CS 4173/5173
COMPUTER SECURITY

DoS Attacks on the Internet

OUTLINE LAST TIME

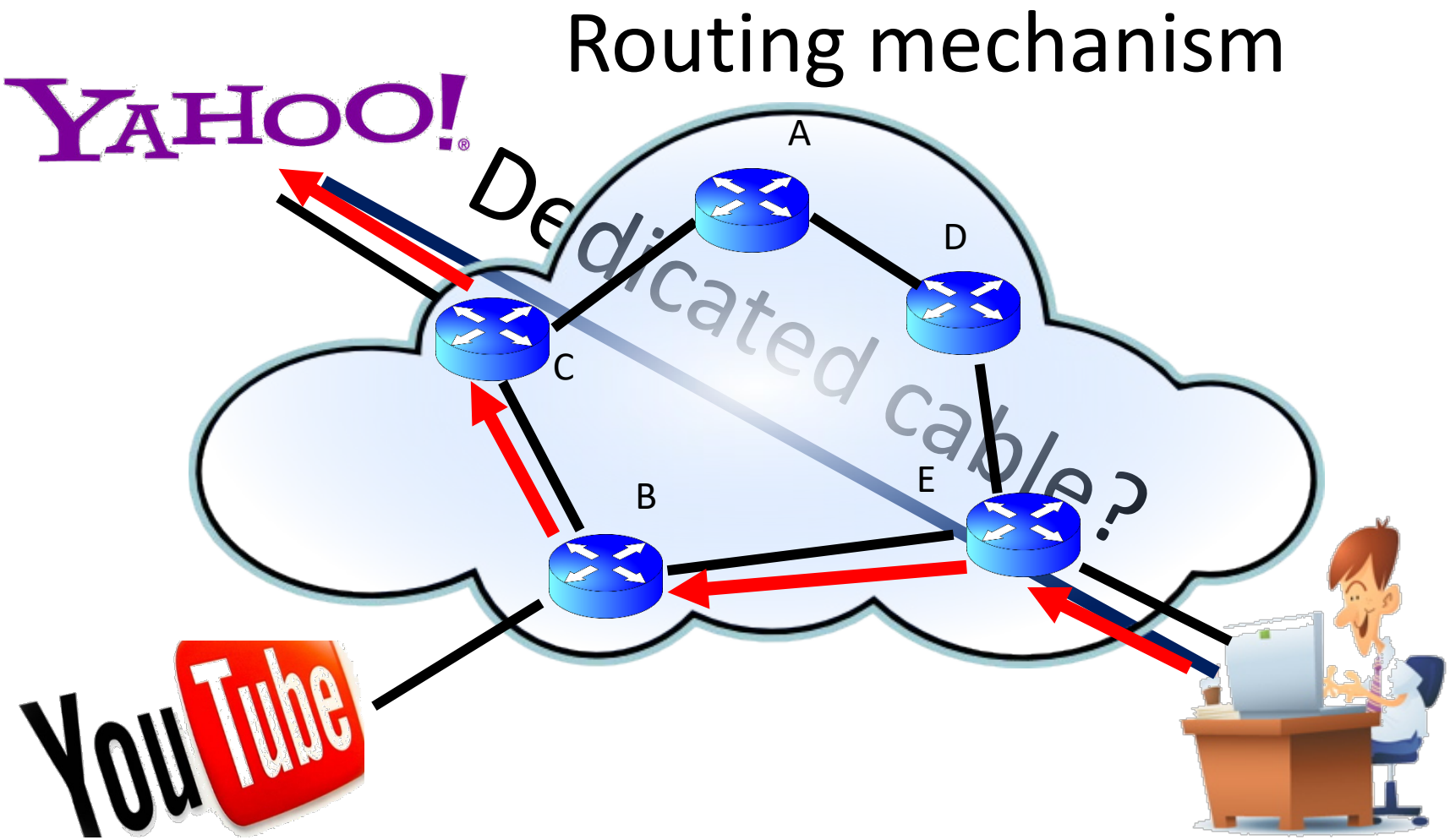
- Security objectives
  - Confidentiality
  - Integrity
  - Availability
- Security services
- Security assurance
- Security by
  - Cryptography
  - Obscurity
  - Legislation
- Threat and vulnerability

DENIAL-OF-SERVICE ATTACKS

- Typical attacks targeting availability
  - Computers
  - Networks

- Cryptography is not designed against Denial-of-service (DoS) attacks

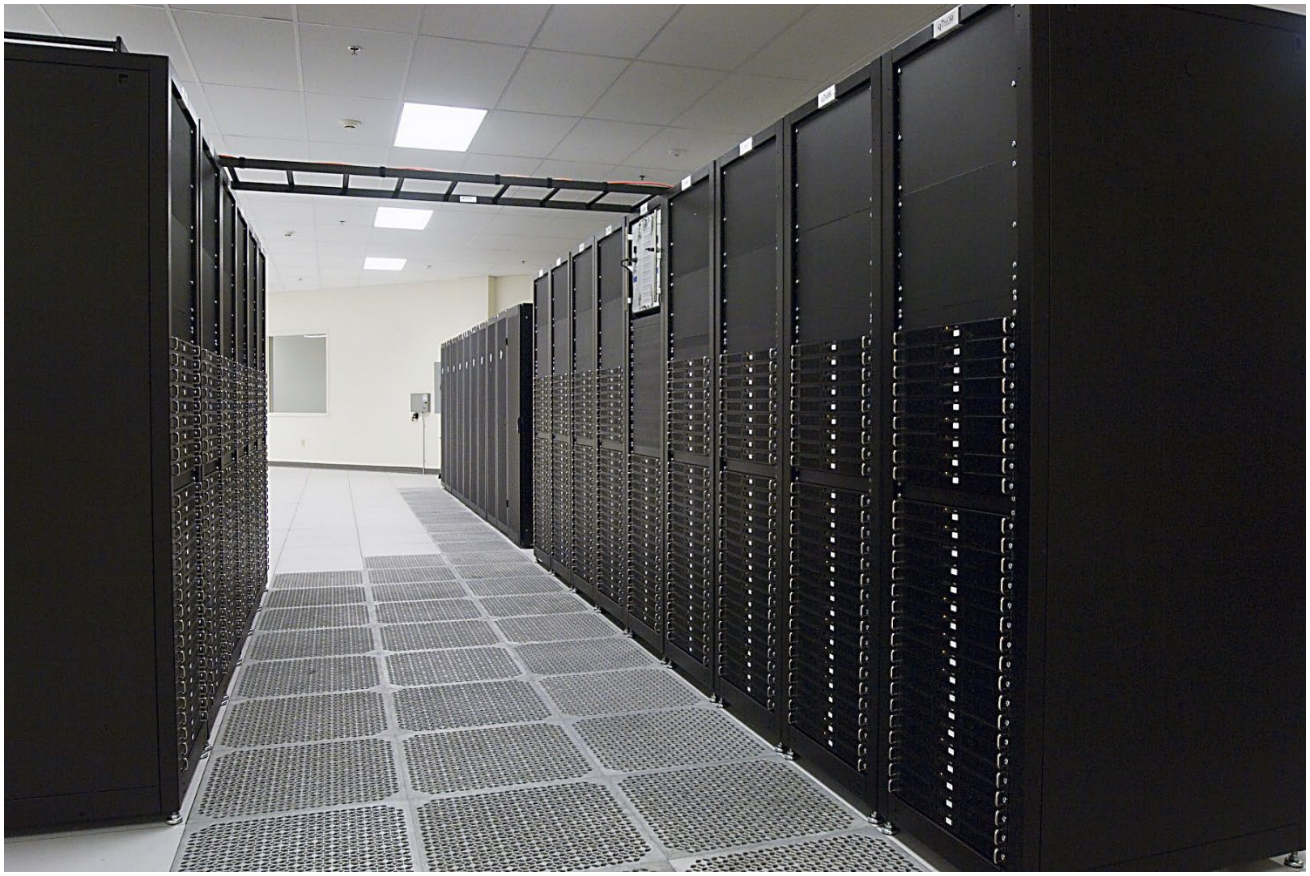
HOW TODAY'S NETWORK WORKS



HOW A WEB SERVER WORKS?

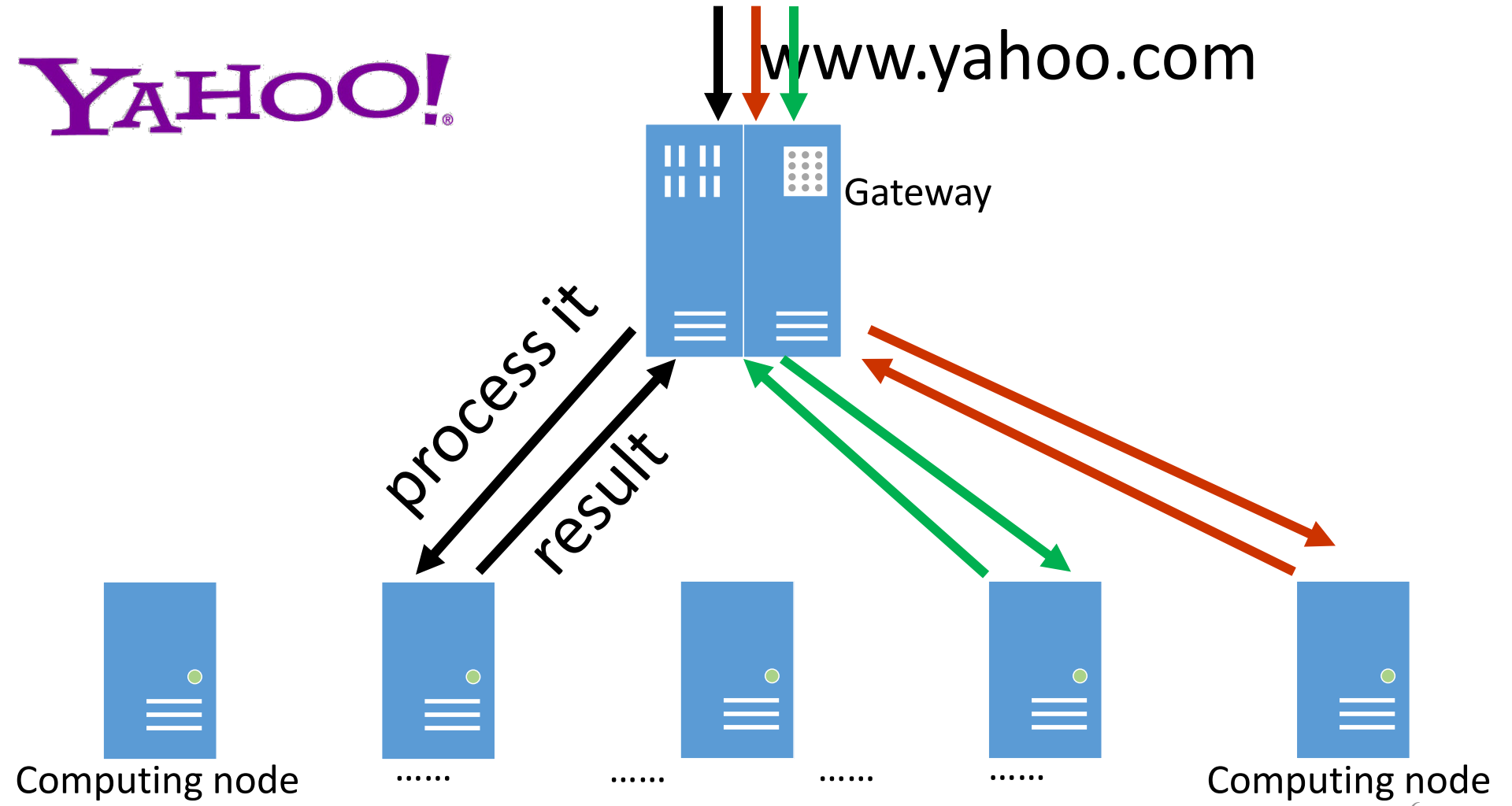
YAHOO!

?



A big center!

HOW A DATA CENTER WORKS?



HOW BUSY A DATA CENTER CAN BE

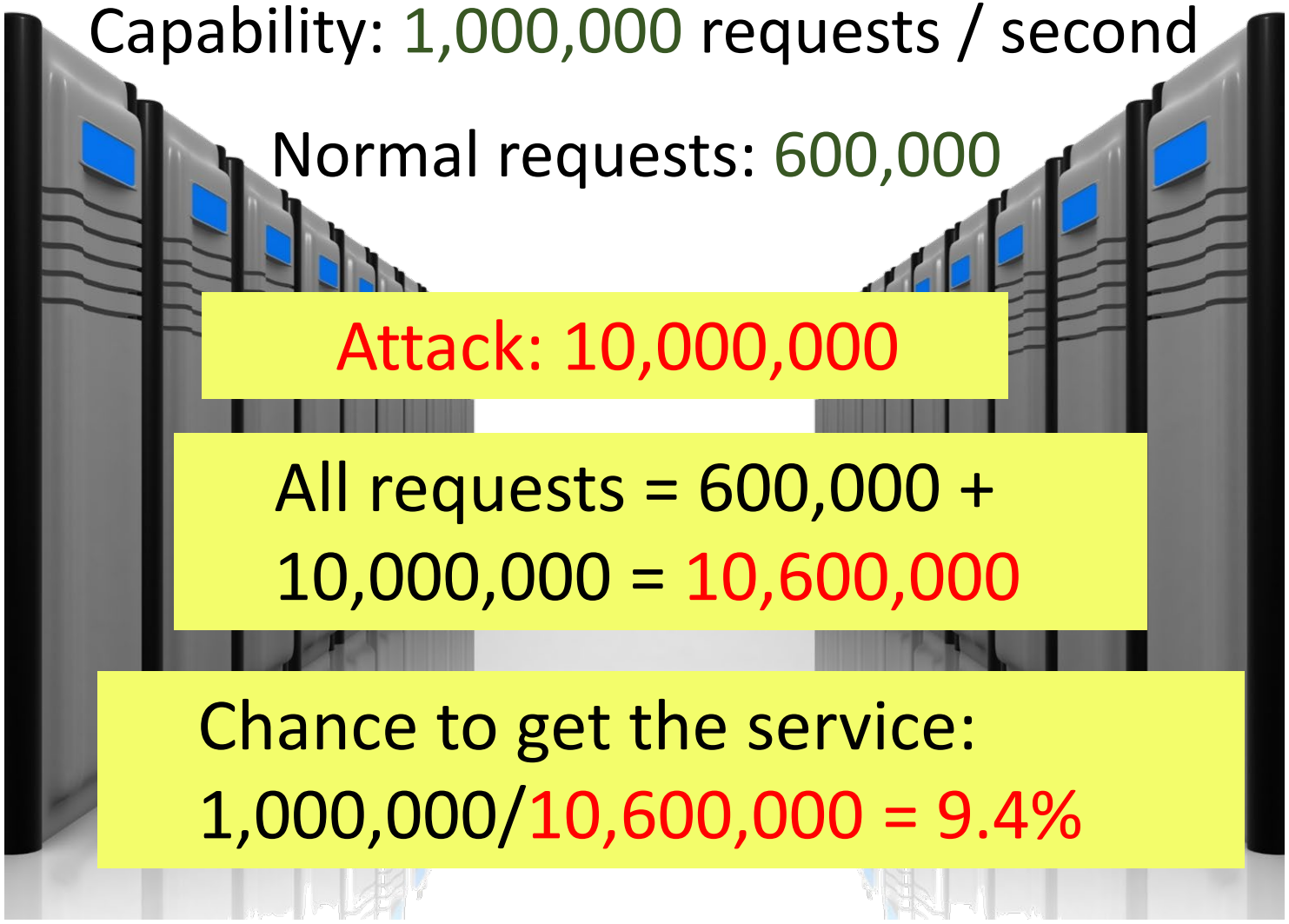
- Typical user connections (Yahoo statistics):
  - 100,000 – 10,000,000 for a particular service.
- Requirements for the capability of a data center
  - Must be able to accommodate typical numbers of connections
  - Should have margin to accommodate some high load
- What if the number of connections goes beyond the capability?
  - The data center drops them!

DENIAL-OF-SERVICE ATTACKS

- Motivation: The dropping rule.
- Objective: Make service unavailable to users.

- How? (Denial-of-service attack mechanism)
  - The data center always has a capability.
  - Flood a very large amount of service requests to the center! (the number > capability)
  - Make the data center heavily overloaded and start to drop user connections.

EXAMPLE: DENIAL-OF-SERVICE ATTACKS



Capability: 1,000,000 requests / second

Normal requests: 600,000

Attack: 10,000,000

All requests = 600,000 + 10,000,000 = 10,600,000

Chance to get the service: 1,000,000/10,600,000 = 9.4%

CAN A SINGLE USER DO THAT?

- Goal: I need 1,000,000,000 attack requests / second
- Each request = 100 bytes = 800 bits
- Total attack data rate = 800 * 1,000,000,000
  = 800 Giga bps

- Can I launch the attack from my home?

CAN A SINGLE USER DO THAT?

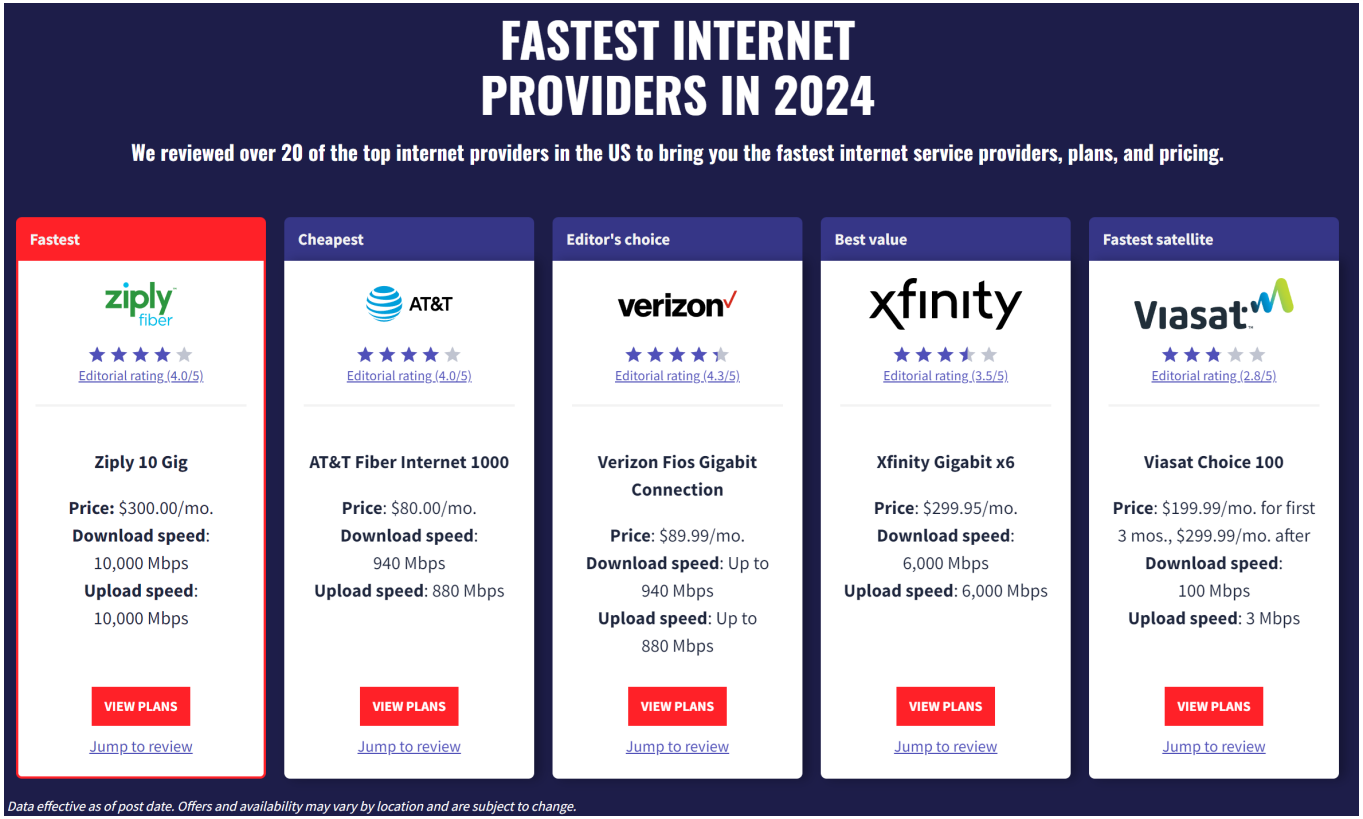
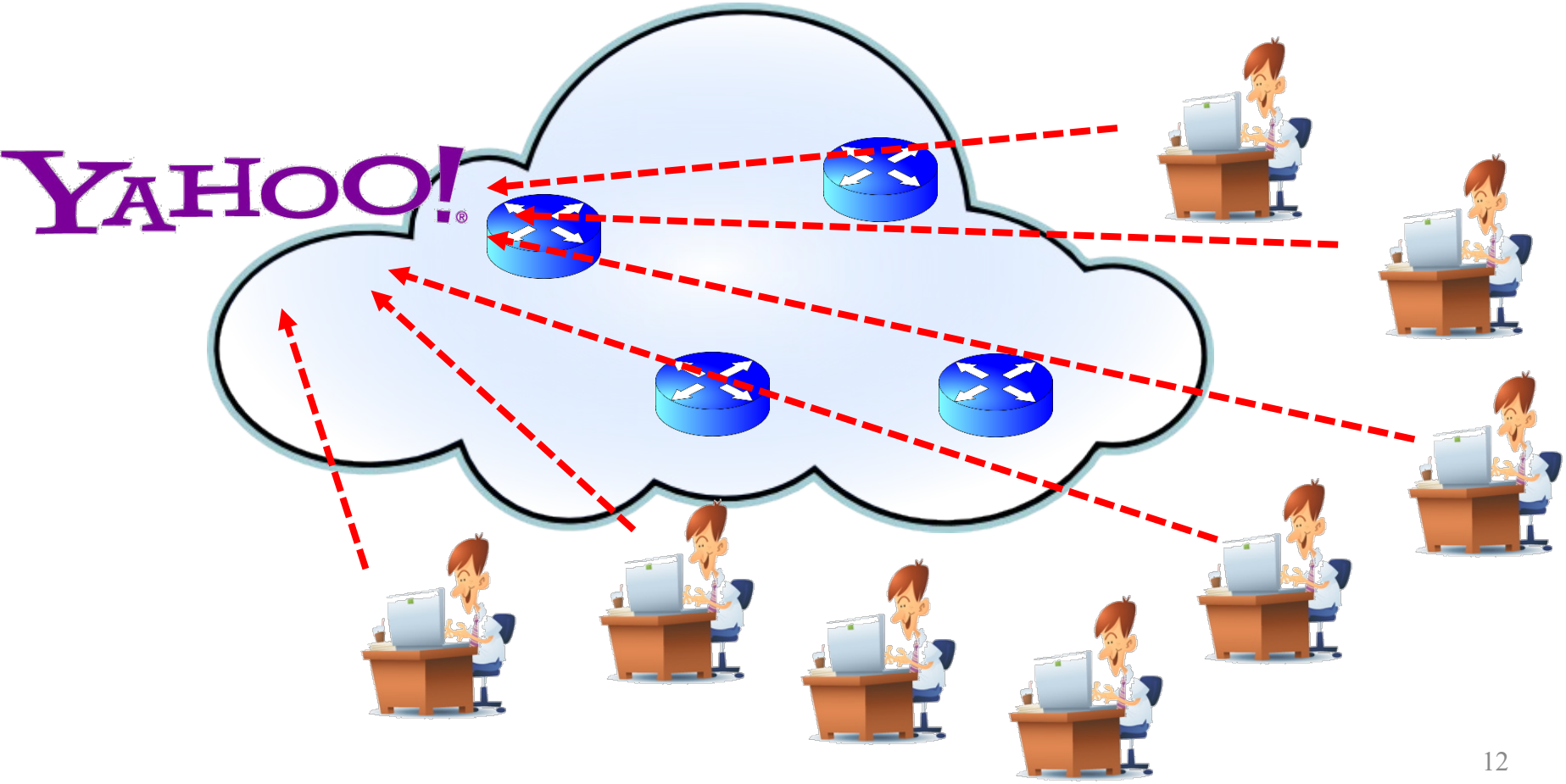


*Image from Internet

- Can I launch the attack from my home?
  - Typical Internet Service: 1000 Mbps upload speed. No!
- I need 800 Giga bps / 1000 Mbps = 800 friends!

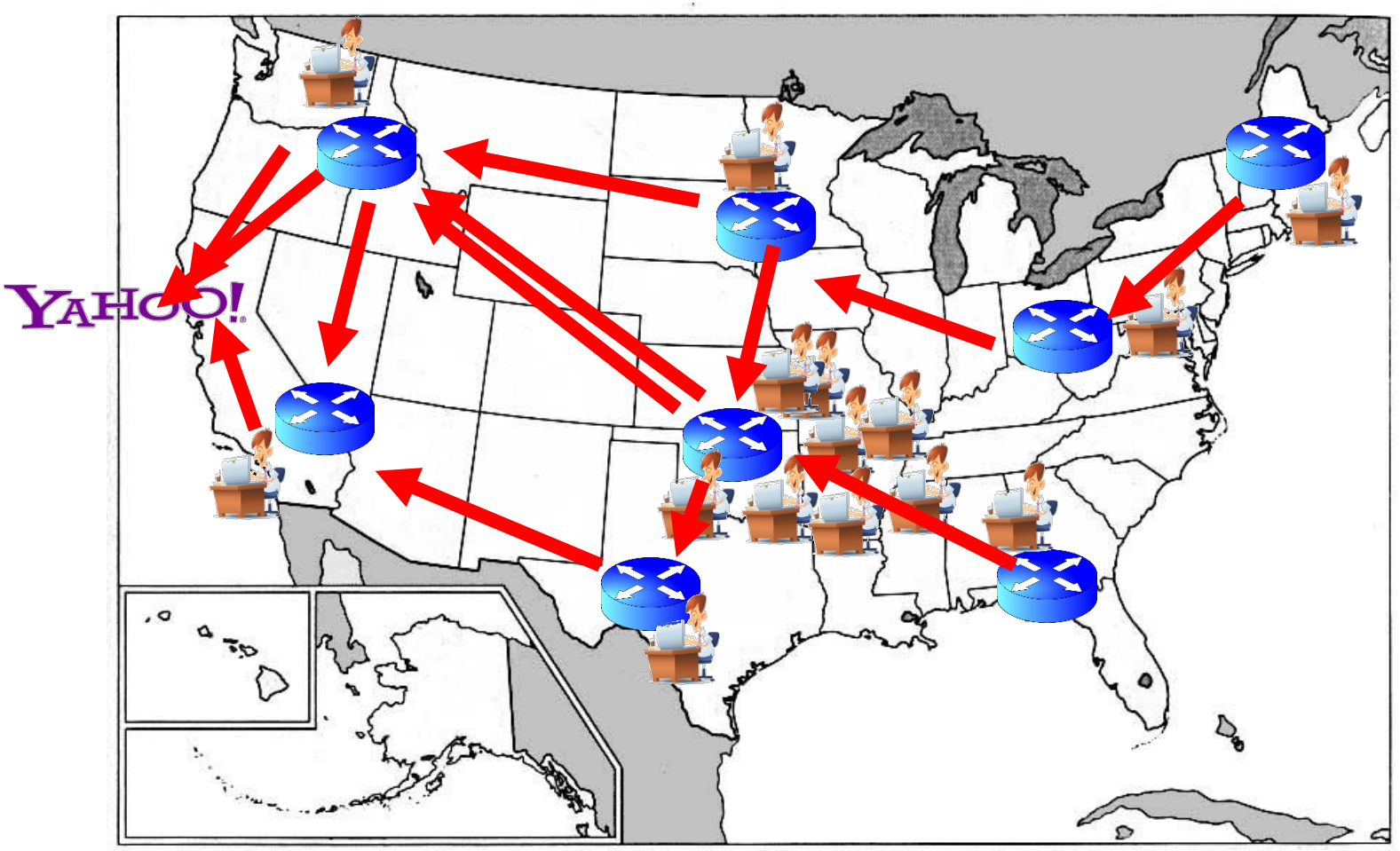
DENIAL-OF-SERVICE ATTACKS: TRUTH

- It's not so easy to launch a successful attack
  - Always needs a large number of attack machines!



DISTRIBUTED DENIAL-OF-SERVICE (DDOS)

- Attacking machines are in different locations!



CAN I FOUND SO MANY ATTACKING MACHINES?

- Botnet (Dark side of the Internet)
  - A large collection of compromised machines.
  - Millions of bots under control of a botmaster
    - Bot: compromised machine infected by viruses or worms.
    - Botmaster: a hacker or malicious user in command.
- Recent Botnets
  - 2008 (November) Downup 10,500,000
  - 2009 (May) BredoLab 30,000,000

RECENT STATISTICS ABOUT DDOS ATTACKS

- **Data in Q1 2013 compared to Q4 2012**
  - Average attack data rate up 718% from 5.9 Gbps to 48.25 Gbps
  - Average attack duration increases 7.14 percent from 32.2 hours to 34.5 hours.
  - 1.75 percent increase in total number of DDoS attacks

  - World record (February 2020) 2.3 Tbps from Amazon

A TOP ATTACK

- Picture from: http://thehackernews.com/2016/09/ddos-attack-iot.html

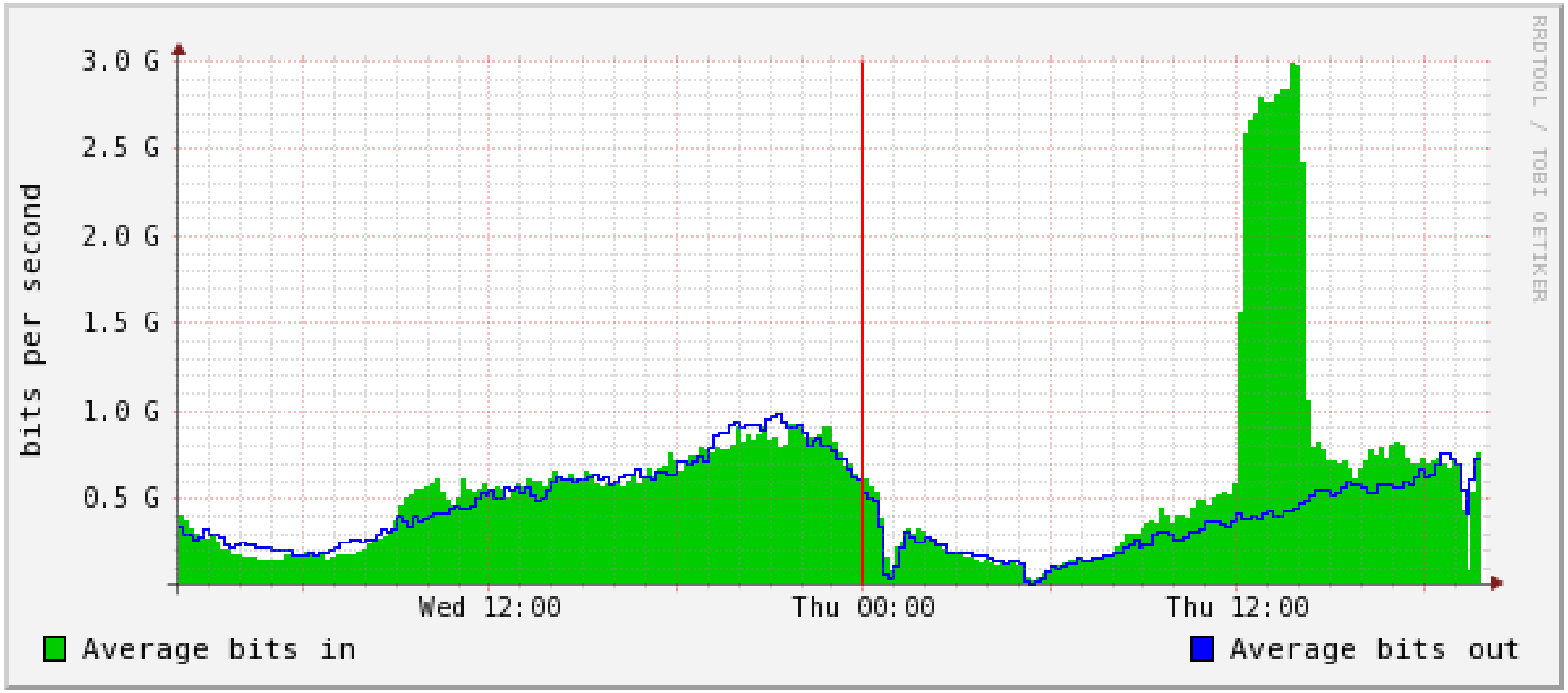
ATTACK STRATEGY

- Mirai (malware)
  - https://en.wikipedia.org/wiki/Mirai_(malware)

- Keep scanning the Internet and identifying Internet-of-Thing (IoT) devices.
  - home routers, modems, and IP cameras
- Try more than 60 common factory default usernames and passwords to log in make the device a bot

HOW TO DETECT ATTACKS

- Network Traffic Monitoring



HOW TO DEFEND AGAINST DOS ATTACKS

- No simple and very effective way!
  - It is not easy to achieve the goal availability!

- Commonly-used approaches:
  - Rating/flow limiting
  - Attack identification and elimination

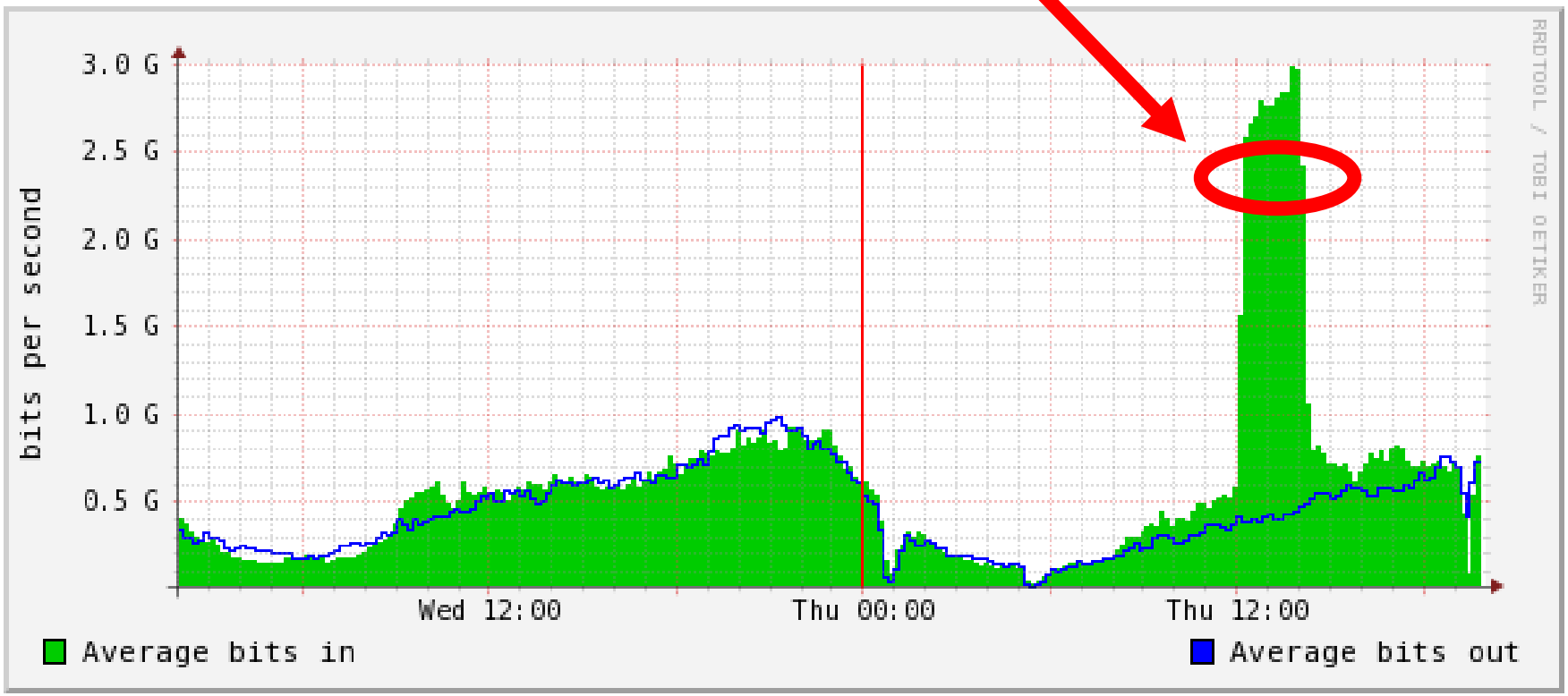
RATE LIMITING

- Example: Website browsing: how frequently you click a link?
  - 5 minutes, 1 minute, 10 seconds?
  - But definitely not every millisecond!

- So for a user, let's only accept one web-request every second

ATTACK IDENTIFICATION AND ELIMINATION

Who is sending so fast? Eliminate them!



PROTECTION AT THE HOST LEVEL

- Strong password and update
- Anti-virus and anti-malware
- Software/firmware patching
- Zero day attack defense mechanisms

CS 4173/5173 COMPUTER SECURITY

Introduction to Cryptography

CRYPTOGRAPHY

- *Cryptography*: the art of secret writing

- Converts data into unintelligible (random-looking) form
  - Encryption: must be reversible (can recover original data without loss or modification)

CRYPTOGRAPHY VS. STEGANOGRAPHY

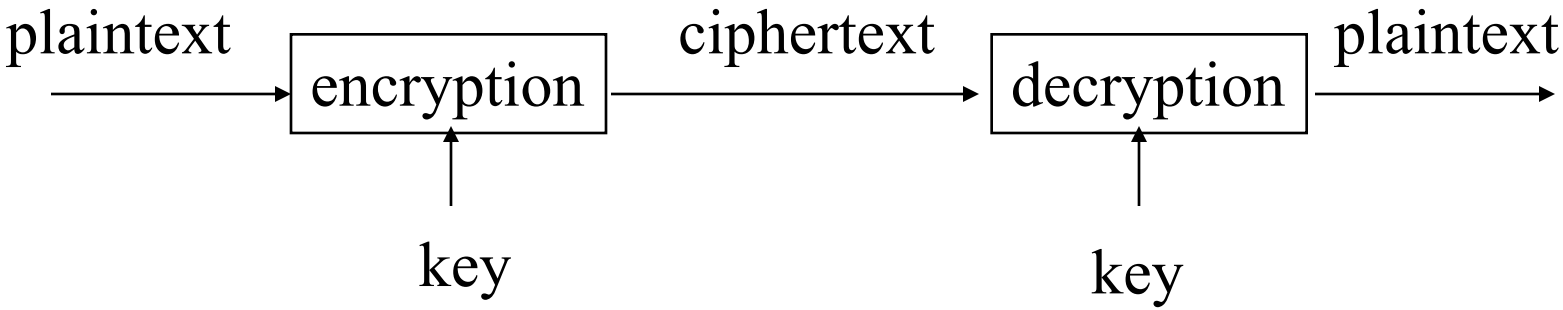
- *Steganography* concerns existence
  - Conceals the very existence of communication
  - Covered writing
    - Examples

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-poducts, ejecting suets and vegetable oils.

Pershing sails from NY June I

- *Cryptography* conceals the contents of communication between two parties
  - Secret writing

ENCRYPTION/DECRYPTION



- Plaintext: a message in its original form
- Ciphertext: a message in the transformed, unrecognized form
- Encryption: the process that transforms a plaintext into a ciphertext
- Decryption: the process that transforms a ciphertext to the corresponding plaintext
- Key: the value used to control encryption/decryption.
- Cipher: algorithm that performs encryption or decryption.

CRYPTANALYSIS

- Cryptanalysis: the art of revealing the secret
  - Defeat cryptographic security systems
  - Gain access to the real contents of encrypted messages
  - Cryptographic keys can be unknown

- Difficulty depends on
  - Sophistication of the encryption/decryption
  - Amount of information available to the code breaker

- We call the party that performs cryptanalysis the attacker.

CIPHERTEXT ONLY ATTACKS

- An attacker intercepts a set of ciphertexts

- Breaking the cipher: analyze patterns in the ciphertext
  - provides clues about the plaintext and key

KNOWN PLAINTEXT ATTACKS

- An attacker has samples of both the plaintext and its encrypted version, the ciphertext

- Makes some ciphers (e.g., mono-alphabetic ciphers) very easy to break

CHOSEN PLAINTEXT ATTACKS

- An attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts
  - More powerful than known plaintext attacks
    - Difference between known plaintext and chosen plaintext attacks
  - How could such attacks be possible?

PERFECTLY SECURE CIPHERS

1. Ciphertext does not reveal any information about which plaintexts are more likely to have produced it
   – e.g., the cipher is robust against ciphertext only attacks

and

2. Plaintext does not reveal any information about which ciphertexts are more likely to be produced
   – e.g, the cipher is robust against known/chosen plaintext attacks

COMPUTATIONALLY SECURE CIPHERS

1. The cost of breaking the cipher quickly exceeds the value of the encrypted information

and/or

2. The time required to break the cipher exceeds the useful lifetime of the information
   - Under the assumption there is not a faster / cheaper way to break the cipher, waiting to be discovered

- Most ciphers today are computationally secure. Sometimes we also say:
  - computationally infeasible or computationally difficult to break a cipher.

EXAMPLE

- If you are fast (2 tries/s), you need $10^3/2$=500s to try all combinations

What if the lock has 10 digits?

$10^{10}/2$=158.5 years to try all combinations

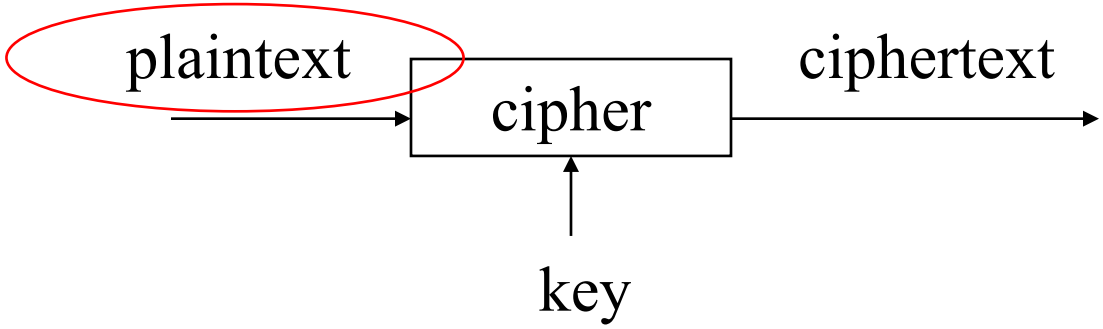
COMPUTATIONALLY SECURE CIPHER

- Design goals:
  - Make ciphertext look completely random regardless of the content of plaintext.
  - There is no fast way to crack it, the only way is to try all combinations
  - Make sure there are a great number of possible combinations.
    - Ensure computational difficulty without key.
  - Computational efficiency with key to do encryption and decryption.

KEEP WHAT SECRET?

- We have
  - plaintext, key, cipher, and ciphertext

Definitely keep secret!



HIDE OR REVEAL ALGORITHMS

- Keep algorithms secret
  - We can achieve better security if we keep the algorithms secret
  - Hard to keep secret if used widely
- Publish the algorithms
  - Security depends on the secrecy of the keys
  - Less unknown vulnerability if all the smart (good) people in the world are examine the algorithms
- Military
  - Both secret key and secret algorithm