Computer and Network Security

Lecture 26: End-to-End Encryption & Usability

COMP-5370/6370
Fall 2025

End-to-End Encryption

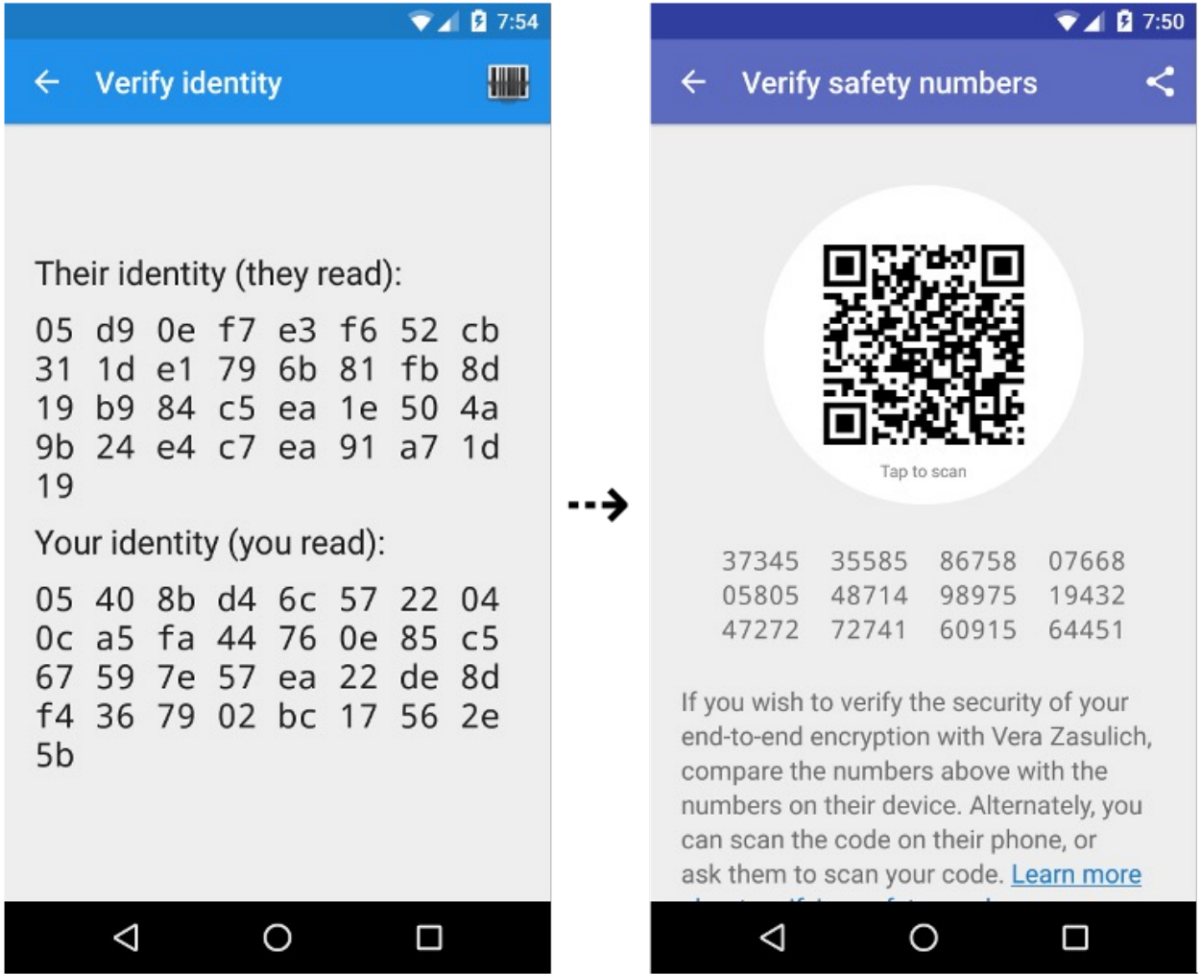
End-to-End Encryption (E2E/E2EE) is a design approach which ensures that the only 1P actors are the end-users.

End-to-End Encryption

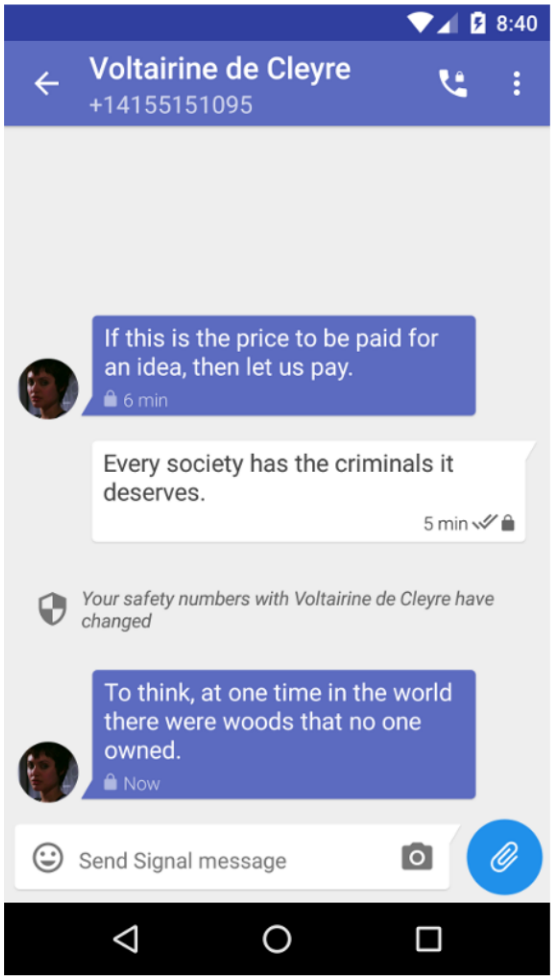
End-to-End Encryption (E2E/E2EE) is a design approach which ensures that the only 1P actors are the end-users.

- Intentionally prevents server-side access
- Separates “key distribution” (handled by service) from “key verification” (handled by users)
- Explicitly treats service as a potential attacker when passing messages

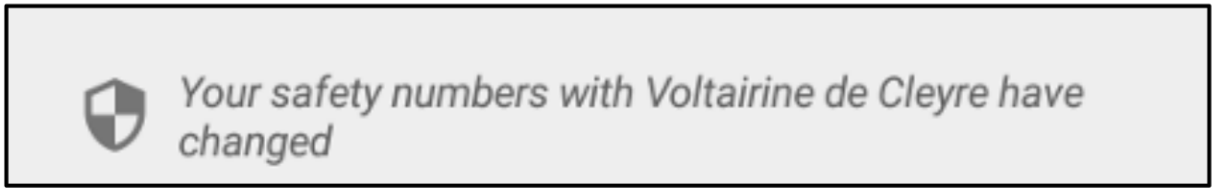
Leverage Existing Knowledge



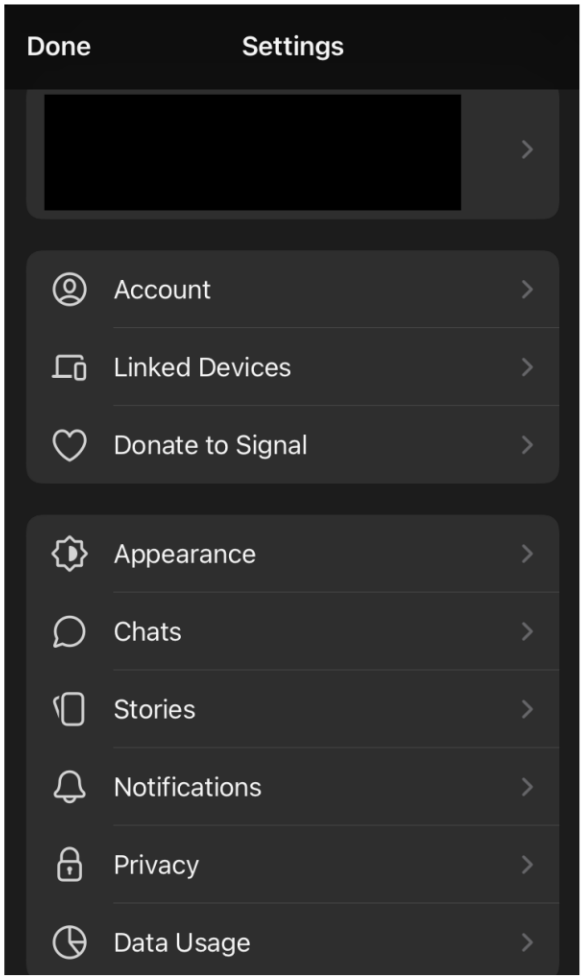
Treat the "Safe-Case" as the Common-Case



- In many scenarios, Trust-on-First-Use is perfectly acceptable
- Only alert when a user changes keys

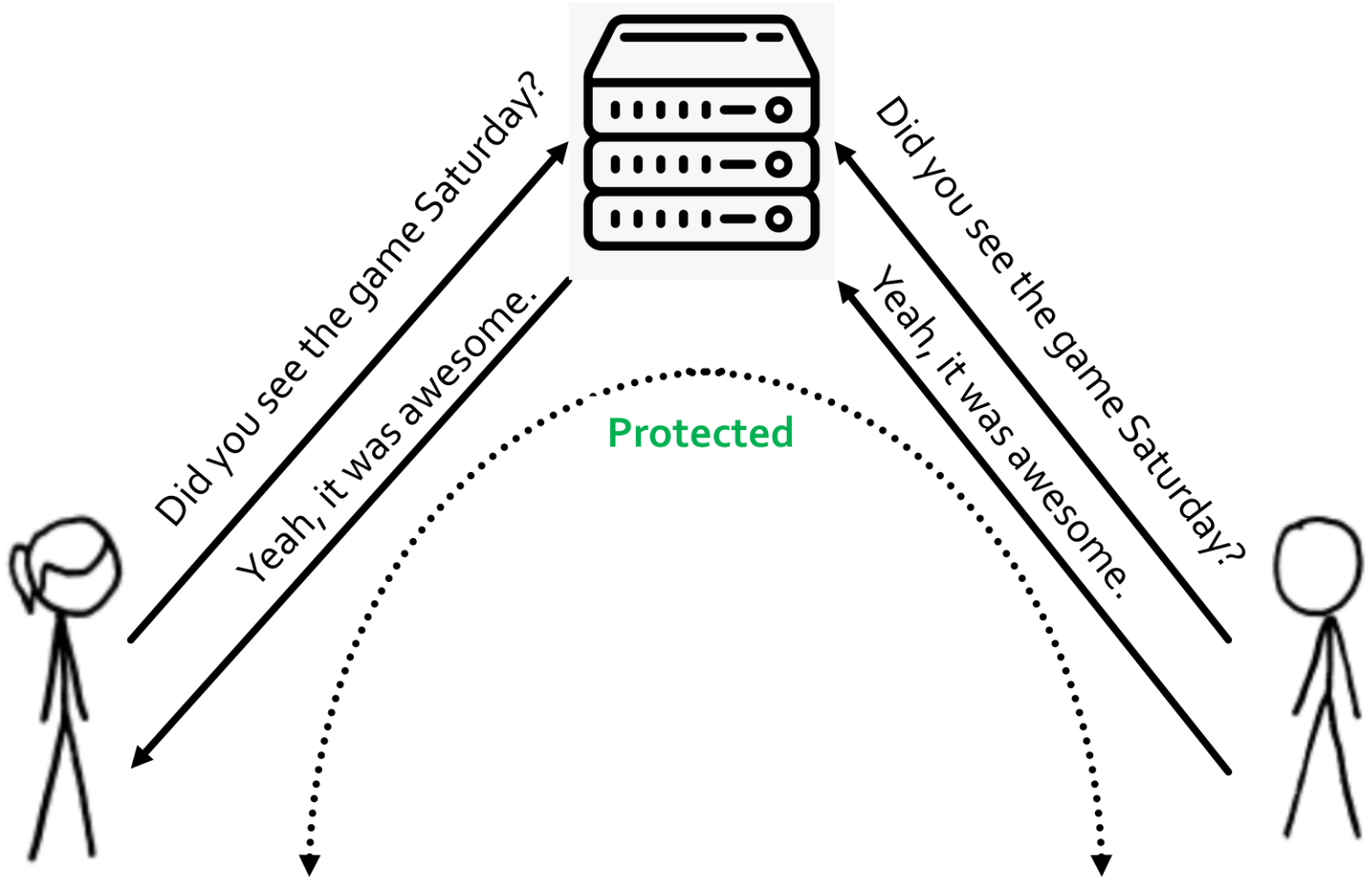


Make Dangerous Things Hard



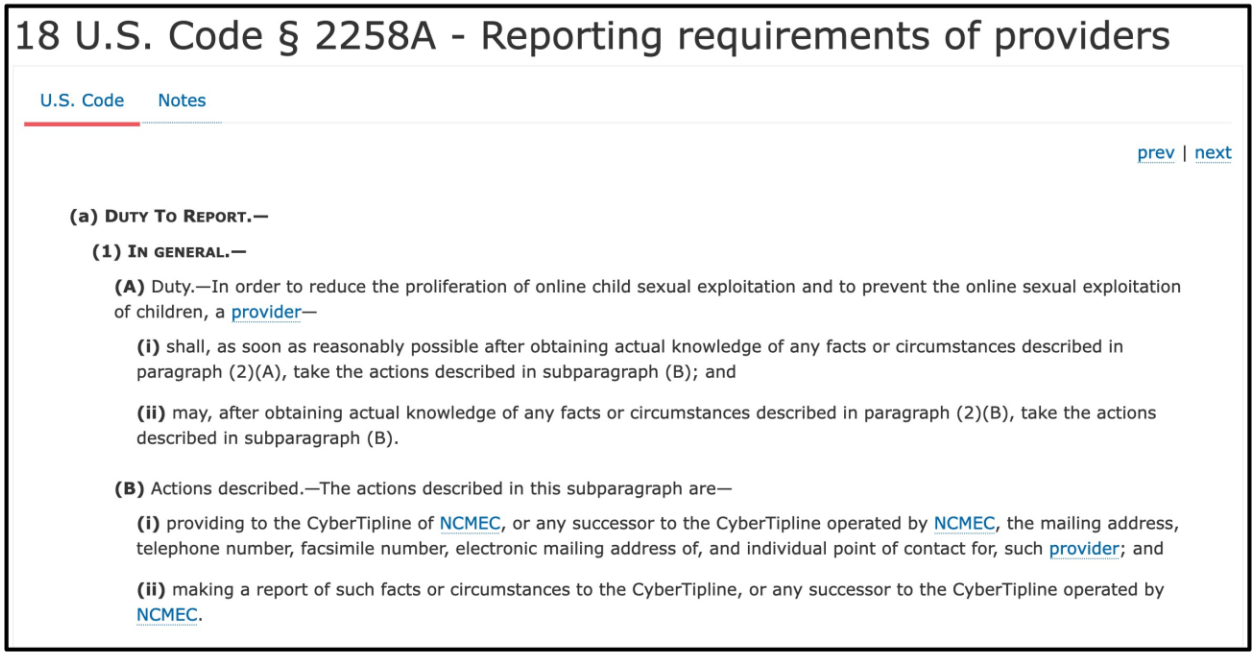
- Don’t allow users to make dangerous choices
  - View private key
  - Disable warnings
  - etc

E2EE Often Struggles WRT Handling Abuse of Service



CSAM

By law, companies are required to report instances of Child Sexual Abuse Material (CSAM) to law enforcement.



18 U.S. Code § 2258A - Reporting requirements of providers

U.S. Code | Notes

prev | next

(a) DUTY TO REPORT.—

(1) IN GENERAL.—

(A) Duty.—In order to reduce the proliferation of online child sexual exploitation and to prevent the online sexual exploitation of children, a provider—

(i) shall, as soon as reasonably possible after obtaining actual knowledge of any facts or circumstances described in paragraph (2)(A), take the actions described in subparagraph (B); and

(ii) may, after obtaining actual knowledge of any facts or circumstances described in paragraph (2)(B), take the actions described in subparagraph (B).

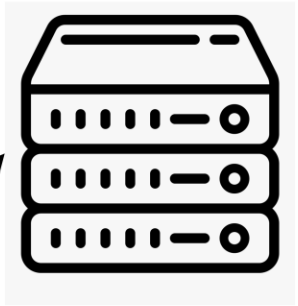
(B) Actions described.—The actions described in this subparagraph are—

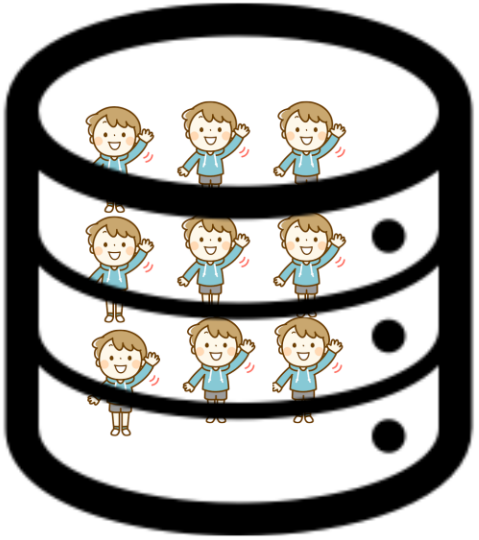
(i) providing to the CyberTipline of NCMEC, or any successor to the CyberTipline operated by NCMEC, the mailing address, telephone number, facsimile number, electronic mailing address of, and individual point of contact for, such provider; and

(ii) making a report of such facts or circumstances to the CyberTipline, or any successor to the CyberTipline operated by NCMEC.

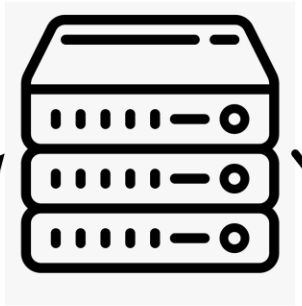
Handling CSAM (non-E2EE)

Handling CSAM (non-E2EE)

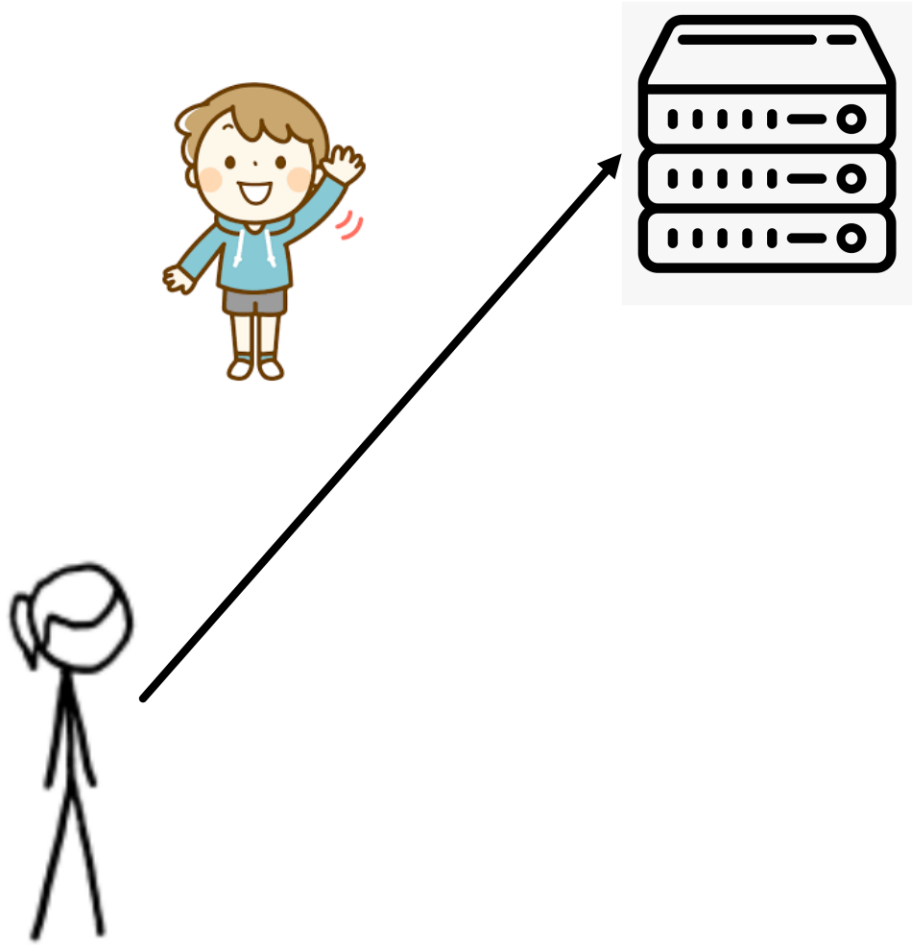




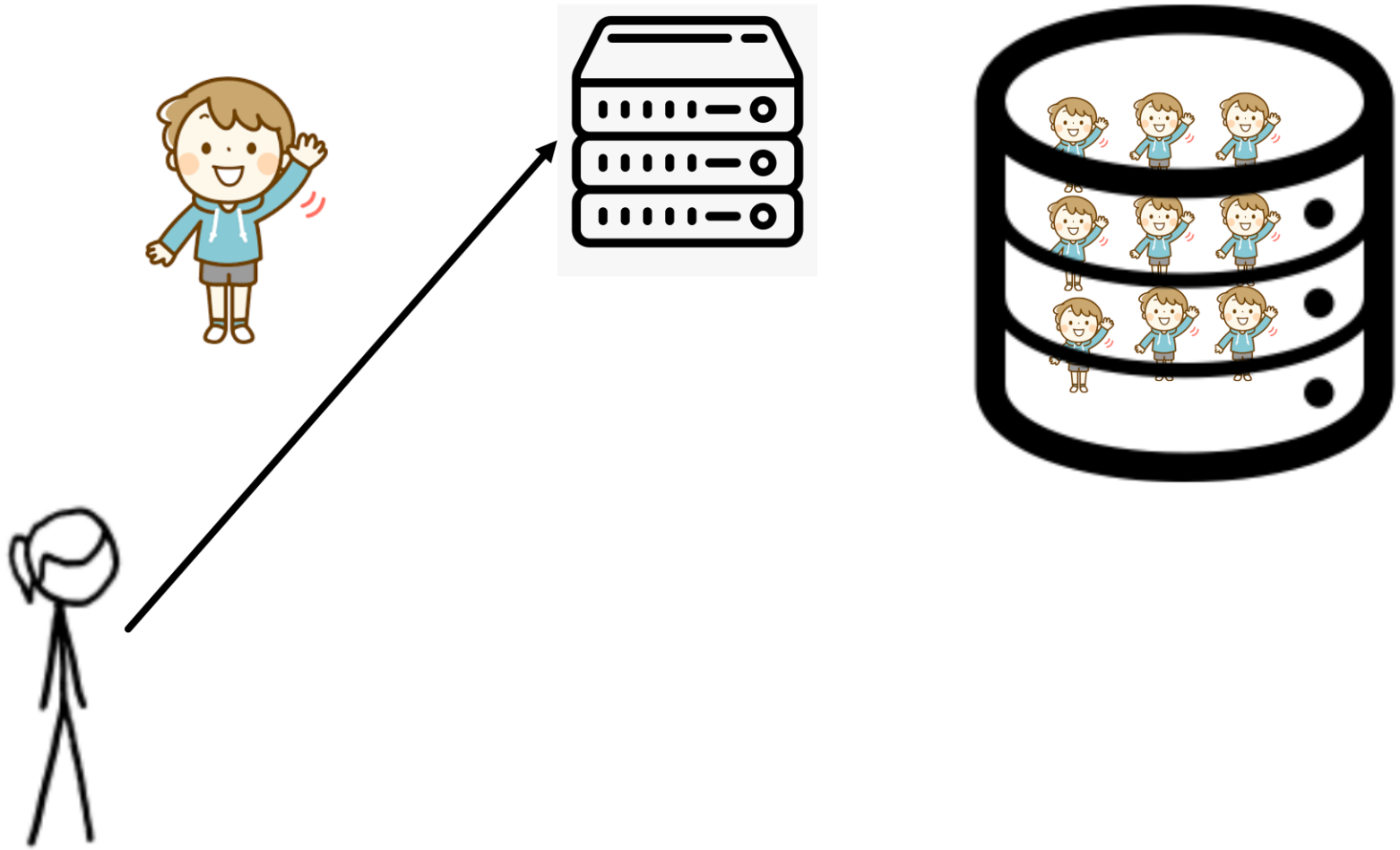
Handling CSAM (non-E2EE)



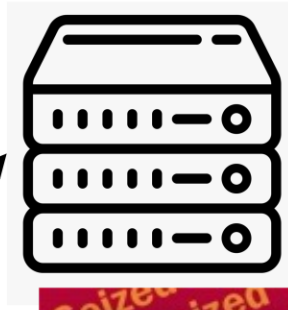
Handling CSAM (non-E2EE)



Handling CSAM (non-E2EE)



Handling CSAM (non-E2EE)



Content scanning is difficult with non-text and/or E2E architectures.

Why?

Must Handle Many Formats & Encodings

BMP

873fdedecaf83cc7a70c026a93aaaaa649aee01a494a9f143e65e32f48515704

JPG

de201cf4cd99637466o4ca44dc16559d0d2e6430f778d332607bd3287e95f76a

PNG

e5eee34489904a6cb623f4269f8d7ec88ace9d272e5ef7c9f335c6711e8bcce6

WebP

340c44fd7ff75c78d9c487e6c39be03af3e05c9df87bf8d77f1f97ca8c67b99f

Trivial False-Negatives

Known Image

Cropped Image

Flipped Image

Modified Image

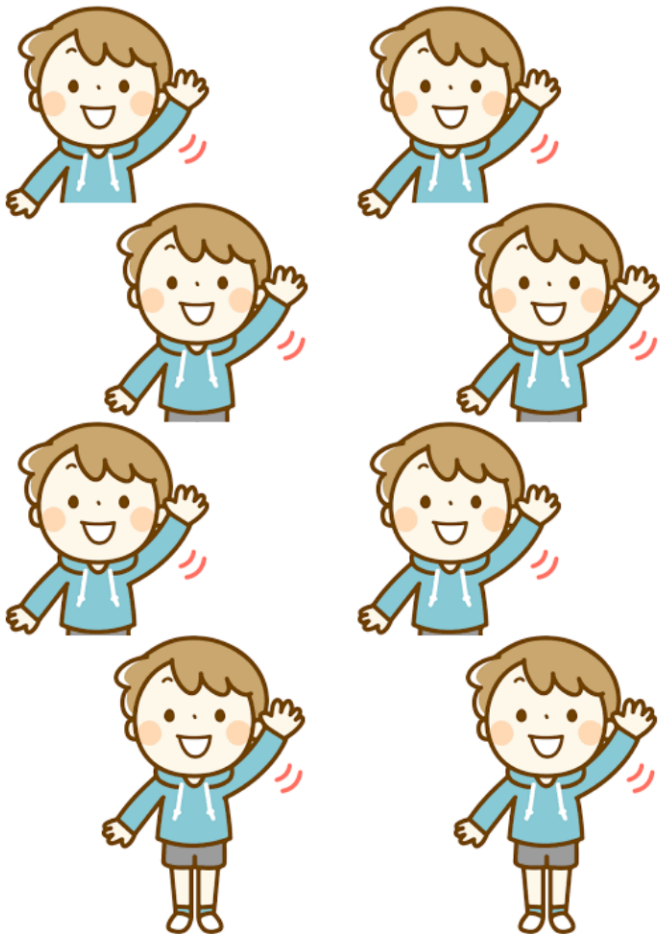
Things That Shouldn't Match Can

Can't Use Distributed Checking

android studio

```
if (image in DB):
    contact_feds()
```

Database on client:



Client-Side Scanning

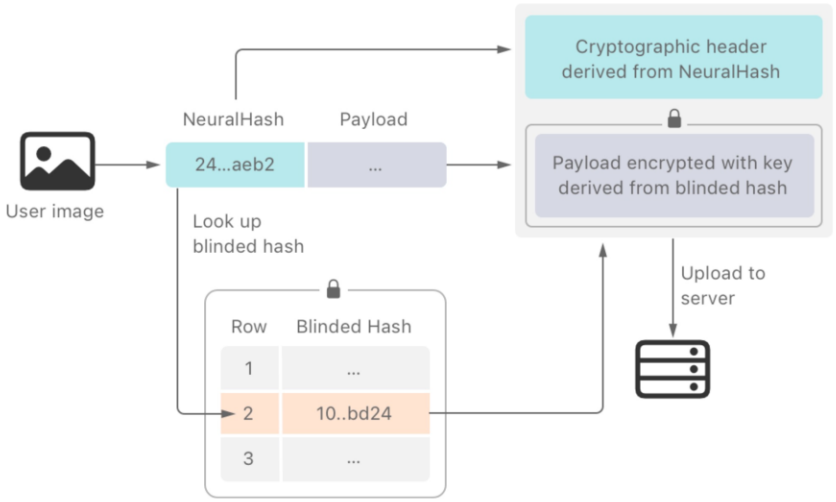
With the proliferation of usable E2E messaging, client-side filtering/scanning is becoming more common and wide-spread.

- Instead of monitoring for illegal content remotely, do it on the user's device
- Claim to only report to law enforcement if illegal content found

Perceptual Hashing

A **Perceptual Hash** (often called “image hash”) is a hash-like function which tries to encode the visual representation of an image and **NOT** the bit-representation.

- Clients compute & compare perceptual hashes to known DB



Many "knobs" to turn

- How to partition?
- Are colors important?
- Which format(s)?
- Is it fast enough?

How similar is "similar"?

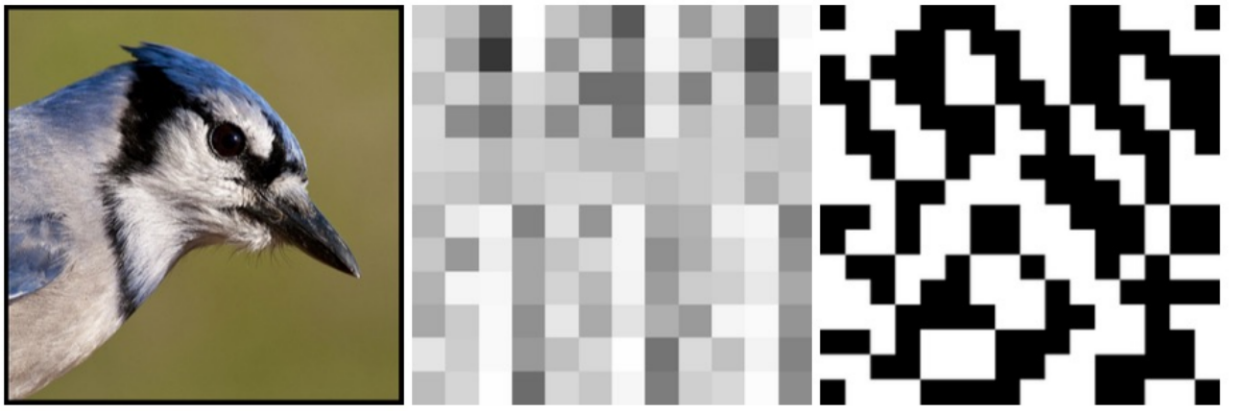


Figure 2: An image from ImageNet [36] (left) and a visualization of its associated PhotoDNA (center) and PDQ (right) hashes.

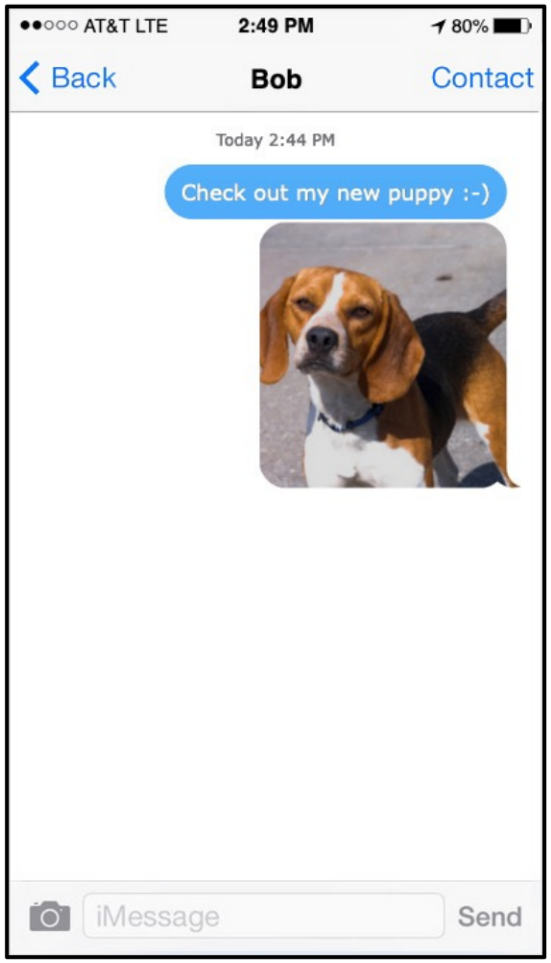
Things That Don't Match Do

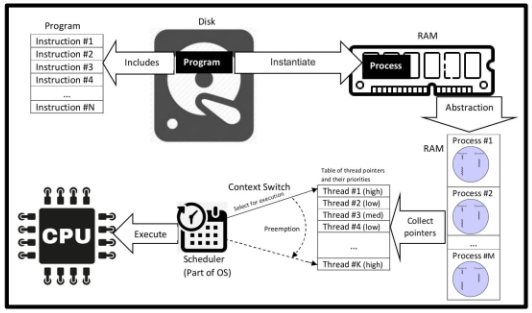
We can confirm the hash collision using `nnhash.py` from AsuharietYgvar/AppleNeuralHash2ONNX:

```
$ python nnhash.py dog.png
59a34eabe31910abfb06f308
$ python nnhash.py adv.png
59a34eabe31910abfb06f308
```

Source: https://github.com/anishathalye/neural-hash-collider

False-Positives Results Are Still Positives Results





=12345

=12345

Computer and Network Security

Lecture 26: End-to-End Encryption & Usability

COMP-5370/6370
Fall 2025

Computer and Network Security

Lecture 26: Exam 3 Review

COMP-5370/6370
Fall 2025

1. Match the class of attack with the *best* description of it.
   (a) (4 points) _____ **ARP Spoofing**
   (b) (4 points) _____ **Cross-Site Scripting (XSS)**
   (c) (4 points) _____ **Content Injection**
   (d) (4 points) _____ **Cross-Site Request Forgery (CSRF)**
   (e) (4 points) _____ **SSL Stripping**

   Possible descriptions *(not all will be used)*:

   A An attack in which A) a domain name is intentionally and maliciously chosen to mimic an existing, non-malicious domain name and B) that similarity is used to trick users into visiting the malicious version under the impression that it is the non-malicious version.

   B A generic name for attacks that present user-content (3P) as service-content (1P).

   C A class of attacks in which 3P user-content is unexpectedly executed in the victim's browser (most often through JavaScript).

   D A class of attacks in which an attacker attempts to harm the target network/device/service by masquerading as benign connections/traffic/etc. from legitimate users of that network/device/service.

   E An active network attacker passes traffic between a non-encrypted client connection and an encrypted server connection to ensure the client does not realize it can encrypt its traffic to the server.

   F A generic name for attacks that present service-content (1P) as user-content (3P).

   G A class of attacks by which 3P user-content causes the victim's in-browser credentials to unexpectedly authenticate a request made at the behest of an attacker.

   H A class of attacks by which a client is tricked into surrendering their in-browser credentials via a browser-based binary exploitation.

   I An active network attacker attempts to modify the switching-logic of Local Area Network (LAN) infrastructure via abuse of a specific, L2 protocol.

   J A class of attacks in which 1P service-content is executed in the victim's browser (most often through JavaScript).

   K An active network attacker attempts to modify the routing-logic of Wide Area Network (WAN) via malicious interactions with its network infrastructure using a specific, L4 protocol.

2. (2 points) Name one of the two canonical defenses against ARP Spoofing attacks. **Do not** describe its operation or its protection mechanism. (1–5 words total)

3. (2 points) Which type of a VPN requires every client to be explicitly configured to use the VPN server? (circle one)

Remote-Access VPN Site-to-Site VPN

4. (2 points) Which type of a VPN is implemented in network infrastructure devices and is transparent to all clients? (circle one)

Remote-Access VPN Site-to-Site VPN

5. (2 points) Given the below *protocol* options, which should you enable when building a website? (circle all that are safe to use in 2025)

SSLv1.0 SSLv2.0 SSLv3.0

TLSv1.0 TLSv1.1 TLSv1.2 TLSv1.3

6. Answer the below True/False questions related to browser cookies (circle one for each).

   (a) (1 point) When browser cookies are set via the HTTP protocol (i.e. **not** via JavaScript) the cookies' value is determined by the *server* and stored on the *client*.

   True False

   (b) (1 point) When browser cookies are set via JavaScript (i.e. **not** the HTTP protocol) the cookies' value is determined by the *client* and stored on the *server*.

   True False

   (c) (2 points) If user navigate to `aaaa.com` and that website instructs the browser to load content from `bbbb.com`, any cookies set by `bbbb.com` are considered "3^{rd} party (3P) cookies" and those set by `aaaa.com` are considered "1^{st} party (1P) cookies".

   True False

   (d) (2 points) If you navigate to `cccc.com` and that website instructs your browser to load content from `dddd.com`, the JavaScript supplied by `dddd.com` is allowed to read the cookies set by `cccc.com`.

   True False

7. Match the description with the web defenses which *best* applies to it.

   (a) (3 points) _____ **When an SSL certificate is issued by a CA, it is posted to a public ledger for archival.**

   (b) (3 points) _____ **Client-side restrictions on how two pieces of content (iframes, scripts, etc.) can interact with each other based on where they were fetched from.**

   (c) (3 points) _____ **A mechanism for websites to whitelist content sources via an HTTP header.**

   Possible Web Defenses *(not all will be used)*:

   A Certificate Transparency

   B Blockchain Technology

   C Content Security Policy (CSP)

   D HyperText Transfer Protocol - Secure (HTTPS)

   E Same-Origin Policy (SOP)

8. (2 points) What protocol/protocol stack most often relies on the "Trust on First Use" (TOFU) solution to the key distribution problem? (circle one)

   ARP TLS SSH VPNs (*assorted*)

9. (2 points) What protocol/protocol stack most often relies on the "Public Key Infrastructure" (PKI) (circle one)

   ARP TLS SSH VPNs (*assorted*)

10. For each of the below categories of network defense components, give a **short** description of its primary *detection* abilities (i.e. what type of logic its traffic-matching rules can use to make policy decisions). [1–2 sentences]

    (a) (3 points) **Firewall** —

    (b) (3 points) **Intrusion Detection System (IDS)** —

    (c) (3 points) **Intrusion Prevention System (IPS)** —

11. Of the above categories of tools, list whether or not they are able to **block** network traffic if it matches a rule as described above. [clearly write "firewall", "IDS", and "IPS" next to the correct prefix]
    (a) (2 points) **Are *able* to block an attack** —
    (b) (2 points) **Are *not able* to block an attack** —

12. Denial of Service (DoS) attacks are a well-known class of attacks against services on the Internet. For each of the below techniques commonly used in DoS attacks, describe the mechanism by which it works [max of 2 sentences each]. Your answers should clearly show your understanding not only of the attack, but **also** of the difference between this class and the other classes.

    (a) (2 points) **Direct Traffic Flooding** —

    (b) (2 points) **Reflection** —

    (c) (2 points) **Amplification** —

    (d) (2 points) **Distributed (DDoS)** —

13. The TLS protocol is commonly used to improve the security and privacy of existing legacy protocols (e.g. FTP → FTPS, SMTP → SMTPS, etc.). List at least two *different* reasons why TLS is well-suited to this use-case. [2-4 sentences]

    (a) (3 points) **Reason #1** —

    (b) (3 points) **Reason #1** —

14. When creating HTTPS connection to a web server and using the Public Key Infrastructure (PKI), the client is responsible for not only validating the SSL certificate chain provided by the server, but also ensuring that the provided certificate chain is specific to to the destination. For each of the below groups of options, select those which are **both correct and necessary** to doing so.

    (a) (2 points) Select **one (1)**:

    - Ensure that the leaf-certificate is previously-known and trusted.
    - Ensure that the intermediate-certificate(s) is previously-known and trusted.
    - Ensure that the root-certificate is previously-known and trusted.

    (b) (3 points) Select **up to three (3)**:

    - Ensure that the leaf-certificate is correctly signed by the intermediate-certificate.
    - Ensure that the leaf-certificate is correctly signed by the root-certificate.
    - Ensure that the intermediate-certificate(s) is correctly signed by the root-certificate.
    - Ensure that the intermediate-certificate(s) is correctly signed by the leaf-certificate.
    - Ensure that the root-certificate is correctly signed by the leaf-certificate.
    - Ensure that the root-certificate is correctly signed by the intermediate-certificate.

    (c) (2 points) Select **one (1)**:

    - Ensure that the leaf-certificate's contents correctly match the destination server's identity.
    - Ensure that the leaf-certificate's contents correctly match the destination server's administrator.
    - Ensure that the leaf-certificate's contents correctly match the destination server's hosting service.

Computer and Network Security

Lecture 26: Exam 3 Review

COMP-5370/6370
Fall 2025