The Hackers Profiling Project (HPP)

Presentation by Raoul Chiesa
United Nations
Interregional Crime and Justice Research Institute (UNICRI)
Co-Speakers: Alessio "mayhem" Pennasilico, Dr. Elisa Bortolani

unicri
advancing security, serving justice, building peace

unicri
advancing security, serving justice, building peace

What is UNICRI?

- A United Nations entity established in 1968 to support countries worldwide in crime prevention and criminal justice
- UNICRI carries out applied research, training, technical cooperation and documentation / information activities
- UNICRI disseminates information and maintains contacts with professionals and experts worldwide
- Counter Human Trafficking and Emerging Crimes Unit: cyber crimes, counterfeiting, environmental crimes, trafficking in stolen works of art…

unicri
advancing security, serving justice, building peace

What is ISECOM?

- Institute for Security and Open Methodologies (Est. 2002)
- A registered Non-Profit Organization
- Headquarters in Barcelona (Spain) and New York (U.S.A.)
- An Open Source Community Registered OSI, using Open and Peer Review process to assure quality and develop a Chain of Trust
- A Certification Authority grounded in trust and backed by Academic Institutions (La Salle University network)

Cybercrime

In recent years we have observed a series of "worrying" developments:

- **A dramatic decrease in the "window of exposure"**
- **Dangerous synergies between *technologically advanced personalities*, *classic* criminality and *terrorism***
- **Increase of the *dependence between* homeland security, telecommunications, fundamental services and ICT Security issues**

Nevertheless, often the cybercrime phenomenon is analysed in a wrong manner

Hackers

The term hacker has been heavily misused since the 80's; since the 90's, the mainstream have used it to justify every kind of "IT crime", from lame attacks to massive DDoS

Lamers, script-kiddies, industrial spies, hobby hackers….for the mass, they are all the same

From a business point of view, companies don't clearly know who they should be afraid of. To them they're all just "hackers"

Hackers: a blurred image

Yesterday: hacking was an emerging phenomenon – unknown to people & ignored by researchers

Today: research carried out in "mono": → one type of hacker: ugly (thin, myopic) , bad (malicious, destructive, criminal purposes) and "dirty" (asocial, without ethics, anarchic)

Tomorrow (HPP is the future): inter-disciplinary studies that merge criminology and information security → different *typologies* of hackers

HPP purposes

- Analyse the hacking phenomenon in its several aspects (technological, social, economic) through technical and criminological approaches
- Understand the different motivations and identify the actors involved
- Observe those *true* criminal actions "in the field"
- Apply the profiling methodology to collected data (4W: who, where, when, why)
- Acquire and disseminate knowledge

unicri
advancing security, serving justice, building peace

Project phases – starting: September 2004

1 – Theoretical collection:
Questionnaire

2 – Observation:
Participation in IT underground security events

3 - Filing:
Database for elaboration/classification of data (phase 1)

4 - Live collection:
Highly customised, new generation Honey-net systems

5 – Gap analysis:
of data from: questionnaire, honey-net, existing literature

6 – HPP "live" assessment
of profiles and correlation of modus operandi through data from phase 4

7 – Final profiling:
Redefinition/fine-tuning of hackers profiles used as "de-facto" standard

8 – Diffusion of the model:
elaboration of results, publication of the methodology, raising awareness

Project phases - detail

PHASE	CARRIED OUT		DURATION	NOTES
1 – Theoretical collection	YES	ON-GOING	16 months	Distribution on more levels
2 – Observation	YES	ON-GOING	24 months	From different points of view
3 – Filing	ON-GOING		21 months	The hardest phase
4 – "Live" collection	TO BE COMMENCED		21 months	The funniest phase ☺
5 – Gap & Correlation Analysis	YET TO COME		18 months	The Next Thing
6 – "Live" Assessment	PENDING		16 months	The biggest part of the Project
7 – Final Profiling	PENDING		12 months	"Satisfaction"
8 – Diffusion of the model	PENDING		GNU/FDL ;)	Methodology's public release

HPP next steps

Goals

- ✓ Data-base delivery
- ✓ Honey-Net systems delivery

What we need

- ✓ Contributors and volunteers
- ✓ Sponsors and donors

Challenges

- ✓ Identification/evaluation of techniques/attack-tools
- ✓ Data-correlation and identification of patterns
- ✓ Public release of the HPP v1.0 methodology

HPP questionnaire – the delivery

2 questionnaire typologies:

Level 1: Full version
Full parts of Modules A, B and C

Level 2: Compact version
Some parts of Modules A, B and C

3 delivery levels:

Verified sources – on-line questionnaire (full version) – QoQ extremely high

Underground world in general – on-line questionnaire (compact version) - QoQ medium

Specialized magazines – hard-copy and on-line questionnaire (compact version) – QoQ low

HPP questionnaire – the modules

Module A
Personal data (gender, age, social status, family context, study/work)

Module B
Relational data (relationship with: the Authorities, teachers/employers, friends/colleagues, other hackers)

Module C
Technical and criminological data (targets, techniques/tools, motivations, ethics, perception of the illegality of their own activity, crimes committed, deterrence)

All questions allow

anonymous answers

HPP questionnaire - excerpts

a) Sex:
Male
Female
b) Age:
e1) Title of study (please, indicate the last):
Elementary school leaving-certificate
Primary school leaving-certificate
Secondary school leaving-certificate
University degree
Beyond (master, PhD, specialization, etc.)
c1) Country and place of residence:
c2) You live in a:
city (more than 500.000 inhabitants)
town (less than 500.000 inhabitants)
village

d1) Do (or Did) you practise:
Hacking
Phreaking
Both

a1) Among your acquaintances, who is (or was) aware of your hacking/phreaking activity?
teachers
members of the underground world
partner
employer(s)
friends
colleagues
schoolmates
Other (Specify)

e) Kinds of data nets, technologies and operative systems targeted and tools used:
1) On what kind of data nets and technologies do (or did) you practise hacking/phreaking? For example: Internet, X.25, PSTN/ISDN, PBX, Wireless, "mobile" nets (GSM/GPRS/EDGE/UMTS), VoIP.

HPP questionnaire – examples of answers

Q: Do (or Did) you obey to the hacker's ethics? Why?

A: I obey my ethics and my rules, not ethics in general. The reason for this is that I don't like to follow what other people are doing. Ethics are like rules and laws, other people are writing them for you and even if sometimes they sound fair and correct, always behind the sweet and hypnotic words there is a trap restricting personal freedom. I am not a sheep who follows ethical or legal rules in general.

Q: How do you perceive your hacking/phreaking activity: legal or illegal?

A: I don't accept the terms legal and illegal. Accepting these terms means that I have the same point of view as people who have nothing common with me.

Ok, I'll try to be more specific to help you with this questionnaire. To me, my activities are legal, to others, they are illegal.

unicri
advancing security, serving justice, building peace

Total received questionnaires: #1073

Full questionnaires filled out - #500*

Compact questionnaires filled out - #573*

*since September 2006

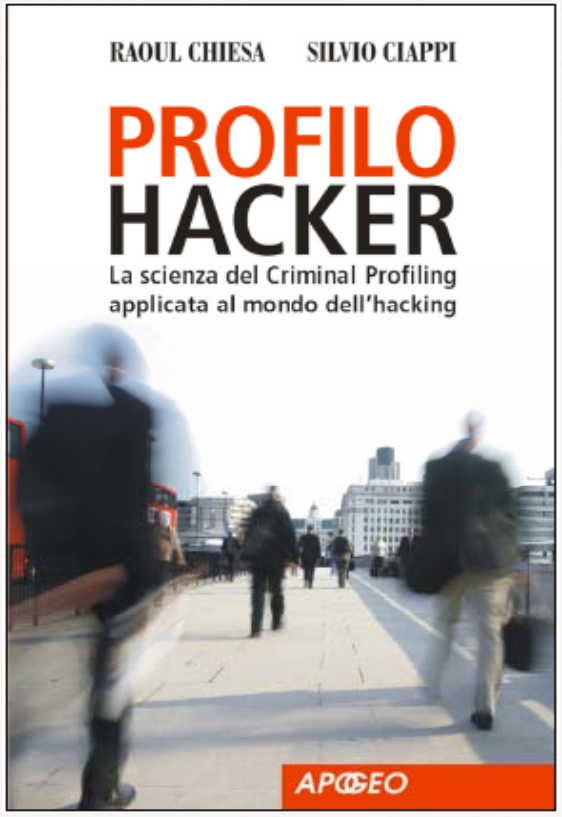
Mainly from:
USA
Italy
UK
Canada
Lithuania
Australia
Malaysia
Germany
Brazil

unicri
advancing security, serving justice, building peace

The questionnaires: some comments

- HPP is not exclusively based on questionnaires for the elaboration and delivery of a profiling methodology
- Some profiles have been elaborated on the basis of personal meetings with hackers belonging to specific categories
- HPP phases 1 and 2 are a kind of requirement for the next project phases
- The grand total of questionnaires received is 1073. Suggestions and advice given are really impressive

Hacker Profile – the book



Content

- Introduction to criminal profiling and cyber-crime
- To be, to think and to live like a hacker
- The Hacker's Profiling Project (HPP)
- Who are hackers? (Part I-II)

Who is it for?

Professionals involved in the networking activity, police detectives, university professors and students of law interested in criminal psychology as well as primary school and high school teachers dealing with potential hacker students. More in general, this book is designed for anyone interested in understanding the mechanisms behind cyber crimes and criminal psychology.

Evaluation and correlation standards

- Modus Operandi (MO)
- Lone hacker or as a member of a group
- Motivations
- Selected targets
- Relationship between motivations and targets
- Hacking career
- Principles of the hacker's ethics
- Crashed or damaged systems
- Perception of the illegality of their own activity
- Effect of laws, convictions and technical difficulties as a deterrent

Level of technical skills

Wannabe Lamer

Script Kiddie

Cracker

Ethical hacker

Q.P.S. Hacker

Cyber-Warrior

Industrial spy

Government Agent

Military Hacker

Degree of danger

Wannabe Lamer

Script Kiddie

Ethical Hacker

Q.P.S. Hacker

Cracker

Cyber-Warrior

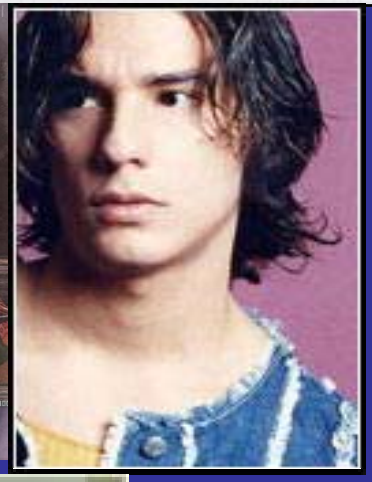
Industrial spy

Government Agent

Military Hacker

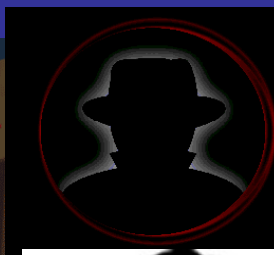
Detailed analysis and correlation of profiles – table #1

PROFILE	RANK	IMPACT LEVEL	TARGET	
Wanna Be Lamer	Amateur	NULL	End-User	
Script Kiddie		LOW	SME	Specific security flaws
Cracker	Hobbiest	MEDIUM / HIGH	Business company	
Ethical Hacker		MEDIUM	Vendor	Technology
Quiet, Paranoid Skilled Hacker		MEDIUM / HIGH	On necessity	
Cyber-Warrior	Professional	HIGH	"Symbol" business company	End-User
Industrial Spy		HIGH	Business company	Corporation
Government agent		HIGH	Government	Suspected Terrorist
			Strategic Company	Individual
Military Hacker		HIGH	Government	Strategic Company




MOD


XS4ALL




?

The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace

Detailed analysis and correlation of profiles – table #2

	OFFENDER ID	LONE / GROUP HACKER	TARGET	MOTIVATIONS / PURPOSES
Wanna Be Lamer	9-16 years "I would like to be a hacker, but I can't"	GROUP	End-User	For fashion, It's "cool" => to boast and brag
Script Kiddie	10-18 years The script boy	GROUP: but they act alone	SME / Specific security flaws	To give vent of their anger attract mass-media attention
Cracker	17-30 years The destructor, burned ground	LONE	Business company	To demonstrate their powe / attract mass-media attention
Ethical Hacker	15-50 years The "ethical" hacker's world	LONE / GROUP (only for fun)	Vendor / Technology	For curiosity (to learn) and altruistic purposes
Quiet, Paranoid, Skilled Hacker	16-40 years The very specialized and paranoid attacker	LONE	On necessity	For curiosity (to learn) => egoistic purposes
Cyber-Warrior	18-50 years The soldier, hacking for money	LONE	"Symbol" business company / End-User	For profit
Industrial Spy	22-45 years Industrial espionage	LONE	Business company / Corporation	For profit
Government Agent	25-45 years CIA, Mossad, FBI, etc.	LONE / GROUP	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker	25-45 years	LONE / GROUP	Government / Strategic company	Monitoring / controlling / crashing systems

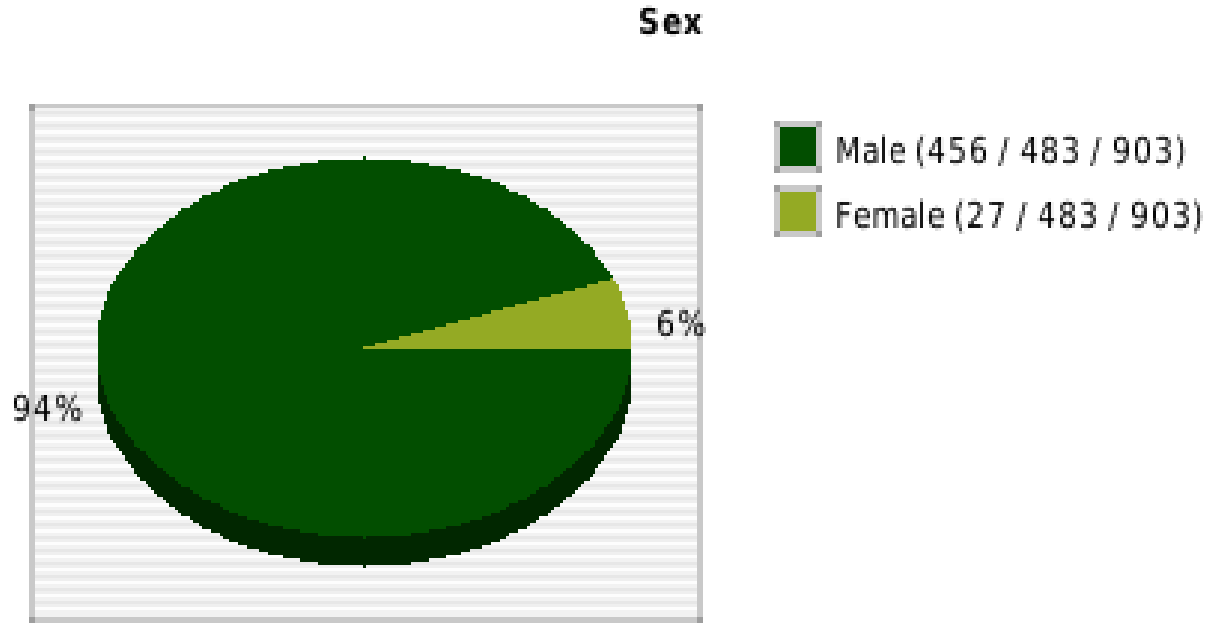
Detailed analysis and correlation of profiles – table #3

	OBEDIENCE TO THE "HACKER ETHICS"	CRASHED / DAMAGED SYSTEMS	PERCEPTION OF THE ILLEGALITY OF THEIR OWN ACTIVITY
Wanna Be Lamer	NO: they don't know "Hacker Ethics" principles	YES: voluntarily or not (inexperience, lack of technical skills)	YES: but they think they will never be caught
Script Kiddie	NO: they create their own ethics	NO: but they delete / modify data	YES: but they justify their actions
Cracker	NO: for them the "Hacker Ethics" doesn't exist	YES: always voluntarily	YES but: MORAL DISCHARGE
Ethical Hacker	YES: they defend it	NEVER: it could happen only incidentally	YES: but they consider their activity morally acceptable
Quiet, Paranoid, Skilled Hacker	NO: they have their own personal ethics, often similar to the "Hacker Ethics"	NO	YES: they feel guilty for the upset caused to SysAdmins and victims
Cyber-Warrior	NO	YES: they also delete/modify/steal and sell data	YES: but they are without scruple
Industrial Spy	NO: but they follow some unwritten "professional" rules	NO: they only steal and sell data	YES: but they are without scruple
Government Agent	NO: they betray the "Hacker Ethics"	YES (including deleting/modifying/stealing data) / NO (in stealth attacks)	
Military Hacker	NO: they betray the "Hacker Ethics"	YES (including deleting/modifying/stealing data) / NO (in stealth attacks)	

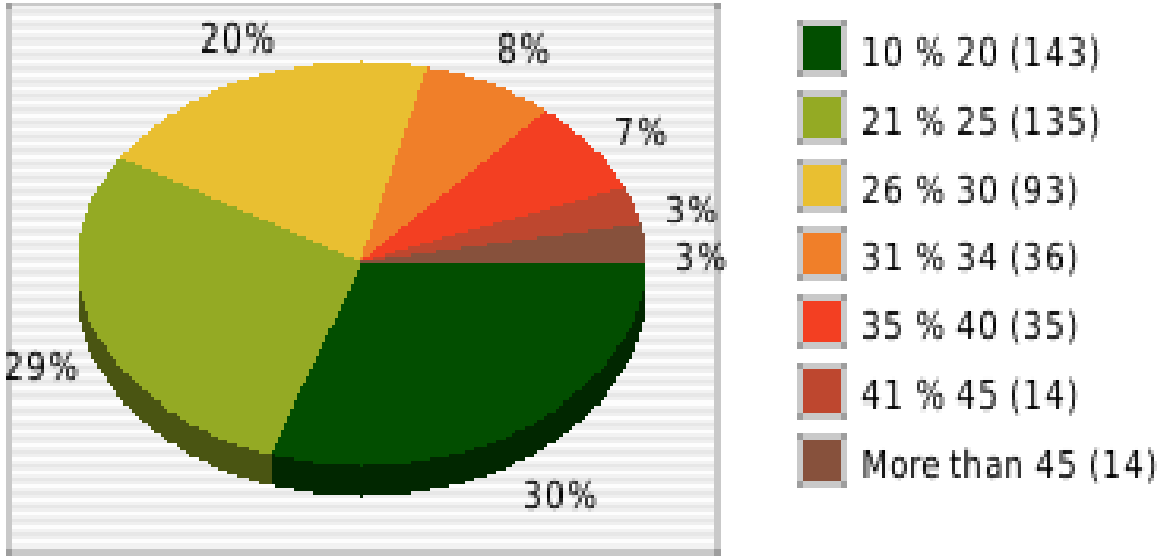
Detailed analysis and correlation of profiles – table #4

DETERRENCE EFFECT OF:	LAWS	CONVICTIONS SUFFERED BY OTHER HACKERS	CONVICTIONS SUFFERED BY THEM	TECHNICAL DIFFICULTIES
Wanna Be Lamer	NULL	NULL	ALMOST NULL	HIGH
Script Kiddie	NULL	NULL	HIGH: they stop after the 1st conviction	HIGH
Cracker	NULL	NULL	NULL	MEDIUM
Ethical Hacker	NULL	NULL	HIGH: they stop after the 1st conviction	NULL
Quiet, Paranoid, Skilled Hacker	NULL	NULL	NULL	NULL
Cyber-Warrior	NULL	NULL	NULL	NULL: they do it as a job
Industrial Spy	NULL	NULL	NULL	NULL: they do it as a job

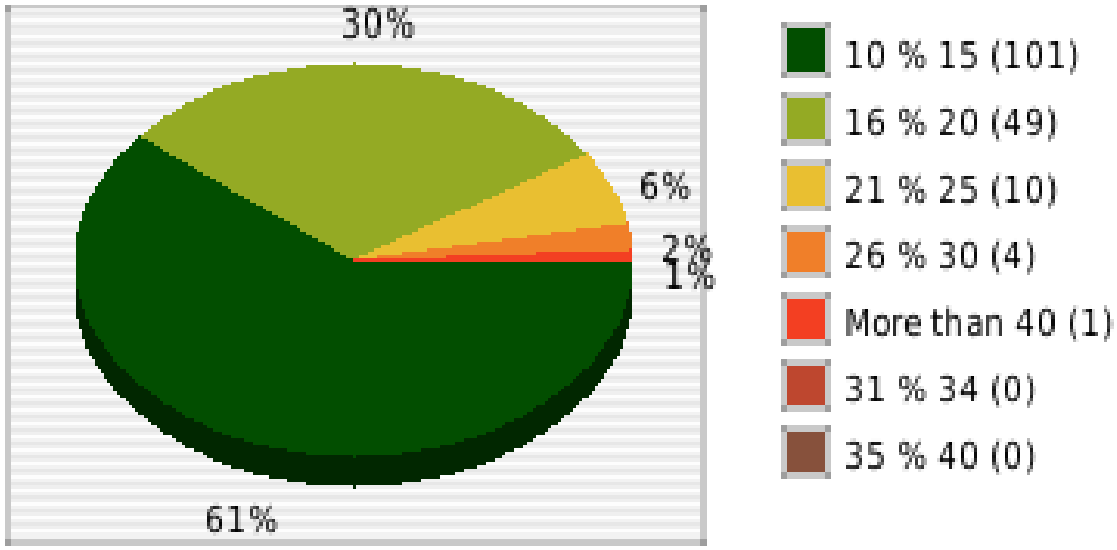
Personalities



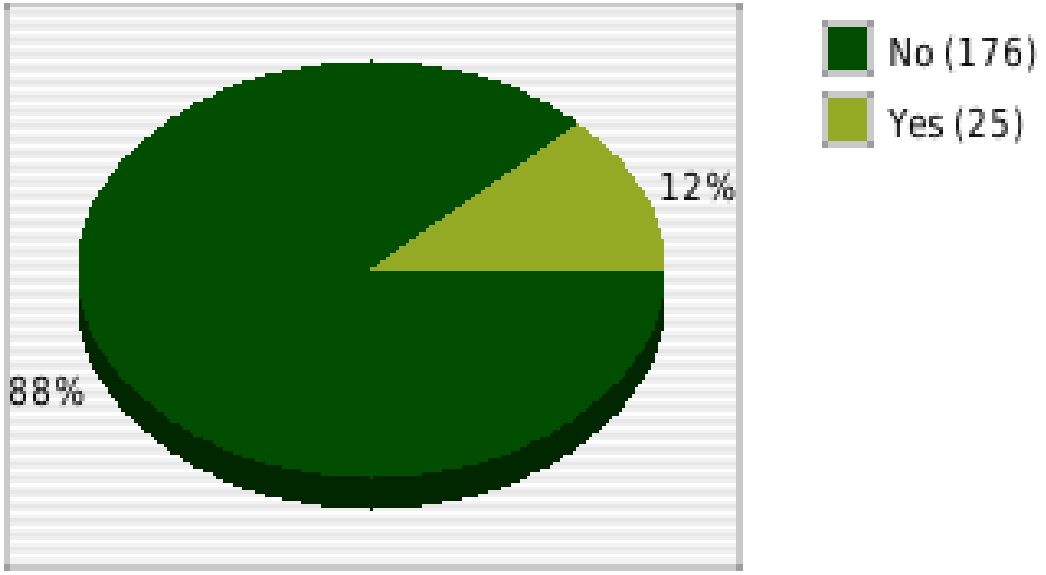
Age [Total: 471, Null: 915]



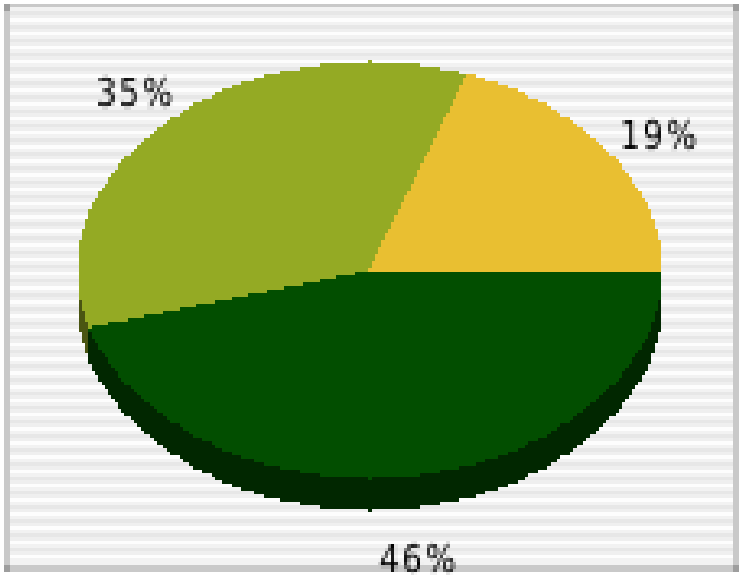
Age that you started with hacking [Total: 171, Null: 1212]



Have you ever practised carding? [Total: 201, Null: 1182]

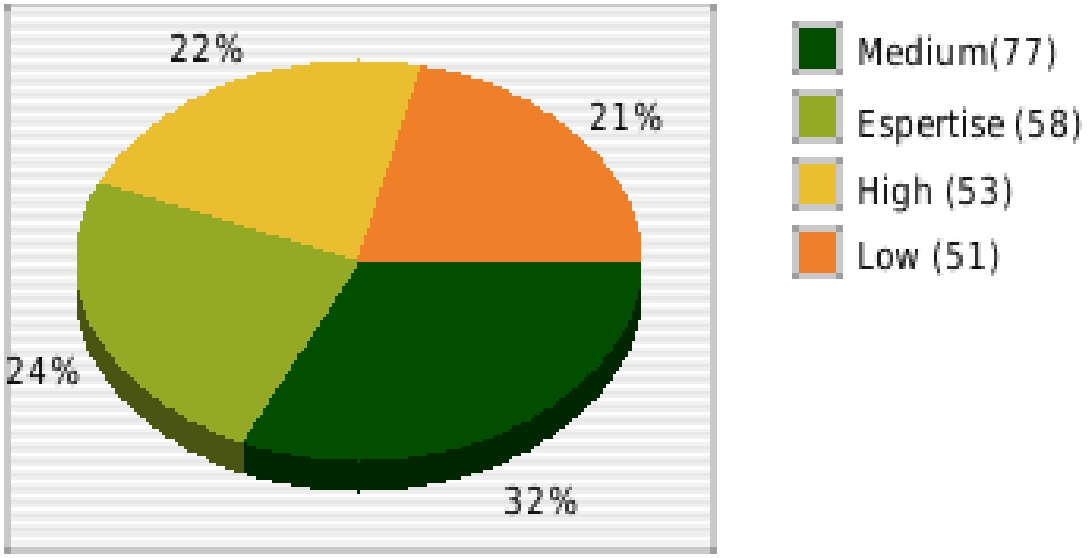


Where do you live?

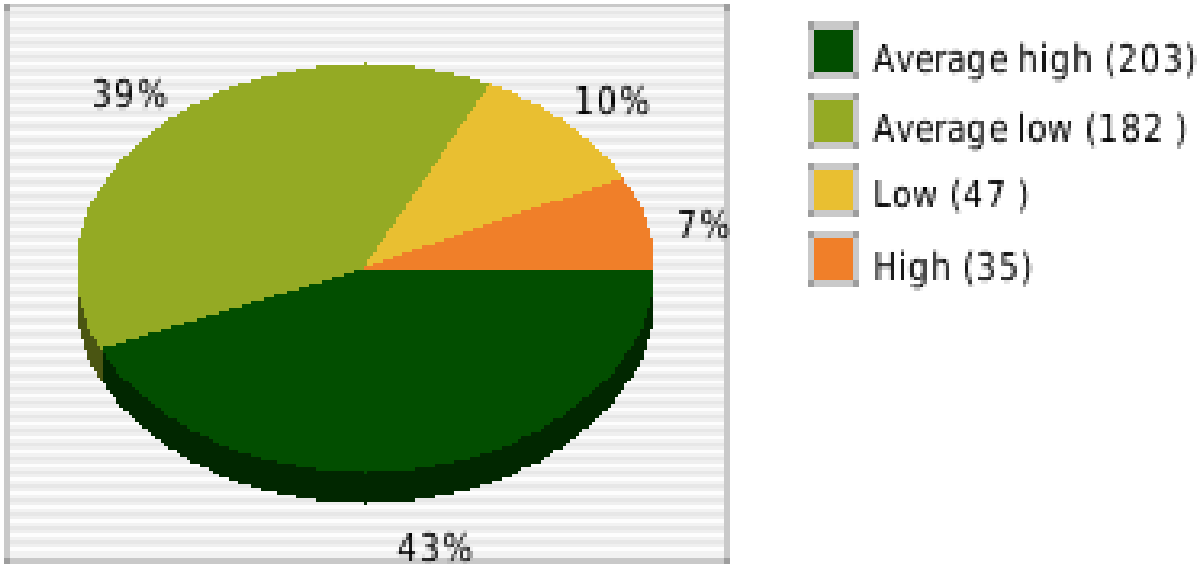


- Big town (215 / 470 / 916)
- Small town (164 / 470 / 916)
- Country (91 / 470 / 916)

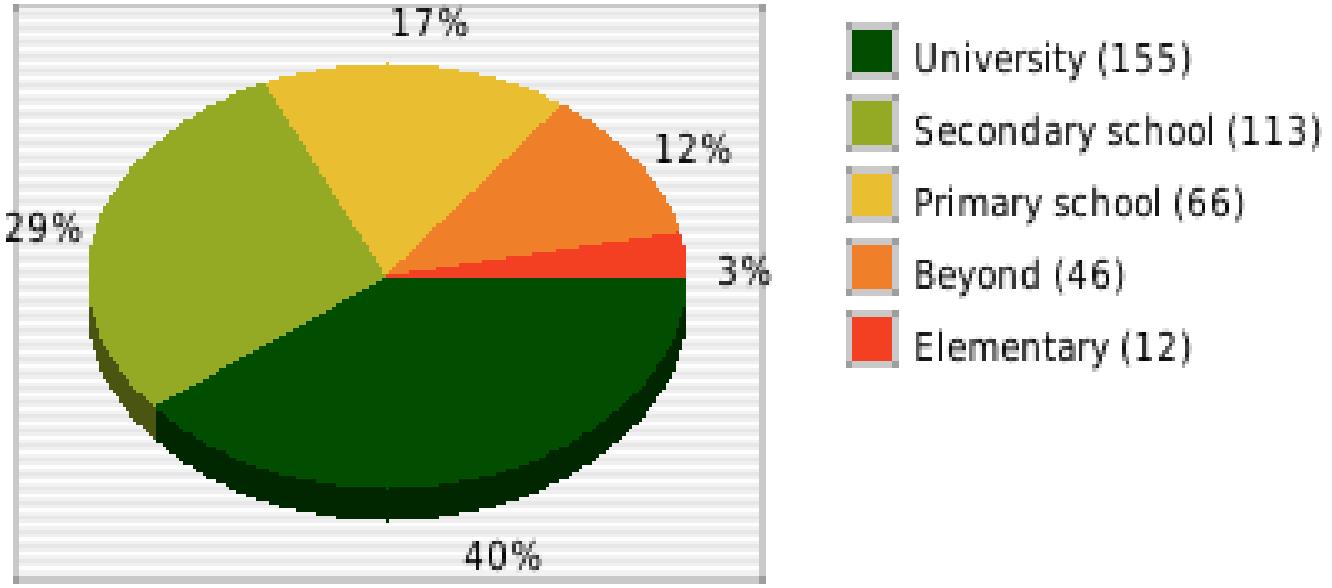
Technical skills [Total: 239, Null: 1180]



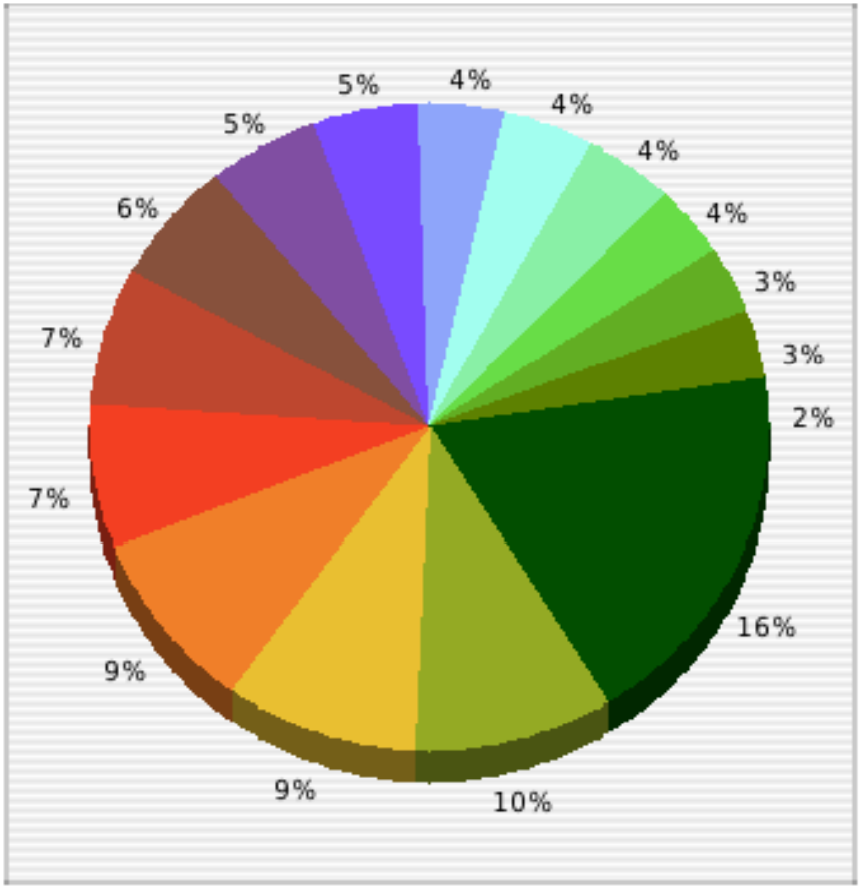
socio-economic status [Totals: 467, Null: 919]



Studies [Total: 426, Null: 954]

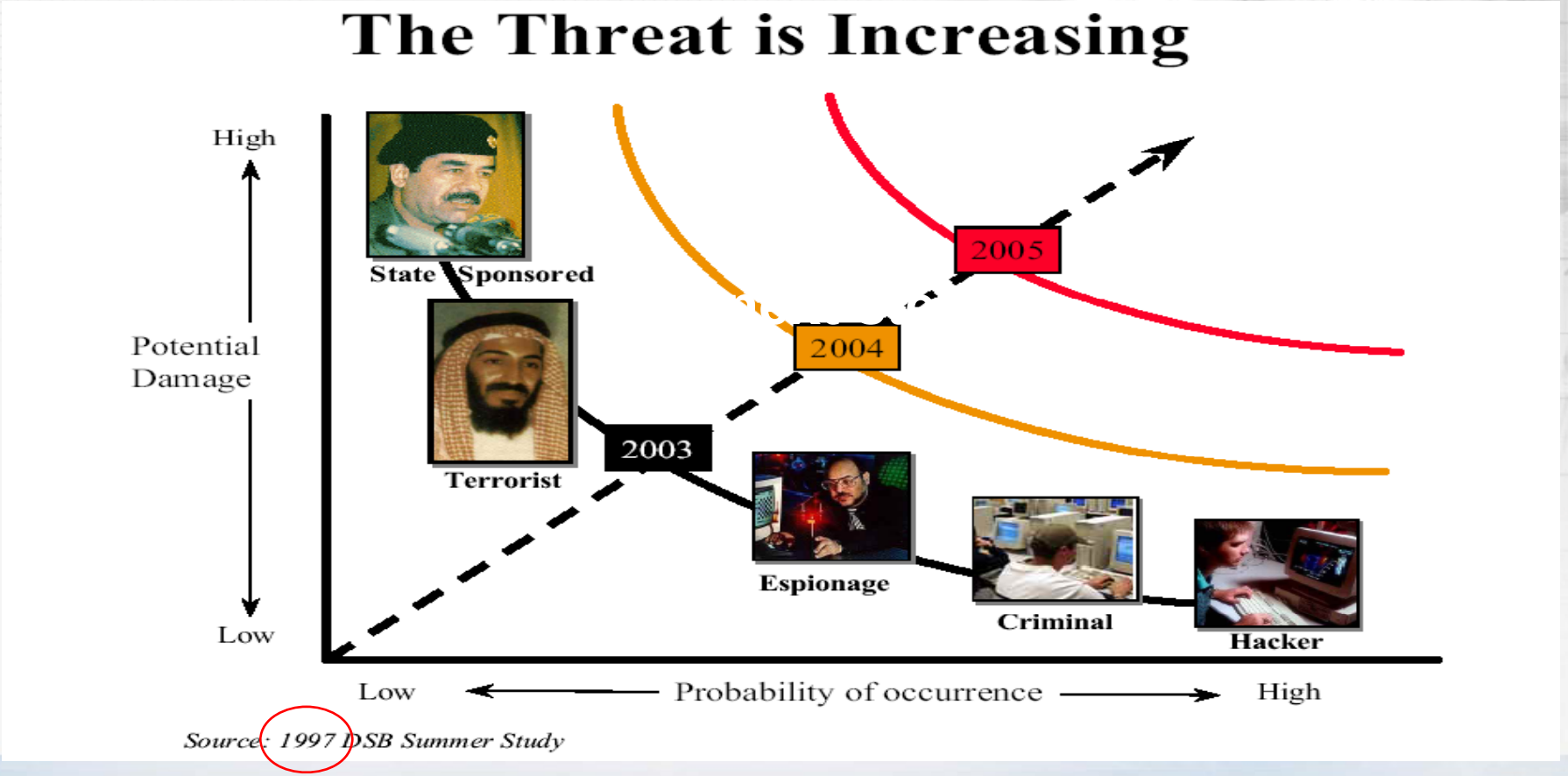


Personalities



- Curious (173)
- Happy (103)
- Lazy (98)
- Committed (92)
- Healthy (79)
- Introverted (71)
- unsatisfied (67)
- Equilibrated (55)
- Paranoid (52)
- Ingenuous (47)
- Manipulator (45)
- Depressed (44)
- Anxious (38)
- Extroverted (37)
- Satisfied (35)
- unscrupulous (25)

Are hackers terrorists?



Are hackers terrorists?

Basically the answer is NO. Or, “not yet”

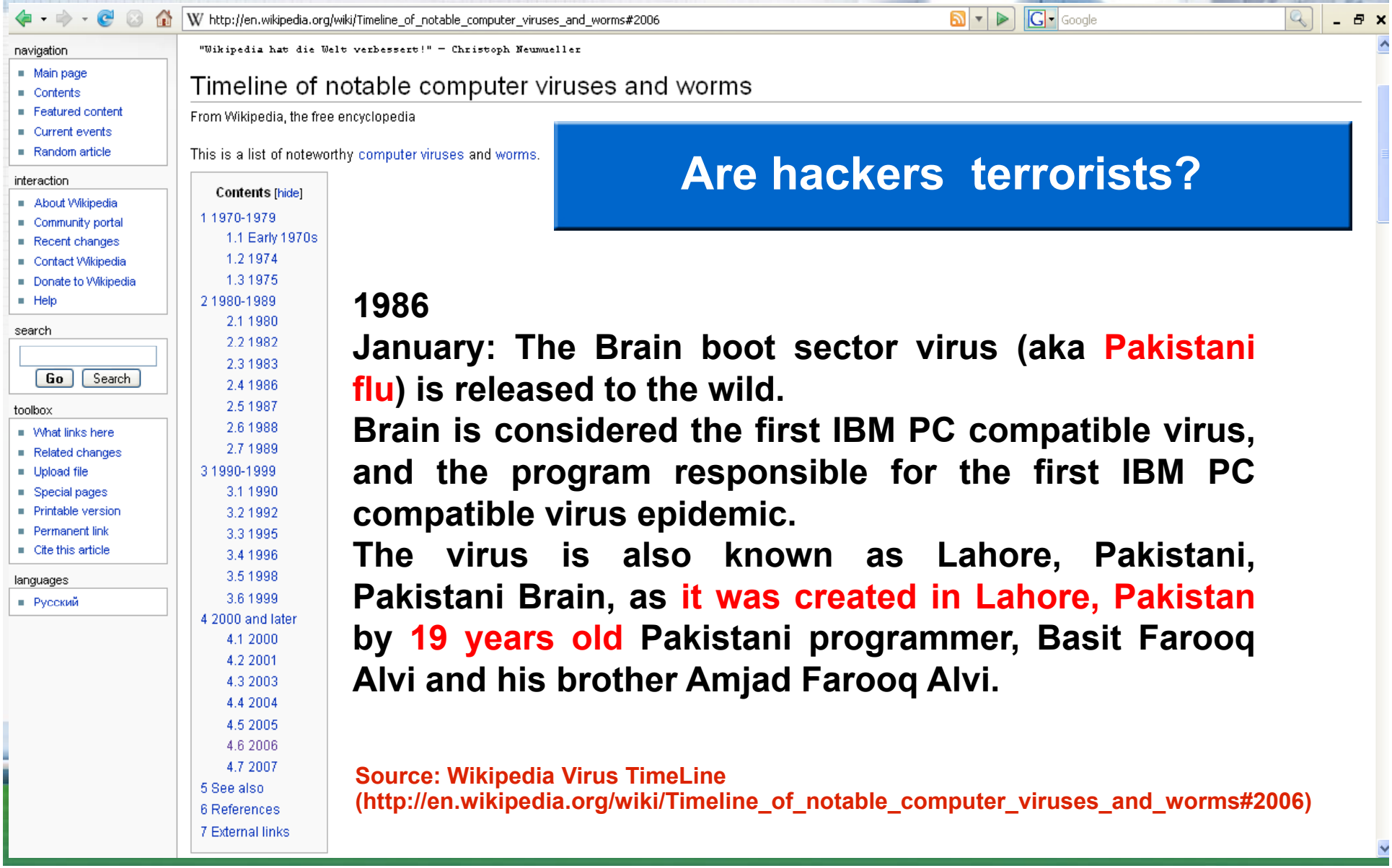
An official cyber-attack against a country, where the attackers could be labeled as terrorists, has not happened yet

Nevertheless, few cases should make us think:
China -> USA/UK/Germany/Italy
Russia -> Estonia

We should rethink the fact that extremists are commonly considered unskilled

The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace



Are hackers terrorists?

1986

January: The Brain boot sector virus (aka Pakistani flu) is released to the wild.

Brain is considered the first IBM PC compatible virus, and the program responsible for the first IBM PC compatible virus epidemic.

The virus is also known as Lahore, Pakistani, Pakistani Brain, as it was created in Lahore, Pakistan by 19 years old Pakistani programmer, Basit Farooq Alvi and his brother Amjad Farooq Alvi.

Source: Wikipedia Virus TimeLine (http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms#2006)

Conclusions

The hacking world **has not always been linked** to criminal actions;

The researches carried out till today have **not depicted properly** a so **complex**, **hierarchical** and in **continuous evolution** phenomenon as the underground world;

The application of a profiling methodology is possible, but **it needs a 360° analysis** of the phenomenon, by analysing it from four principal point of views: **Technological**, **Social**, **Psychological**, **Criminological**;

We still have a **lot of work to do** and **we need support**: if by ourselves we have reached these results, imagine what we can do by joining our forces and experiences !

The H.P.P. Project is **open for collaborations.**

Considerations

- **The whole Project** is self-funded and based on independent research methodologies.
- Despite many problems, we have been carrying out the Project for four years.
- The final methodology is going to be released under GNU/FDL and distributed through ISECOM.
- It is welcome the research centres, public and private institutions, and governmental agencies' **interest in the Project**.
- We think that we are elaborating something **beautiful**...
- …something that **did not exist…**

…and it seems – really – to **have a sense** ! :)

- It is not a simple challenge. However, we think to be on **the right path**.

Biography and References (1)

During the different phases of bibliography research, the Authors have made reference (also) to the following publications and on-line resources:

- **H.P.P. Questionnaires**
- **Stealing the Network: How to 0wn a Continent**, (AA.VV), Syngress Publishing, 2004
- **Stealing the Network: How to 0wn the Box**, (AA.VV.), Syngress Publishing, 2003
- **Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier**, Suelette Dreyfus, Random House Australia, 1997
- **The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage**, Clifford Stoll, DoubleDay (1989), Pocket (2000)
- **Masters of Deception: the Gang that Ruled Cyberspace**, Michelle Stalalla e Joshua Quinttner, Harpercollins, 1995
- **Kevin Poulsen, Serial Hacker**, Jonathan Littman, Little & Brown, 1997
- **Takedown: sulle tracce di Kevin Mitnick**, John Markoff e Tsutomu Shimomura, Sperling & Kupfler, (Hyperion Books), 1996
- **The Fugitive Game: online with Kevin Mitnick**, Jonathan Littman, Little & Brown, 1997
- **The Art of Deception**, Kevin D. Mitnick e William L. Simon, Wiley, 2002
- **The Art of Intrusion**, Kevin D. Mitnick e William L. Simon, Wiley, 2004
- **@ Large: the Strange Case of the World's Biggest Internet Invasion**, Charles Mann & David Freedman, Touchstone, 1998
- **The Hacker Diaries: Confessions of Teenage Hackers**, Dan Verton, McGraw-Hill Osborne Media, 2002
- **Cyberpunk: Outlaws and Hackers on the Computer Frontier**, Katie Hafner, Simon & Schuster, 1995
- **SecurityFocus.com** (BugTraq, VulnDev), **Mitre.org** (CVE), **Isecom.org** (OSSTMM), many "underground" web sites & mailing lists, private contacts & personal friendships, the Academy and Information Security worlds

Biography and References (2)

During the different phases of bibliography research, the Authors have made reference (also) to the following publications and on-line resources:

- **Compendio di criminologia**, Ponti G., Raffaello Cortina, 1991
- **Criminalità da computer**, Tiedemann K., in Trattato di criminologia, medicina criminologica e psichiatria forense, vol.X, Il cambiamento delle forme di criminalità e devianza, Ferracuti F. (a cura di), Giuffrè, 1988
- **United Nations Manual on the Prevention and Control of Computer-related Crime**, in International Review of Criminal Policy – Nos. 43 and 44
- **Criminal Profiling: dall'analisi della scena del delitto al profilo psicologico del criminale,** Massimo Picozzi, Angelo Zappalà, McGraw Hill, 2001
- **Deductive Criminal Profiling: Comparing Applied Methodologies Between Inductive and Deductive Criminal Profiling Techniques**, Turvey B., Knowledge Solutions Library, January, 1998
- **Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology**, Täterpro

Acknowledgements

The H.P.P. Project's Authors would like to thanks for their contribution, support and time:

- Key People: **Dr.ssa Elisa Bortolani**, **Job De Haas, Kevin D. Mitnick, Mayhem, Venix.**

- Events, Associations and Organizations: **HITB**, ***SecWest**, **Italian Hackmeeting**, **SysCan**, **MOCA**, **BLACKHAT**, **RUXCON**, **EUROSEC**, **CLUSIT**, **ISECOM**, **ISACA** (Italian Chapter), **OWASP meetings** (Italian Chapter), **ISO 27001 IUG** (Italian Chapter), **BeIIUA**, **Telecom Security Task Force, Phrack**, **2600 Magazine**, **Xcon/Xfocus Team, CONfidence.**

- Mailing lists: SecurityFocus.com, Full-Disclosure, sikurezza.org, private mailing lists & discussion groups.

- Gurus: **Raist**, **Raptor**, **Inode**, **Synack**, **Cla'75**, **Lamerone**, **Dialtone**, Pete **Herzog**, Stefano **Chiccarelli**, Emmanuel **Gadaix**, Avv. Gabriele **Faggioli**, **Trek/3K**, Phlippe **Langlois**, Gabriella **Mainardi**, Antonis **Anagnostopoulos**, Marco **Tracinà**, **Sentinel**, Vittorio **Pasteris**, Pietro **Gentile**, Fabrizio **Ciraolo,** Alessandra **Vitagliozzi,** Jim **Geovedi,** Anthony **Zboralski, t**he **Grugq,** Fabrice **Marie, Roelef9,** Dhillon **Kannabhiran.**

Special thanks to:

- Daniele **Poma**, Andrea "**Pila**" **Ghirardini**, Andrea **Barisani**, Fabrizio **Matta**, Marco **Ivaldi**, Dr. Angelo **Zappalà**, D.ssa Angela **Patrignani**, Patrizia **Bertini**, Dr. Mario **Prati**, Vincenzo **Voci**, Massimiliano **Graziani**, Dr. Mimmo **Cortese**, Lapo **Masiero**, Simona **Macellari**, Salvatore **Romagnolo**, Avv. Annarita **Gili**, Raffaela **Farina**, Enrico **Novari**, Fabrizio **Cirilli**, Stavroula **Ventouri**, Dr. Alberto Pietro **Contaretti**, Dr.ssa Alicia **Burke.**

unicri
advancing security, serving justice, building peace

Ms. Stefania Ducci
E-mail ducci@unicri.it
Tel. +39 011 6537157

Mr. Raoul Chiesa
E-mail chiesa@unicri.it
raoul@isecom.org
Tel. +39 348 2337600

HPP home page:
www.isecom.org/hpp

HPP questionnaire:
hpp.recursiva.org

www.unicri.it

Thank you
for your attention

unicri
advancing security, serving justice, building peace

Ms. Stefania Ducci
E-mail ducci@unicri.it
Tel. +39 011 6537157

Mr. Raoul Chiesa
E-mail chiesa@unicri.it
raoul@isecom.org
Tel. +39 348 2337600

HPP home page:
www.isecom.org/hpp

HPP questionnaire:
hpp.recursiva.org

www.unicri.it

QUESTIONS?