The Dangerous Jungle

CSC 154

Basic questions

- Is network security important? Why?
- Why are today's networks so vulnerable?
- Based on your personal experience, what attacks do you know?

Why is network security important?

- The jungle (public networks, including internet) becomes more and more dangerous (vulnerable).
  - Observation
    - Increasing numbers of vulnerability and exploit incidents;
  - Impact
    - Critical mission asset concerns in business;
    - User privacy concerns;
    - National security concerns;

Why are networks vulnerable?

- More complexity, more security holes, more risk
  - Increasing number of internet users;
    - More users and system admins with poor security understanding, such as using the same password everywhere;
  - Increasing number and exposure to attack tools;
  - Increasing business infrastructures based on networks;
    - Security is an add-on, not an initial design part;
    - Business investment is more cost-oriented, not security-oriented;
  - The corporate networks (intranets) tend to “globalize” based on Internet;
    - Insider attackers with more insider knowledge;
    - More exposure to external attackers;

What network attacks do you know?

- Virus
- DoS
  - DDoS
- Worm

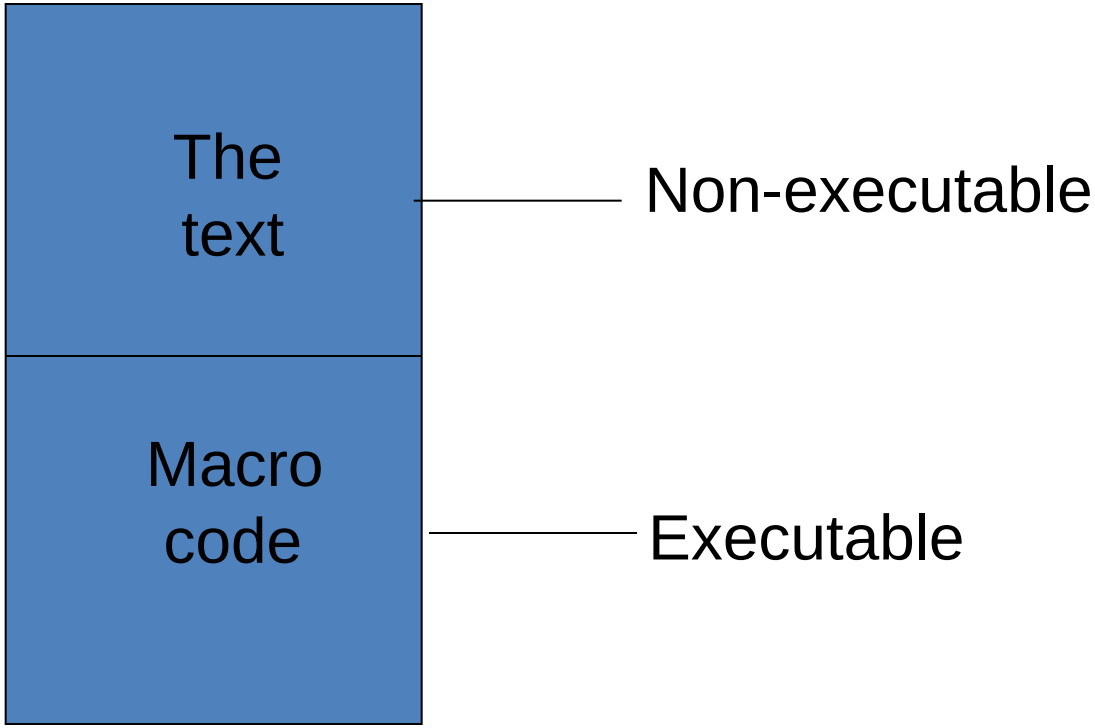
How does Melissa virus work?

- (step 1) launched as an email with a malicious attachment;
- (step 2) the attachment contains an executable macro program;
- (step 3) exploit the user's address book to flood emails out by copying itself;
  - take the 50 out of the user's address book
- (step 4) if the user click/open the attachment, the code will be executed → you are infected!
  - If the user does not click the attachment? -Nothing happen.

- **What could be the consequences?**
  - Performance problems, denial of services on mail servers clogged with propagating virus e-mails

Melissa

- email attachment: “list.doc”
  - a Word document that contains code!



How does “I love you” virus work?

- Use email attachment → user click and open → execute → break passwords → address book to self-propagate → replace certain file names with itself

- “Social engineering” words makes user more prone to click:
  - “I love you” (Love-Letter-For-You.txt.vbs);
  - Very-Funny.vbs;
  - virus_warning.jpg.vbs;
  - protect.vbs;
  - Others: you got an award; read this paper

What is the effects of denial-of-service attacks?

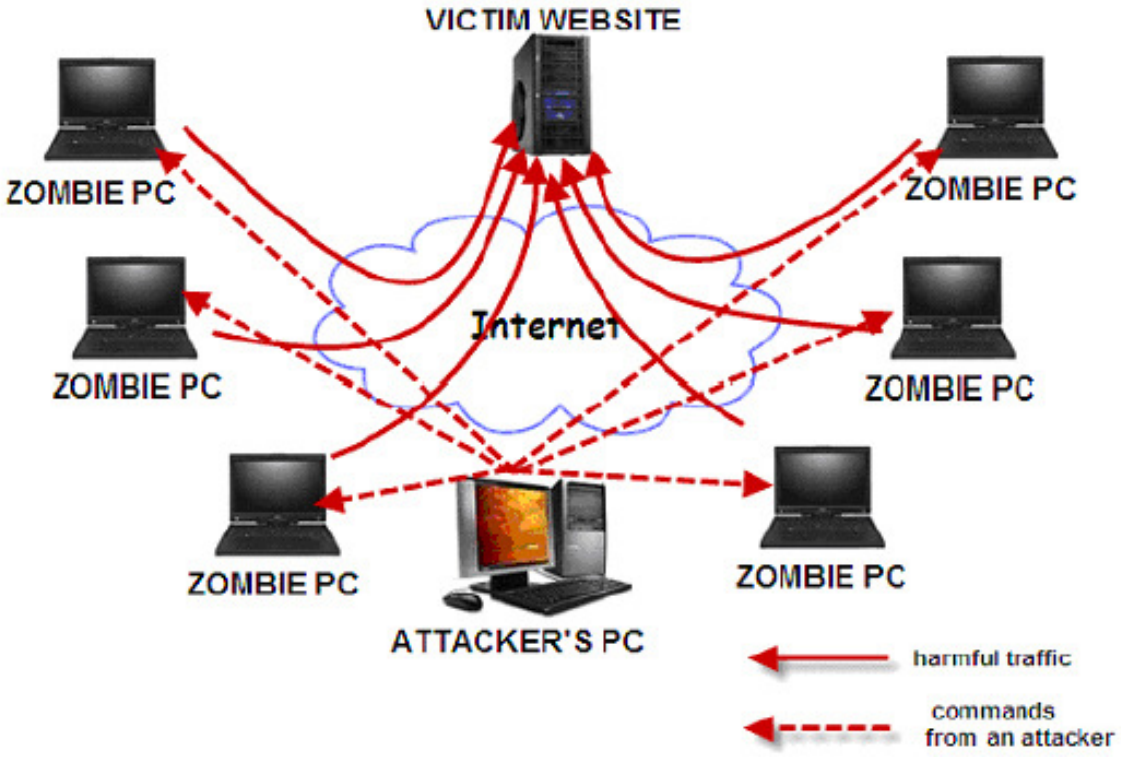
- **unavailability** (services like email, web)
  - web/email server down

- Characteristics:
  - keep users from access to necessary resources;
  - servers are attacked instead of clients;
  - hard to detect since the each zombie's connection looks legitimate;
  - time and money costly for a company;
  - does not disclose information for an individual;
  - possible network performance drop even a non-target;
  - more with a brute force attack;

What is the difference between Melissa and “I love you”

- social engineering aspects;
- a visual basic script instead of a macro;
- break passwords and report back;
- usually also corrupt files;

DDoS Attack



http://www.slashgear.com/whats-a-ddos-attack-zombies-shopping-help-explain-it-all-11333110/ (picture borrowed from SlashGear)
http://business.singtel.com/upload_hub/mnc/SingNet_DDoS_protect.htm (video borrowed from SingTel)

What is a worm?

- Self-propagating programs that kill the Internet
- Compare virus and worm:
  - worms do not need user interaction (clicking to open);
    - In Melissa, the users need to click
- Compare DDoS with worm:
  - Worms are self-propagating but DDoS attacks are not;
  - DDoS attacks target certain servers, while a worm may target any vulnerable host in the Internet, and worms may attack both servers and clients;
  - Worms also collect info, but DDoS do not;
  - Both DDoS attack and worms may cause large-scale network congestion and performance slowdown.

Some historical worms of note

Worm	Date	Distinction
Morris	11/88	Used multiple vulnerabilities, propagate to “nearby” sys
ADM	5/98	Random scanning of IP address space
Ramen	1/01	Exploited three vulnerabilities
Lion	3/01	Stealthy, rootkit worm
Cheese	6/01	Vigilante worm that secured vulnerable systems
Code Red	7/01	First sig Windows worm; Completely memory resident
Walk	8/01	Recompiled source code locally
Nimda	9/01	Windows worm: client-to-server, c-to-c, s-to-s, …
Scalper	6/02	11 days after announcement of vulnerability; peer-to-peer network of compromised systems
Slammer	1/03	Used a single UDP packet for explosive growth

Kienzle and Elder, Recent Worms: A Survey and Trends, WORM 03