

Security by harnessing the power of RouterOS

Mihai Săftoiu - MUM România
29 October 2018

Why this presentation?

What this presentation is not.

What this presentation is.

Who is in the audience ?

What is security?





Security is the consequence of the following situation:

When an unauthorized person:

- does not have the key
- cannot find/copy the key
- if the key gets found, it

cannot be used



Conclusion:

Security is the applied logic
(algorithm, way of doing etc.)
which leads to that consequence.



Defining the goal:

To have a system which even if compromised (**revealed password**) will remain secure from a functional authentication perspective.

Is that even possible?



Discussion topics:

General communication principles

RouterOS security mechanisms

Applying authentication logic on
different layers

Putting it all together



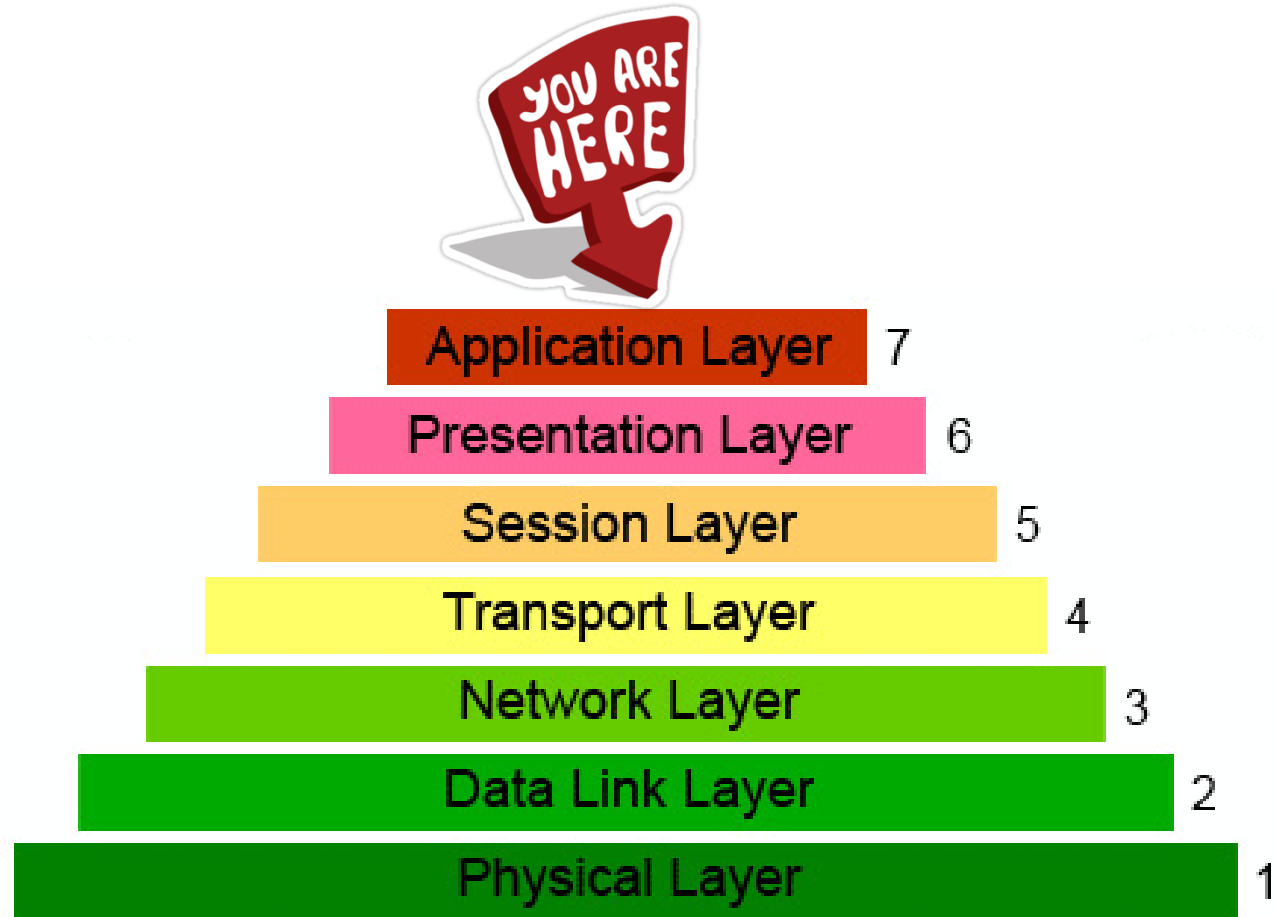
General principles

The OSI model is the basis of all inter-system communication.

Understanding the OSI model is the first step in understanding where to apply security concepts.

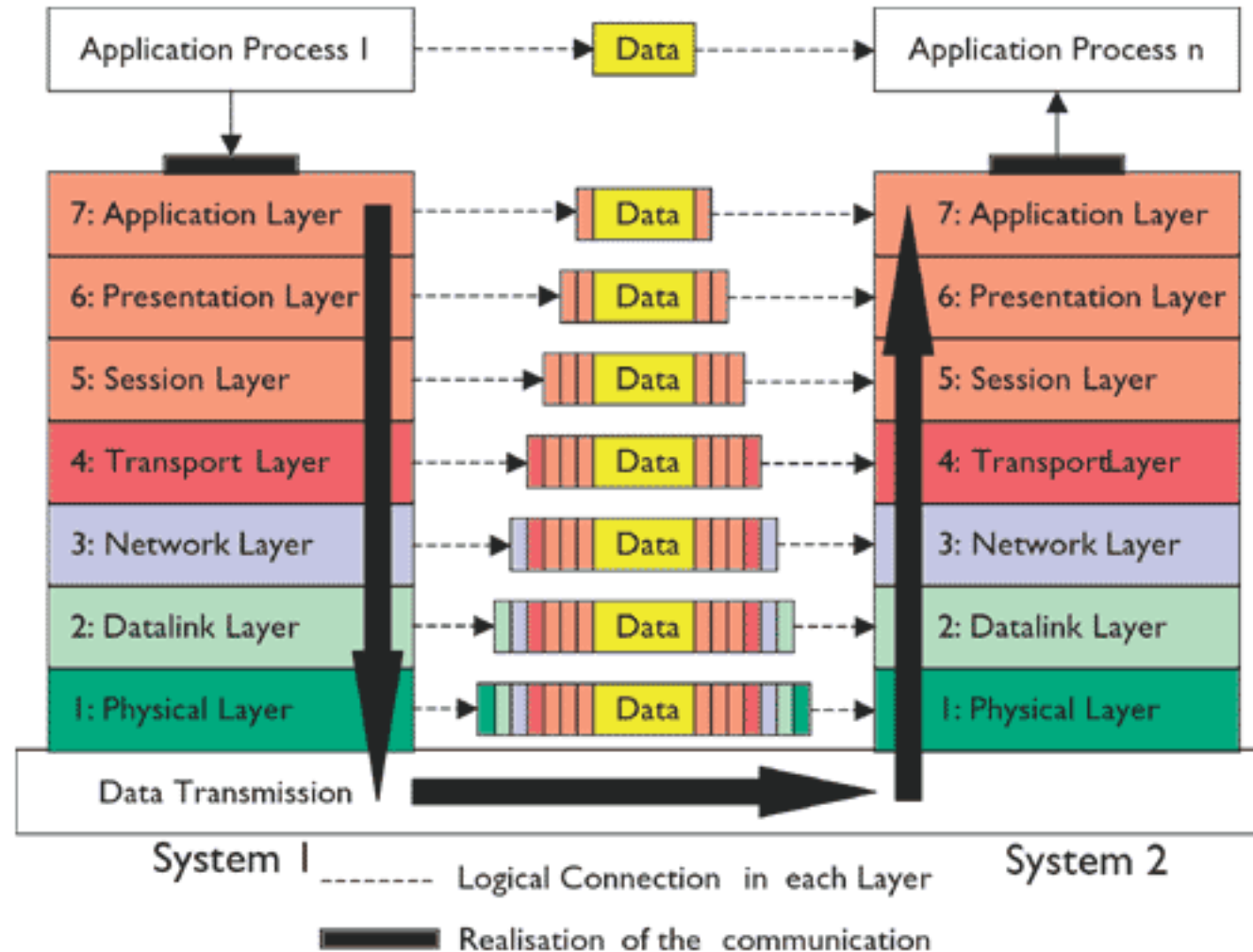


General principles - OSI



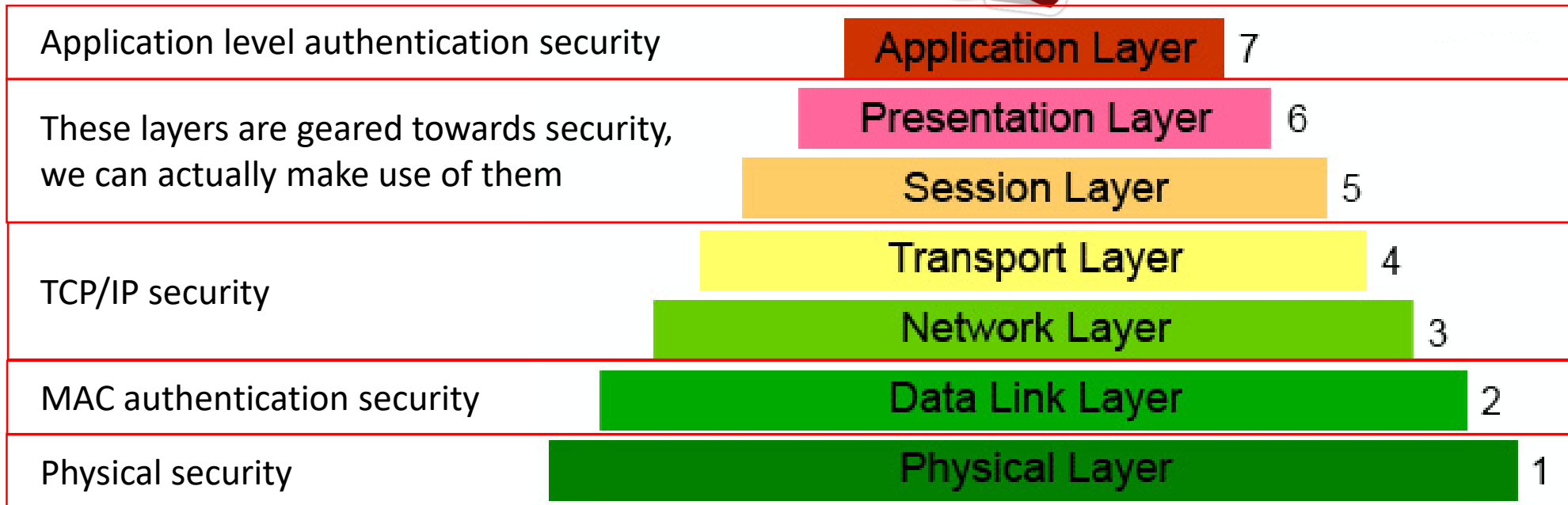


General principles - OSI



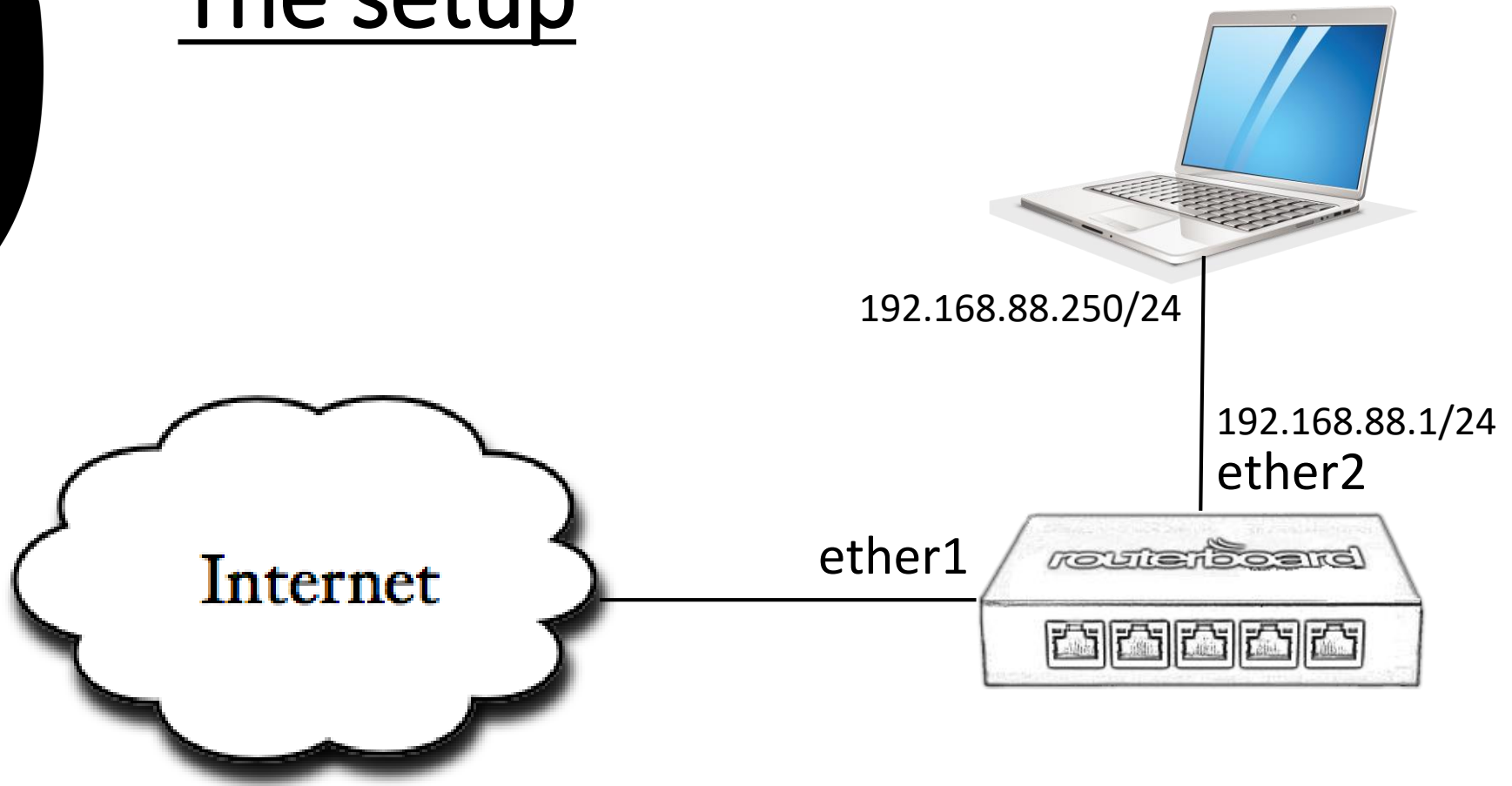


General principles - OSI





The setup





RouterOS security mechanisms

Physical security

MAC authentication security

TCP/IP security

Application level security



Physical security

1. Using secure enclosures/racks
2. Using centralized logging
3. Disabling unused interfaces
4. Protecting from factory reset



Physical security

2. Using centralized logging

Centralized logging is possible for free using The Dude

https://wiki.mikrotik.com/wiki/Manual:The_Dude_v6/Syslog



Physical security

2. Using centralized logging

The screenshot shows the Mikrotik WinBox interface. In the left sidebar, the 'System' menu item is highlighted with a red box. Below it, the 'Logging' option is also highlighted with a red box. The main window displays the 'Logging' configuration page, which includes a 'Rules' tab and a table of logging rules. The table has columns for 'Name' and 'Type'. The table contains the following data:

Name	Type
* disk	disk
* echo	echo
* memory	memory
* remote	remote

The status bar at the bottom of the window indicates '4 items'.



Physical security

2. Using centralized logging

Log Action <TheDude>

Name: TheDude

Type: remote

Remote Address: 192.168.88.5

Remote Port: 514

Src. Address:

BSD Syslog

Syslog Facility: 3 (daemon)

Syslog Severity:

OK

Cancel

Apply

Copy

Remove



Physical security

2. Using centralized logging

Logging

Rules Actions

+ - ✓ ✗ ⌵ Find

Topics	Prefix	Action
* critical		echo
* error		memory
* info		memory
info, interface	MyRouter	TheDude
warning		memory

5 items

Log Rule <info, interface>

Topics: info interface

Prefix: MyRouter

Action: TheDude

OK Cancel Apply Disable Copy Remove

enabled



Physical security

3. Disabling unused interfaces

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Interface List

Interface Interface List **Ethernet** EoIP Tunnel IP Tunnel GRE Tunnel VLAN

Power Cycle

	Name	Type	MTU	Actual MTU	L2 MTU
	ether1	Ethernet	1500	1500	1598
R	ether2	Ethernet	1500	1500	1598
X	ether3	Ethernet	1500	1500	1598
X	ether4	Ethernet	1500	1500	1598
X	ether5	Ethernet	1500	1500	1598
X	ether6	Ethernet	1500	1500	1598
X	ether7	Ethernet	1500	1500	1598
X	ether8	Ethernet	1500	1500	1598
X	ether9	Ethernet	1500	1500	1598
X	ether10	Ethernet	1500	1500	1598
	stp 1	Ethernet	1500	1500	1598



Physical security

4. Protection from hardware reset

The screenshot displays the Mikrotik WinBox interface. On the left, the 'System' menu item is highlighted with a red box. The main window shows the 'Routerboard' configuration dialog box, where the 'Settings' button is highlighted with a red box. The Routerboard dialog shows the following information:

- Routerboard
- Model: 2011UiAS-2HnD
- Serial Number: 614A05385A6A
- Firmware Type: ar9344
- Factory Firmware: 3.22
- Current Firmware: 6.43.4
- Upgrade Firmware: 6.43.4

Buttons in the Routerboard dialog include 'OK', 'Upgrade', 'Settings' (highlighted), and 'USB Power Reset'. The 'Settings' dialog on the right contains the following options:

- Auto Upgrade
- Baud Rate: 115200
- Boot Delay: 2 s
- Enter Setup On: any key
- Boot Device: nand-if-fail-then-ethernet
- CPU Frequency: 600MHz
- Boot Protocol: bootp
- Reformat Hold Button: 00:00:20
- Enable Jumper Reset
- Force Backup Booter
- Silent Boot
- Protected Routerboot (highlighted)



MAC authentication security

1. Disabling unwanted local login
2. Allowing only specific devices to access the physical ports



MAC authentication security

1. Disabling unwanted local login

The screenshot displays the Mikrotik WinBox interface with several windows open to demonstrate the steps for disabling local login:

- Interfaces:** The left sidebar shows the 'Interfaces' menu highlighted.
- Interface List:** The main window shows the 'Interface List' tab selected, with the 'Lists' button highlighted in red.
- Interface Lists:** A window showing a list of interface lists. The '+' button is highlighted in red, and the 'LocalLogin' entry is selected.
- Interface List <LocalLogin>:** A configuration window for the 'LocalLogin' list. The 'Name' field is highlighted in red and contains 'LocalLogin'. The 'Include' and 'Exclude' fields are empty.
- Comment for Interface List <LocalLogin>:** A dialog box with the text 'Mac login allowed' and 'OK'/'Cancel' buttons.



MAC authentication security

1. Disabling unwanted local login

The screenshot shows a network configuration interface with a tabbed menu at the top including 'Interface', 'Interface List', 'Ethernet', 'EoIP Tunnel', 'IP Tunnel', 'GRE Tunnel', 'VLAN', 'VRRP', and 'Bonding'. The 'Interface List' tab is active, displaying a table with two columns: 'List' and 'Interface'. The table contains one entry: 'LocalLogin' under 'List' and 'ether2' under 'Interface'. A red box highlights the '+' icon in the toolbar above the table.

An 'Interface List Member' dialog box is open, showing 'List: LocalLogin' and 'Interface: ether2' in dropdown menus. A red box highlights these two dropdowns. The dialog also features buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'. At the bottom of the dialog, the status 'enabled' is displayed.



MAC authentication security

1. Disabling unwanted local login

The screenshot shows a network management application with a sidebar menu on the left. The 'Tools' menu item is highlighted with a red box. The 'MAC Server' option is selected in the main menu, also highlighted with a red box. The main window displays a table of MAC servers with columns for 'Interface', 'Src. Address', and 'Uptime'. Two configuration windows are open: 'MAC Telnet Server' and 'MAC WinBox Server'. Both windows have 'Allowed Interface List' set to 'LocalLogin', which is highlighted with a red box. The 'MAC Telnet Server' window also shows 'OK', 'Cancel', and 'Apply' buttons. The 'MAC WinBox Server' window also shows 'OK', 'Cancel', and 'Apply' buttons. The bottom right corner of the application window shows the number '26'.



MAC authentication security

2. Allowing only trusted devices

The screenshot displays the Mikrotik WinBox configuration interface. On the left, the 'IP' menu item is highlighted with a red box. The main configuration area shows the 'ARP List' configuration page. The 'ARP List' table contains one entry:

	IP Address	MAC Address	Interface
C	192.168.88.250	F0:1F:AF:32:19:99	ether2

Below the table, a dialog box titled 'ARP <192.168.88.250>' is open. The 'IP Address' field is set to '192.168.88.250', the 'MAC Address' field is set to 'F0:1F:AF:32:19:99', and the 'Interface' field is set to 'ether2'. These three fields are highlighted with a red box. The dialog also includes 'OK', 'Cancel', 'Apply', and 'Disable' buttons, and a 'Published' checkbox.



MAC authentication security

2. Allowing only trusted devices

The screenshot displays a network configuration tool with a sidebar on the left and a main configuration area on the right. The sidebar includes categories like Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, and Tools. The 'Interfaces' category is selected, showing a list of interfaces: ether1, ether2, ether3, ether4, ether5, ether6, ether7, ether8, ether9, ether10, sfp1, and wlan1. The 'ether2' interface is selected and highlighted. The main configuration area shows the 'Interface <ether2>' configuration page, with the 'General' tab active. The configuration fields include Name (ether2), Type (Ethernet), MTU (1500), Actual MTU (1500), L2 MTU (1598), Max L2 MTU (4074), and MAC Address (E4:8D:8C:23:5A:CA). The ARP mode is set to 'reply-only', which is highlighted with a red box. The interface list table is as follows:

	Name	Type
	ether1	Eth
R	ether2	Eth
X	ether3	Eth
X	ether4	Eth
X	ether5	Eth
X	ether6	Eth
X	ether7	Eth
X	ether8	Eth
X	ether9	Eth
X	ether10	Eth
	sfp1	Eth
X	wlan1	Wif



TCP/IP Security

Practices found on the Internet usually employ techniques such as:

- IP ACL trust relationship (firewall)
- filtering invalid packet sources
- some form of port knocking technique



TCP/IP Security

IP ACL trust relationship (firewall)

- the most common layer 3 method
- easy to configure
- useful when used with static IPs
- easy to bypass using spoofing
- what to do when in another city?



TCP/IP Security

Filtering invalid packet sources

- also common in modern firewalls
- a skilled attacker will not send invalid packets and will not get blacklisted



TCP/IP Security

Some form of port knocking

- employs a set of ports which are “knocked” which then enables the login to the device
- the ports used can also be sniffed or discovered by specialized tools



Application layer security

1. Disabling unwanted services
2. Using built-in ACL mechanism and changing default ports

P.S. We'll get back to TCP/IP soon



Application layer security

1. Disabling services (IP -> Services)

	Name	Port	Available From	Certificate
X	api	8728		
X	api-ssl	8729		none
X	ftp	21		
X	ssh	22		
X	telnet	23		
	winbox	8291		
X	www	80		
X	www-ssl	443		none

8 items (7 selected)



Application layer security

2. ACL and default port change

IP Service List

	Name	Port	A
X	api	8728	
X	api-ssl	8729	
X	ftp	21	
X	ssh	22	
X	telnet	23	
	winbox	8291	
X	www	80	
X	www-ssl	443	

8 items (1 selected)

IP Service <winbox>

Name: winbox

Port: 18291

Available From: 192.168.88.0/24

8.8.8.8

enabled

OK
Cancel
Apply
Disable



Reiterating the goal:

To have a system which even if compromised (**revealed password**) will remain secure from a functional authentication perspective.

Is that even possible?



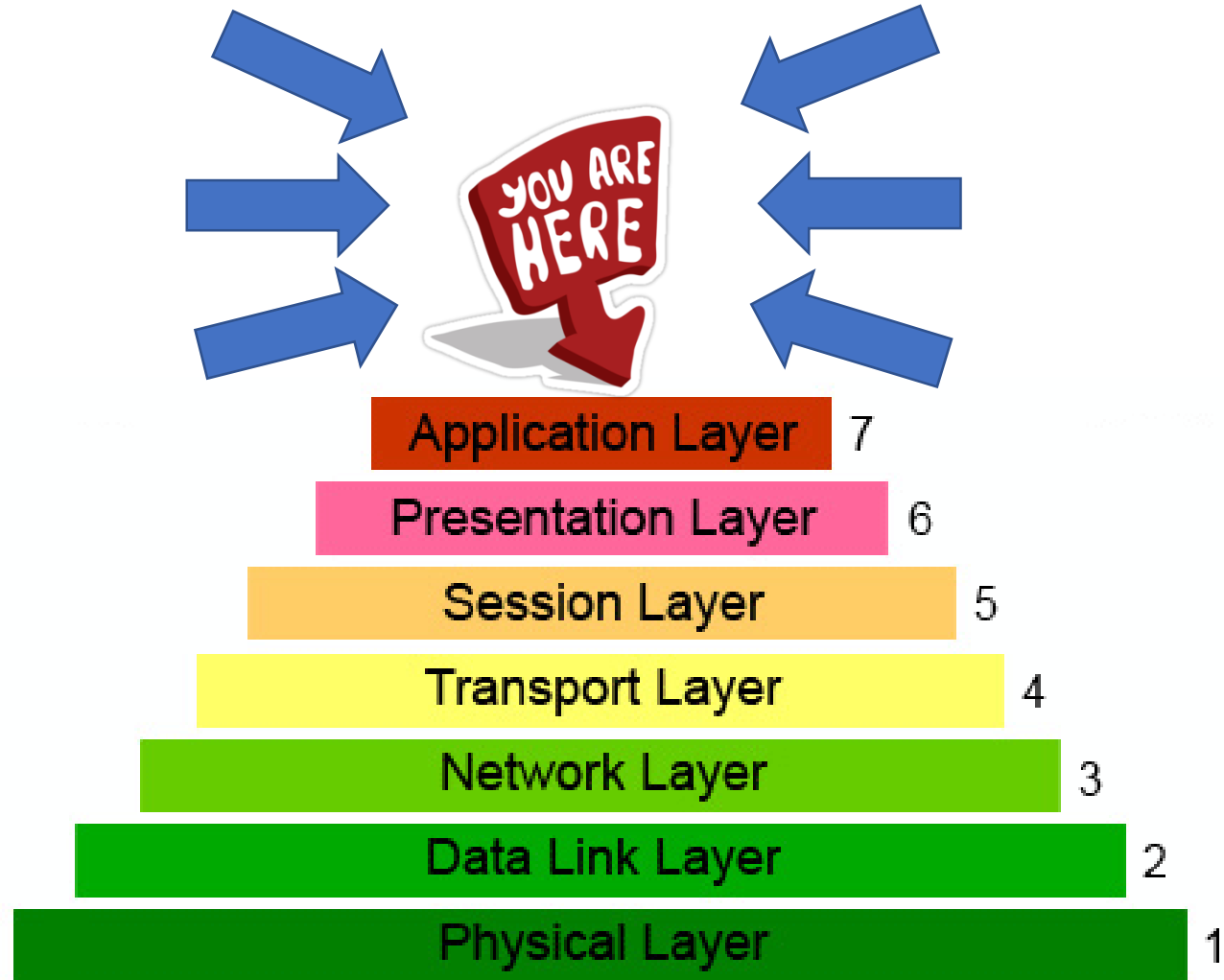
What is the problem with these setups?



Are there any improvements we
can make?



The most important security layer





How can this 8-th layer actually
come into play ?



Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

The word steganography combines the Greek words **steganos** (στεγανός), meaning "covered, concealed, or protected", and **graphein** (γράφειν) meaning "writing".

source: Wikipedia



My birthday is: 01 February 1983

Let's change the date format: 01.02.1983

Let's turn it into a numerical code:

01021983



To express the same idea into a different format we could say: *“At 01 hours and 02 minutes you should ping the equipment 47 times in order to access it and then 111 times.”*

01021983

IP header 20B, ICMP header 8B
 $47 - 20 - 8 = \mathbf{19}$, $111 - 20 - 8 = \mathbf{83}$



01021983

Let's read the true logic decoded:

- protocol 1
- 2-nd packet relevant
- length 19, encrypted length 83



Protocol 1: ICMP, echo request (ping)

2-nd packet relevant: the MikroTik router will only process the odd packets

length 19, encrypted length 83: the MikroTik router will respond in a receptive manner if two sets of data are involved: unencrypted 19 bytes, the second sent over encryption 83 bytes



So for a highly secured device the algorithm is as follows:

- drop icmp echo request of size 19 (True size: $19 + 20 + 8 = 47$) and add source to trusted1
- allow encrypted connections from trusted1
- drop icmp echo request of size 83 over encryption (True size: $83 + 20 + 8 = 111$) and add source to trusted2
- allow to port 8291 encrypted from trusted2
- allow discovery over encryption (optional)
- drop everything else



Setting up the authentication system:

1. Set up a PPTP server (you can use any type of more advanced tunneling server SSTP with SSL, L2TP over IPSec etc.)
2. Set up a PPTP user and password
3. Set up the firewall



PPTP server

PPP

Interface | PPPoE Servers | Secrets | Profiles | Active Connections | L2

PPP Scanner | PPTP Server

Name	Type	Actual MTU	L2 MTU
------	------	------------	--------

PPTP Server

Enabled

Max MTU: 1450

Max MRU: 1450

MRRU: [dropdown]

Keepalive Timeout: 30

Default Profile: default-encryption

Authentication: mschap2 mschap1
 chap pap

OK
Cancel
Apply



PPTP user and password

PPP

Switch

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

LCD

MetaROUTER

Partition

Make Supout.tif

PPP

Interface PPPoE Servers **Secrets** Profiles Ac

+ - ✓ ✗ [icon] [icon] PPP Authent

Name	Password	Service	Caller ID
0 items			

New PPP Secret

Name: user1

Password: password1

Service: pptp

Caller ID:

Profile: default-encryption

Local Address: 192.168.88.2

Remote Address: 192.168.88.3

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

enabled



Firewall rules

```
Terminal
[admin@MikroTik] > ip firewall filter export
# jan/02/1970 05:47:52 by RouterOS 6.43.4
# software id = N53Q-VEGT
#
# model = 2011UiAS-2HnD
# serial number = 614A05385A6A
/ip firewall filter
add action=add-src-to-address-list address-list=Trusted1 address-list-timeout=\
  lh chain=input connection-bytes=47 icmp-options=8:0-255 nth=2,1 protocol=\
  icmp
add action=accept chain=input dst-port=1723 protocol=tcp src-address-list=\
  Trusted1
add action=accept chain=input protocol=gre src-address-list=Trusted1
add action=add-src-to-address-list address-list=Trusted2 address-list-timeout=\
  lh chain=input connection-bytes=111 icmp-options=8:0-255 in-interface=\
  all-ppp nth=2,1 protocol=icmp
add action=accept chain=input dst-port=8291 protocol=tcp src-address-list=\
  Trusted2
add action=accept chain=input dst-port=20561 protocol=udp src-address-list=\
  Trusted2
add action=drop chain=input
[admin@MikroTik] > █
```



Firewall rules applied

```
Terminal
[admin@MikroTik] > ip firewall filter export
# jan/02/1970 05:47:52 by RouterOS 6.43.4
# software id = N53Q-VEGT
#
# model = 2011UiAS-2HnD
# serial number = 614A05385A6A
/ip firewall filter
add action=add-src-to-address-list address-list=Trusted1 address-list-timeout=\
lh chain=input connection-bytes=47 icmp-options=8:0-255 nth=2,1 protocol=\
icmp
add action=accept chain=input dst-port=1723 protocol=tcp src-address-list=\
Trusted1
add action=accept chain=input protocol=gre src-address-list=Trusted1
add action=add-src-to-address-list address-list=Trusted2 address-list-timeout=\
lh chain=input connection-bytes=111 icmp-options=8:0-255 in-interface=\
all-ppp nth=2,1 protocol=icmp
add action=accept chain=input dst-port=8291 protocol=tcp src-address-list=\
Trusted2
add action=accept chain=input dst-port=20561 protocol=udp src-address-list=\
Trusted2
add action=drop chain=input
[admin@MikroTik] >
```

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

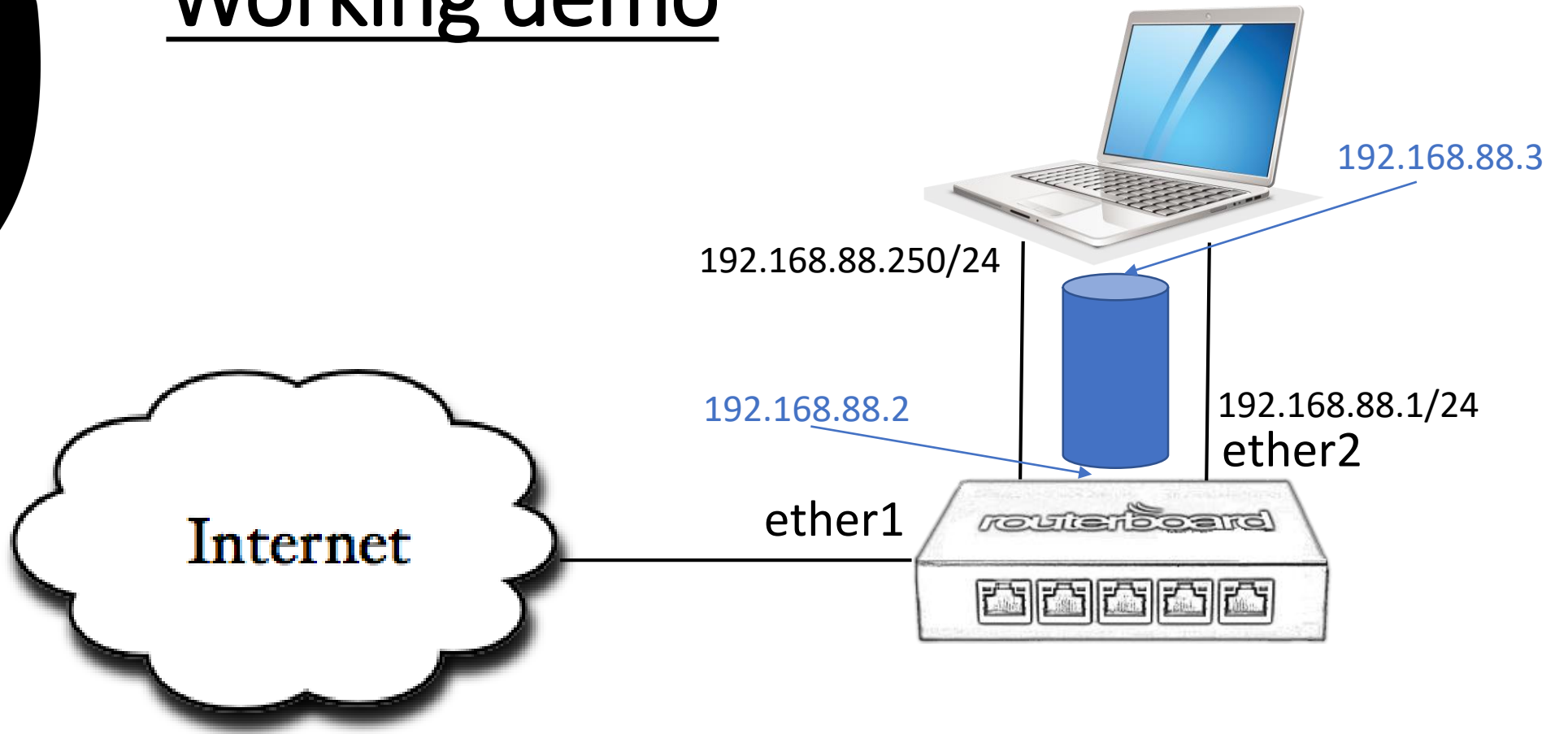
+ - ✓ ✗ 🗑️ 🔍 00 Reset Counters 00 Reset All Counters Find all

#	Action	Chain	Protocol	Dst. Port	In. Interface	Src. Address List	Connection Bytes	ICMP Options/...	Nth/Every	Nth/Package	Address List	Timeout	Bytes	Packets
0	add src to address list	input	1 (icmp)				47	8 (echo request)	2	1	Trusted1	01:00:00	0 B	0
1	✓ accept	input	6 (tcp)	1723		Trusted1							0 B	0
2	✓ accept	input	47 (gre)			Trusted1							0 B	0
3	add src to address list	input	1 (icmp)		all ppp		111	8 (echo request)	2	1	Trusted2	01:00:00	0 B	0
4	✓ accept	input	6 (tcp)	8291		Trusted2							0 B	0
5	✓ accept	input	17 (udp)	20561		Trusted2							0 B	0
6	✗ drop	input											1367.2 KB	19 359

7 items 51



Working demo





Final conclusions

A subtle but important difference in logic makes the difference in security.

By making use of this technique, a system which has a compromised admin password will remain unaccessible by attackers.

Questions?