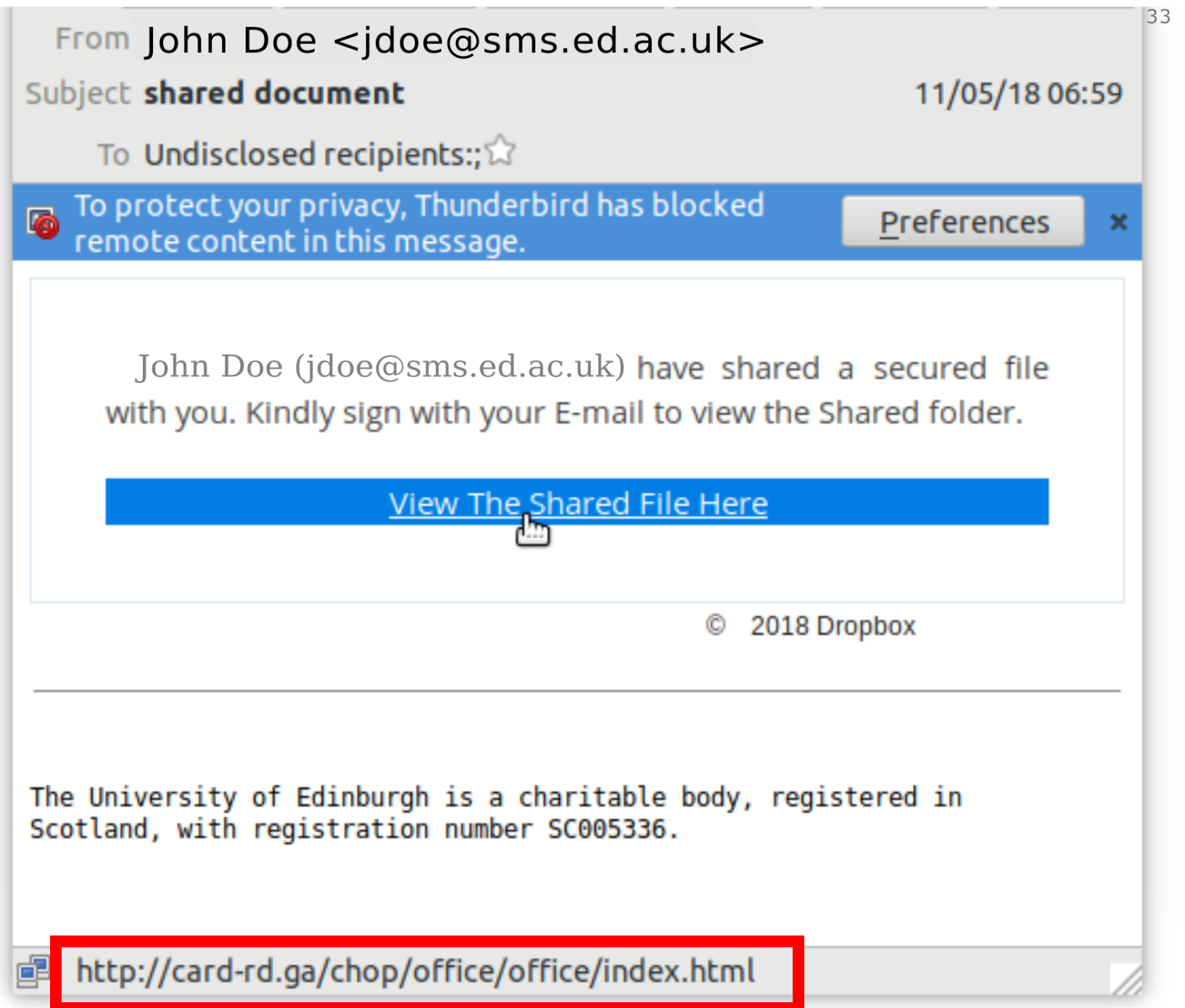
# This is a phishing email

Look real

- Realistic event
- Real student
- Visually identical to real email

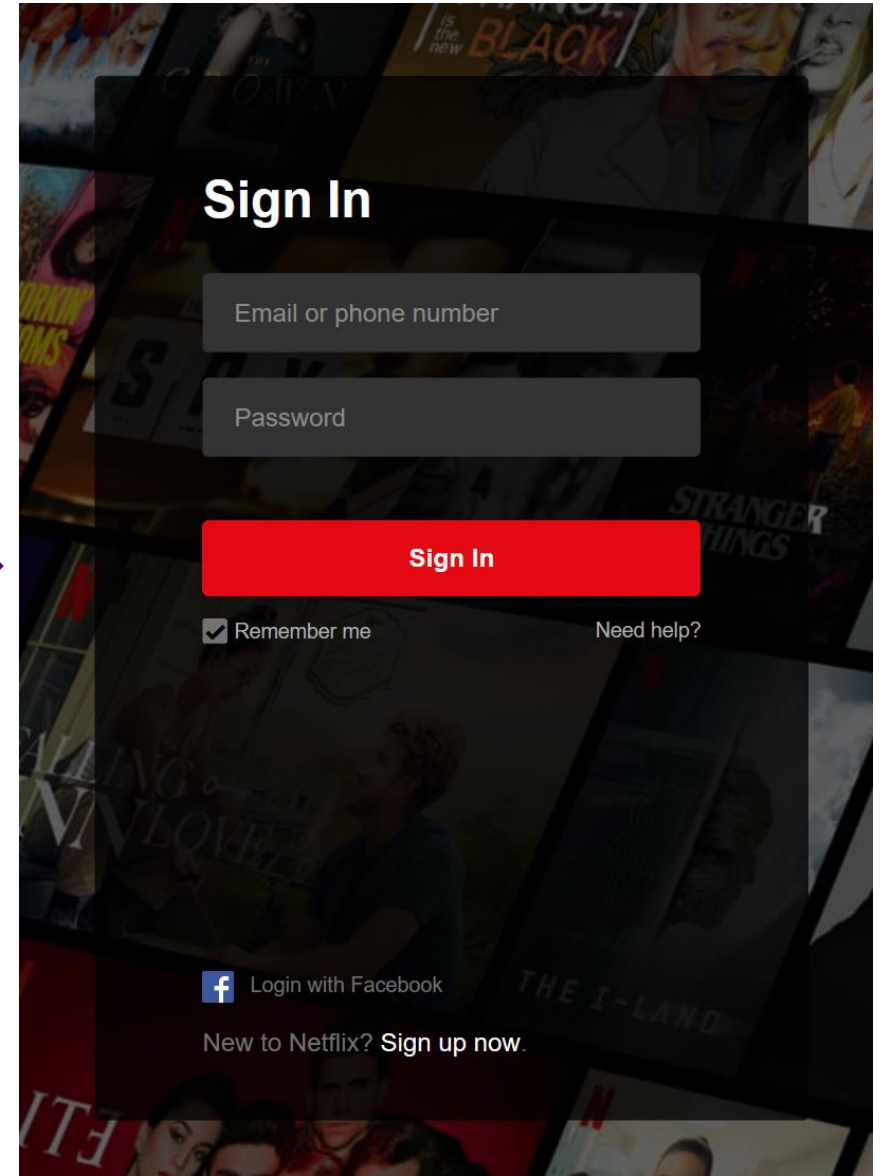
But

- Wrong URL





# But it is actually two directional



The user must first make sure they are interacting with the “correct” website. Then the website must make sure that they are interacting with the “correct” user.

# CRYPTOGRAPHY

# Assume the attacker knows how the crypto is done



# Caesar Cipher, shift 7 (a->h)

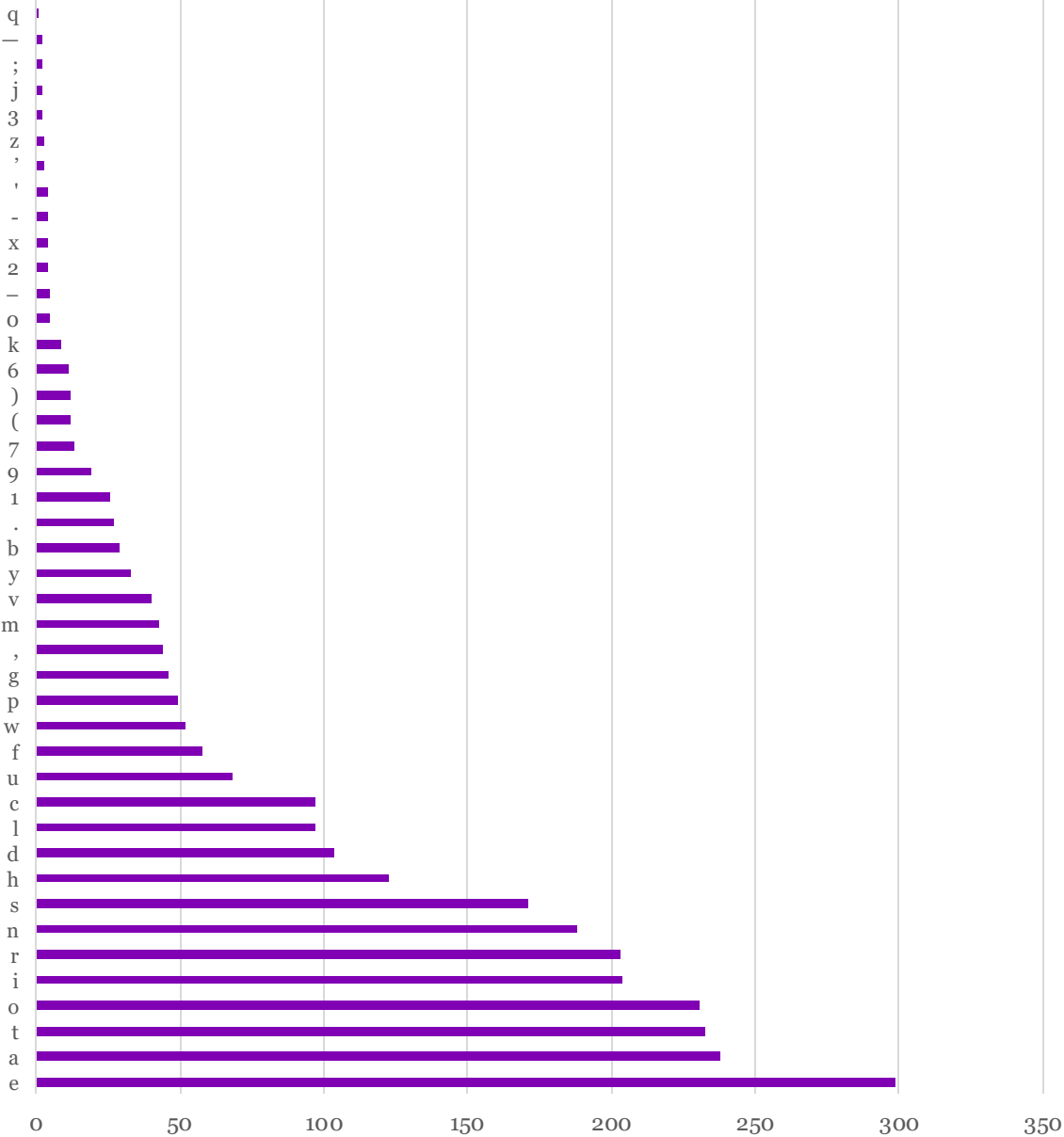
## Plaintext

margaret eleanor atwood, cc, o ont, frsc, poet, novelist, critic, professor (born 18 november 1939 in ottawa, on). a varied and prolific writer, margaret atwood is among the most celebrated authors in canadian history. her writing is noted for its careful craftsmanship and precision of language, which lend a sense of inevitability and a resonance to her words. in her fiction, atwood has explored the issues of our time, capturing them in the satirical, self-reflexive mode of the contemporary novel. she has written 14 novels, nine short-story collections, 16 books of poetry, and 10 volumes of non-fiction. she has received two governor general's literary awards, two booker prizes, a scotiabank giller prize, and numerous other honours and accolades. she is a companion of the order of canada and a chevalier of the l'ordre des arts et des lettres of france.

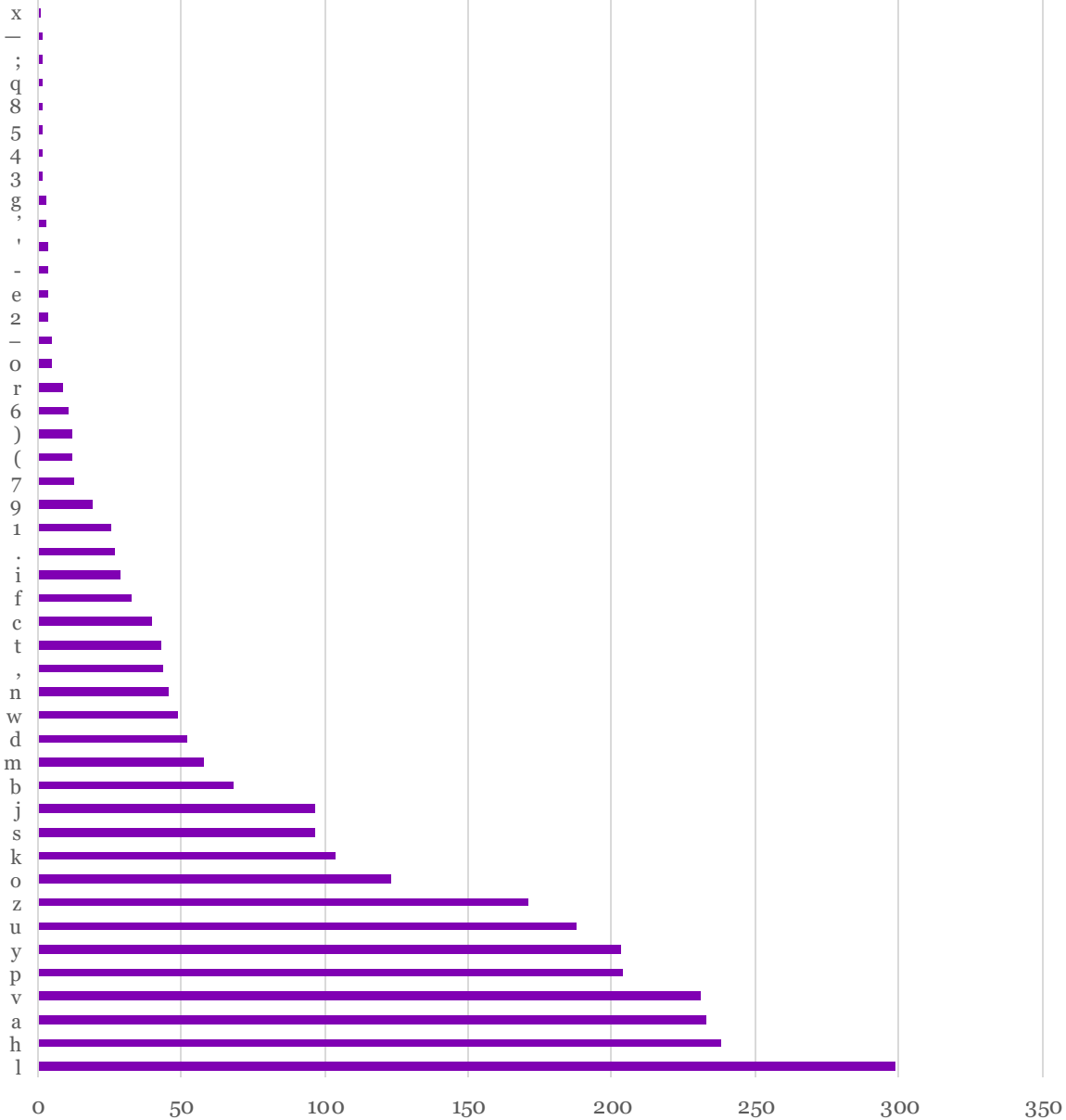
## Ciphertext

thynhyla lslhuvy hadvvk, jj, v vua, myzj, wvla, uvclspza, jypapj, wyvmlzzvy (ivyu 18 uvcltily 1939 pu vaahdh, vu). h chyplk huk wyvspmpj dypaly, thynhyla hadvvk pz htvun aol tvza jlsllyhalk hbaovyz pu jhuhkphu opzavyf. oly dypapun pz uvalk mvy paz jhylmbs jymazthuzopw huk wyljpzpvu vm shunbhnL, dopjo sluk h zluzl vm pulcpahipsfaf huk h ylvuhujl av oly dvykz. pu oly mpjapvu, hadvvk ohz lewsvylk aol pzzblz vm vby aptl, jhwabypun aolt pu aol zhapyphs, zlsm-ylmslepcl tvkl vm aol jvualtwvyhyf uvcls. zol ohz dypaalu 14 uvcls, upul zovya-zavyf jvssljapvuz, 16 ivvrz vm wvlayf, huk 10 cvsbtlz vm uvu-mpjapvu. zol ohz yljlpcl adv nvcluyvy nlulyhs'z spalyhyf hdhykz, adv ivvrly wypglz, h zjvaphihur npssly wypgl, huk ubtlyvbz vaoly ovuvbyz huk hjjvshklz. zol pz h jvtwhupvu vm aol vykly vm jhuhkh huk h jolchsply vm aol s'vykyl klz hyaz la klz slaaylz vm myhujl.

Letter Frequencies (Plaintext)



Letter Frequencies (Ciphertext)



# Playfair Cipher – Early Block Cipher

- **Rectangle:** pick from same row but opposite corner
- **Column:** pick letter one row down, wrapping if necessary.
- **Row:** pick letters one step to right, wrapping if necessary.

Z	*	*	O	*
*	*	*	*	*
*	*	*	*	*
R	*	*	X	*
*	*	*	*	*

Hence, OR → ZX

*	*	O	*	*
*	*	B	*	*
*	*	*	*	*
*	*	R	*	*
*	*	Y	*	*

If detailed Playfair shows up on the exam, the rules on this slide will be provided.

*	*	*	*	*
*	*	R	*	*
*	*	O	*	*
*	*	I	*	*
*	*	*	*	*

*	*	*	*	*
*	O	Y	R	Z
*	*	*	*	*
*	*	*	*	*
*	*	*	*	*

Hence, OR → YZ

*	*	*	*	*
*	*	*	*	*
*	O	R	W	*
*	*	*	*	*
*	*	*	*	*

Hence, OR → RW

Key: Playfair Example

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

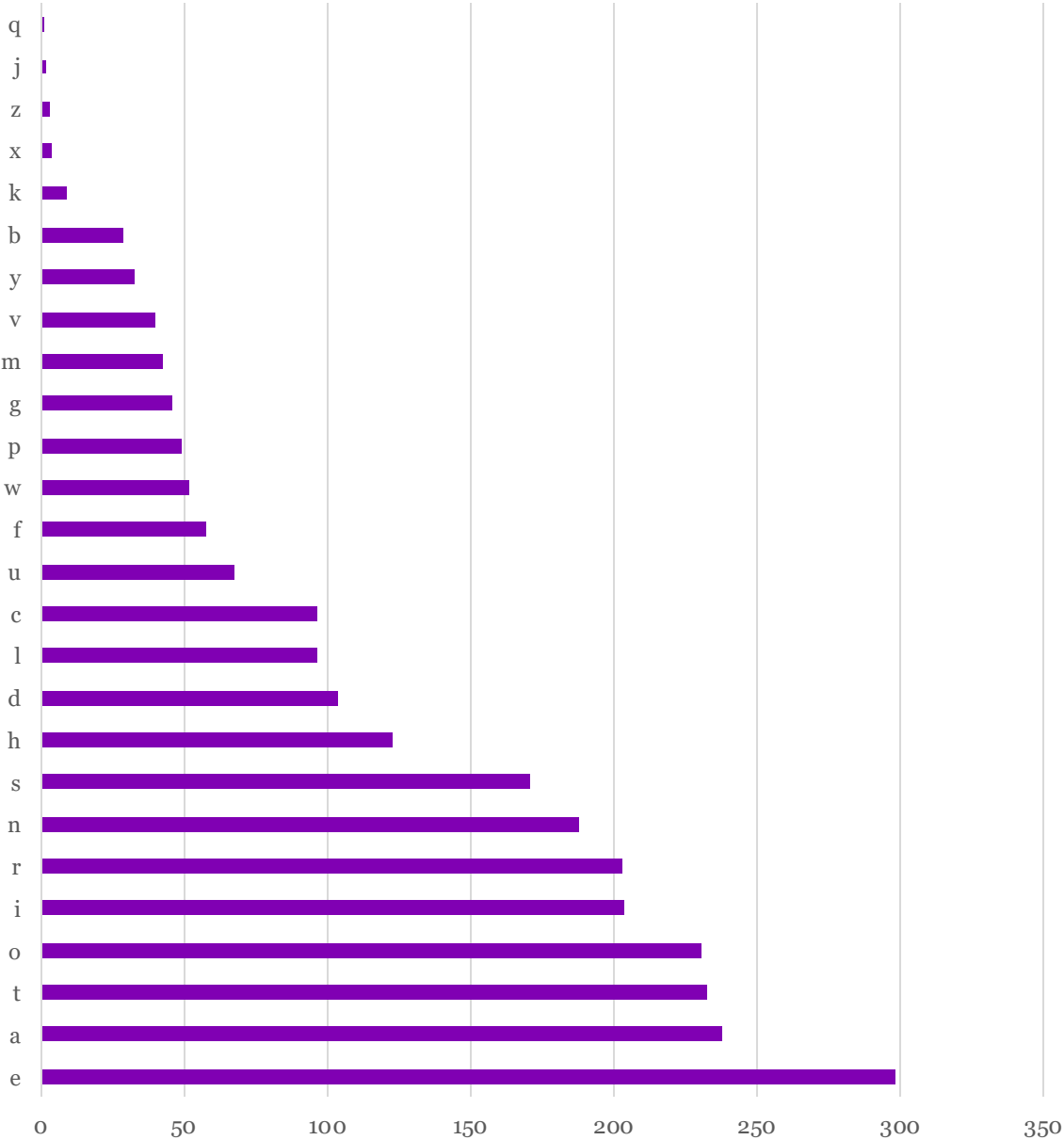
Plain text: Hello World

HE LX LO WO RL DX

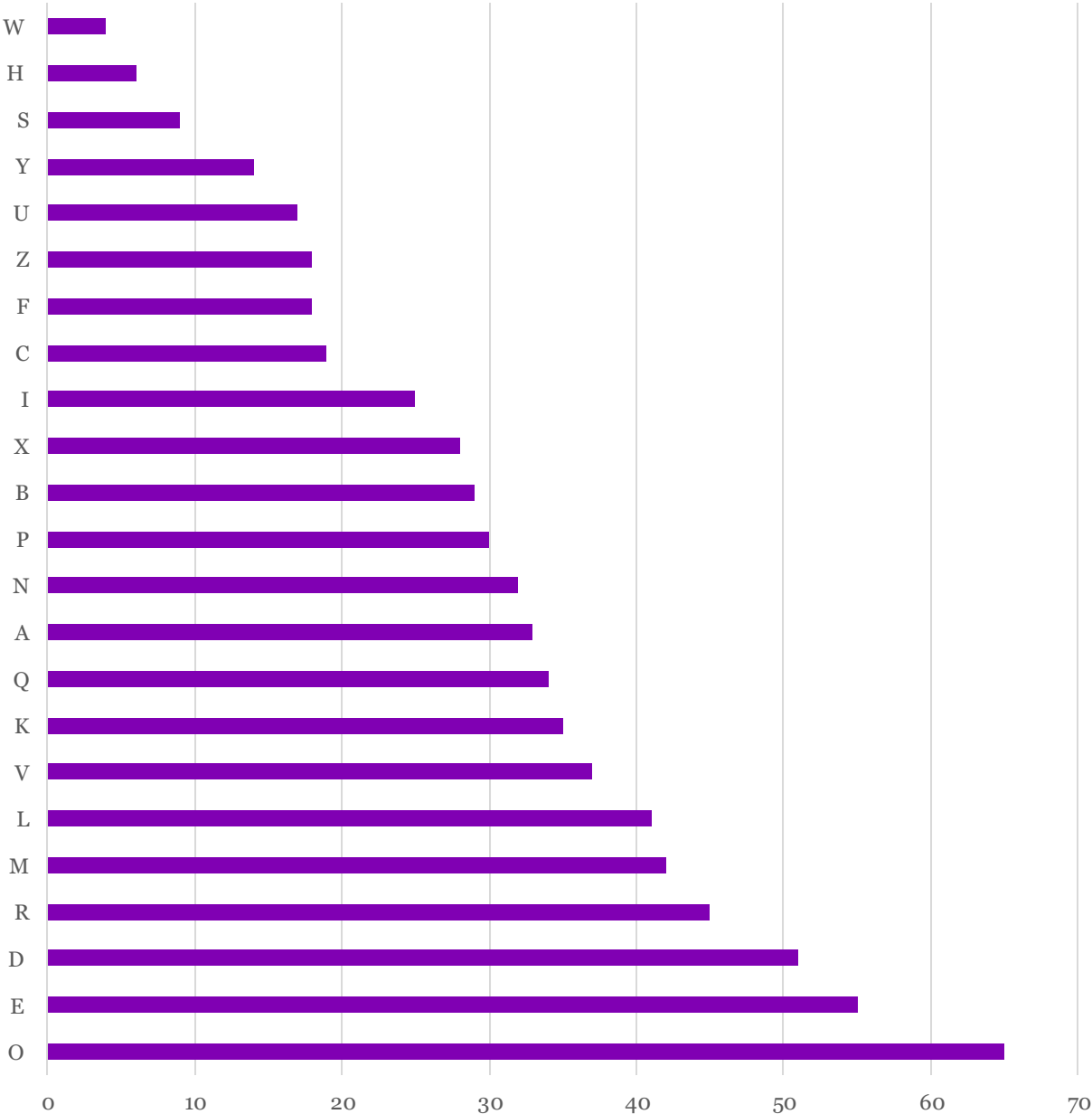
Diagram HE -> DM (rule 3)

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
K	N	O	Q	S
T	U	V	W	Z

Frequency - Plaintext



Frequencies - Ciphertext



# Stream vs Block

## Stream Ciphers

- Pros
  - Speed of transformation, each character can be encrypted/decrypted as it comes in
  - Low error propagation, a transcription error on one character will not impact the other characters
- Cons
  - Low diffusion, one character in plaintext results in one character of ciphertext
  - Susceptible to malicious insertions and modifications

## Block Ciphers

- Pros
  - High diffusion, information from the plaintext is spread across several ciphertext characters
  - Immunity to insertion, inserting one character will cause issues in deciphering
- Cons
  - Slow to encrypt, the entire block must be encrypted/decrypted at once
  - Padding, message must be a certain length and sometimes irrelevant text must be added
  - Error propagation, an error in one character will impact all other characters in the block



# Symmetric ciphers

- The same key is used for encryption and decryption
- Sharing the key can be problematic



Leo Marks with letter One Time Pad written on silk. These were used during WWII by spies. Letters unraveled after use to prevent decryption of earlier messages if captured.



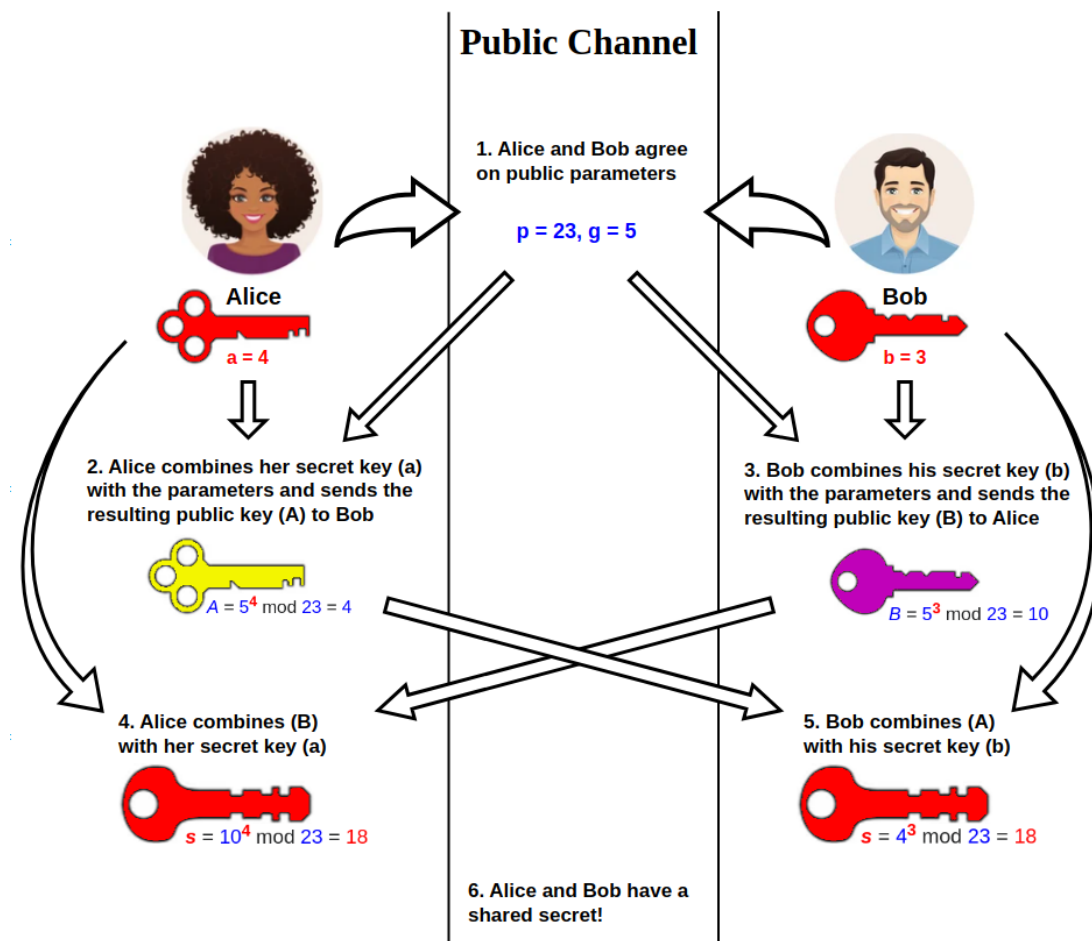
# Diffie-Hellman key exchange (Invented 1976... or maybe 1969)

- Allows two entities to agree on a secret key while communicating publicly.
- Protocol uses the multiplicative group of integers modulo  $p$  where  $p$  is prime and  $g$  is a primitive root modulo  $p$ .

## Primitive Root:

The number 3 is a primitive root modulo 7<sup>[5]</sup> because

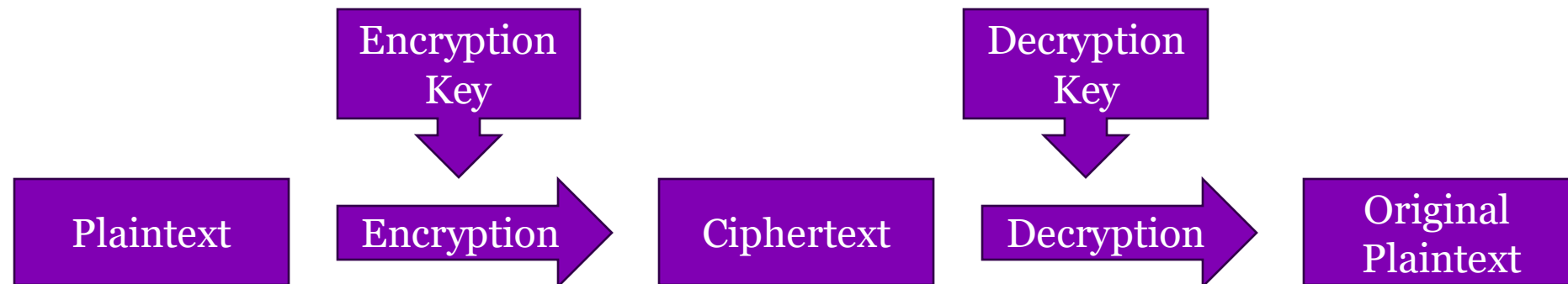
$$\begin{aligned}
 3^1 &= 3^0 \times 3 \equiv 1 \times 3 = 3 \equiv 3 \pmod{7} \\
 3^2 &= 3^1 \times 3 \equiv 3 \times 3 = 9 \equiv 2 \pmod{7} \\
 3^3 &= 3^2 \times 3 \equiv 2 \times 3 = 6 \equiv 6 \pmod{7} \\
 3^4 &= 3^3 \times 3 \equiv 6 \times 3 = 18 \equiv 4 \pmod{7} \\
 3^5 &= 3^4 \times 3 \equiv 4 \times 3 = 12 \equiv 5 \pmod{7} \\
 3^6 &= 3^5 \times 3 \equiv 5 \times 3 = 15 \equiv 1 \pmod{7}
 \end{aligned}$$



Epachamo via Wikimedia Commons

# Asymmetric ciphers

- Different keys are used to encrypt and decrypt
- Public/private key encryption is one of the more famous asymmetric ciphers



# Public/private key cryptography

- Generate two “keys” that are paired
- **Whatever one key encrypts only the other key can decrypt**



- Public keys are given out to everybody



- Private keys are kept private

- $k_{\text{PRIV}}$  can encrypt and  $k_{\text{PUB}}$  can decrypt

$$P = D(k_{\text{PUB}}, E(k_{\text{PRIV}}, P))$$

- $k_{\text{PUB}}$  can encrypt and  $k_{\text{PRIV}}$  can decrypt

$$P = D(k_{\text{PRIV}}, E(k_{\text{PUB}}, P))$$

## My public key



-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v2

```
mQENBFHMcGABCAC9WrYDO6K2L3VHy14eHN6suHLqMpJ+SO+IUTuLEVNuzIoXAUXH
KozHejfV/9XoG8j933ZtszXKCog3aMESeoEoz6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnqoCplgXcN2GJxFeHHUaf27COSobCJxPMeshU4ZHKke+g6DatmiEtBpVp41Ot
1zxdmMQkgb2H2xw28RYfykdDoueteIkOrFLrCy9ZF9KdMhA1eBH94Knw1QshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvHo
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUjodABEBAAgoIkthbWkgVmFuaWVhIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwELACkFALYKYvECGyMFCQlMAYAHcwkI
BwMCAQYVCAIJGsgEFgIDAQIEAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QAqew
GWh8K4gCdiYoxDqJwq3PHxmyhZmQeN/1a1KcOrIj12b+Q75/5t+EgXOHpRoP1xfG
lZ6zOEpf6A18iFXx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYg3so2VueQoeXcq3dbYp
5vstVxD+TKHq5CioT75P2bzYq/XLT5aIbNqHqDPcToDgBRH+FvqsRXr7yeaf
JaPnxXo+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQk7JuQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOARxAgVf48jiWvrxuJ8YfHWSohEScNOCYCp8q2oLjwwE26T
lpdtrwCqtB1LYW1pIFZhbmlYSA8a2FtaUB2YW5pZWUy9tPobkBgQTAQIALAlb
IwUJCWYBgAcLCQgHAWIBBhULAgKcQWAgMBAh4BAheABQJWCmMeAhkBAaoJEJN2
zGX38dl9JJAIAIWorxIYsrmKS6CbW8MgTxxTDOXA Ct1b7FoWoQZHskIUqhEcE+a
XBYibiA5uHaatLfyeXaD3qMEoZnQHoyMGEoGKuooWsbhfoQzHPgwzRLkDii75M
BibawwoKWoVB9e4AkMakXJcNf5BXeo6AHLRL2v15V205DikVnlCRXocKtu8b7LnkM
cLn7oLobr1de1uyKoNzbSnO/vpKDJPo/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUs9+/P8pz4JILMDSevjfT7zSRSL/YP3fOfZ6N4bc+KODwPM7u5Iyoeu9zh
pzibv3ge7VhH2xIWz8vYz/2xT1345tWRRMOJAhwEEwECAAyFALTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4l7PpD1weJDF3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUulrwezYiNebWNCRQHzQvRv/VJwjbTUX+Q3HsjkKlHbE7iCiQXXiTRkoEny
2nu dcjGI2vo3C3B2JCucEw6esF1x79PI/1Pv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBFH1YSJgnzwo2JkhhohcHdF9oZem1eMeiDeeVkh63893N8Swk5fBKdTj+SKZ/L
rQElBBlpMR9BmeY6bPvWRuyvKkonIMR8oG9iFABxjTpWBL8aGk6EeVK5EqYDgVkd
ZlarK84r+KU1KD5lfgOCN7nhwgy7VI me68caZHSRiPWZP1fVVMhydiRjv8WsoUs6
InfVU3nxH+ZYthPbYoT86leGSchBT5K/fbQvbjhrRTbTfwwjzSifb9efWylDi994
nzP6cNorir3GIpsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDSaHps2+1meFPooJFvNetz2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYzTSSo5x1RdXHqpEbgap8dtuHhVvJw9QYDQBjroK4aKyG9qqMD8cta
Pl/FAdyAqWH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MkP3YMfmu5ki5AQoEUcxy
AAEIALyXYy8G2ZaTDJpdGcRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLvcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTSXIUkAt3T1oGBtXmGvqbGBq8ljSGl1UTwdF
5yu5oJyRSf2fQRND6P/2eHNXejDUdtvhUXIU8h9MuUO/ipDoDnwIvMnAATJHA+R
Zqw6oNpyjRGzvr3iuWUw4PtyJDI3ELAFkbp/NAc5TtUvHRHNOwnpldJhMzJHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZf
2Tozd7h9MXtGJDlPKJ8eLG8ogcMAEQEAAYkBJQQYAQIADwUCUcxyAAIbDAUJCWYB
gAAKCRCTdsxl9/HZfS+hB/9BJqSmIgcOHFXnb1PVikxekzL8+WVm5Pk/EgMQSLZ2
HX4p3ial5PEPEYgUw9YnaG4ioodwJGw5/daTWrrTzcnKd8YqoP+DUOt96HZDSu3m
mCzE9NVAQYboFbVmGOxoeo627UBSvFqaXvAxBDYkoR8BoTnKhrQFwXkZVb3ohKwD
TgAFjOGlZiE6uAdST231tFaqobizYfe5AVXRqro2oxBqNbaJNqs3SWoD83iSyvdv
lIOBx83/Rogg7hUkI6F2vzXicWmUwFSXRggCSbLosHsP6isBWwvIHeRmna/aQab
YKG3gbV9iyzAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
```

=x5FK

-----END PGP PUBLIC KEY BLOCK-----

# SP-Networks (Substitution and Permutation Circuits)

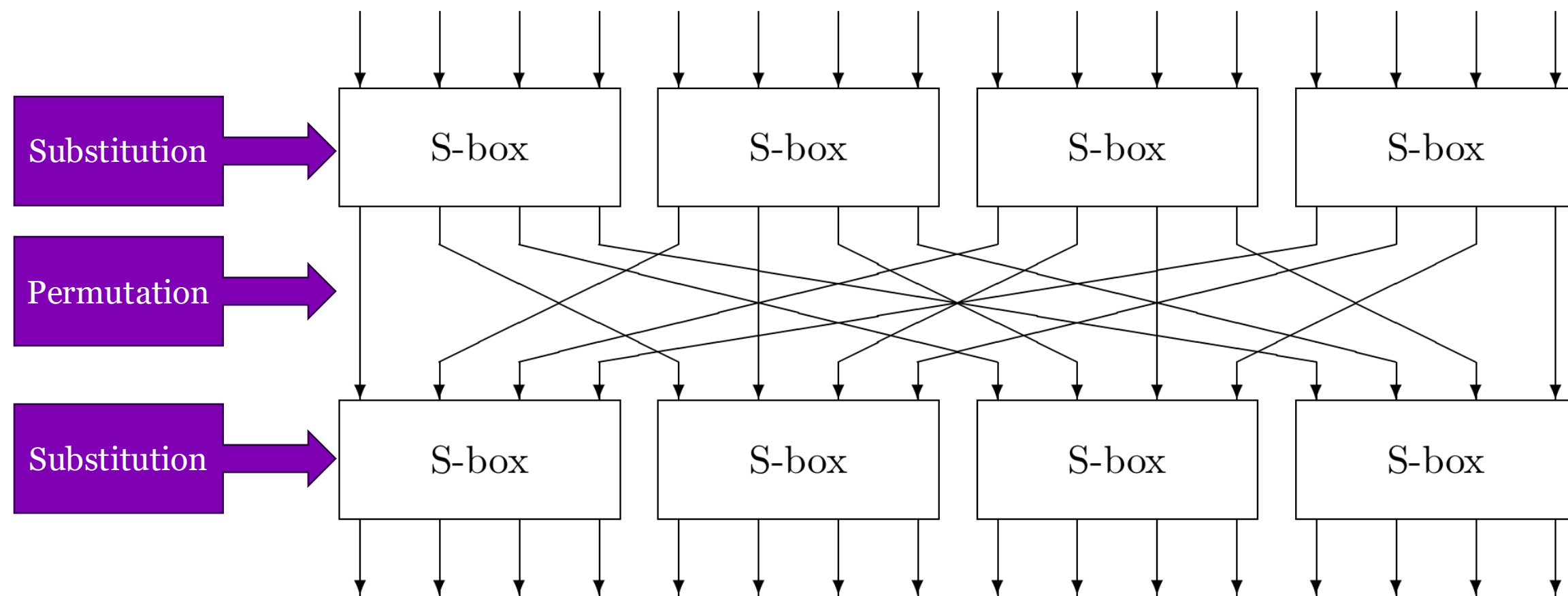
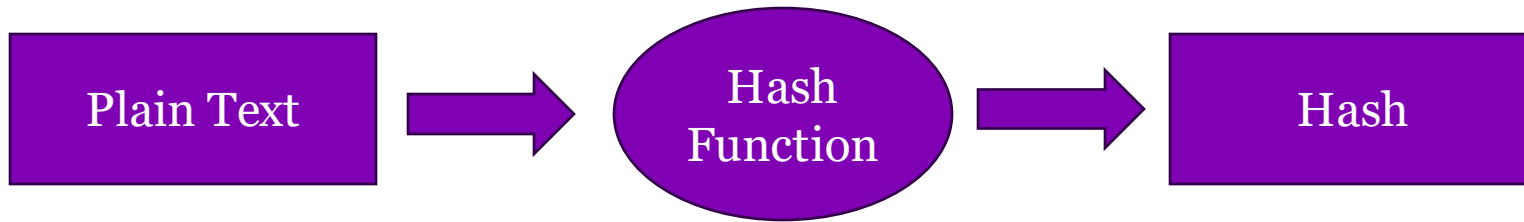


Figure 5.10: – a simple 16-bit SP-network block cipher

# Hashing

- A hash is a one way function. So the same plaintext will always produce the same hash. But the hash cannot be used to produce the plaintext.

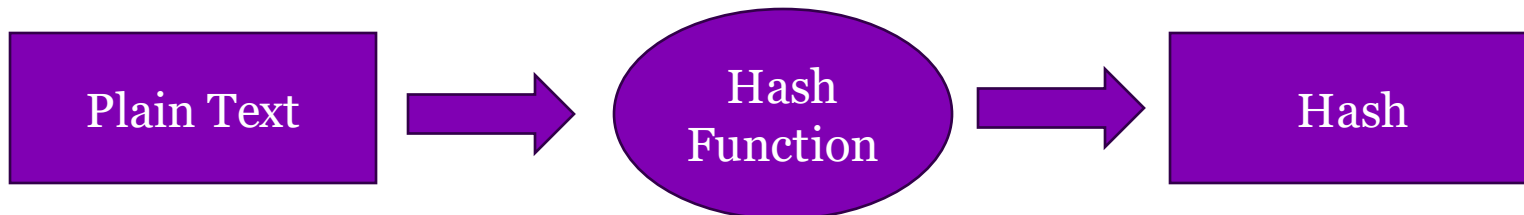


# Hashing passwords

A row from /etc/shadow

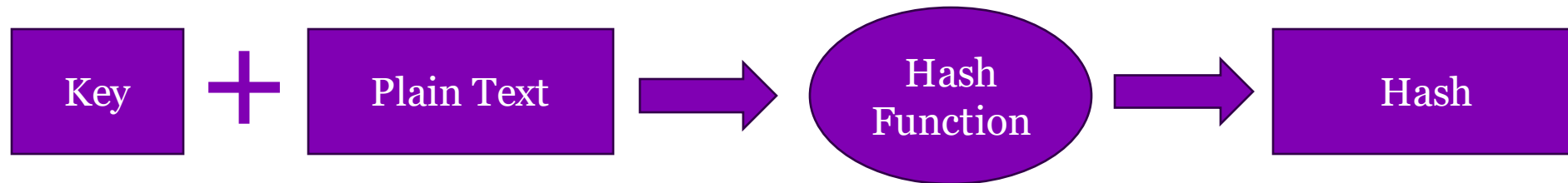
aychedee:\$6\$vb1tLY1qiY\$M.1ZCqKtJBxBtZm1gRi8Bbkn39KU0YJW1cuMFzTRANcNKFKR4RmAQV4k4rqQQCkaJT6wXqjUkFcA/qNxLyqW.U/:15405:0:99999:7:::

- There are two ways to protect a password on a server:
  - You can encrypt the password and keep the key in a *really really* safe place
  - You can hash the password. Hashing does not require a secret key so there is no secret key to lose
- A hash is a one way function. So the same password will always produce the same hash. But the hash cannot be used to produce the password.



# Hashing + key: Hash-based message authentication code (HMAC)

- A simple trick is to concatenate a key onto the plaintext.
- Only someone with the key could have produced that hash.





# AES and DES

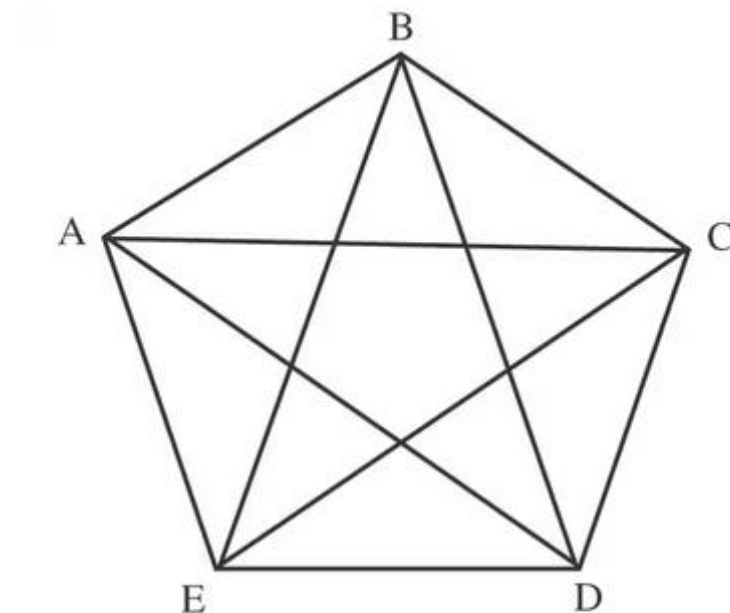
- Minimally covered
- You should understand what an SP-Network is and how it relates to both AES and DES
- You should also know why DES is not considered secure
- How AES fixed that issue

# **LINKING KEYS WITH IDENTITIES (OR PROPERTIES)**

**Approach scales poorly**

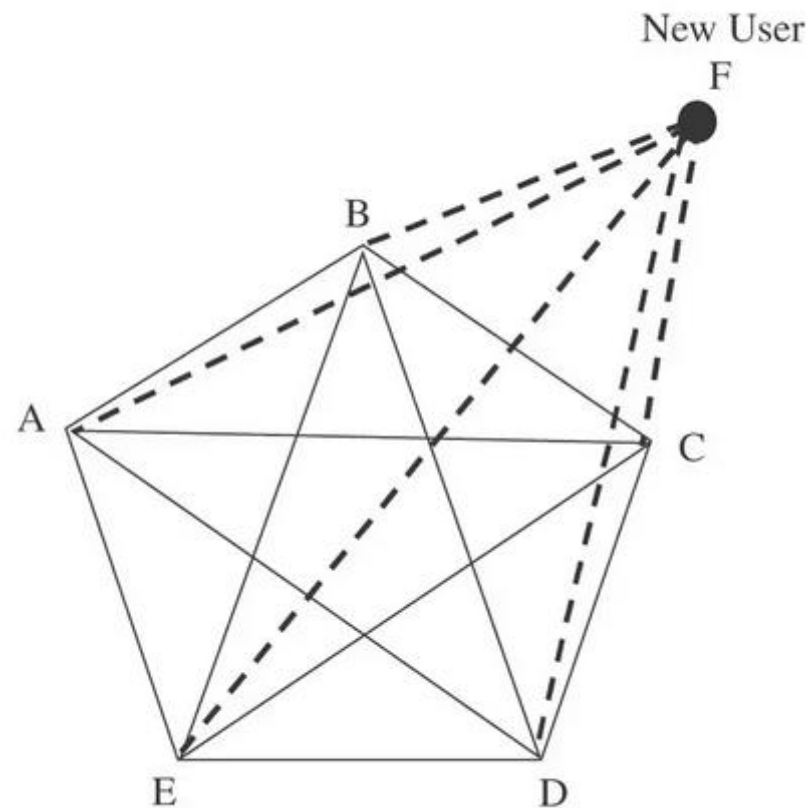
**An  $n$  user system requires  $n*(n-1)/2$  keys**

**Expecting people to verify that many keys, as well as store and not lose them is unreasonable**



Existing Users

New Keys to Be Added - - - - -



# Certificate Authorities

- A certificate authority verifies some properties of a person/organization and issues a “certificate” signed by their private key.
- Certificates can be quite detailed about what has been verified, and what they have been verified to do.

## Certificate Hierarchy

▸ QuoVadis Root CA 2

▸ QuoVadis EV SSL ICA G1

www.ease.ed.ac.uk

## Certificate Fields

Issuer

▸ Validity

Not Before

Not After

Subject

▸ Subject Public Key Info

Subject Public Key Algorithm

Subject's Public Key

## Field Value

Modulus (2048 bits):

```
9d 6b 8a 90 ff 2a c7 ad 11 f0 5f 95 ff 34 f5 c1
fa 9b d6 38 9c d6 90 49 8f b5 2c 9c 8b 51 ec 74
9b 69 17 ed b7 25 8c c0 8c ac 90 28 55 97 00 0b
d2 e4 88 c5 4b 03 ae 3d 73 d6 92 ac 25 06 99 39
b1 13 c8 2a 56 9d 6d 89 47 b0 eb 8b e8 c8 17 25
fd 60 1c b6 f5 62 fb 5f 82 33 cb a5 5d 0f 24 92
25 04 c2 16 4a 35 66 a6 66 b3 c5 75 ff 5e cb 94
31 c6 e6 a5 aa f4 3a 40 72 42 e4 93 43 b2 a6 0e
```

Export...

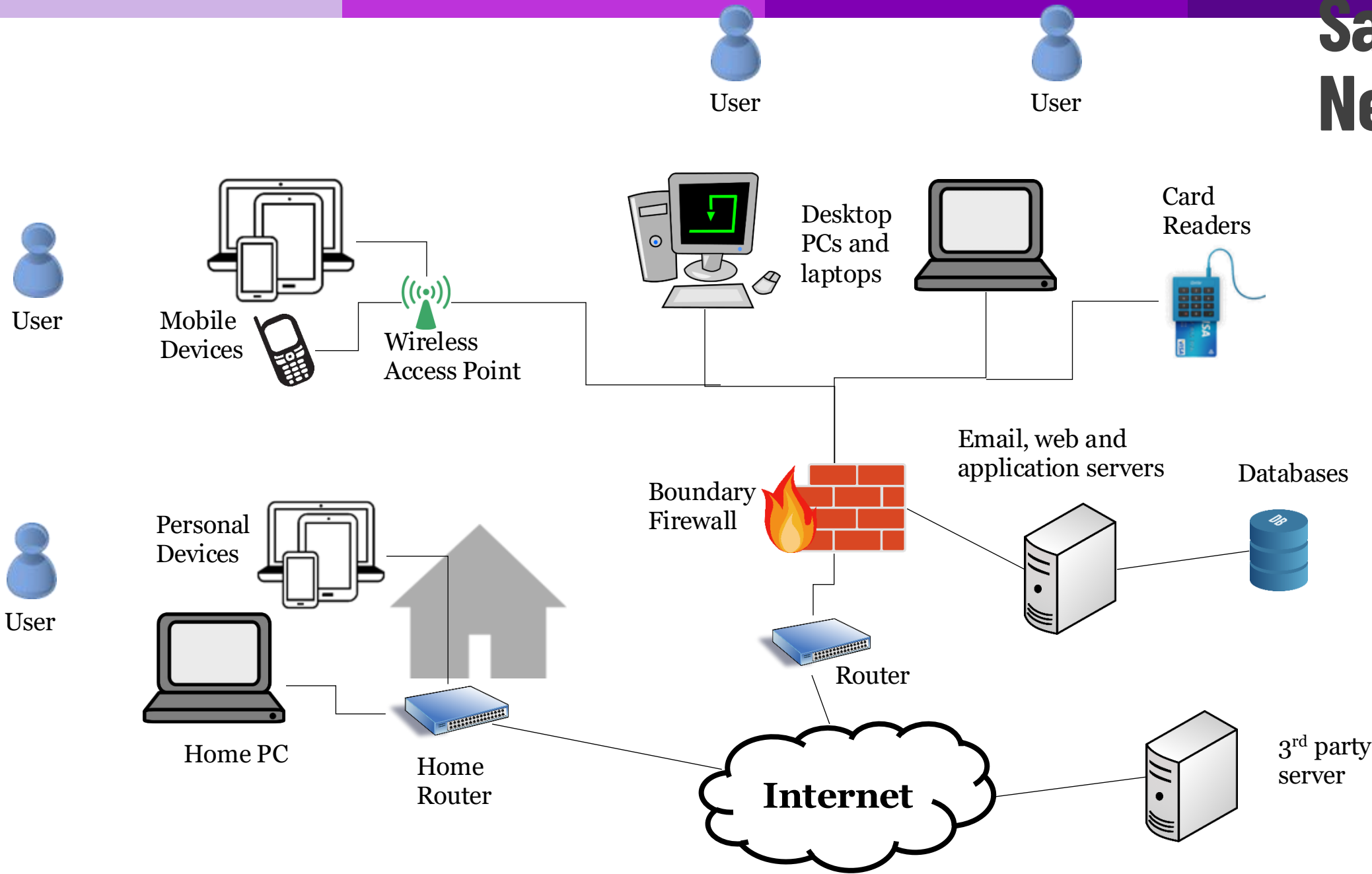
# Steganography

- Hiding information in plain sight
- Used to hide that a message is even being sent
- Or used to hide the real message in a less problematic message



# NETWORKING

# Sample Network



# Types of threats

- **Interception** – Unauthorized viewing of information (Confidentiality)
  - **Inference/Privacy** – Unauthorized deduction of information based on traffic (Confidentiality)
- **Modification** – Unauthorized changing of information (Integrity)
- **Fabrication** – Unauthorized creation of information (Integrity)
- **Interruption** – Preventing authorized access (Availability)

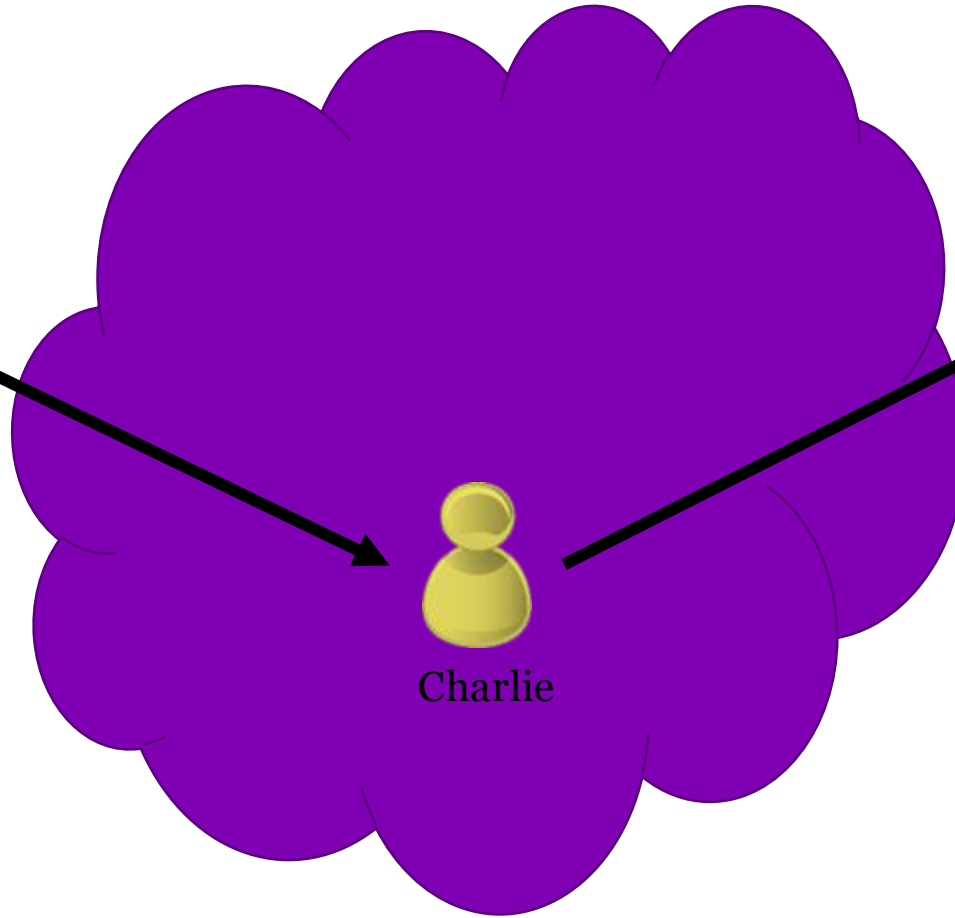


Alice's  
Computer



Alice

The Internet



Bob's Server

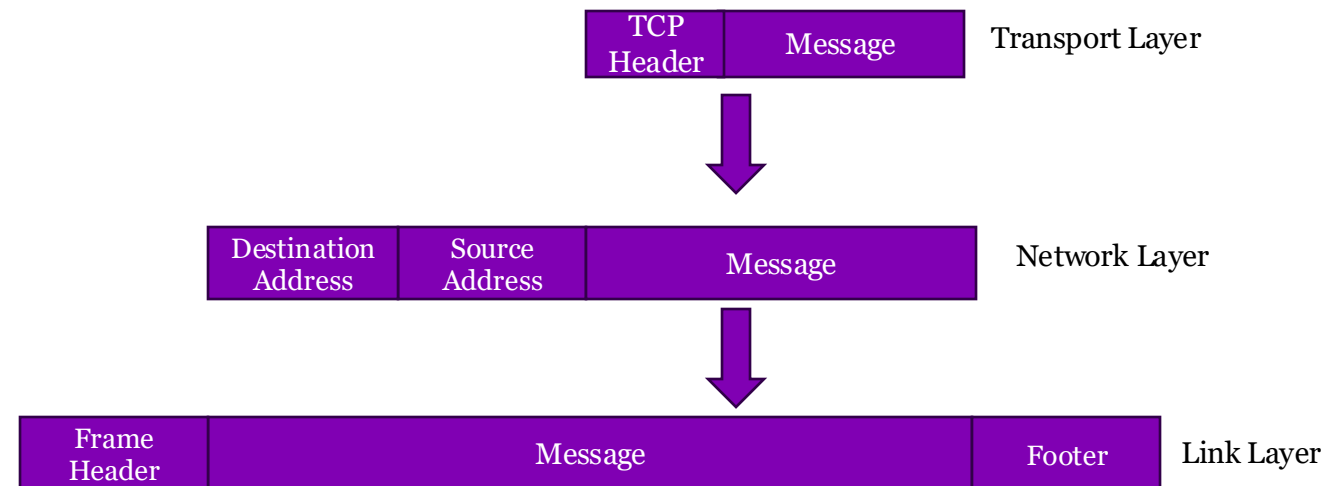


Bob

**Man in the Middle Attack**

# Packet

- Smallest individually addressable data unit transmitted.
- A packet is a simple concept: it has a destination address, source address and message.
- Usually created in layers by different parts of the software stack.

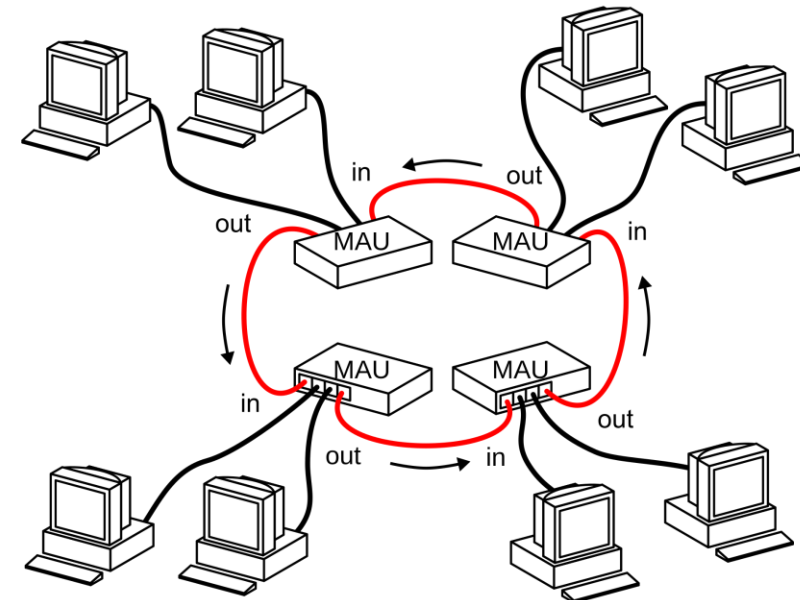


# MAC address

- Medium Access Control (MAC) address
- Assigned at time of manufacture (mostly)
- Six groups of 2 hexadecimal digits
- Used to identify unique devices on a local network



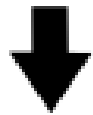
By © Raimond Spekking / CC BY-SA 4.0 (via Wikimedia Commons), CC BY-SA 4.0



By Andrew28913 on Wikipedia

An IPv4 address (dotted-decimal notation)

**172 . 16 . 254 . 1**



10101100 . 00010000 . 11111110 . 00000001



One byte=Eight bits




Thirty-two bits (4 x 8), or 4 bytes

# OSI Network Model

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<!-- DOCTYPE Needs to be the very first thing on the page, or IE 6 goes
into quirks mode, rather than standards mode -->
<!-- DOCUMENT STARTS -->
<!-- START: ssi/doctype.inc -->
<html>
<head>
<!-- END: ssi/doctype.inc -->
<!-- TITLE HERE -->
<!-- START: ssi/bin/metadata -->
<!-- Metadata information automatically generated -->
<!-- META NAME="DC:Title" CONTENT="Computer Security Course - University of Ed
<!-- META NAME="DC:Creator" CONTENT="Neil Brown" -->
<!-- META NAME="DC:Creator.Address" CONTENT="neilb@inf.ed.ac.uk" -->
```

**Sender:**  
**Apache**

7	 <b>Application</b> Network process to application
6	<b>Presentation</b> Data representation and encryption
5	<b>Session</b> Interhost communication
4	<b>Transport</b> End-to-end connection and reliability
3	<b>Network</b> Path determination and IP (Logical Addressing)
2	<b>Data Link</b> MAC and LLC (Physical Addressing)
1	<b>Physical</b> Media, signal, and binary transmission


Data starts at the top of the OSI stack at level 7.

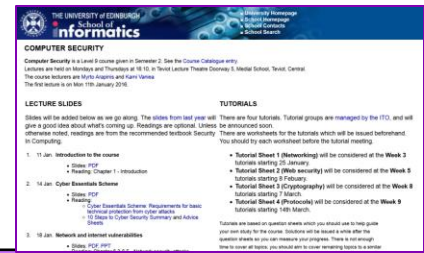
It progresses down the stack with each successive level adding or changing information.

At level 1 it travels across the physical layer to the recipient computer.

The recipient then processes the data up the stack. At level 7 an application processes the data.

**Recipient:**  
**Firefox user**

7	 <b>Application</b> Network process to application
6	<b>Presentation</b> Data representation and encryption
5	<b>Session</b> Interhost communication
4	<b>Transport</b> End-to-end connection and reliability
3	<b>Network</b> Path determination and IP (Logical Addressing)
2	<b>Data Link</b> MAC and LLC (Physical Addressing)
1	<b>Physical</b> Media, signal, and binary transmission



- IP addresses
- MAC addresses
- Transmission Control Protocol (TCP)
- Ports
- Autonomous Systems (AS)
- Border Gateway Protocol (BGP)
- VPN
- Onion Routing
- Firewalls
- DNS
- Denial of Service Attacks
- Distributed Denial of Service Attacks

# What is a URL?

- Uniform Resource Locators (URLs) are a standardized format for describing the location and access method of resources via the internet.

`<scheme>://<user>:<password>@<host>:<port>/<url-path>?<query-string>`

`<subdomain>.<domain>.<topdomain>`

eg. `https://profile.facebook.com`

# SECURE PROGRAMMING



# Errors vs Flaws

## Errors

- Unintentional
- Mistakes
- Typos
- Possible to find through testing
- If you were to compare a system diagram or specification to the code, there should be a discrepancy
- Can only be detected after programming

## Flaws

- Code intentionally written that way, security side-effects likely unintentional
- Code follows intended design
- Hard to impossible to find from testing, if test and code are both based on the same system design plan
- Can be detected at the project planning phase

# Buffer Overflow

- More data is written into a buffer than the buffer has allocated memory
- As a result, the memory allocated next to the buffer gets overwritten
- For example, initiate a character array (A) and an unsigned short integer (B). Then copy a string into A that has a length  $> A$ . Result B is overwritten.

```
char          A[8] = "";  
unsigned short B = 1979;
```

	← A →								← B →	
Value	null								1979	
Hex	0	0	0	0	0	0	0	0	07	BB

```
strcpy(A, "excessive");
```

Value	e	x	c	e	s	s	i	v	25856	
Hex	65	78	63	65	73	73	69	76	65	00

# Incomplete Mediation

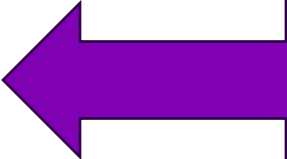
- Buffer overflows are an example of “incomplete mediation”
- Mediation – checking
- Incomplete mediation – failing to check the authorization and properties of a subject/object before using it

**Client sends:**

`https://exampleShop.com?price=4.99&user=4837&login=true`

**Server:**

```
function f(price, user, login)
    if (login == true)
        chargeUser(price, user)
```

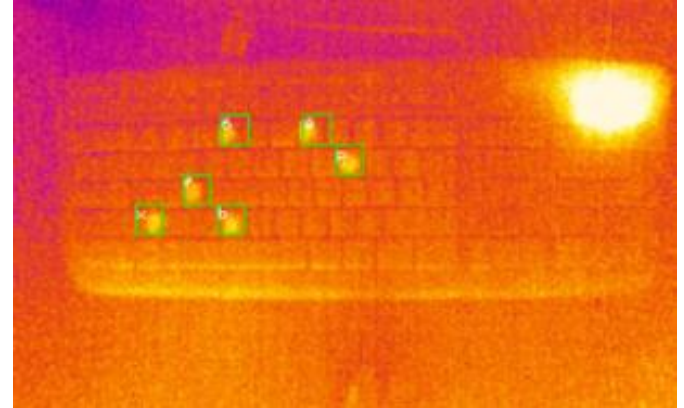


No server-side check if user is logged in. No server-side check if price is appropriate.

# Examples of Side Channels

Side Channels are an exercise in creativity:

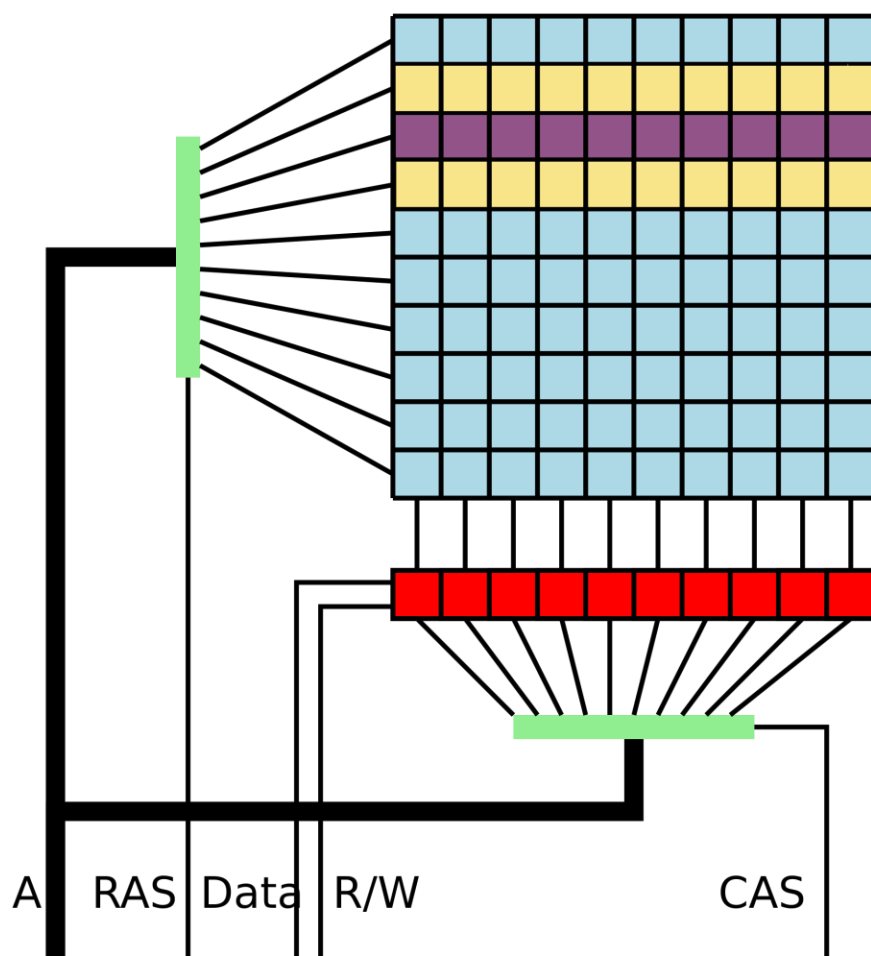
- ✦ Timing
  - ✦ A command doing 'more' will take longer
  - ✦ E.g., Square and multiply problem
- ✦ Temperature
  - ✦ Relies on the processor heating up when it's working hard
- ✦ Radio waves
  - ✦ More power being transmitted over a wire will emit more RF
- ✦ Power
  - ✦ A command doing 'more' will consume more power
- ✦ Many more...



Side channels allow us to acquire information about a target in unexpected ways

E.g., A thermal image of the keyboard for a user who has just logged in...

# RowHammer (2014)



- Repeated activation of rows can cause bits in neighboring rows to change
- Happens because DRAM is becoming more compact and with lower noise margins
- A low-access process could in theory overwrite bits in a high-access process

hammer:

```
mov (X), %eax // read from address X
mov (Y), %ebx // read from address Y
clflush (X)    // flush cache for address X
clflush (Y)    // flush cache for address Y
jmp hammer
```

A snippet of [x86 assembly](#) code that induces the row hammer effect (memory addresses `X` and `Y` must map to different DRAM rows in the same [memory bank](#))<sup>[1]:3[4][18]:13–15</sup>

## Spectre (2017/2018)

- Timing attack using speculative execution in the CPU
- “[induces] a victim to speculatively perform operations that would not occur during strictly serialized in-order processing of the program’s instructions, and which leak victim’s confidential information via a covert channel to the adversary.”

## Meltdown (2017/2018)

- Race condition attack between memory access and privilege level check
  1. Attacker chooses a memory location inaccessible to them and gets it loaded into a register
  2. A transient instruction access a cache line based on that register
  3. Attacker uses Flush+Reload (timing) to determine the accessed cache line

# WEB SECURITY

# Cute Dogs!



Cute dog sleeping  
on a park bench.



Playing with a ball all  
day is hard work. But  
that is no reason to  
release the ball.

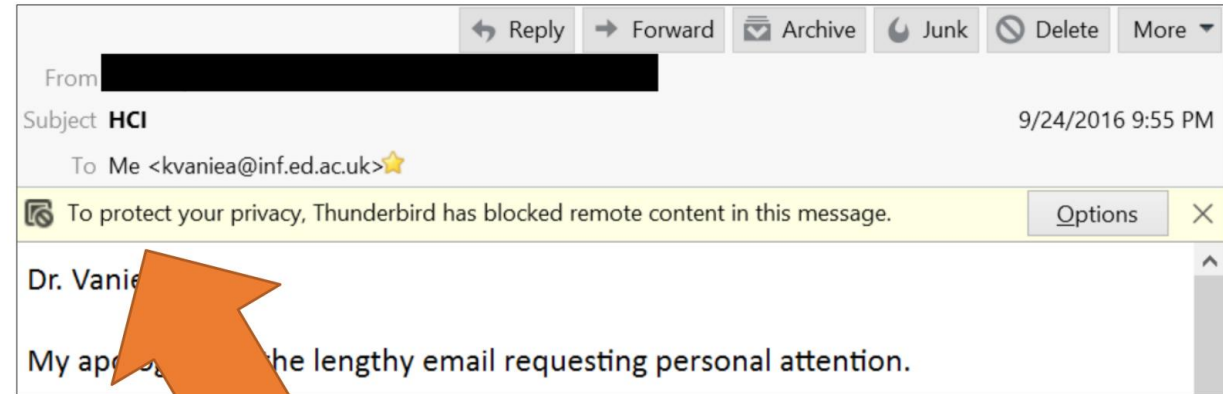


Loaded:

- index.html from cutedog.com
- dog.jpg from instagram.com
- sad\_dog.jpg from instagram.com
- style.css from cutedog.com
- tracker.js from beacon.krxd.net
- invisible.jpg from doubleclick.com
- connect.js from connect.facebook.net
- logo.jpg from connect.facebook.net



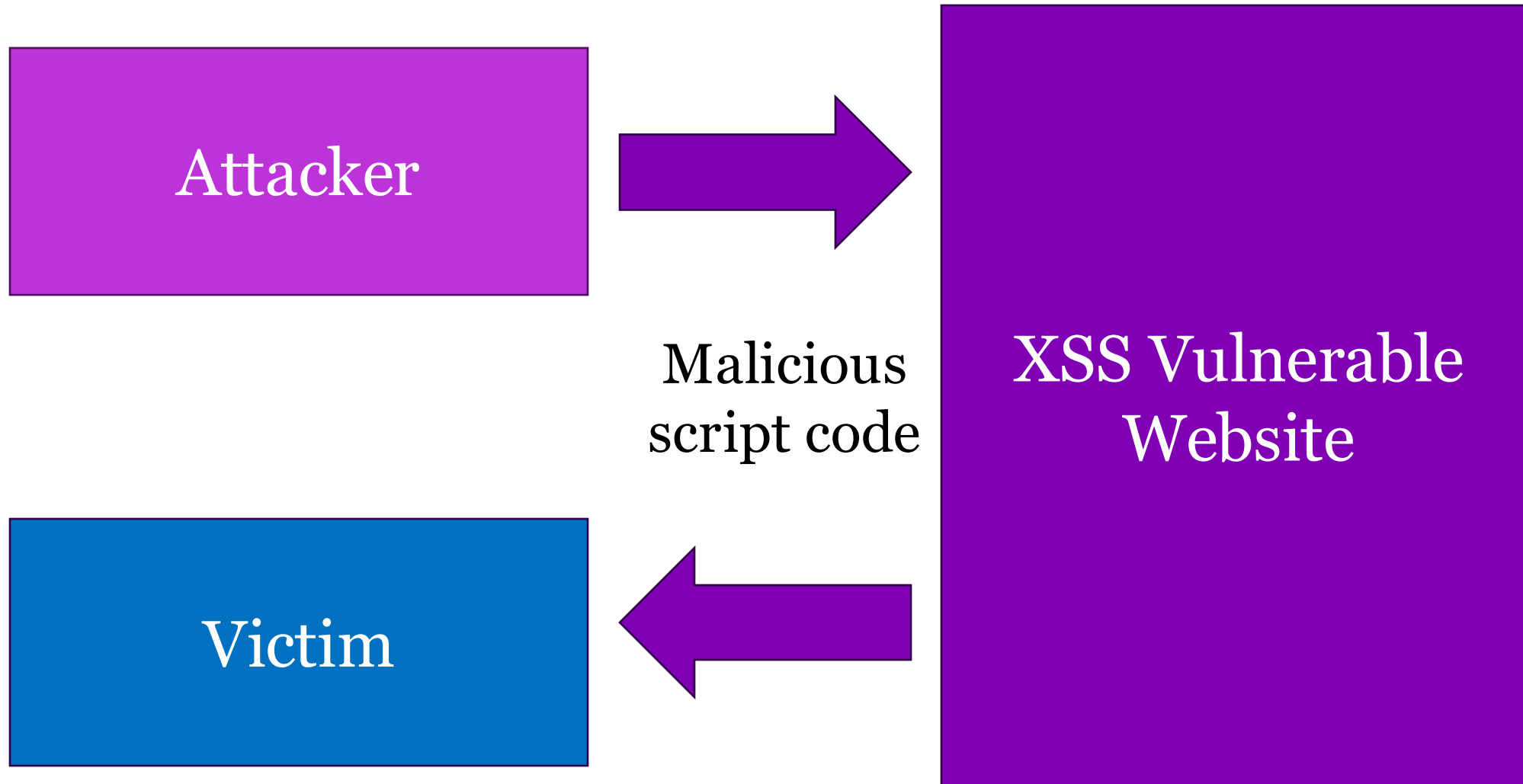
Emails are similar to mini web pages, they load content the same way.



```
iv><div><br></div><div>Regards,</div><div>Chris</div></div><img src=3D"http=
://t.sidekickopen65.com/e1t/o/5/f18dQhb0S7ks8dDMPbW2n0x6l2B9gXrN7sKj6v4LGzz=
VQZptn64JsbFW3Lyy-Y2z1ZNzW40Hqy21k1H6H0?si=3D6208290593964032&pi=3D2ee4=
f8a0-67ac-43f0-cbe4-30cede291a88" style=3D"display:none!important" height=
=3D"1" width=3D"1"></div>
```

The above code loads an invisible image (display:none) of size 1 pixel. Doing so causes your email client to ask for the image from the server, letting them know that you opened the email.

# Classic Persistent XSS Attack



# Guestbook persistent XSS example

```
<html>

<title>My Guestbook!</title>

<body>

  You comments are greatly appreciated! <br/>

  Here is what everyone said: <br/>

  Sam: Hello
  <script>alert("XSS injection!")</script>

  Joe: Hi! <br/>

  John: Hello how are you? <br/>

  Jane: How does the guestbook work?<br/>

</body>

</html>
```

## Sign my Guestbook!

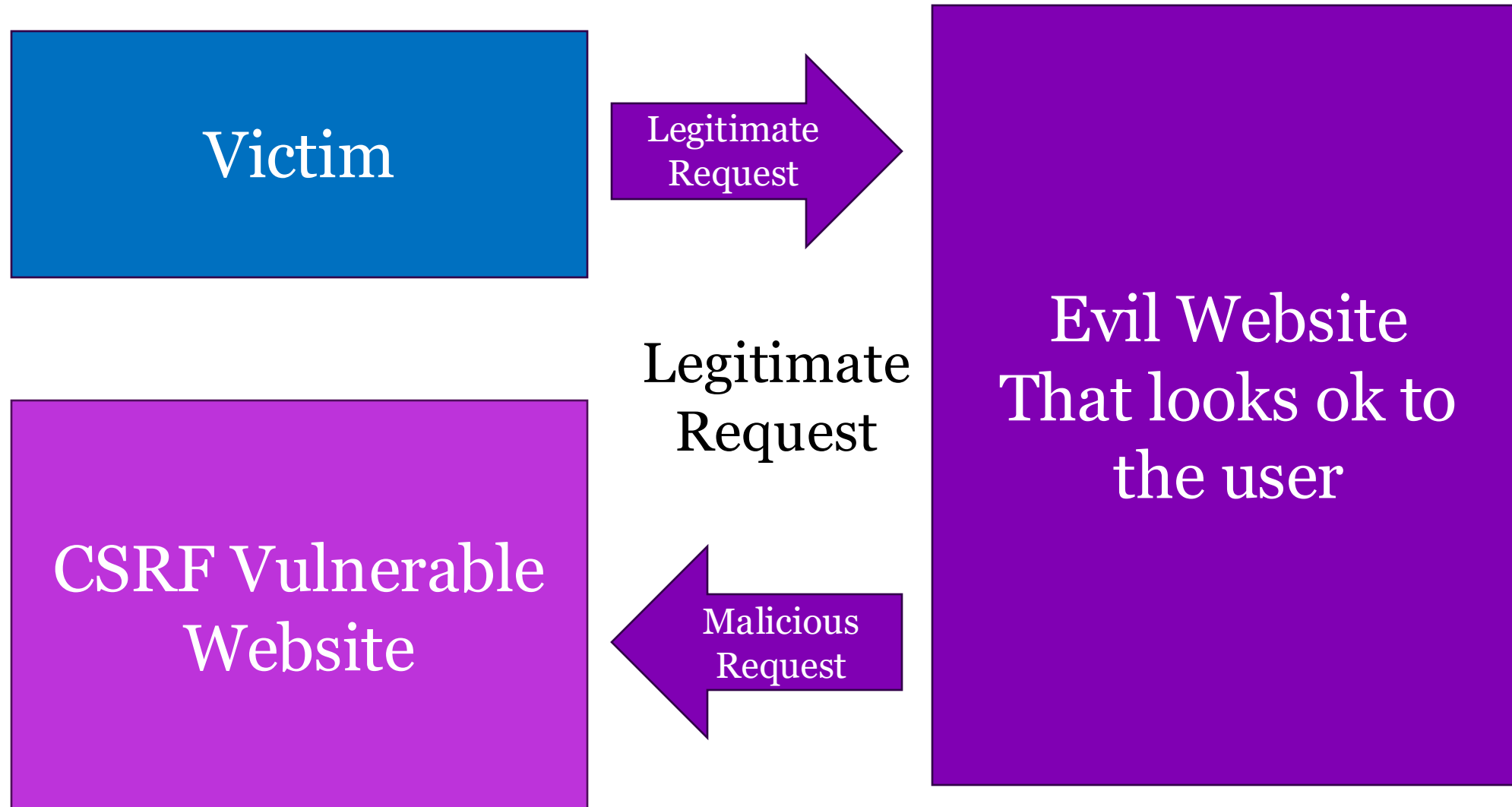
Here is what everyone said:

Sam: Hello

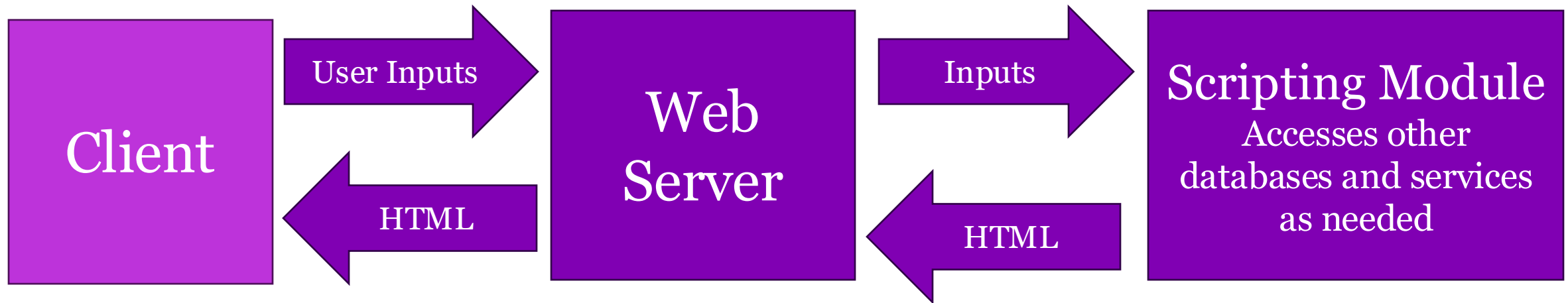
Joe: Hi! John: Hello how are you?

Jane: How does the guestbook work?

# Classic CSRF Attack

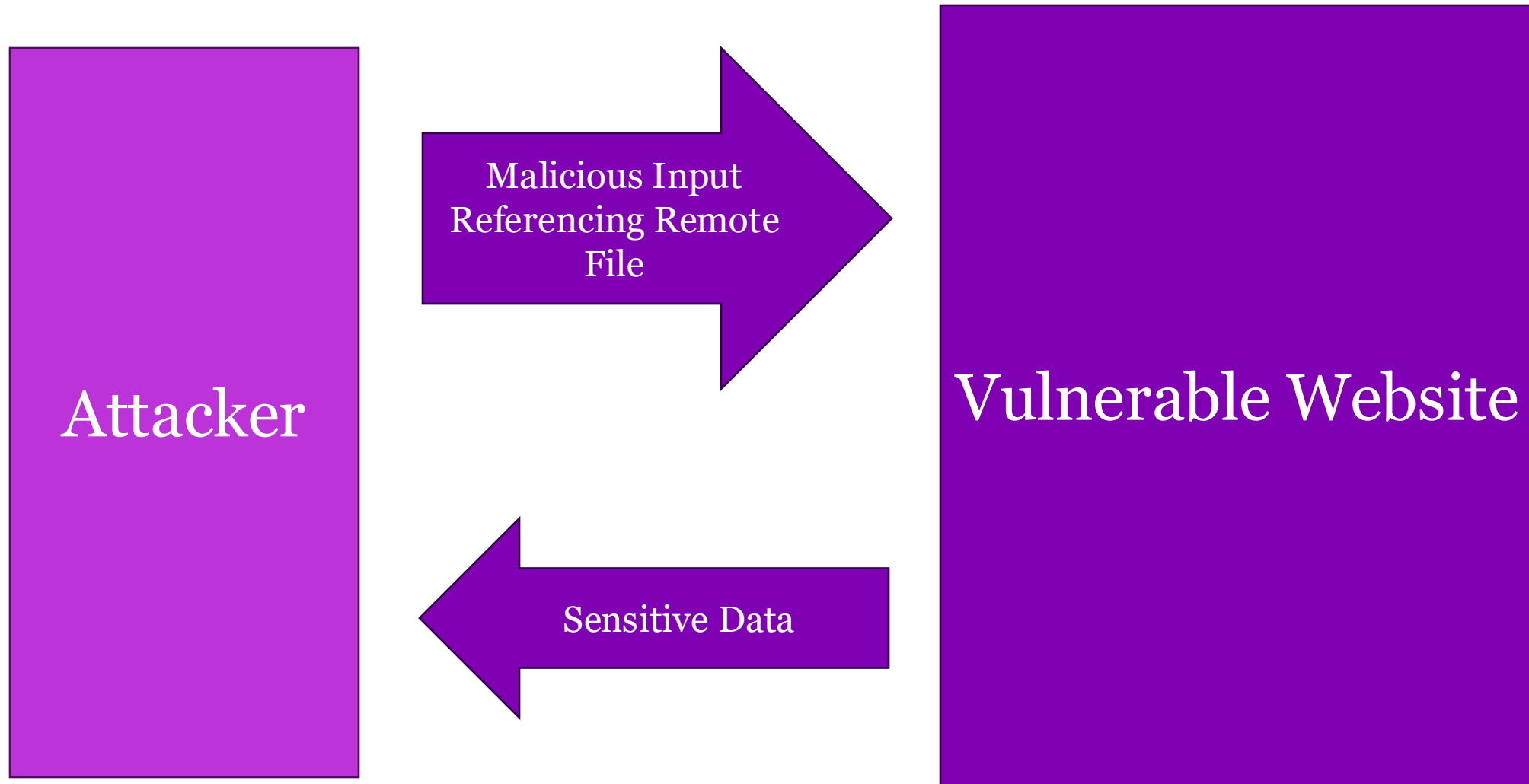


# Server-Side Scripting: Server Code

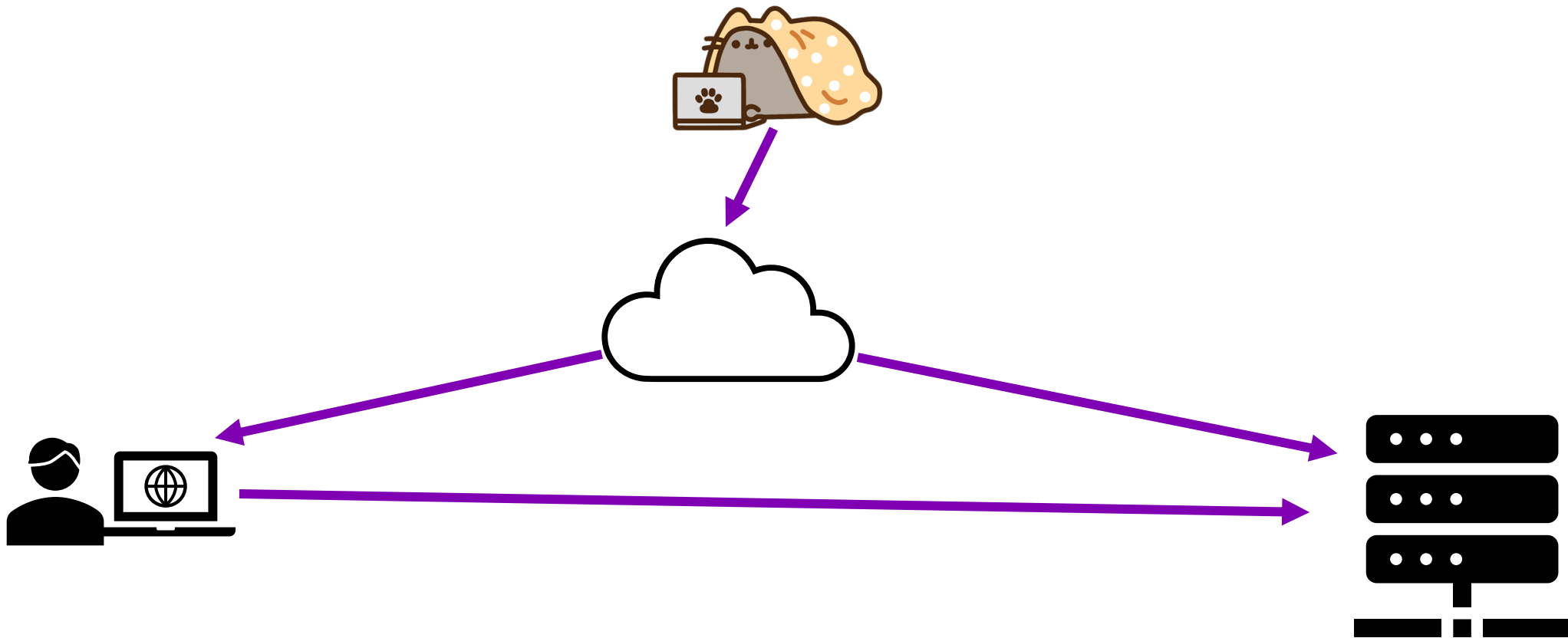


```
<html>
<body>
  <p>Your number was <?php echo $x=$_GET['number'];?>.</p>
  <p>The square of your number is <?php $y=$x*$x; echo $y; ?>.</p>
</body>
</html>
```

# Remote File Inclusion



# Session Hijacking



# SQL Injection is adding attacker code to the SQL query string

- SQL queries can be (incorrectly) built from GET data:
  - `https://insecure-website.com/login?username=administrator"--`
  - Select \* from user-logins where username="<?=\$\_GET['username'] ?>" AND password="<?=\$\_GET['password'] ?>"
  - Select \* from user-logins where username="administrator"-- AND password="123"

ID	Username	Password	Active
1	yuanyuan	97a37374	True
2	monkey	b2db	True
3	catch22	4010a414	True
4	mouse	f17eedeff4d0	False

-- is the comment command in SQL



# PRIVACY

# Federal Trade Commission (FTC)

- Unfair practices
  - Injure consumer
  - Violate established policy
  - Unethical
- Deceptive practices
  - Mislead consumer
  - Differ from reasonable consumer expectations

# Office of the Privacy Commissioner of Canada

- Oversees compliance with:
  - Privacy Act - how federal government handles personal data
  - Personal Information Protection and Electronic Documents Act (PIPEDA) - private sector privacy law
- Activities like:
- Investigation of complaints
  - Auditing
  - Public awareness
  - Advise parliament



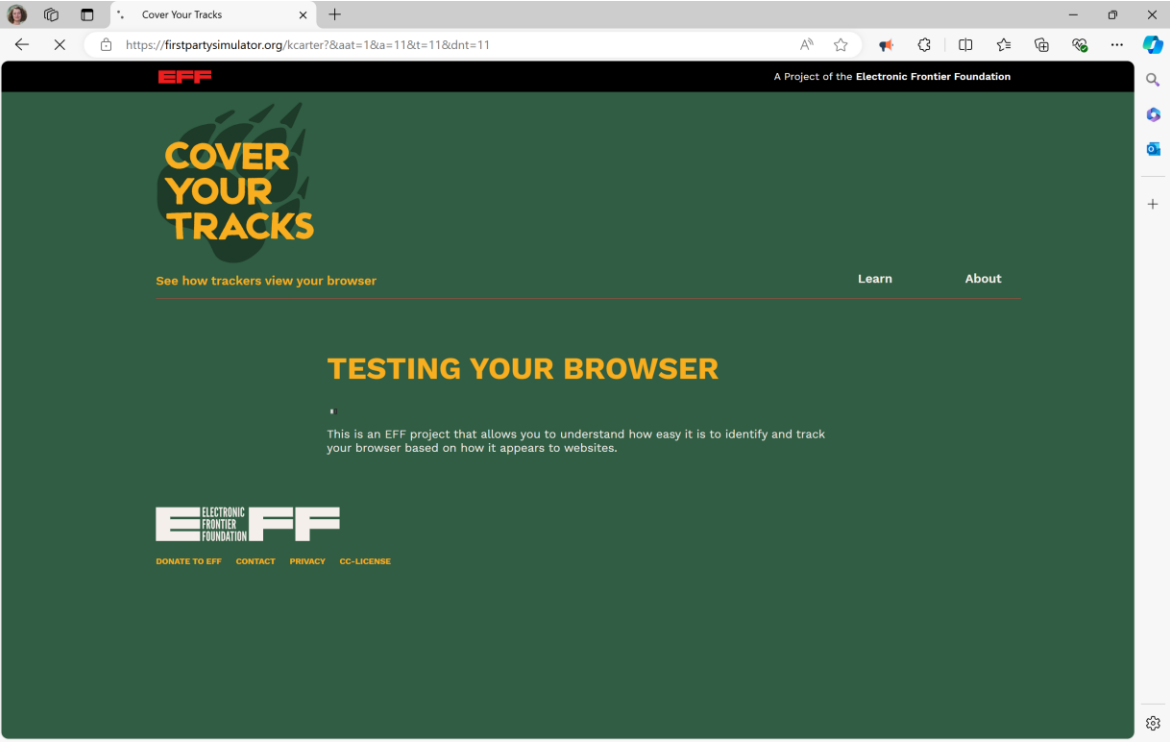
# GDPR Principles

- **Lawfulness, fairness and transparency** – there needs to be a lawful basis for processing and the data subject as the right to know how their data will be used.
- **Purpose limitation** - data must be collected with the purpose and only used for it or compatible purposes.
- **Data minimization** – personal data should be adequate, relevant, and limited to what is necessary.
- **Accuracy** – personal data should be kept updated and incorrect data must be deleted.
- **Storage limitation** – only keep personal data as long as you need it
- **Integrity and confidentiality** (security) – appropriate security measures should be taken. Follow “integrity and confidentiality”.
- **Accountability** – take responsibility and keep records showing compliance.

# Privacy topics

- FTC
- GDPR
- Notice and Choice
  - Privacy policies and consent
- How developers define and learn about privacy
- Designing backends for privacy (Little blue book)

# Browser Fingerprinting: <https://coveryourtracks.eff.org/> Visited via Edge on a Windows Surface



Our tests indicate that you are not protected against tracking on the Web.

IS YOUR BROWSER:

Blocking tracking ads?	<u>No</u>
Blocking invisible trackers?	<u>No</u>
Protecting you from <u>fingerprinting</u> ?	Your browser has a unique fingerprint

Still wondering how fingerprinting works?

LEARN MORE

*Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.*

## Your Results

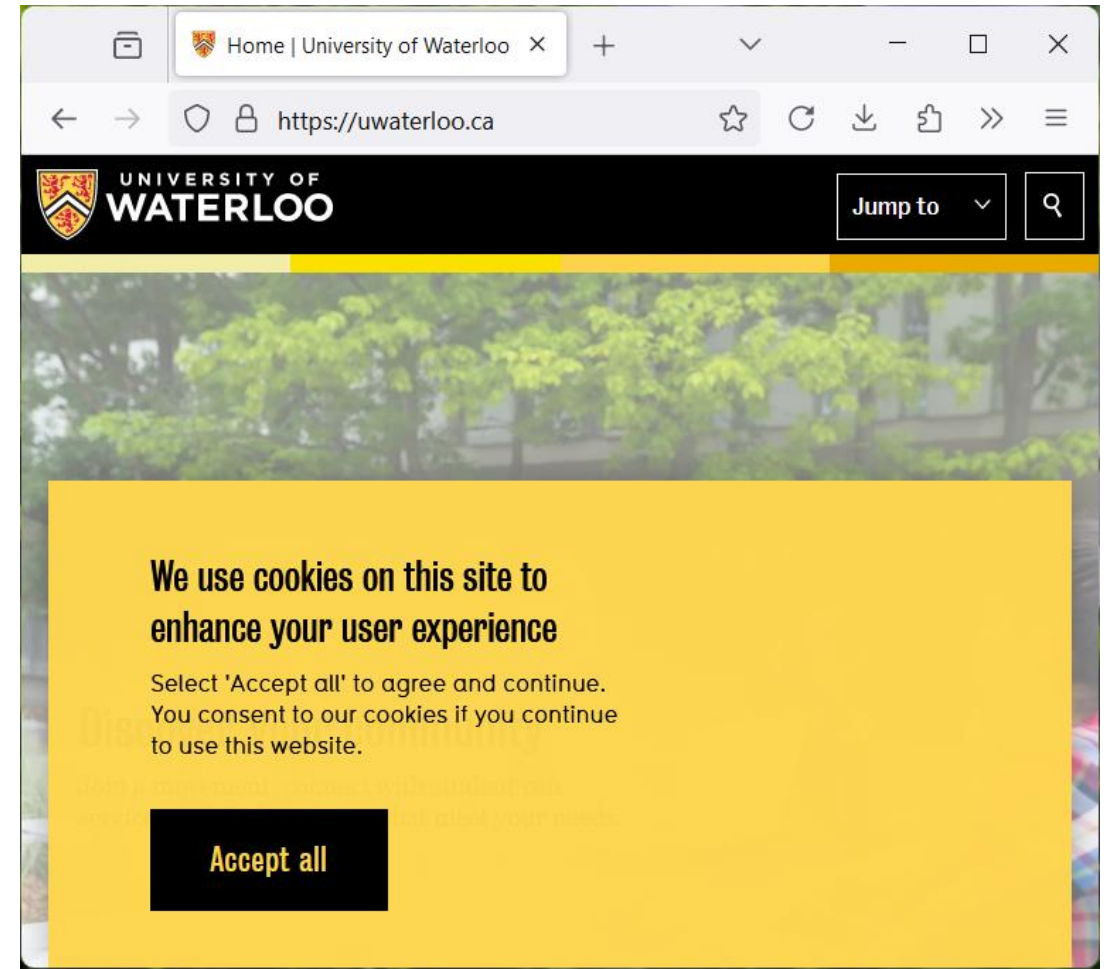
Your browser fingerprint **appears to be unique** among the 169,763 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.37 bits of identifying information.**

# NOTICE AND CHOICE

# Notice and Choice: the idea

- Users have the right to know how their data will be used, that information should be available
- Once users are aware, they can make good choices
- Interacting with a site or service is a choice
- Market pressures will force companies to provide good choices that customers demand

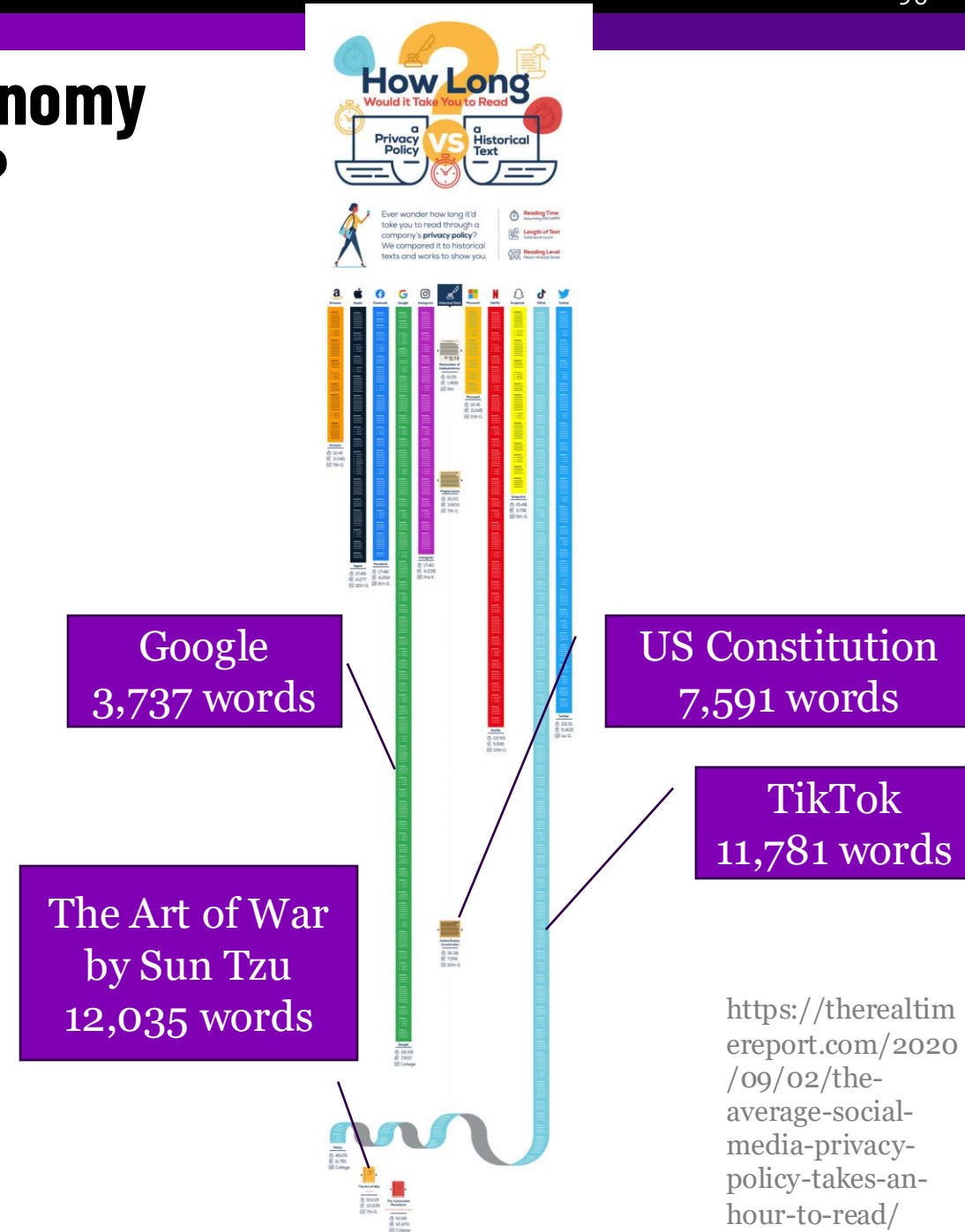


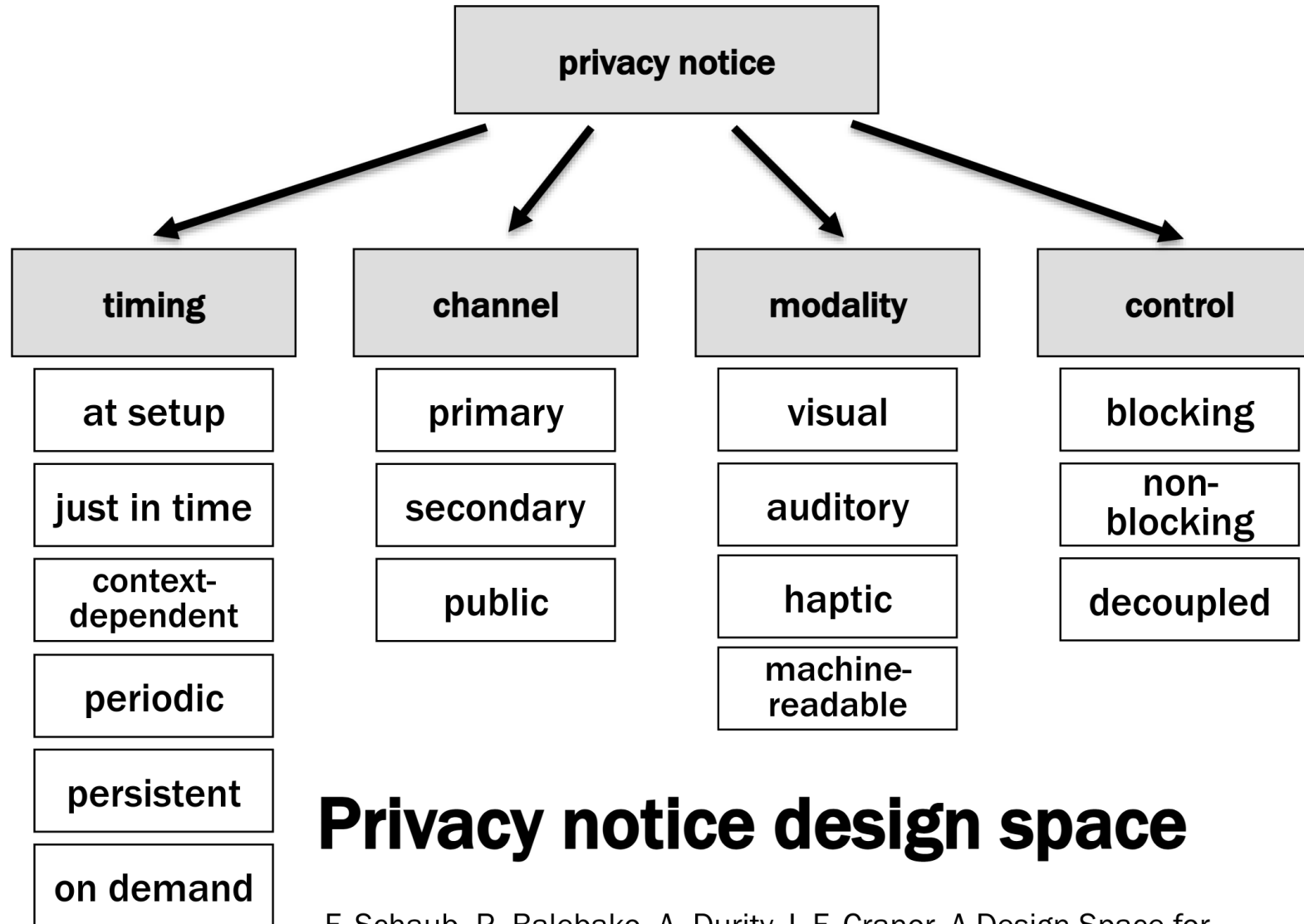


# How much money would it cost the US economy if everyone read through privacy policies?

- Notice and choice is dependent on awareness of content of privacy policies
- People do not read all the privacy policies, but if they did, how much would it cost the US economy?
- This information is important for policy makers and regulatory bodies (i.e. OPC)

Aleecia McDonald and Lorrie Faith Cranor. The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society, 2008.





## Privacy notice design space

F. Schaub, R. Balebako, A. Durity, L.F. Cranor, A Design Space for Effective Privacy Notices, SOUPS'15

# QUESTIONS