Lecture 07 – Passwords and Authentication

Michael Bailey
University of Illinois
ECE 422/CS 461 – Spring 2018

Major Portions Courtesy Ryan Cunningham

AUTHENTICATION

Authentication Basics

- Authentication binds identity to a subject
- Two step process
  - Identification - establish identity to system
  - Verification - process verifies and binds entity and identity

PASSWORD AUTHENTICATION

Basics

- User keeps a secret string (password)
- Something the user *knows*
- Advantages?
- Disadvantages?

Attacks

- Steal from the user
  - Install a keylogger (hardware or software)
  - Find it written down
  - Social engineering/Phishing
  - Intercept the password over network
  - Use a side channel
- Steal from the service
  - Install malware on the web server
  - Dump the password database with SQL injection
- Steal from a third party (password reuse)

Password Guessing

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

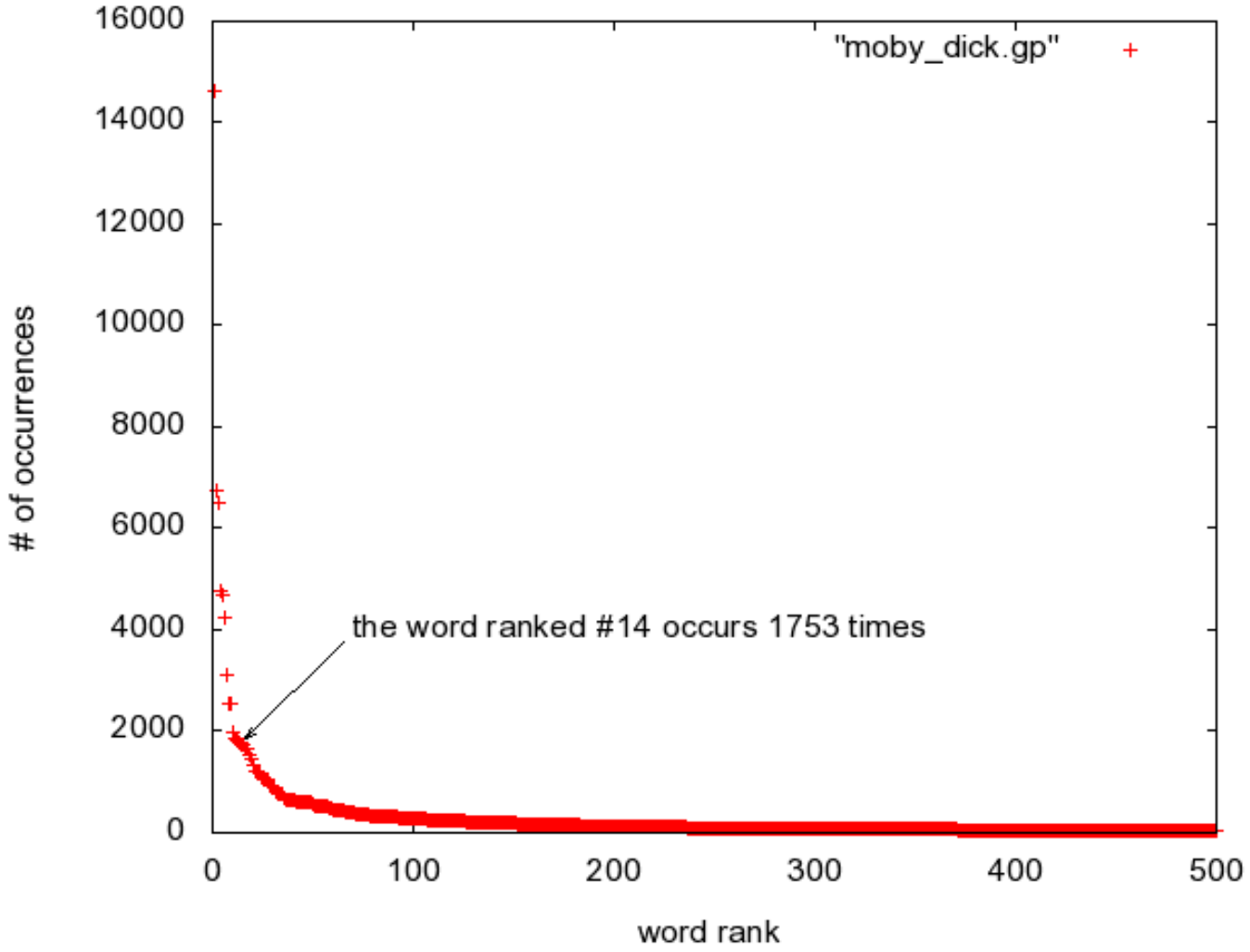
http://www.datagenetics.com/blog/september32012/

Top 20 Passwords (Mark Burnett)

password, 32027
123456, 25969
12345678, 8667
1234, 5786
qwerty, 5455
12345, 4523
dragon, 4321
pussy, 3945
baseball, 3739
football, 3682
letmein, 3536
monkey, 3487
696969, 3345
abc123, 3310
mustang, 3289
michael, 3249
shadow, 3209
master, 3182
jennifer, 2581
111111, 2570

https://xato.net/10-000-top-passwords-6d6380716fe0#.lo0geeq99

Power Law



http://www.philippeadjiman.com/blog/2009/10/26/drawing-the-long-tail-of-a-zipf-law-using-gnuplot-java-and-moby-dick/

Secure Passwords

- Uneven distribution makes guessing easier
- Passwords should be *uniformly* distributed
  - All characters in password chosen with equal probability
- Passwords should be long
  - Longer password = larger brute force search space
- Passwords should never be reused
- Passwords chosen randomly are difficult to remember
  - Tradeoff of security vs. convenience

STORING PASSWORDS

Confirmed Attack At Opera, 1.7M Password Leak Possible

Passwords for 32M Twitter accounts may have been hacked and leaked

Posted Jun 8, 2016 by Catherine Shu (@catherineshu), Kate Conger (@kateconger)

Next Story

Epic Games forums hacked again: Over 800,000 gamers put at risk

BY GRAHAM CLULEY POSTED 23 AUG 2016 - 02:50AM

DATA LEAKAGE

CrunchBase

Twitter

FOUNDED
2006

OVERVIEW
Twitter is a global social networking platform that allows its users to send and read 140-character messages known as "tweets". It enables registered users to read and post their tweets through the web

2016 mega breaches continue as hackers steal and leak 33 million QIP.ru accounts

- Breach appeared to have occurred in 2011 and user passwords were allegedly not encrypted.

By India Ashok
September 10, 2016 11:52 BST

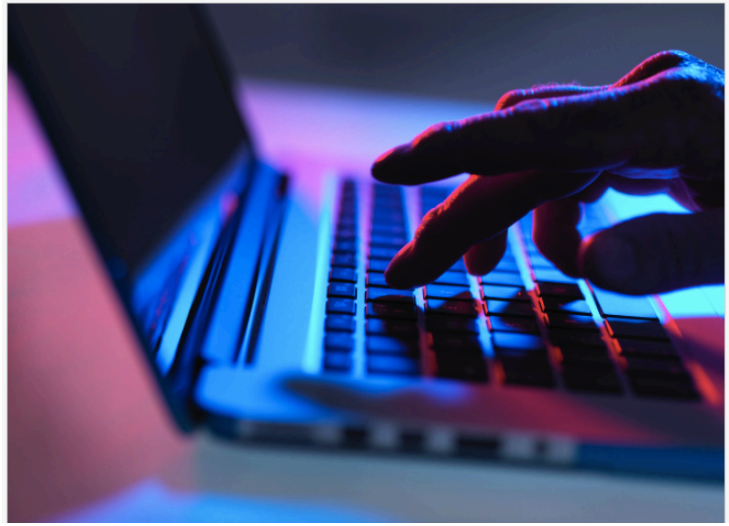
43 million passwords hacked in Last.fm breach

Posted Sep 1, 2016 by John Mannes (@JohnMannes)

Hackers breach porn site, expose 800,000 user accounts

A massive data breach has invaded the popular porn repository Brazzers' sister site, Brazzers Forum, after hackers took control of the website with nearly 800,000 user account information, including usernames and passwords.

By Yves Matthew Amodia | Sep 13, 2016 09:55 AM EDT



TC NEWS

The Daily Crunch
Our top headlines
Delivered daily

CrunchBase Daily
The latest startup funding announcements
Delivered daily

Enter Address

Storing Passwords

- Password database is highly sensitive
- We should never store *plaintext* passwords
- Store something that lets user prove they know the password

Hash functions (more later)

- Input – data of an arbitrary size
- Output – fixed length
- Same input always produces the same output
- One way function – cannot deduce input from output
- A “fingerprint” for the input
- Examples: MD5, SHA-1, SHA-256, SHA3-512

- `md5("welcome")= "M3ULPLtx$K6.aFwEvavGgNx8SGe9fq"`

Password Hashes

- We store a database of password *hashes*
- e.g. /etc/shadow on UNIX

```
rcunnin2:$6$vb1tLY1qiY$M.
1ZCqKtJBxBtZm1gRi8Bbkn39KU0YJW1cu
MFzTRANcNKFKR4RmAQVk4rqQQCkaJT6wX
qjUkFcA/qNxLyqW.U/:
15405:0:99999:7::
```

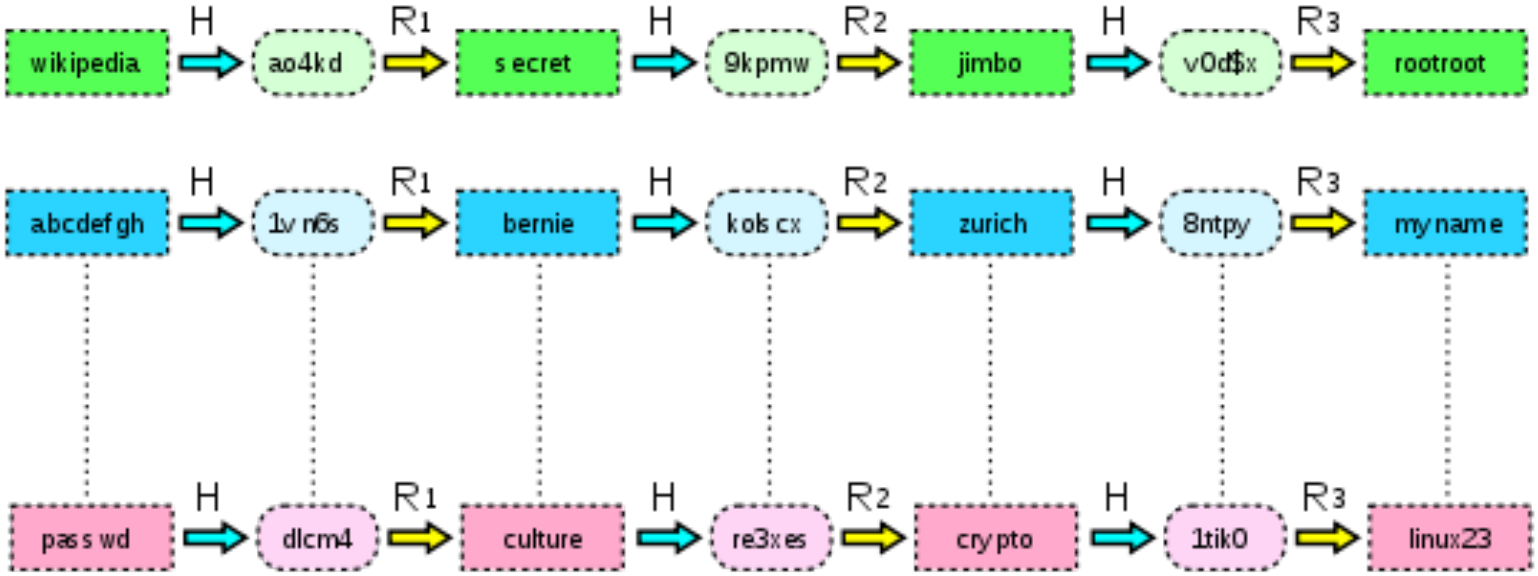
Password Cracking

- Brute force search through all possible passwords in order
- Use a dictionary
- Use a dictionary of common passwords
- Combine dictionary with common passwords and heuristics (e.g. p@$$w0rd and password123)
- Use statistical models of user passwords

- Easy to parallelize
  - hash password guess, compare to entire hash database
- Commonly done with arrays of GPUs

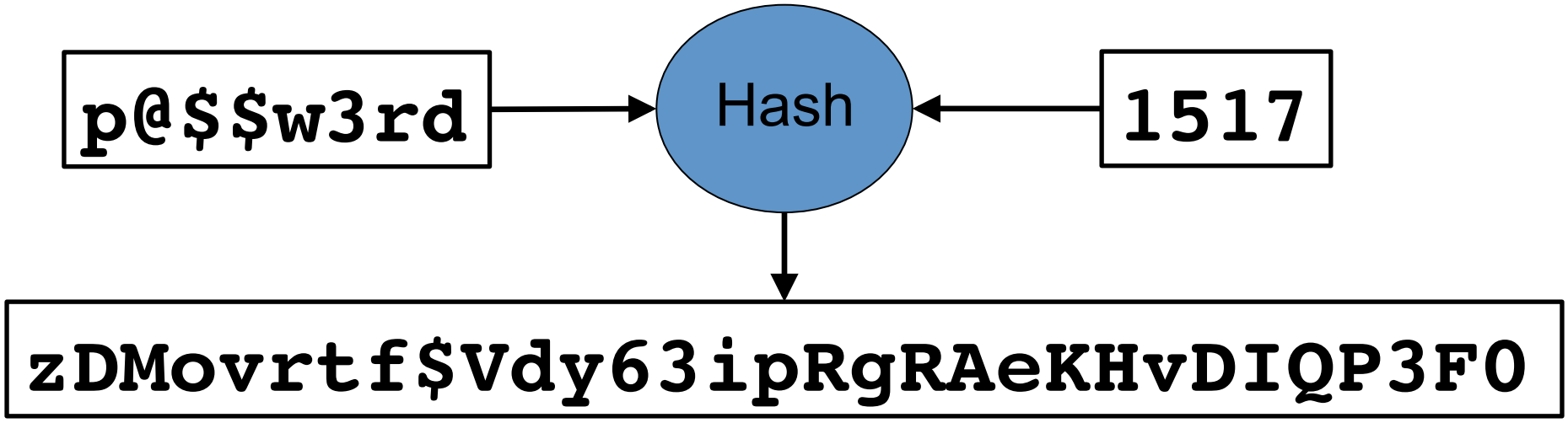
Rainbow Tables

- Many passwords are common
- Precompute them in a lookup table
- Time/space tradeoff



Salting Password Database

- Generate and store a random number (nonce) for each password (salt)
- Concatenate password and salt to compute hash
- Effectively a unique hash function for each password



Password Security Policies

- Educate users about password security
  - Specifically train them to use good passwords
  - But they might or might not follow through
- Generate passwords randomly
  - Perfect uniform distribution
  - But not very psychologically acceptable
- Reactive password checking
  - Crack your own user's passwords
  - But expensive and passwords vulnerable until cracked
- Complex password policy/proactive checking

Complex Password Policy/Proactive Checking

- Let the user select their own password
- Force them to follow a policy
- Reject passwords that don't follow policy
- But…
  - Technically *reduces* number of possible passwords
  - Policy might not be psychologically acceptable
  - We don't know if users are reusing their passwords

Password Reuse

http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/all/

Security Questions

- Are also a shared secret
- Bruce Schneier calls them “a backup password”
- Easier to guess and social engineer
- Some cannot be changed

OPM Breach


KrebsonSecurity
In-depth security news and investigation
BLOG ADVERTISING
ABOUT THE AUTH
Congressional Report Slams OPM on Data Breach
nassive data breach at the U.S. Office of Personnel Management (OPM) that
ed background investigations and fingerprint data on millions of Americans was the
of a cascading series of cybersecurity blunders from the agency's senior leadership on
to the outdated technology used to secure the sensitive data, according to a lengthy
t released today by a key government oversight panel.
My New Book!
SPAM
NATION
NEW YORK TIMES BESTSELLER

RECENT PASSWORD SOLUTIONS

Password Managers

- Application that generates and maintains passwords
- Examples: LastPass, KeePass, DashLane, 1Password
- Advantages:
  - Can handle random passwords
  - Can create unique passwords for every website and service
- Disadvantages
  - One point of failure
  - Requires a strong password (could be snooped)
  - Could be hacked (only as secure as the password manager)
  - Inconvenient (doesn't work for some sites, set up time, etc.)

One Point of Failure…

Trend Micro password manager had remote command execution holes and dumped data to anyone: Project Zero

Google's Project Zero discovered multiple trivial remote code execution vulnerabilities sitting within a password manager installed by Trend Micro as default alongside its AntiVirus product.

By Chris Duckett | January 12, 2016 -- 01:32 GMT (17:32 PST) | Topic: Security

A password management tool installed by default alongside Trend Micro AntiVirus was

RELATED STORIES

Security

ClixSense data breach exposes personal information of million of subscribers

Single Sign-On (SSO)

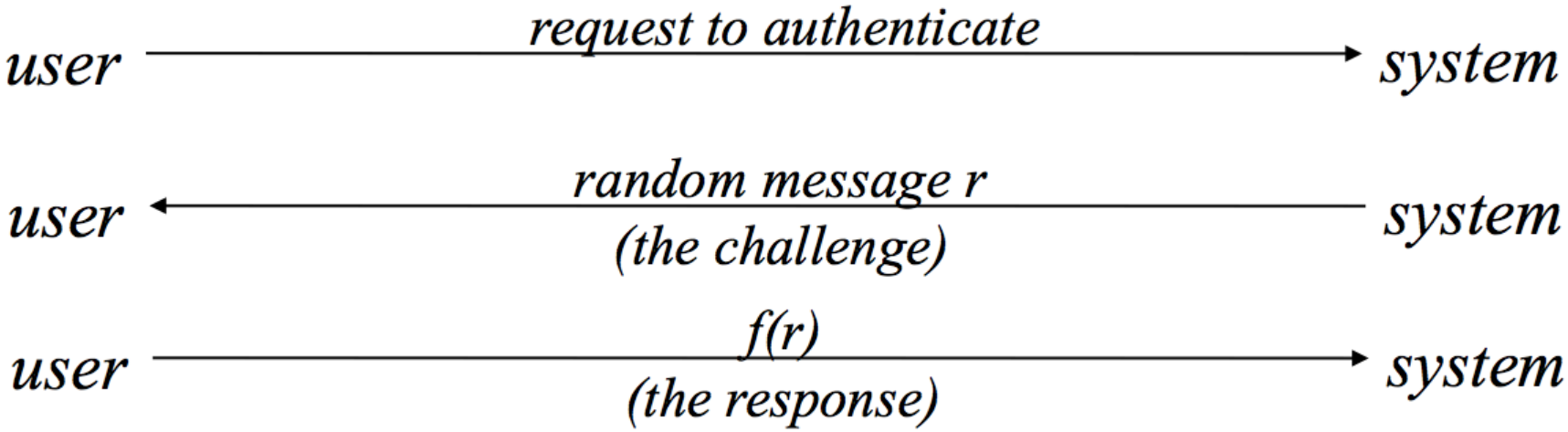
- Login to trusted 3rd party, who vouches for user identity
- Examples: Facebook Connect, OAuth, OpenID
- Pros and cons similar to Password Managers
- Third party can track users…

TOKEN-BASED AUTHENTICATION

Basics

- Something the user *has*
- Static memory cards
  - Read only
  - e.g. ATM card/Credit Card
  - Vulnerable to replay attack
- Smart card
  - Storage and computation
  - Enables challenge-response or one-time password
  - Protects against replay attack

Challenge-Response



One-time-password

- Smart card can also implement one-time password scheme
- S/Key is one such scheme:
  - Start with a random seed
  - Hash the current seed to produce the next
- Basically, share a pseudorandom number generator with shared state
- Use the hash outputs *in reverse order*

Disadvantages

- Token can be lost, stolen, or counterfeited
- Requires an individual physical token
- Requires an extra step (inconvenient)
- Hardware can be expensive

BIOMETRIC AUTHENTICATION

Biometrics

- Something the user *is* or *does*
- Derive a signature from biological features of user
  - Voice, fingerprint, face, retina, handwriting, gait
- Advantages?
- Disadvantages?

Disadvantages

- Imprecise measurements require *approximate* matching
  - Essentially a machine learning task
  - False negatives *and* false positives have a cost
- Measurements change over time
- Poor accessibility
- Cannot be replaced or concealed
- Replay attacks/spoofing possible
- Can be legally compelled to provide biometrics

OPM Breach


KrebsonSecurity
In-depth security news and investigation
BLOG ADVERTISING
ABOUT THE AUTH
Congressional Report Slams OPM on Data Breach
nassive data breach at the U.S. Office of Personnel Management (OPM) that
ed background investigations and fingerprint data on millions of Americans was the
of a cascading series of cybersecurity blunders from the agency's senior leadership on
to the outdated technology used to secure the sensitive data, according to a lengthy
t released today by a key government oversight panel.
My New Book!
SPAM
NATION
NEW YORK TIMES BESTSELLER

Facial Recognition

Spoofing Face Recognition With 3D Masks

2
Author(s)

Nesli Erdogmus ; Sébastien Marcel

View All Authors

Abstract:
Spoofing is the act of masquerading as a valid user by falsifying data to gain an illegitimate access. Vulnerability of recognition systems to spoofing attacks (presentation attacks) is still an open security issue in biometrics domain and among all biometric traits, face is exposed to the most serious threat, since it is particularly easy to access and reproduce. In this paper, many different types of face spoofing attacks have been examined and various algorithms have been proposed to detect them. Mainly focusing on 2D attacks forged by displaying printed photos or replaying recorded videos on mobile devices, a significant portion of these studies ground their arguments on the flatness of the spoofing material in front of the sensor. However, with the advancements in 3D reconstruction and printing technologies, this assumption can no longer be maintained. In this paper, we aim to inspect the spoofing potential of subject-specific 3D facial masks for different recognition systems and address the detection problem of this more complex attack type. In order to assess the spoofing performance of 3D masks against 2D, 2.5D, and 3D face recognition and to analyze various texture-based countermeasures using both 2D and 2.5D data, a parallel study with comprehensive experiments is performed on two data sets: the Morpho database which is not publicly available and the newly distributed 3D mask attack database.

OTHER SCHEMES

2 Factor Authentication (2FA)

- Something you have AND something you know
- Either factor is useless without the other
- Chip and PIN
- Commonly implemented in mobile phones via SMS
  - Disadvantages:
    - ONE device (if hacked)
    - SMS is easy to redirect
    - ONE point of failure for SE (phone company)

Multifactor Authentication

- Next level 2FA
- Combination of biometrics, knowledge, and possession

Behavior Profiling

- Track access behavior of users
  - Systems used
  - Times and locations when active
  - Typical usage
- Look for anomalous or fraudulent behavior
- “Why is this guy who was in Iowa 2 minutes ago logging in from Nigeria?”
- Used in fraud prevention