What does security mean?

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

What does security mean?

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

What does security mean?

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

What are the threats?

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

What are the threats?

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

What are the threats?

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

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

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

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

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

- 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!

**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
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

- 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