Simon Kuznets Kharkiv National University of Economics
Information Systems Chair

Network operating system tools and information security

Oleksandr Kolgatin

Recommended Literature

1. Tanenbaum A. S. Modern Operating Systems / Andrew S. Tanenbaum, Herbert Bos. – Amsterdam: Pearcon Education, Inc, 2015. – 1101 p.

2. Russinovich M. Windows Internals. Part 1 / Mark Russinovich, David A. Solomon, Alex Ionescu. – Washington: Microsoft Press, 2012. – 726 p.

3. Russinovich M. Windows Internals. Part 2 / Mark Russinovich, David A. Solomon, Alex Ionescu. – Washington: Microsoft Press, 2012. – 645 p.

4. Neso Academy. URL: https://www.youtube.com/playlist?list=PLBlnK6fEyqRiVhbXDGLXDk_OQAeuVcp2O

5. Scott Charney. Trustworthy Computing Next / Microsoft Corporation, 2012. URL: http://download.microsoft.com/download/e/3/3/e33d31c2-e075-44ca-b4e8-dacdbc8882e7/trustworthy%20computing%20next%20white%20paper.pdf

6. Bill Gates. Trustworthy Computing. URL: https://www.wired.com/2002/01/bill-gates-trustworthy-computing/

Lecture questions:

1 Threats and Security Goals

2 User Authentication

3 Access Control

4 Anti-Virus Protection

5 Encrypting

Threats and Security Goals

Goal	Threat
Confidentiality	Exposure of data
Integrity	Tampering with data
Availability	Denial of service

Authenticity,
Accountability,
Non repudiability,
Privacy (protecting individuals from misuse of information about them)

Confidentiality

Having secret data must remain secret.

If the owner of some data has decided that these data are to be made available only to certain people and no others, the system should guarantee that release of the data to unauthorized people never occurs.

As an absolute minimum, the owner should be able to specify who can see what, and the system should enforce these specifications, which ideally should be per file.

Integrity

Unauthorized users should not be able

- to modify any data without the owner's permission.

Data modification in this context includes not only changing the data, but also removing data and adding false data.

Availability

Nobody can disturb the system to make it unusable.

Such denial-of-service attacks are increasingly common.

For example,
if a computer is an Internet server, sending a flood of requests to it may cripple it by eating up all of its CPU time just examining and discarding incoming requests. If it takes, say, 100 μ sec to process an incoming request to read a Web page, then anyone who manages to send 10,000 requests/sec can wipe it out.

Reasonable models and technology for dealing with attacks on confidentiality and integrity are available; foiling denial-of-service attacks is much harder.

Bill Gates: Trustworthy Computing

Key aspects include:

Availability: Our products should always be available when our customers need them. System outages should become a thing of the past because of a software architecture that supports redundancy and automatic recovery. Self-management should allow for service resumption without user intervention in almost every case.

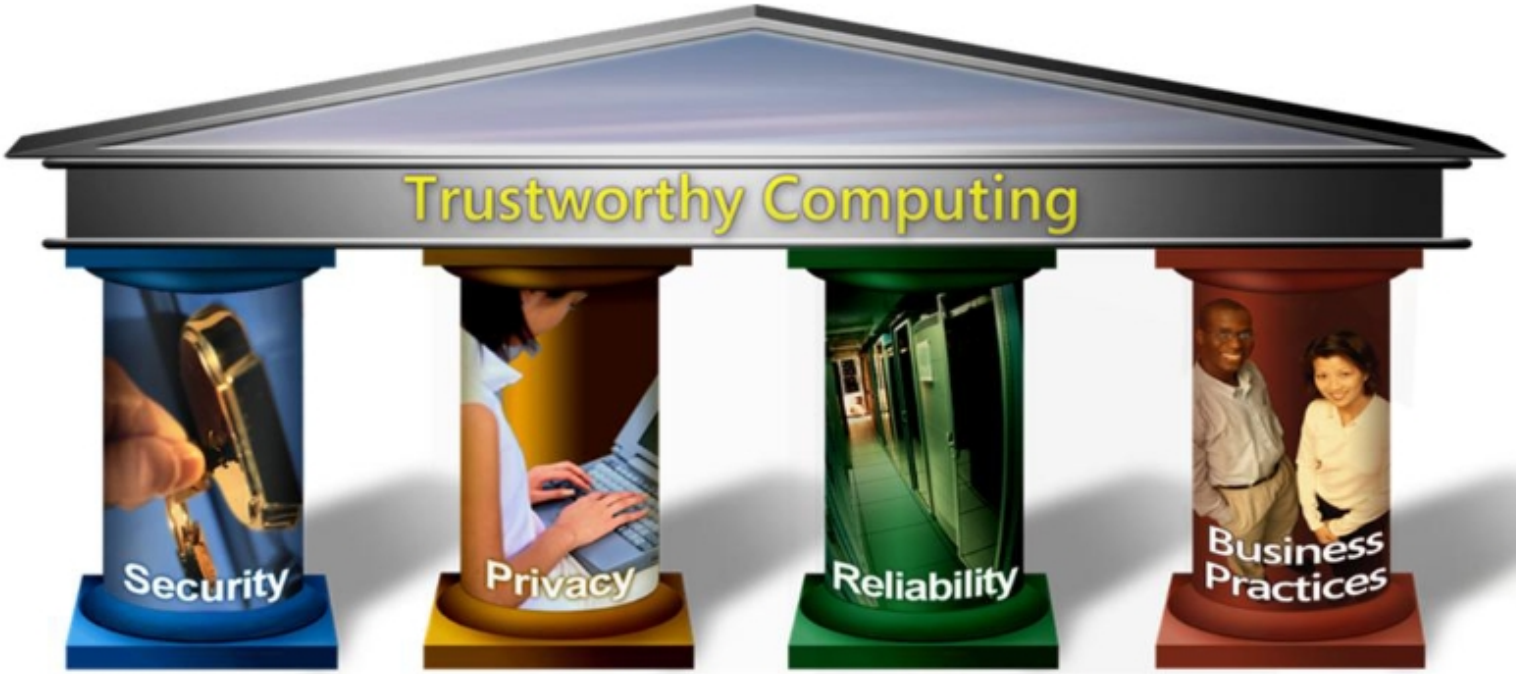
Security: The data our software and services store on behalf of our customers should be protected from harm and used or modified only in appropriate ways. Security models should be easy for developers to understand and build into their applications.

Privacy: Users should be in control of how their data is used. Policies for information use should be clear to the user. Users should be in control of when and if they receive information to make best use of their time. It should be easy for users to specify appropriate use of their information including controlling the use of email they send.

January 15, 2002, citing by

https://www.wired.com/2002/01/bill-gates-trustworthy-computing/

A graphic representation of TwC with its four pillars and early workstreams:



- Secure against attacks
- Protects confidentiality, integrity and availability of data and systems
- Manageable

- Protects from unwanted communication
- Controls for informational privacy
- Products, online services adhere to fair information principles

- Dependable, Available
- Predictable, consistent, responsive service
- Maintainable
- Resilient, works despite changes
- Recoverable, easily restored
- Proven, ready

- Commitment to customer-centric Interoperability
- Recognized industry leader, world-class partner
- Open, transparent

This picture from Scott Charney

http://download.microsoft.com/download/e/3/3/e33d31c2-e075-44ca-b4e8-dacdbc8882e7/trustworthy%20computing%20next%20white%20paper.pdf

1 User Authentication

Some Terminology

LSA – Local Security Authority – **управляющий локальной безопасностью**

SSPI – Security Support Provider Interface – **интерфейс обеспечения безопасности**

SSP – security support provider – **провайдер поддержки безопасности**

LUID – locally unique identifier – **локальный уникальный идентификатор**

SAS – secure attention sequence – **комбинация CTRL+ALT+DEL**

SID – security identifier **идентификаторы безопасности**

PT – primary token - **первичный маркер доступа**

RT – restricted token - **ограниченным маркером доступа**

ACL – access control list – **список контроля доступа**

ACE – access-control entries - **элементы контроля доступа**

DACL – discretionary access-control list – **список разграничительного контроля доступа**

SACL – system access-control list – **системный список контроля доступа**

CSP - Cryptographic Service Provider - **криптопровайдер**

Settings

Home

Find a setting

Accounts

Your info

Email & accounts

Sign-in options

Access work or school

Family & other users

Sync your settings

Sign-in options

Manage how you sign in to your device

Select a sign-in option to add, change or remove it.

Windows Hello Face
This option is currently unavailable – click to learn more

Windows Hello Fingerprint
Sign in with your fingerprint scanner (Recommended)

Windows Hello PIN
Sign in with a PIN (Recommended)

Security Key
Sign in with a physical security key

Password
Sign in with your account's password

Picture Password
Swipe and tap your favourite photo to unlock your device

Require sign-in

If you've been away, when should Windows require you to sign in again?

When PC wakes up from sleep

2 Access Control

Protection Domain

A domain is a set of (object, rights) pairs.

Each pair specifies
an object and some subset of the operations that can be performed on it. A right in this context means permission to perform one of the operations.

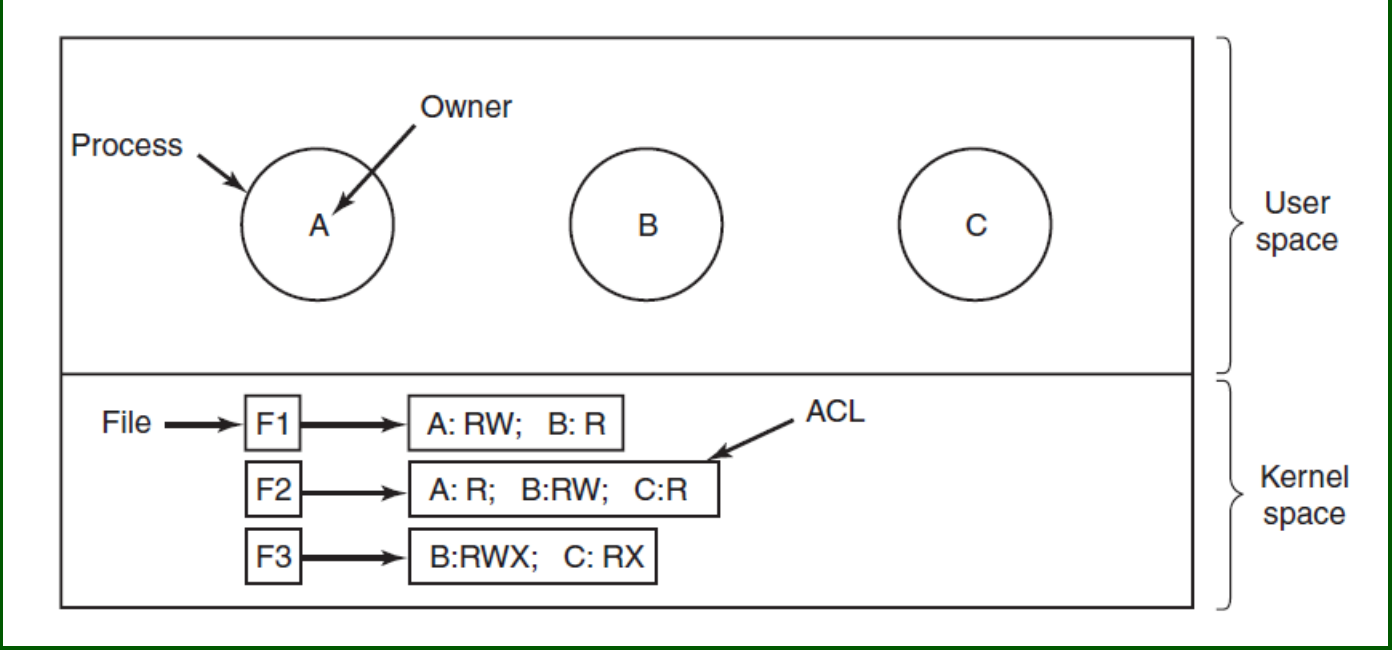
	Object							
	File1	File2	File3	File4	File5	File6	Printer1	Plotter2
Domain 1	Read	Read Write						
2			Read	Read Write Execute	Read Write		Write	
3						Read Write Execute	Write	Write

At every instant of time, each process runs in some protection domain.

Access Control Lists

A domain is a set of (object, rights) pairs.

Each pair specifies
an object and some subset of the operations that can be performed on it. A right in this context means permission to perform one of the operations.

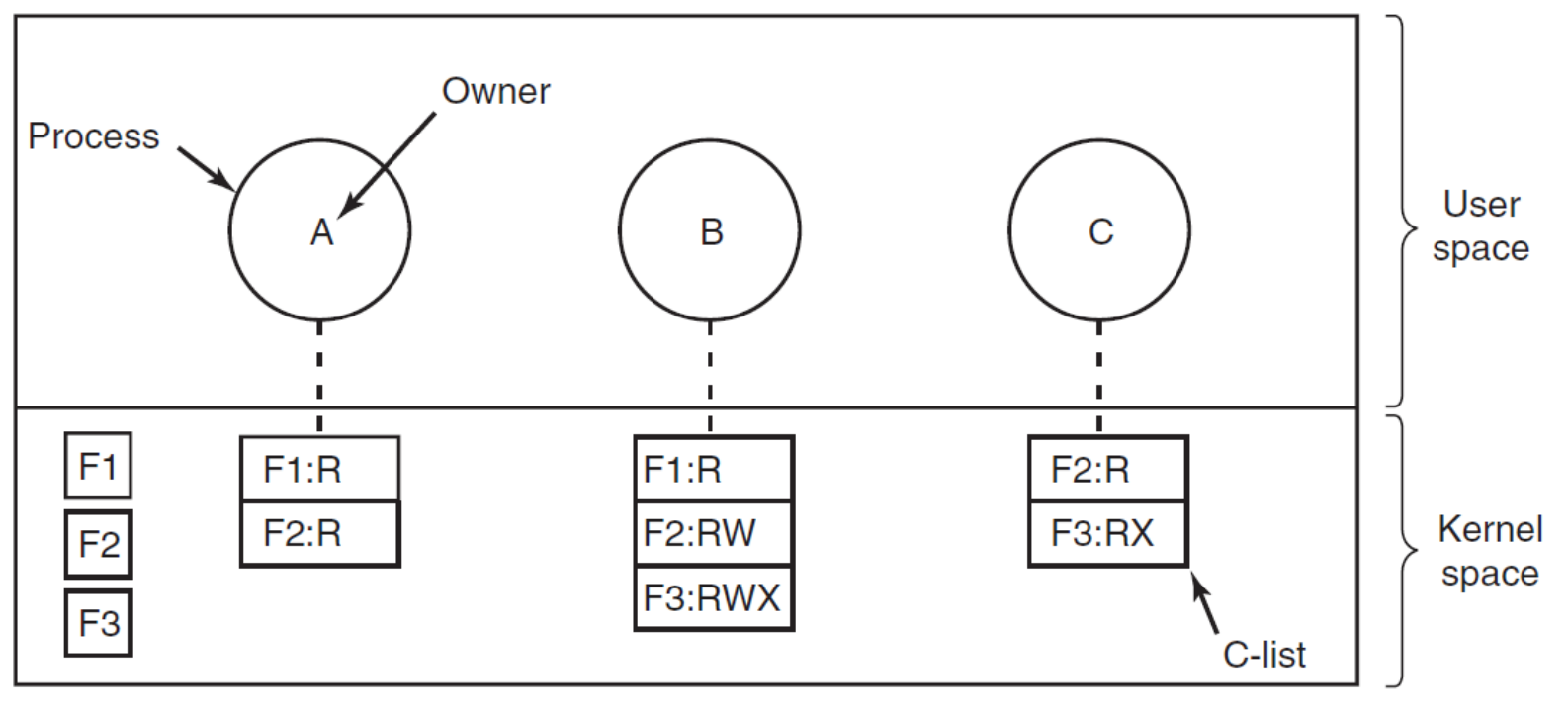


Many systems support the concept of a group of users.

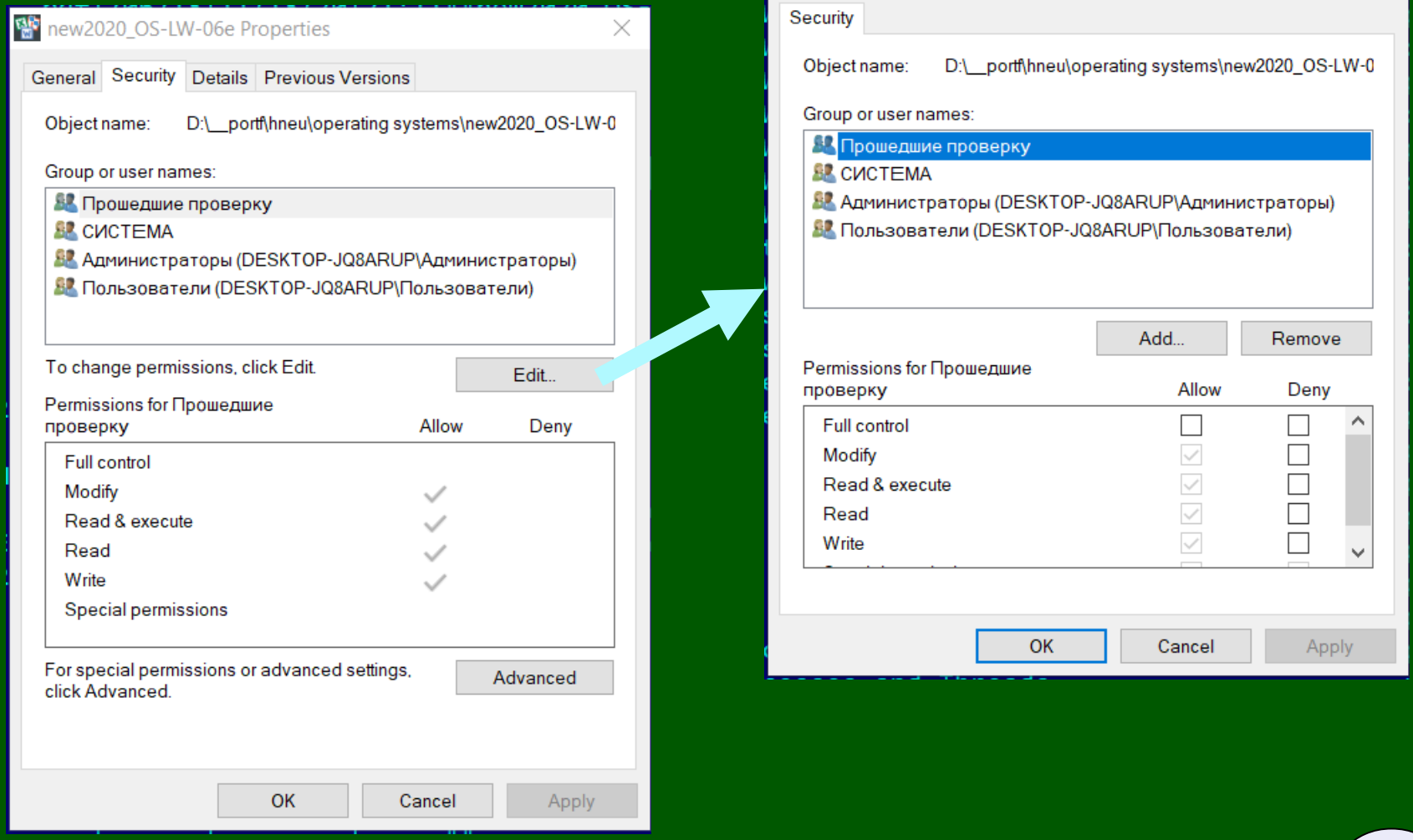
A. Tanenbaum, H. Bos

Capability List

Each capability grants the owner certain rights on a certain object.



Security File properties in NTFS



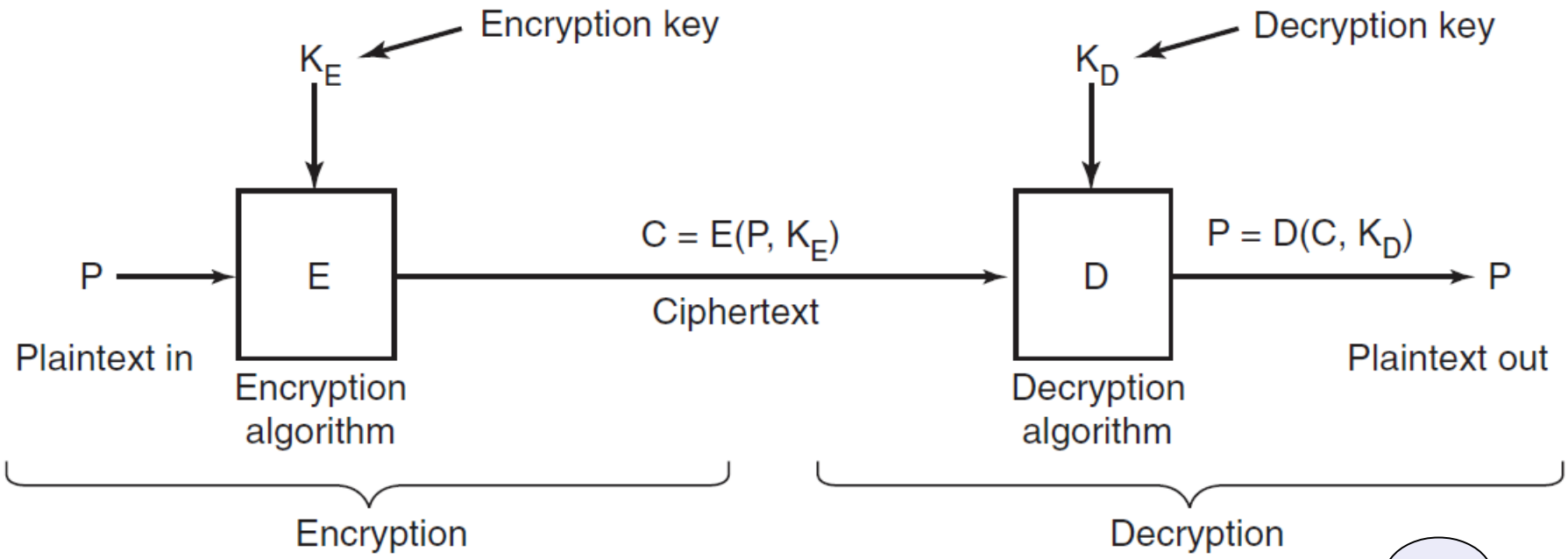
Encrypting

Main Principles

The purpose of cryptography is to take a message or file, called the **plaintext**, and encrypt it into **ciphertext** in such a way that only authorized people know how to convert it back to **plaintext**.

The encryption and decryption algorithms (functions) should always be public.

The secrecy depends on parameters to the algorithms called **keys**.



Secret Key or Symmetric-Key Cryptography

One key for encryption and decryption.

For serious security,
minimally 256-bit keys should be used, giving a search space of $2^{256} \approx 1.\ 2 \times 10^{77}$ keys. Shorter keys may thwart amateurs, but not major governments.

Secret-key systems are efficient because the amount of computation required to encrypt or decrypt a message is manageable.

Secret-key systems are now realised at hardware level and provides high performance.

For example, such algorithms (AES - Advanced Encryption Standard) is used for encrypting the disks data in Windows operating system.

But they have a big drawback:

the sender and receiver must both be in possession of the shared secret key.
They may even have to get together physically for one to give it to the other.

A. Tanenbaum, H. Bos

Public-Key Cryptography

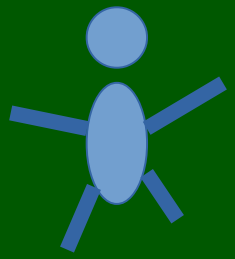
Distinct keys are used for encryption and decryption.

If an encryption key is chosen well, it is virtually impossible to discover the corresponding decryption key.

Under these circumstances, the encryption key can be made public and only the decryption key kept secret.
This keys are usually named - **Public Key** and **Private Key** respectively.

For example, a public-key system named RSA (from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977)
This system exploits the fact that multiplying really big numbers is much easier for a computer to do than factoring really big numbers, especially when all arithmetic is done using modulo arithmetic and all the numbers involved have hundreds of digits.

The main problem with public-key cryptography is that it is a thousand times slower than symmetric cryptography.



Here is my key:
01010101...10100.
Write to me confidentially!

Cryptographic Hash Function - One-Way Functions

Given f and its parameter x, computing $y = f(x)$ is
easy to do, but given only $f(x)$, finding x is computationally infeasible.

Hash function can be view as an algorithm of compressing with losses.

The most simple example of the Hash function is the check sum.

Hash function reflect the message of arbitrary length to the message of fixed length.

Digital Signatures

Digital signatures make it possible to sign emails and other digital documents in such a way that they cannot be repudiated by the sender later.

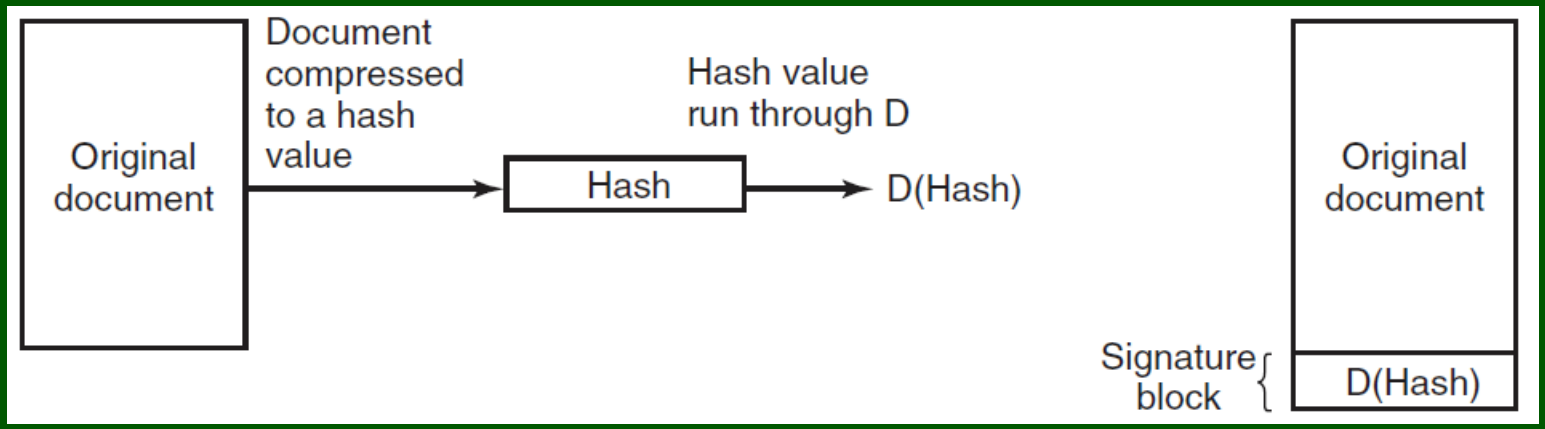
STEP 1 - sender obtain a HASH

One common way is to process the document through a one-way cryptographic hashing algorithm that is very hard to invert.

The hashing function typically produces a fixed-length result independent of the original document size.

SHA-1 (Secure Hash Algorithm) produces a 20-byte result.

Newer versions of SHA-256 and SHA-512 produce 32-byte and 64-byte results, respectively.



A. Tanenbaum, H. Bos

Digital Signatures

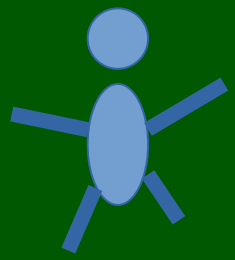
STEP 2 - **sender** obtains the document **signature block**
by transforming the HASH with asymmetric cryptography
using the **private** key

STEP 3 - **receiver** obtains the HASH independently from sender.
STEP 4 - receiver process the signature block with asymmetric cryptography
using the **public** key of this sender - he should obtain the same HASH
STEP 5 - receiver compare the HASH obtained by these two ways.

Certification Authority - Key Certification Center
(In Ukraine : Tsenter sertifikatsii kluchiv)

I like the course
"Operating Systems"

111010111110...111



A. Tanenbaum, H. Bos

Here is my Public Key
for digital sign:
01010101...10100.
1. Process my document with hash function.
2. Process my signature block with my key.
3. compare the results!

3 Anti-Virus Protection

INSIDER ATTACKS

Logic Bombs

This device is a piece of code written by one of a company's (currently employed) programmers and secretly inserted into the production system.
As long as the programmer feeds it its daily password, it is happy and does nothing. However, if the programmer is suddenly fired and physically removed from the premises without warning, the next day (or next week) the logic bomb does not get fed its daily password, so it goes off.

INSIDER ATTACKS

Back Doors

This problem is created by code inserted into the system by a system programmer to bypass some normal check.

For example, a programmer could add code to the login program to allow anyone to log in using the login name ‘‘zzzzz’’ no matter what was in the password file.

INSIDER ATTACKS

Login Spoofing

In this insider attack, the perpetrator is a legitimate user who is attempting to collect other people's passwords through a technique called login spoofing. It is typically employed in organizations with many public computers on a LAN used by multiple users.

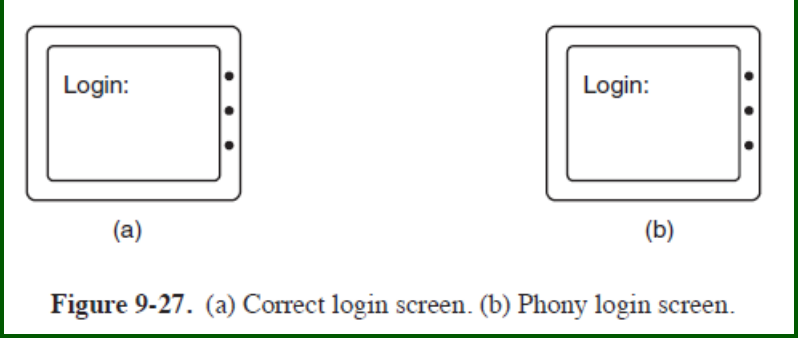


Figure 9-27. (a) Correct login screen. (b) Phony login screen.

A malicious user, Mal, writes a program to display the screen of Fig. 9-27(b). It looks amazingly like the screen of Fig. 9-27(a), except that this is not the system login program running, but a phony one written by Mal.

MALWARE

Application of malware, Trojan Horses

Viruses

- a virus is a program that can reproduce itself by attaching its code to another program, analogous to how biological viruses reproduce. The virus can also do other things in addition to reproducing itself.

Worms

- use some bugs to infect the computer

for example:

buffer overflow

THANK YOU !