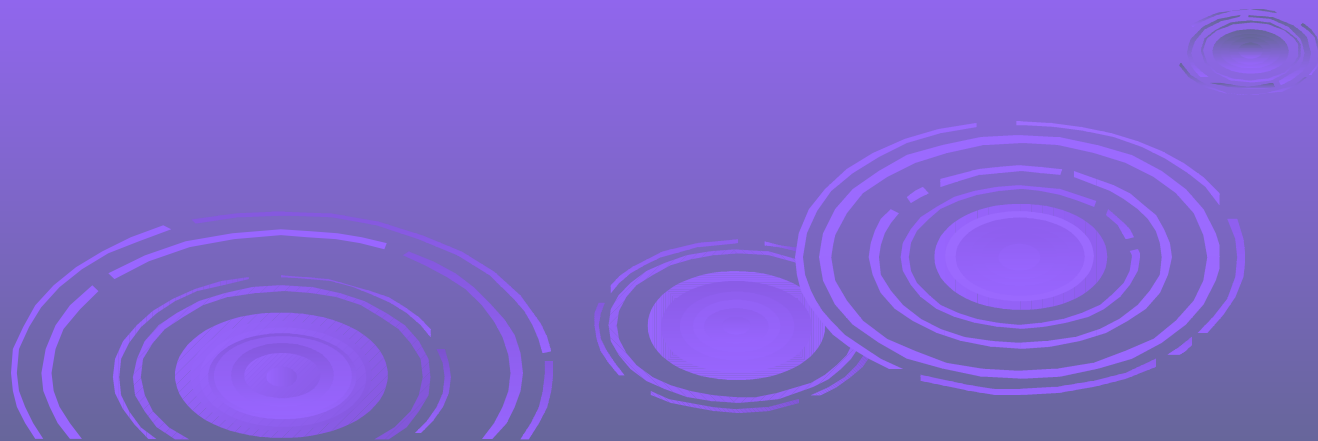


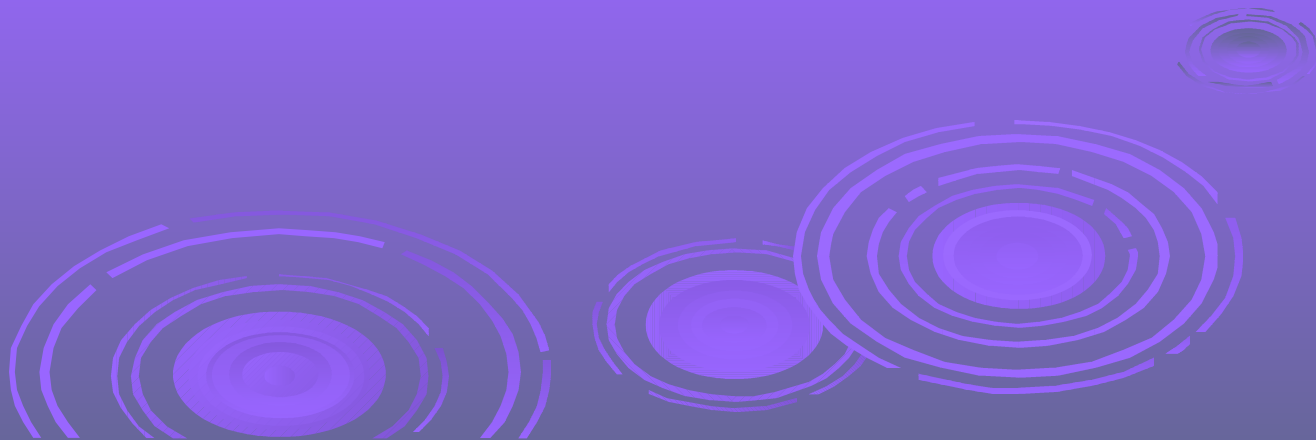
Cryptography and Network Security

Chapter 1



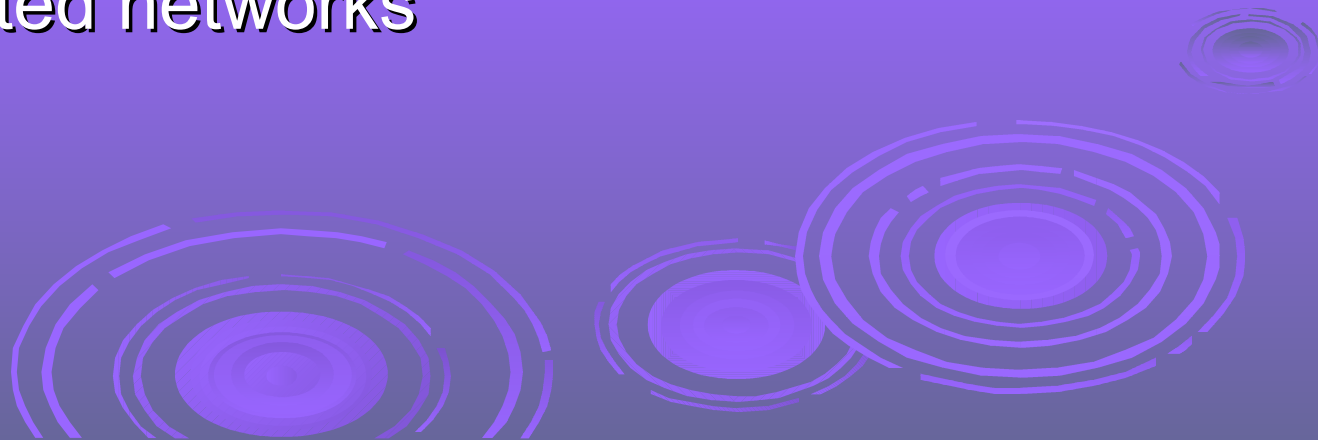
Background

- Information Security requirements have changed in recent times
- traditionally provided by physical and administrative mechanisms
- computer use requires automated tools to protect files and other stored information
- use of networks and communications links requires measures to protect data during transmission

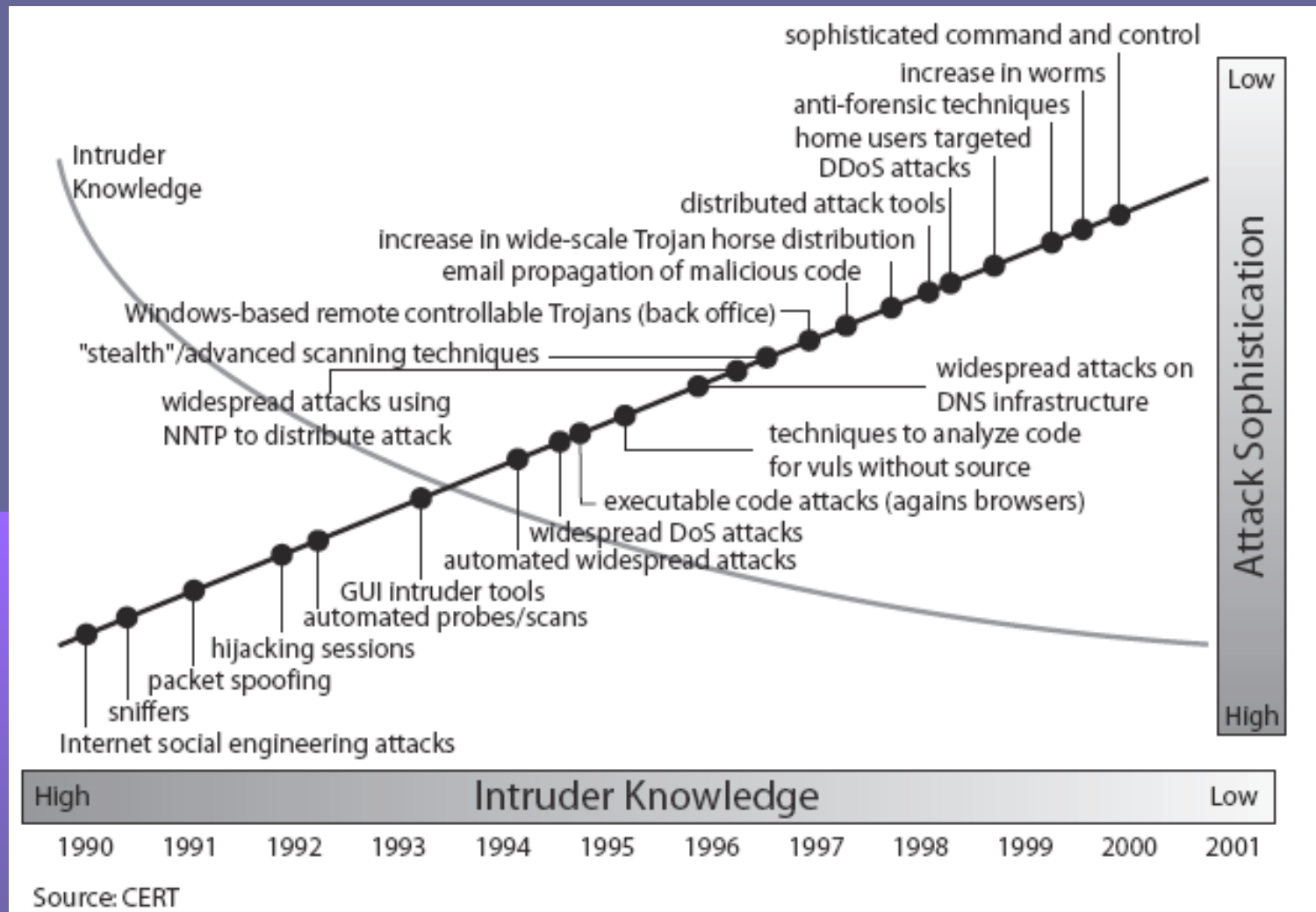


Definitions

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

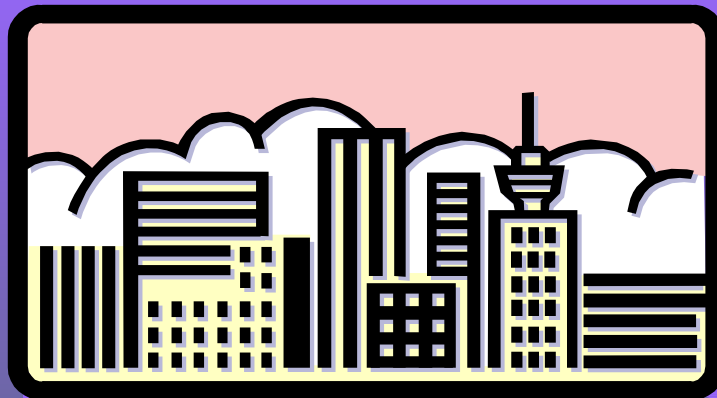


Security Trends



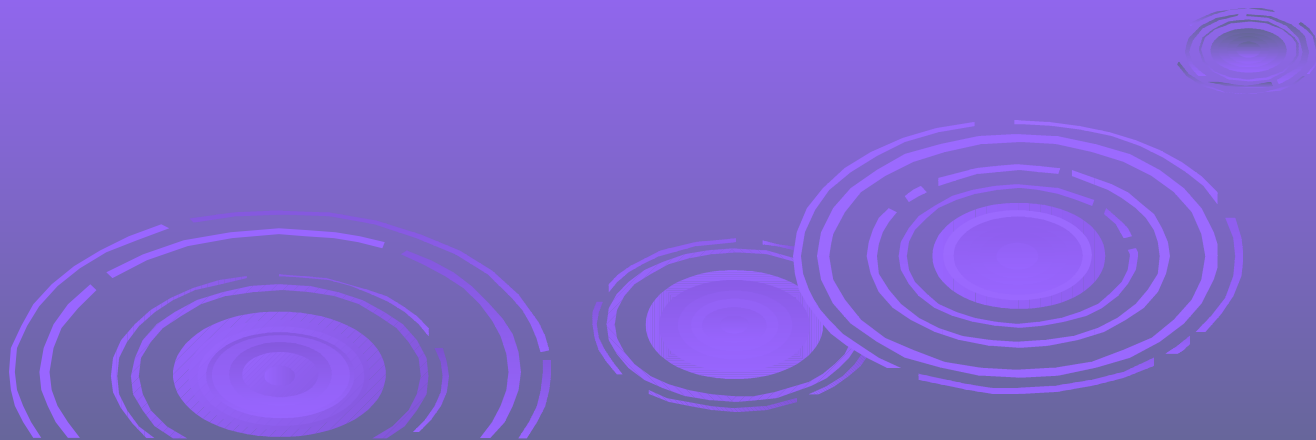
OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study



Aspects of Security

- consider 3 aspects of information security:
 - **security attack**
 - **security mechanism**
 - **security service**

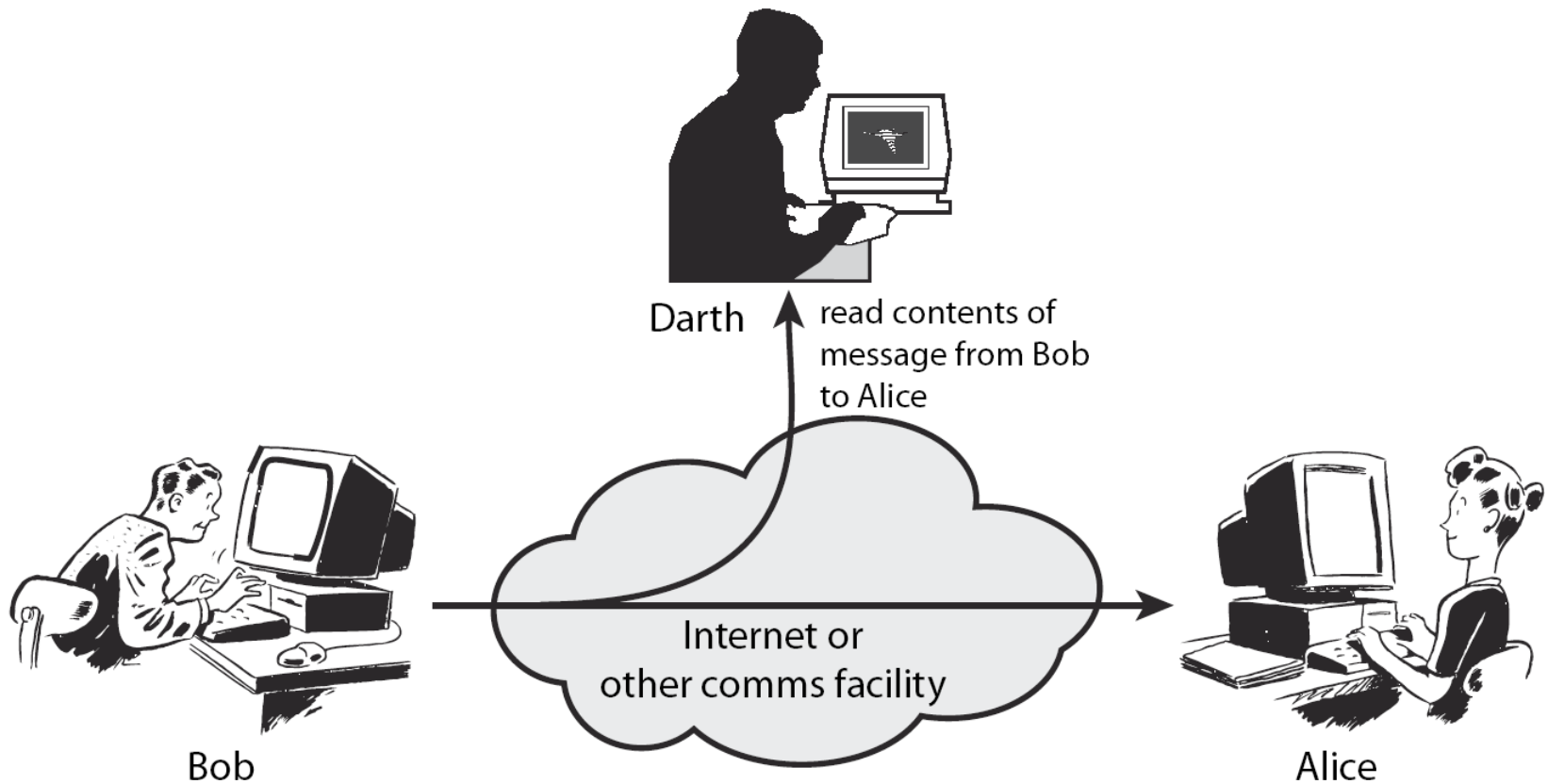


Security Attack

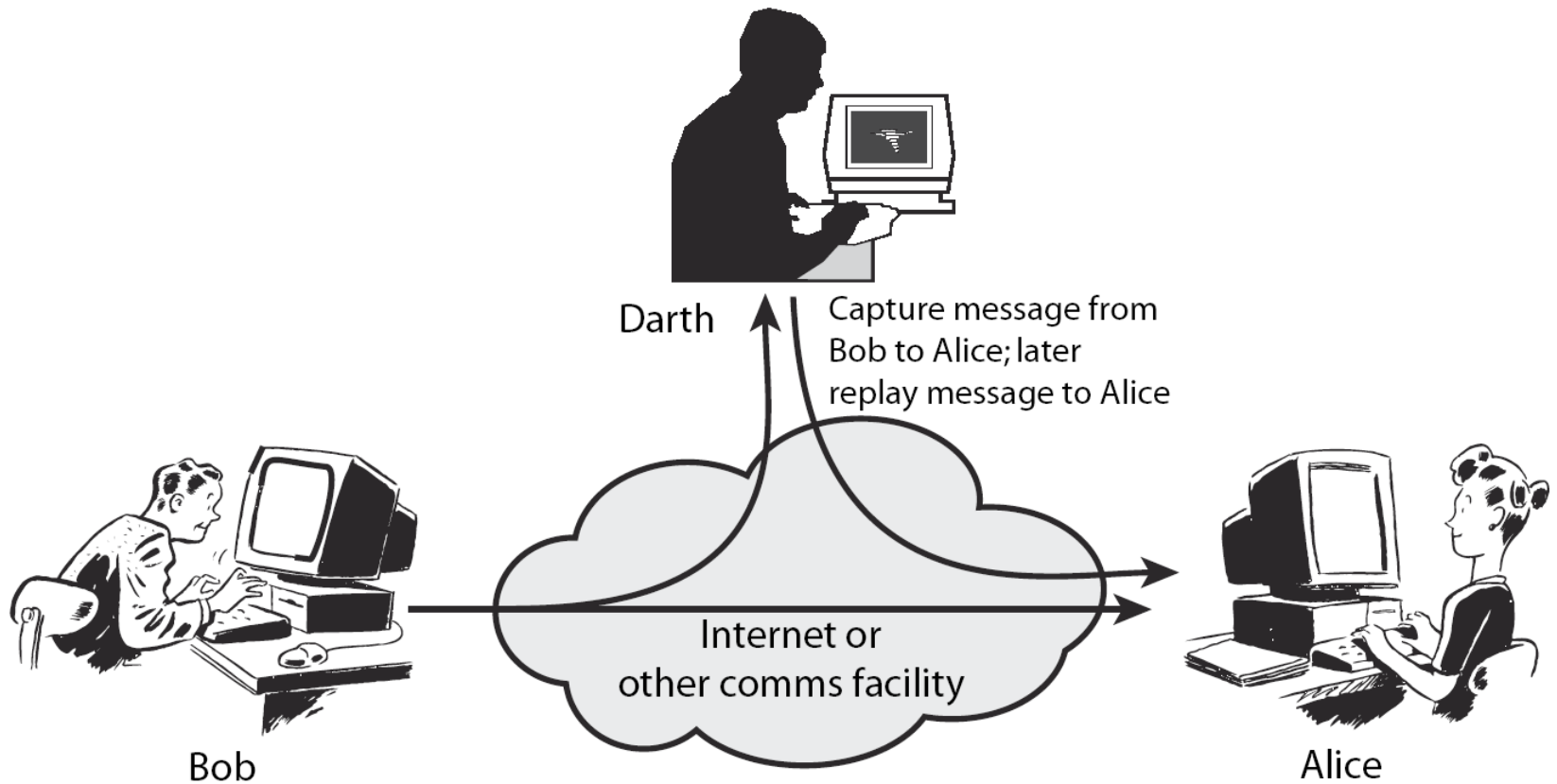
- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- often *threat* & *attack* used to mean same thing
- have a wide range of attacks
- can focus of generic types of attacks
 - passive
 - active



Passive Attacks



Active Attacks



Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
 - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Services

- X.800:

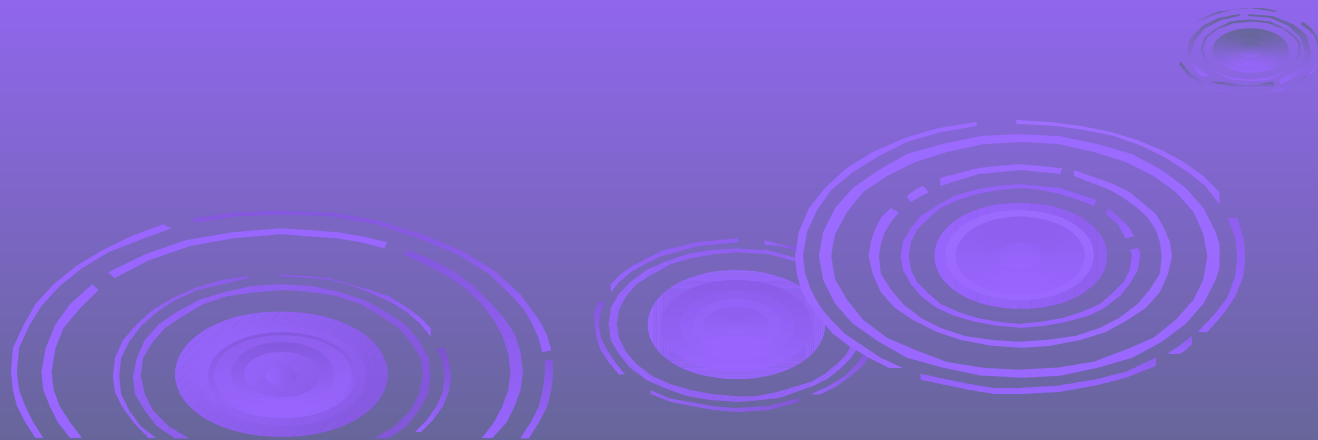
“a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”

- RFC 2828:

“a processing or communication service provided by a system to give a specific kind of protection to system resources”

Security Services (X.800)

- **Authentication** - assurance that the communicating entity is the one claimed
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication



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**
- hence our focus on this topic



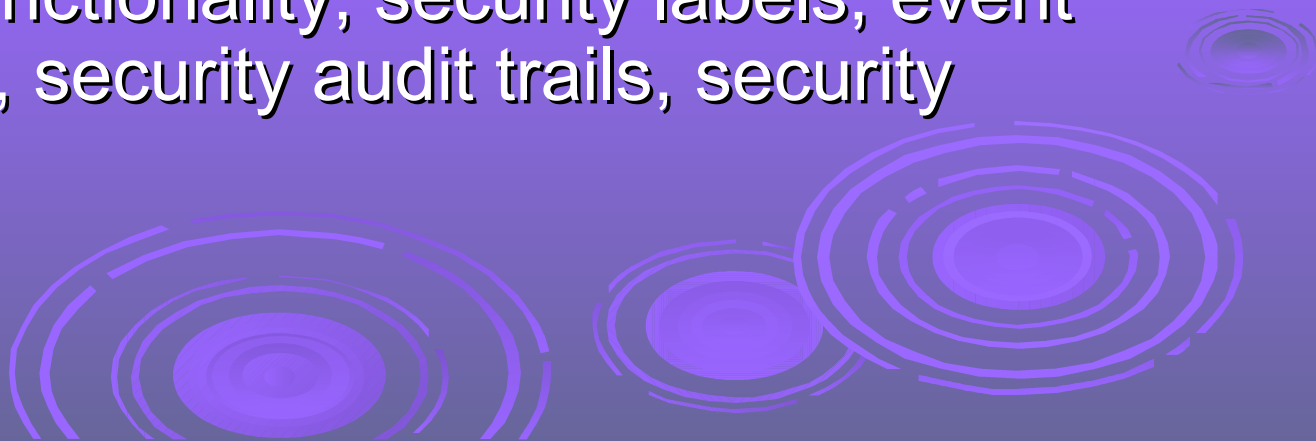
Security Mechanisms (X.800)

➤ specific security mechanisms:

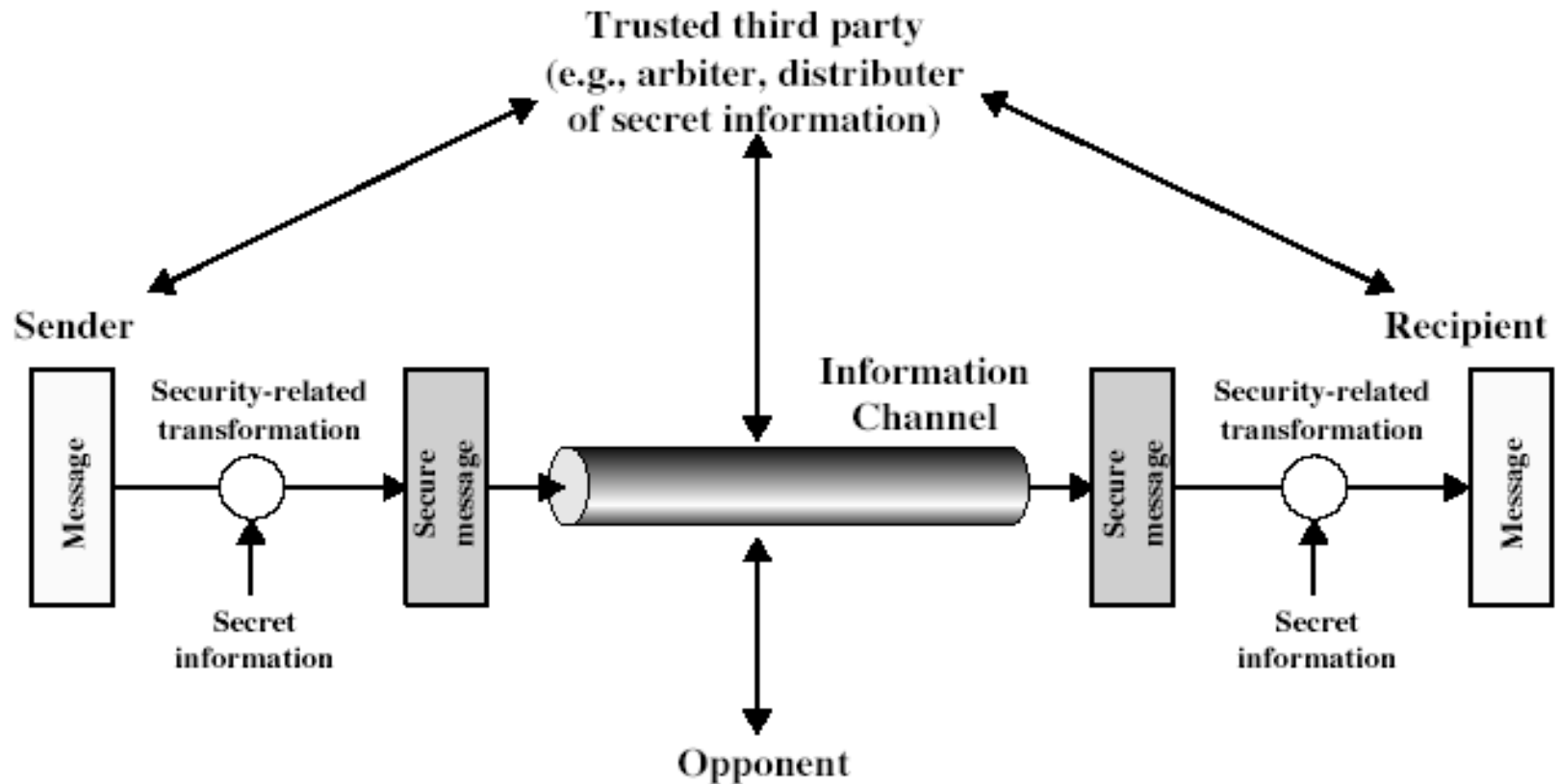
- encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization

➤ pervasive security mechanisms:

- trusted functionality, security labels, event detection, security audit trails, security recovery



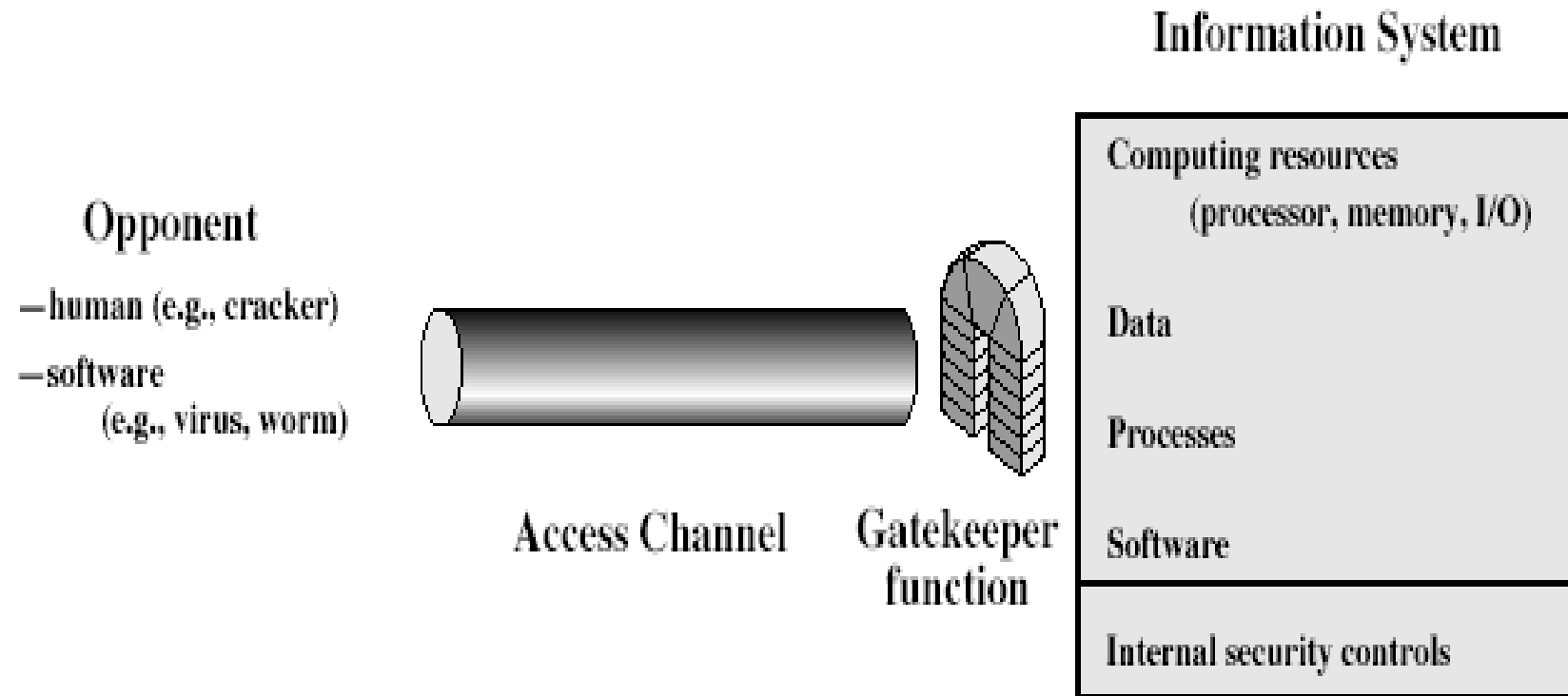
Model for Network Security



Model for Network Security

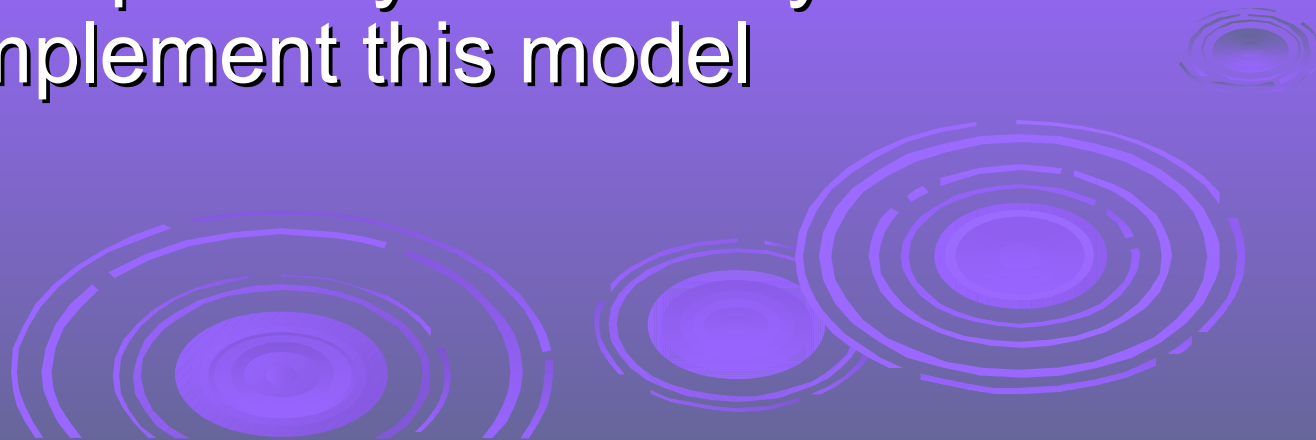
- using this model requires us to:
 1. design a suitable algorithm for the security transformation
 2. generate the secret information (keys) used by the algorithm
 3. develop methods to distribute and share the secret information
 4. specify a protocol enabling the principals to use the transformation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



Summary

- have considered:
 - definitions for:
 - computer, network, internet security
- X.800 standard
- security attacks, services, mechanisms
- models for network (access) security

