Authentication

KAMI VANIEA

First, the news …

- **Kaspersky admits to reaping NSA code from US PC**
- http://www.zdnet.com/article/kaspersky-admits-to-reaping-nsa-code-from-us-pc/

Most recommended security behaviors

- 2/5 non-experts advice involves authentication
- 4/5 expert advice involves authentication

https://googleonlinesecurity.blogspot.com.au/2015/07/new-research-comparing-how-security.html

Authentication

- Verifying a fact about an entity before allowing it 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
- Authentication should happen every time an action is taken and there is no way to be certain that the authenticated entity has not changed.
  - When logging into a website it looks like you only authenticate once, but your computer is actually authenticating for you every time it talks to the server to prevent session hijacking

Think about what you are authenticating

- Actual identity of the person
- That they are the same entity who setup the account
- They have a specific property
  - Above the legal drinking age
  - Student of the university
  - Facebook user
- That another authenticator thinks they are the same entity

Authentication factors

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

Also jokingly known as:

- Something you **can forget**
  - Password, mother's maiden name, your address
- Something you **can loose**
  - Student ID card, credit card chip, RSA key
- Something you **can't change**
  - Finger prints, voice tones, iris, typing patterns

Multi factor authentication

- Authentication that requires two or more of the factors.
- Two-factor
  - Chip and pin in a credit card. Something you have (chip) something you know (pin).
  - Chip and signature credit card. Something you have (chip) something you are (signature pattern).
- Three-factor
  - Security guard that check's your ID against what you look like and then requires a code.
  - Secure finger print reading fob that gives you a code after it reads your fingerprint, then you use the code and a password to log in.

Invisible continuing authentication

1. You log into a website using a password (something you know).
2. Website sets a cookie with a secret and a timestamp.
3. Every time you visit a new page your computer sends the cookie (something you have) and the server verifies it.
4. When you log out the cookie is destroyed.

How banks do (mostly) invisible 2-factor authentication

1. You log into a website using a password (something you know).
2. The website is also sent the cookie from the last time you logged in (something you have).
3. If the password and the cookie both match you get to log in.
4. If the cookie is missing, or wrong, the bank will ask you to prove that you have something else by calling you (phone) or emailing you a code (email).

Passwords

Password protections

- Hashing
- Lockout
- Reset on

Hashing

A row from /etc/shadow

aychedee:6vb1tLY1qiY$M.1ZCqKtJBxBtZm1gRi8Bbkn39KU0YJW1cuMFzTRANcNKFKR4RmAQVk4rqQQCkaJT6wXqjUkFcA/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 safe place
  - You can hash the password. Hashing does not require a secret key so there is no secret key to lose

Hashing

A row from /etc/shadow

aychedee:6vb1tLY1qiY$M.1ZCqKtJBxBtZm1gRi8Bbkn39KU0YJW1cuMFzTRANcNKFKR4RmAQVk4rqQQCkaJT6wXqjUkFcA/qNxLyqW.U/:15405:0:99999:7:::

- What type of hash function was used
  - 6
- Salt
  - vb1tLY1qiY
- Encrypted password
  - M.1ZCqKtJBxBtZm1gRi8Bbkn39KU0YJW1cuMFzTRANcNKFKR4RmAQVk4rqQQCkaJT6wXqjUkFcA/qNxLyqW.U/

Lockout

- Password guessing attacks work because a computer can guess many times a second
- Humans don’t guess many times a second
- Idea: if a user can’t guess a password in 10 tries or less lock them out for a time period or require another factor

Something you have

Physical keys

- Simplest and one of the most common examples of something you have
- Each key contains a “code” in the form of notches on the key
- Having one allows you to open physical locks
- Single factor authentication

RSA key fob

- When a button is pushed the fob prints out a number
- The number is generated securely using methods we will talk about later
- The number must be typed in along with a password
- Two factor authentication

Chip in a credit card

- Similar to RSA fob, the chip generates a unique code
- The user

A public/private digital key

- We will discuss these in more detail later in the course
- Simply: A public key can unlock what a private key locks, and vice versa
- A PGP key is something you have which authenticates you
- For example, if a file is encrypted using the key on the right only I can decrypt it using my matching private key which only I possess

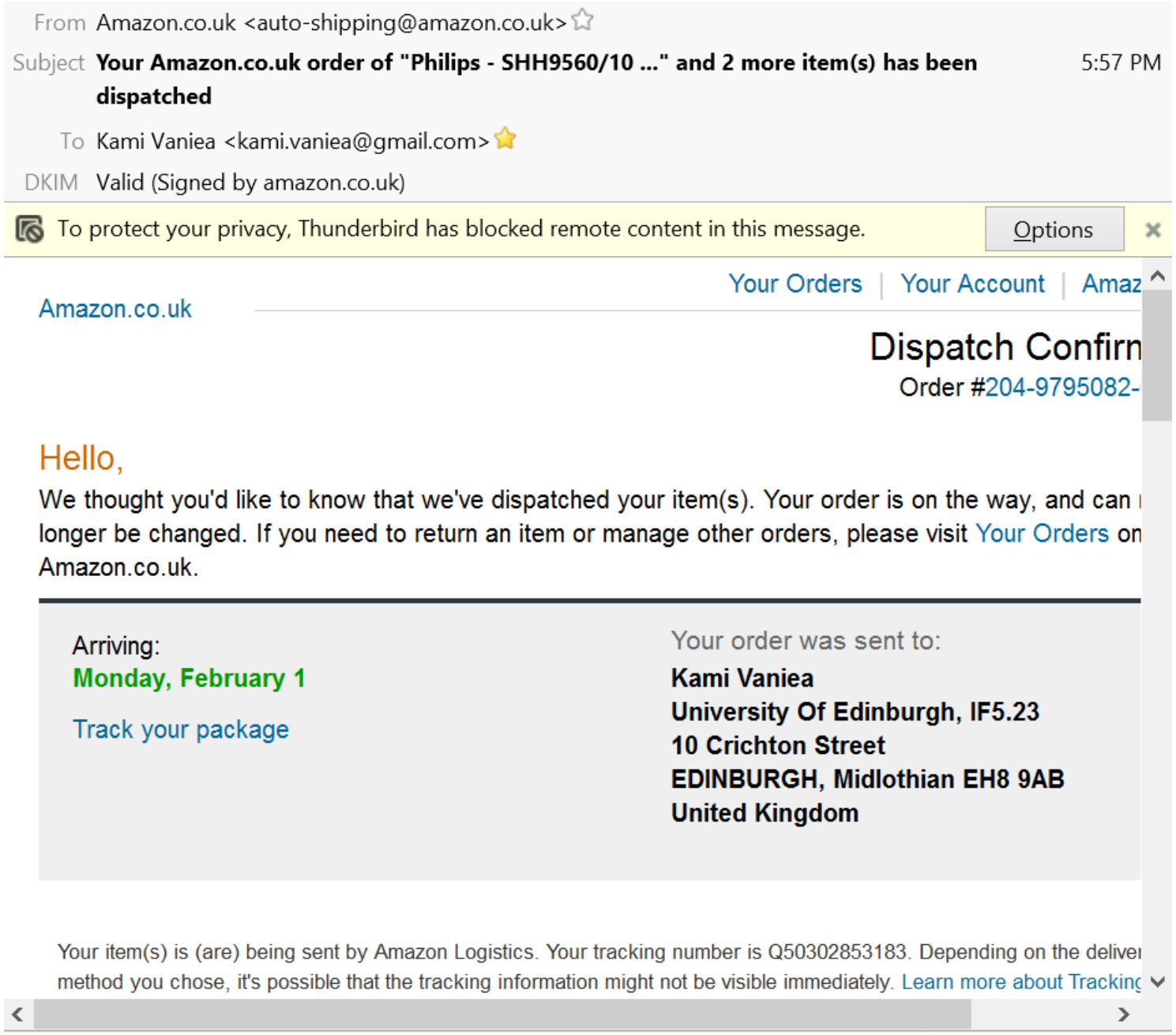
My public key

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFHMcgABCAC9WrYDO6K2L3VHyi4eHN6suHLqMpJ+SO+IUTuLEVnUzIoXAUXH
KozHejfV/9XoG8j933ZtszXKCog3aMESe0E0z6fNGfolvaCe5B4jwqoJt8NHwb5L
B2dnq0CplgXcN2GJxfEHHUaf27COSobCJxPMeshUh4ZHke+g6DatmiEtBpVp41Ot
1zgxdMQkgb2H2xw28RYfYkdDouetelkOrFLrCy9ZF9KdMhA1eBH94KnwIQshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFRW40UsY52OfveOyfQPzkkRto7u2339hvH0
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXJVsUj0dABEBAAG0IkthbWkgVmFuaWVhIDxr
dmFuaWVhQGluZi5lZC5hYy51az6JAT8EEwEIACkFAlYKYvECGyMFCQlmAYAHCwkI
BwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRCTdsxl9/HZffG+CACShuKxje3QAqew
GWh8K4gCdiY0xDqJwq3PHxmyhZmQeN/1a1KcOrIjI2b+Q75/5t+EgXOHpR0PIxfG
lZ6zOEpf6A18iFXx3JgQZdwPD0jtBiWNpOyMeBGTgIvEYG3so2VueQoeXcq3dbYp
5vstVxtD+TKHQ5CioIT75P2bzYq/XLT5aIbNQhQDPcTo0DgbRH+FvqsRXr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrIPBJ2VYCDzQkJ7uQ5eFh4ZhsMgOmzLQD4
YiGr5weIMFwAvxZOaRxEa9Vf48jiWvrxuJ8YfHWS0hEScNOcYC2P8q20IJwwE26T
lpdtrwCqtB1LYW1pIFZhbmllYSA8a2FtaUB2YW5pZWEuY29tPokBQgQTAQIALAIb
IwUJCWYBgAcLCQgHAwIBBhUIAgkKCwQWAgMBAh4BAheABQJWCmMeAhkBAAoJEJN2
zGX38dl9JJAIAIW0rxrlYsrmKS6CbW8MgTxxTDOXaCt1b7F0W0QZHskIUQhEcE+a
XBYib1A5uHaatLfyjeXaD3qMEoZnQHoYMGE0GKu00wWsbhfoQzHPgwzRLkD1i75M
BIbaww0KWoVB9e4AkMakXJCnF5BXeo6AHRL2v15V205DikVnlCRXocKtu8b7LnkM
cLn7oLobr1de1uyKoNzbSnO/vpKDJp0/EY5yUeV9oIypZy/6wFQBehg1sXye6znO
9wb9uUsu9+/P8pz4JILMDSevjfT7zSRSl/YP3fOfZ6N4bc+KOdwPM7u5Iyoeu9zh
pzibv3ge7VhH2xIWz8vYZ/2xT1345tWRRMOJAhwEEwECAAYFAlTnSpEACgkQjyxM
p99tBt2B8A/+OpIzOsQbQJB8yxti4I7PpD1weJDf3a81Vhm7JyXE/Xy66ypfdt3w
XmFRUuIrwezY1NebWNCRQHzQvRv/VJwjbTUx+Q3HsjlkKlHbE7iCiQXXtTRk0Eny
2nudcjGI2v03C3B2JCucEw6esF1x79PI/lPv2+6tgUBKmDfOpsB2vbtqrHnmAYKL
4lQBFH1YSJgnzwo2Jkh0hcHdF90Zem1eMeiDEeVkH63893N8Swk5fBKdTj+SKZ/L
rQElBBlpMR9BmeY6bPvWRuycVK0nIMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGvkd
ZlarK84r+KU1KD5IfgOCN7nhwgy7VImE68caZHSRiPWZP1fVVMhydiRJv8WsoUs6
INfVU3nxH+ZYthPbY0T86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994
nzP6cNorir3GIpsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuyKkFWPZwnEvDJYaC
NN/3jWcbhLFwKBDsaHps2+1meFP0oJFvNetzp2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYZTSS05x1RdXHqpEbgap8dtuHhVvJw9QYDQBJr0K4aKyG9qqMD8cta
Pl/FAdyAqwH8Nw9efqAK+RQxSVUaue9BYEnbIRpsDK6MkP3YMFmu5ki5AQ0EUcxy
AAElALyXYy8G2ZaTDJpdGcRhmIqOOSUlzPV7/5E5BbYKBNu4KU3nX+JLVcF5jxPQ
42c7i/WRVxE1BJTiarKGsEvCi94TTXSIUKAt3T1oGBtXmGvqbGBq8ljSGl1UTwdF
5yu50JyRSf2fqRND6P/2eHNXejDUtdvhUXIUt8h9MuUO/ipD0DnwIvMnAATJHA+R
Zqw6oNpyjRGzvr3iuWUwe4PtyJDI3ELAFkbp/NAc5TIuVHRHNOWNplcIJhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPOdbCZf
2Tozd7h9MXtGJDlPKJ8eLG8ogcMAEQEAAYkBJQQYAQIADwUCUcxyAAIbDAUJCWYB
gAAKCRCTdsxl9/HZfS+hB/9BJqSmIgcoHFXnb1PVIKxekzL8+WVm5Pk/EgMQSLZ2
HX4p3ial5PEPcYgUw9YnaG4i00dwJGw5/daTWRrTzcnKd8YqoP+DU0t96HZDSu3m
mCzE9NVAQYboFbVmGOx0eo627UBSvFqaXvAxBDYkoR8B0TnKhrQFwXkZVb30hKwD
TgAFjOGlZiE6uAdST231tFaq0bizYfe5AVXRqro20xBqNbaJNqs3SW0D831Syvdv
llOBx83/R0gg7hUkI6F2vzXicWmUwFSXRrggCSbLosHsP6isBWwvlHeRmna/aQab
YKG3gbV9iyczAS31gbogVLAZqNSWhp8vVIEE28Fyf/Ed
=x5FK
-----END PGP PUBLIC KEY BLOCK-----

DKIM

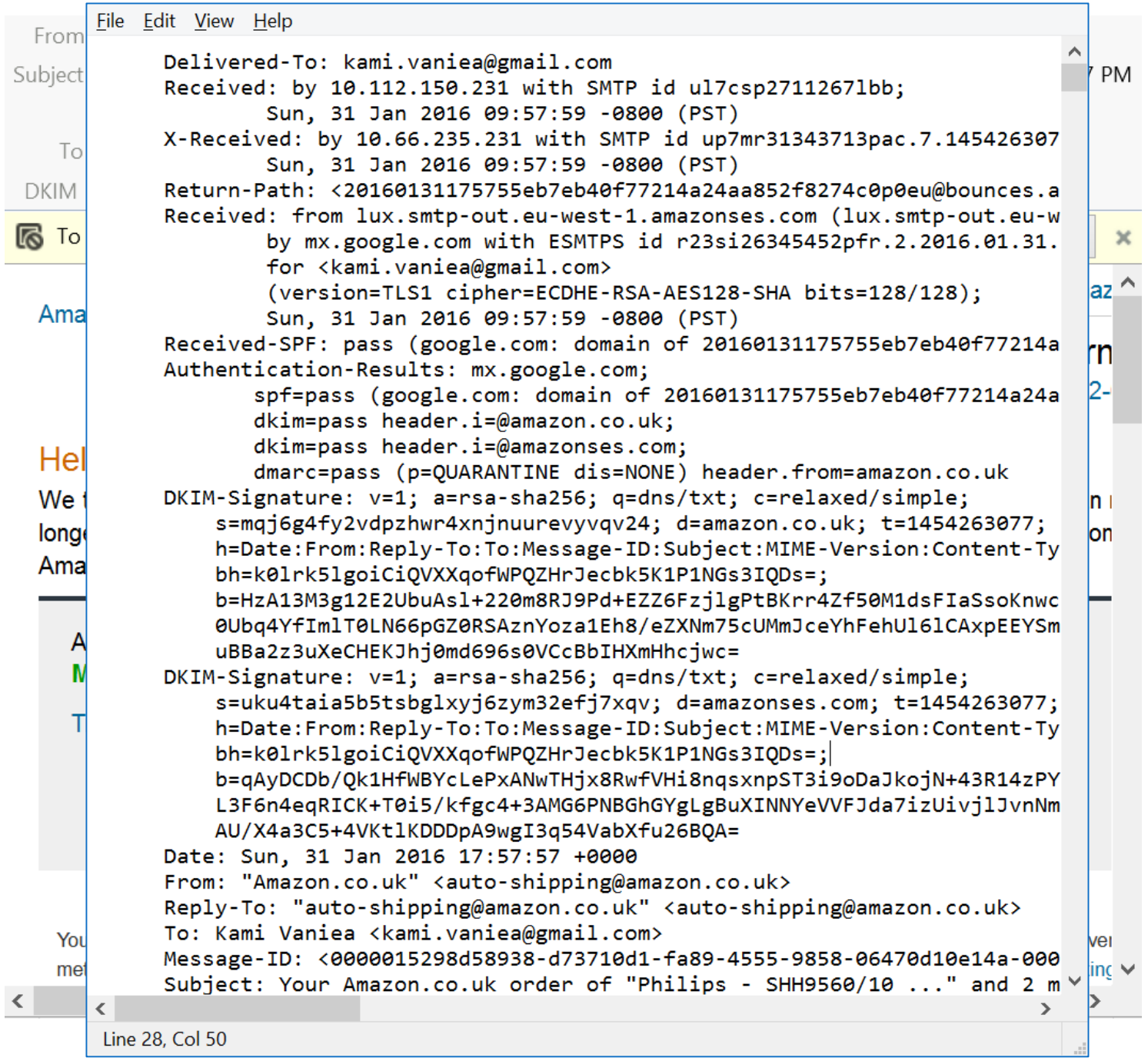
- People are not the only ones who authenticate
- Servers also need to authenticate to each other
- One of the most visible is DKIM signatures in email



DKIM

- Problem: Spam
- Solution:

1. Sending email server signs the email using a private key
2. Receiving email server checks the key to authenticate the sending server



Something you are

Finger print readers

- Fingerprints are nearly unique so they seem like a good authenticator
- Not all people have fingerprints
  - Some professions destroy fingerprints
  - Some fingerprints are too faint to read
- Fingerprints can never be changed
- You leave fingerprints everywhere

Most biometric readers have similar problems

Continuous authentication

- Your interaction with a computer is unique and we can measure it
  - Mouse movements
  - Keyboard typing patterns
- Nearly impossible to duplicate a real user's typing patterns
- Easy to loose access if the user hurts their hand, or is doing something non-standard
- Repetitive Stress Injury (RSI) patients trigger continuous authentication warnings regularly while healing

Privacy

- Users have a right to privacy, that is, a right to keep aspects of themselves hidden that are not necessary to expose
- Authentication mechanisms need to take privacy into account and not ask for more than they need
- Identifying a user using a Facebook, Google, or Apple account may be easy, but it gives away large amounts of data
- Similarly, requiring a validated ID such as drivers or passport information also exposes quite a bit of information

Questions