

Authentication



CSE 565 - Fall 2025
Computer Security

Hongxin Hu (hongxinh@buffalo.edu)

Updates

■ Assignment 1

- Deadline: **Monday, September 16**

■ Project 1 Secret-Key Encryption

- Deadline: **Thursday, September 18**
- **Environment Setup**

- ▶ Mac OS (M1/M2) users please check the new setup document:
<https://docs.google.com/presentation/d/1EY0cLCB5-1yMwqHT9NS8McxTpZI-gTLzm7lrha3Y8bM/edit?usp=sharing>
- ▶ Other users:
https://piazza.com/class_profile/get_resource/llmmx2es9cn5pv/lm4e2j8ed3u6w1

- **One question from each project in midterm (projects 1/2) or final exam (projects 3/4/5)**

What goes into system protection?

- **Authentication:** Who goes there?(password/crypto/etc.)
 - Determine whether access is allowed
 - Authenticate human to machine
 - Authenticate machine to machine
- **Authorization:** Are you allowed to do that? (Access control)
 - Once you have access, what can you do?
 - Enforces limits on actions
- **Enforcement Mechanism**
 - How its policy implemented/enforced

Night Club Example

■ Authentication

- ID Check

■ Access Control

- Over 18 - allowed in
- Over 21 - allowed to drink
- On VIP List - allowed to access VIP area

■ Enforcement Mechanism

- Walls, Doors, Locks, Bouncers



Authentication

Who Goes There?

- How to authenticate a human to a machine?
- Can be based on...
 - Something you **know**
 - For example, a password
 - Something you **have**
 - For example, a smartcard
 - Something you **are**
 - For example, your fingerprint

Something You Know

- Passwords
- Lots of things act as passwords!
 - PIN
 - Social security number
 - Mother's maiden name
 - Date of birth
 - Name of your pet, etc.
- *Passwords are one of the **biggest** practical problems facing security engineers today*

Why Passwords?

- Why is “something you know” more **popular** than “something you have” and “something you are”?
- **Cost**: passwords are free
- **Convenience**: easier for a System Administrator to reset pwd than to issue user a new thumb

Keys vs Passwords

■ Crypto keys

- Key is 64 bits
- Then 2^{64} keys
- Choose key at random
- Then attacker must try about 2^{63} keys

■ Passwords

- Passwords are 8 characters, and 256 different characters
- Then $256^8 = 2^{64}$ pwds
- Users do **not** select passwords at random
- Attacker has far less than 2^{63} pwds to try (**dictionary attack**)

Good and Bad Passwords

■ Bad passwords

- frank
- Fido
- password
- 4444
- Pikachu
- 102560
- AustinStamp

■ Good Passwords?

- jflej,43j-EmmL+y
- 09864376537263
- P0kem0N
- FSa7Yago
- 0nceuP0nAt1m8
- PokeGCTall150

Attacks on Passwords

■ Attacker could...

- Target one particular account
- Target any account on system
- Target any account on any system
- Attempt denial of service (DoS) attack

■ Common attack path

- Outsider → normal user → administrator
- May only require **one** weak password!

Password File

- Bad idea to store passwords in a file (Plaintext)
- But need a way to verify passwords
- Cryptographic solution: **hash** the passwords
 - Store $y = h(\text{password})$
 - Can verify entered password by hashing
 - If attacker obtains password file, he does not obtain passwords
 - But attacker with password file can guess x and check whether $y = h(x)$
 - If so, attacker has found password!

Dictionary Attack

- Attacker pre-computes $h(x)$ for all x in a **dictionary** of common passwords
- Suppose attacker gets access to password file containing hashed passwords
 - Attacker only needs to compare hashes to his **pre-computed** dictionary
 - Same attack will work each time
- Can we prevent this attack? Or at least make attacker's job more difficult?

Password File

- Store hashed passwords
- Better to hash with **salt**
- Given password, choose random s , compute

$$y = h(\text{password}, s)$$

and store the pair (s, y) in the password file

- Note: The salt s is **not secret**
- Easy to verify password
- Attacker must **recompute** dictionary hashes for each user — lots more work!

Password Cracking: Do the Math

- Assumptions
- Pwds are 8 chars, 128 choices per character
 - Then $128^8 = 2^{56}$ possible passwords
- There is a **password file** with 2^{10} pwds
- Attacker has **dictionary** of 2^{20} common pwds
- Probability of **1/4** that a pwd is in dictionary
- **Work** is measured by number of hashes

Other Password Issues

- Too many passwords to remember
 - Results in password reuse
 - Why is this a problem?
- Who suffers from bad password?
 - Login password vs ATM PIN
- Failure to change default passwords
- Social engineering
- Error logs may contain “almost” passwords
- Bugs, keystroke logging, spyware, etc.

Passwords

- The bottom line
- **Password cracking is too easy!**
 - One weak password may break security
 - Users choose bad passwords
 - Social engineering attacks, etc.
- The bad guy has all of the advantages
- All of the math favors bad guys
- Passwords are a **big** security problem

Password Cracking Tools

- Popular password cracking tools
 - Password Crackers
 - Password Portal
 - L0phtCrack and LC4 (Windows)
 - John the Ripper (Unix)
- *Admins should use these tools to test for weak passwords since attackers will!*

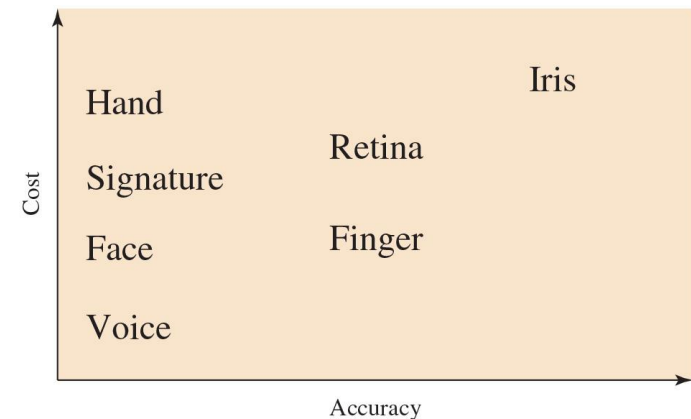
Something You Are

■ Biometric

- “You are your key” — Schneier

□ Examples

- Fingerprint
- Handwritten signature
- Facial recognition
- Speech recognition
- Gait (walking) recognition
- “Digital doggie” (odor recognition)
- Many more!



Cost versus accuracy of various biometric characteristics in user authentication schemes

Why Biometrics?

- Biometrics seen as desirable replacement for passwords
- Cheap and reliable biometrics needed
- Today, a very active area of research
- Biometrics are used in security today
 - Thumbprint mouse
 - Palm print for secure entry
 - Fingerprint to unlock car door, etc.
- But biometrics not too popular
 - Deed additional devices
 - Cannot be changed

Something You Have

- Something in your possession
- Examples include
 - Car key
 - Laptop computer
 - Or specific MAC address
 - Password generator
 - We'll look at this next
 - ATM card, smartcard, etc.
 - Google Wallet

2-factor Authentication

- Requires 2 out of 3 of

1. Something you know
2. Something you have
3. Something you are

- Examples

- ATM: Card and PIN
- Credit card: Card and signature
- Password generator: Device and PIN
- Smartcard with password/PIN

Single Sign-on

- A hassle to enter password(s) repeatedly
 - Users want to authenticate only once
 - “Credentials” stay with user wherever he goes
 - Subsequent authentication is transparent to user
- Single sign-on for the Internet?
 - Microsoft: **Passport**
 - Everybody else: **Liberty Alliance**
 - Security Assertion Markup Language (**SAML**)

Social Engineering Attacks



Invoice- #98AS8H2358F3K

Date : 09-15-2023

Dear Customer,

Your Account Has Been Charged With USD 489.99 And Will Be Going To Debit From Your Account. If You Did Not Recognize This Transaction Or Want To Cancel These Charges. Please Contact Toll Free Customer Care Number : **+1 (808) 978 9198**

Product Information

Product	Price	Quantity	Gand Total
Security Service	\$489.99	1	\$489.99

Product Code:- GV58JN69IK

Payment Method : Auto-Debit

Once the amount has been debited we will send you a notification mail about the charges of your current account

Terms and Conditions

If this payment never done by you then please contact us at soon as possible

How to Stop Subscription, Call Customer Care Executive : **+1 (808) 978 9198**

Social Engineering Attacks


Renewal Invoice Payment Status Update #JUHG-8754 Inbox x

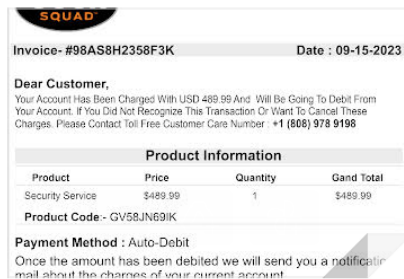


Gerald fields <fieldsgerald280@gmail.com>

to bcc: me ▼

#LKMB-2587

One attachment • Scanned by Gmail 



Questions?

A horizontal bar spanning the width of the slide, divided into three equal segments. The left and right segments are orange, and the middle segment is green.