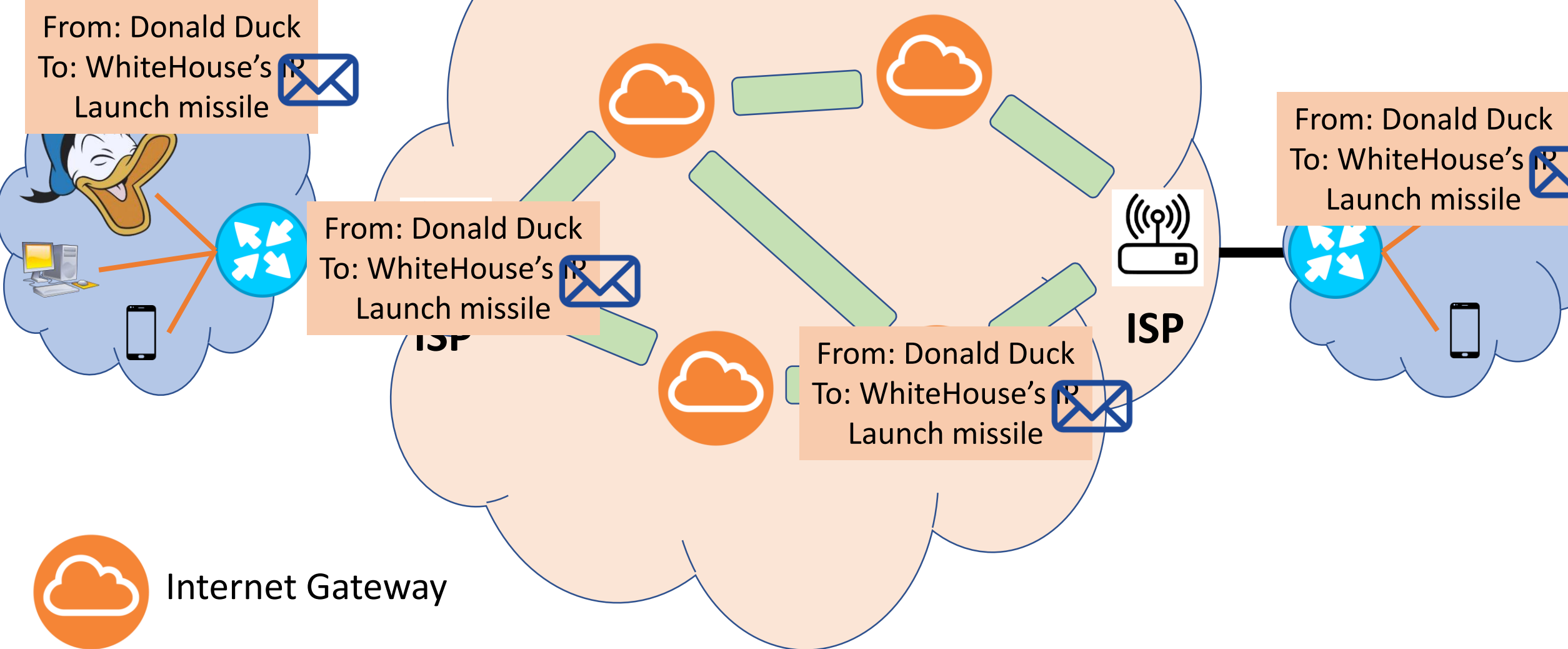


Internet Security

Subject: 805-182 Computer: the Internet and Society

Dr. Norrathep Rattanvipanon

Good o' Internet



From: Donald Duck
To: WhiteHouse's IP
Launch missile

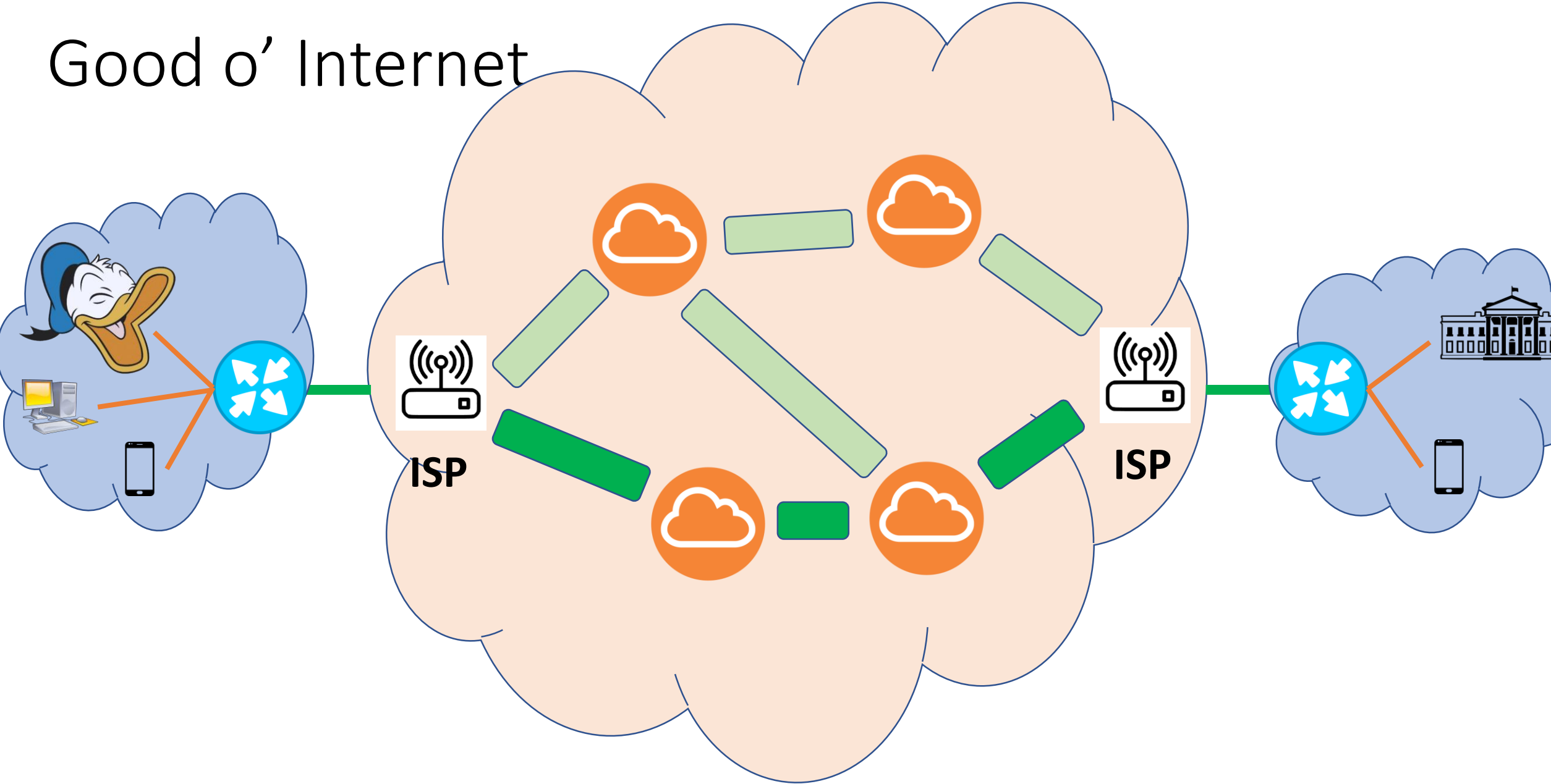
From: Donald Duck
To: WhiteHouse's IP
Launch missile

From: Donald Duck
To: WhiteHouse's IP
Launch missile

From: Donald Duck
To: WhiteHouse's IP
Launch missile

 Internet Gateway

Good o' Internet



What could go wrong?



Confidentiality Problem:

Intermediate gateways can read messages

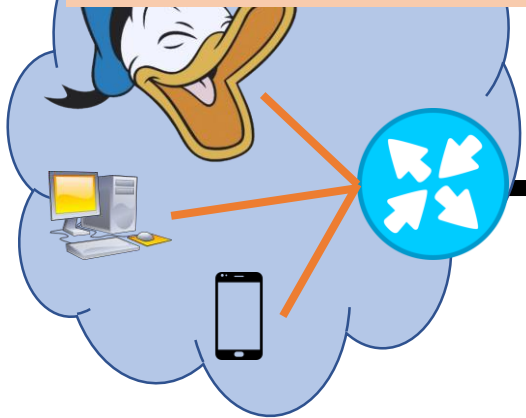
Integrity Problem:

Part of messages could get dropped or modified

Authenticity Problem:

Can impersonate as Donald Duck and send messages on his behalf

From: Donald Duck
To: WhiteHouse's IP
Launch missile

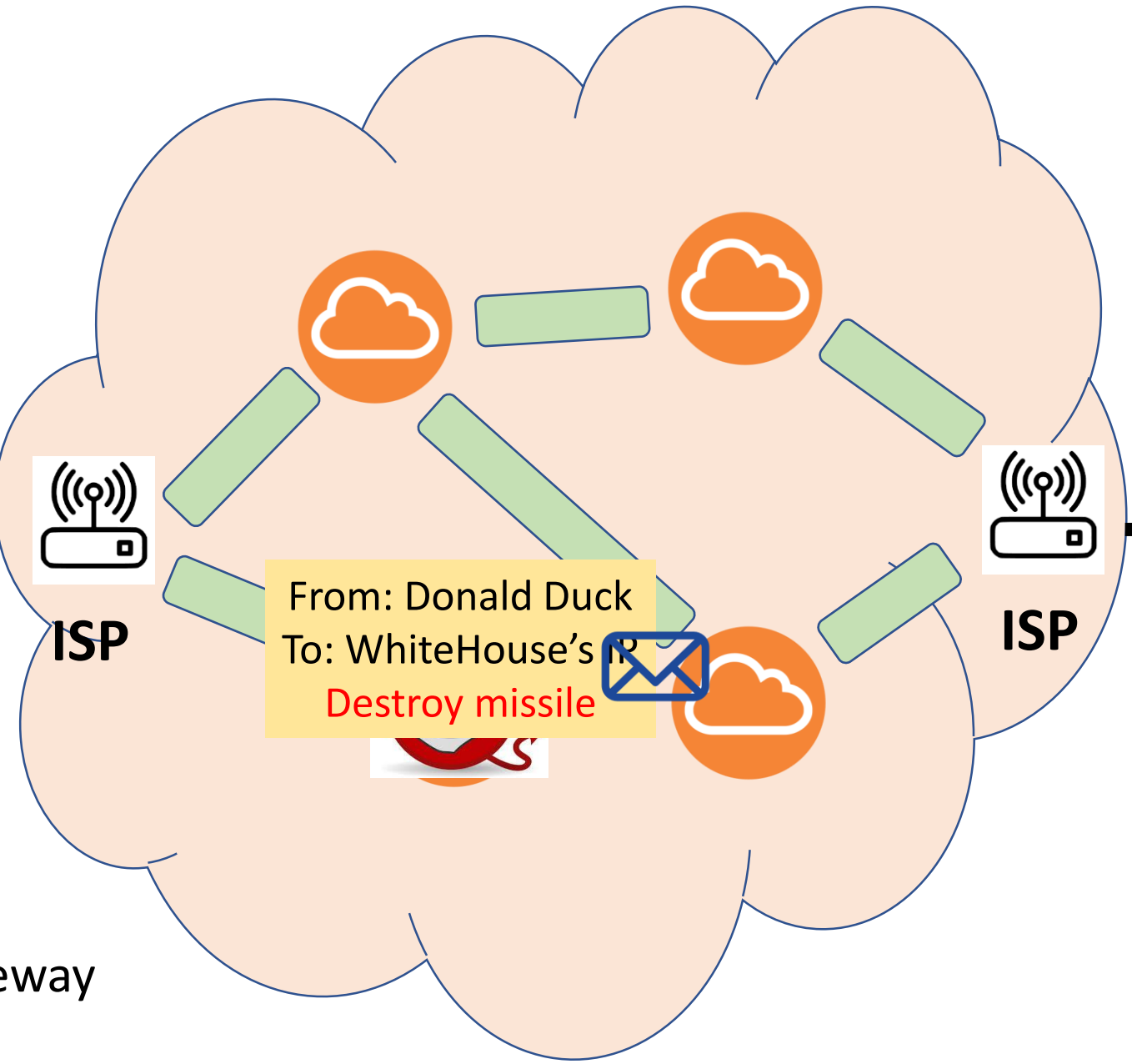


ISP

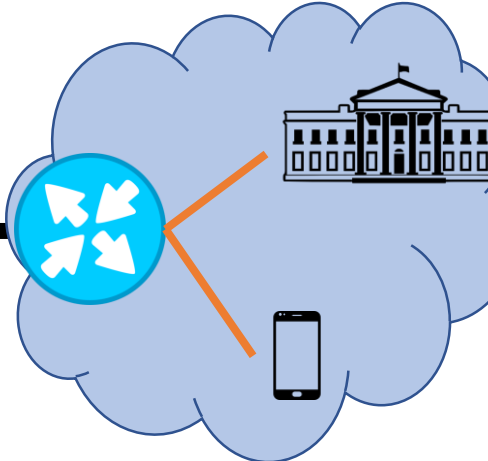
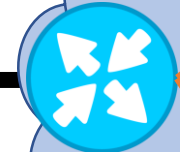
From: Donald Duck
To: WhiteHouse's IP
Destroy missile



Internet Gateway



ISP

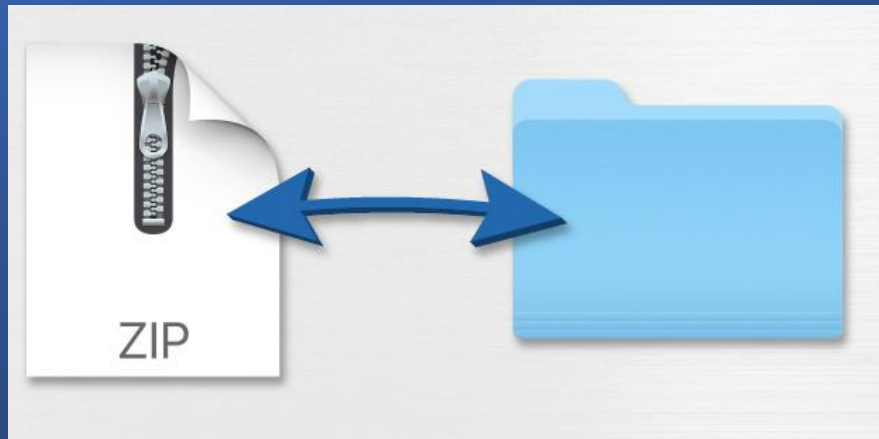




Encryption

- Analogy: put a lock on your envelope
- Only the receiver has access to the corresponding key
- Prevent anyone without key to open your envelope
- **Solve Confidentiality Problem**
- **No one except the receiver can read your message**

Message Hash



- A compressed version of a message
- Think of a hash to be a zip file of the message
- Sender: send message and hash
- Receiver: only accept message if hash = $\text{HASH}(\text{message})$
- Guarantee that message is received **entirely**
- **Solve Integrity Problem**
- **If your message is modified during transmission, the receiver will notice this**

Digital Certificate



- **Solve Authenticity Problem**
- Attach a certificate along with a message
- Certify that message is created by you
- **No one can claim to be you!**



Preventing
Confidentiality,
Integrity, and
Authenticity
Problems

Encryption + Hash + Digital Certificate

- = HTTPS
- **HTTPS websites** = secure websites
- No one can read/modify your messages or impersonate you in HTTPS websites
- **HTTP website = non-secure website**

Task: 10- minute



How can you tell whether a website is HTTPS or HTTP?



How do you check whether a website certificate is valid?



Give examples of HTTP websites

What you
should NOT
do when
using **HTTP**
websites

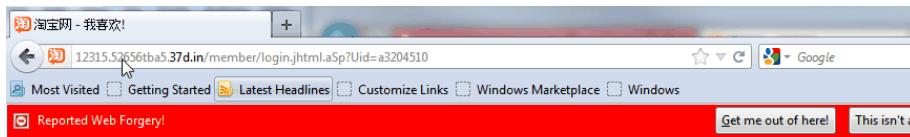
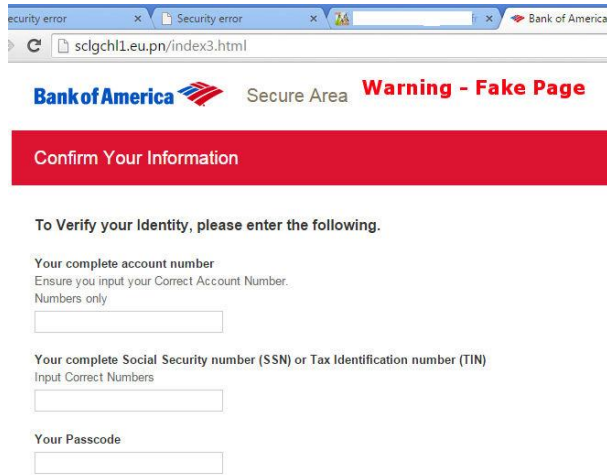
- Provide sensitive/confidential information
 - National ID, bank account number, passwords, etc.

Why?

- Trust everything as if it comes from that website

Why?

- (In fact, don't trust everything from the internet)
- My suggestion: avoid using HTTP websites



淘宝网



手机登录m.taobao.com, 随时随地购物

推荐使用搜狗浏览器-淘宝专版, 点此下载>>

Phishing Website

- Look like or the same as legit websites
- Aim to steal sensitive information, e.g., username/passwords, national ID, social security number
- Trick you to download malware/virus
- Caused by: mistyping URL, clicking links from email/social media, etc.

Preventing Phishing Websites



Check website URL
(every character):

www.facebook.com

vs

www.faceb00k.com



Check certificate and whom it is
issued to



If possible, use multi-factor
authentication (MFA)

Email Scams



From: updates@em.linkedin.com
Date: November 29, 2011 7:49:07 AM EST
To: Your Name
Subject: LinkedIn Security Notice

LinkedIn

For security reasons, ju-spandau.de/415420/index.html has been blocked due to inactivity or because of too many failed logins. [Click to follow link](#)
Please [click here](#) for details.

Thank you for using LinkedIn!

--The LinkedIn Team
<http://www.linkedin.com/>
© 2011, LinkedIn Corporation

NOTE: Do not click link. Move your mouse over link and notice that it does not direct towards LinkedIn. This is not from LinkedIn.

From: WellsFargo - Support_Online <WellsOnlineBank2@comcast.net> **1**
Date: December 8, 2017 at 2:23:01 PM EST
To: Undisclosed-Recipients;;
Subject: **!Alerts!** **2**



wellsfargo.com

Security Information Regarding Your Account.

We are sorry, **For your protection and security reasons,** your Wells Fargo account has been locked. **2**

Please click on the following link to unlock your account.

Log-in to :<https://www.wellsfargo.com/online-banking/updating> **3**

Thank you for bringing this matter to our attention.

Sincerely,
Wells Fargo Online Banking Team.

wellsfargo.com | [Fraud Information Center](#)

From: State Bar <suzie.chamberlain.statebar@madiii.se>
Sent: Tuesday, September 6, 2005 11:36 AM
To: Joubert, Erica <ejoubert@mcmanislaw.com>
Subject: You login needs to be changed
Attachments: info.zip

Dear Attorney:

We see you have attempted several times to login to your account. Your account access has been locked out. Click here to change your password quickly. [Change password Here.](#)

When accessing our site simply enter your social security number to update your password.

Thank you for using our online access,

james jackson
Online accounts manager

STATE BAR

Want to help? You can! State Bar is committed to helping those effected by Hurricane Katrina. You can make a [donate here.](#)



Recognize and Prevent Email Scams

- Always check the sender email address
 - Use search engine to confirm authenticity
 - Email address can be spoofed easily
- Always double check URL links
- Be suspicious of “too-good-to-be-true” email
 - Especially about money

A close-up, grayscale photograph of a computer keyboard. The central focus is a single key marked with a white 'X'. The surrounding keys are blurred, creating a shallow depth of field. The overall tone is dark and professional.

Password

Rule#1: Don't tell anyone your password!

What are passwords?

- Secret codes used to access devices/services/applications
 - Email, phone, social media
- Something you know
- Only persons with the correct password can have access
- Consist of: numbers, upper/lowercase letters and symbols

Username

Password [Forgot your password?](#)

Keep me logged in (for up to 30 days)

Log in



Why need strong
passwords?

Techniques for cracking passwords

- Shoulder surfing attacks
 - Look over your shoulder when you input passwords
- Prevent: Make sure no one is watching when you input passwords

- Brute-force attacks
 - 4-digit PIN: 0001, 0002, 0003, 0004, 0005, ..., 9999
- Prevent: Make it long, use a wide range of characters

- Dictionary attacks
 - People tend to use dictionary words when creating password
 - Dictionary words: cat, dog, people, password, eat, etc.
- Prevent: avoid using only 1 or 2 words in your password



```
Dictionary Attack
Trying apple      : failed
Trying blueberry  : failed
Trying justinbeiber : failed
...
Trying letmein    : failed
Trying s3cr3t    : success!
```

How long does it take to crack your passwords?

How long will it take to crack your password?

Length of Password (Chars)	Only Numbers	Mixed Lower and Upper case alphabets	Mixed numbers, Lower and Upper case alphabets	Mixed numbers, Lower and Upper case alphabets , symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years
18	126 years	1tn years	374tn years	1qt years

Most Commonly Used Passwords

What Are the 50 Most Common Passwords?



Based on most common duplicate passwords within a breach of over 30 million accounts.

1.	123456	11.	123321	21.	222222	31.	333333	41.	password1
2.	123456789	12.	1q2w3e4r5t	22.	112233	32.	123qwe	42.	q1w2e3r4
3.	qwerty	13.	iloveyou	23.	abc123	33.	159753	43.	qqww1122
4.	password	14.	1234	24.	999999	34.	q1w2e3r4t5y6	44.	sunshine
5.	1234567	15.	666666	25.	777777	35.	987654321	45.	zxcvbnm
6.	12345678	16.	654321	26.	qwerty123	36.	1q2w3e	46.	1qaz2wsx3edc
7.	12345	17.	555555	27.	qwertyuiop	37.	michael	47.	liverpool
8.	1234567890	18.	gfhjkm	28.	888888	38.	lovely	48.	monkey
9.	111111	19.	7777777	29.	princess	39.	123	49.	1234qwer
10.	123123	20.	1q2w3e4r	30.	1qaz2wsx	40.	qwe123	50.	computer

Characteristics of strong passwords

- Minimum length: 10
- Both uppercase and lowercase characters
- At least one number and one symbol

**WHEN YOU HAVE TO CHANGE YOUR
PASSWORD AND IT REQUIRES IT TO**

**HAVE OVER TWENTY LETTERS, FIVE
NUMBERS, THREE SYMBOLS AND THE
BATMAN SYMBOL**

Never reuse passwords (even though they are secure passwords)

Case Study:

1. Hacker gets a victim's username and password (due to password leakage from a webprovider)
2. He uses the same password to log in victim's email and Facebook accounts
3. He looks at the victim's email and realizes that the victim stays at a specific hotel for a vacation
4. Using this information, hacker gives the victim a smartphone and tricks him to insert his SIM card to the smartphone
5. Using the SIM card, hacker controls victim's banking application (that requires SMS authentication) and transfer all his money to hacker's bank account
6. Also, hacker logs in to victim's Facebook account asking more money from victim's friends

Damage: victim lost 400,000 baht

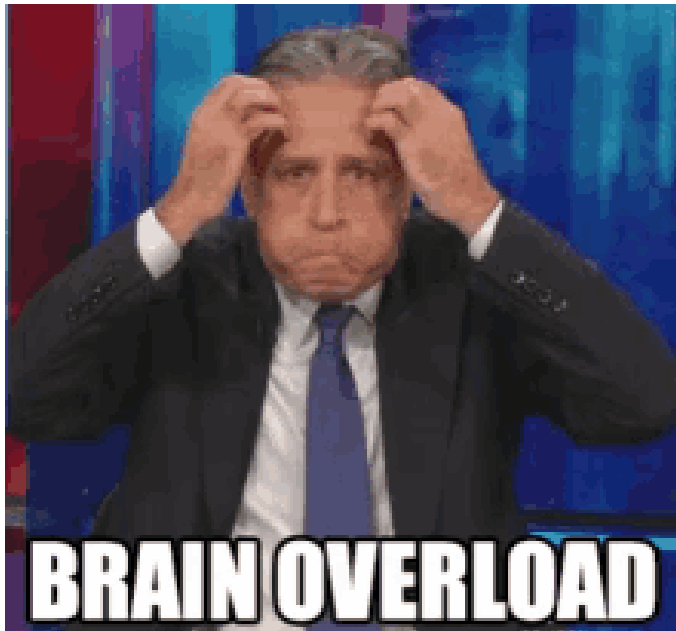
<https://hilight.kapook.com/view/202574>

Password Rules

- Don't use weak passwords (e.g., your public info, dictionary word, only numbers)
- Don't reuse passwords
- Don't write down passwords
- Also don't tell anyone your passwords 😊

Activity: Kahoot

Password Rules



- Don't use weak passwords (e.g., your public info, dictionary word, only numbers)
- Don't reuse passwords
- Don't write down passwords
- Also don't tell anyone your passwords 😊
- Best password: random password like "Gx`p5<W&2Jfn9^`"

How do you expect to remember all your passwords?

Password Manager

- No need to memorize multiple passwords, only memorize one master password!
- Automatically provide a strong password when you:
 - Create a password for a new website
 - Login to a website
- Work for all websites
- Only need to remember master password
 - Master password must be very strong



Demo: Lastpass

Task: 10-
minute



Give examples of password manager that also works on your mobile phone



What are disadvantages of using password manager?

Disadvantage of Password Manager

- Trust your password manager
- If it is malicious or compromised, all your passwords will be leaked
- Make sure your master password is strong and not reused

Passwords are bad

- Even if you have the best password and protect it well ...
- ... this password may be leaked from the website.

Massive breach leaks 773 million email addresses, 21 million passwords

The best time to stop reusing old passwords was 10 years ago. The second best time is now.

Russia gang hacks 1.2 billion usernames and passwords

🕒 6 August 2014

12 DEC 2019 **NEWS**

Over One Billion Email-Password Combos Leaked Online

Passwords are bad

- Is there a better way to strengthen security of your email/application account if we don't use passwords?
- We will talk about this on Thursday!



A dark, irregular ink blot with the word "Malware" written in white text in the center. The blot has a textured, splattered appearance with some lighter areas and small droplets around the edges. The background is white.

Malware

What is malware?

- **Malicious Software**
- Ransomware
- Spyware
- Worms
- Keyloggers
- Bots
- Etc.

Defense against Malware

01

Do not install suspicious or pirated software/applications

02


Always have firewall and anti-virus software enabled

03

Scan virus (in anti-virus software) regularly

04

Always keep software and operating systems up-to-date



Q/A

In-class assignment

Passwords are bad. One way to strengthen security of your email/application account is to use “multi-factor authentication” (MFA)

Each person answers one of the following question:

- Describe and explain 3 “authentication factors” and give a real-world example of each authentication factor
- Give an advantage of each authentication factor
- Give a disadvantage of each authentication factor
- Explain why MFA is more secure than just using a password
- Find a mobile application that requires using MFA to login and list step-by-step how you use MFA to login that application
- Explain why using SMS messages as an authentication factor is considered a bad idea.

Group Presentation

- Online research a real-life case study of security or privacy issues on the internet
- Make PPT presentation with the following suggested topics:
 - Detailed story: what happened in that case study?
 - Problem: What is a source of the problem?
 - Solution: How would it have been mitigated?
- Present it next Thursday: 5-10 minutes
- Example: [Garmin hack](#), [Twitter Bitcoin Scam](#), [Dyn Attack](#), [Equifax Breach](#), [Sina Weibo Breach](#)