Network Security

192654000: INF (BSc), TEL (BSc, MSc), CS, EE, MBI (MSc)
201000086: Kerckhoffs (MSc)

Design and Analysis of Communication Networks (DACS)

University of Twente

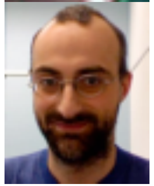
The Netherlands

Teaching staff

- Dr.ir. Aiko Pras
  a.pras@utwente.nl - http://wwwhome.cs.utwente.nl/~pras/

- Dr.ir. Georgios Karagiannis
  g.karagiannis@utwente.nl - http://wwwhome.cs.utwente.nl/~karagian/

- Dr.ir. Pieter-Tjerk de Boer
  p.t.deboer@utwente.nl - http://wwwhome.cs.utwente.nl/~ptdeboer/



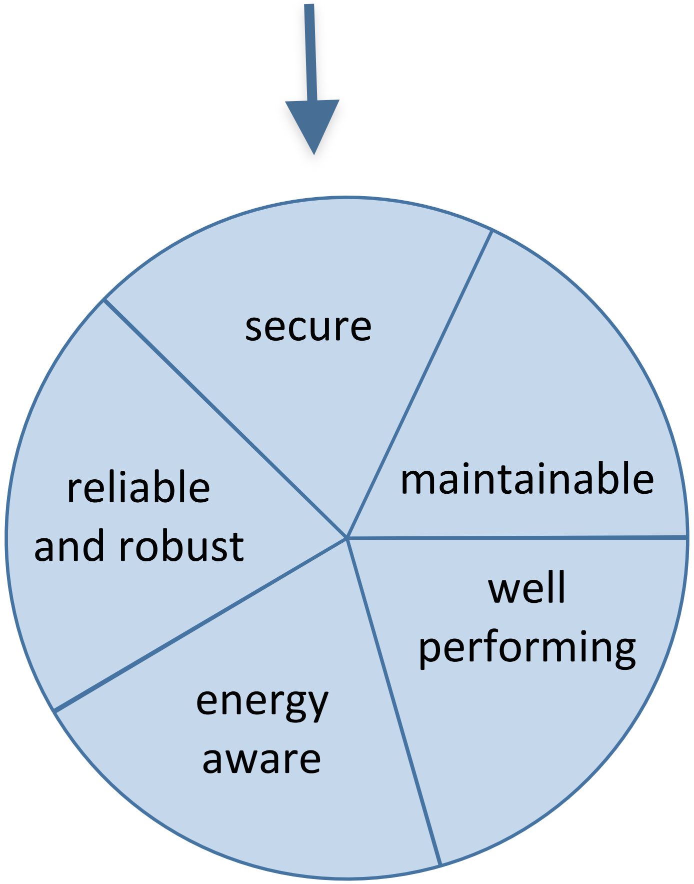
- Dr. Ramin Sadre
  sadrer@ewi.utwente.nl - http://wwwhome.cs.utwente.nl/~sadrer/

- Anna Sperotto
  a.sperotto@utwente.nl - http://wwwhome.cs.utwente.nl/~sperottoa/

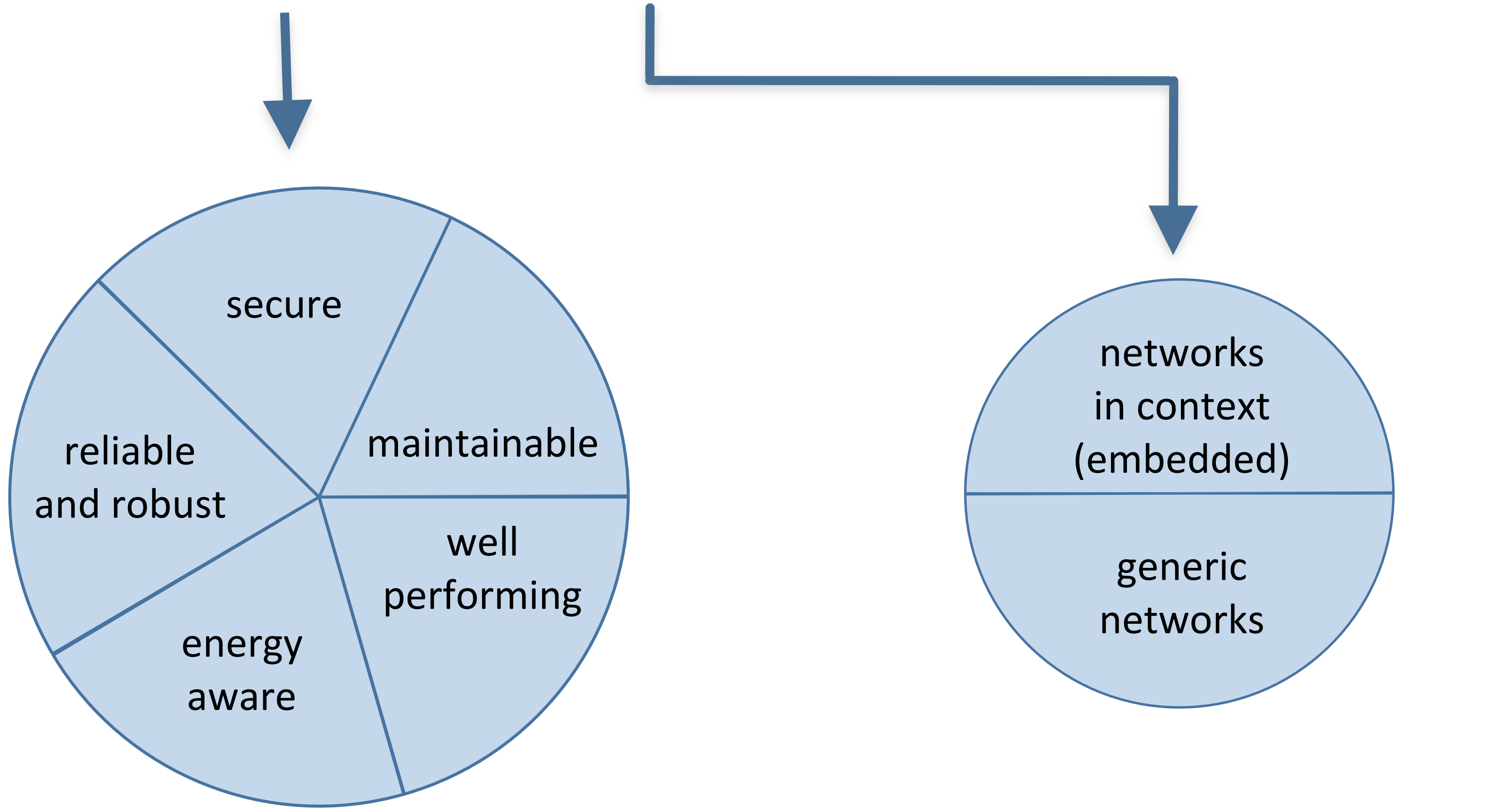
About DACS

Dependable networking in a dynamic world

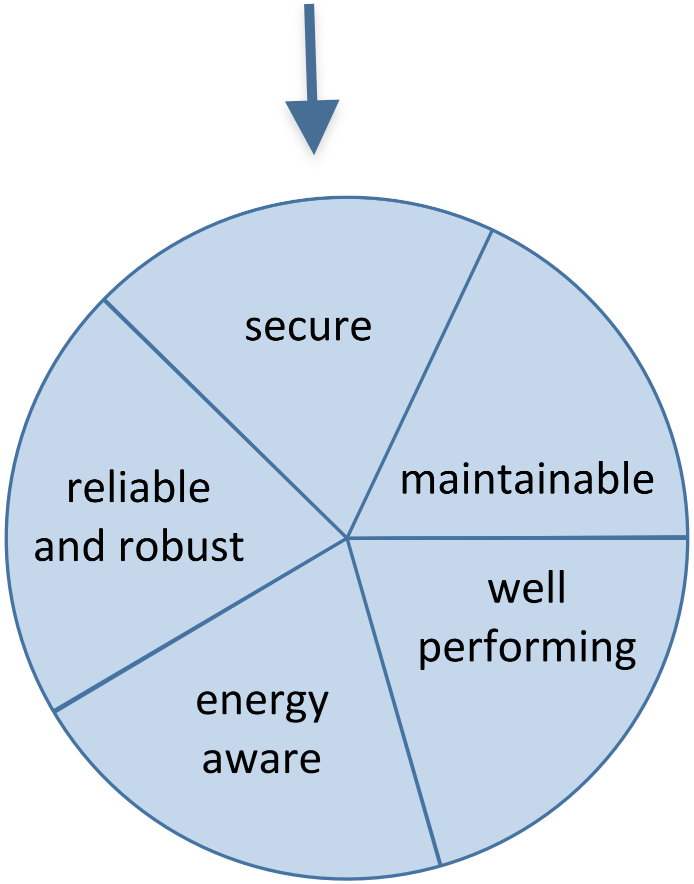
Dependable networking in a dynamic world

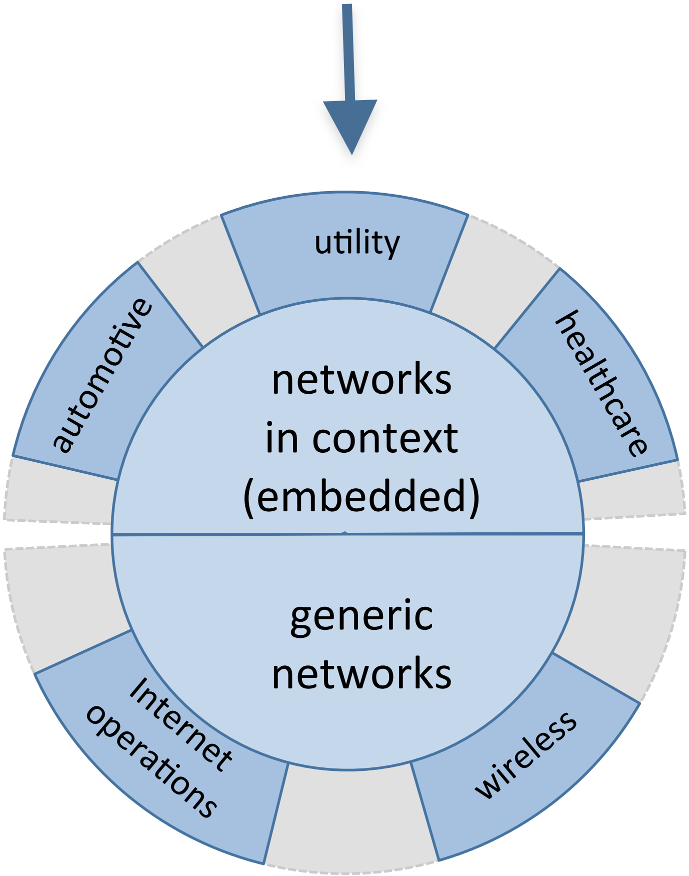


Dependable networking in a dynamic world



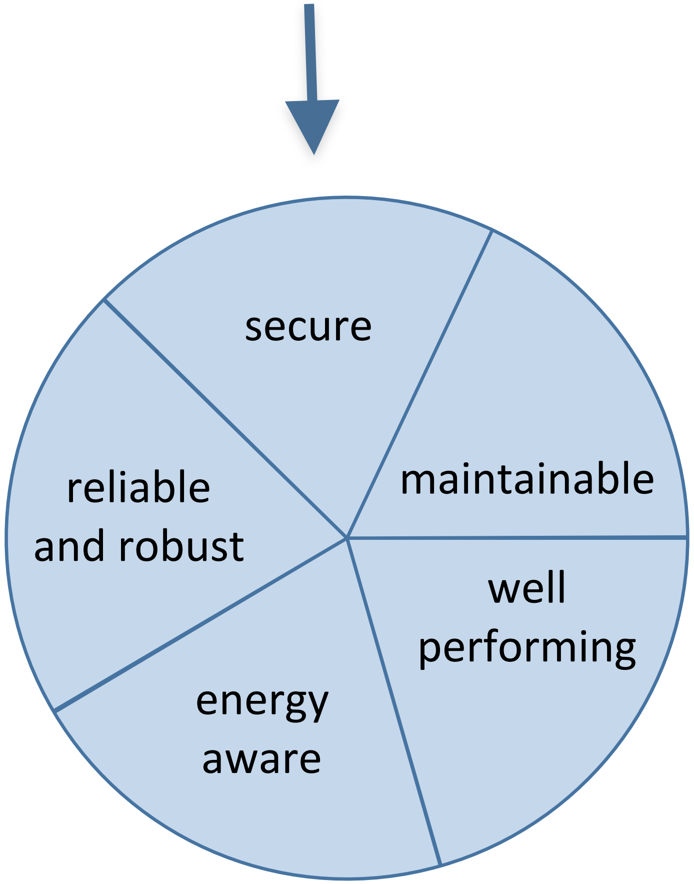
Dependable networking in a dynamic world

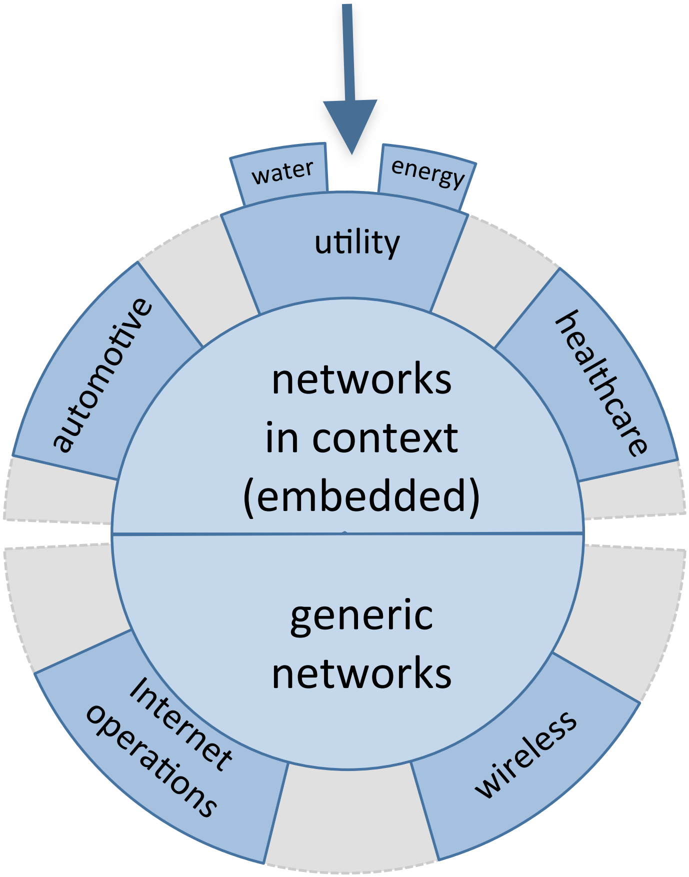




UNIVERSITY OF TWENTE.

Dependable networking in a dynamic world





Study Material

- Network Security Essentials - Applications and Standards (Fourth ed.)
  William Stallings
  Prentice Hall
  ISBN 0-13-706792-5

- Papers (see Blackboard)
- Slides (will be put on Blackboard)
- See also: http://wwwhome.cs.utwente.nl/~pras/netsec/

After following this course you can

- Critically discuss, select and compare security mechanisms in data communication protocols on the link layer (wireless), network layer (IPsec), transport layer (TLS, SSL) and application layer (web, RADIUS/ DIAMETER).
- Identify, compare and discuss several security risks and countermeasures at the networked system level (intrusion detection, scans, denial-of-service attacks and firewalls) and the web (SQL injection, Cross-site scripting).
- Set up an Intrusion Detection System (like: a honeypot) and detect and analyze intrusions. (*)

*) applies only to the students in the joint Kerckhoffs Master program

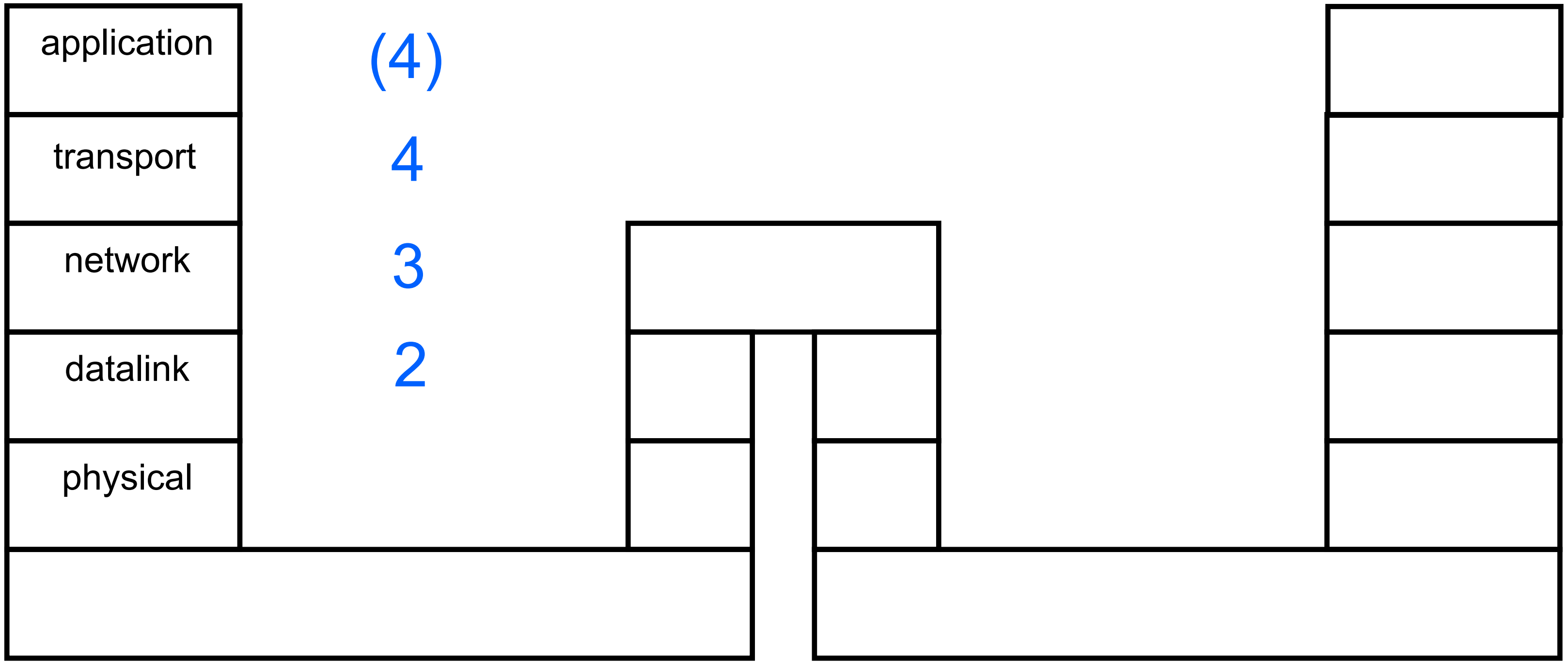
Lecture	Part	TOPIC	Presented by	Book Stallings
1		Introduction Cryptography Overview	Aiko Pras Pieter-Tjerk de Boer	Chapter 1 Chapter 2+3
2	🟦	Datalink Layer (WLAN)	Georgios Karagiannis	Papers & chapter6
3	🟦	Network Layer (IPsec)	Aiko Pras	Chapter 8
4	🟦	Transport Layer (SSL/TLS, SSH) AAA (Radius, Diameter)	Aiko Pras Georgios Karagiannis	Chapter 5 Papers
5	🟩	Web security	Ramin Sadre	Additional material
6	🟩	Attack techniques (Scans, DoS)	Ramin Sadre	Chapter 9 & 10
7	🟩	Defense techniques (NATs, Firewalls, IDS)	Anna Sperotto	Chapter 9, 10 & 11
8		Guest Lecture Exam info	Roelof Klein (Alliander) Georgios Karagiannis	

legend: 🟦 *security mechanisms in data communication protocols*

🟩 *security risks and countermeasures*

Security mechanisms in data communication protocols

LECTURE



Credits

- 4 EC: Exam (80%) plus Homework exercises (20%)
- 1 EC: Web hacking exercise
  - *All, except Kerckhoffs*
- 2 EC: Honeypot exercise
  - *Only for Kerckhoffs*

Homework exercises

- Most lectures have one or more exercises
- Submit by email to: network.security@ewi.utwente.nl
- Either as pure text or as pdf attachment; *no .doc*
- Deadline: Monday (24:00) before next lecture
- Intermediate grades will not be published
- Mandatory for all students

If you can’t access Blackboard

- Read instructions at: http://wwwhome.cs.utwente.nl/~pras/netsec/
- Ask for a normal account
  - this takes 2 to 3 weeks
- Ask also for a temporary guest account
  - send an email to: blackboard-ewi@utwente.nl (Diane Muller)
  - Include in that email:
    - first name
    - family name
    - your email address
    - as subject "request for guest account network security"
  - With a guest account you can download information, but not upload anything

Non-Kerckhoffs: Web hacking exercise

- New since 2010
- Lecture on web security
- Remote hacking exercise
  - Certified Secure (Frank van Vliet)
- Exercise can be found at: https://www.certifiedsecure.com
- Registration at that website mandatory
- Registration details should be provided via email to: network.security@ewi.utwente.nl
- Work individually
- 1 EC => 1/5 of final grade
- Deadline: 12 November 2012
- More details at later lectures

Kerckhoffs: Honeypot exercise

- Special exercise on Intrusion Detection Systems (IDS)
- Building and analyzing a honeypot
- Working in groups of 3 students
- 2 EC => 1/3 of final grade
- Deadline: end of Quarter 2 (January 2013)
- Supervisor: Anna Sperotto, Rick Hofstede

When and where

Lecture	When	Where
1	04-09-2012	Carre 3F
2	11-09-2012	Carre 3F
3	18-09-2012	Carre 3F
4	25-09-2012	Carre 3F
5	02-10-2012	Carre 3F
6	09-10-2012	Carre 3F
7	16-10-2012	Carre 3F
8	23-10-2012	Carre 3F

Some terminology

See also Chapter 1 of Stallings

Attacks, Services and Mechanisms

- *Security Attack:* Any action that compromises the security of information exchanges and systems
- *Security Service:* A service that enhances the security of information exchanges and systems. A security service makes use of one or more security mechanisms
- *Security Mechanism:* A mechanism that is designed to detect, prevent, or recover from a security attack

Kind of attacks

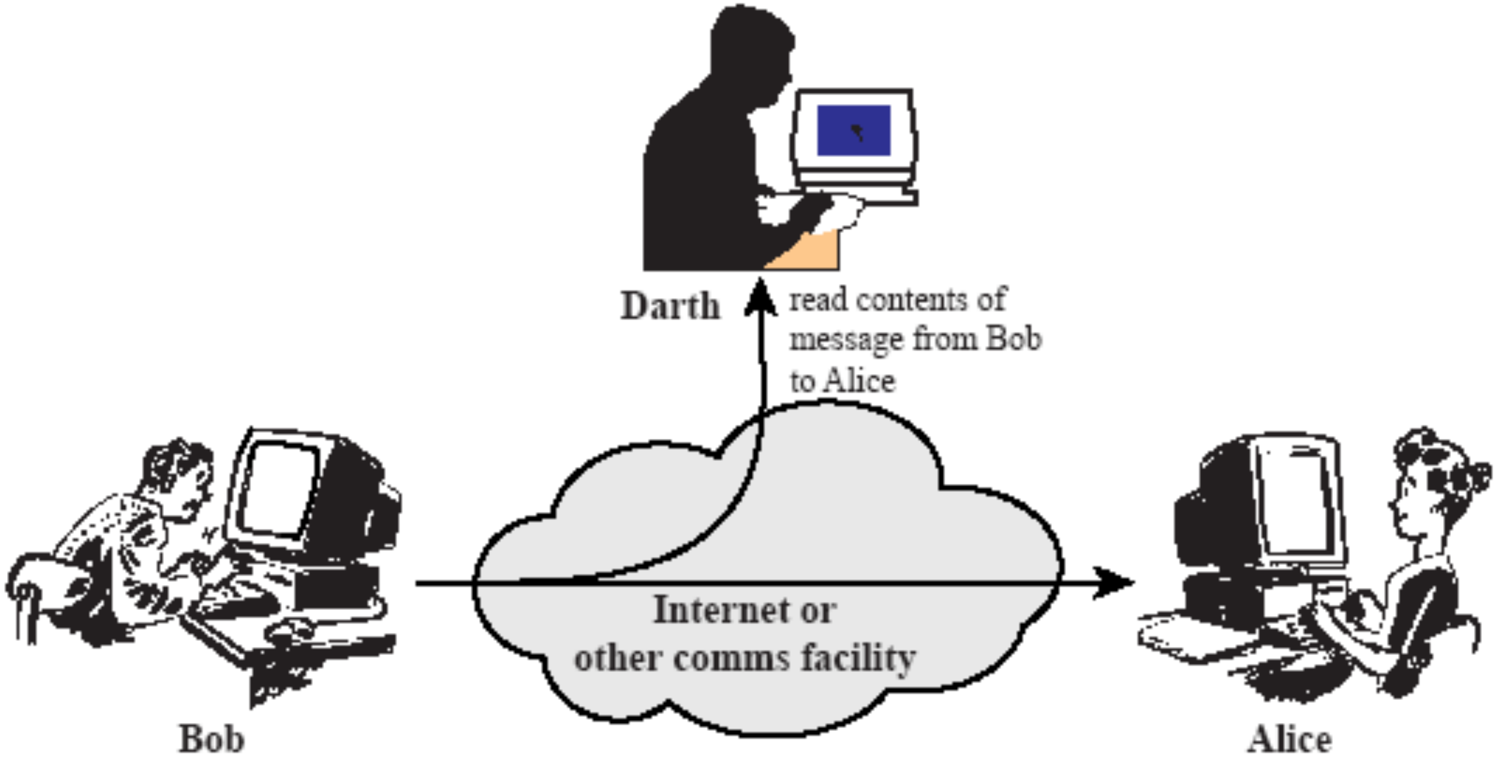
Passive attacks

- Release of message contents (disclosure)
- Traffic analysis

Active attacks

- Masquerade
- Replay
- Message modification
- Denial of Service

Release of message contents



Darth

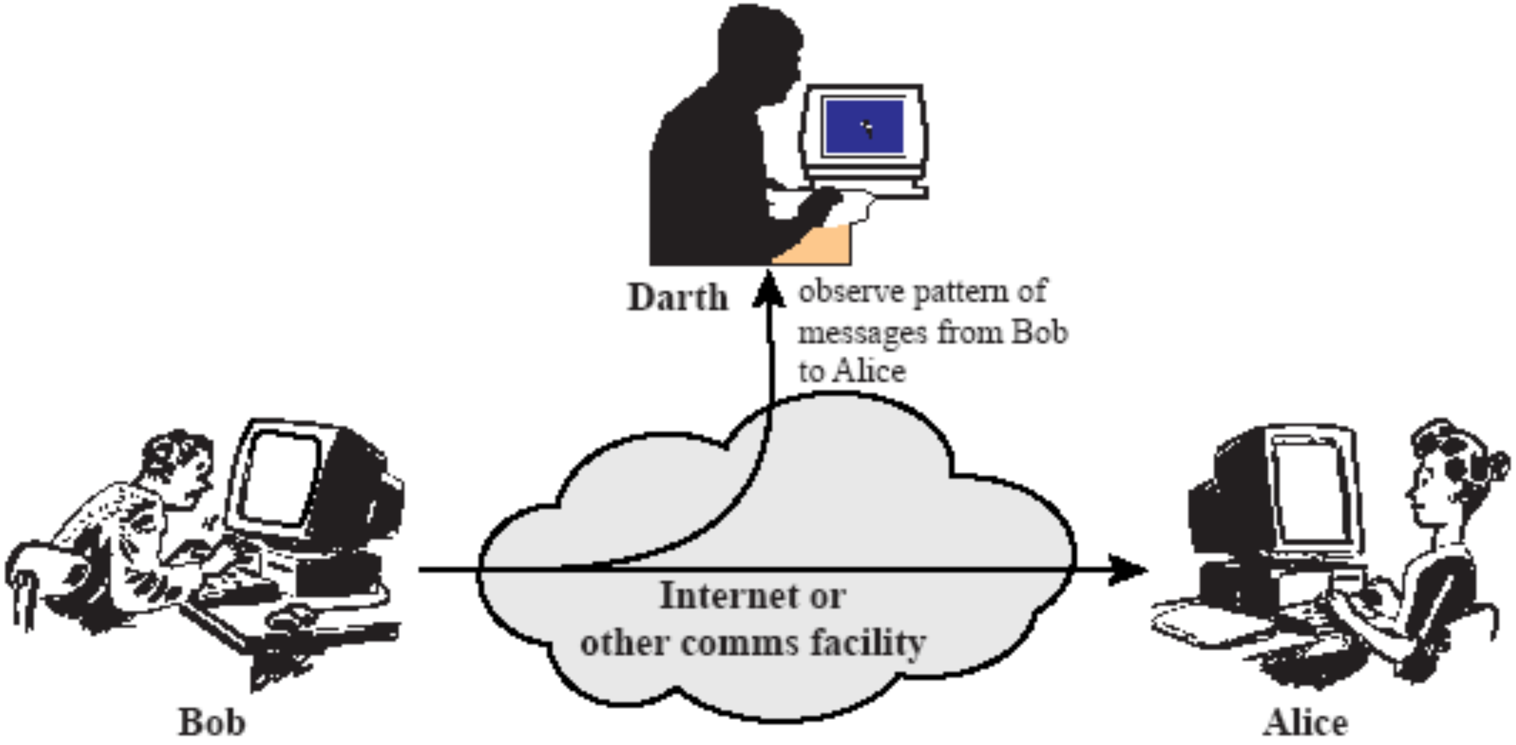
read contents of message from Bob to Alice

Internet or other comms facility

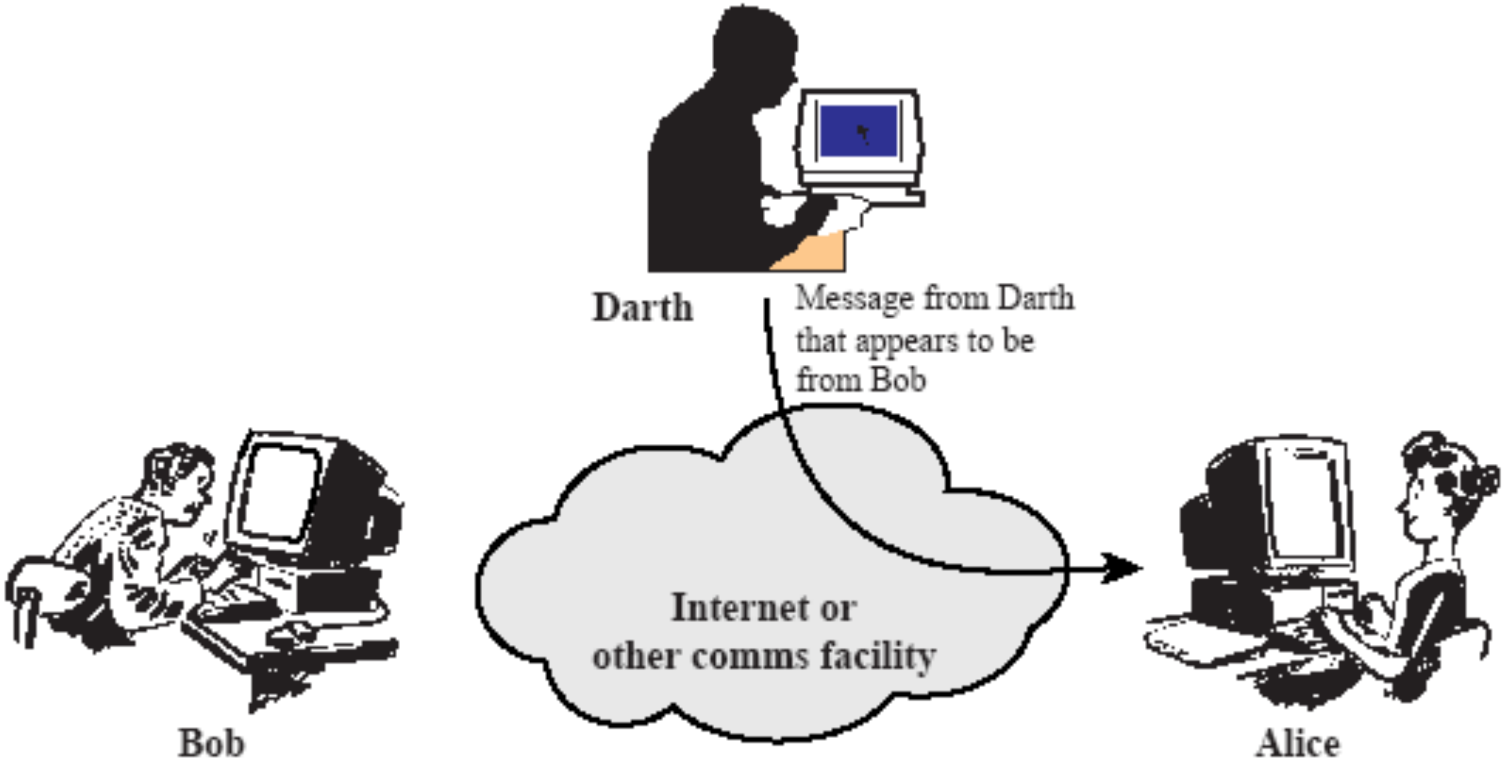
Bob

Alice

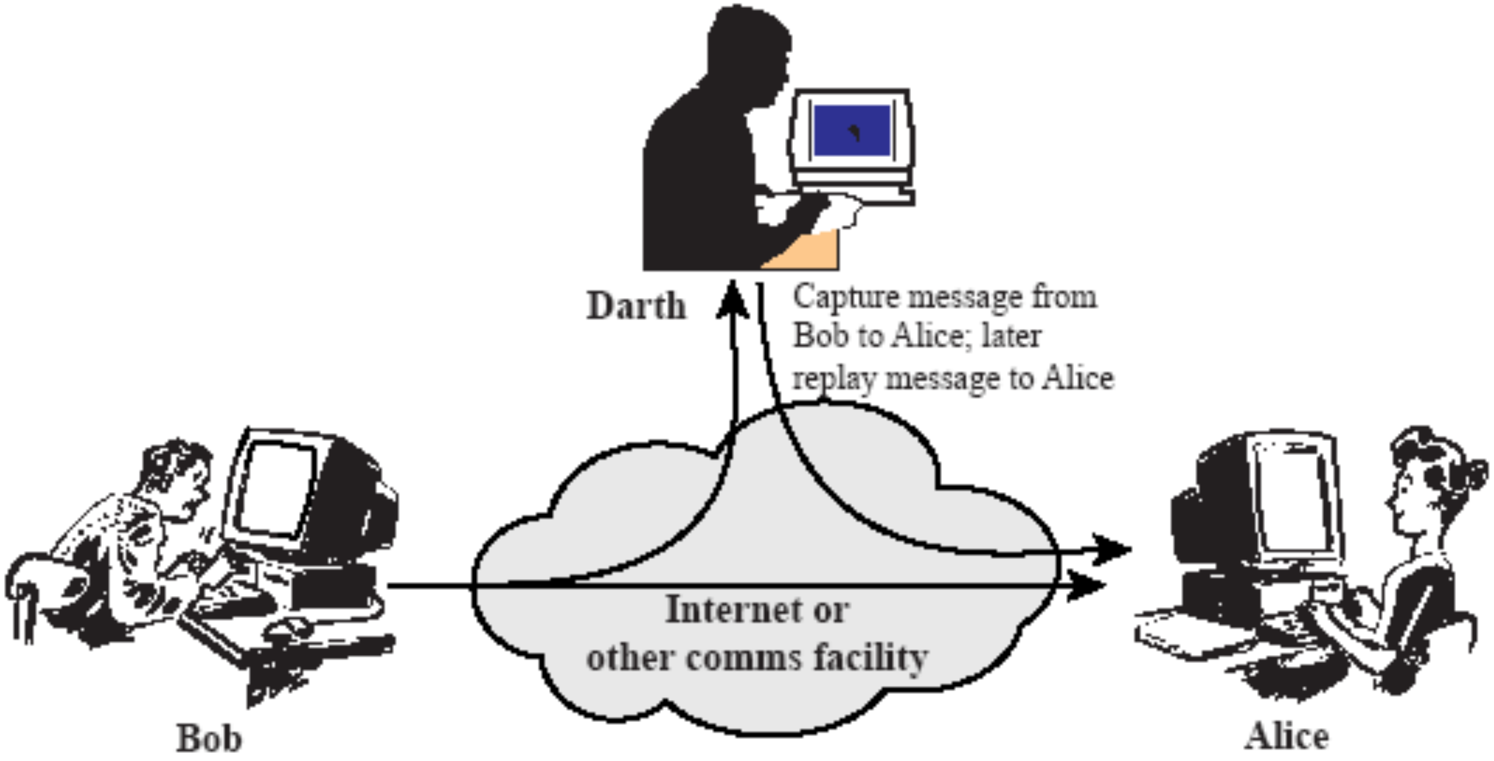
Traffic analysis


Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

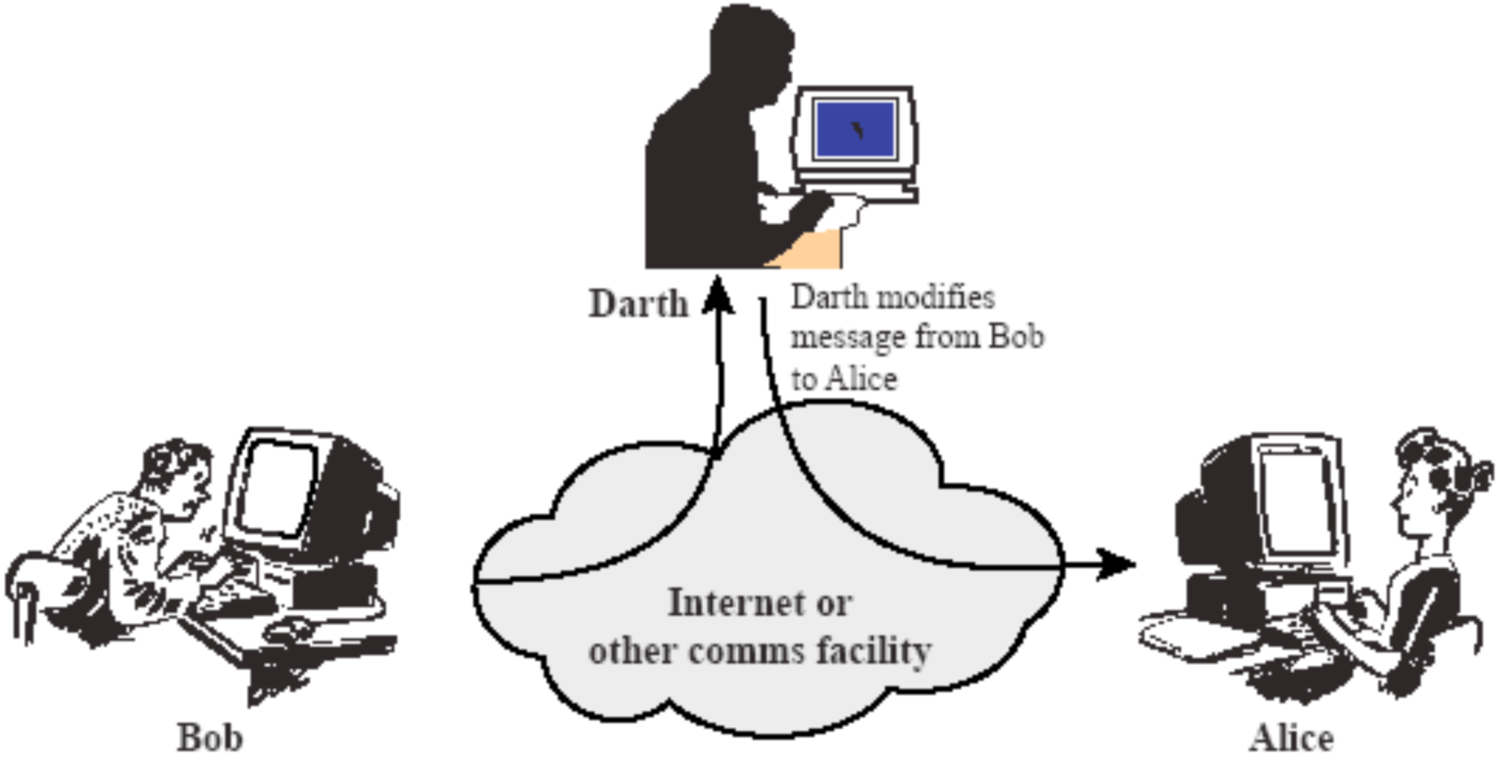
Masquerade


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

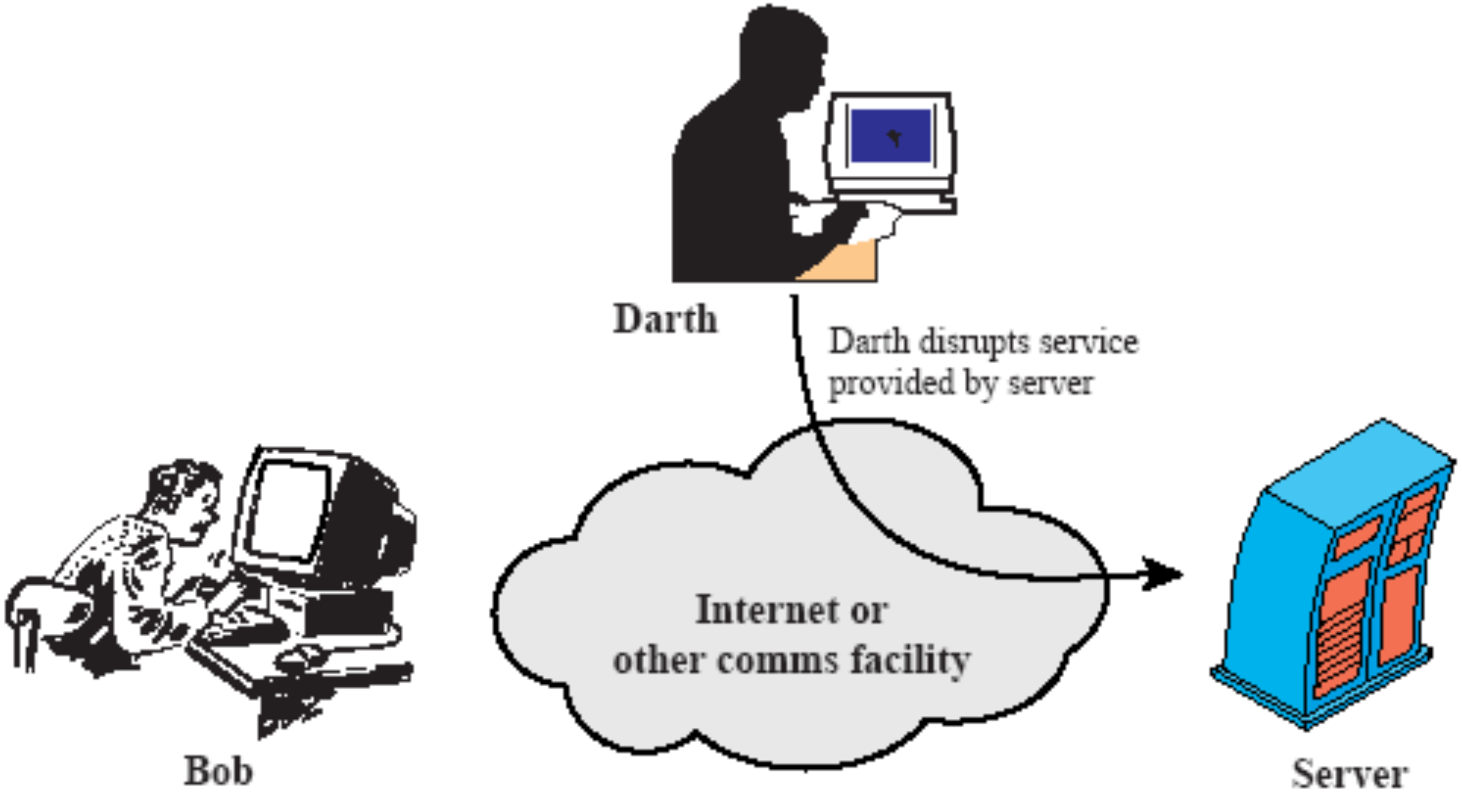
Replay


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Message modification


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Denial of Service

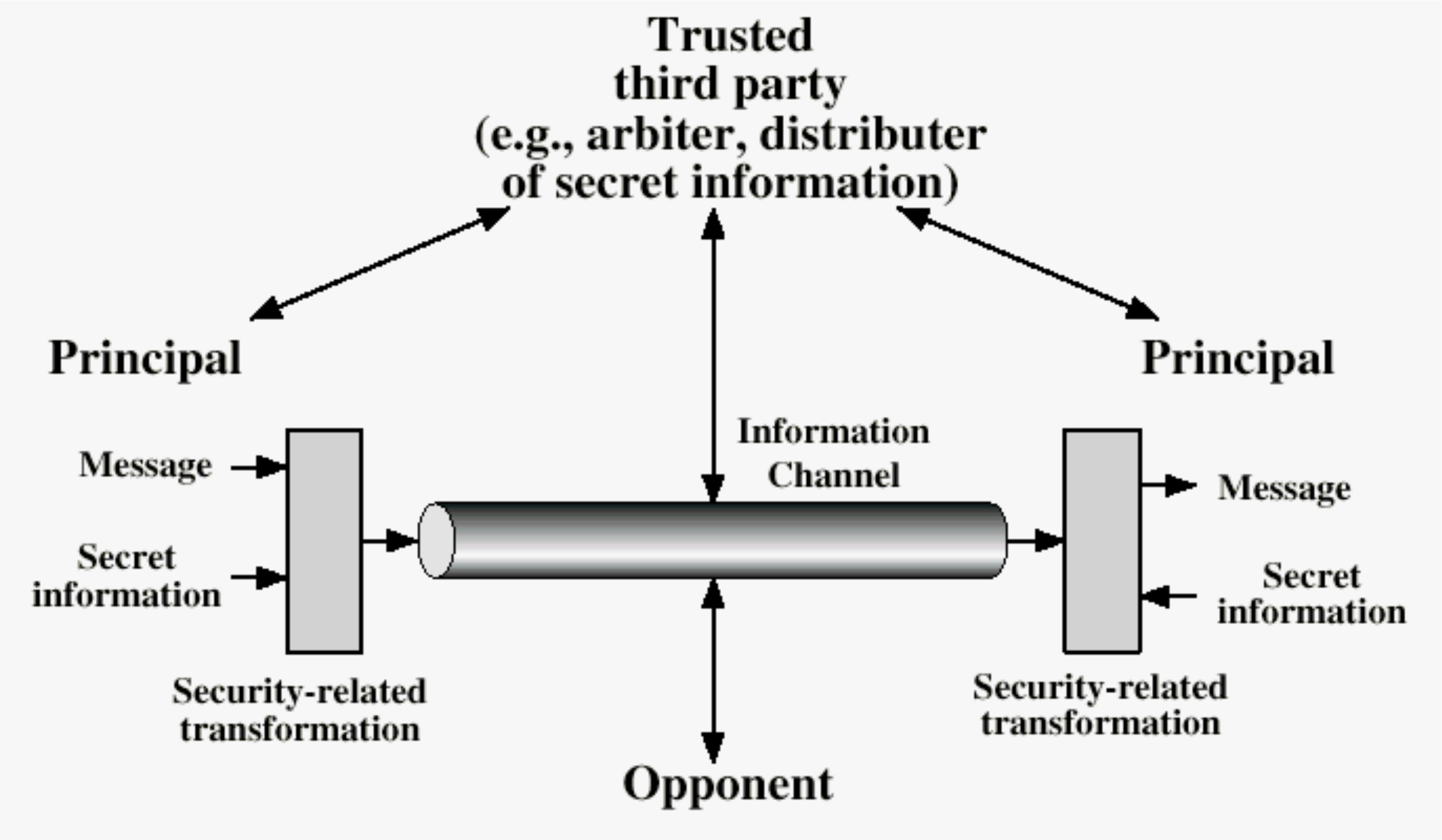

Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

Security services

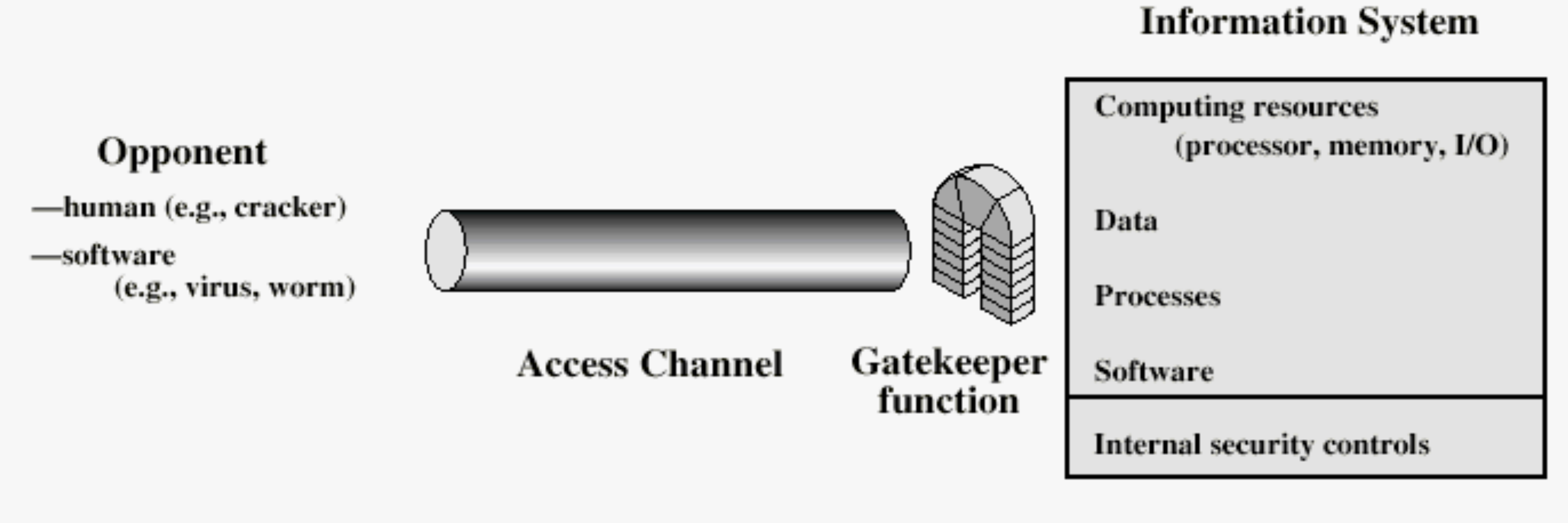
- Authentication
  - Assures communicating entity is the one that it claims to be
- Access control
- Data confidentiality
  - Protection from disclosure
  - Message contents / Traffic flow
- Data integrity
  - No modification, insertion, deletion or replay
- Nonrepudiation
  - Sender / receiver
- Availability

	Release of message contents	Traffic analysis	Masquerade	Replay	Message modification	Denial of Service
Authentication			Y			
Access control			Y			
Confidentiality (message)	Y					
Confidentiality (header)		Y				
Data integrity				Y	Y	
Nonrepudiation						
Availability						Y

Secure communication


Trusted third party (e.g., arbiter, distributer of secret information)
Principal
Principal
Message
Secret information
Information Channel
Message
Secret information
Security-related transformation
Security-related transformation
Opponent

Secure systems



Opponent

—human (e.g., cracker)

—software
(e.g., virus, worm)

Access Channel

Gatekeeper function

Information System

Computing resources
(processor, memory, I/O)

Data

Processes

Software

Internal security controls