

## What does security mean?

- In real life:
  - No one should be able to break into my house
  - Or steal something from me
  - Or impersonate me or others I know
  - Or attack me
  - Or take my time with irrelevant things
  - Or damage my property
  - How about my hairdresser's shop?

1

## What does security mean?

- In networks: I want to communicate with A
  - No one should be able to break into my computer
  - Or sniff information I exchange
  - Or spoof my address and act in my name (or somebody else's)
  - Or attack me and disable my machine
  - Or take my resources with bogus packets
  - Or plant malicious code
  - Or attack anything on route from me to A
  - Or misuse my machine to attack someone else

2

## What does security mean?

- Goal of networking is to enable communication
  - **At all times and in all scenarios!!!**
- Security = robustness or fault tolerance?
- Security also means keeping communication private

3

## What are the threats?

- No one should be able to break into my computer
  - Hackers
    - Break password
    - Misuse vulnerability
    - Sniff my network
    - Use social engineering
    - Impersonate someone I trust
  - Viruses
  - Worms

4

## What are the threats?

- No one should sniff the information I exchange
  - I will use cryptography!
    - There are many ways to break ciphers
    - There are many ways to divulge partial information (e.g. who do you talk to)
  - I would also like to hide who I talk to and when
    - I will use anonymization techniques
    - Anonymization hinders other security approaches that build models of normal traffic patterns

5

## What are the threats?

- No one should spoof my address or act in my name
  - It is hard to impersonate someone in two-way communication, such as TCP
    - But it has been done
  - Plain spoofing seems extremely hard problem to solve
  - I want to be sure who I am talking to (authentication and digital signatures)

6

## What are the threats?

- No one should attack me and disable my machine
  - Denial-of-service attacks
  - Viruses

7

## What are the threats?

- No one should take up my resources with bogus packets
  - Denial-of-service attacks
  - Spam mail
  - Malicious mail
  - Worms

8

## What are the threats?

- No one should plant malicious code on my machine
  - Viruses
  - Worms
  - Denial-of-service attacks (preparatory phase)

9

## What are the threats?

- No one should attack anything on route to A
  - A could be attacked
  - Routers could be overloaded
  - DNS servers could be attacked

10

## What are the threats?

- No one should misuse my machine to attack someone else
  - Zombies
  - Reflector attacks
  - Worms
  - E-mail with viruses
  - Be a good citizen
  - But that may be expensive!

11

## What are the challenges?

- Your security frequently depends on others
- Good solution must
  - Handle the problem to a great extent
  - Handle future variations of the problem, too
  - Be inexpensive
  - Have economic incentive
  - Require a few deployment points
  - Require non-specific deployment points

12

## What are the challenges?

- Fighting a live enemy
  - Security is adversarial field
  - No problem is likely to be completely solved
  - New advances lead to improvement of attack techniques
  - Researchers must play double game

## What are the challenges?

- Attack patterns change
- Frequently there is scarce attack data
- No agreement about legitimate traffic patterns
- No agreement about metrics
- There is no standardized evaluation procedure
- Some security problems require a lot of resources to be reproduced realistically