Cipher 5

Lexi Pimenidis

iDev GmbH

Capture The Flag

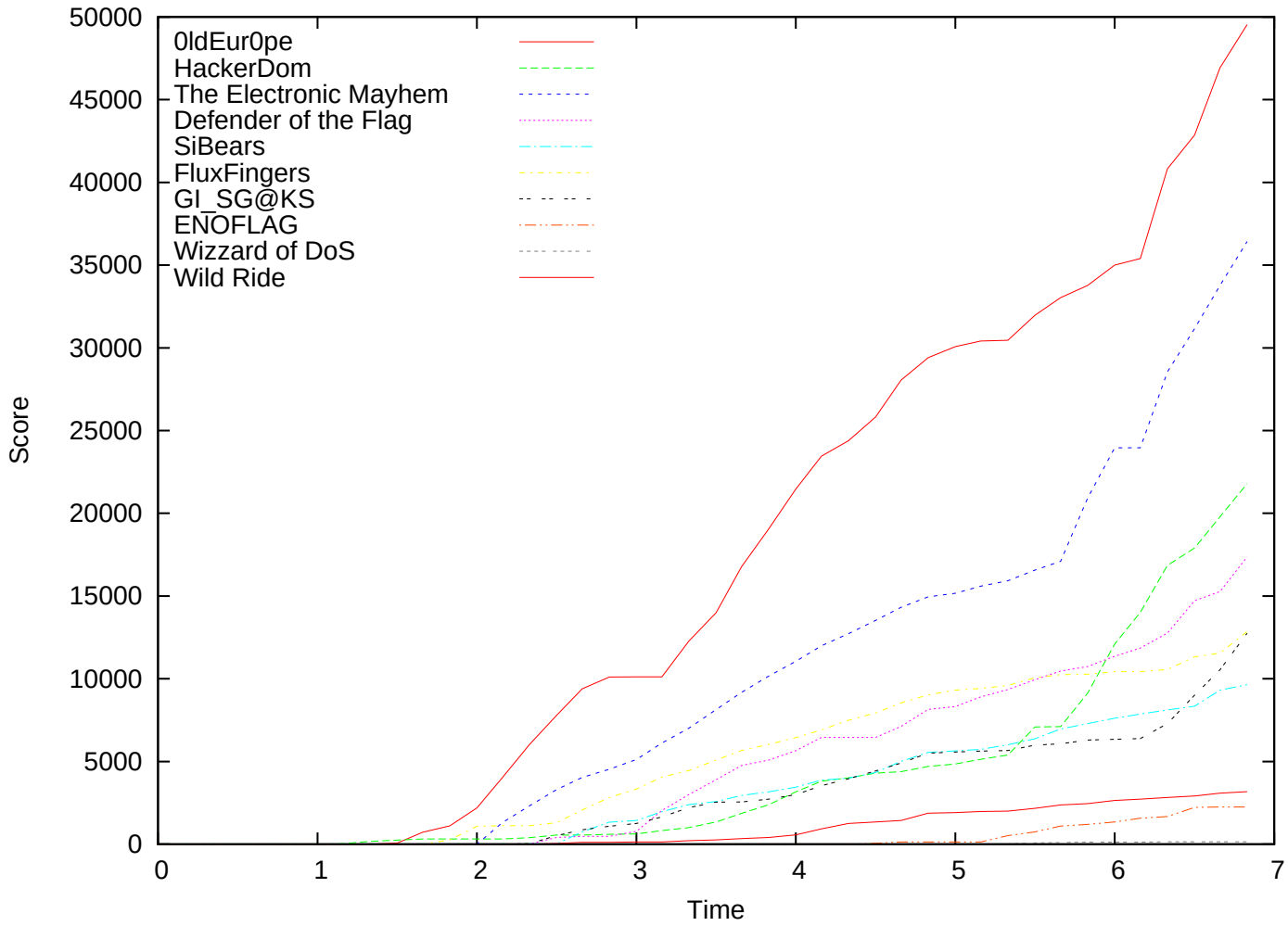
- about 30 teams each host a server
- like soccer: keep the own box clean while hitting the other box(es) as often as possible
- analyse, document, secure and attack

- focuses on application layer and administration
- code written specifically for this event

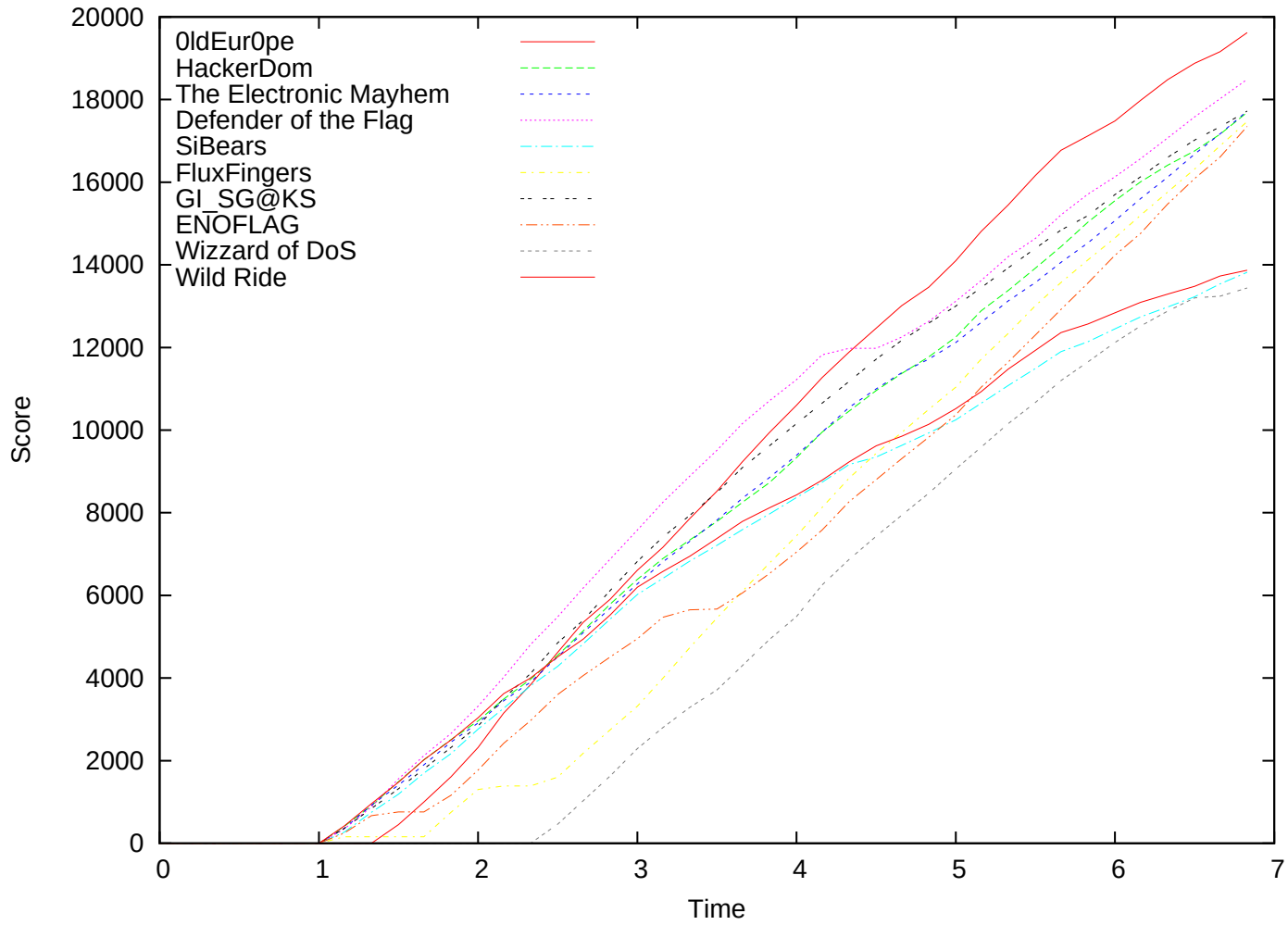
Benefits

- learn to work under pressure
- learn that there are many ways to compromise security
- learn how difficult it is to actually find bugs in software
- . . . and fix them afterwards
- learn that crypto is not the answer (. . . to everything)
- learn that security by obscurity does not work

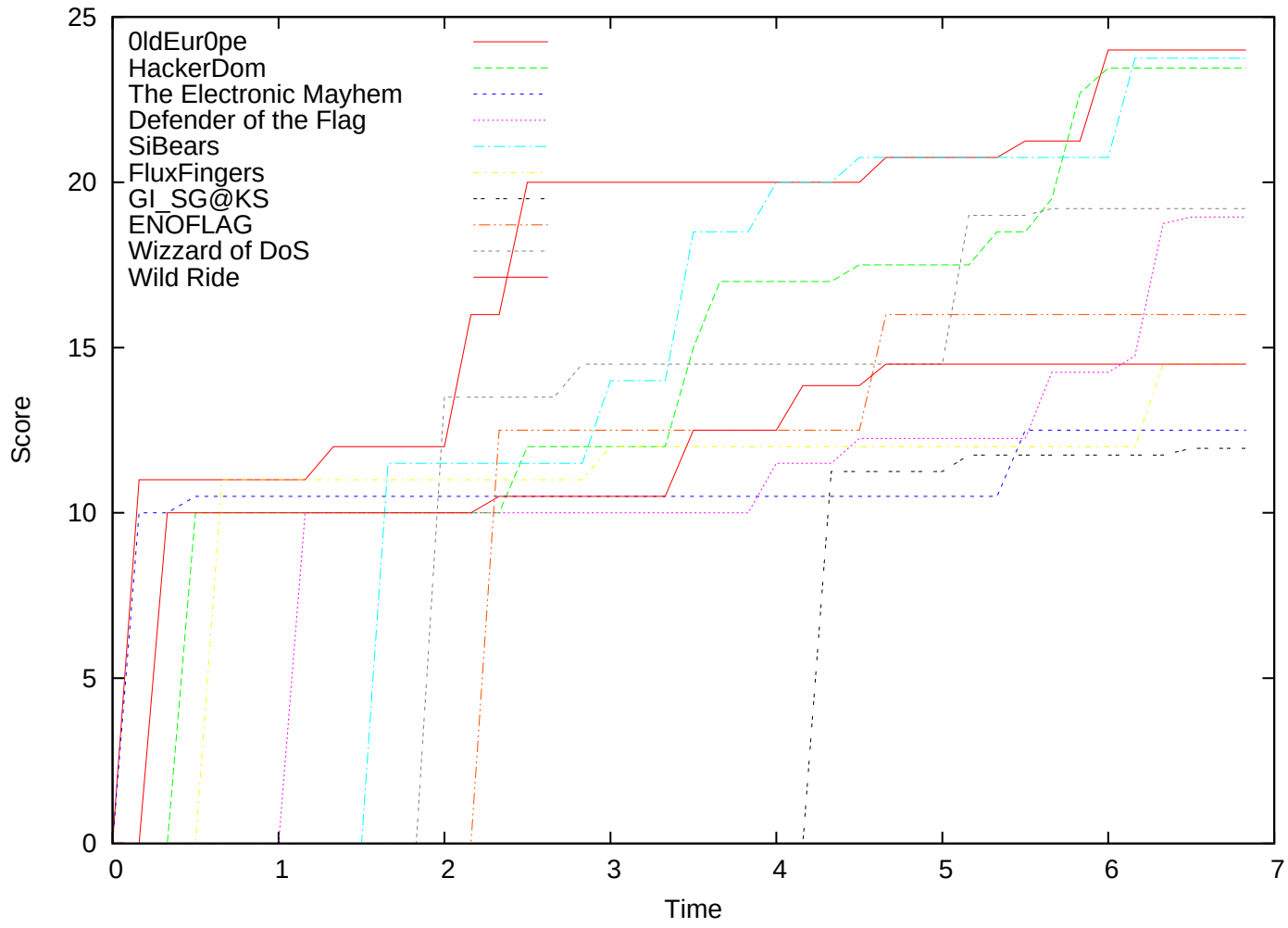
offensive scores



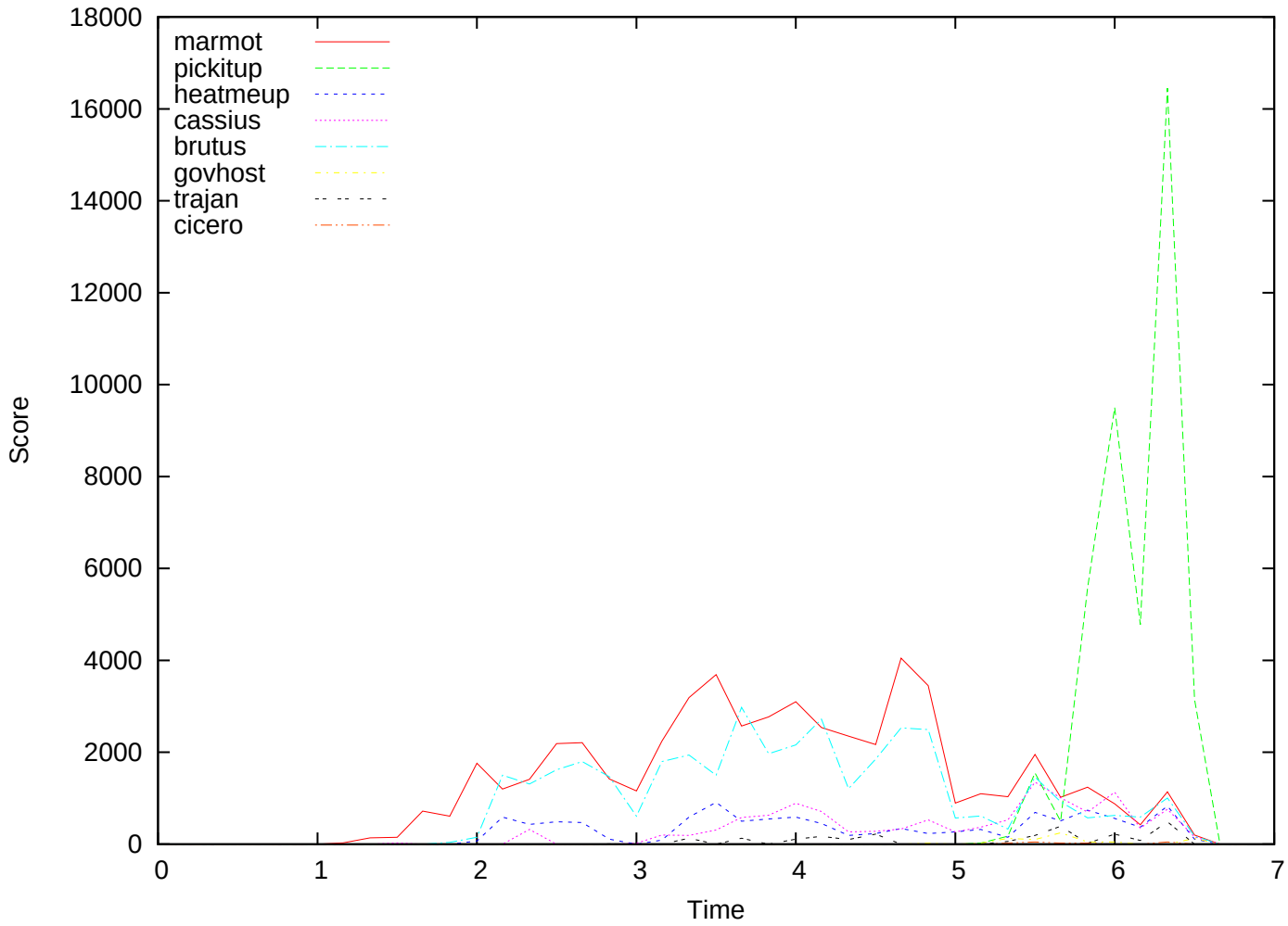
defensive


0ldEur0pe
HackerDom
The Electronic Mayhem
Defender of the Flag
SiBears
FluxFingers
GI_SG@KS
ENOFLAG
Wizzard of DoS
Wild Ride
Score
Time
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
0
1
2
3
4
5
6
7

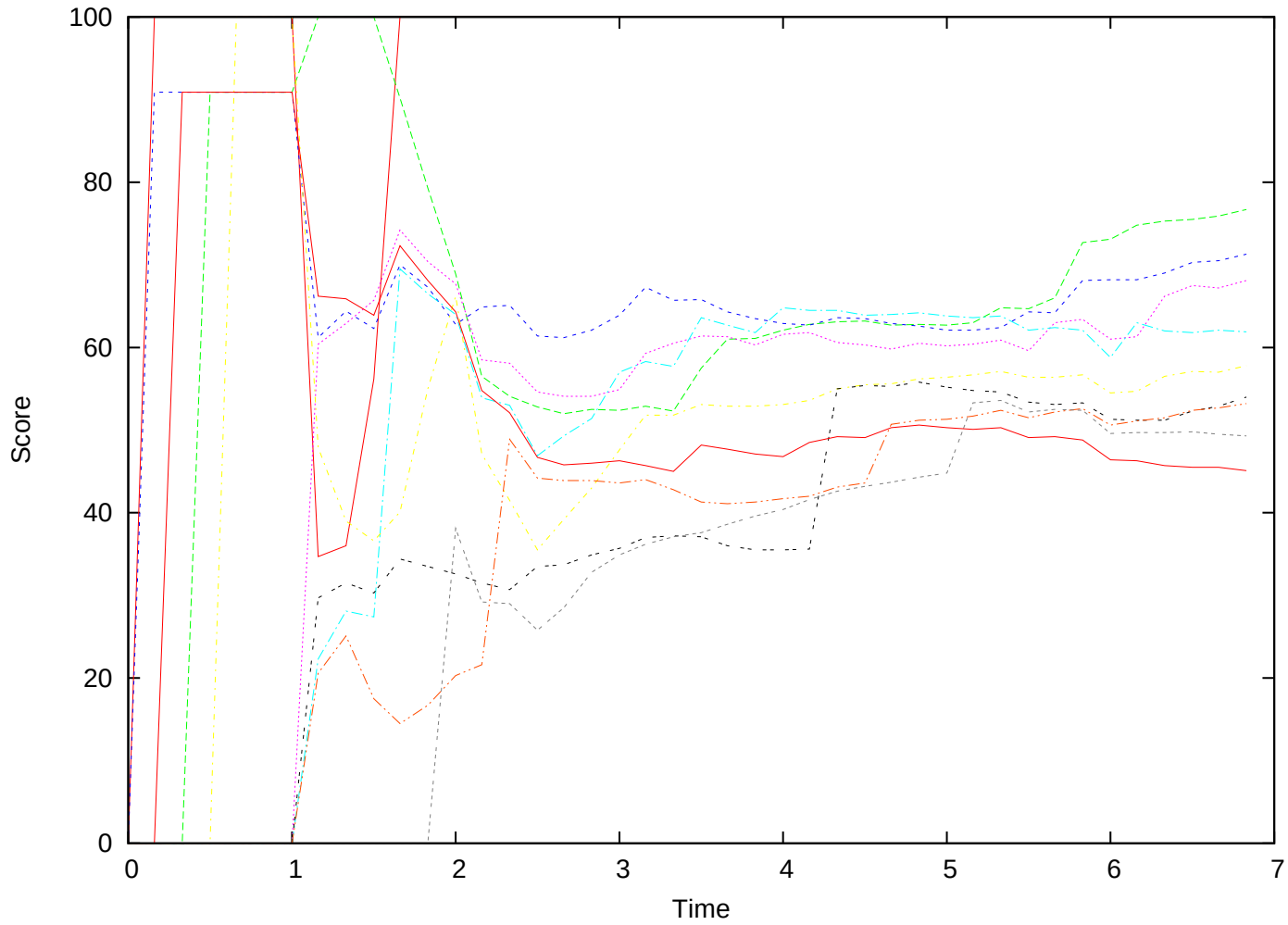
advisories


0ldEur0pe
HackerDom
The Electronic Mayhem
Defender of the Flag
SiBears
FluxFingers
GI_SG@KS
ENOFLAG
Wizzard of DoS
Wild Ride
Score
Time
0
5
10
15
20
25
0
1
2
3
4
5
6
7

services


marmot
pickitup
heatmeup
cassius
brutus
govhost
trajan
cicero
Score
Time
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
0
1
2
3
4
5
6
7

total



How "Security" Prevents Security Exercises

Communication with teams

- about one third of emails are lost in spam filters
- real time communication in IRC is getting difficult
- (no one reads their emails carefully)

Exchanging data

- How would you exchange a 5GB blob to 50 people all over the world?
- *bittorrent* is blocked or throttled
- some teams simply were not able to download 5 GB within 20 hours
  - need constantly 75KB per second
  - what if TCP-checksum fails? Guess, what – they failed

Connecting people

- setting up a VPN takes more than 6 hours for students?
- students do not know the meaning of a netmask?
- students not knowing the impact of using different subnets?
- principles of SNAT are unknown
- (some universities using IPs from 10/8 with a /8-netmask?)

- strange port filters at hotels (and universities and conferences?)

Encrypting data?

- practical application of *pgp/gpg* is unknown

Epilog

Final Standings

	Total	Offensive	Defensive	Ethical
1) 0ldEur0pe	100	100	100	100
2) HackerDom	77	46	89	97
3) The Electronic Mayhem	72	73	90	52
4) Defender of the Flag	69	35	93	78
5) SiBears	62	19	70	98
6) FluxFingers	59	28	89	60
7) GI_SG@KS	55	27	89	49
8) ENOFLAG	53	4	89	66
9) Wizzard of DoS	49	0	67	80
10) CInsects	48	22	73	47
11) Epic Fail	47	36	49	56
12) squareroots	45	11	60	65
13) Wild Ride	45	6	69	60
14) h4ck!nb3rg	43	2	74	54
15) milky way	38	6	56	54
16) StopUsToo	38	1	61	52
17) CIT	38	0	65	48
18) ESSE@INSO	37	0	69	43
19) 0x28 Thieves	36	3	64	41
20) SYPER	34	0	54	47
21) NUCIA	32	1	53	43
22) Bios	29	0	47	41
23) Kav@Buga	29	0	45	43

Epilog

is C (again) a programming language to write secure programs in?

Epilog

is C (again) a programming language to write secure programs in?

can we survive the Internet with students asking the wrong questions?

Epilog

is C (again) a programming language to write secure programs in?

can we survive the Internet with students asking the wrong questions?

why do "security" measure have to bother us all over the place?