Authentication and Authorization (2)

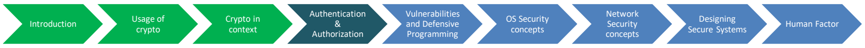
Moshe Kravchik
Credits: Mark Stamp

https://flic.kr/p/8xzAnc

Agenda

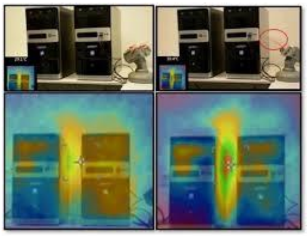
- Covert and Side Channels
- Authentication Methods (passwords, tokens, biometrics)
- Identity Federation

https://flic.kr/p/6keSjR



Covert Channel

- MLS are designed to restrict legitimate channels of communication
- Other ways for information to flow
- **Covert channel**: a communication path not intended as such by system's designers
- For example, resources shared at different levels could be used to "signal" information



Covert Channel Example

- Alice has **TOP SECRET** clearance, Bob has **CONFIDENTIAL** clearance
- Suppose the file space shared by all users
- Alice creates file FileXYzW to signal "1" to Bob, and removes file to signal "0"
- Once per minute Bob lists the files
  - If file FileXYzW does not exist, Alice sent 0
  - If file FileXYzW exists, Alice sent 1
- Alice can leak **TOP SECRET** info to Bob!

https://flic.kr/p/6hb4dv

Covert Channel

- Covert channels are everywhere
- “Easy” to eliminate covert channels:
  - Eliminate all shared resources…
  - …hurting communication and usability
- Virtually impossible to eliminate covert channels in any useful system
  - DoD guidelines: **reduce covert channel capacity** to no more than 1 bit/second
  - May be still not good enough to protect a key from leaking …

Removing covert channels

- Covert channel requires:
  - A sender can change
  - A receiver can read
  - They can synchronize
- Remove either one from the 3 requirements
- Add random noise to the channel
- Decrease bandwidth of time-based channel (no precise timers)
- Audit the channel

https://flic.kr/p/hwC4He

Side channel attacks

- Help an **external** enemy to learn a secret
- Based on physical implementation
  - Timing, power consumption, electromagnetic waves, cache attacks
- Prevention: reduce the information or the relation to the data
  - Bad for performance

```
static int strcmp2(p1, p2)
  const char *p1;
  const char *p2;
{
  const unsigned char *s1 = (const unsigned char *) p1;
  const unsigned char *s2 = (const unsigned char *) p2;
  unsigned char c1, c2;

  do
  {
     c1 = (unsigned char) *s1++;
     c2 = (unsigned char) *s2++;
     if (c1 == '\0')
        return c1 - c2;
  }
  while (c1 == c2);

  return c1 - c2;
}
```

Good Meltdown & Spectre lecture:

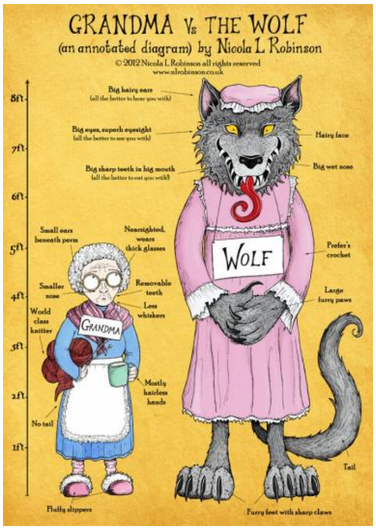
https://www.youtube.com/watch?v=UTHkYa3YQjA

Authentication

- Who are you? (Prove it!)
- Hard for others to fake
- Basis for deciding what you're allowed

Authentication methods

- Something you know
  - Password
- Something you have
  - Token
- Something you are
  - Biometrics
- Two factor authentication
  - ATM card and pin


GRANDMA Vs THE WOLF
(an annotated diagram) by Nicola L Robinson
© 2012 Nicola L Robinson all rights reserved
www.nlrobinson.co.uk
Big hairy ears (all the better to hear you with)
Big eyes, superb eyesight (all the better to see you with)
Big sharp teeth in big mouth (all the better to eat you with)
Hairy face
Big wet nose
Small ears beneath perm
Nearsighted, wears thick glasses
Smaller nose
Removable teeth
Less whiskers
World class knitter
GRANDMA
WOLF
Prefer's crochet
Large furry paws
Mostly hairless hands
No tail
Tail
Fluffy slippers
Furry feet with sharp claws
8ft
7ft
6ft
5ft
4ft
3ft
2ft
1ft

http://businessboomcollective.com/0821/nicola-lrobinson/

9

Passwords

- Most popular approach
- Free, easy to distribute and change
- Needs to be:
  - Easy to remember to be useful
  - Hard to guess (random) to be secure

10

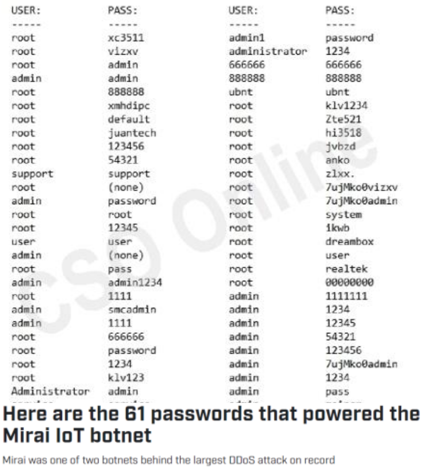
Humans cause failures!

Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)

Passwords practical problems

https://goo.gl/UFf9ba

- 8 letters and 256 characters give 2^{64}, no?
- NO, dictionary attacks!
- Try:
  - – Common
  - – Dictionary
  - – All possible
- John The Ripper will automate this for you



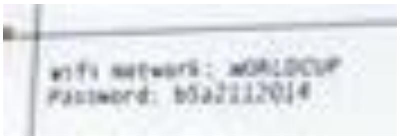
```
USER:          PASS:          USER:          PASS:
-----          -----          -----          -----
root           xc3511         admin1         password
root           vizxv          administrator  1234
root           admin          666666         666666
admin          admin          888888         888888
root           888888         ubnt           ubnt
root           xmhdipc        root           klv1234
root           default        root           Zte521
root           juantech       root           hi3518
root           123456         root           jvbzd
root           54321          root           anko
support        support        root           zlxx.
root           (none)         root           7ujMko0vizxv
admin          password       root           7ujMko0admin
root           root           root           system
root           12345          root           ikwb
user           user           root           dreambox
admin          (none)         root           user
root           pass           root           realtek
admin          admin1234      root           00000000
root           1111           admin          1111111
admin          smcadmin       admin          1234
admin          1111           admin          12345
root           666666         admin          54321
root           password       admin          123456
root           1234           admin          7ujMko0admin
root           klv123         admin          1234
Administrator  admin          admin          pass
```

Here are the 61 passwords that powered the Mirai IoT botnet

Mirai was one of two botnets behind the largest DDoS attack on record

Passwords, good and bad

- Users will pick a weak password
- Generate a strong one and they will stick it to the monitor
- Force them to change it and they will use the old one
- And use the same one for many apps!
- And will share good ones with colleagues!

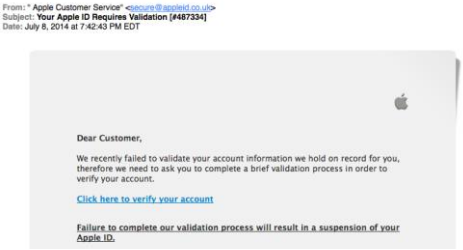


https://twitter.com/apbarros/status/481157619261116416

13

Attacks on passwords

- One weak account is enough to penetrate the network
- Phishing attacks are effective
- Default passwords
- Key loggers
- Passwords reuse
- Social engineering



From: " Apple Customer Service" <secure@appleid.co.uk>
Subject: **Your Apple ID Requires Validation [#487334]**
Date: July 8, 2014 at 7:42:43 PM EDT

Dear Customer,

We recently failed to validate your account information we hold on record for you, therefore we need to ask you to complete a brief validation process in order to verify your account.

Click here to verify your account

Failure to complete our validation process will result in a suspension of your Apple ID.

14

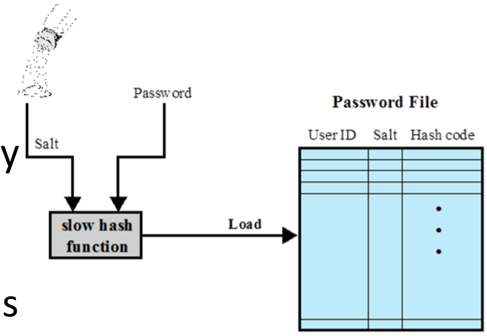
Passwords verification

- Store the password in the clear?
  - Single Point Of Failure
- Storing **<u>hashes</u>** instead
- Precomputed hashes of dictionary!
  - One-time job automates the attack

15

Adding a grain of salt

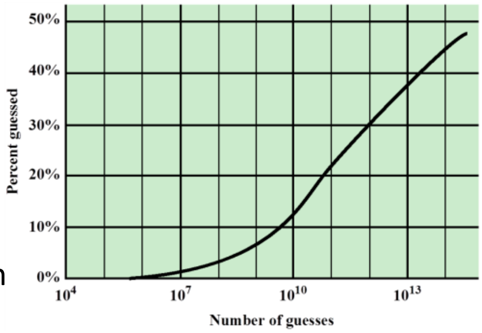
- Choose random salt s and compute $y = h(\text{password} \mid s)$ and store (s, y) in the password file
- No offline dictionary attacks!
  - 128 bits of salt in Open BSD
- Salt hides duplicates
- Slow hash function



16

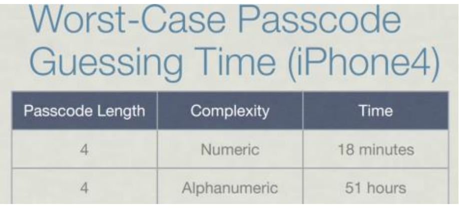
Password cracking

- Huge rainbow tables (precomputed small salts)
  - Win 2003: use 1.4G, break in 13sec
- Using GPU (and the cloud)
- Beyond the dictionary:
  - Password generation algorithms
  - Leaked passwords analysis



Preventing passwords attacks

- Lock-up or slow down after few failed password attempts
  - Better to cause inconvenience than to let guessing
- Non-computer interface prevents brute force
  - You can't automate it
  - (Make sure there's no API to do that)



Worst-Case Passcode Guessing Time (iPhone4)

Passcode Length	Complexity	Time
4	Numeric	18 minutes
4	Alphanumeric	51 hours

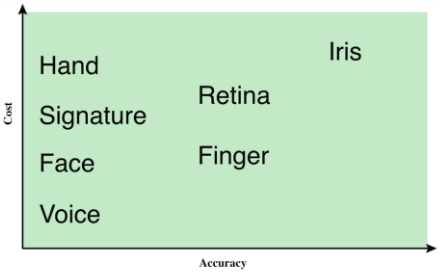
Biometry

- People use this for a long time:
  - Mother's voice
  - Passport picture
  - (Cats use this too 😆)
- You're your authenticator
  - Face recognition
  - Fingerprint
  - Form of palm
  - Retina/iris scan
  - Voice
  - Activity patterns: handwriting, typing, walk

Biometry requirements

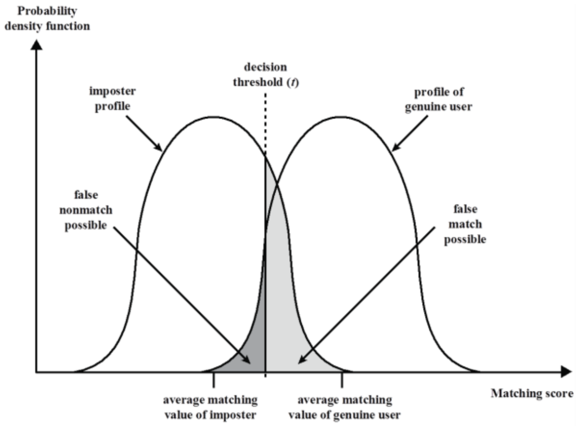
- Universal
  - Guitar player's fingerprints?
- Distinguishing
- Permanent
- Usable
  - Reliable
  - Robust
  - Collectable/User friendly
- Identification vs. verification

https://flic.kr/p/7zhv3Q



Biometry precision

- Unlike passwords: probability of matching
- Precision: detecting false positives and negatives



Biometry challenges

- Spoofable
  - Need to verify it came from person
- Securely storing the measurement
- Can't change!

Tokens

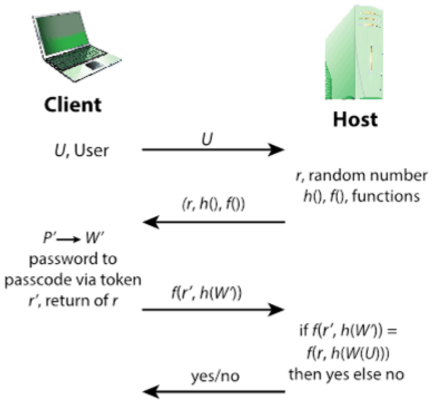
- Key is the classical token
- King’s seal is another
- Passive - Magnetic cards
  - If it gets stolen?
    - Combine with PIN
  - Needs a reader
  - Can be reprogrammed

Smart cards

- Embedded microprocessor
- Contact/contactless interface to the reader
- Authentication protocol
  - Static
  - Password generator
  - Challenge-Response
- Can be reversed
- Relatively expensive

Challenge Response with Token

- Protects from:
  - Server-side breach
  - Eavesdropping
  - Replay
- User sends identity
- User password transformed by token – never exposed
- Hash never exposes the password to the server
- Random (nonce) prevents replay attack

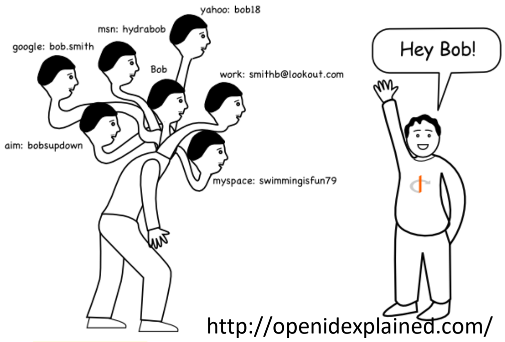


(b) Protocol for a token

25

Identity Federation/SSO

- How do you authenticate users from different organization/site?
  - Technology, standards, policies, processes to allow trust identities from other org
- Single Sign On – authentication within same organization



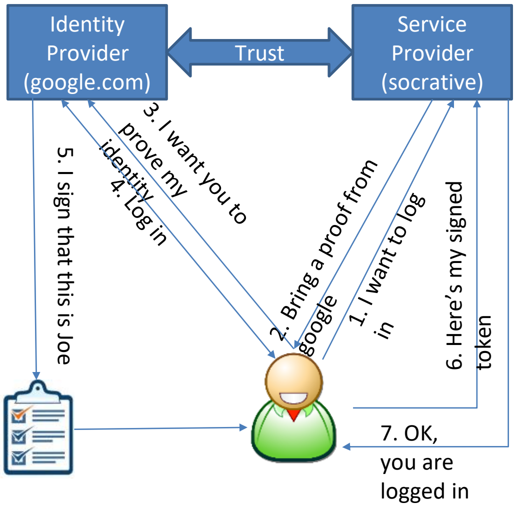
http://openidexplained.com/

○ Cancel OpenID login

26

Identity Federation

- Advantages:
  - 1 password to remember
  - Faster log in
  - More secure
  - 1 identity
- Involves
  - Identity Provider
  - Relying Party (Service Provider)
  - Token/Claim



Identity Provider (google.com)

Trust

Service Provider (socrative)

1. I want to log in

2. Bring a proof from google

3. I want you to prove my identity

4. Log in

5. I sign that this is Joe

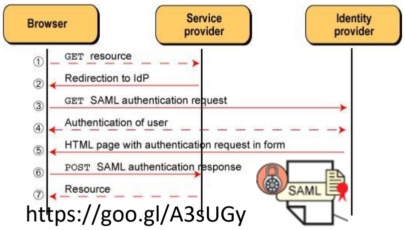
6. Here's my signed token

7. OK, you are logged in

27

Federated Access Technologies

- SAML – Security Assertion Markup Language
  - XML format for authentication and authorization
- OAuth – protocol for authorization delegation
  - Can access shared photos on Facebook for the next 10 minutes
- OpenID Connect
  - Lightweight authentication and authorization protocol


Browser
Service provider
Identity provider
① GET resource
② Redirection to IdP
③ GET SAML authentication request
④ Authentication of user
⑤ HTML page with authentication request in form
⑥ POST SAML authentication response
⑦ Resource
SAML

https://goo.gl/A3sUGy

http://goo.gl/Ta5v73

http://goo.gl/ayztik

28

Questions?

https://flic.kr/p/pqiJNt

29

Terms learnt (2)

- Covert channel
- Two Factor Authentication
- Dictionary Attacks
- Key Loggers
- Salt

- Rainbow Tables
- Biometry
- Smart Card
- Token
- Challenge/Response
- Replay Attack
- Nonce
- Identity Federation
- SSO, SAML, OAuth

30

30

Summary

- Covert channels bypass traditional policies
- Authentication - Prove who you are
- Something you know, you have, you are
- Humans can’t remember good passwords!
- Challenge-Response and Federated Identity for distributed systems

31