SECURITY

DT211/DT228/3

Dr. Yupeng Liu

Course Outline

- Introduction to cryptography
- Number theory
- Symmetric and Asymmetric Cryptograph
- Public-Key Cryptography and RSA, Key management,
- Steganography
- Network, Internet Security, ethical hacking
- System Security
  - Electronic Mail Security, Firewalls.
  - Virus, Worms etc

References

- Cryptography and Network Security : Principles and Practices, 5th Ed, Williams Stallings (2011) Prentice Hall.
- Network Security Essentials: Applications and Standards, 4th Ed, William Stallings (2011), Prentice Hall.
- Network perimeter Security: Building Defense In-Depth, Cliff Riggs (2003), Auerbach Publications.

The future of Security threats

- Cyberwar declared – Stuxnet a politically motivated attack (weaponized malware)
- Advanced Persistent Threat (APT) – advanced malware attack
- VoIP attacks – brute force and directory traversal class attacks against VoIP servers

The future of Security threats

- Car hacking – cars are more connected with built-in Bluetooth, 3G internet, GPS, Onstar, and dashboard computers
- The Facebook challenge - users trust of web
- Manufactured-delivered malware – products arriving with infections out of the box
- DLP for IP – shift from physical to digital production.

Cybercrime Knows No Borders

- Prosecuting cybercrime is no easy task
  - Legal inadequacies in various jurisdictions
  - Uneven enforcement
- Fighting internet crime does not come cheap. For example, cyber intrusions cost the British economy $43 Billion annually.
- The Cyber industrial complex is emerging, which is very similar to the military industrial complex of the cold war.

Steps for Cloud Security

- Take responsibility for your own security
- Ring fence your data
- Think about encryption
- Strong passwords for cloud services
- Consider making your user devices ‘dumb’

Common Sense Security

- Security is not a specialist subject – it's everyone's responsibility
- The attackers only have to get lucky once and the defenders have to get it right 100% of the time

Why Cryptography?

- Defense in Depth
- RGVmZW5zZSBpbiBEZXB0aA==
- 00ac8a98d8f6df9d2b60b55e47a716b6e53a d4b064738ea6f9a088ab613c2d2b48bcabc6 8c3fc05c4e2779ca60700ac891e4e0a6c1bfb 6aa7df6dafdce123acb
- 446566656E736520696E204465707468
- F ƒ ´ ä ` ´ t8è»ôê?õ»=Ä^^ßØZ²Ûpu

The Adversarial Setting

- The biggest difference between security systems and any other engineering is the adversarial setting.
- Factors such as storms, heat, wear and tear are fairly predictable to an experienced engineer.
- In security systems opponents are intelligent, clever, malicious and devious. They do things nobody ever thought before, do not play by the rules and are completely unpredictable.

Professional Paranoia

- To work in this field, you have to become devious yourself.
- You have to think like a malicious attacker to find weaknesses in your own work.
- Cryptographers are professional paranoids.
- Developing this mindset (security mindset) will help you observe things about systems and your environment that most other people do not notice

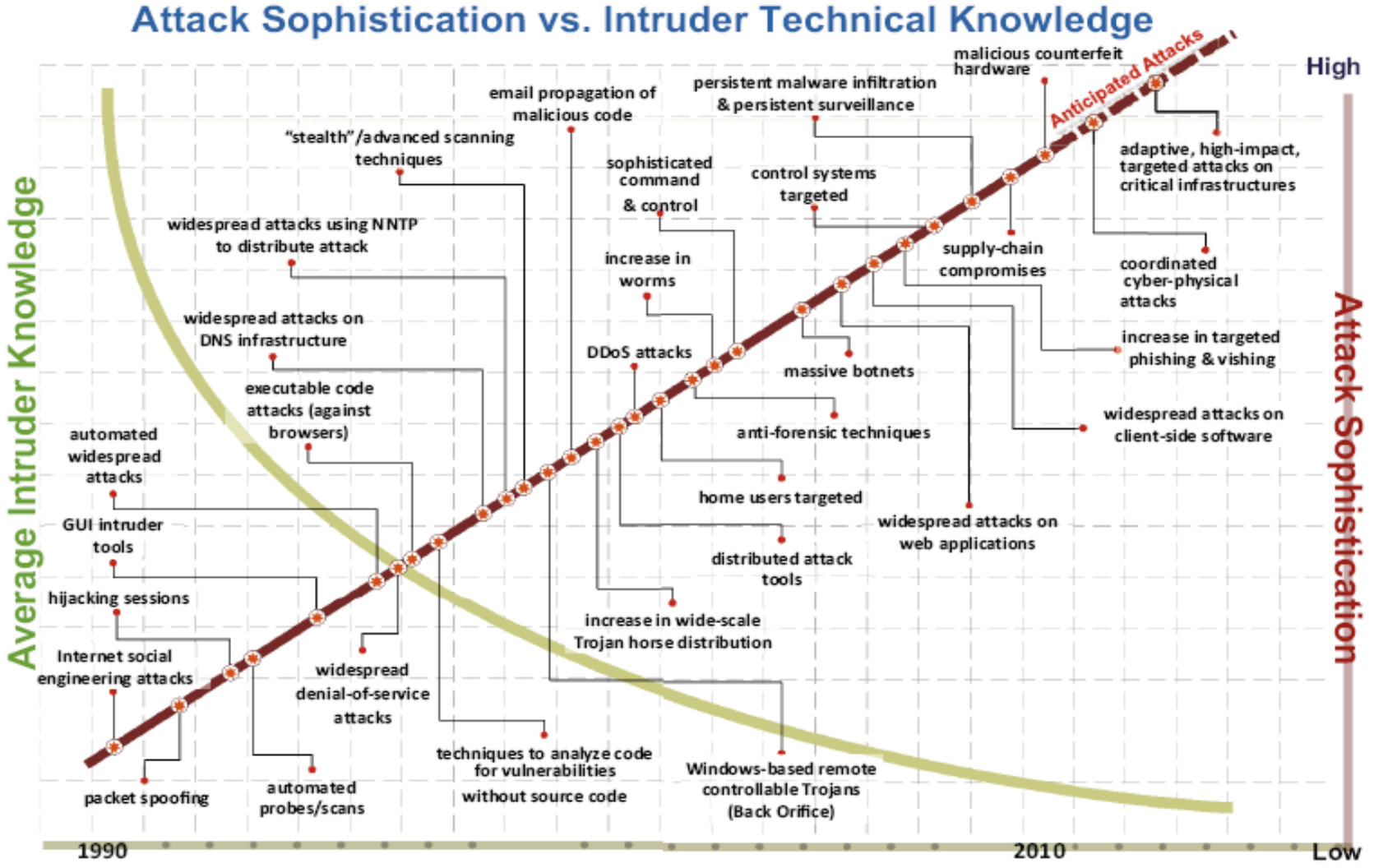
Why Cryptography?

- Cryptography can be compared to locks in the Physical world. A lock by itself is a singularly useless thing.
- Cryptography is just a small part of a much larger security system.

Why Cryptography?

- Cryptography as a Mathematical Science vs Cryptography as an Engineering discipline.
- Security is only as strong as the weakest link, and the Mathematics of Cryptography is almost never the weakest link.

The Evolution of attack techniques/technologies



Security Threats

- Spyware and Ad ware
- Viruses
- Phishing and Pharming
- Worms, Bots
- SQL injection
- Sophisticated targeted attacks
- Politically motivated attacks (Weaponized malware) - Stuxnet

Security Certification

- International Information Systems Security Certification Consortium $(ISC)^2$
- Certified Information System Security Professional (CISSP)
- Global Information Assurance Certification
- Cisco Certified Security Professional (CCSP)
- etc

It's going to get worse - 1

- Explosive growth of the Internet continues
  - continues to double in size every 10-12 months
  - where will all the capable system administrators come from?
- Market growth will drive vendors
  - time to market, features, performance, cost are primary
  - "invisible" quality features such as security are secondary

It's going to get worse - 2

- More sensitive applications connected to the Internet
  - low cost of communications, ease of connection, and power of products engineered for the Internet will drive out other forms of networking
  - hunger for data and benefits of electronic interaction will continue to push widespread use of information technology

It's going to get worse - 3

- The death of the firewall
  - traditional approaches depend on complete administrative control and strong perimeter controls
  - today's business practices and wide area networks violate these basic principles
    - no central point of network control
    - more interconnections with customers, suppliers, partners
    - more network applications
      - **"the network is the computer"**
    - who's an "insider"and who's an "outsider"

Before it gets better - 1

- Strong market for security professionals will eventually drive graduate and certificate programs.
- Increased understanding by technology users will build demand for quality security products; vendors will pay attention to the market.
- Insurance industry will provide incentives for improved business security practices.

Before it gets better - 2

- Technology will continue to improve and we will figure out how to use it
  - encryption
  - strong authentication
  - survivable systems
- Increased collaboration across government and industry.

Good news

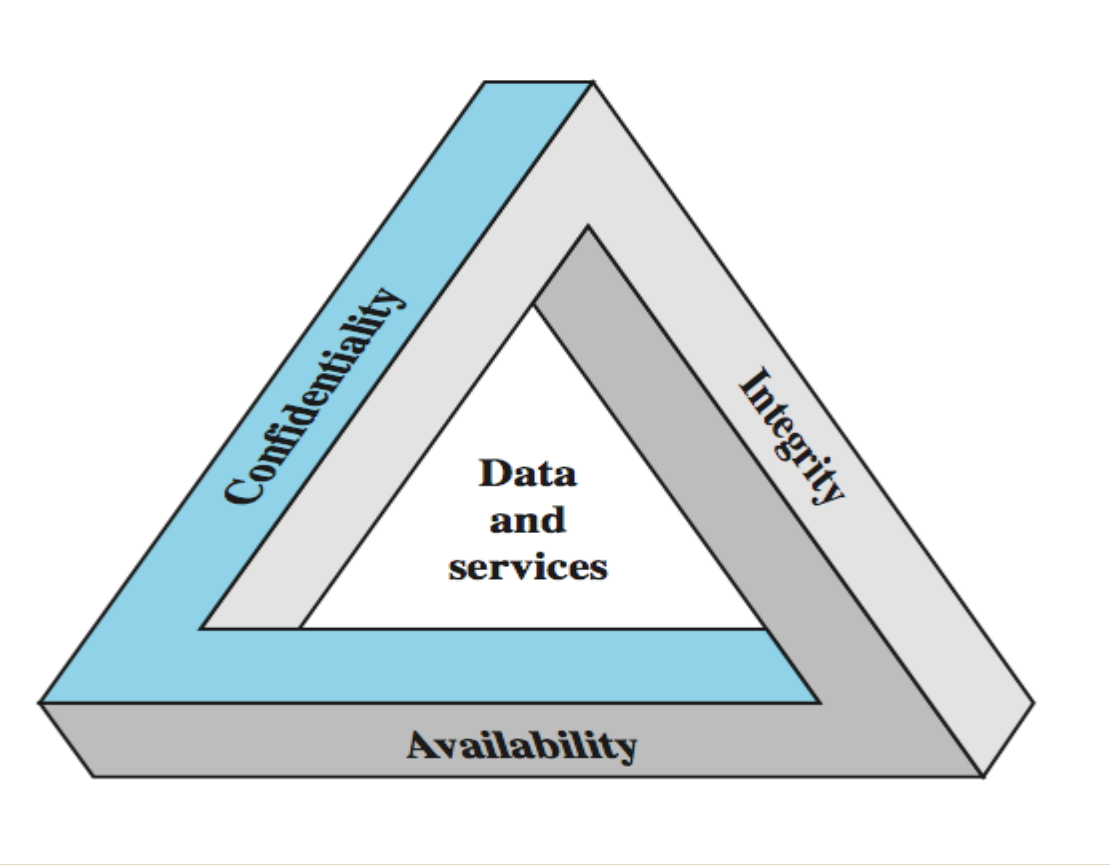
Our research has shown pay for information security and security jobs, skills and certifications have been above average for two years straight … The writing is on the wall: If you are not in that business, you might want to point your career toward that …. Security has not been a sexy place to work. It has not been funded well. But clearly when the smoke clears it will be funded, and it will be funded well.

Source: David Foote – President and chief research officer at Foote partners (www.footepartners.com)

Computer Security

- the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

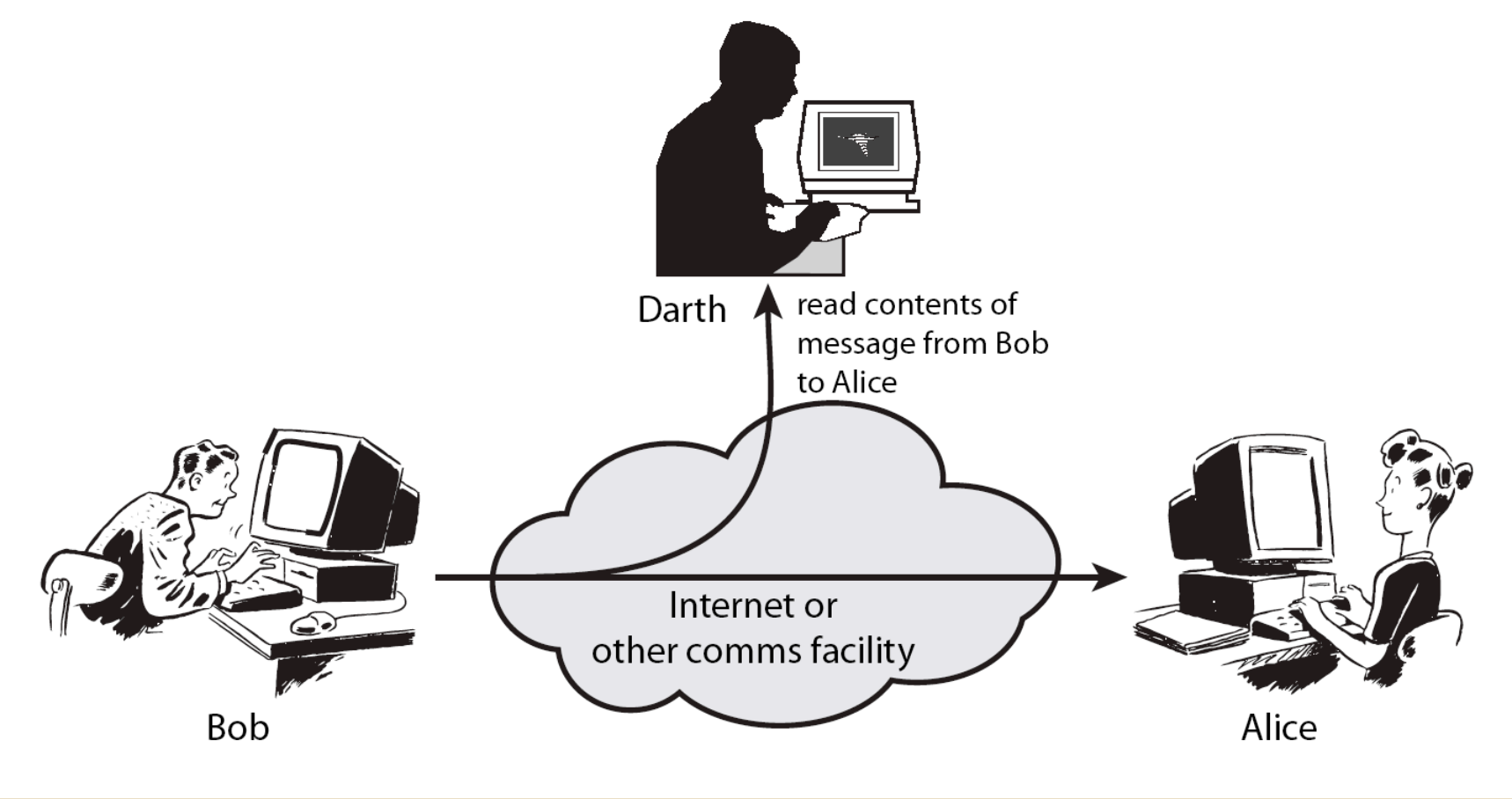
Key Security Concepts



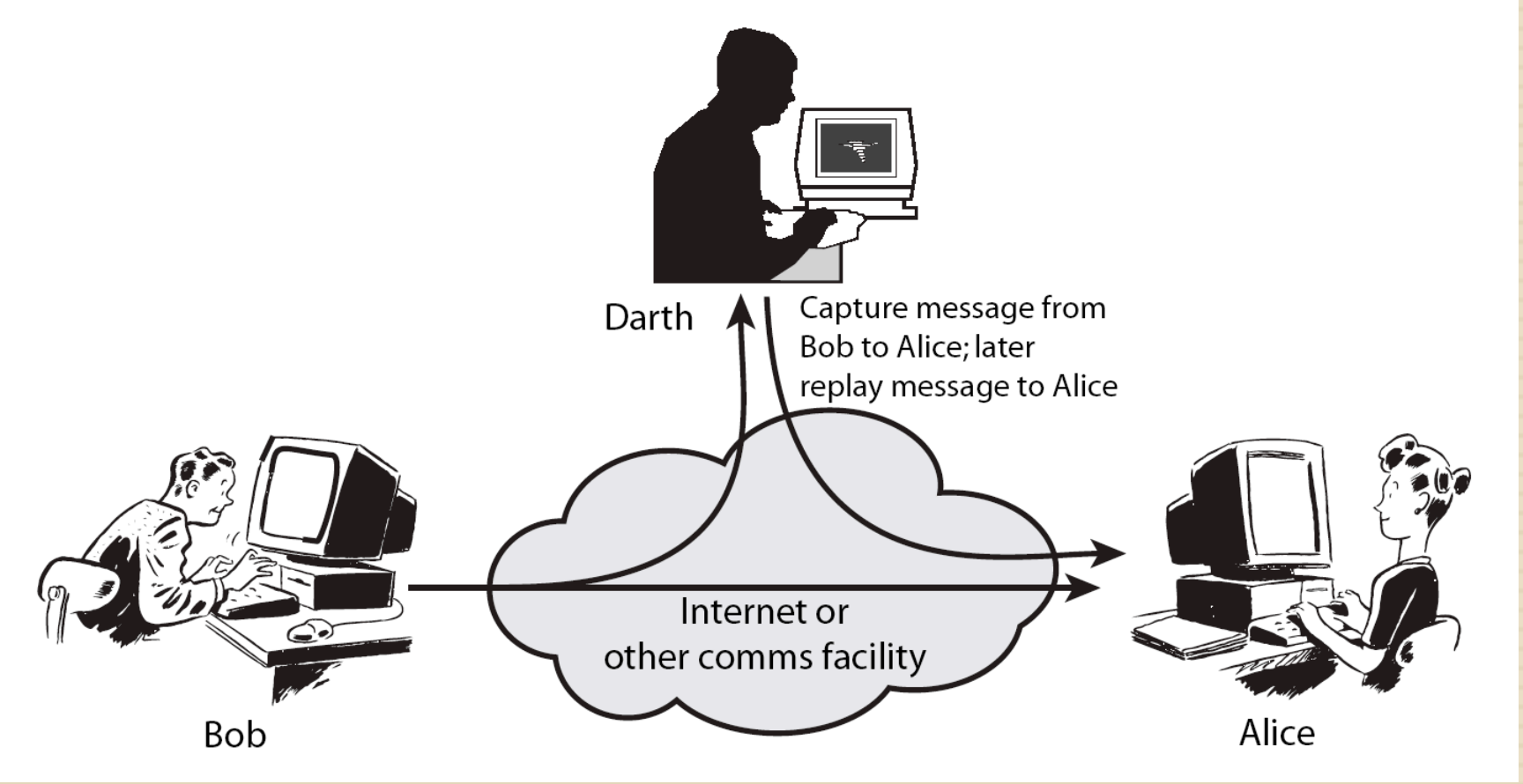
Levels of Impact

- can define 3 levels of impact from a security breach
  - Low
  - Moderate
  - High

Passive Attacks



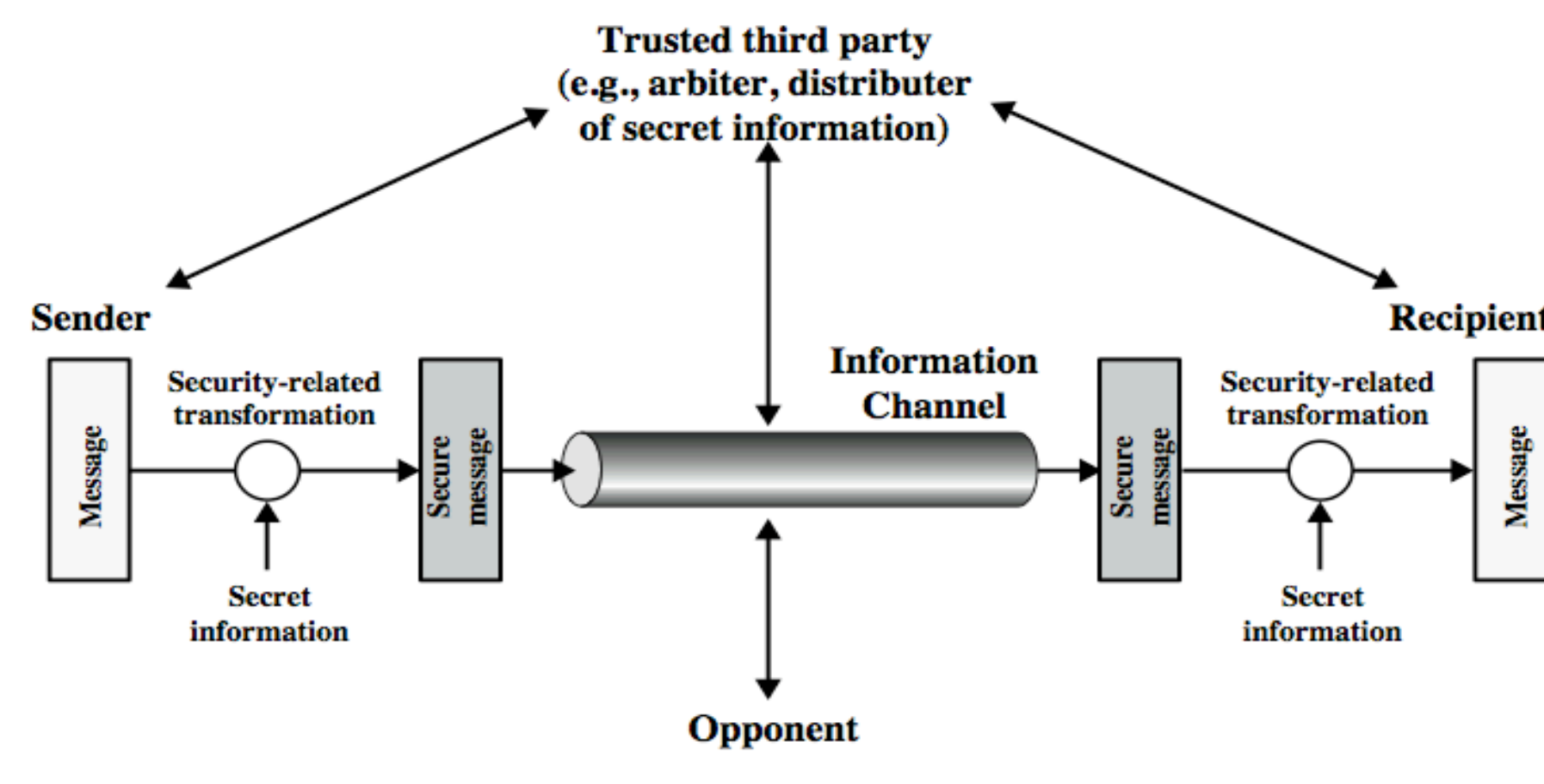
Active Attacks



Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - **cryptographic techniques**

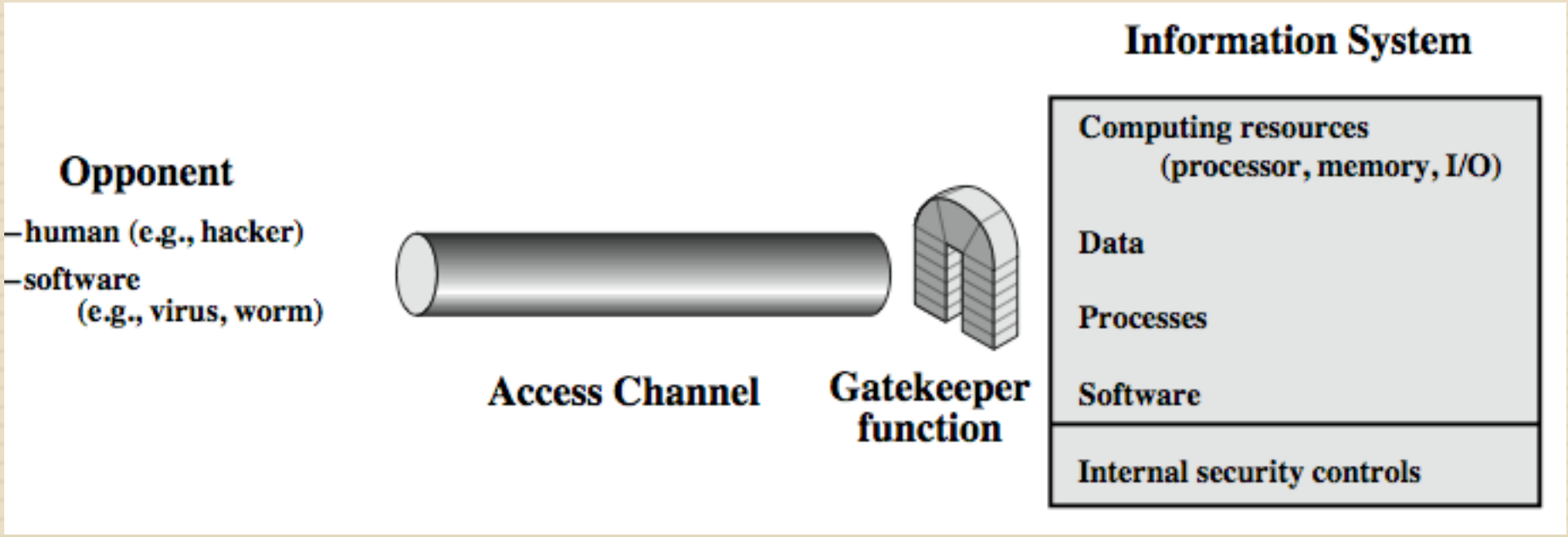
Model for Network Security



Model for Network Security

- using this model requires us to:
  1. design a suitable algorithm for the security transformation
  2. generate the secret information (keys) used by the algorithm
  3. develop methods to distribute and share the secret information
  4. specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

- using this model requires us to:
  1. select appropriate gatekeeper functions to identify users
  2. implement security controls to ensure only authorised users access designated information or resources

Security and Cryptography

The bottom line

- You are all 'digital natives' and the rest of us are 'digital immigrants'.
- However, are you 'digitally competent'
- It is projected that by 2015 the professional ICT shortage in EU will be approximately 700,000
  - Source: Enterprise & Industry Magazine, European Commission, Issue 13, July 2012.

Security Books you may want to read