Network Thinking

Responsible Computing

安全，隐私，职业规范

zxu@ict.ac.cn
zhangjialin@ict.ac.cn

Outline

- What is network thinking?
- Network terms
- Connectivity
    - Naming
    - Topology
- Protocol stack
    - The Web over TCP/IP stack
    - Web programming
- Network laws
    - Performance metrics
    - Network effect
- Responsible computing

These slides acknowledge sources for additional data not cited in the textbook

6. What is responsible computing?

- Ideas and practices to design and use computing products and services responsibly
  - Cybersecurity issues 安全
  - Privacy awareness 隐私
  - Professional norms 职业规范、职业操守

- Why bother?
- Computing has beneficial and harmful impact to society
  - 计算有正面和负面的社会影响

6.1 Cybersecurity issues 网络空间安全

- The global Internet is under constant attacks
  - Cause harm to society
  - 全球互联网随时被攻击，危害社会

- Example study 危害大，且快速增长
  - McAfee (2020): The Hidden Costs of Cybercrime
    - Cybercrime costed companies worldwide US$1 trillion
    - > 1% of global GDP
    - Was about US$500 billion in 2016

- Compare these to the worldwide computing market

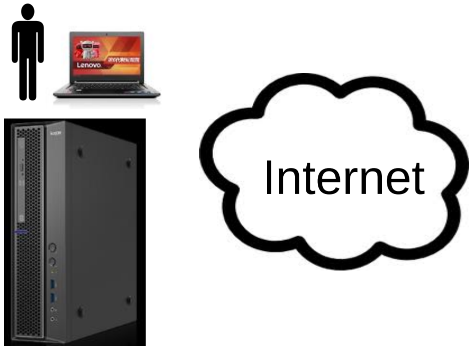
The global ICT market:	US$3.4 trillion in 2016
The global digital economy:	US$11.5~24 trillion in 2016
The global cybercrime cost:	US$0.5 trillion in 2016

Cybersecurity issues

- Cybersecurity problems involve hardware, software and people 网络空间安全涉及硬件、软件、人
  - Not only software such as computer viruses，尽管软件似乎更明显
- Cyber attack types 存在多种攻击，不都是软件侵入
  - Malware: malicious software enabling an attacker to damage or gain unauthorized access to a computer 恶意软件
    - Computer viruses, worms, Trojan horses and spyware 病毒、蠕虫、木马、间谍软件
  - An attack does not have to be in a software form
    - Hardware exploitation 利用硬件的攻击
      - Meltdown: exploiting “out-of-order execution”, a feature of processor hardware 利用硬件的乱序执行
        - Enabling an attacker to read privileged information passwords
  - An attack does not have to install anything on the targeted system
    - Denial-of-service (DoS) attacks, distributed denial-of-service (DDoS) attack 拒绝服务攻击
    - Spams: unwanted emails 垃圾邮件
    - *Phishing*: phishing websites or phishing emails 钓鱼邮件、钓鱼网站

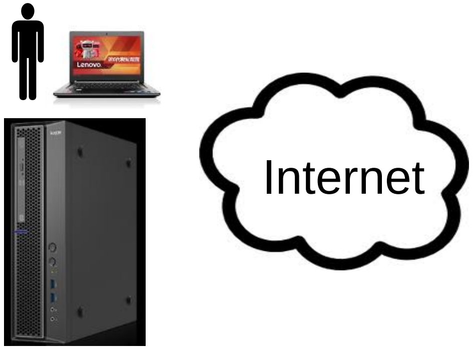
Counter measures 安全措施

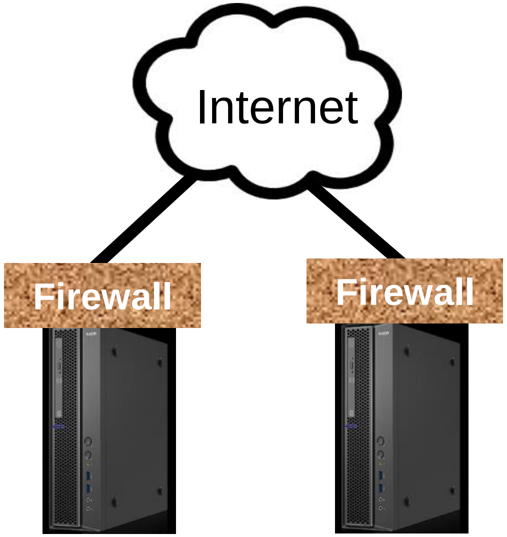
- Physical isolation: critical computing systems disconnected from the Internet
- 物理隔离



Counter measures

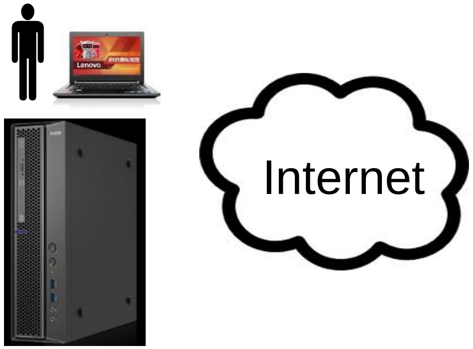
- Physical isolation: core computing systems disconnected from the Internet
- Firewalls: block or filter out undesirable messages
  防火墙

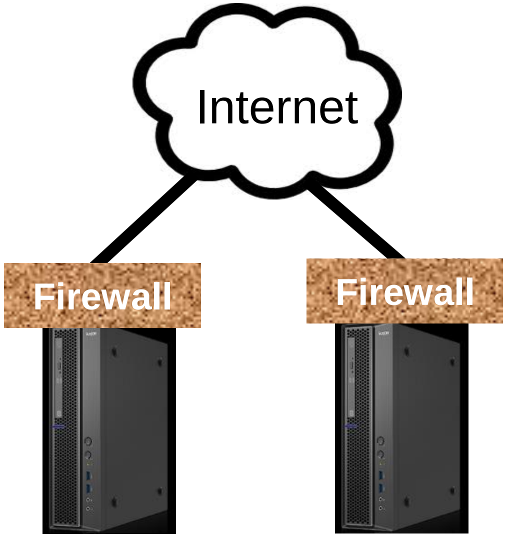


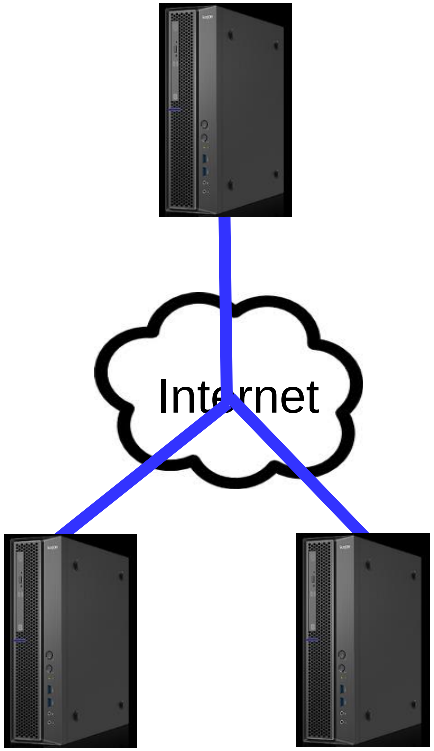


Counter measures

- Physical isolation: core computing systems disconnected from the Internet
- Firewalls: block or filter out undesirable messages
- Virtual private networks (VPNs)
  虚拟私有网







Counter measures

- Physical isolation: core computing systems disconnected from the Internet
- Firewalls: block or filter out undesirable messages
- Virtual private networks (VPNs)

- Antivirus software: detect and kill computer viruses 防病毒软件、杀毒软件

- Cryptography 密码学
  - Secure message communication in the presence of adversaries
  - Encryption: plaintext → ciphertext HELLO → KHOOR 加密：明文→密文
  - Decryption: ciphertext → plaintext KHOOR → HELLO 解密：密文→明文

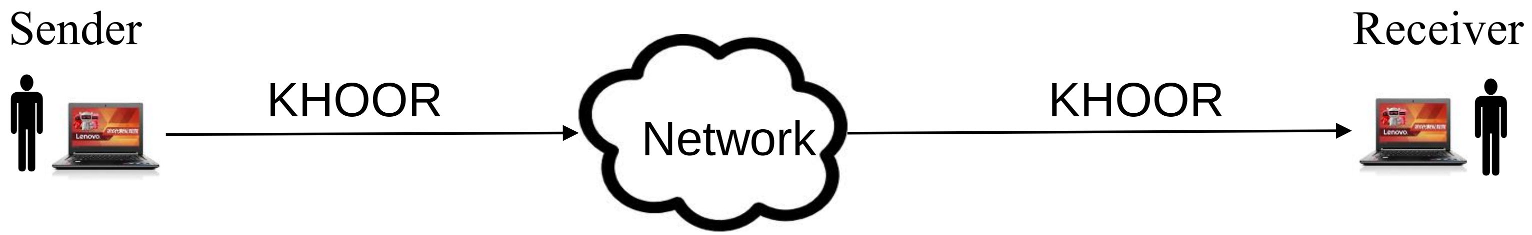
Symmetric-key encryption: Caesar cipher

对称加密：发送方与接收方共享秘钥；凯撒密码

- Sender and receiver share a key (**3** in this example) 此例中秘钥是**3**
  - **Only a single key is used by both parties, thus symmetric**
- Sender encrypts the plaintext (string of capital letters)
  - By shifting each letter L **3** positions down the alphabet, i.e., ASCII(L)+**3**
  - E.g., ‘**H**’+**3** = 72+**3** = 75 = ‘K’

  and sends the ciphertext over the network to the receiver
- Receiver decrypts the ciphertext
  - By shifting each letter L up **3** positions, i.e., ASCII(L)-**3**
  - E.g., ‘K’-**3** = 75-**3** = 72 = ‘**H**’

Alphabet	
A	65
B	66
C	67
D	68
E	69
F	70
G	71
H	72
I	73
J	74
K	75
…	



HELLO → KHOOR
Shift **3** positions down
Encryption

KHOOR → **H**ELLO
Shift **3** positions up
Decryption

***Public-key encryption: the RSA method 公钥加密的RSA方法

- Receiver has two keys
  - Public key $\boldsymbol{K_P}$: known to everybody, including the eavesdropper
    - Used by the sender to encrypt plaintext into ciphertext
  - Private key $\boldsymbol{K_S}$: known only to receiver; also called **secrete key**
    - Used by the receiver to decrypt ciphertext into plaintext
- Process of securely communicating a plaintext decimal number **920**
  - Receiver makes the magic assumption: *n*=2773,*d*=157,*e*=17
  - Sender
    - Knows the public key $\boldsymbol{K_P} = (e, n) = (17{,}2773)$
    - Uses encryption algorithm $C = M^e \bmod n$ to obtain ciphertext *C* from plaintext *M*

      $$C = M^e \bmod n = \mathbf{920}^{17} \bmod 2773 = 948 = 0948$$
    - Sends ciphertext 0948 over the open Internet to receiver
  - Receiver
    - Knows both $\boldsymbol{K_P} = (e, n) = (17{,}2773)$ and $\boldsymbol{K_S} = (d, n) = (157{,}2773)$
    - Uses decryption algorithm $C = M^e \bmod n$ to obtain plaintext *M* from ciphertext *C*

      $$M = C^d \bmod n = 948^{157} \bmod 2773 = \mathbf{920}$$

Securely communicating a message

- The plaintext message
    - A 20-character message “ITS ALL GREEK TO ME ”
- Process
    - Sender
        - Encode the text message by: space=00, A=01, B=02, …, Z=26 to obtain a 40-digit number
            - 0920190001121200071805051100201500130500
        - Divide into 4-digit groups
            - 0920 1900 0112 1200 0718 0505 1100 2015 0013 0500
        - Encrypt plaintext number sequence into ciphertext number sequence
            - 0948 2342 1084 1444 2663 2390 0778 0774 0219 1655
        - Sends this ciphertext number sequence to receiver
    - Receiver
        - Decrypt ciphertext number sequence into plaintext number sequence
            - 0920 1900 0112 1200 0718 0505 1100 2015 0013 0500
        - Decode number sequence into character string
            - “ITS ALL GREEK TO ME ”

How are the magic numbers determined?

- Magic numbers: *n* = 2773, *d* = 157, *e* = 17

- Process by receiver
  - Randomly choose two large prime numbers *p* and *q*, and set $n = p \times q$
    - $p = 47,\ q = 59,\ n = p \times q = 47 \times 59 = 2773$
  - Compute the Euler number $(p-1) \times (q-1)$
    - $(p-1) \times (q-1) = 46 \times 58 = 2668$
  - Randomly choose a large integer *d* such that $\mathrm{GCD}(d, 2668) = 1$
    - Set $d = 157$ which satisfies $\mathrm{GCD}(157, 2668) = 1$
    - Complete private key information: $K_S = (d, n) = (157, 2773)$
  - Find value *e* satisfying $(d \times e) \bmod 2668 = 1$
    - $e = 17$ which satisfies $(157 \times 17) \bmod 2668 = 1$
    - Complete public key information: $K_S = (e, n) = (17, 2773)$

RSA allows eavesdropper to know a lot

- A lot of information is open to the world to know
    - The encryption algorithm $C = M^e \bmod n$
    - The decryption algorithm $M = C^d \bmod n$
    - The public key $K_P = (e, n) = (17, 2773)$
    - The character converting scheme: space=00, A=01, B=02, …, Z=26
    - The ciphertext number sequence
        - 0948 2342 1084 1444 2663 2390 0778 0774 0219 1655
- Yet, the eavesdropper cannot decipher the message
    - He lacks the private key $K_P = (d, n) = (157, 2773)$
    - He does not know $d = 157$, which is the solution to $\mathrm{GCD}(d, 2668) = 1$
    - He does not know 2668, which is the Euler number $(p-1) \times (q-1)$
    - He knows $n = p \times q$, but does not know the prime numbers $p,\ q$
- Can the eavesdropper find an efficient algorithm
    - Which recovers prime numbers $p,\ q$?
- Not likely

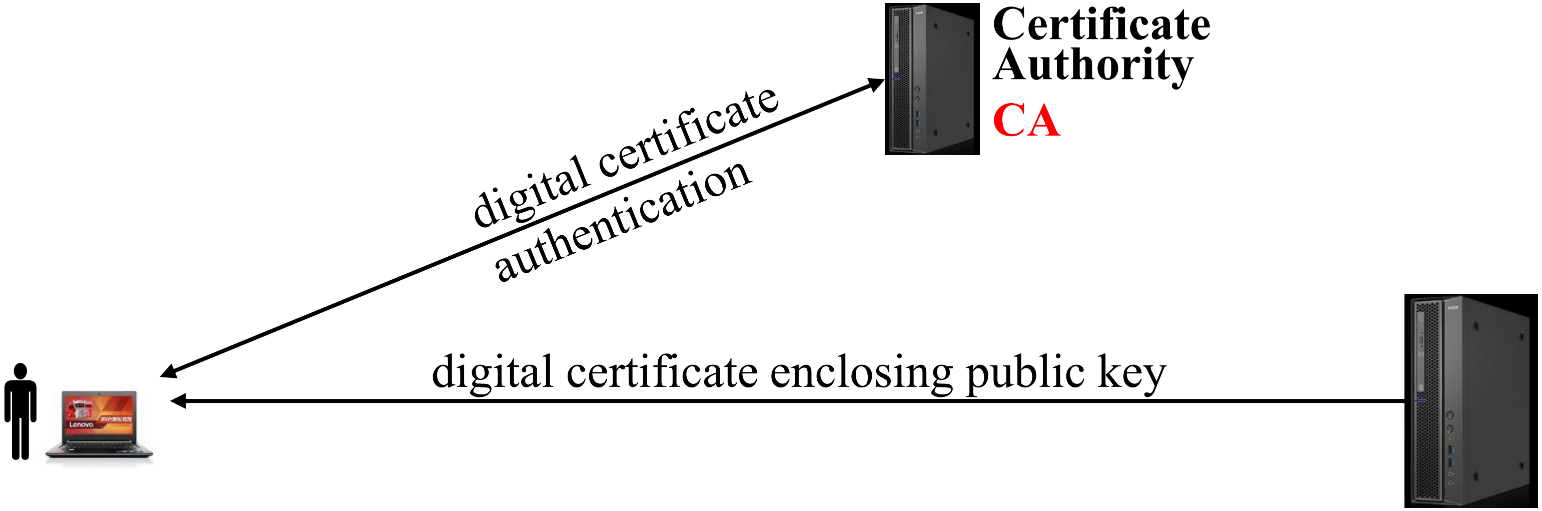
The prime factorization problem

- Given a large natural number n, find the prime numbers $p,\ q$ such that $n = p \times q$
  - Given $n = 2773$, find $p = 47,\ q = 59$, such that $p \times q = 2773$
- This problem has no known efficient algorithm
- RSA relies on this fact

- As of year 2020, the largest RSA integer factored is RSA-250, which has 250 decimal digits
  - A French-US team accomplished the prime factorization task utilizing a network of parallel computers in Europe and the USA
  - The total computing resources used are roughly 2700 core-years
  - At least hundreds of years of computing on a student’s laptop

HTTPS: RSA application

- HTTPS = HTTP + Transport Layer Security (TLS)
  - For secure communication between a browser and a website
  - Use symmetric-key and public-key encryption techniques
    - For the long term, use public-key encryption
    - For the short term, use onetime symmetric-key encryption
      - E.g., a HTTP GET session



Certificate Authority

CA

digital certificate authentication

digital certificate enclosing public key

Browser

Website: www.ccf.gov.cn
China Computer Federation

6.2 Privacy issues 隐私

- Privacy: keeping a user’s identity and personally identifiable information (PII) *private*.
- Personal information 个人信息=自然人信息
  - Any information relates to a natural person’s identity
  - Includes personally identifiable information (PII)
    可区分、追溯到自然人的信息
  - Does not include anonymized personal information
- Personal information is broad
  - Such as personal names, ID numbers, personal photos or videos, website clicks records, voice signals, financial records, medical data
- Personal data can be revealed by technology
  - Utilizing metadata, data mining, AI

Sources of further information

- In the computing field
  - *IEEE Security and Privacy* is a professional magazine exploring security and privacy issues
  - Tim Berners-Lee’s Solid initiative

- In the legal field
  - GDPR: European Union enacted a law framework, called *General Data Protection Regulation* 通用数据保护条例
    - Went into effect in 2018
  - PIPA: the National People’s Congress of the People’s Republic of China published a request for comments of a *Personal Information Protection Act* 个人信息保护法
    - Draft published in 2020

Basic principles of the laws

- Facilitate protection as well as use of personal information
  - 兼顾个人信息的保护与使用
- A person has basic rights to his/her personal information, such as:
  - Right to permit a third party to collect and use personal data
  - Right to timely rectification of personal data
  - Right to be forgotten
  - Right to port one’s personal data to another website
- These rights are protected by law, even when a piece of personal data is not owned by the person
  - A person’s cellphone number is protected, even though the number belongs to the telecom company, and the person only “rents” it
- Another person or institution can collect, store, process, and otherwise use a person’s data in a legal and fair way
  - PIPA used 合法、正当、必要

6.3 Professional norms

- ACM code of conduct: seven principles
  国际计算机协会行为规范的七原则
  - Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
    为社会和人类的幸福做出贡献，承认所有人都是计算的利益相关者
  - Avoid harm. 避免伤害
  - Be honest and trustworthy. 诚实可靠
  - Be fair and take action not to discriminate. 做事公平，采取行动无歧视
  - Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.
    尊重他人工作，该工作产生新想法、新发明、创造性作品和计算工件
  - Respect privacy. 尊重隐私
  - Honor confidentiality. 尊重保密协议

https://www.acm.org/code-of-ethics

Form your own thoughtful judgement
了解ACM规范，形成自己的判断

- Understand the ACM code of conduct
  - You don’t have to agree to it completely
    - The ACM code itself is evolving
  - But should try to understand what it says
- Apply it to the three examples in textbook, and form your own thoughtful judgement
  应用到教科书三个例子：Examples 67, 68, 69
  - Free flow versus professionally sharing of scientific data
    - 科学数据应该自由流动还是专业性分享？
      全球共享流感数据倡议组织（GISAID）的规范
  - Full disclosure versus responsible disclosure
    - 组织内部出现可能有害社会的漏洞，应该向社会完全曝光还是负责任地通报
  - The case of the Morris worm
    - 善意的（无恶意的）科学研究工作是否可以越界？