

# 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

SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES	VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES
1. USE ANTIVIRUS SOFTWARE 		 1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS 		 2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY 		<b>2</b> 3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW 		 4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION 		 5. USE A PASSWORD MANAGER

# 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 lose**
  - 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:$6$vb1tLY1qiY$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:\$6\$vb1tLY1qiY\$M.1ZCqKtJBxBtZm1gRi8Bbkn39KU0YJW1cuMFzTRANcNKFKR4RmAQV4k4rqQQCkaJT6wXqjUkFcA/qNxLyqW.U/:15405:0:99999:7:::

- What type of hash function was used
  - 6
- Salt
  - vb1tLY1qiY
- Encrypted password
  - M.1ZCqKtJBxBtZm1gRi8Bbkn39KU0YJW1cuMFzTRANcNKFKR4RmAQV4k4rqQQCkaJT6wXqjUkFcA/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



# My public key

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

Version: GnuPG v2

```
mQENBFHMcgABCAC9WRyDO6K2L3VHyi4eHN6suHLqMj+SO+IUTuLEvNUzloXAUXH
KozHejfv/9XoG8j933ZtsXKCog3aMESe0E0z6fNGfolvaCe5B4JwqJt8NHwb5L
B2dnq0CplgXcN2GjxfEHHUaf27COSobCjxPMeshU4ZHke+g6DatmiEtBpVp410t
1zgxDMQkgb2H2xw28RyYfYkdDoueteIkOrFlrCy9ZF9KdMhA1eB894KnlwQshdiZR
QYEX25+M8cKCb++Rc9H6an7EG9WHOFrW40UsY52OfveOyfQzpkRto7u2339hvH0
B/h+7xLM6FQbOUZQ9BD5w7IQHgYtXjVsUj0dABEBAAQ0lktbWkgVmFuaVWVhDxr
dmFuaVWVhQGluzi5IZC5hYy51az6JAT8EEwEIAckFAIKYyECGyMFCQlMAYAHcWkl
BwMCAQYVCAIJGcsEFGIDAQleAQIXgAAKCRCTdsxI9/HZffG+CACShukxje3QAqew
GWh8K4gCdiY0xDqJwq3PHxmyhZmQeN/1a1KcOrljl2b+Q75/5t+EgXOHpR0PxfG
Iz6zOEpf6A18iFxx3JgQZdwPD0jtBiWNpOyMeBGTglvEYG3so2VueQoeXcq3dbYp
5vtVxtD+TKHQ5CioIT75P2bzYq/XLT5albNqHQDPcTo0DgbRH+VvqsRXr7yeaef
JaPnxX0+1L33t2QY9zctiGyebwrvHMrlPBJ2VYCDzQk7uQ5eFh4ZhsMgOmLQD4
YiGr5weIMFwAvxZOaRxEa9Vf48jiWvrXuJ8YfHWS0hEScNOCyC2P8q20lJwwE26T
lpdtrwCqtB1LYW1pIFZhbmlYSA8a2FtaUB2Yw5pZWEuY29tPokBQgQTAQIALAIB
lwUJCWYBgAcLCQgHAWiBBhUIAgkKcWQWAgMBAH4BAheABQJWCMMeAhkBAAOEJN2
zGX38d9JAIWI0rXlYsrmKS6CbW8MgTxxTDOXact1b7F0W0QZHSkiUQHecE+a
XBYib1A5uHaatLfjjeXaD3qMEoZnQHoYMGEOGKu00wWsbhfoQzHPgwzRLkD1i75M
Blbaww0KWoVB9e4AkMakXJcNf5BXeo6AHLR2v15V205DikVnICRocKtu8b7LnkM
cLn7oLobr1de1uyKoNzbSnO/vpKDjP0/EY5yUeV9oIypZy/6wFQBehg1sXye6znQ
9wb9uUusu9+/P8pz4JILMDsejvft7zSRSl/YP3fofZ6N4bc+KODwPM7u5Iyoee9zh
pzibv3ge7VhH2xlWz8vYz/2xT1345tWRRMOJAhwEEwECAAYFAITnSpEACgKjyxM
p99tBt2B8A/+OplzOsQbQJ8yxti4I7PpD1weJDF3a81Vhm7JyXe/Yy6yfpfdt3w
XmFRUulrwezY1NebWNCQRHzQvRv/VjwjbTUX+Q3HsjlKIHbE7iCiQXXtTRk0Eny
2nudcjG12v03C3B2JCucEw6esF1x79PI/Pv2+6tgUBKMDfOpsB2vbtqrHnmAYKL
4IQBFH1YSjgnzwo2Jkh0kHdF90Zem1eMeiDEeVkh63893N8Swk5fBKdJt+SKZ/L
rQEIBBlpMR9BmeY6bPvWRuycVK0niMR80G9iFABxjTpWBL8aGk6EeVK5EqYDGVkd
ZlarK84r+KU1KD5lfgOCN7nhwgy7VImE68caZHSRiPWZP1fVVMhydiRjv8WsoUs6
INfVU3nXH+ZYthPbY0T86leGSchBT5K/fBQvbjhrRTbTFwvjzSifb9efWylDi994
nzP6cNorir3GipsT8gPgBB2/NjxaWiM6y3X1az1vRnsunQHuykKFWPZwnEvDJYaC
NN/3jWcbhLFwKBDSaHps2+1meFP0oJfVnNetzp2bjT9a9pXaQ6KhOmo5DnhLcaV97
bFBpsUuBGaYzTS05x1RdXHqPebgap8dtuHhVvJw9QYDQBJr0K4aKyG9qgMD8cta
PI/FadyAqW8Nw9efqAK+RQxSVUaue9BYEnbRpsDK6Mkp3YMFmu5ki5AQ0EUcxy
AAEIALyXYy8G2ZaTDJpdGcRhmlqOOSUlzPV7/5E5BbYKBNu4KUB3XN+JLVcf5jxPQ
42c7i/WRVxE1BJTiarKGSvEvCi94TTXSIUKat3T1oGBtXmGvqBq8lJSG1IUTwdf
5yu50jYRSf2fqRND6P/2eHNxejDUtdvhuXUit8h9MuUO/ipDODnwlVmnAATJHA+R
Zqw6oNpyjRGzvr3iuWUwe4PtyJD13ELAFkbp/Nac5TiuVRRHNOwNplcIjhM5zHuB
QQb3G/EsCn2PQZ5w5SDzavF2SpvQfDqxYpDaTLAXtF+wsJL5iaUjxwRgJPodbCZF
2Tozd7h9MxtGJDIPKJ8eLg8ogcMAEQEAAYkBJQYQAQIADwUUCuXyAAIBDAUJCWYB
gAAKCRCTdsxI9/HZfs+hB/9BJqSmlgocHFxnB1PVIkxekzL8+WvM5Pk/EgMQSLZ2
HX4p3ial5PEPcYgUw9YnaG4i00dwJGw5/daTWRRtZcnKd8YqoP+DU0t96HZDSu3m
mCzE9NVAQYboFbVmGOx0e0627UBSvFqaXvAXBDYkor8B0TnKhrQFwXkZvB30hKwD
TgAFjOGIZIE6uAdST231tFaq0bizYfe5AVXRqro20xBqNbaJNqs35W0D831Syydv
lIOBx83/R0gg7hUkl6F2vXicWmUwFSXRrggCSbLosHsP6isBWwvliHerMna/aQab
YKG3gbV9iyCzAS31gbogVLAZqNSWWhp8vVIEE28Fyf/Ed
=x5FK
-----END PGP PUBLIC KEY BLOCK-----
```

# 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

# 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

From Amazon.co.uk <auto-shipping@amazon.co.uk> ☆

Subject **Your Amazon.co.uk order of "Philips - SHH9560/10 ..." and 2 more item(s) has been dispatched** 5:57 PM

To Kami Vaniea <kami.vaniea@gmail.com> ☆

DKIM Valid (Signed by amazon.co.uk)

To protect your privacy, Thunderbird has blocked remote content in this message. Options x

Amazon.co.uk [Your Orders](#) | [Your Account](#) | [Amazon](#) ^

**Dispatch Confirmation**  
Order #204-9795082-

Hello,

We thought you'd like to know that we've dispatched your item(s). Your order is on the way, and can no longer be changed. If you need to return an item or manage other orders, please visit [Your Orders](#) on Amazon.co.uk.

Arriving: <b>Monday, February 1</b> <a href="#">Track your package</a>	Your order was sent to: <b>Kami Vaniea</b> <b>University Of Edinburgh, IF5.23</b> <b>10 Crichton Street</b> <b>EDINBURGH, Midlothian EH8 9AB</b> <b>United Kingdom</b>
--	---

Your item(s) is (are) being sent by Amazon Logistics. Your tracking number is Q50302853183. Depending on the delivery method you chose, it's possible that the tracking information might not be visible immediately. [Learn more about Tracking](#) v

< >

# 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

```
File Edit View Help
From:
Subject:
To:
DKIM:
To:
Amazon
Hello
We
long
Amazon
A
M
T
You
me
<
>
Line 28, Col 50
```

```
Delivered-To: kami.vaniea@gmail.com
Received: by 10.112.150.231 with SMTP id ul7csp27112671bb;
Sun, 31 Jan 2016 09:57:59 -0800 (PST)
X-Received: by 10.66.235.231 with SMTP id up7mr31343713pac.7.145426307
Sun, 31 Jan 2016 09:57:59 -0800 (PST)
Return-Path: <20160131175755eb7eb40f77214a24aa852f8274c0p0eu@bounces.a
Received: from lux.smtp-out.eu-west-1.amazonaws.com (lux.smtp-out.eu-w
by mx.google.com with ESMTPS id r23si26345452pfr.2.2016.01.31.
for <kami.vaniea@gmail.com>
(version=TLS1 cipher=ECDHE-RSA-AES128-SHA bits=128/128);
Sun, 31 Jan 2016 09:57:59 -0800 (PST)
Received-SPF: pass (google.com: domain of 20160131175755eb7eb40f77214a
Authentication-Results: mx.google.com;
spf=pass (google.com: domain of 20160131175755eb7eb40f77214a24a
dkim=pass header.i=@amazon.co.uk;
dkim=pass header.i=@amazonses.com;
dmarc=pass (p=QUARANTINE dis=NONE) header.from=amazon.co.uk
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
s=mqj6g4fy2vdpzhwr4xnjnuurevyvqv24; d=amazon.co.uk; t=1454263077;
h=Date:From:Reply-To:To:Message-ID:Subject:MIME-Version:Content-Ty
bh=k0lrk5lgoiCiQVXXqofWPQZHRJecbk5K1P1NGs3IQDs=;
b=HzA13M3g12E2UbuAsl+220m8RJ9Pd+EZZ6FzjlgPtBKrr4Zf50M1dsFIaSsoKnwc
0Ubq4YfIm1T0LN66pGZ0RSAznYoza1Eh8/eZXNm75cUMmJceYhFehU161CAxpEEYSm
uBBa2z3uXeCHEKJhj0md696s0VCCbBIHXmHhcjwc=
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
s=uku4taia5b5tsbglxyj6zym32efj7xqv; d=amazonses.com; t=1454263077;
h=Date:From:Reply-To:To:Message-ID:Subject:MIME-Version:Content-Ty
bh=k0lrk5lgoiCiQVXXqofWPQZHRJecbk5K1P1NGs3IQDs=;
b=qAyDCDb/Qk1HfWBYcLePxANwTHjx8RwfvHi8nqsxnpST3i9oDaJkojN+43R14zPY
L3F6n4eqRICK+T0i5/kfgc4+3AMG6PNBGHGyGlgBuXINNYeVVFJda7izUivjlJvnNm
AU/X4a3C5+4VKt1KDDDDpA9wgI3q54VabXfu26BQA=
Date: Sun, 31 Jan 2016 17:57:57 +0000
From: "Amazon.co.uk" <auto-shipping@amazon.co.uk>
Reply-To: "auto-shipping@amazon.co.uk" <auto-shipping@amazon.co.uk>
To: Kami Vaniea <kami.vaniea@gmail.com>
Message-ID: <0000015298d58938-d73710d1-fa89-4555-9858-06470d10e14a-000
Subject: Your Amazon.co.uk order of "Philips - SHH9560/10 ..." and 2 m
```

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 lose 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

---