SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

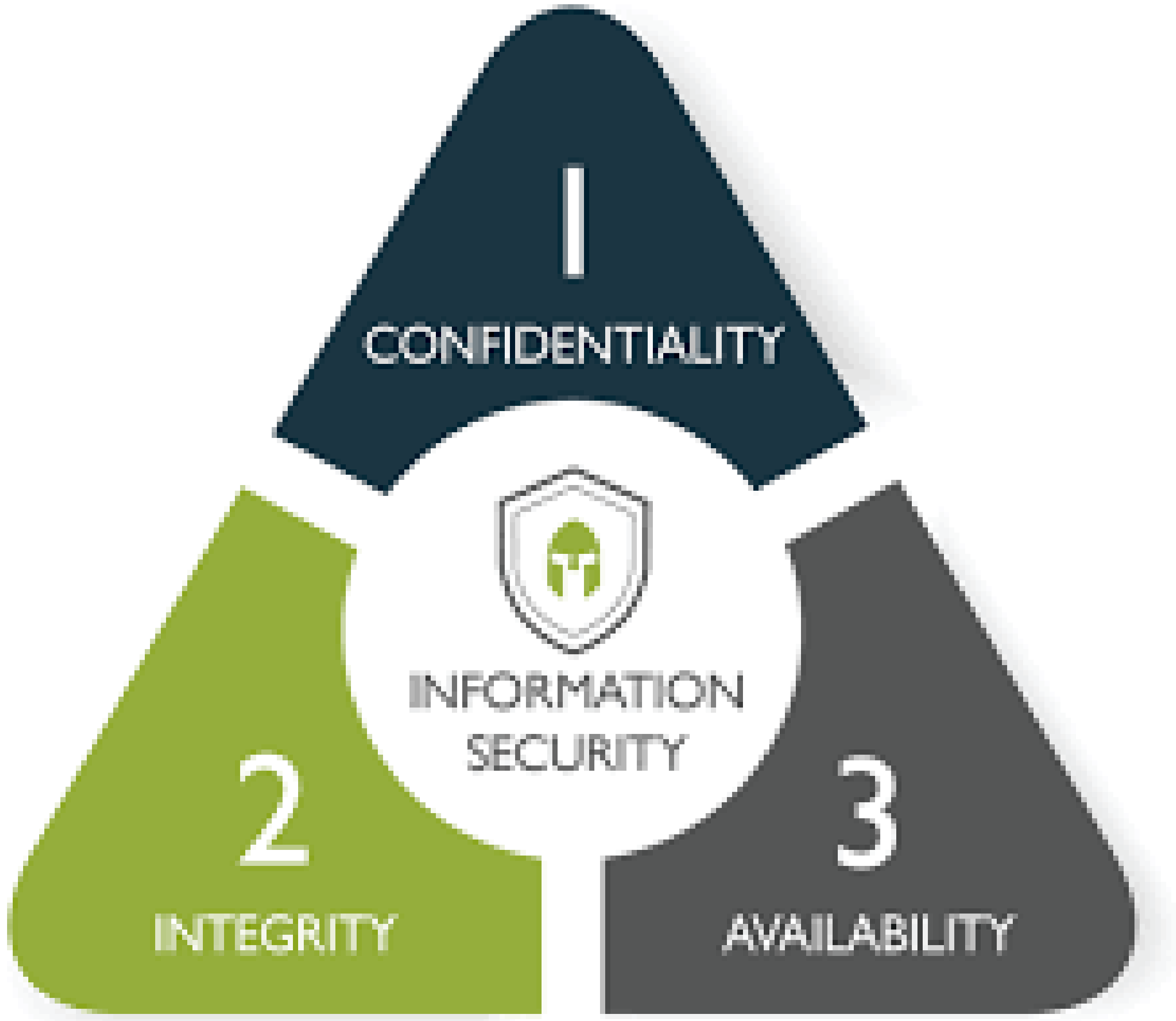
Course Code and Name : 19CS503 – CRYPTOGRAPHY AND NETWORK SECURITY

III YEAR /V SEMESTER

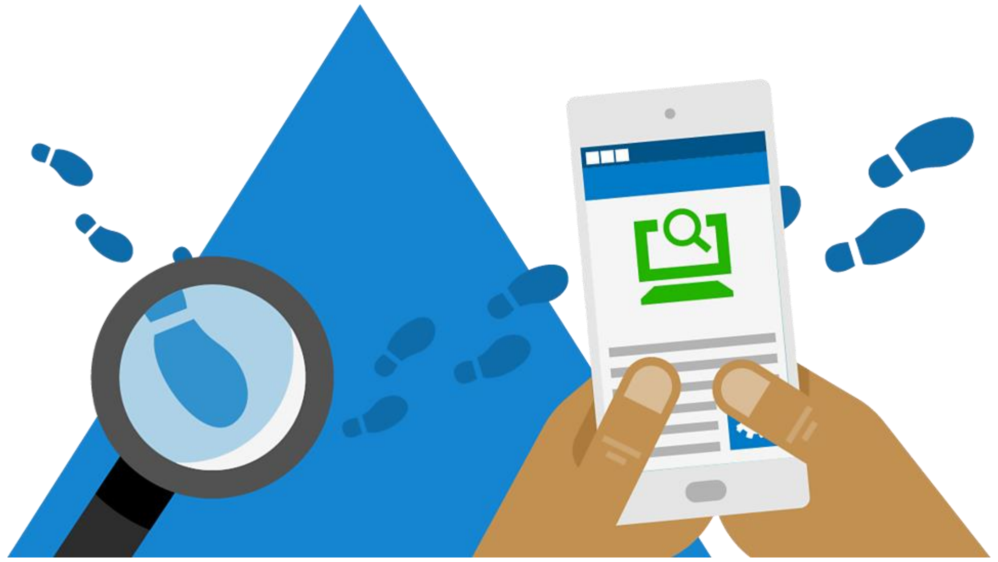
Unit 1: Introduction

Topic : Need for Security at Multiple levels, Security Policies and Model of Network security

RECAP


1
CONFIDENTIALITY
INFORMATION SECURITY
2
INTEGRITY
3
AVAILABILITY

IP



SECURITY ARCHITECTURE

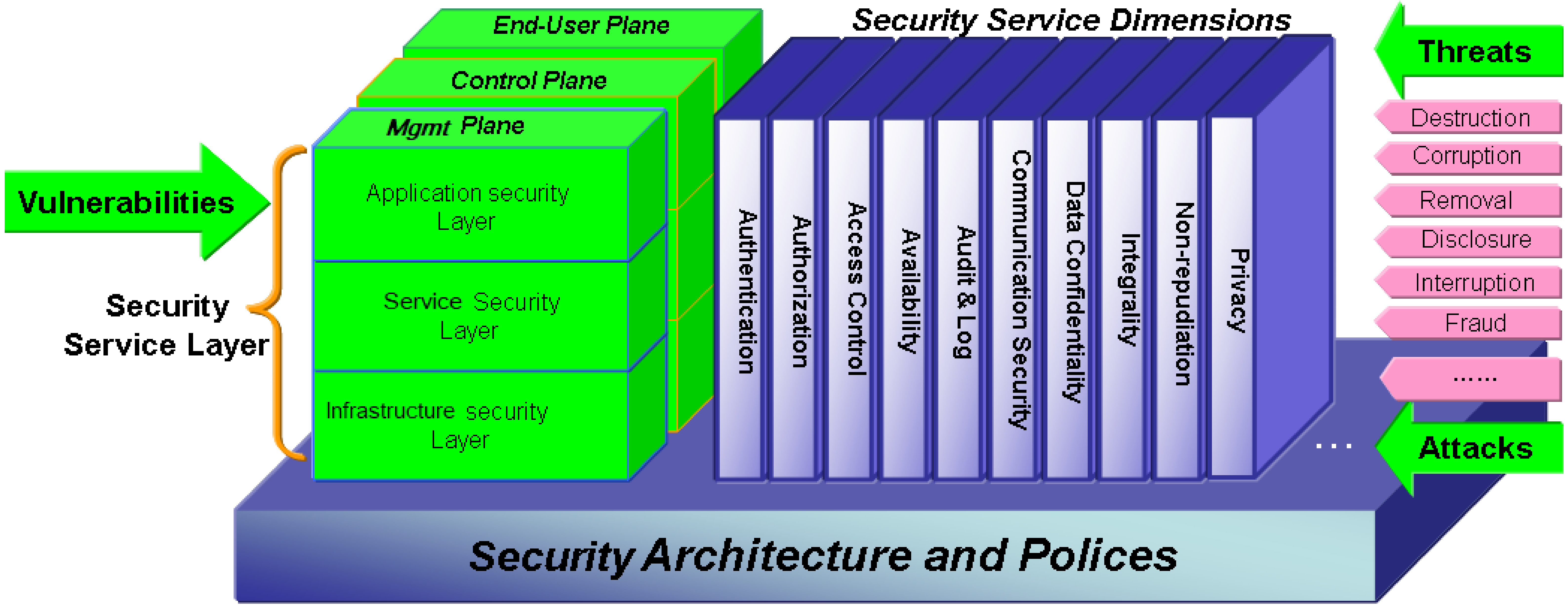
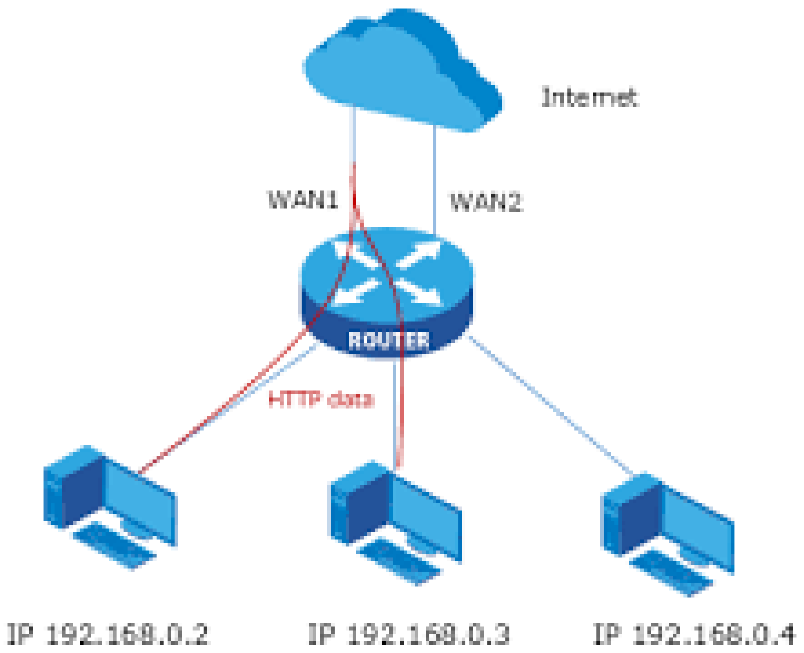
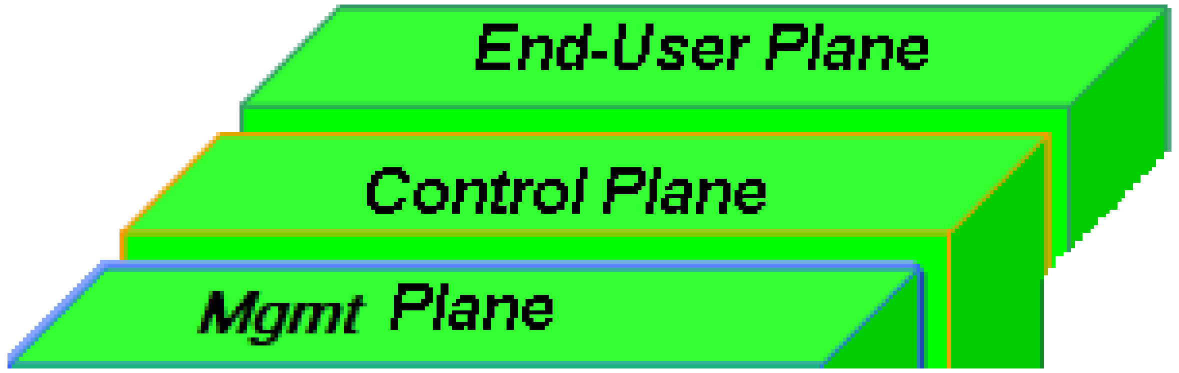


Image Source: https://support.huawei.com/enterprise/en/doc/EDOC1100011874/b7d1754f/esight-security-model

Security Planes

- Events are kept isolated from one another for effective Security implementation
- Facilitates identifying security concerns and effectively addressing them.



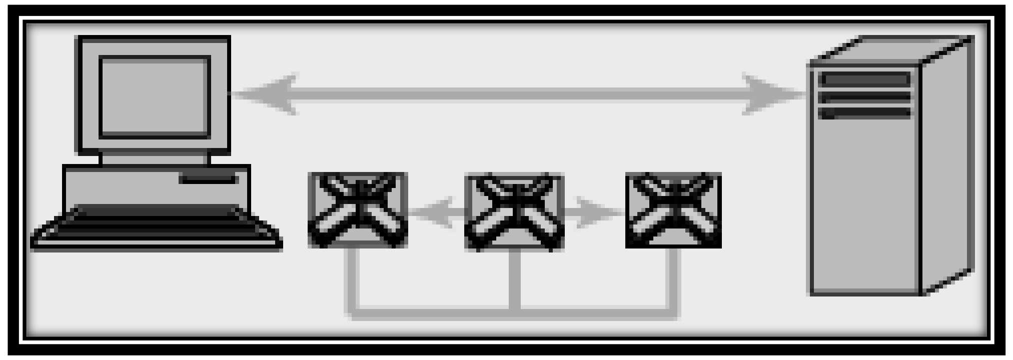


End-User Plane

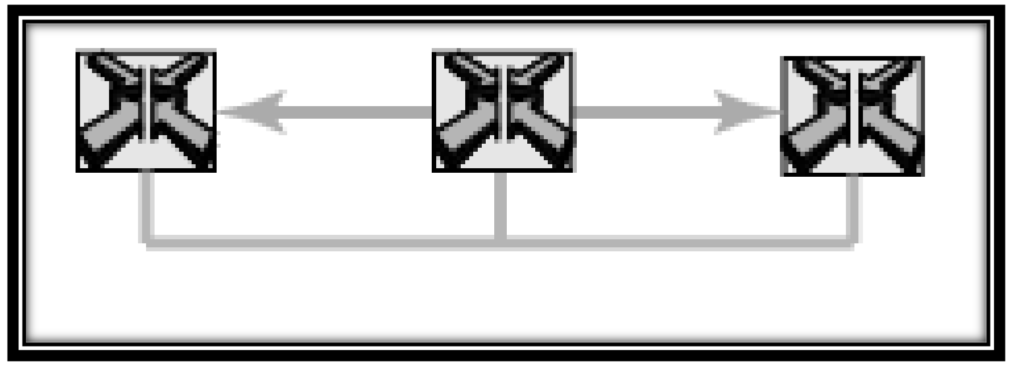
Control Plane

Mgmt Plane

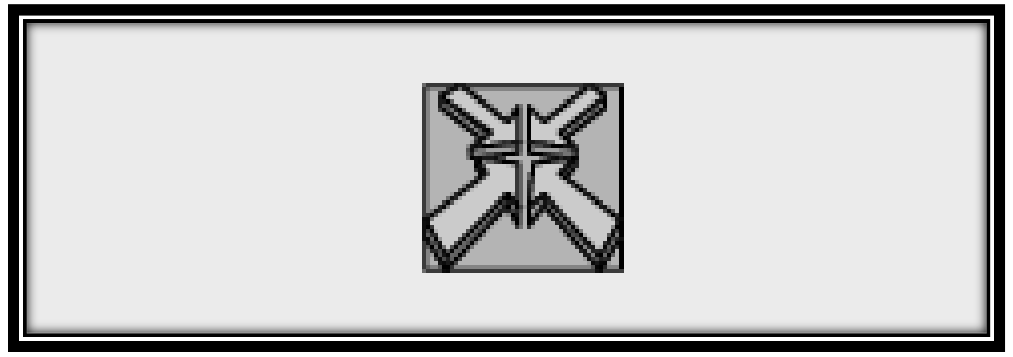
Security Layers



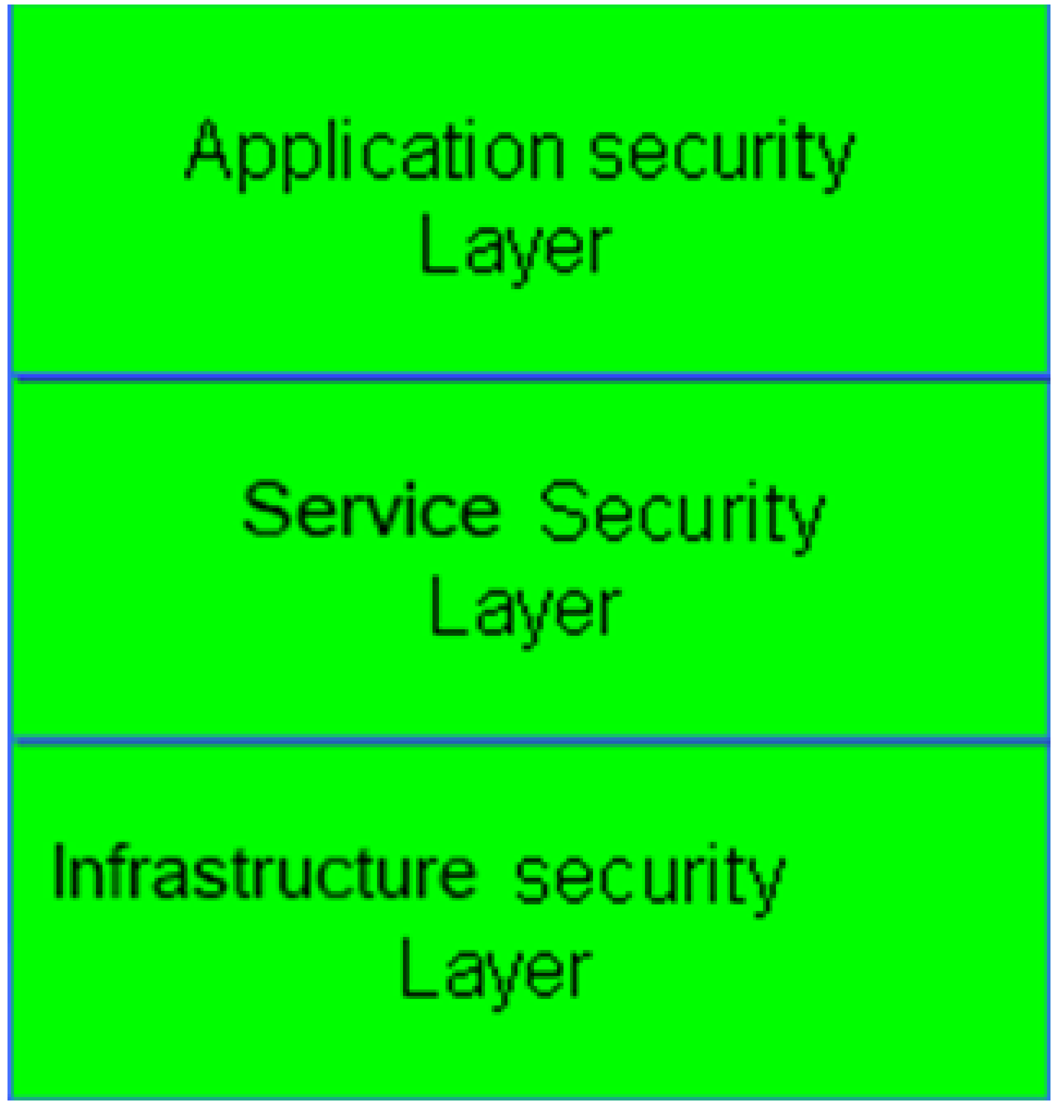
FTP, Web Browsing, e-Commerce



Frame Relay, ATM, IP, Wi-Fi, VoIP



Servers, Switches, Routers, Wan and Ethernet Links



Application security Layer

Service Security Layer

Infrastructure security Layer

Image Source: https://support.huawei.com/enterprise/en/doc/EDOC1100011874/b7d1754f/esight-security-model

Threats and Attacks

Destruction

Corruption

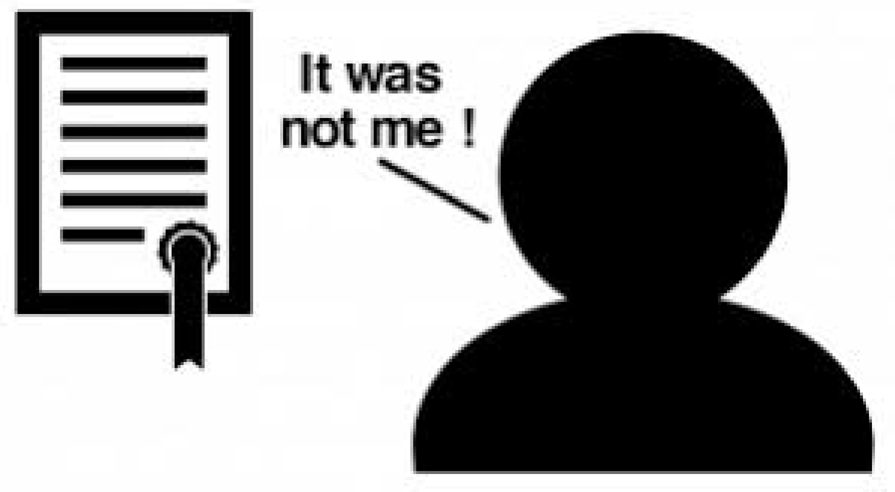
Removal

Disclosure

Interruption

Security Dimensions

- Access Control
- Authentication
- Non- Repudiation
- Data Confidentiality
- Communication
- Data Integrity
- Availability
- Privacy



IMAGINE YOU ARE A KEY PROFESSIONAL IN A COMPANY...

WHO IS RESPONSIBLE FOR THE SECURITY OF DATA?

WHY DO YOU DEVELOP A POLICY?

SECURITY POLICIES

- **Security policy refers to clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an organization's system and the information included in it.**
- Good policy protects not only information and systems, but also individual employees and the organization as a whole.
- It also serves as a prominent statement to the outside world about the organization's commitment to security.

Source: https://nces.ed.gov/pubs98/safetech/chapter3.asp

How to develop a Policy

- Identify sensitive information and critical systems
- Incorporate local, state, and federal laws, as well as relevant ethical standards
- Define institutional security goals and objectives
- Set a course for accomplishing those goals and objectives
- Ensure that necessary mechanisms for accomplishing the goals and objectives are in place

What does a Security Policy include?

- What is the reason for the policy?
- Who developed the policy?
- Who approved the policy?
- Whose authority sustains the policy?
- Which laws or regulations, if any, are the policy based on?
- Who will enforce the policy?
- How will the policy be enforced?
- Whom does the policy affect?

- What information assets must be protected?
- What are users actually required to do?
- How should security breaches and violations be reported?
- What is the effective date and expiration date of the policy?

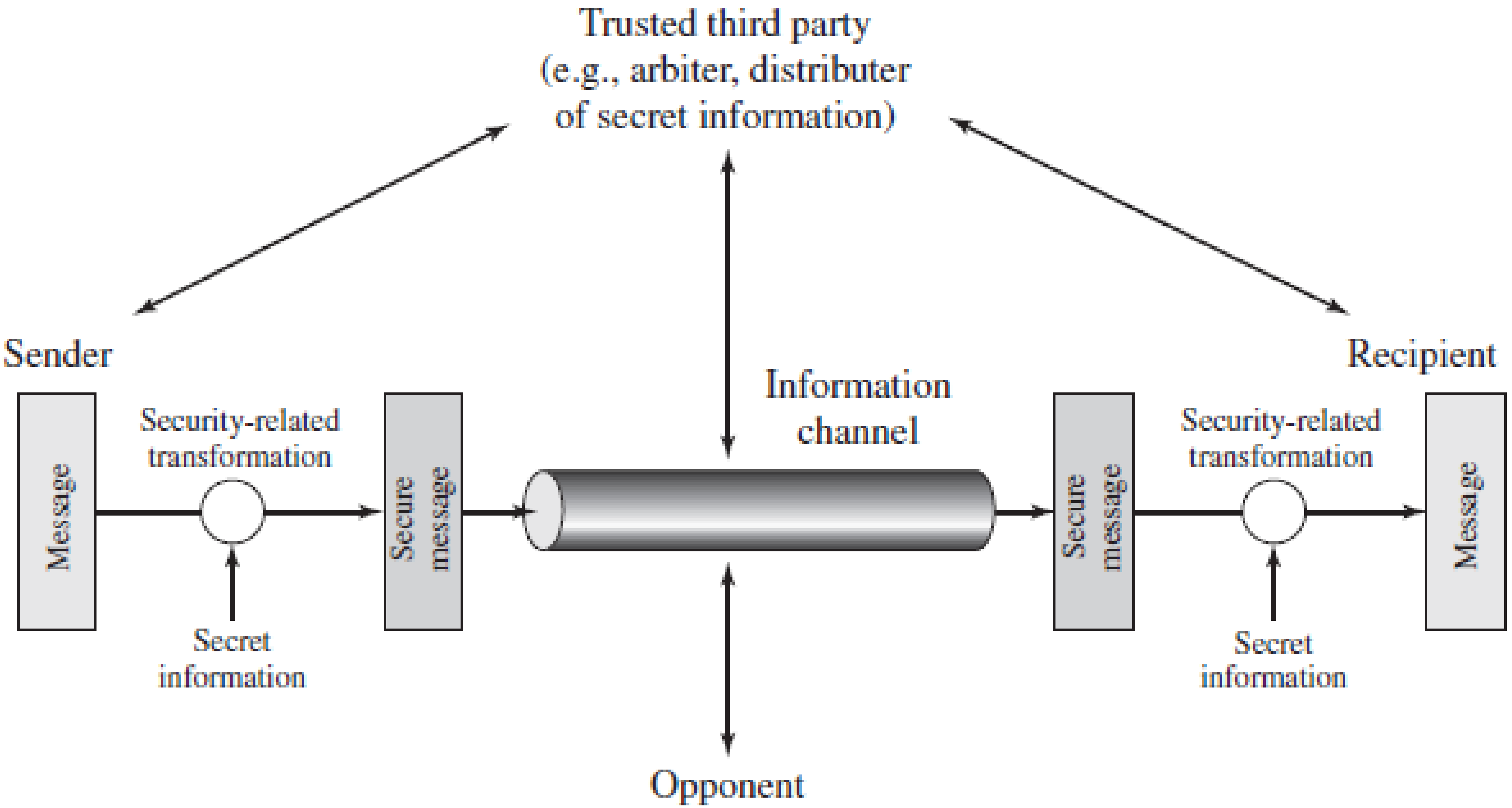
Right tone to write a policy

- Be **concise**--focus on expectations and consequences, but explain the underlying rationale when appropriate
- **Don't temper** the message--truth is, you're not asking but telling, so don't propose, suggest, or insinuate unless that is specifically what you mean to do
- Use **simple, straightforward language** as is possible
- **Define** any **term** that could potentially **confuse** a reader--no need to make things more difficult than need be
- Be **creative--presentation** should never interfere with content, but checklists and reference cards increase utility

Employees need to be informed..

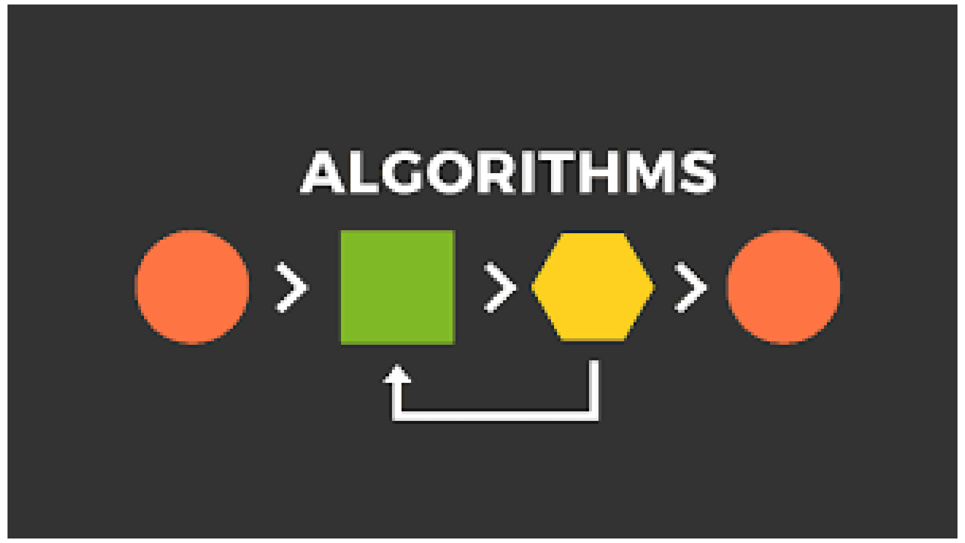
- Employees must be told in writing
  - Acceptable and Not in use of equipments
  - Penalties on violation
  - Activities monitored
  - Security as a part of Performance Review
- Employees should be reminded that
  - Organizational resource belong to organization
  - Privacy of Information stored in organization's Equipments
- Employees should be required to sign a Security Agreement
  - Read / Understood the policies
  - Forum to clarify doubts
  - Provide access after signing the agreement

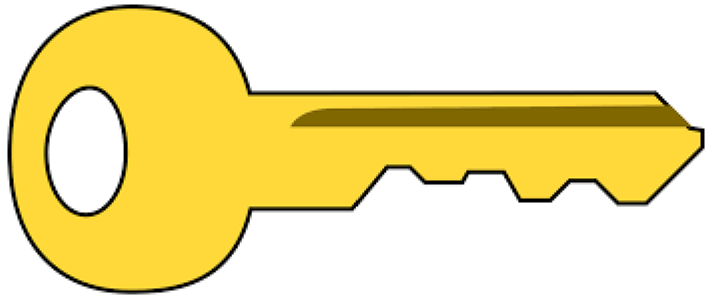
MODEL FOR NETWORK SECURITY



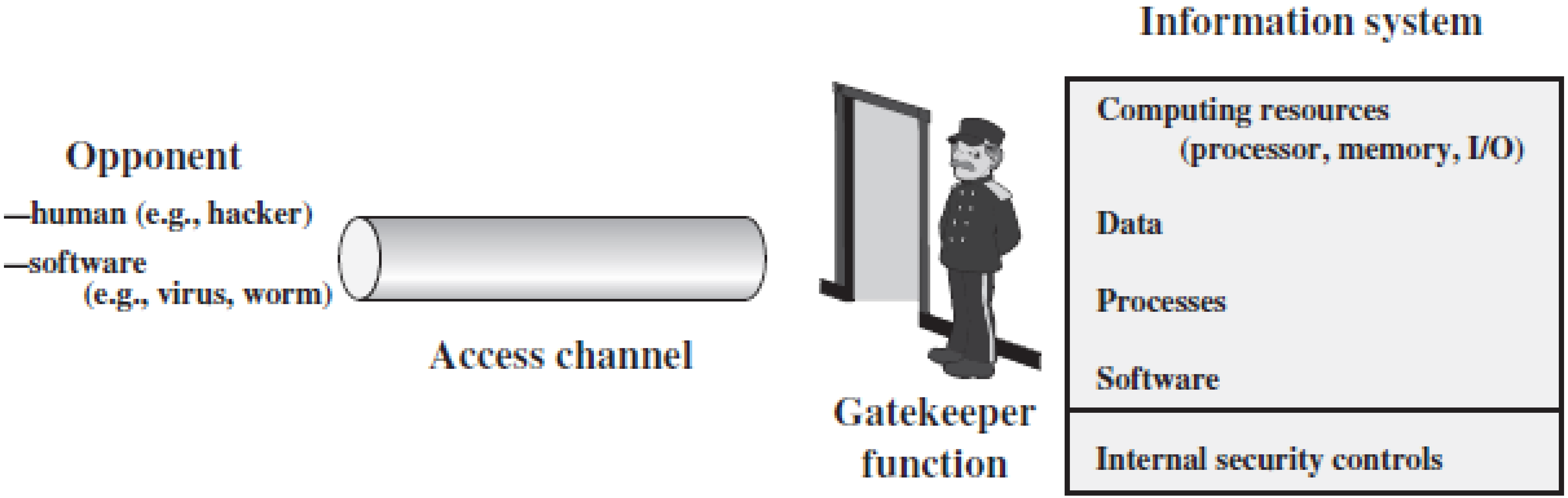
Four basic tasks in designing a particular security service

- Design a suitable algorithm for the security transformation
- Generate the secret information (keys) used by the algorithm
- Develop methods to distribute and share the secret information
- Specify a protocol enabling the principals to use the transformation and secret information for a security service





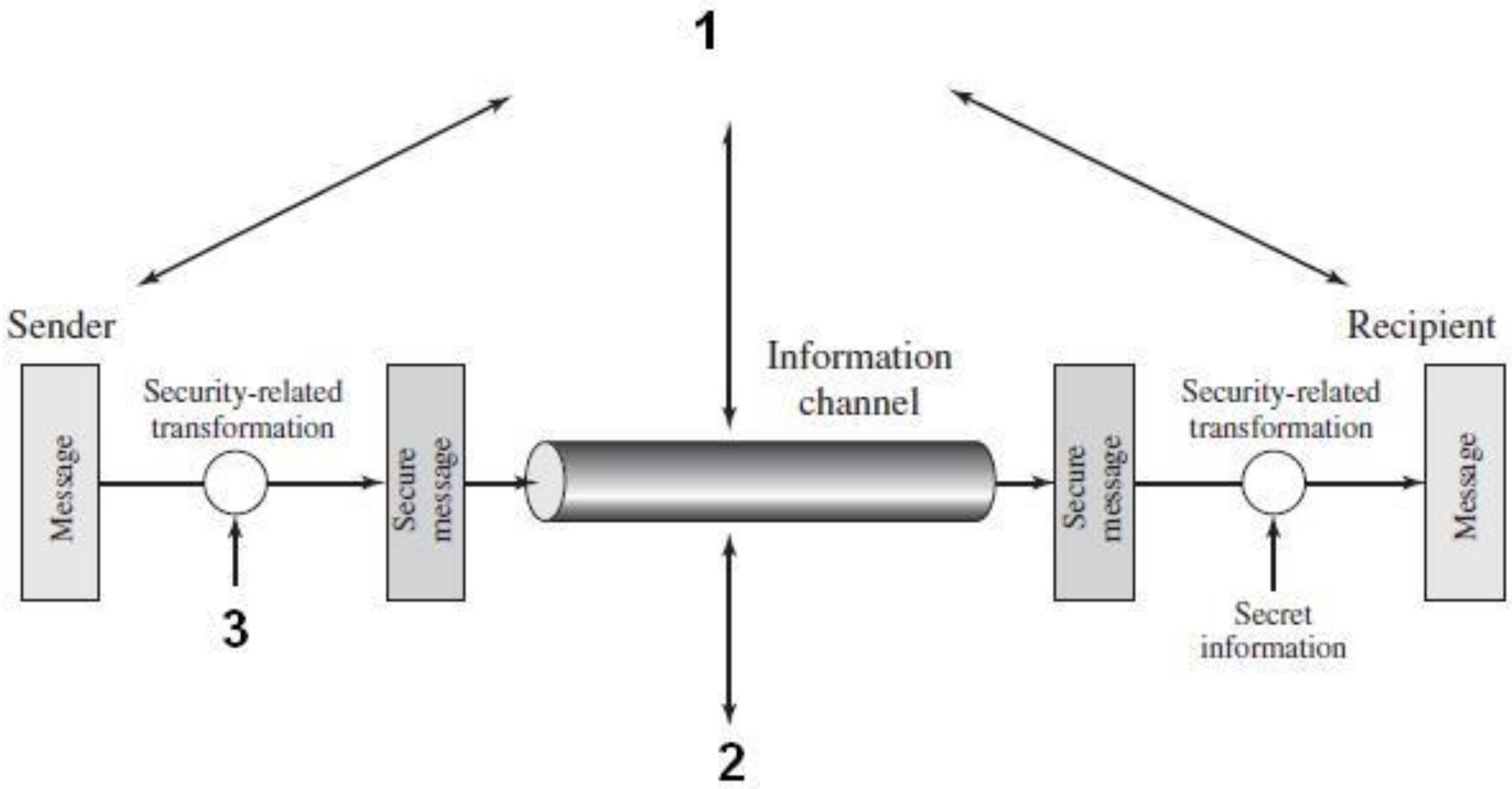
Network Access Security Model



Hacker / Intruder

- **Hacker**
- No malign intent
- Simply gets satisfaction from breaking and entering a computer system
- **Intruder**
- Do damage
- A criminal who seeks to exploit computer assets for financial gain

ASSESSMENT - Complete the diagram.



REFERENCES

- William Stallings, Cryptography and Network Security: Principles and Practice, PHI 3rd Edition, 2006.
- https://nces.ed.gov/pubs98/safetech/chapter3.asp
- https://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=3
- C K Shyamala, Cryptography and Network Security

THANK YOU