Information Security and Privacy

BCS1110

Dr. Ashish Sai

🗓️ Week 5 - Lecture 1 & 2

💻 bcs1110.ashish.nl

Plan

- Encryption
- Misconception vs Reality
- Passwords
- ~~Viruses and Malware~~
- ~~Other Common Attacks~~
- ~~Cryptocurrency~~
- ~~Privacy~~

Why care

- **Technology is not 100% safe!**
- So many people have been compromised on the Internet
- "Help I'm in trouble and I need you to wire me €5000" emails from friends
- People steal credit card numbers on sketchy websites
- Sites that "look" like the original but are fakes (www.stanfordedu.com)

Why care

- **Physical analogy**
- Usually, we don't leave our door unlocked when we leave home. Similarly, we have passwords for Internet accounts
- Having a password like "password" is like leaving an unlocked lock on your door

Encryption

Part 1/7

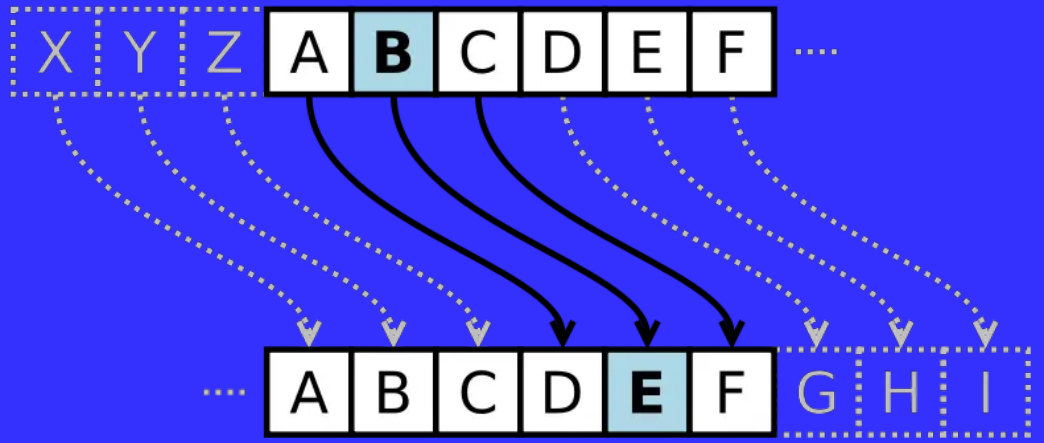
Security and Encryption

- Protects data from prying eyes. Several checks to make sure only you can access your information.
- **Encryption: puts the data in a secret code (ciphertext)**
- **Decryption converts the ciphertext to plaintext using a key**

Security and Encryption

- **Basic encryption: Caesar cipher**
  - Shift all the letters in the text by some number
  - The number you shifted by is the key
- **More complicated: One-time Pad**

> Hacker's ultimate goal: get the plaintext



Hiding in plain sight: Steganography

- Can hide sensitive information inside other information (need to know what you're looking for)
- Encryption protects the message when overheard
- Steganography prevents the message from being found

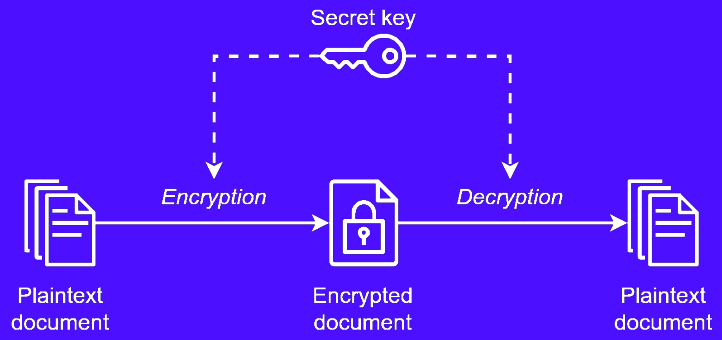
Open and Secret

- Surprisingly, the best practice is:
  - Use a scheme that is open and published (i.e. peer review)
  - Only keep the key secret

Example: World War 2 Enigma

Classical Cryptography (“Symmetric”)

- Encrypts and decrypts with the same key (kept secret)
- AES standard, mature, reliable and widely used
  - Provides **secrecy** and **authenticity**



Can you break it?

- Encryption is reliable if the attacker must guess through all the keys —aka "brute force" attack
- Any encryption can be attacked brute force

Key-Length vs Brute Force

- Suppose: the attacker guesses 1 thousand keys per second
- 86400 seconds in a day so **86 Million **guesses per day
- Suppose: the key is 8 letters long (Lowercase+Uppercase)
- **Question**: How many keys are there? -> $(26 + 26)^8$ = $5 * 10^{13}$
- **Question**: How long does it take to guess the right key?
  $5 * 10^{13}$/8.6e6 = Almost 500,000 days!
- **Double key length squares the key space!**

Encryption Application: HTTPS

- When you visit https://bcs1110.ashish.nl
  - Browser on one end and Ashish.nl server on the other
  - These two create an encrypted pipeline for communication using a key only known to these two (the actual implementation is a lot more complicated!)

> Logging in to ashish.nl from Coffeelovers is safe!

Encryption Application: Disk Encryption

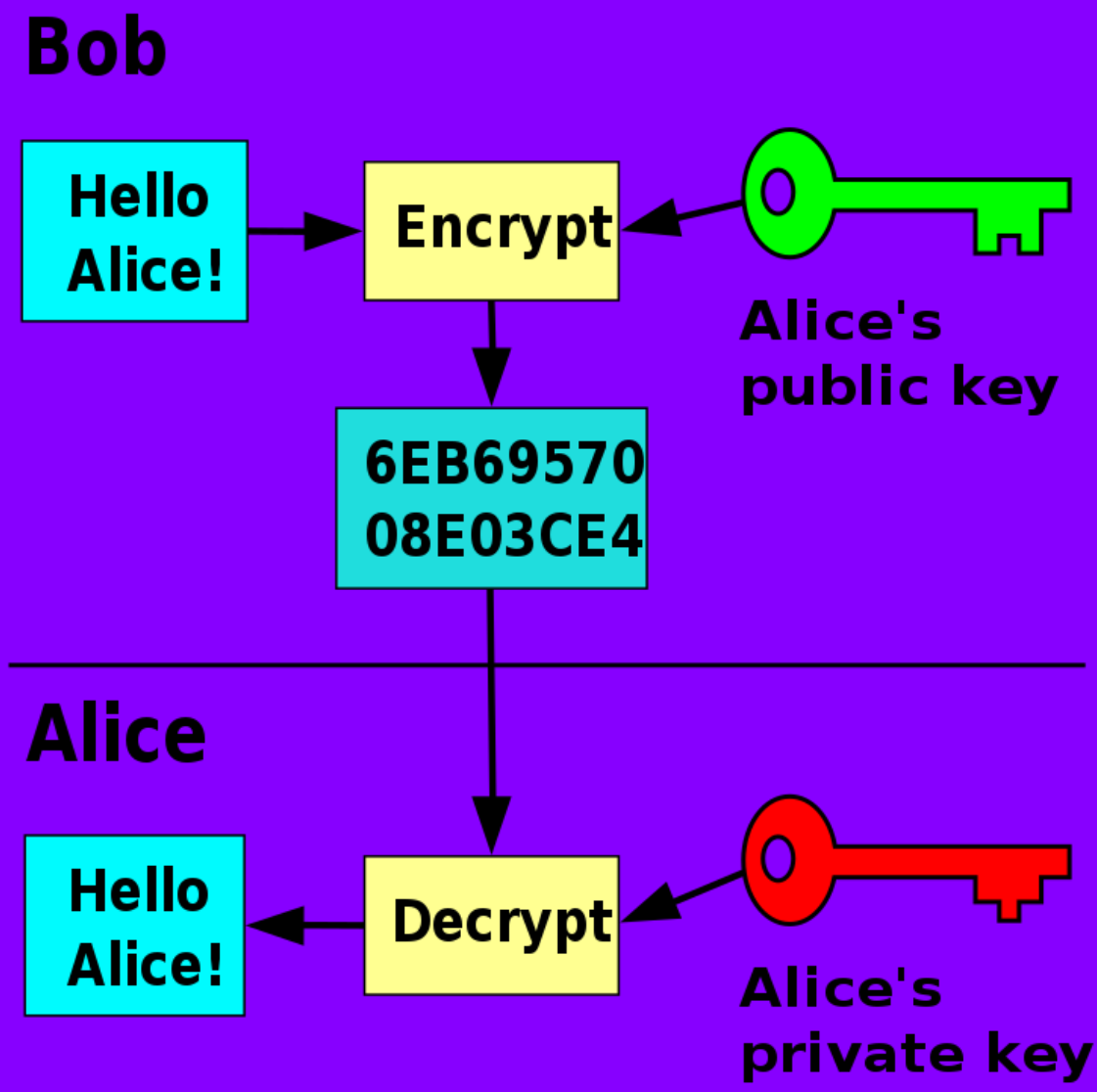
- Suppose you have a spreadsheet with your clients BSN
  - Laptop gets stolen!
- Solution: Encryption (whole disk or just the sensitive files)
- UM Staff are supposed to enable disk-encryption!
- Issues: San Bernardino terrorist phones were encrypted

Modern Cryptography: Public Key ("Asymmetric")

- Significant jump up in capability from classical-symmetric crypto
- Instead of a single secret key, there are 2 keys:
  - private key – kept secret (priv)
  - public key – can be shared (pub)
- The 2 keys are mathematically linked

Public Key Encryption

- Motivation: How do you prove your identity on the internet?
- **A website has a private key and gives out its public key**
- Public key lets you check that the site is who they say they are
- Public key is issued by a certificate authority to limit impersonation
- **Private keys are used to generate a shared key for the actual encryption**


Bob
Hello Alice!
Encrypt
Alice's public key
6EB69570 08E03CE4
Alice
Hello Alice!
Decrypt
Alice's private key

Public Key Application: Digital Signature

- Generate a pub/priv pair on a machine
- Publish the pub key
- Priv key never leaves the machine
- Digital signature: use the priv key to "sign" a PDF, creating a signature
  - 1 Anyone can use the pub key to verify signature
  - 2 Only the holder of the priv key can make the signature

Public Key Application: Bitcoin

More on this later!

Misconception vs Reality

Part 2/7

Misconception vs Reality

Myth 1: Humans read my Facebook messages and give me ads

- All messages sent through Messenger are NOT encrypted
- When you send a message to a friend, your message is sent in plaintext, Facebook's AI extracts keywords from it, and your friend receives the message in plaintext
- The keywords inform the ads
- This sounds bad. What message services send/receive data in plaintext?
  - Facebook (Messenger)
  - Gmail (and Hangouts)

Misconception vs Reality

Myth 1: Humans read my Facebook messages and give me ads

- What message services are end-to-end encrypted?
  - WhatsApp
  - Signal
  - iMessage
- End-to-end encrypted means the message is encrypted when it leaves your phone and decrypted only on your friend's end. The service provider sees gibberish.

Misconception vs Reality

Myth 2: I'm "safe" if I use incognito mode

- The only thing incognito / private browsing modes do is not record your browser history
- Every server knows every client IP address that makes a request to it (ex: Google knows every IP address that hits google.com)
- IP addresses can be traced back to a device

Misconception vs Reality

Myth 2: I'm "safe" if I use incognito mode

- What can I do to visit websites without them knowing who I am?
- Use a VPN or proxy. VPN services mask your IP address with an IP address in a foreign location. So if you visit a website, the server will think you're coming from a different location.

Misconception vs Reality

Myth 3: My password is long and non-guessable. I can use this password for all my accounts and not be worried.

- Just because your password is hard to crack doesn't mean you can use it everywhere
- Some sites store passwords in plaintext (horrible!) If someone attacks the site and gets your password, you'd have to update all your other passwords...

Misconception vs Reality

Myth 3: My password is long and non-guessable. I can use this password for all my accounts and not be worried.

- Solution: use a different password for every site (password manager). You have one password to get into your password manager, which stores generated passwords for all your accounts.
- Why is this a good solution?

Passwords

Part 3/7

Passwords

- Computer security is a critical area often **dramatized** in movies
- Computer security is like a castle with walls
  - Computers have internal and external aspects
  - Bad guys need strategies like obtaining passwords or tricking computers

Hashing

- What happens when there is a security breach?
- **Sensitive information is "hashed" - turned into random-looking information**
- Hash: mathematical function that takes in a plaintext, returns random-looking information
- **Idea: instead of comparing the password entered to your password, we compare the hash of the entered password to your password**
- Companies should only store hashed passwords

Passwords

- Should be between sites
- Should be long
- Use a password manager!
- **What if someone attacks the password manager? Okay because they don't store your master password. Your master password is stored in Dropbox or Google Drive.**

Multi-Factor Authentication

- Knowledge: something you know (password)
- Possession: something you have (device, such as a cellphone or yubikey)
- Bio-metric: something you are (fingerprint, retina scan)

Attacks to get passwords

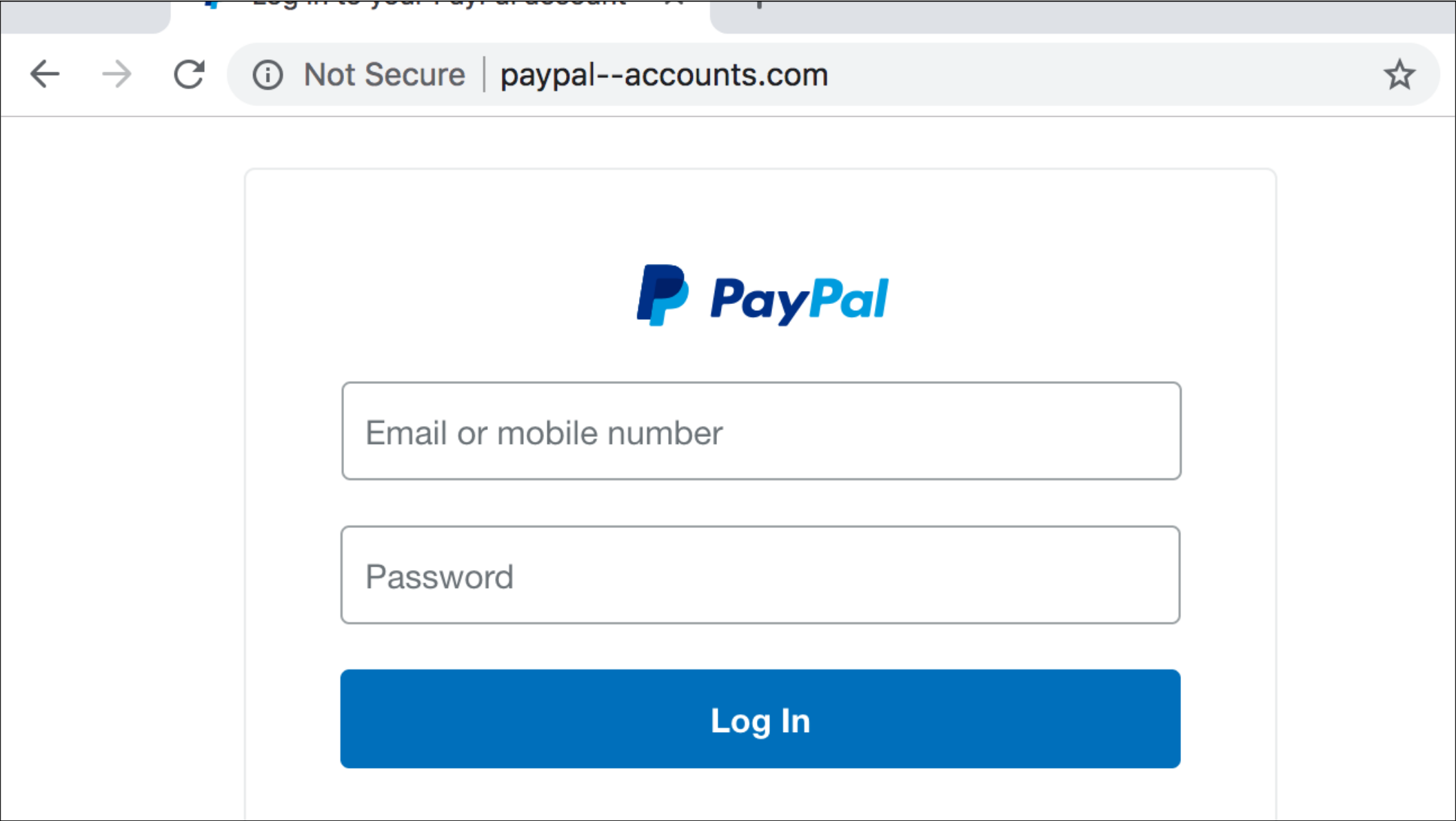
- Phishing
- Dictionary Attack

Social Attacks (Phishing)

- “Phishing" is a type of attack where the bad guy tricks you into typing your password into a bad guy site, thus the bad guy gets your password
- You have probably received many phishing emails. The phishing email most often includes a link to a page such as the one shown below

Social Attacks (Phishing)

- Attacker relies on goodwill/gullibility of people
- Redirect to a fake URL and get the user to type in a password (Google Docs)
- Impersonate someone else and ask for a password (Clinton Leaks)
- **Counter: Always check the URL, and verify whom you give info to**
- Other social attack: pretend to belong, and tailgate into a building
- **Counter: it's better to be safe than to be nice**


Not Secure
paypal--accounts.com
PayPal
Email or mobile number
Password
Log In

Fake ATM Machine

- Funny "phishing" crime in real life
- Fake ATM in front of bank, prints error message, but records card details and PIN for bad guy

Email Phishing vs 2016 US Election

- John Podesta got a fake google-account email reset
- His IT person meant to write "illegitimate" but wrote "legitimate" - typo of the century!
- Apparently Podesta used same password to secure twitter, so they got that too
- Podesta did not have two-factor enabled


From: Google <no-reply@accounts.googlemail.com>
Date: March 19, 2016 at 4:34:30 AM EDT
To:
Subject: *Someone has your password*
Someone has your password
Hi John
Someone just used your password to try to sign in to your Google Account
.
Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine
Google stopped this sign-in att u should change your password
immediately.
CHANGE PASSWORD <https://bit.ly/>

HTTPS: Secure Web Communication

HTTPS: secure version of HTTP for web data transfer.

- Two Main Purposes:
  - a. Domain Verification: Prevents phishing via domain identification
  - b. Data Encryption: Safeguards transmitted data from interception
- HTTPS assures secure connections, yet users must verify URLs to avoid phishing.
- It demands domain ownership authentication through certificates, impeding malicious replication
- Users can verify sites via HTTPS certificates, usually denoted by a padlock icon

Atypical Spear Phishing Case

- A specifically crafted and sophisticated attack against a specific person
- Likely to succeed if the attacker has money and motivation
  - e.g. if the CIA or someone with a billion dollars really wants your files ..
    - They could sneak into your house/hotel at night and tamper with your hardware
- Therefore: super-motivated attacker will likely succeed
  Except "encryption" which nobody can break (**yet**)

Typical Attacks - Bulk

- Typically the bad guys are not crafting some attack just for you
- They send out millions of generic attacks, just snaring who falls for it
- If you avoid the most common errors, you will probably be fine

Dictionary Attack

- Try every known password
  - as if they are trying all the words in a dictionary
- Try common passwords as guesses (“password” or “password1”)
- 1 guess/second = 31 million guesses per year

> fails mostly, but works some percentage of the time

```
...
May  6 09:12:20 bcs1110 sshd[30924]: Failed password for invalid user alex from 49.212.7.205 port 36268 ssh2
May  6 09:12:22 bcs1110 sshd[30926]: Failed password for invalid user alex from 49.212.7.205 port 36605 ssh2
May  6 09:12:26 bcs1110 sshd[30928]: Failed password for invalid user alex from 49.212.7.205 port 36937 ssh2
May  6 09:12:29 bcs1110 sshd[30930]: Failed password for invalid user adam from 49.212.7.205 port 37212 ssh2
May  6 09:12:32 bcs1110 sshd[30932]: Failed password for invalid user fax from 49.212.7.205 port 37546 ssh2
May  6 09:12:34 bcs1110 sshd[30934]: Failed password for invalid user fax from 49.212.7.205 port 37864 ssh2
May  6 09:12:38 bcs1110 sshd[30936]: Failed password for invalid user demo from 49.212.7.205 port 38201 ssh2
May  6 09:12:41 bcs1110 sshd[30938]: Failed password for invalid user demo from 49.212.7.205 port 38561 ssh2
May  6 09:12:44 bcs1110 sshd[30940]: Failed password for invalid user amanda from 49.212.7.205 port 38911 ssh2
May  6 09:12:47 bcs1110 sshd[30942]: Failed password for invalid user angie from 49.212.7.205 port 39244 ssh2
May  6 09:12:51 bcs1110 sshd[30944]: Failed password for invalid user angie from 49.212.7.205 port 39552 ssh2
...
```

Who is attacking us?

Announced By		
Origin AS	**Announcement**	**Description**
AS4134	202.109.128.0/18 ✅	CHINANET Jiangxi province network

Weak Passwords

- How would a hacker guess password?
  - 1 Dictionary of words
  - 2 List of commonly used passwords from other sites
  - 3 Heuristic changes
    - batman
    - generate automatic variations: batman1, batman2, batman3,bat.man,iheartbatman

> Avoid anything from common list

Strong Passwords

- No need to have super elaborate passwords to be secure (some sites go crazy with this!)
- What makes a password stronger:
  - Longer
  - More characters: lower, upper case, digits etc
  - Not a word or pun
- Simple password = kittens
- Strong password = KottensX,97erx

Cracking Passwords

- Very different from outside case, the bad guys already have encrypted or hashed password from site
  - "cracking" is trying to decrypt the stolen passwords, many per second
  - cracking can be done at rates of a billions of guesses per second: most passwords are guessed within a few days
- Therefore: If a site is compromised, assume the passwords will be exposed

What to do

- Counter: programmers can build in a short delay so it takes longer to try passwords
- Counter: programmers can limit number of attempted logins
- Counter: make your password unique AND long
- Counter: Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA)

- Second thing to log in
  - Typically something you
    - SMS
    - OTP generator App (Microsoft Authenticator, Apple Passwords)
    - U2F (Apple Passkey)

Issues with SMS based 2FA

- 3 weaknesses
  - 1 Bad guys could trick your mobile provider: FTC's lead Technologist gets hacked
  - 2 Phishing
  - 3 Malware on phone (more on this in a bit)

Future of 2FA: U2F

- Device acts as the 2nd factor
  - Apple passkeys
  - Google passkeys

See you doing Exam prep!