Authentication and Access Control

CS-576 Systems Security

Instructor: Georgios Portokalidis

Spring 2018

Authentication vs Authorization

Authentication is the process of verifying an identity claimed by or for a system entity.

Authorization is the function of specifying access rights to resources related to information security and computer security in general and to **access control** in particular.

Means/Factors of Authentication

- Something the individual knows
- Something the individual possesses
- Something the individual is/does

Something the User Knows

Password

As56kf#dfjd8%d

John123

JustinBieber14

Y3llow5ubm4rine

PIN

123456

654321

1248

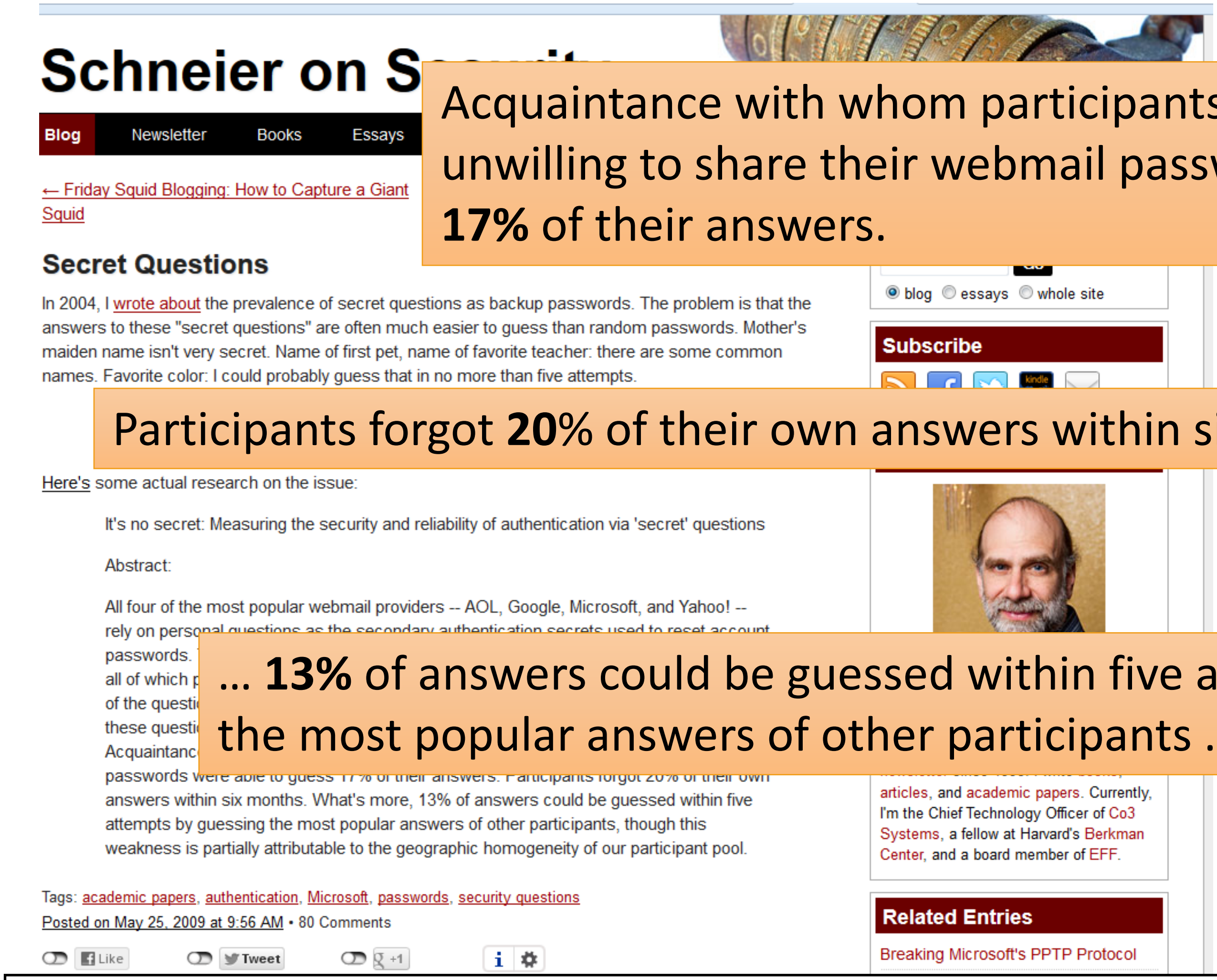
338

Answers (to questions)

What is the name of your dog?

What is your favorite color?

What... is the air-speed velocity of an unladen swallow?



Schneier on S

← Friday Squid Blogging: How to Capture a Giant Squid

Secret Questions

In 2004, I wrote about the prevalence of secret questions as backup passwords. The problem is that the answers to these "secret questions" are often much easier to guess than random passwords. Mother's maiden name isn't very secret. Name of first pet, name of favorite teacher: there are some common names. Favorite color: I could probably guess that in no more than five attempts.

Here's some actual research on the issue:

> It's no secret: Measuring the security and reliability of authentication via 'secret' questions
>
> Abstract:
>
> All four of the most popular webmail providers -- AOL, Google, Microsoft, and Yahoo! -- rely on personal questions as the secondary authentication secrets used to reset account passwords. all of which p of the questi these questi Acquaintanc passwords were able to guess 17% of their answers. Participants forgot 20% of their own answers within six months. What's more, 13% of answers could be guessed within five attempts by guessing the most popular answers of other participants, though this weakness is partially attributable to the geographic homogeneity of our participant pool.

Tags: academic papers, authentication, Microsoft, passwords, security questions

Posted on May 25, 2009 at 9:56 AM • 80 Comments

○ blog ○ essays ○ whole site

Subscribe

articles, and academic papers. Currently, I'm the Chief Technology Officer of Co3 Systems, a fellow at Harvard's Berkman Center, and a board member of EFF.

Related Entries

Breaking Microsoft's PPTP Protocol

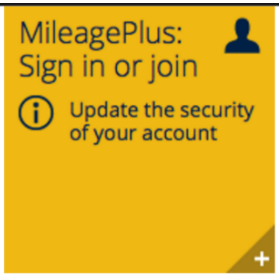
Acquaintance with whom participants reported being unwilling to share their webmail passwords were able to guess **17%** of their answers.

Participants forgot **20%** of their own answers within six months.

… **13%** of answers could be guessed within five attempts by guessing the most popular answers of other participants …

It's no secret: Measuring the security and reliability of authentication via 'secret' questions

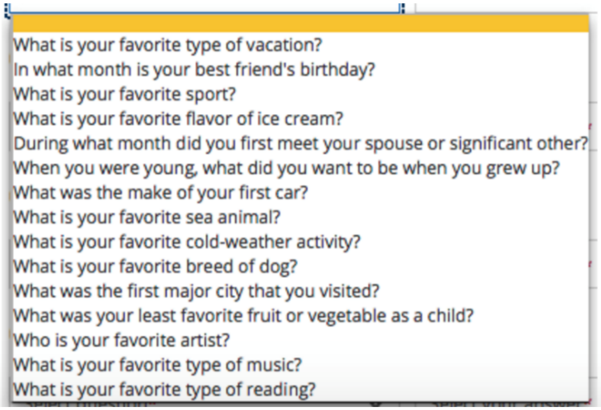
http://research.microsoft.com/apps/pubs/default.aspx?id=79594



United Mileage Plus

Yesterday, Yan Zhu (@bcrypt) pointed out on Twitter that United Airlines Mileage Plus program has started collecting answers to security questions. They have a new twist: you must select one of a menu of answers.

United wants the answers to five questions, chosen from a list:



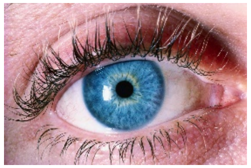
What is your favorite type of vacation?
In what month is your best friend's birthday?
What is your favorite sport?
What is your favorite flavor of ice cream?
During what month did you first meet your spouse or significant other?
When you were young, what did you want to be when you grew up?
What was the make of your first car?
What is your favorite sea animal?
What is your favorite cold-weather activity?
What is your favorite breed of dog?
What was the first major city that you visited?
What was your least favorite fruit or vegetable as a child?
Who is your favorite artist?
What is your favorite type of music?
What is your favorite type of reading?

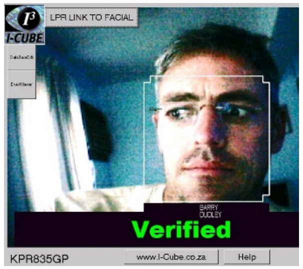
Something the User Possesses

SMART CARD
07/17

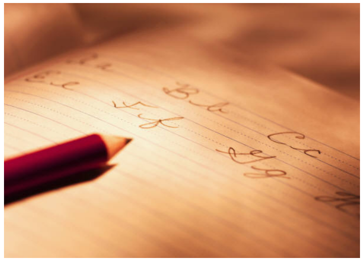
Something the Individual…

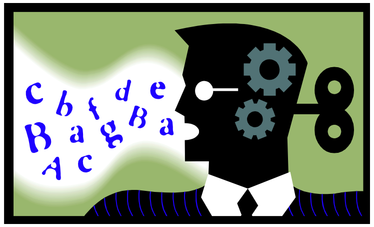
..Is





..does



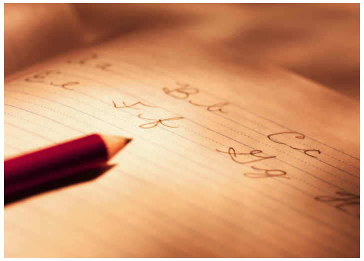


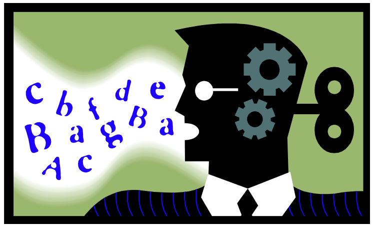
Something the Individual…

..Is

NOT just face recognition

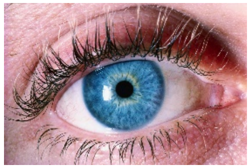
..does

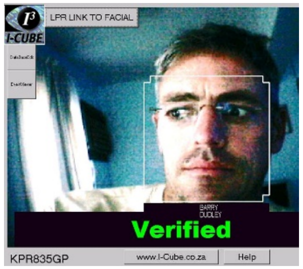




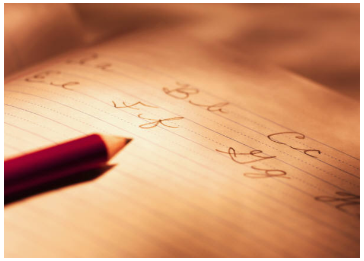
Something the Individual…

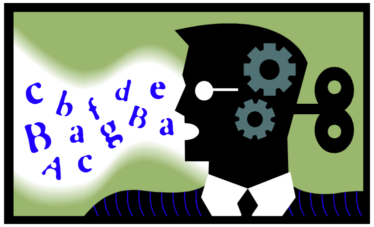
..Is





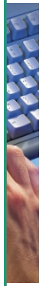
..does

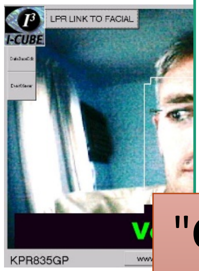




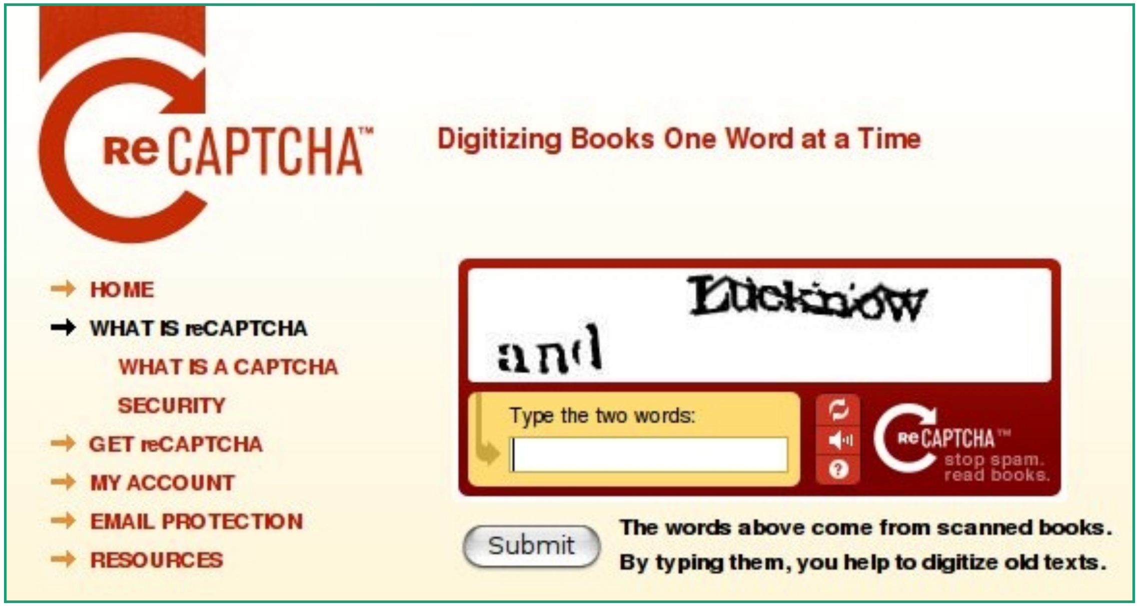
Something the Individual…

..Is





How about CAPTCHA?



reCAPTCHA™ Digitizing Books One Word at a Time

- HOME
- WHAT IS reCAPTCHA
  - WHAT IS A CAPTCHA
  - SECURITY
- GET reCAPTCHA
- MY ACCOUNT
- EMAIL PROTECTION
- RESOURCES

Type the two words:

Submit

The words above come from scanned books.
By typing them, you help to digitize old texts.

"**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part"

Password Authentication

Passwords

Widely used

Process

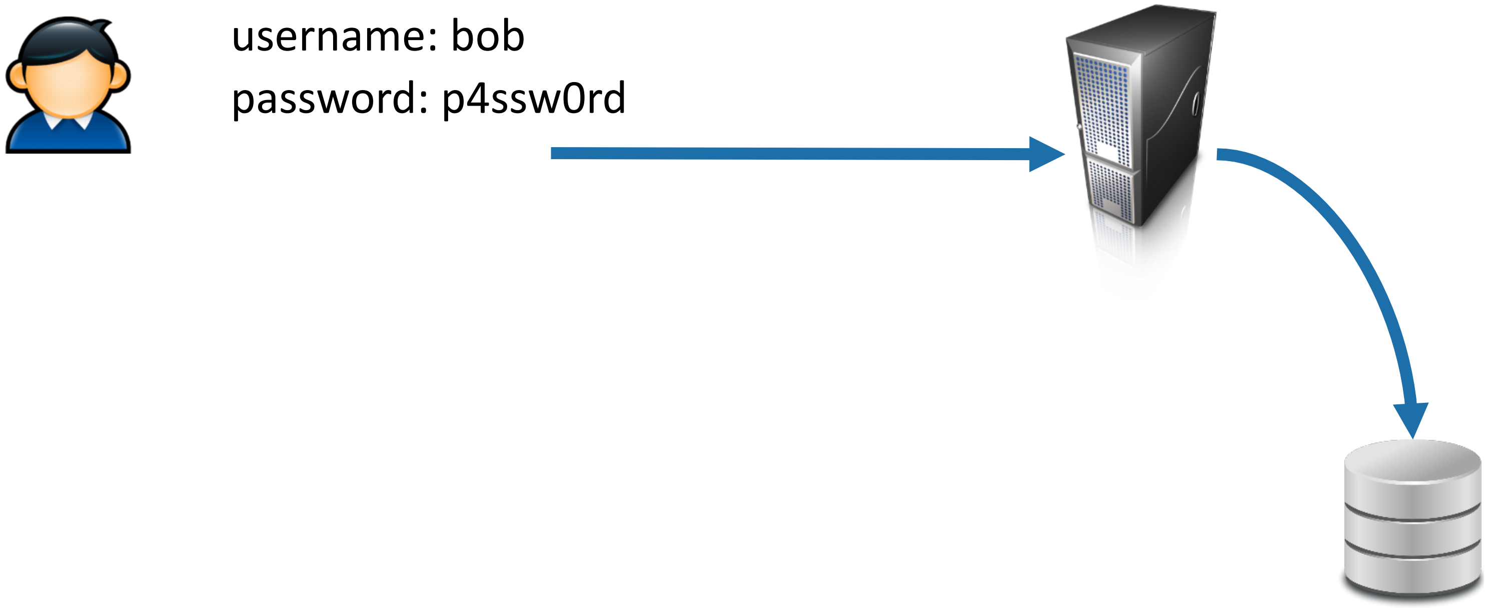
- User provides name/login and password
- System compares password with the one stored for that specified login

The user ID:

- Determines that the user is authorized to access the system
- Determines the user's privileges
- Is used in discretionary access control

Passwords Naïve Implementation

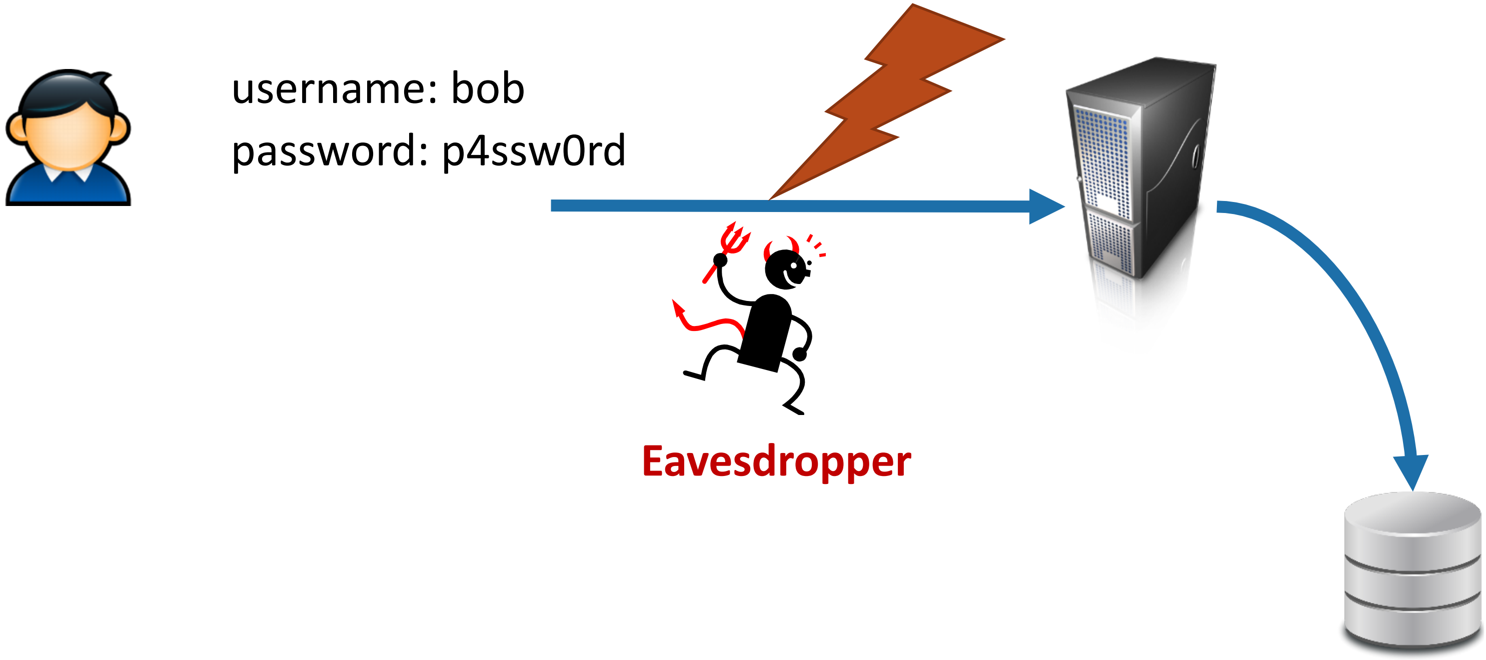
Non-confidential channel



username: bob
password: p4ssw0rd

Passwords Naïve Implementation

Non-confidential channel



username: bob

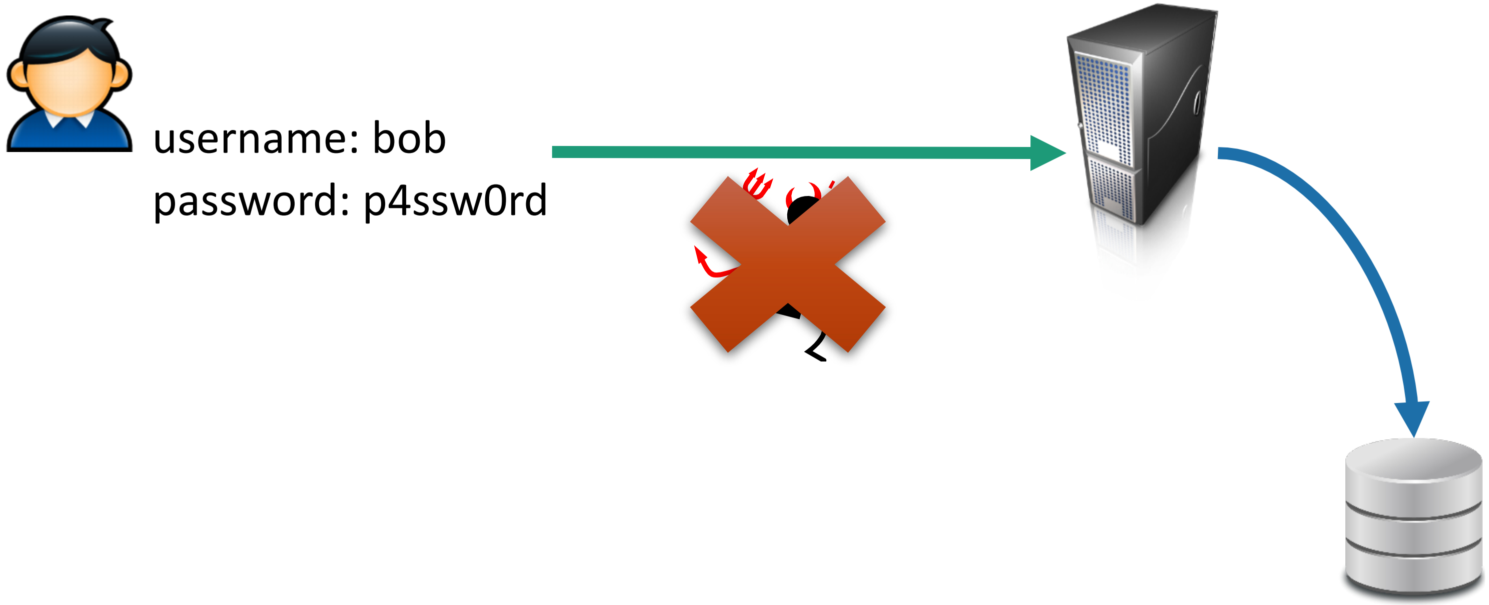
password: p4ssw0rd

Eavesdropper

Passwords Naïve Implementation

Non-confidential channel ━━━

Confidential channel ━━━

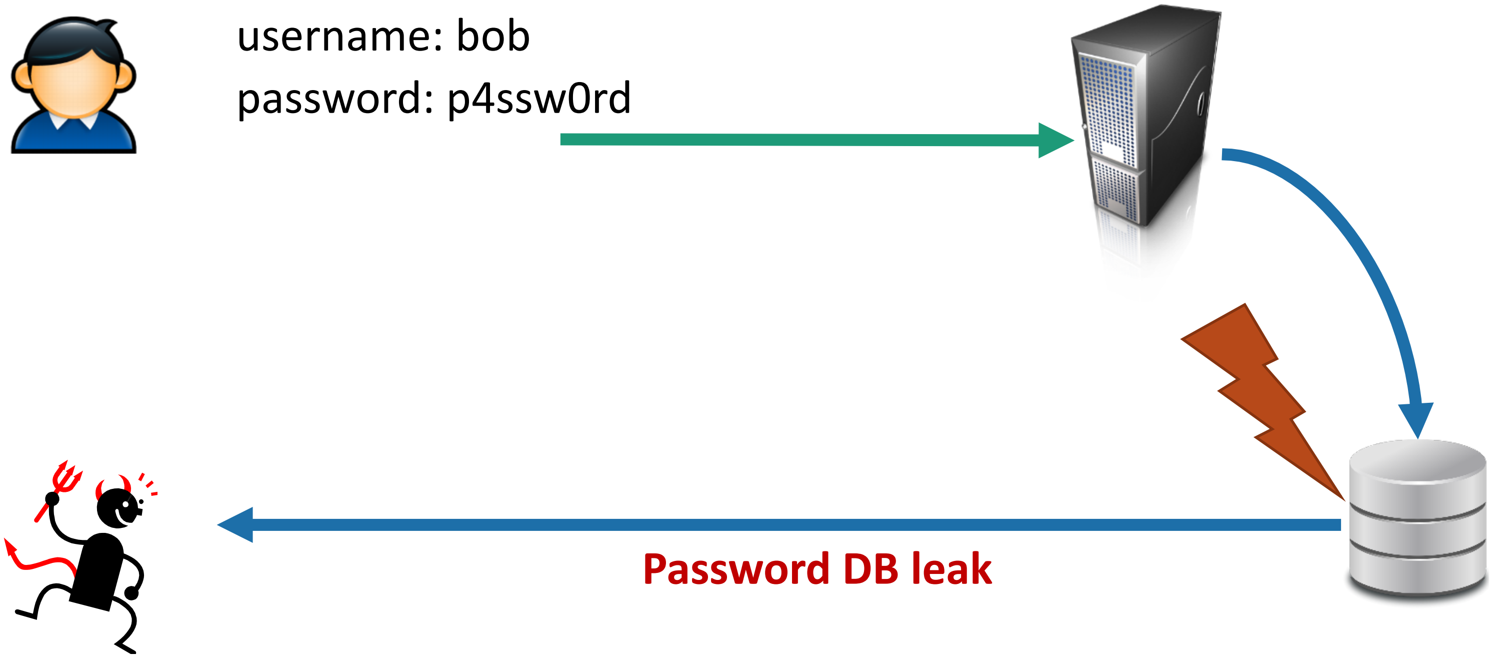


username: bob
password: p4ssw0rd

Passwords Naïve Implementation

Non-confidential channel

Confidential channel



username: bob

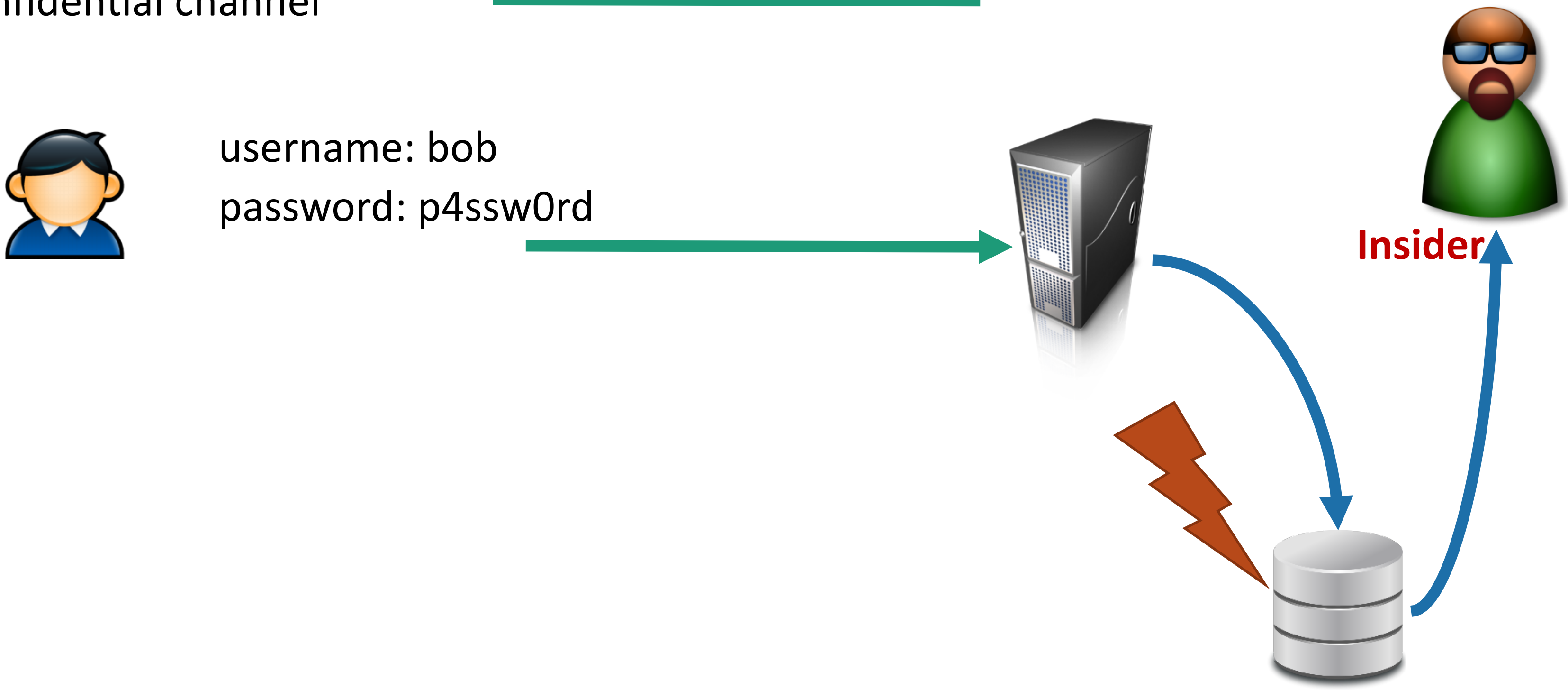
password: p4ssw0rd

Password DB leak

Passwords Naïve Implementation

Non-confidential channel 🟦

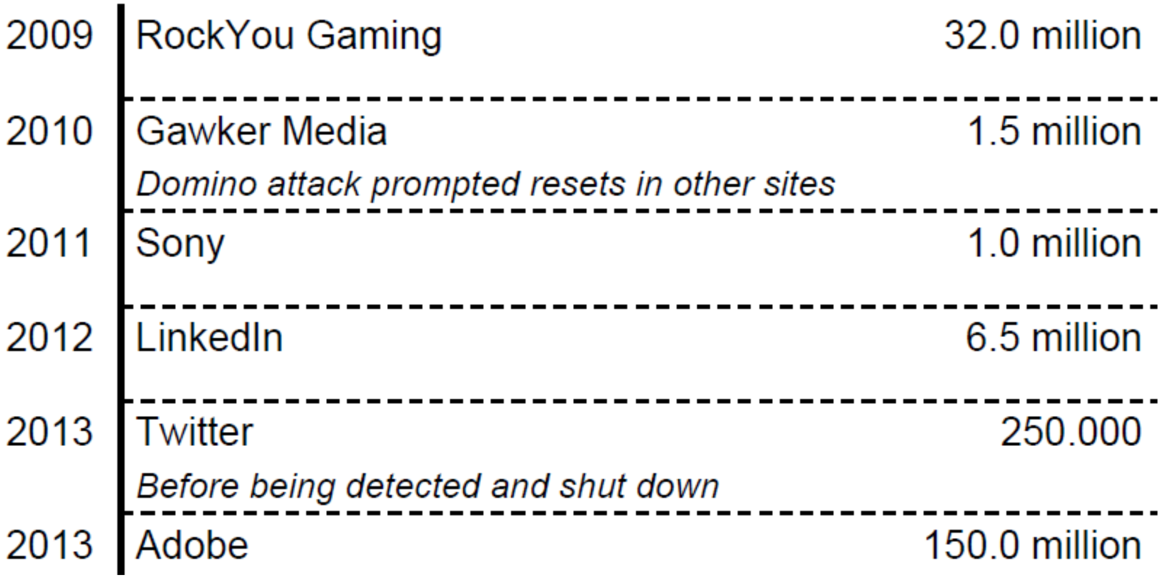
Confidential channel 🟩



username: bob

password: p4ssw0rd

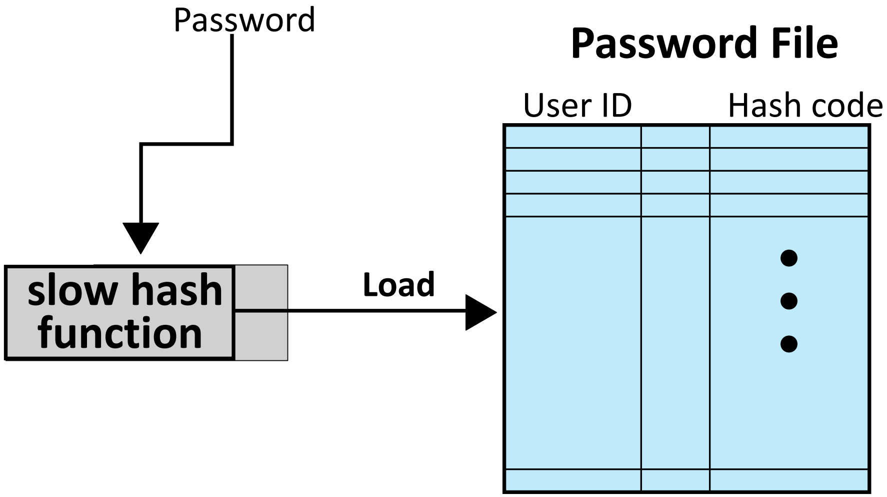
Password Leaks Happen All the Time



2009	RockYou Gaming	32.0 million
2010	Gawker Media *Domino attack prompted resets in other sites*	1.5 million
2011	Sony	1.0 million
2012	LinkedIn	6.5 million
2013	Twitter *Before being detected and shut down*	250.000
2013	Adobe	150.0 million

2015 ashley madison **15.26 million**

Hashed Passwords



Hash Function Requirements

Can be applied to a block of data of any size

Produces a fixed-length output

H(x) is relatively easy to compute for any given x

Computationally infeasible to find x such that H(x) = h

Computationally infeasible to find

y ≠ x such that H(y) = H(x)

Computationally infeasible to find

any pair (x,y) such that H(x) = H(y)

Security of Hash Functions

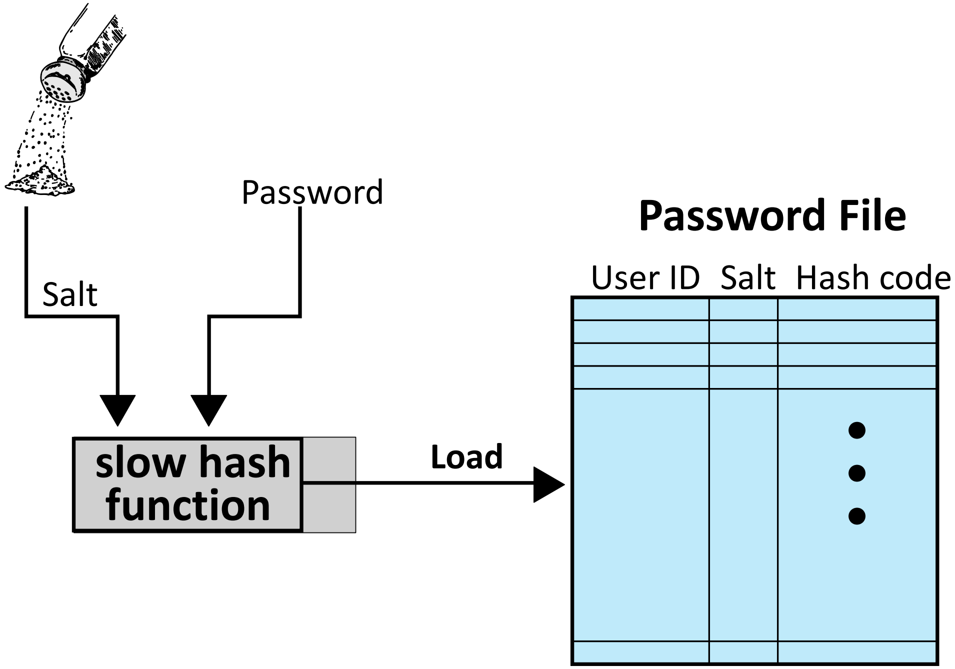
There are two approaches to attacking a secure hash function:

- **Cryptanalysis:** Exploit logical weaknesses in the algorithm
- **Brute-force attack:** Strength of hash function depends solely on the length of the hash code produced by the algorithm

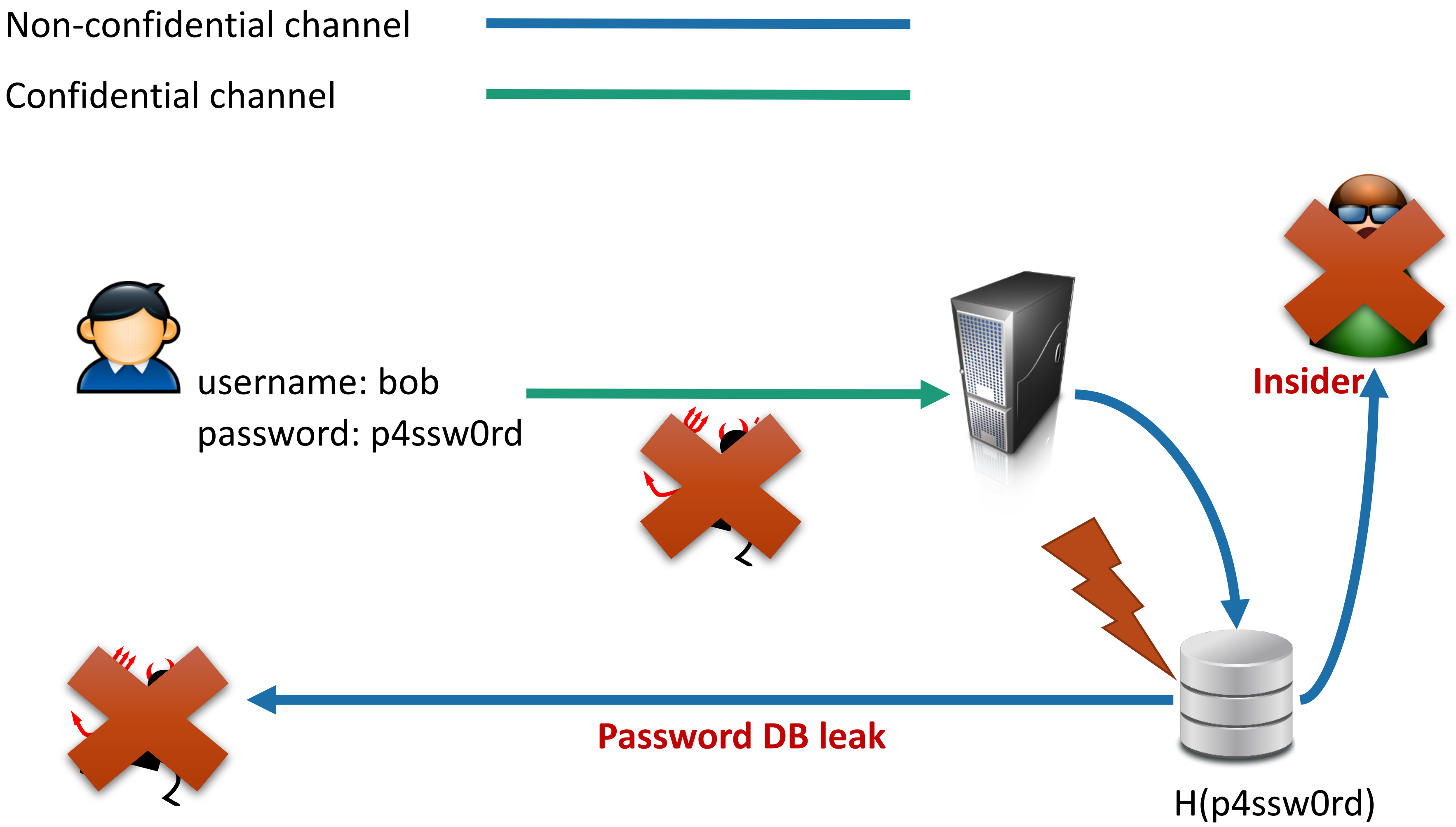
MD5 and SHA-1 have been broken through cryptanalisys

SHA-2 or later is suggested

Adding Salt


Password
Salt
Password File
User ID
Salt
Hash code
slow hash function
Load

Hashed Passwords Today



Non-confidential channel

Confidential channel

username: bob
password: p4ssw0rd

Insider

Password DB leak

H(p4ssw0rd)

Password Cracking

Dictionary attacks

Brute-force

Combination of the above

John the Ripper – first open-source password cracker developed in 1996

Dictionary Attacks

Develop a large dictionary of possible passwords and try each against the password file

Each password must be hashed using each salt value and then compared to stored hash values

Good dictionaries and heuristics for combining words give attackers an advantage.

Publicly available databases of cracked passwords also help

Rainbow Table Attacks

Pre-compute tables of hash values for all salts

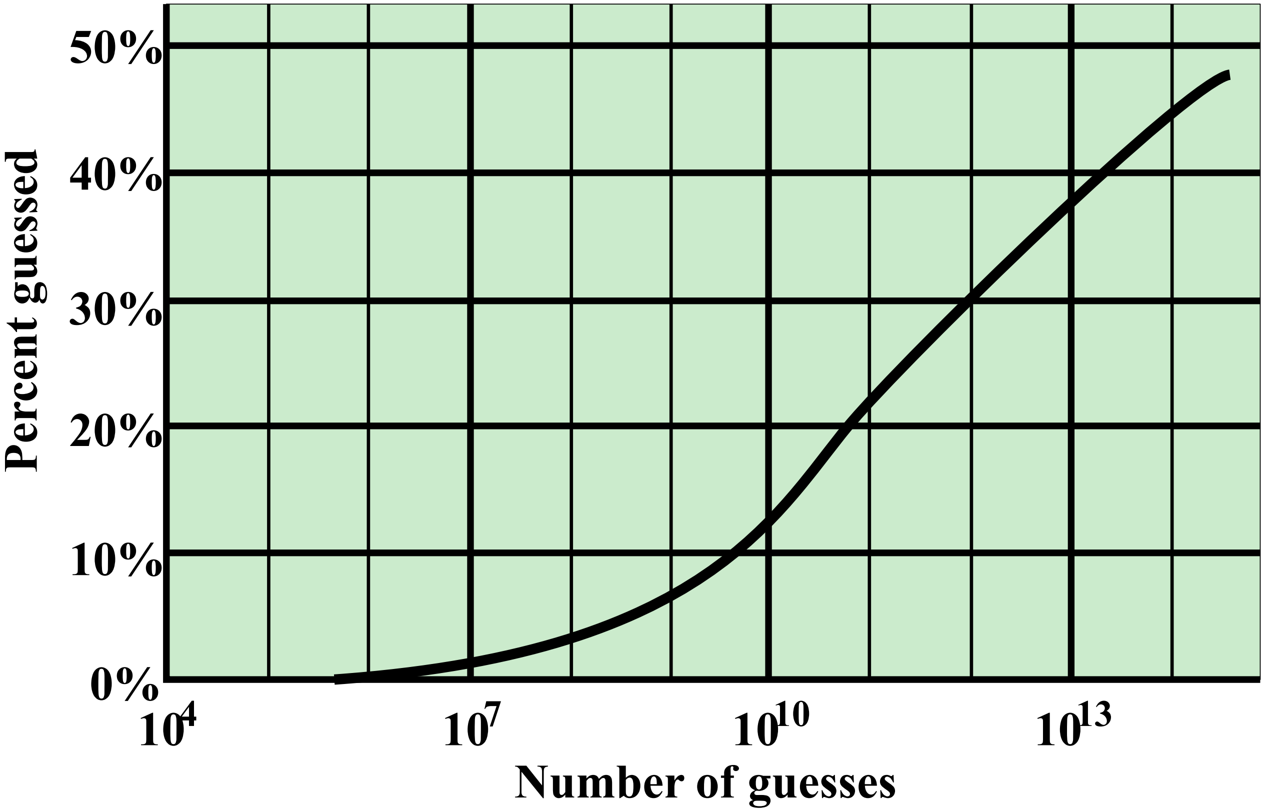
A mammoth table of hash values

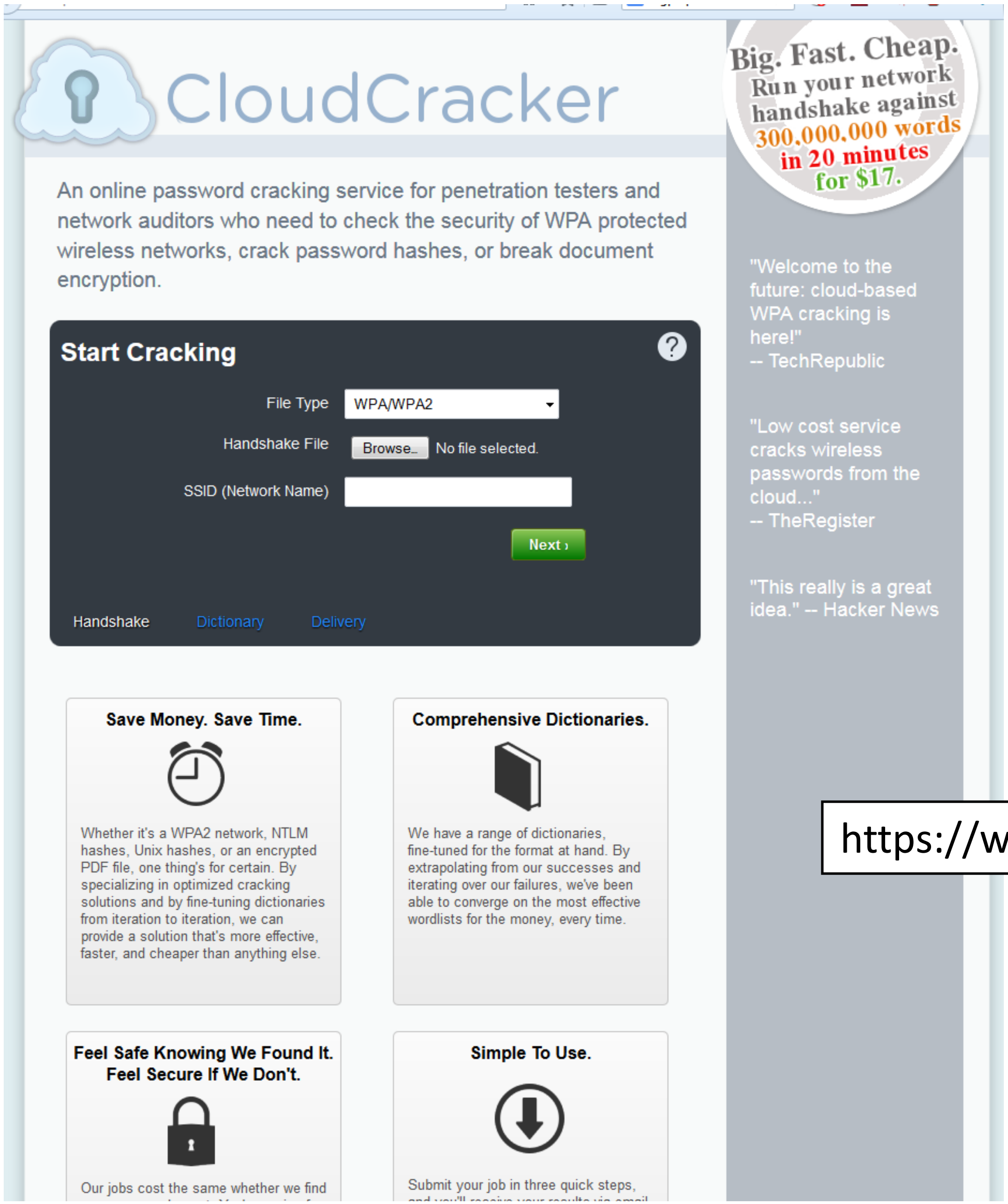
Can be countered by using a sufficiently large salt value and a sufficiently large hash length

Researchers have shown that using 1.4 GB of data, they could crack 99.9% of all alphanumeric Windows password hashes in 13.8 seconds.

Percentage of Passwords Guessed

Using DB of leaked password files, including the RockYou file.





Big. Fast. Cheap.
Run your network handshake against 300,000,000 words in 20 minutes for $17.

An online password cracking service for penetration testers and network auditors who need to check the security of WPA protected wireless networks, crack password hashes, or break document encryption.

Start Cracking

File Type: WPA/WPA2

Handshake File: Browse... No file selected.

SSID (Network Name):

"Welcome to the future: cloud-based WPA cracking is here!"
-- TechRepublic

"Low cost service cracks wireless passwords from the cloud..."
-- TheRegister

"This really is a great idea." -- Hacker News

Save Money. Save Time.

Whether it's a WPA2 network, NTLM hashes, Unix hashes, or an encrypted PDF file, one thing's for certain. By specializing in optimized cracking solutions and by fine-tuning dictionaries from iteration to iteration, we can provide a solution that's more effective, faster, and cheaper than anything else.

Comprehensive Dictionaries.

We have a range of dictionaries, fine-tuned for the format at hand. By extrapolating from our successes and iterating over our failures, we've been able to converge on the most effective wordlists for the money, every time.

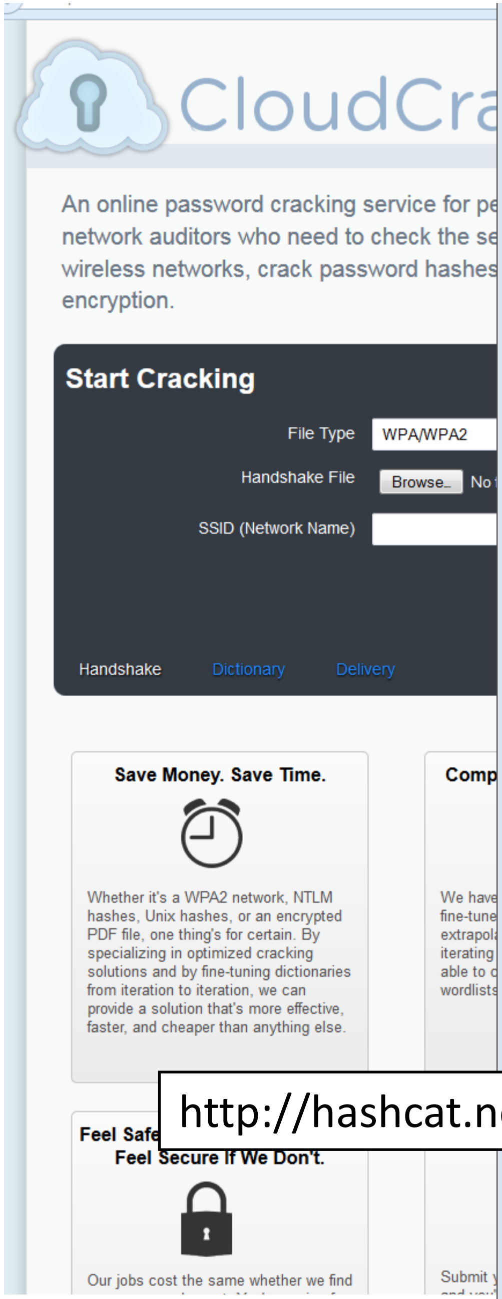
Feel Safe Knowing We Found It. Feel Secure If We Don't.

Our jobs cost the same whether we find

Simple To Use.

Submit your job in three quick steps,

https://www.cloudcracker.com/



CloudCra

An online password cracking service for pe network auditors who need to check the se wireless networks, crack password hashes encryption.

Start Cracking

File Type WPA/WPA2

Handshake File Browse... No f

SSID (Network Name)

Save Money. Save Time.

Whether it's a WPA2 network, NTLM hashes, Unix hashes, or an encrypted PDF file, one thing's for certain. By specializing in optimized cracking solutions and by fine-tuning dictionaries from iteration to iteration, we can provide a solution that's more effective, faster, and cheaper than anything else.

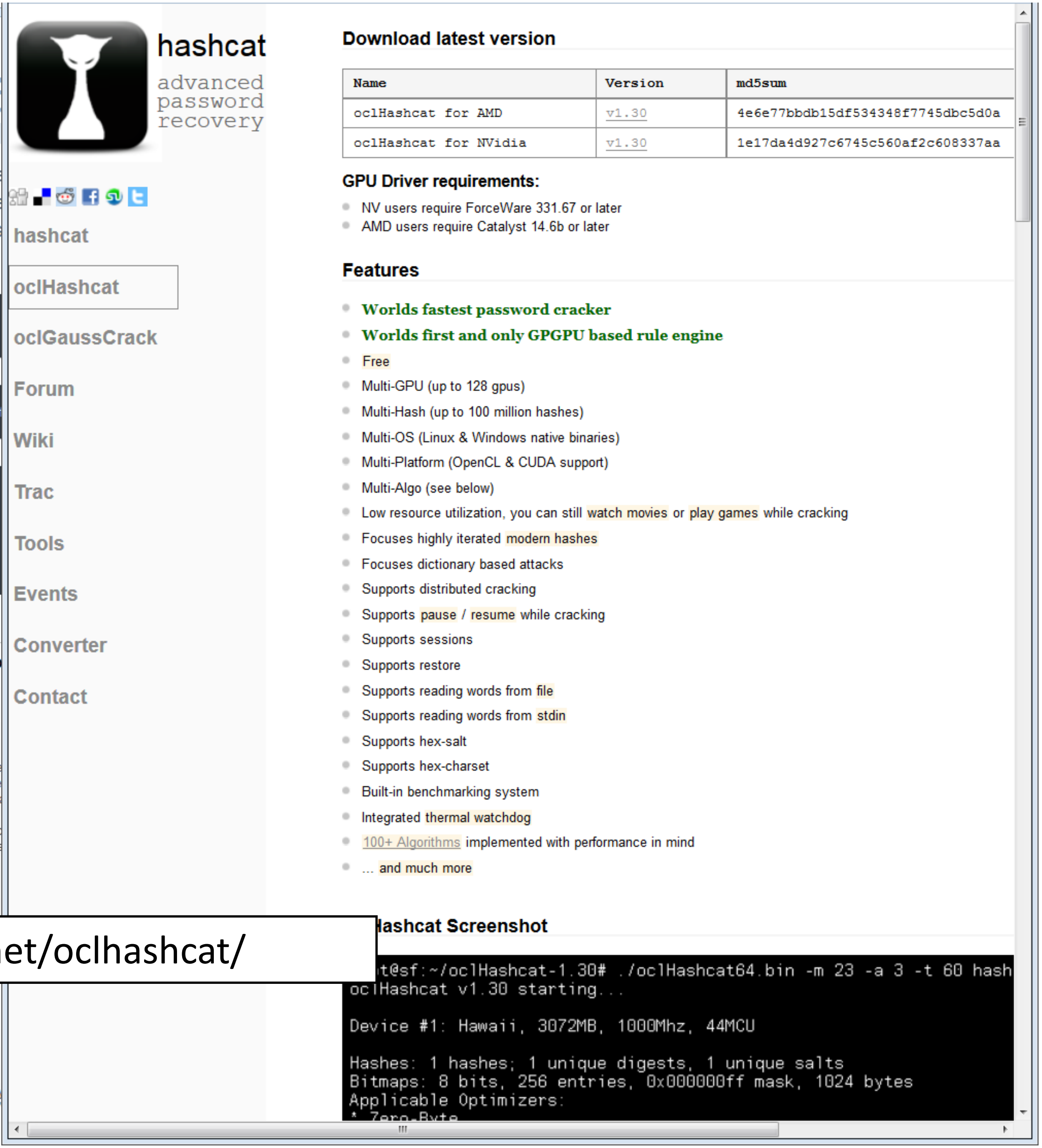
Comp

We have fine-tune extrapola iterating able to c wordlists

Feel Safe Feel Secure If We Don't.

Our jobs cost the same whether we find

Submit y



hashcat

advanced password recovery

Download latest version

Name	Version	md5sum
oclHashcat for AMD	v1.30	4e6e77bbdb15df534348f7745dbc5d0a
oclHashcat for NVidia	v1.30	1e17da4d927c6745c560af2c608337aa

GPU Driver requirements:

- NV users require ForceWare 331.67 or later
- AMD users require Catalyst 14.6b or later

Features

- **Worlds fastest password cracker**
- **Worlds first and only GPGPU based rule engine**
- Free
- Multi-GPU (up to 128 gpus)
- Multi-Hash (up to 100 million hashes)
- Multi-OS (Linux & Windows native binaries)
- Multi-Platform (OpenCL & CUDA support)
- Multi-Algo (see below)
- Low resource utilization, you can still watch movies or play games while cracking
- Focuses highly iterated modern hashes
- Focuses dictionary based attacks
- Supports distributed cracking
- Supports pause / resume while cracking
- Supports sessions
- Supports restore
- Supports reading words from file
- Supports reading words from stdin
- Supports hex-salt
- Supports hex-charset
- Built-in benchmarking system
- Integrated thermal watchdog
- 100+ Algorithms implemented with performance in mind
- ... and much more

ashcat Screenshot

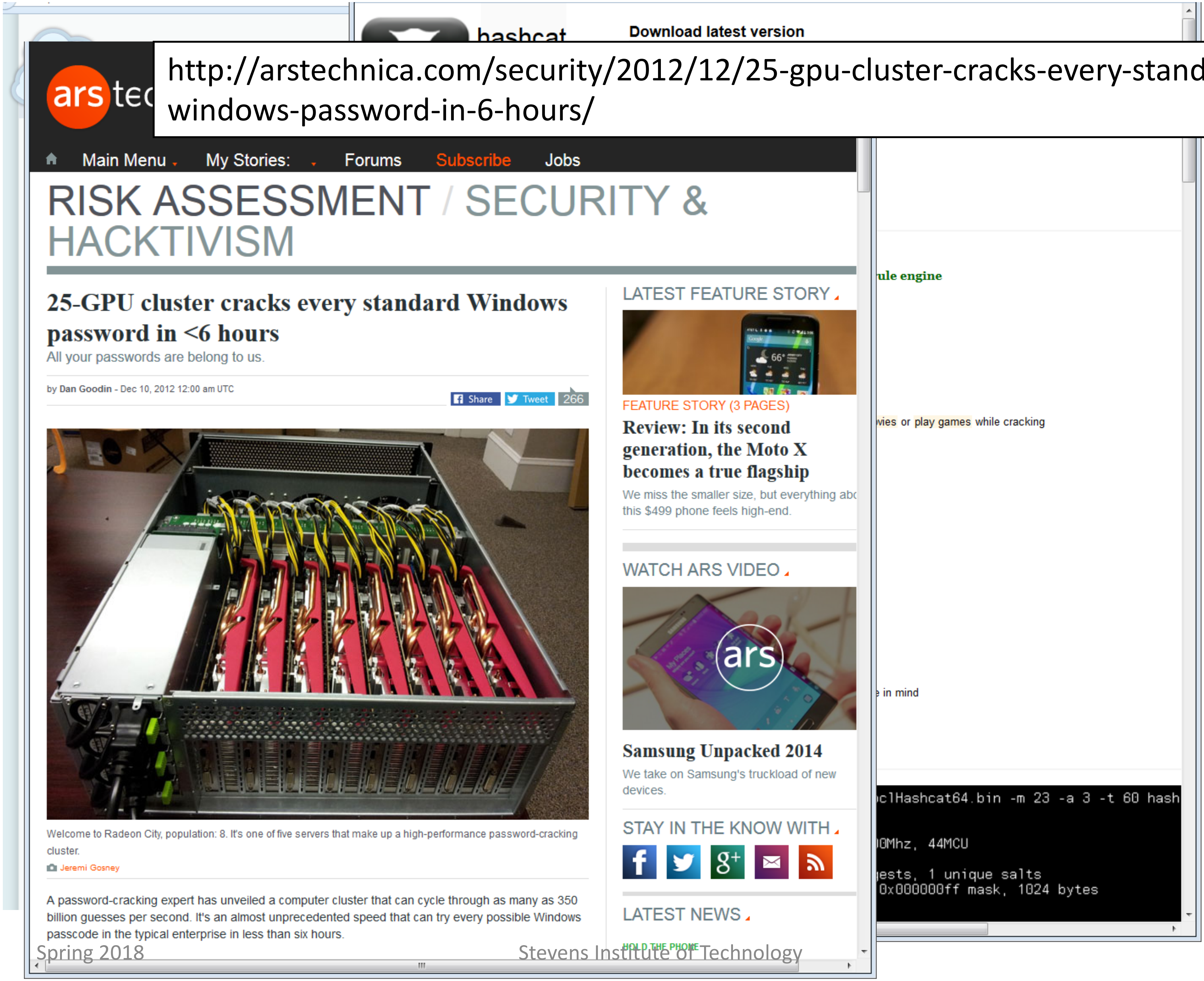
```
t@sf:~/oclHashcat-1.30# ./oclHashcat64.bin -m 23 -a 3 -t 60 hash
oclHashcat v1.30 starting...

Device #1: Hawaii, 3072MB, 1000Mhz, 44MCU

Hashes: 1 hashes; 1 unique digests, 1 unique salts
Bitmaps: 8 bits, 256 entries, 0x000000ff mask, 1024 bytes
Applicable Optimizers:
* Zero-Byte
```

http://hashcat.net/oclhashcat/

http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/



RISK ASSESSMENT / SECURITY & HACKTIVISM

25-GPU cluster cracks every standard Windows password in <6 hours

All your passwords are belong to us.

by Dan Goodin - Dec 10, 2012 12:00 am UTC

Welcome to Radeon City, population: 8. It's one of five servers that make up a high-performance password-cracking cluster.

Jeremi Gosney

A password-cracking expert has unveiled a computer cluster that can cycle through as many as 350 billion guesses per second. It's an almost unprecedented speed that can try every possible Windows passcode in the typical enterprise in less than six hours.

LATEST FEATURE STORY

FEATURE STORY (3 PAGES)

Review: In its second generation, the Moto X becomes a true flagship

We miss the smaller size, but everything abc this $499 phone feels high-end.

WATCH ARS VIDEO

Samsung Unpacked 2014

We take on Samsung's truckload of new devices.

STAY IN THE KNOW WITH

LATEST NEWS

HOLD THE PHONE

ule engine

vies or play games while cracking

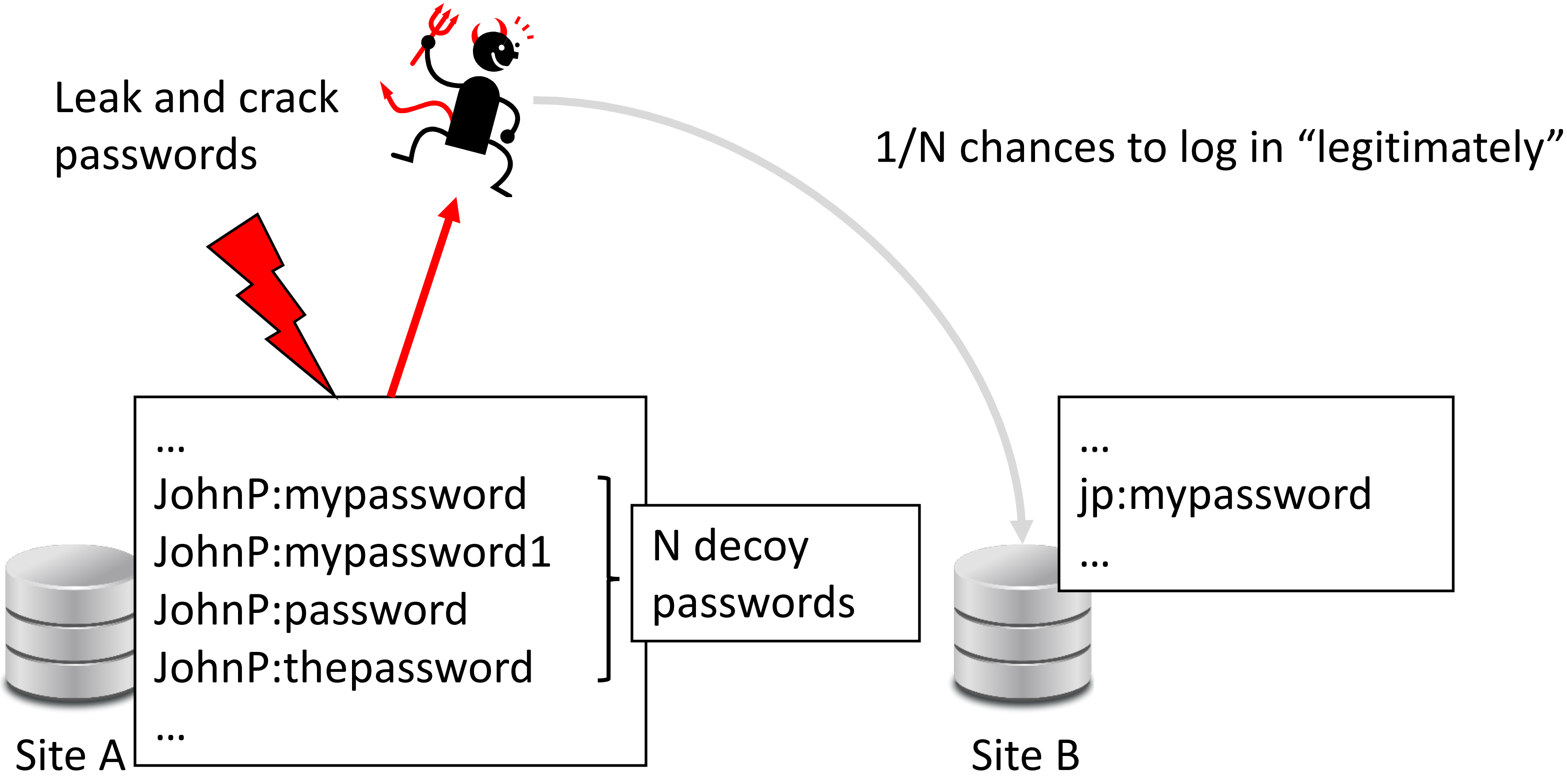
e in mind

```
clHashcat64.bin -m 23 -a 3 -t 60 hash

0Mhz, 44MCU

gests, 1 unique salts
0x000000ff mask, 1024 bytes
```

HoneyPasswords



Leak and crack passwords

1/N chances to log in “legitimately”

…
JohnP:mypassword
JohnP:mypassword1
JohnP:password
JohnP:thepassword
…

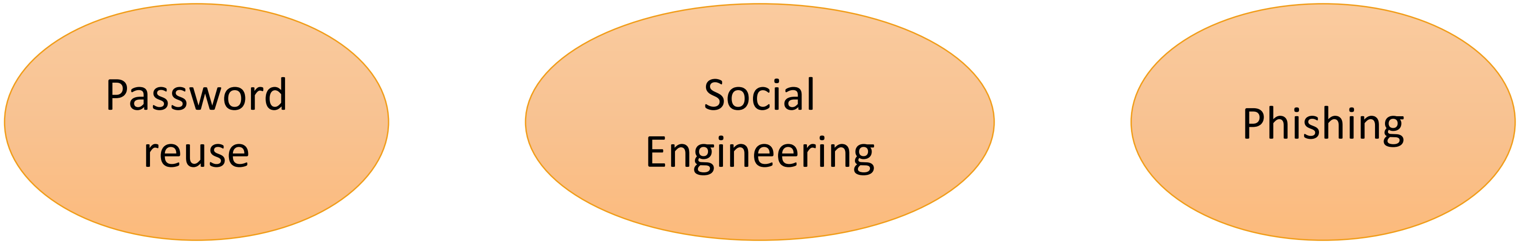
N decoy passwords

Site A

…
jp:mypassword
…

Site B

Other Threats

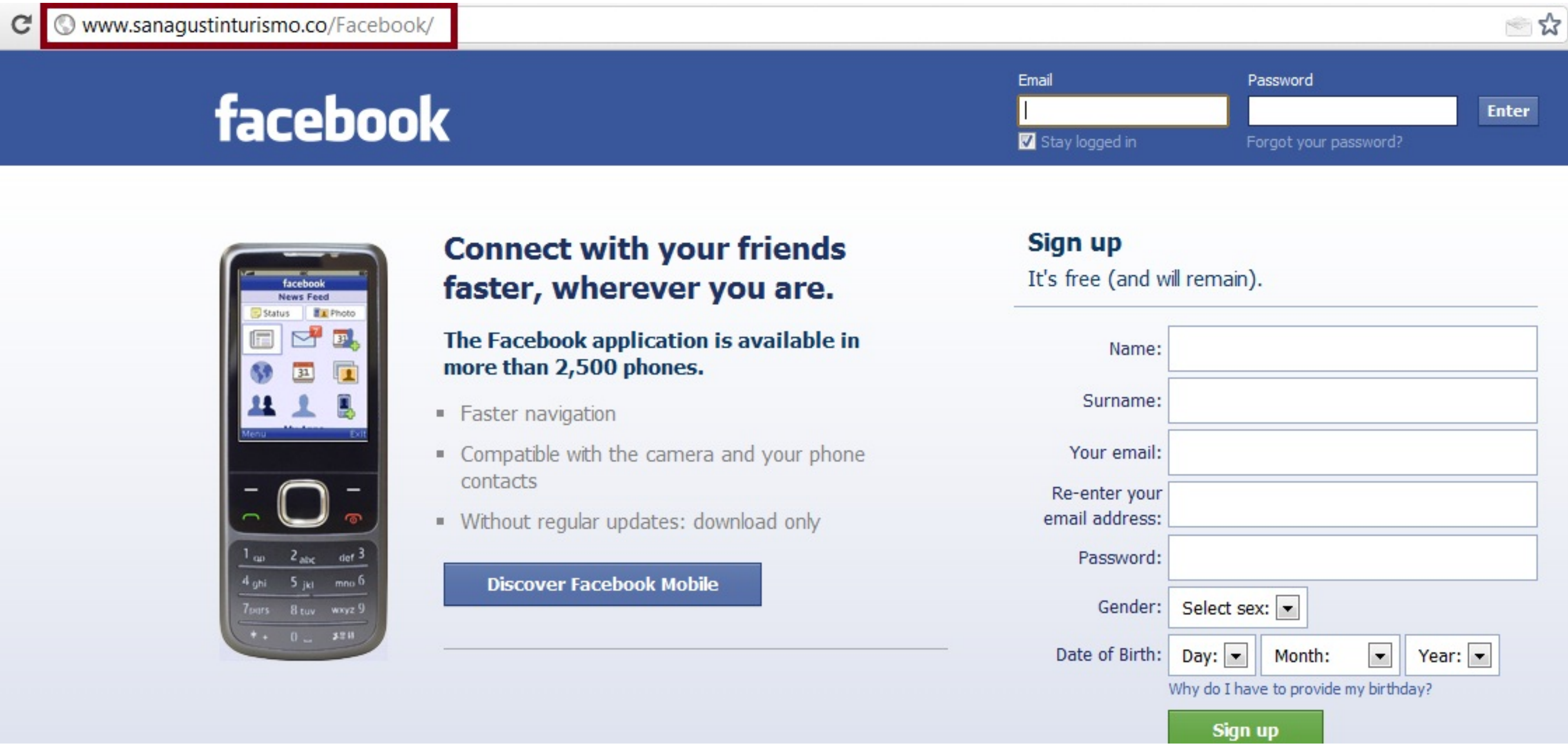


Password reuse

Social Engineering

Phishing

Phishing



www.sanagustinturismo.co/Facebook/

facebook

Email

Password

Enter

☑ Stay logged in

Forgot your password?

Connect with your friends faster, wherever you are.

The Facebook application is available in more than 2,500 phones.

- Faster navigation
- Compatible with the camera and your phone contacts
- Without regular updates: download only

Discover Facebook Mobile

Sign up

It's free (and will remain).

Name:

Surname:

Your email:

Re-enter your email address:

Password:

Gender: Select sex: ▾

Date of Birth: Day: ▾ Month: ▾ Year: ▾

Why do I have to provide my birthday?

Sign up

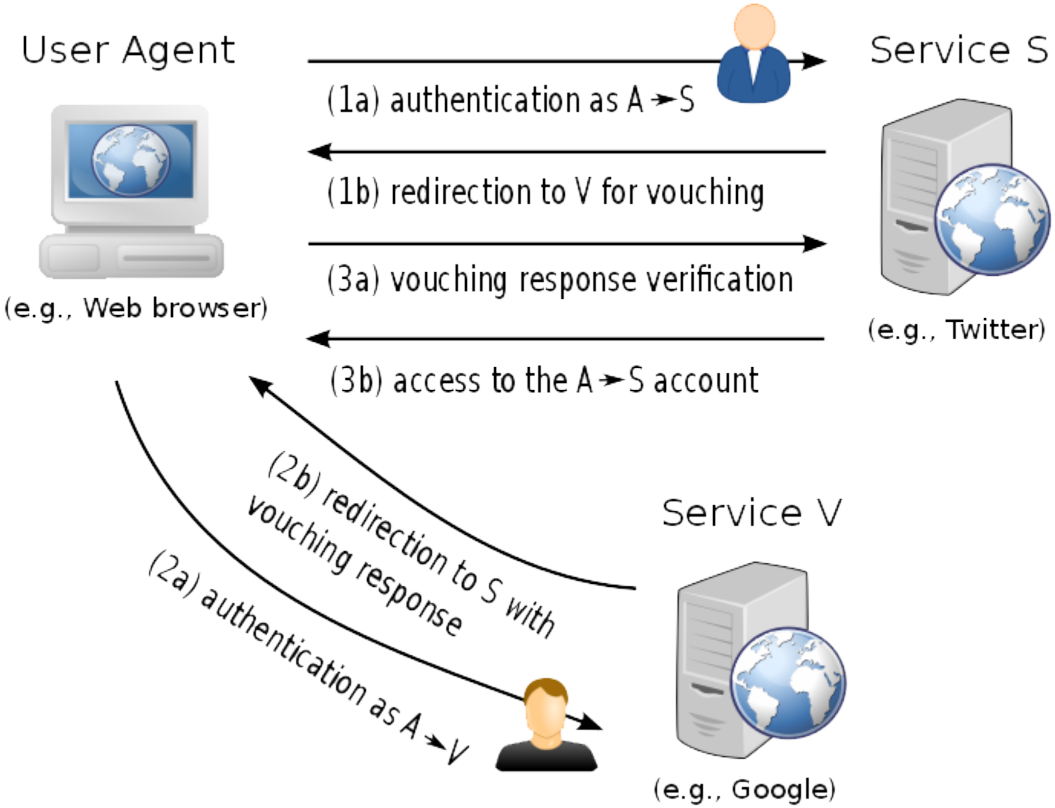
Synergistic Authentication (Sauth)

Most users login in multiple web services

…and they stay logged in

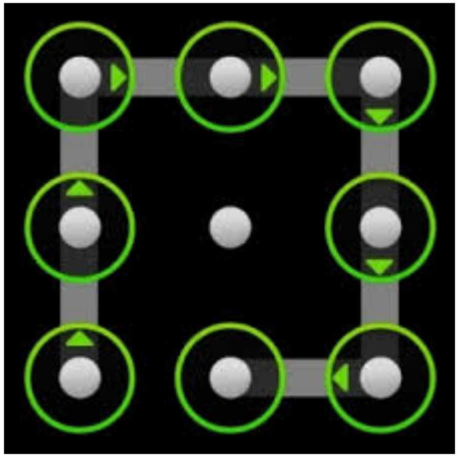
Exploit this to protect ourselves from attackers that have obtained our password

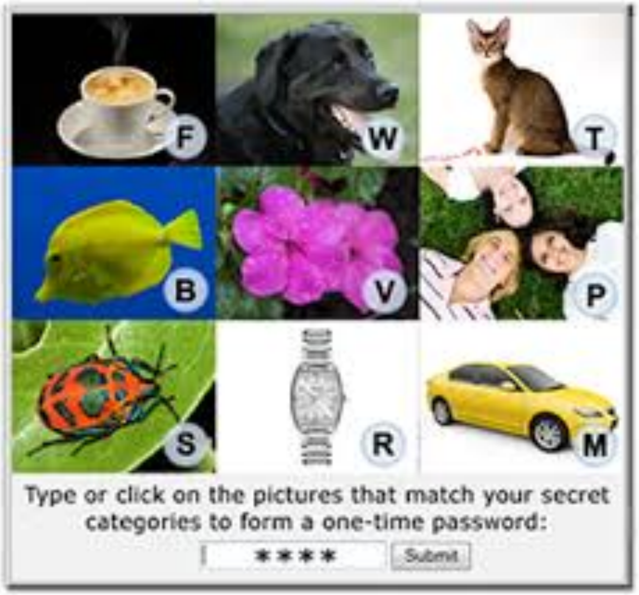
Services Can Vouch for the User


User Agent
(e.g., Web browser)
Service S
(e.g., Twitter)
Service V
(e.g., Google)
(1a) authentication as A→S
(1b) redirection to V for vouching
(3a) vouching response verification
(3b) access to the A→S account
(2b) redirection to S with vouching response
(2a) authentication as A→V

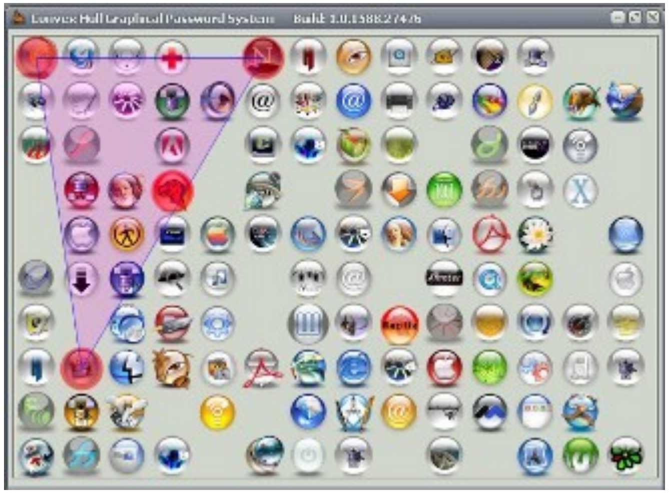
Password Alternatives

Graphical Passwords





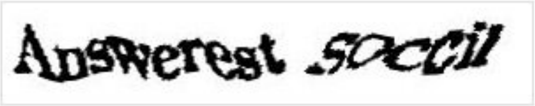
Type or click on the pictures that match your secret categories to form a one-time password:



Convex Hull Graphical Password System Build: 1.0.1588.27476

Social Authentication

Why is this hard?



Traditional captcha

Instead of showing you a tradit
verify your identity is through s
friends and ask you to name th
might know your password, but

“Social Authentication: Harder than it Looks”
https://www.cl.cam.ac.uk/~rja14/Papers/socialauthentication.pdf

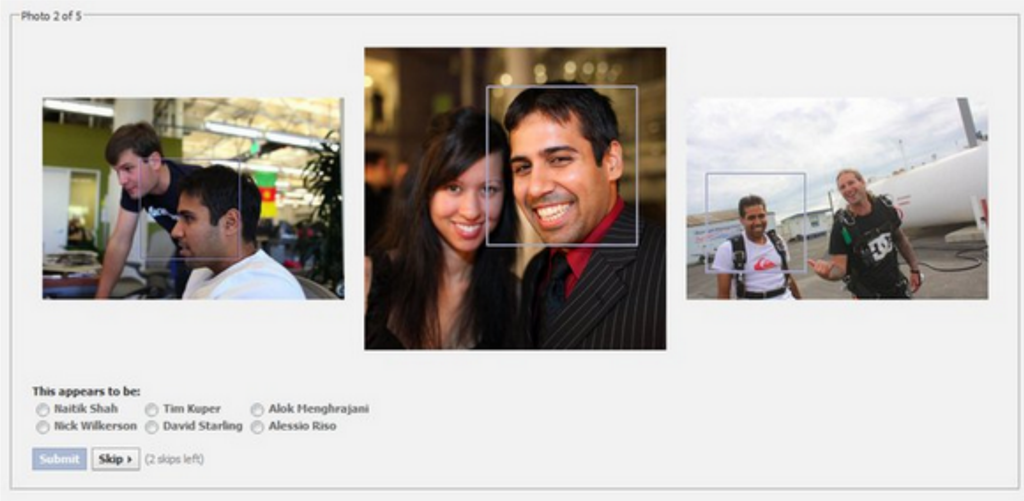


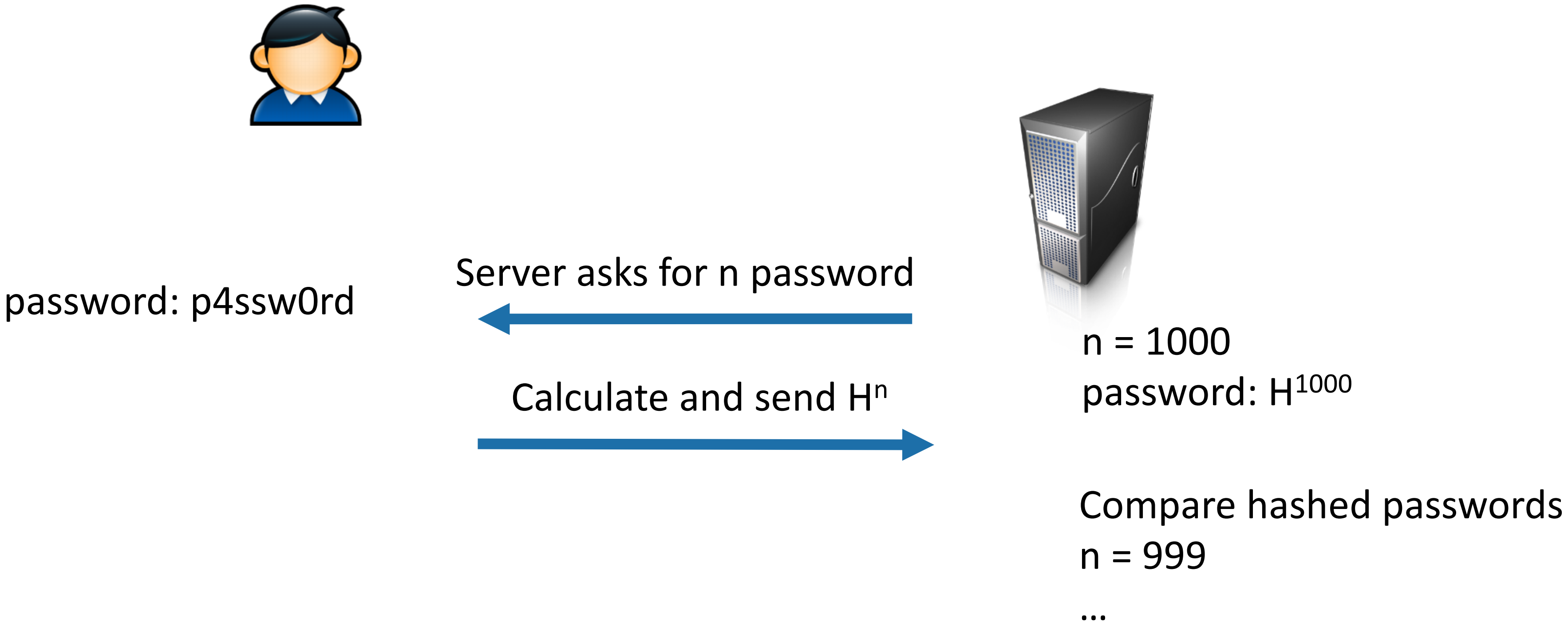
Photo 2 of 5

This appears to be:
○ Naitik Shah ○ Tim Kuper ○ Alok Menghrajani
○ Nick Wilkerson ○ David Starling ○ Alessio Riso

(2 skips left)

Authentication with Insecure Communication

n^{th} password → H^n = *n times* … H(H((“p4ssw0rd”)



password: p4ssw0rd

Server asks for n password

Calculate and send H^n

n = 1000
password: H^{1000}

Compare hashed passwords
n = 999
…

Lamport’s Hash

When n == 0 password needs to be reset

No mutual authentication

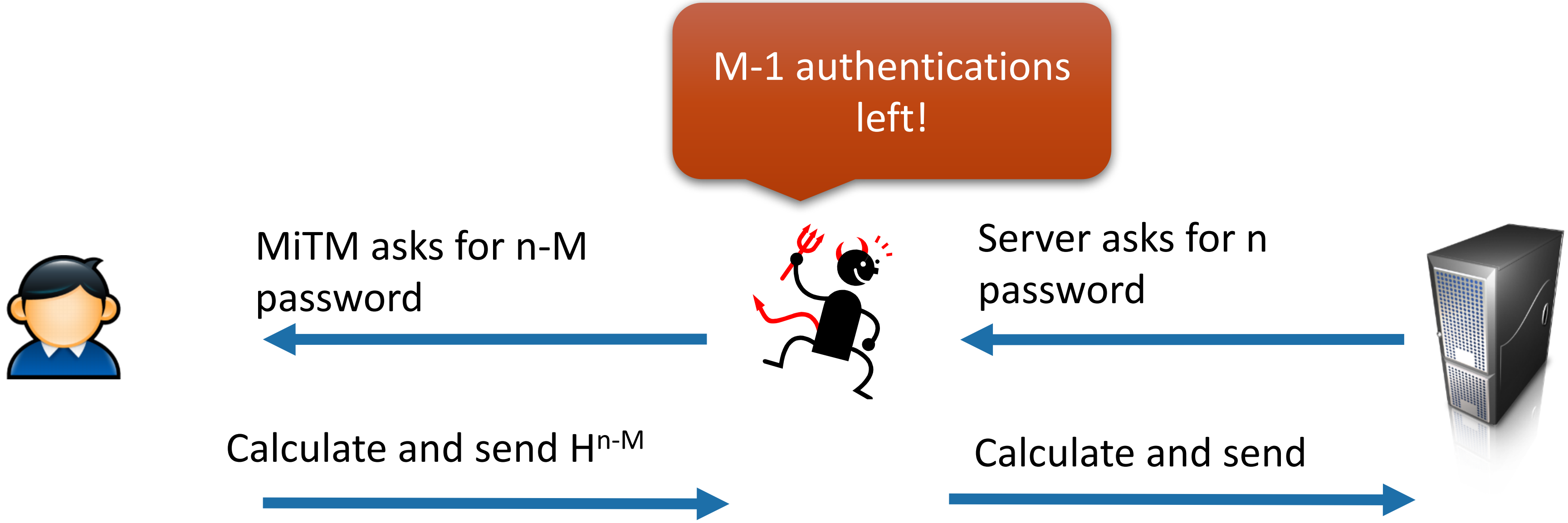
Still vulnerable to MiTM

Why?

Authentication with Insecure Communication

Leslie Lamport, Password Authentication with Insecure Communication, 1981

n^{th} password → H^{n} = *n times* … H(H((“p4ssw0rd”)



M-1 authentications left!

MiTM asks for n-M password

Server asks for n password

Calculate and send H^{n-M}

Calculate and send

Tokens

Memory Cards

Can store but do not process data

The most common is the magnetic stripe card

Can include an internal electronic memory

Can be used alone for physical access

- Hotel room
- ATM

Provides significantly greater security when combined with a password or PIN

Drawbacks of memory cards include:

- Requires a special reader
- Can be stolen
- User needs to carry them

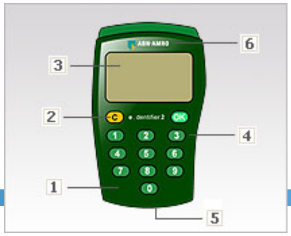
Token-based Authentication

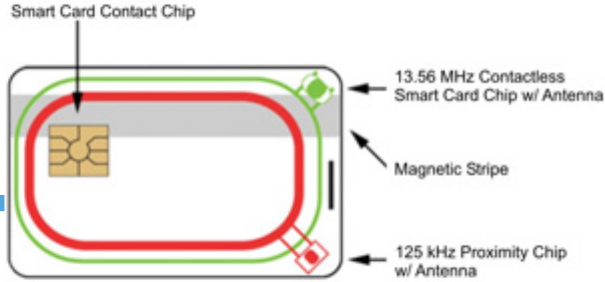
TOKEN

Channel requires contact or close proximity

TOKEN

Smart Tokens




Smart Card Contact Chip
13.56 MHz Contactless Smart Card Chip w/ Antenna
Magnetic Stripe
125 kHz Proximity Chip w/ Antenna

Physical characteristics:

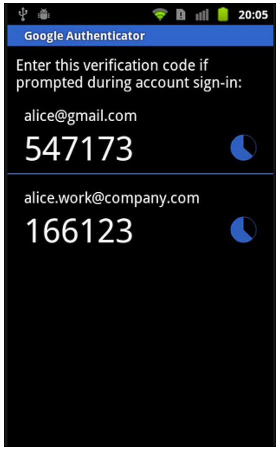
- Include an embedded microprocessor
- A smart token that looks like a bank card
- Can look like calculators, keys, small portable objects

Interface:

- Manual interfaces include a keypad and display for interaction
- Electronic interfaces communicate with a compatible reader/writer

Authentication protocol:

- Classified into three categories:
  - Static
  - Dynamic password generator
  - Challenge-response



Google Authenticator

Enter this verification code if prompted during account sign-in:

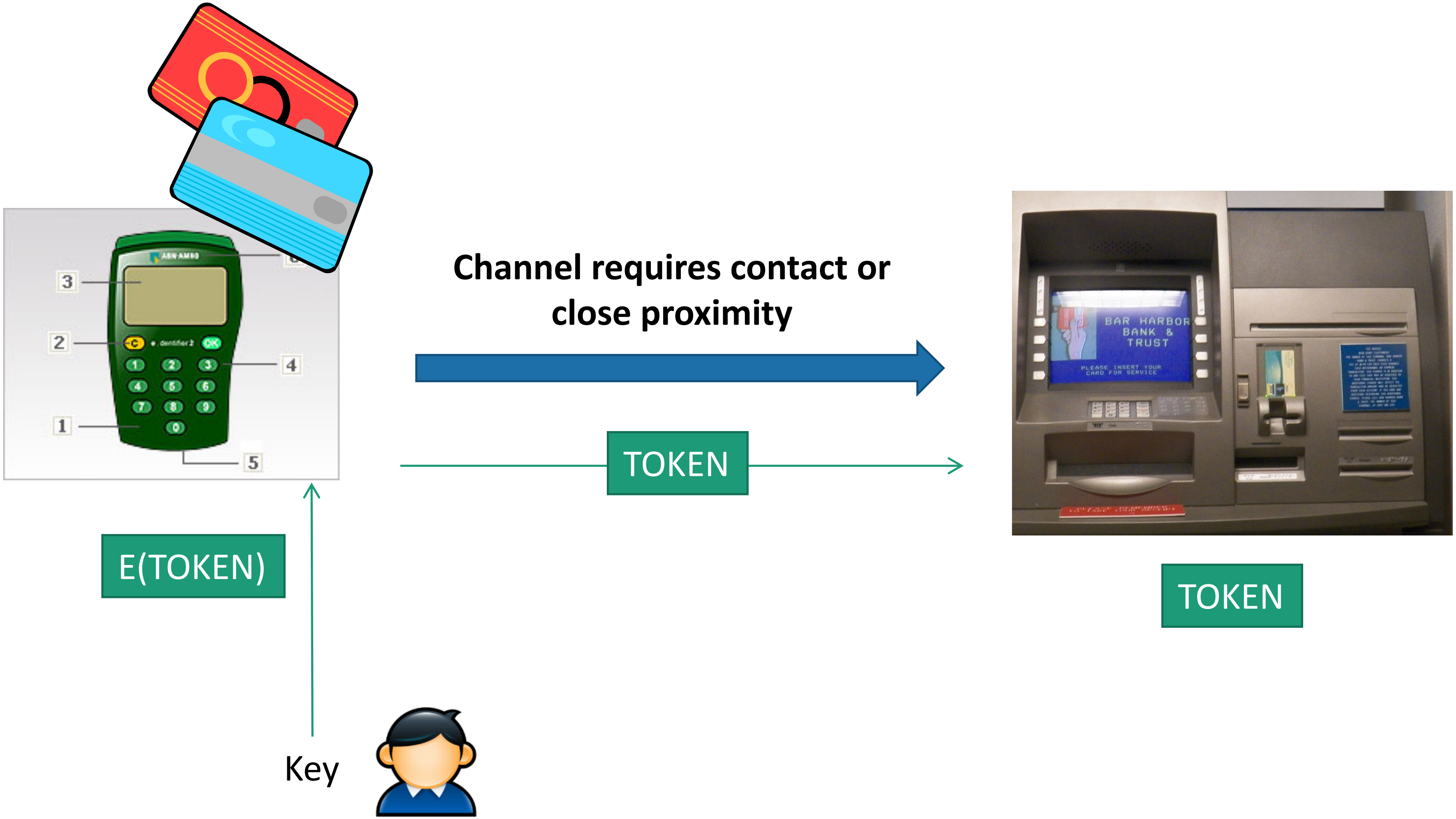
alice@gmail.com

547173

alice.work@company.com

166123

Static Protocol



Channel requires contact or close proximity

TOKEN

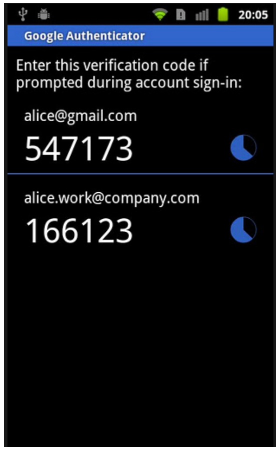
E(TOKEN)

TOKEN

Key

Dynamic Protocol

Time-based One Time Password Generation



20:05

Google Authenticator

Enter this verification code if prompted during account sign-in:

alice@gmail.com

547173

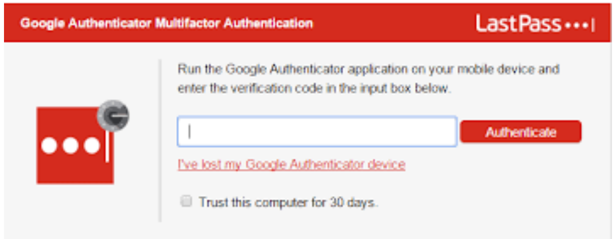
alice.work@company.com

166123

SECRET

Valid for a limited amount of time

OTP



Google Authenticator Multifactor Authentication

LastPass•••|

Run the Google Authenticator application on your mobile device and enter the verification code in the input box below.

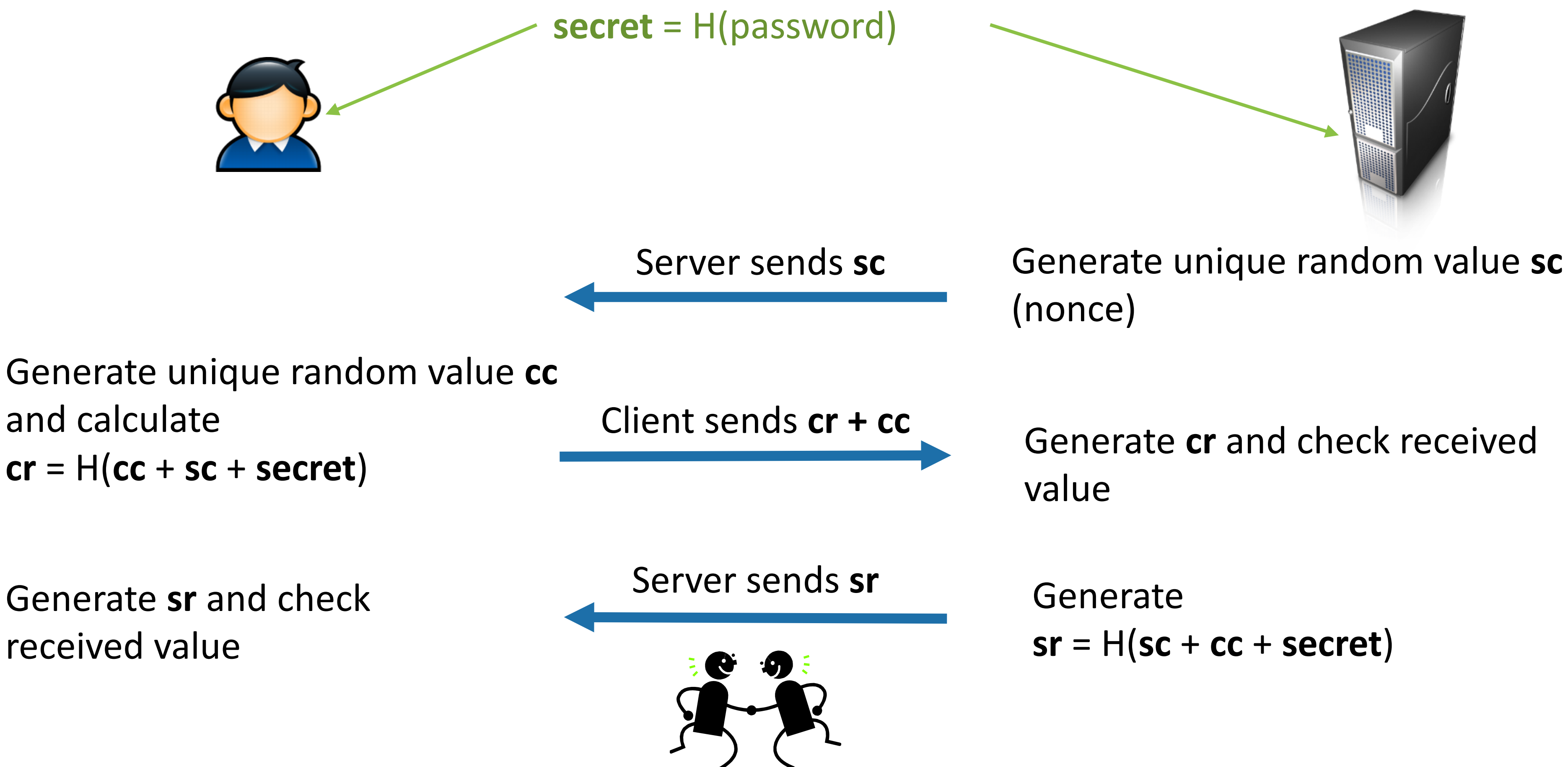
Authenticate

I've lost my Google Authenticator device

□ Trust this computer for 30 days.

SECRET

Simple Mutual Authentication (Challenge-Response)



secret = H(password)

Server sends **sc**

Generate unique random value **sc** (nonce)

Generate unique random value **cc** and calculate
cr = H(**cc** + **sc** + **secret**)

Client sends **cr + cc**

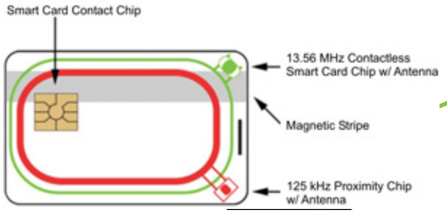
Generate **cr** and check received value

Server sends **sr**

Generate
sr = H(**sc** + **cc** + **secret**)

Generate **sr** and check received value

Simple Mutual Authentication (Challenge-Response)


Smart Card Contact Chip
13.56 MHz Contactless Smart Card Chip w/ Antenna
Magnetic Stripe
125 kHz Proximity Chip w/ Antenna

secret = H(password)

Server sends **sc**

Generate unique random value **sc** (nonce)

Generate unique random value **cc** and calculate
cr = H(**cc** + **sc** + **secret**)

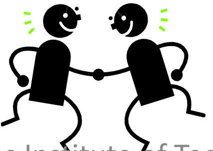
Client sends **cr + cc**

Generate **cr** and check received value

Server sends **sr**

Generate
sr = H(**sc** + **cc** + **secret**)

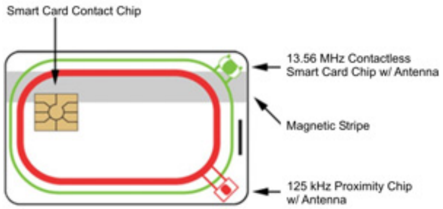
Generate **sr** and check received value



Challenge-Response Protocol

Using public-key cryptography

Secret key PK^+


Smart Card Contact Chip
13.56 MHz Contactless Smart Card Chip w/ Antenna
Magnetic Stripe
125 kHz Proximity Chip w/ Antenna

Public key PK^-

Generate unique random value **sc** (nonce)

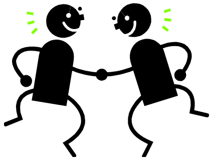
Server sends **sc+SIG(PK$^-$, sc)**

Verify signature

Generate unique random value **cc**

Client sends **cr+SIG(PK$^+$, cr)**

Verify signature



Security Issues with Cards

Information may be unencrypted on the card

They can be reverse engineered

Cracking the Mifare Chip

https://www.youtube.com/watch?v=NW3RGbQTLhE

Biometrics

Biometric Authentication

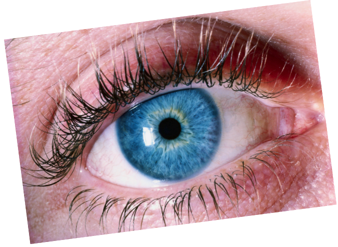
Attempts to authenticate an individual based on unique physical characteristics

Based on pattern recognition

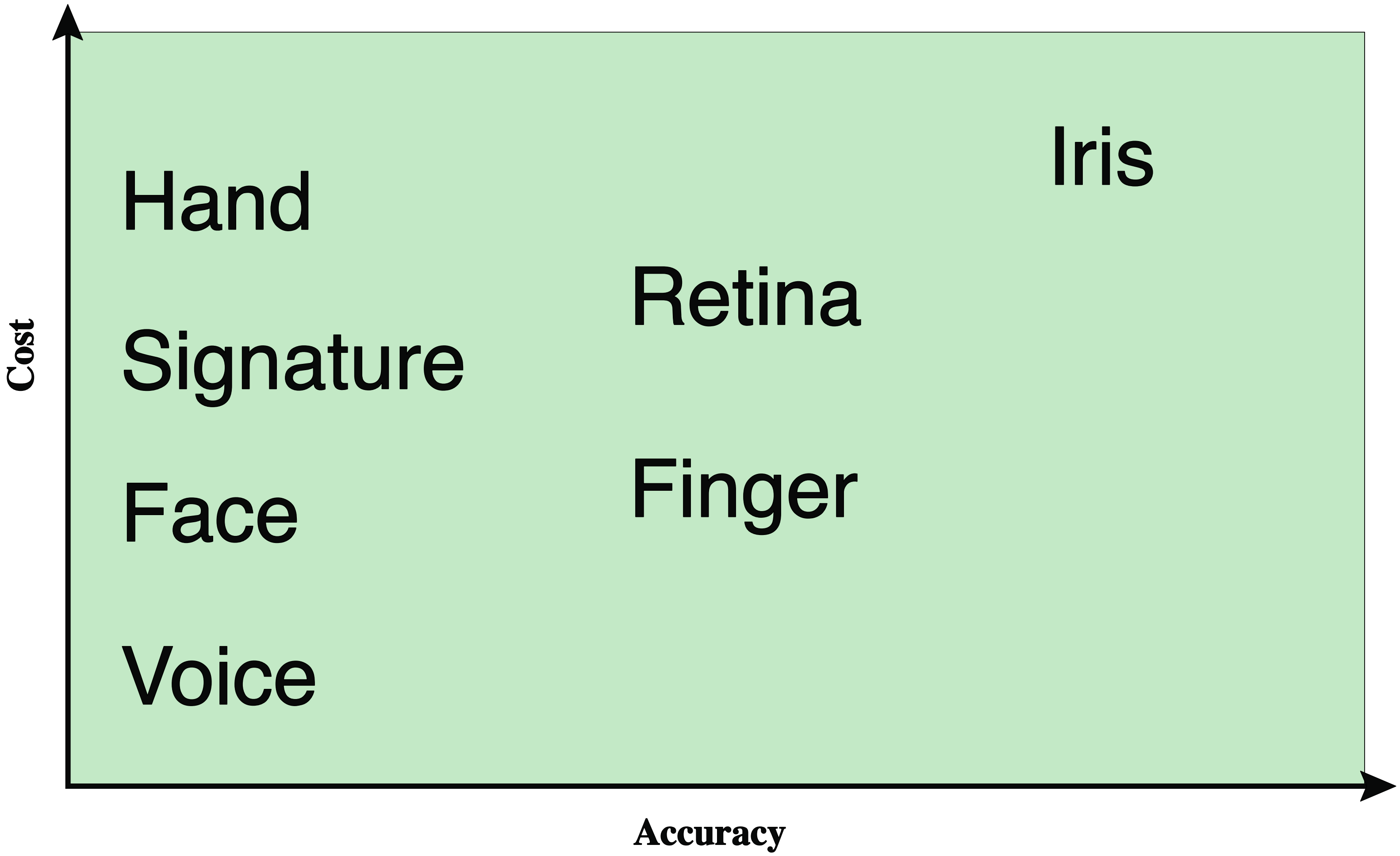
Is technically complex and expensive when compared to passwords and tokens

Physical characteristics used include:

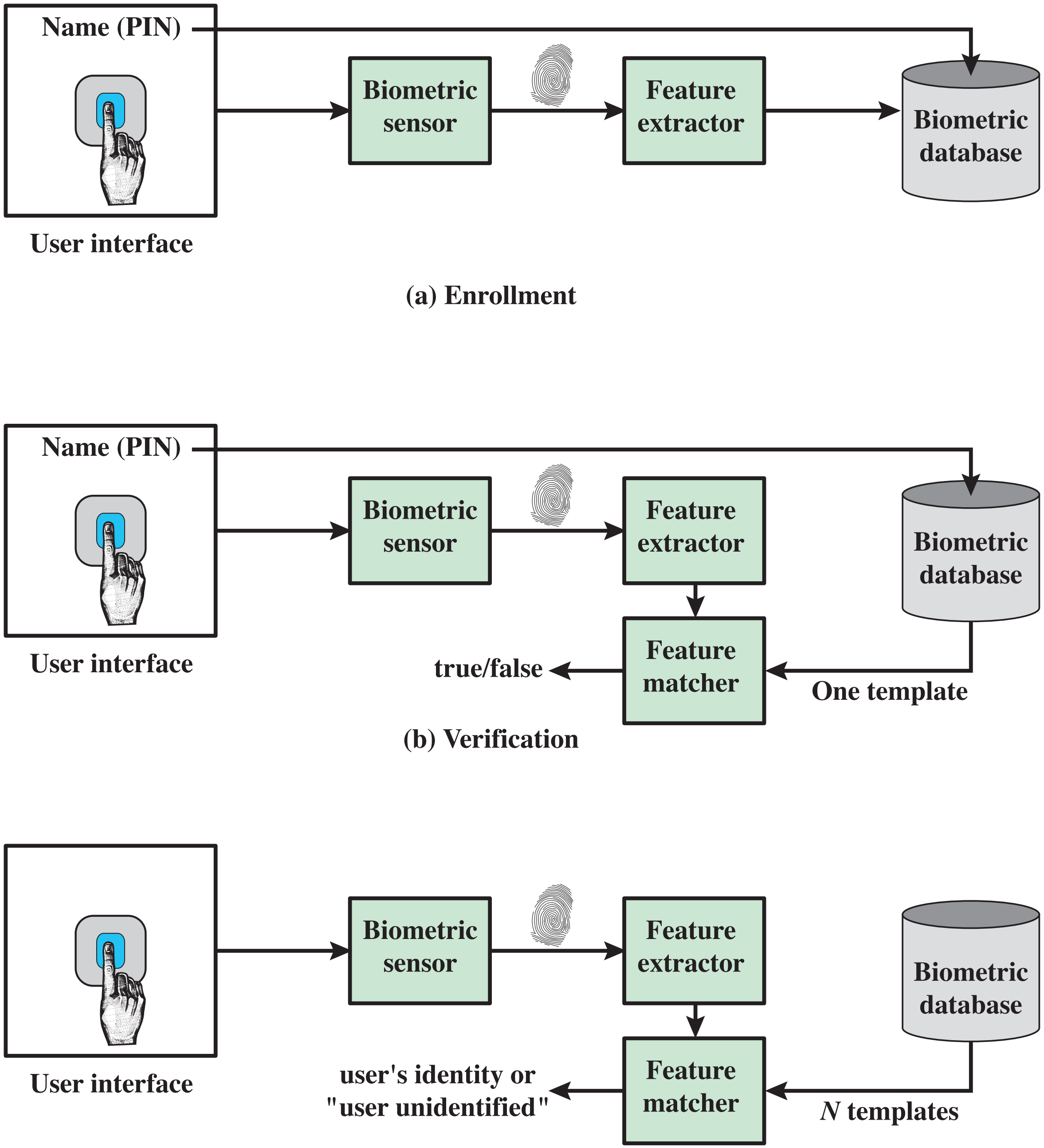
- Facial characteristics
- Fingerprints
- Hand geometry
- Retinal pattern
- Iris
- Signature
- Voice



Cost vs Accuracy for Biometrics



Using Physical Biometrics

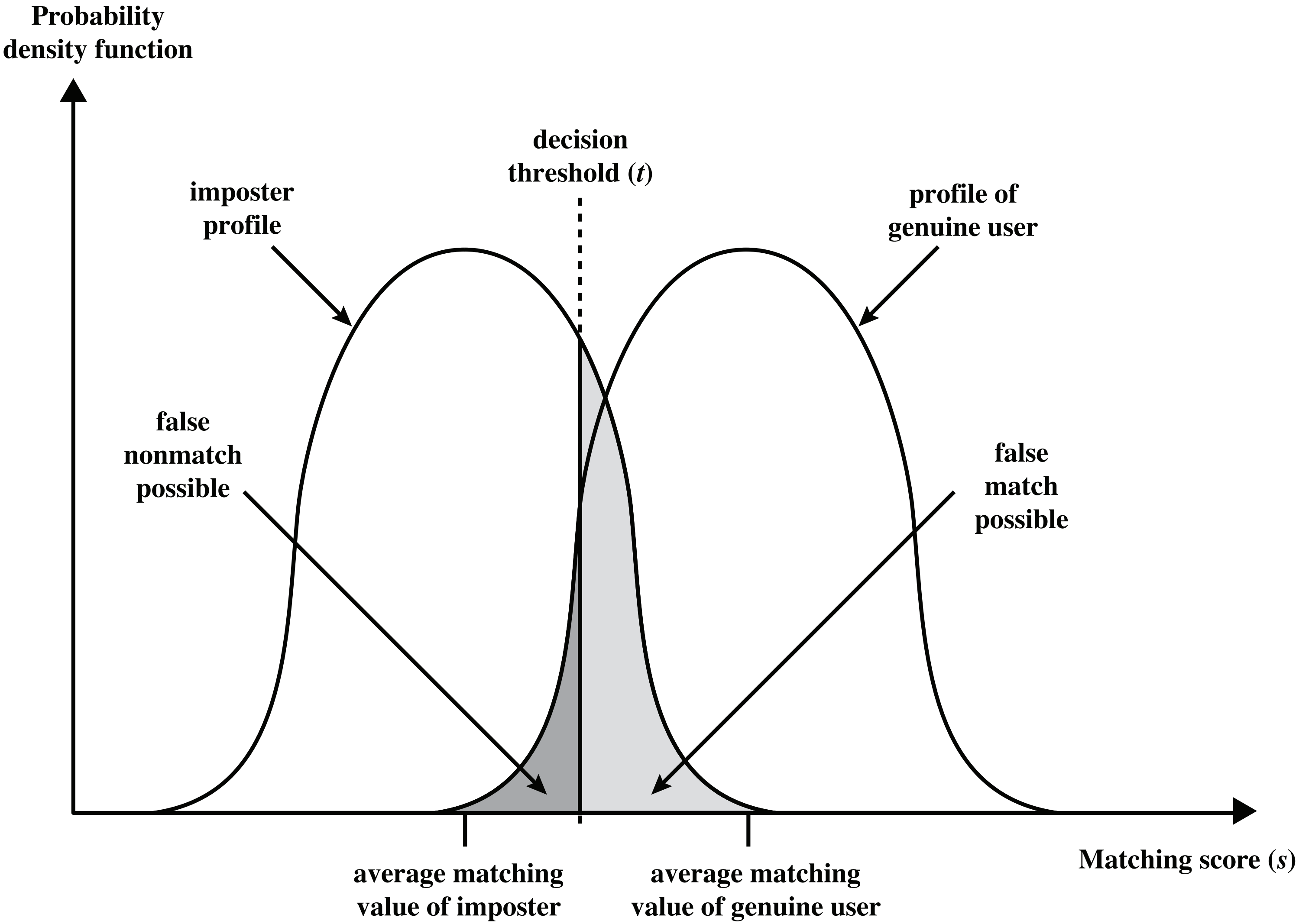


(a) Enrollment

(b) Verification

(c) Identification

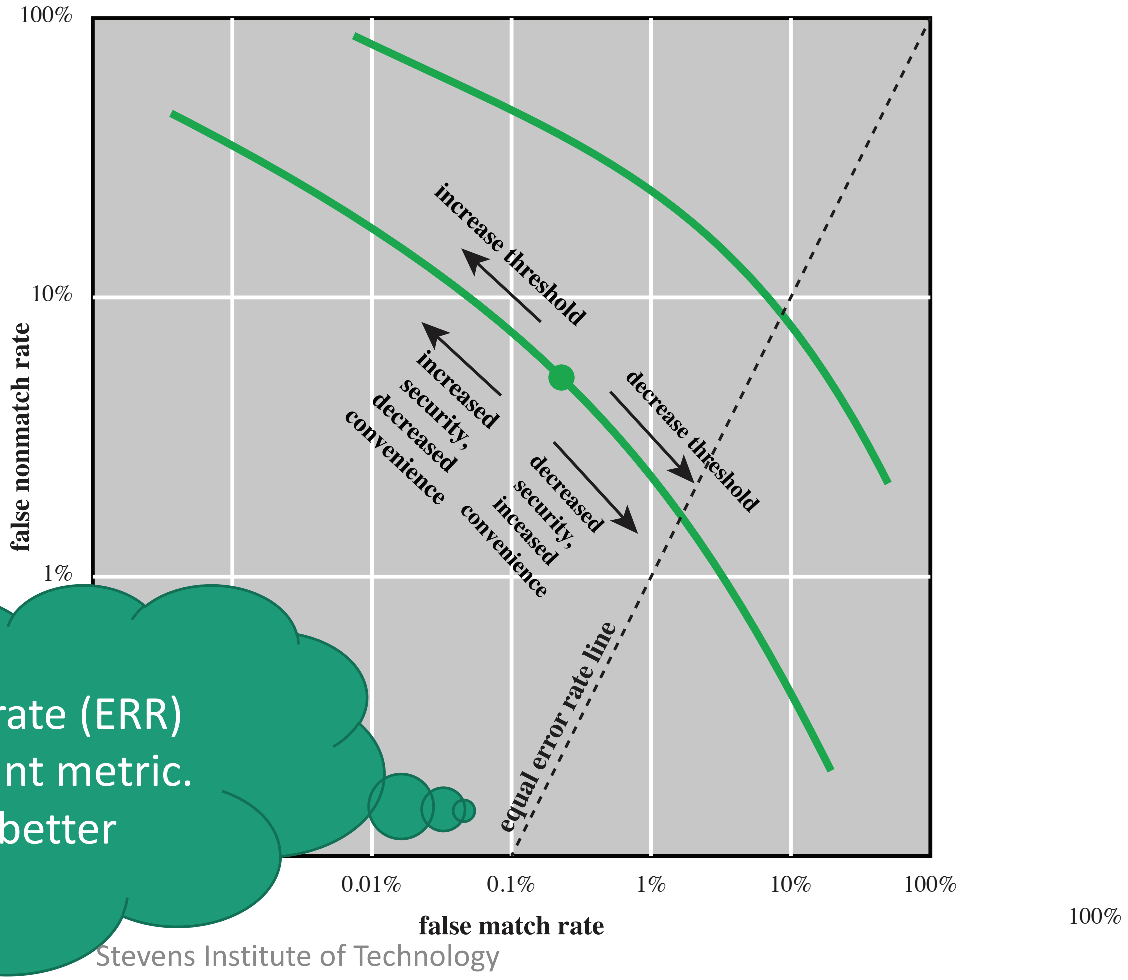
Probabilistic Identification



Operating Characteristic Curves

Idealized measurement

log-log scale



Equal-error rate (ERR) is an important metric. Lower is better

Actual Measurement

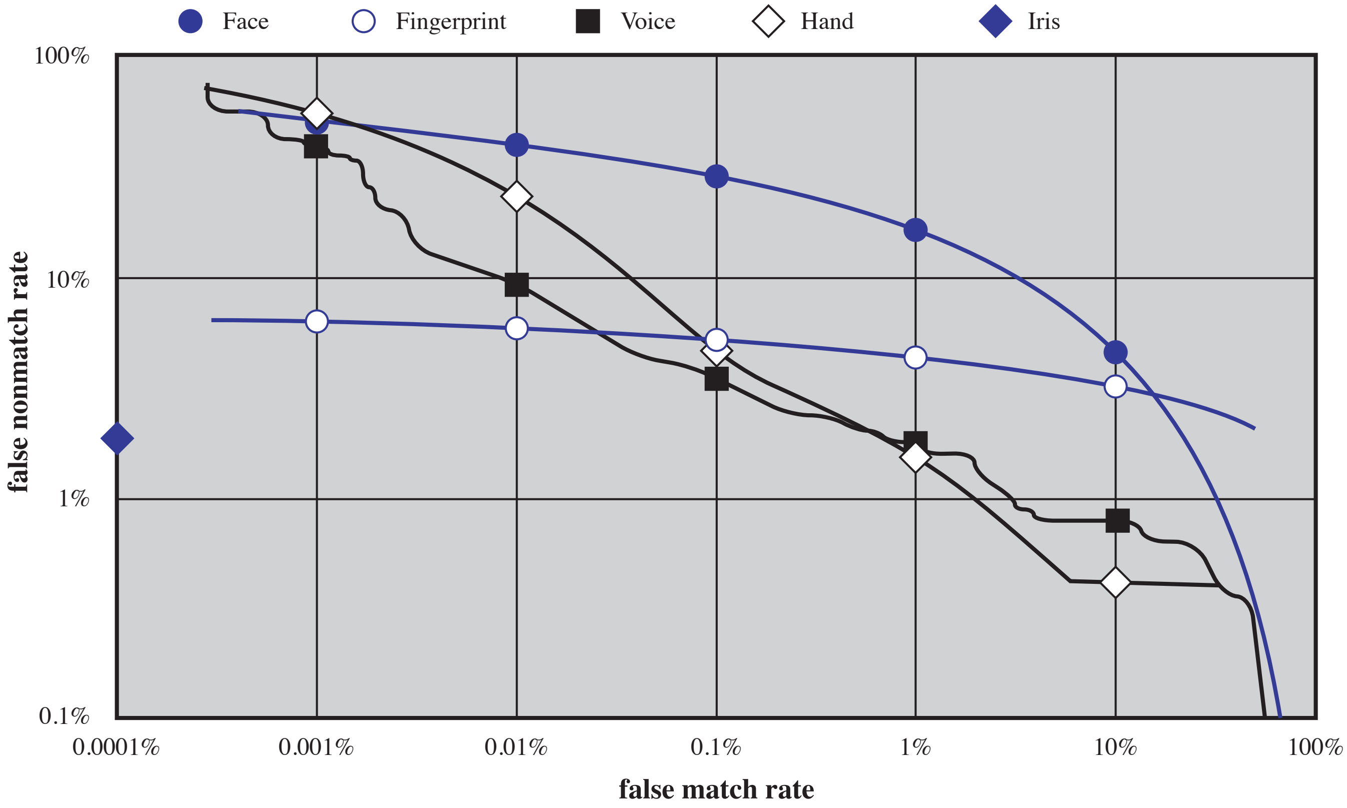
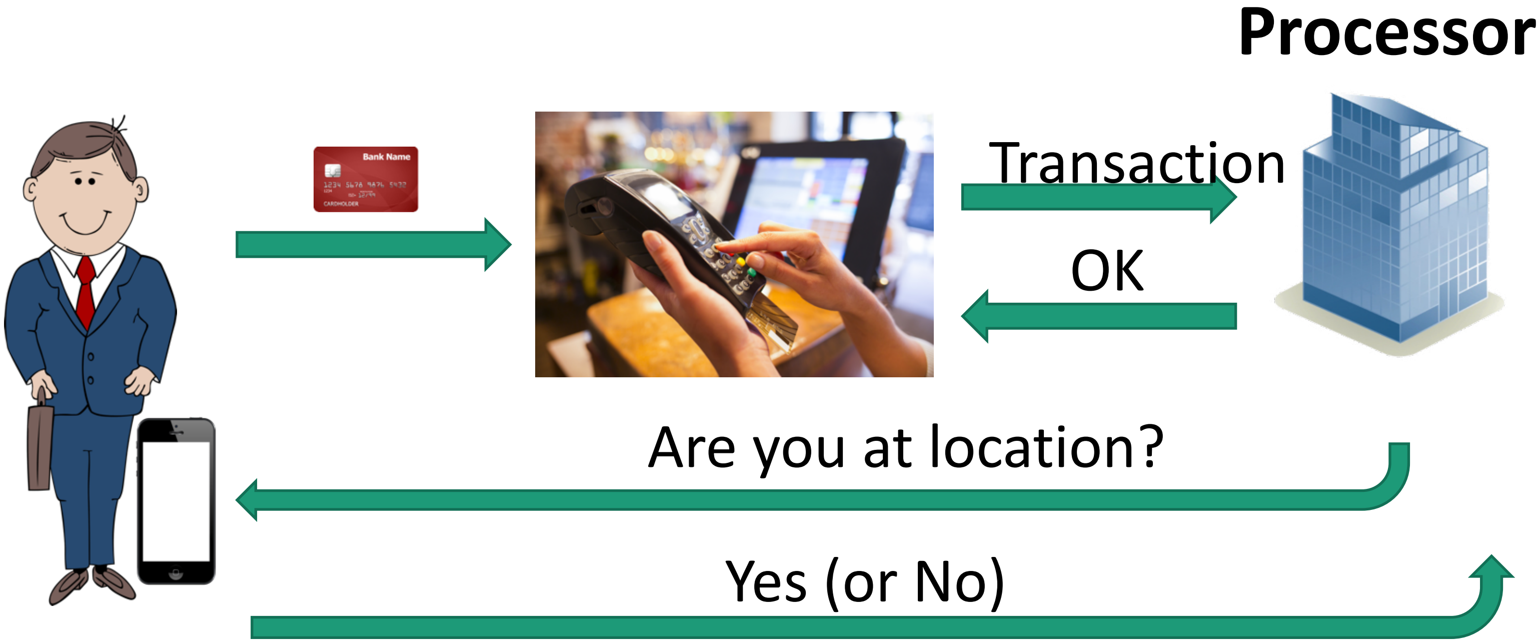


Figure 3.11 Actual Biometric Measurement Operating Characteristic Curves, reported in [MANS01]. To clarify differences among systems, a log-log scale is used.

Location as a 4th Factor

Location-Based Verification Using Smartphones



Processor

Transaction

OK

Are you at location?

Yes (or No)

Location-Based Verification

Advantages

79% of people aged 18–44 have their smartphones with them 22 hours a day

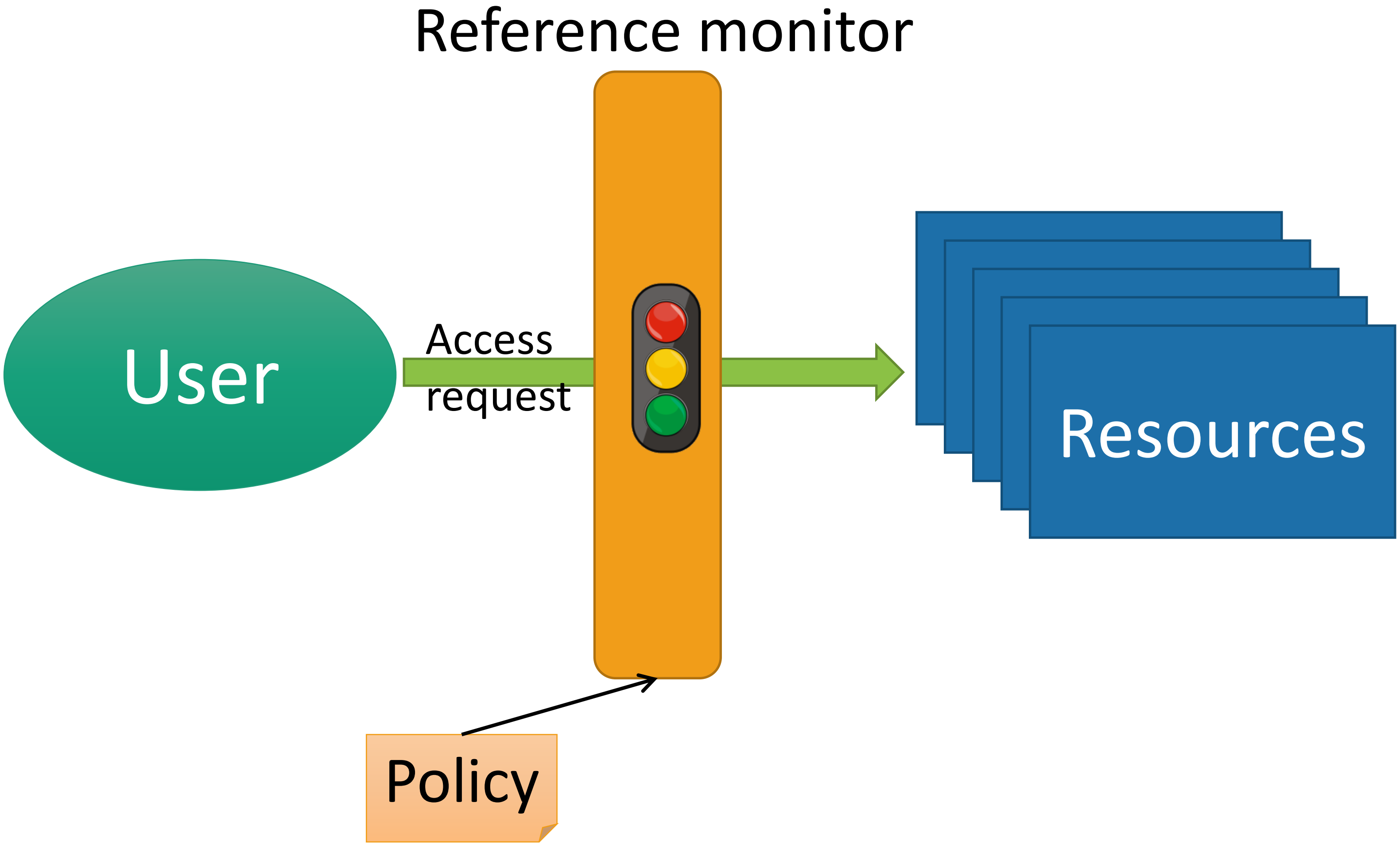
Disadvantages

It’s not 100%

- May forget phone
- Phone can run out battery
- May leave phone behind during certain activities (e.g., running in the park)

Access Control

High-level Overview



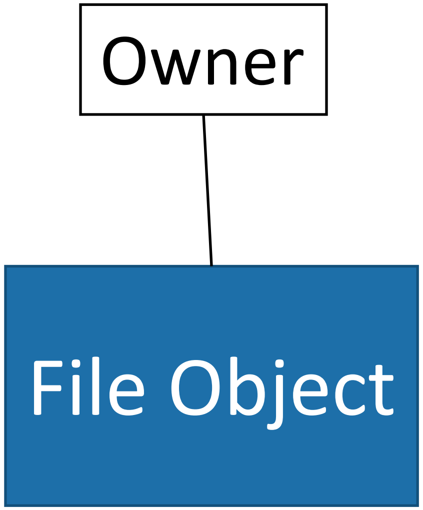
Access Control Approaches

Discretionary Access Control (DAC)

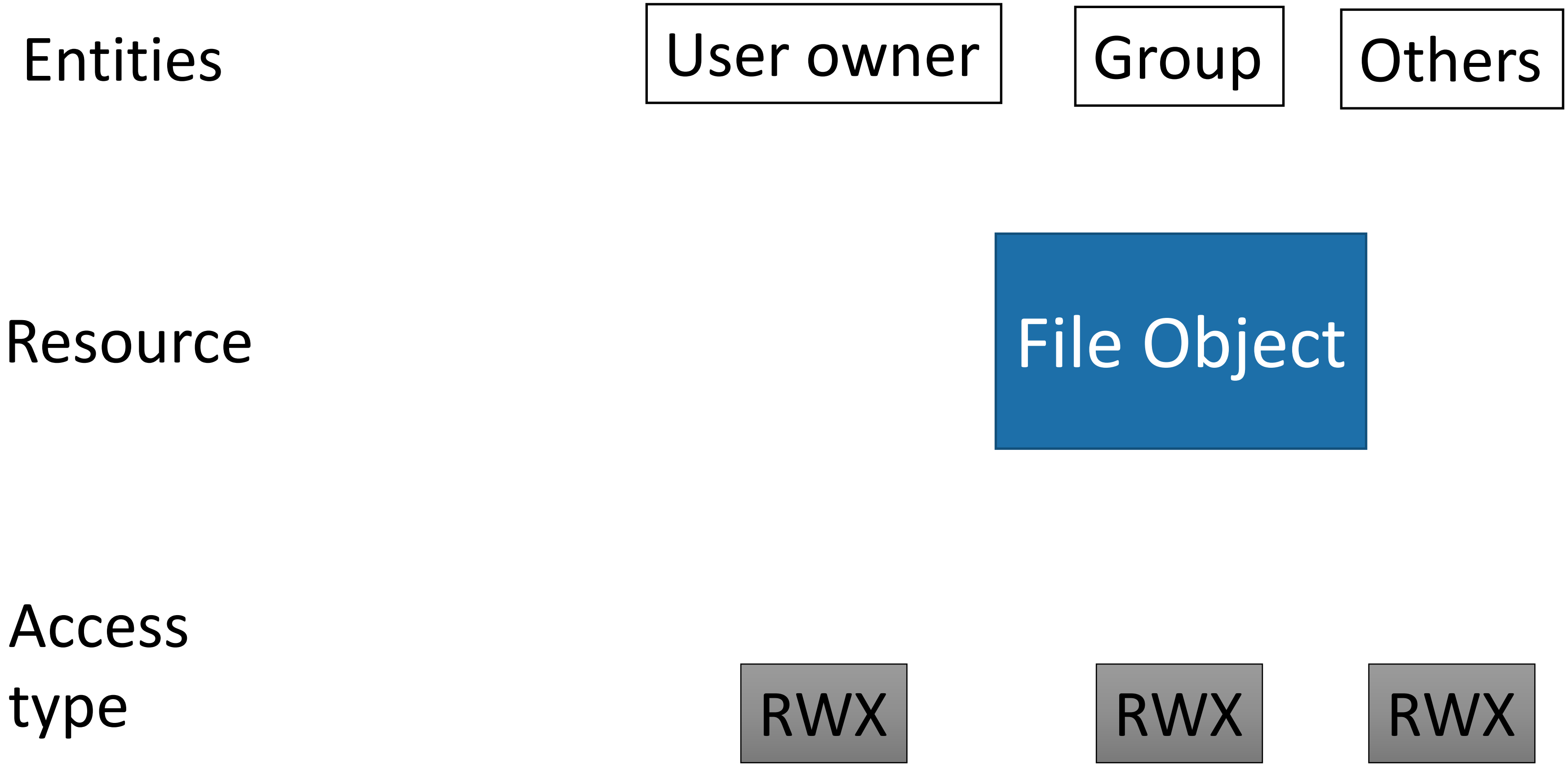
- Resources are usually associated with an owner
- Discretionary because the owner can delegate access

Mandatory Access Control (MAC)

- Operating system or reference monitor strictly manages access
- Access can not be delegated



DAC Example: UNIX Permissions



Entities

User owner

Group

Others

Resource

File Object

Access type

RWX

RWX

RWX

MAC Example: Access control list (ACL)

Resource

File Object

Entity	Access type

⋮

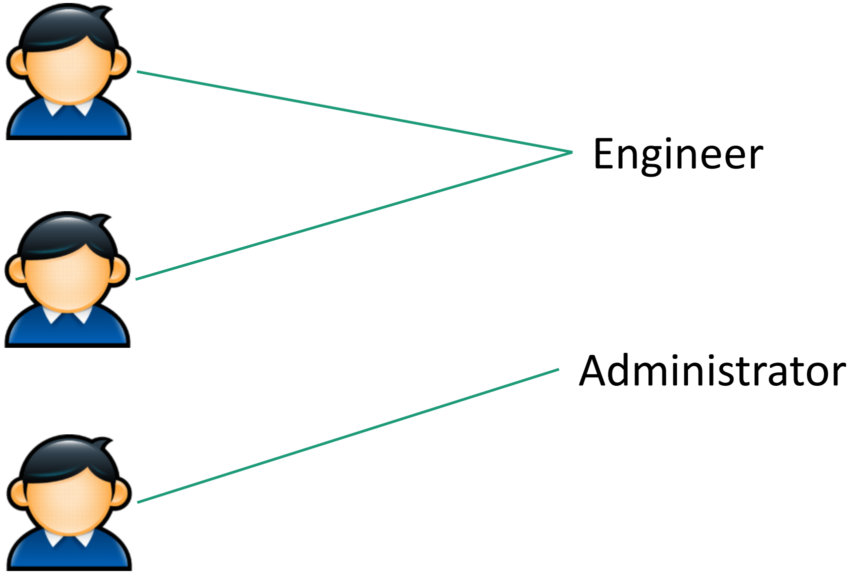
Role-based Access Control (RBAC)

Policies apply on roles

- Roles are similar to groups

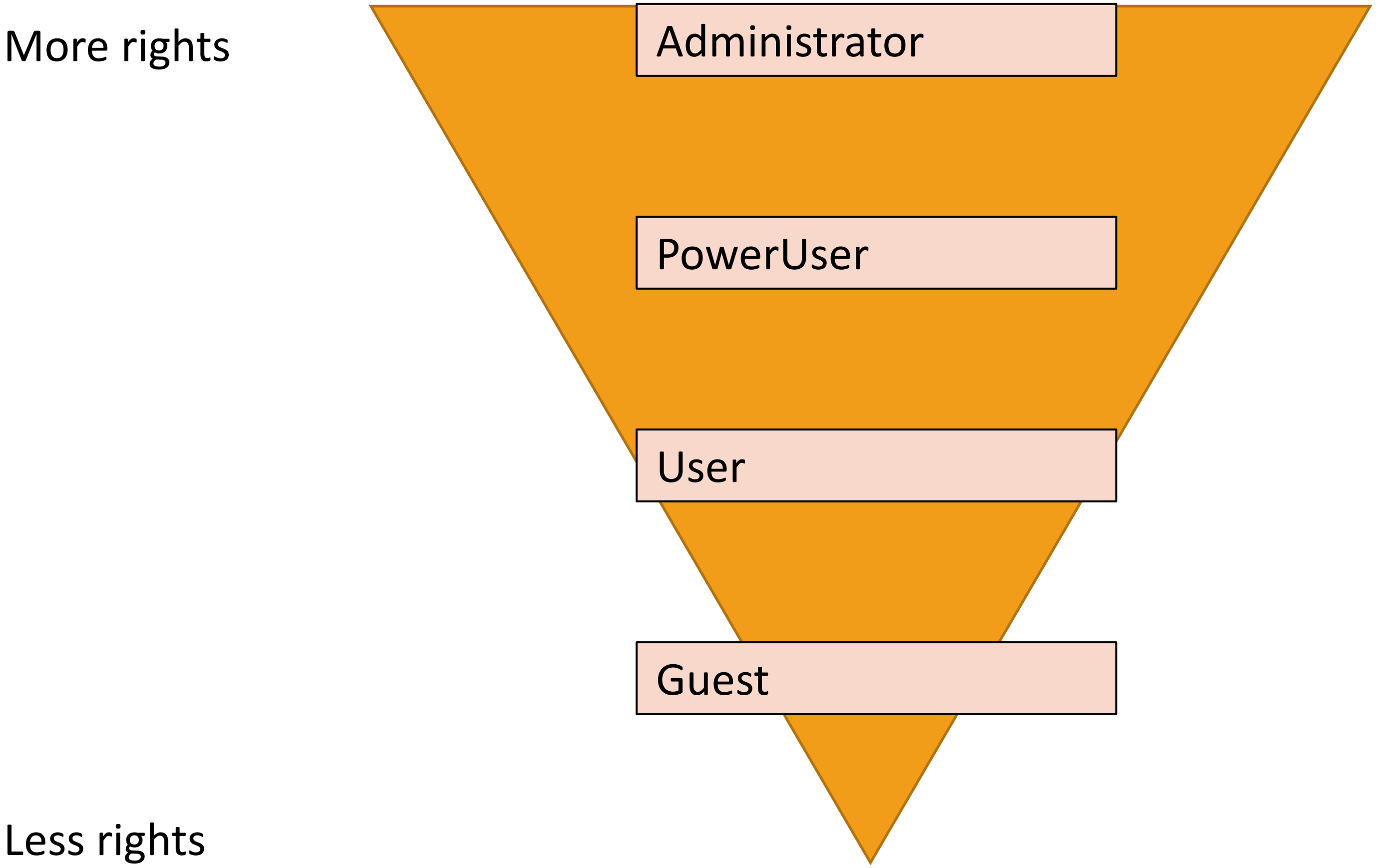
Usually less roles than users → easier management

Easy to handle users switching roles



DAC or MAC afterwards

Role Hierarchy



Mix and Match

In practice multiple approaches are usually combined to control different type of requests and resources

Additional Reading

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes

Social Authentication: Harder than it Looks

Honeywords: Making Password-Cracking Detectable

SAuth: Protecting User Accounts from Password Database Leaks

Smartphones as Practical and Secure Location Verification Tokens for Payments

Dos and Don’ts of Client Authentication on the Web

Kerberos: The Network Authentication Protocol