Profiling Hackers:
real data, real experiences, wrong myths and the Hackers Profiling Project (HPP)

Presentation by Raoul Chiesa
Senior Advisor, Strategic Alliances & Cybercrime Issues
Human Traficking and Emerging Crimes Unit
United Nations - Interregional Crime and Justice Research Institute (UNICRI)

Virus Bulletin Conference 2009
Geneva, Switzerland
September 24th, 2009
Corporate Track

unicri
advancing security, serving justice, building peace

Disclaimer

- The use of this document is under **ISECOM's document licensing** (GNU/FDL).
- The information contained within this presentation **does not infringe** on any intellectual property nor does it contain tools or recipe that could be in breach with known laws.
- The statistical data presented **belong to** the Hackers Profiling Project.
- Quoted trademarks belongs to **registered owners**.
- The views expressed are those of the author and **do not necessary reflect** the views of UNICRI.
- Contents of this presentation **may be quoted or reproduced**, provided that the **source of information is acknowledged**.

Agenda

- ✓ UNICRI & ISECOM
- ✓ Cybercrime
- ✓ Profiling the enemy
- ✓ Hackers…
- ✓ The Hackers Profiling Project
- ✓ Correlation of the profiles
- ✓ Some stats (hackpies)
- ✓ Conclusions
- ✓ References: books you should read
- ✓ Acknowledgements & Contacts

unicri
advancing security, serving justice, building peace

Agenda

- ✓ UNICRI & ISECOM
- ✓ Cybercrime
- ✓ Profiling the enemy
- ✓ Hackers…
- ✓ The Hackers Profiling Project
- ✓ Correlation of the profiles
- ✓ Some stats (hackpies)
- ✓ Conclusions
- ✓ References: books you should read
- ✓ Acknowledgements & Contacts

unicri
advancing security, serving justice, building peace

What is UNICRI?

United Nations Interregional Crime & Justice Research Institute

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…

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)

unicri
advancing security, serving justice, building peace

Overview of ISECOM Projects

- **OSSTMM** – The **Open Source Security Testing Methodology Manual**
- **RAV**s – The Security Metrics
- **BIT** – Business Integrity Testing Methodology Manual
- **OPRP** – Open Protocol Resource Project
- **SIPES** – Security Incident Policy Enforcement System
- **SPSMM** – The Secure Programming Standards Methodology Manual
- **STICK** – Software Testing Checklist
- **ISM 3.0** – Information Security Maturity Model
- **HHS** – Hacker High School
- **HPP** – **Hacker's Profiling Project** **New!**

OSSTMM Professional Security Analyst

OSSTMM Professional Security Tester

HACKERS PROFILING PROJECT

unicri
advancing security, serving justice, building peace

Agenda

- ✓ UNICRI & ISECOM
- ✓ Cybercrime
- ✓ Profiling the enemy
- ✓ Hackers…
- ✓ The Hackers Profiling Project
- ✓ Correlation of the profiles
- ✓ Some stats (hackpies)
- ✓ Conclusions
- ✓ References: books you should read
- ✓ Acknowledgements & Contacts

Crime->Yesterday

"**Every new technology, opens the door to new criminal approaches**".

- The relationship between **technologies and criminality** has always been – since the very beginning – characterized by a kind of "competition" by the good and the bad guys, just like cats and mice.
- As an example, at the beginning of 1900, when **cars** appeared, the "bad guys" started **stealing them (!)**
- ….the police, in order to contrast the phenomenon, defined the **mandatory use** of car plates…
- ….and the thieves began **stealing the car plates** from the cars (and/or falsifying them).

Crime->Today:Cybercrime

- **Cars** have been substituted by **information**.

*You got the **information**, you got the **power**..*

(at least, in **politics**, in the **business world**, in our **personal relationships…**)

- Very simply, this happens because the "*information*" is **at once transformable** in "something else":

✓ Competitive advantage

✓ Sensible/critical information

✓ Money

- … that's why all of us we want to "*be secure*".

- It's not by chance that it's named "IS": **Information Security** ☺

Cybercrime

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

- **A dramatic decrease in the so-called "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 cyber crime phenomenon is analysed in a wrong manner.

unicri
advancing security, serving justice, building peace

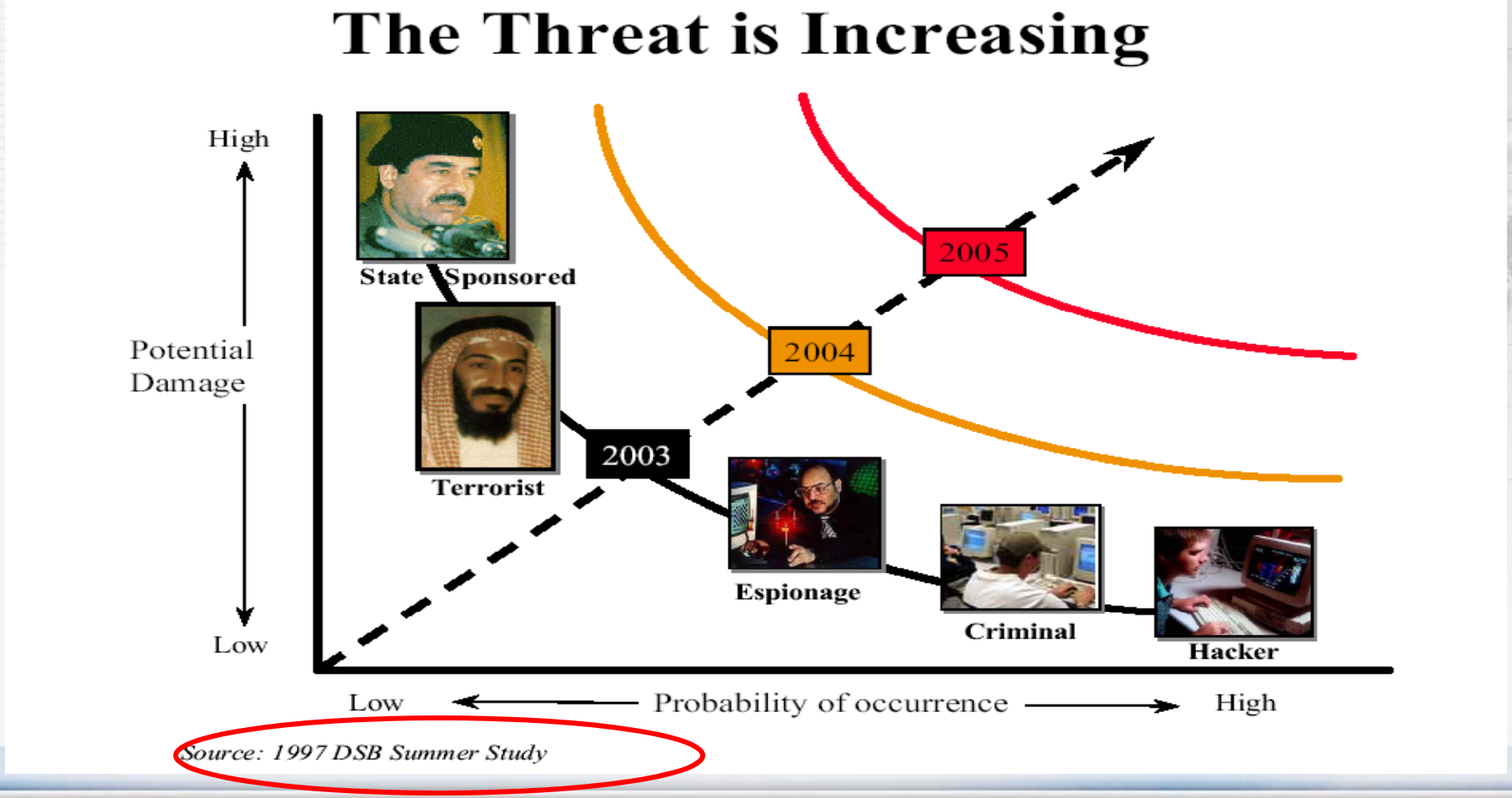
Agenda

- ✓ UNICRI & ISECOM
- ✓ Cybercrime
- ✓ Profiling the enemy
- ✓ Hackers…
- ✓ The Hackers Profiling Project
- ✓ Correlation of the profiles
- ✓ Some stats (hackpies)
- ✓ Conclusions
- ✓ References: books you should read
- ✓ Acknowledgements & Contacts

Profiling the Enemy: current issues

- Classic criminal profiling methodologies and approaches often **can not** be applied to the "cyberspace" (e.g. "**geographical profiling**").
- We do also have different issues, involving **technical**, **ethical** and **legal** aspects.
- Last but not least, the above must be applied to an **unknown** enemy, that evolves **very quickly**, since it's a **dynamic** threat, not a **static** threat!
- Giving what I have showed you until now, this is why the profiles of those "classic actors" **can't always be applied** to the cybercrime world.
- Also, profiles **likely very different each other** started to **talk** (what do you think about this…?), **exchanging information** (I'm going to tell you about X, and you will tell me about Y), **black market** (0-day), **engagements** (hacking on-demand).

New actors, new links ☹



unicri
advancing security, serving justice, building peace

Agenda

- ✓ UNICRI & ISECOM
- ✓ Cybercrime
- ✓ Profiling the enemy
- ✓ Hackers…
- ✓ The Hackers Profiling Project
- ✓ Correlation of the profiles
- ✓ Some stats (hackpies)
- ✓ Conclusions
- ✓ References: books you should read
- ✓ Acknowledgements & Contacts

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 low-skill attacks to massive DDoS

"Lamers", script-kiddies, industrial spies, hobby hackers….for the mass, they are all the same. YOU do not belong to "the mass", since you belong to IS

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

Attacker's macro typologies

- **Low-level hackers: "script-kiddies" hunting for known security flaws**
  - ✓ (kind of "NEW") Phishing, Remote low-level Social Engineering Attacks
  - ✓ Insiders (user/supervisor/admin)
  - ✓ Disgruntled Employees
- **High-level, sophisticated hackers, Organized Crime: middle and high level attacks**
  - ✓ Hobbyist hackers
  - ✓ Unethical "security guys" (Telecom Italia and Vodafone Greece scandals)
  - ✓ Unstructured attackers (SCAMs, medium & high-level hi-tech frauds,VISHING …)
  - ✓ Structured attackers ("the italian job", targeted attacks)
- **Industrial Espionage, Terrorism**
  - ✓ Foreign Espionage
  - ✓ Hacktivist (unfunded groups)
  - ✓ Terrorist groups (funded groups)
  - ✓ State sponsored attacks

unicri
advancing security, serving justice, building peace

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

unicri
advancing security, serving justice, building peace

Agenda

- ✓ UNICRI & ISECOM
- ✓ Cybercrime
- ✓ Profiling the enemy
- ✓ Hackers…
- ✓ The Hackers Profiling Project
- ✓ Correlation of the profiles
- ✓ Some stats (hackpies)
- ✓ Conclusions
- ✓ References: books you should read
- ✓ Acknowledgements & Contacts

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 "on the field"
- Apply the profiling methodology to collected data (4W: who, where, when, why)
- Acquire and worldwide disseminate knowledge

unicri
advancing security, serving justice, building peace

Project phases – starting: September 2004

1 – Theoretical collection:
Questionnaires (10 languages)

2 – Observation:
Participation in IT underground security events, worldwide

3 - Filing:
Database for elaboration/classification of data gathered from phases 1 and 4

4 - Live collection:
Highly customised, next generation Honeynet systems

5 – Gap analysis:
of data gathered from questionnaire, NG honeynets, 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

- ✓ Database delivery
- ✓ Honeynet 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: #1200

Full questionnaires filled out - #500*

Compact questionnaires filled out - #573*

*since September 2006

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

unicri
advancing security, serving justice, building peace

The questionnaires: some comments

Regarding the elaboration and the delivery of a profiling methodology, HPP is not exclusively based on questionnaires from phase 1

Some profiles have been elaborated on the basis of (many) personal meetings with hackers belonging to specific categories

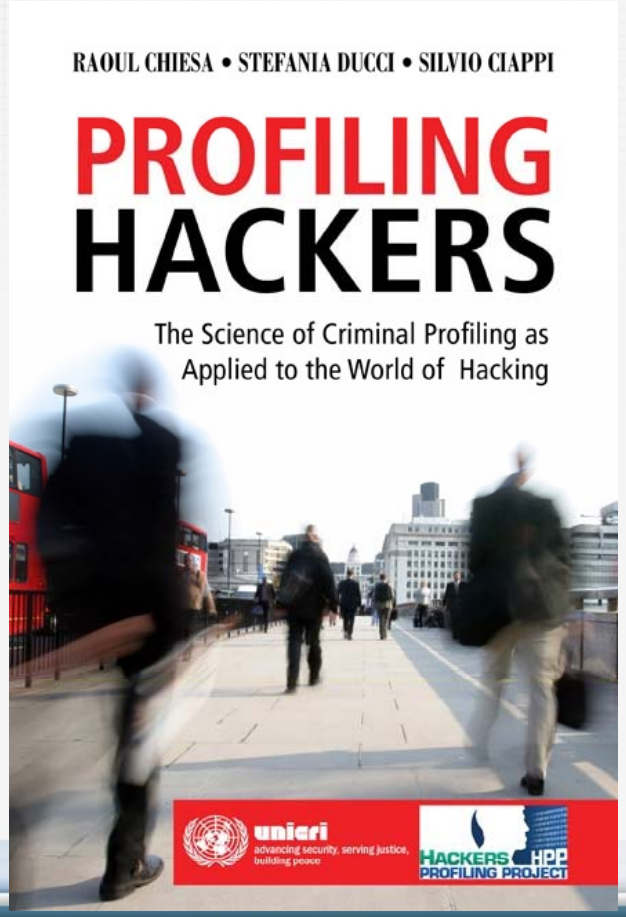
HPP phases 1 and 2 are kind of a requirement for the next project phases

The grand total of questionnaires received is 1200 * Suggestions and advice given are really impressive

(* Updated August 2009)

unicri
advancing security, serving justice, building peace

Profiling Hackers – the book/1



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.

Profiling Hackers – the book/2

Contents

unicri
advancing security, serving justice, building peace

Agenda

- ✓ UNICRI & ISECOM
- ✓ Cybercrime
- ✓ Profiling the enemy
- ✓ Hackers…
- ✓ The Hackers Profiling Project
- ✓ Correlation of the profiles
- ✓ Some stats (hackpies)
- ✓ Conclusions
- ✓ References: books you should read
- ✓ Acknowledgements & Contacts

Evaluation and correlation standards

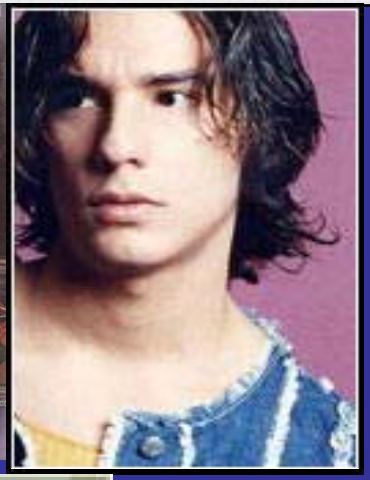
- Modus Operandi (MO)
- Lone hacker or as a member of a group
- Motivations
- Selected targets
- Relationship between motivations and targets
- Hacking career
- Principles of the hacker's ethics
- Crashed or damaged systems
- Perception of the illegality of their own activity
- Effect of laws, convictions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

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

The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace



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 power / 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

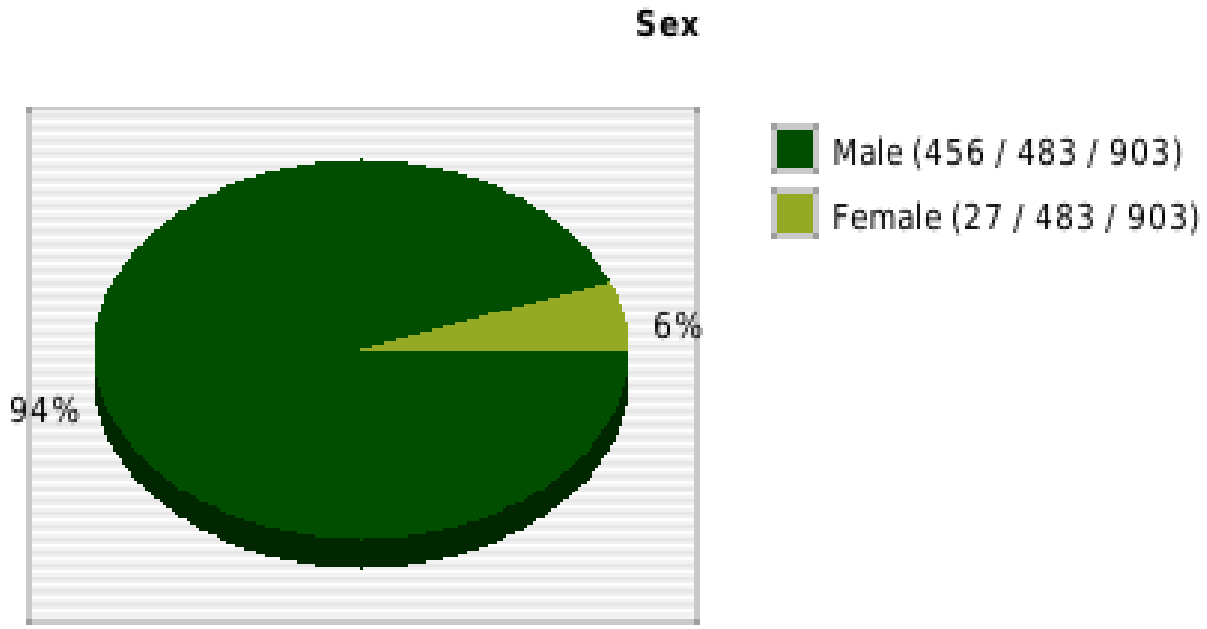
unicri
advancing security, serving justice, building peace

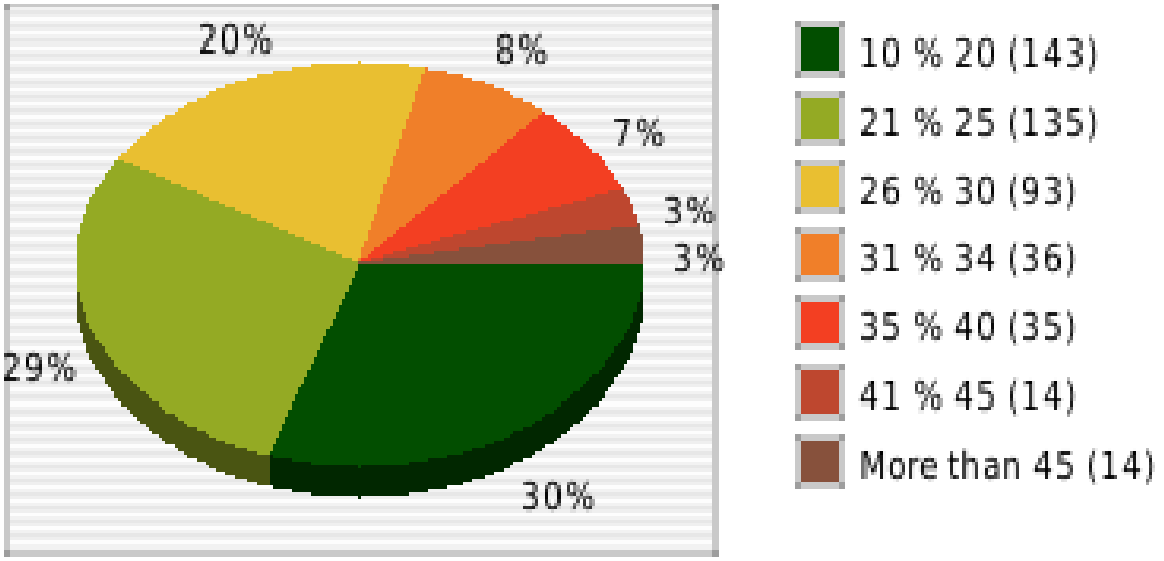
Agenda

- ✓ UNICRI & ISECOM
- ✓ Cybercrime
- ✓ Profiling the enemy
- ✓ Hackers…
- ✓ The Hackers Profiling Project
- ✓ Correlation of the profiles
- ✓ Some stats (hackpies)
- ✓ Conclusions
- ✓ References: books you should read
- ✓ Acknowledgements & Contacts

The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace

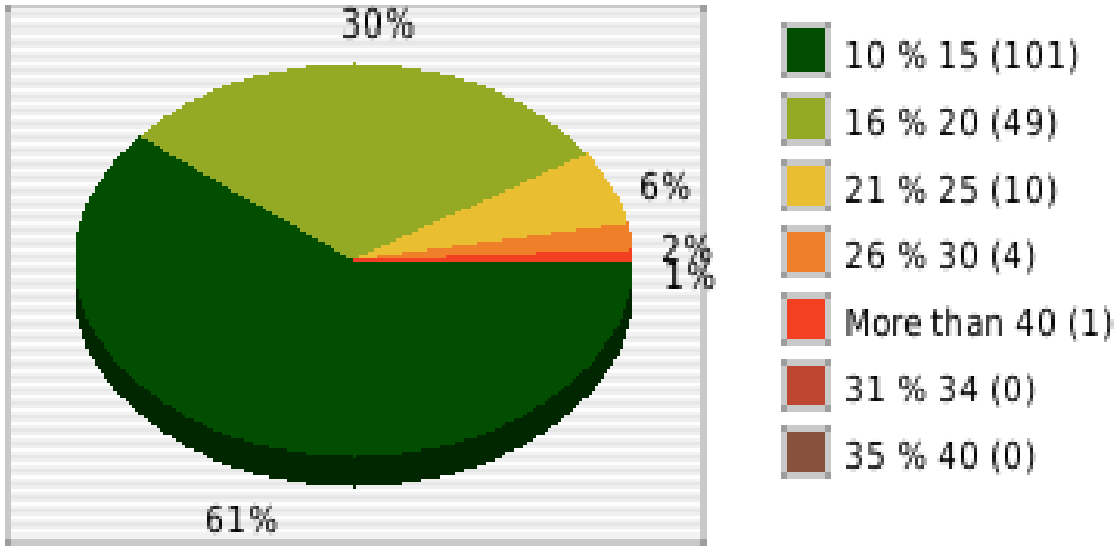


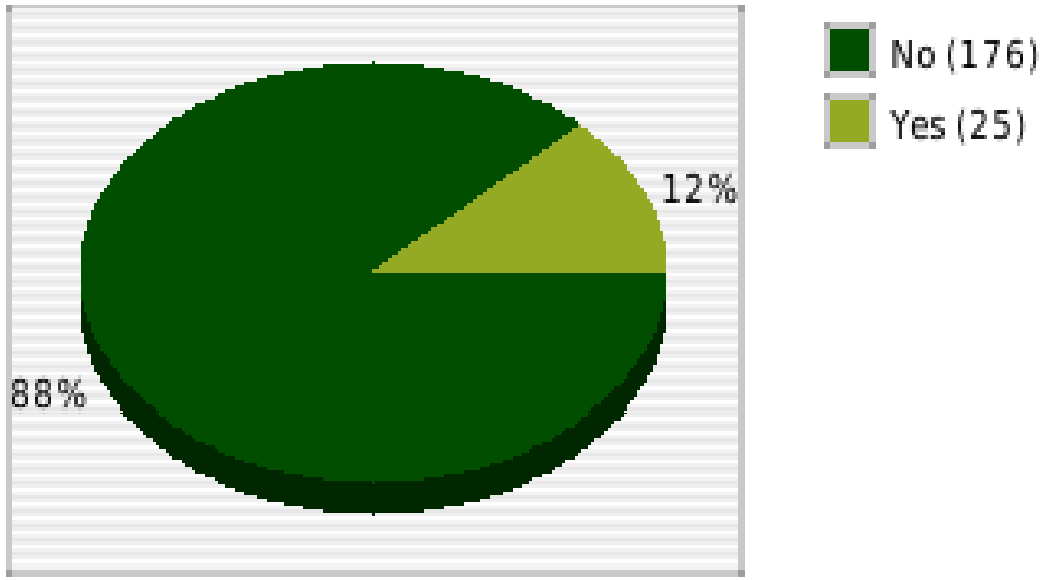

Age [Total: 471, Null: 915]
20%
8%
7%
3%
3%
29%
30%
10 % 20 (143)
21 % 25 (135)
26 % 30 (93)
31 % 34 (36)
35 % 40 (35)
41 % 45 (14)
More than 45 (14)

The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace

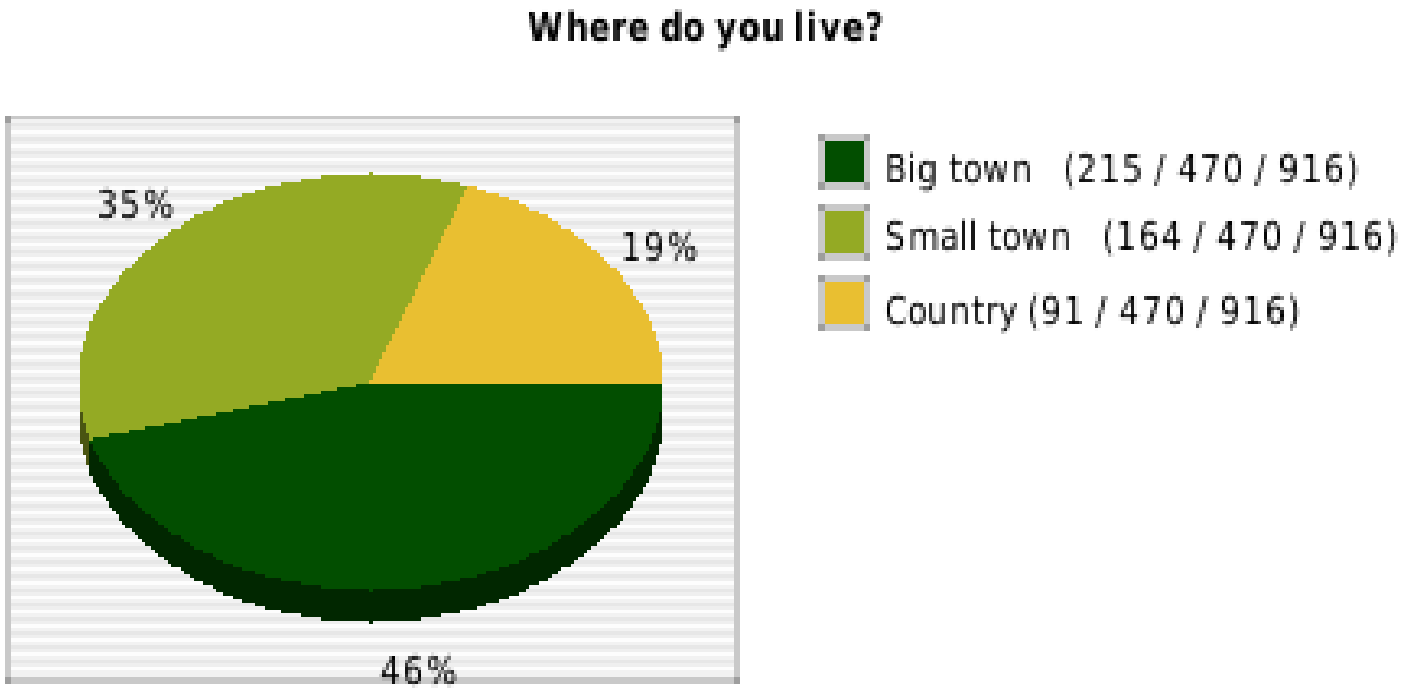
Age that you started with hacking [Total: 171, Null: 1212]

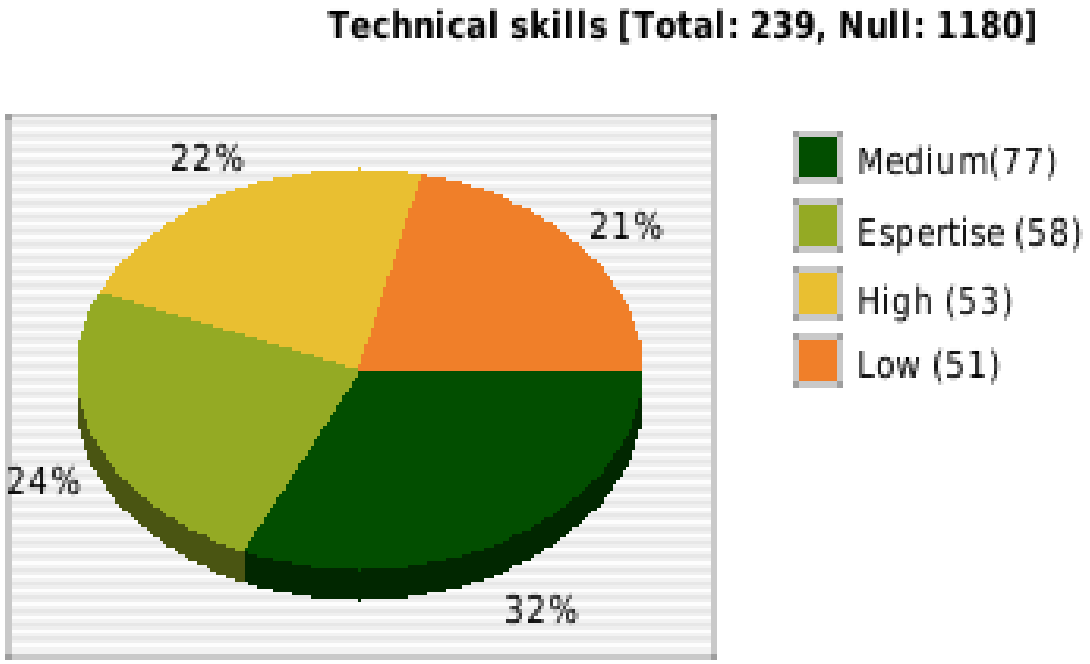



Have you ever practised carding? [Total: 201, Null: 1182]
12%
88%
No (176)
Yes (25)

The Hackers Profiling Project (HPP)

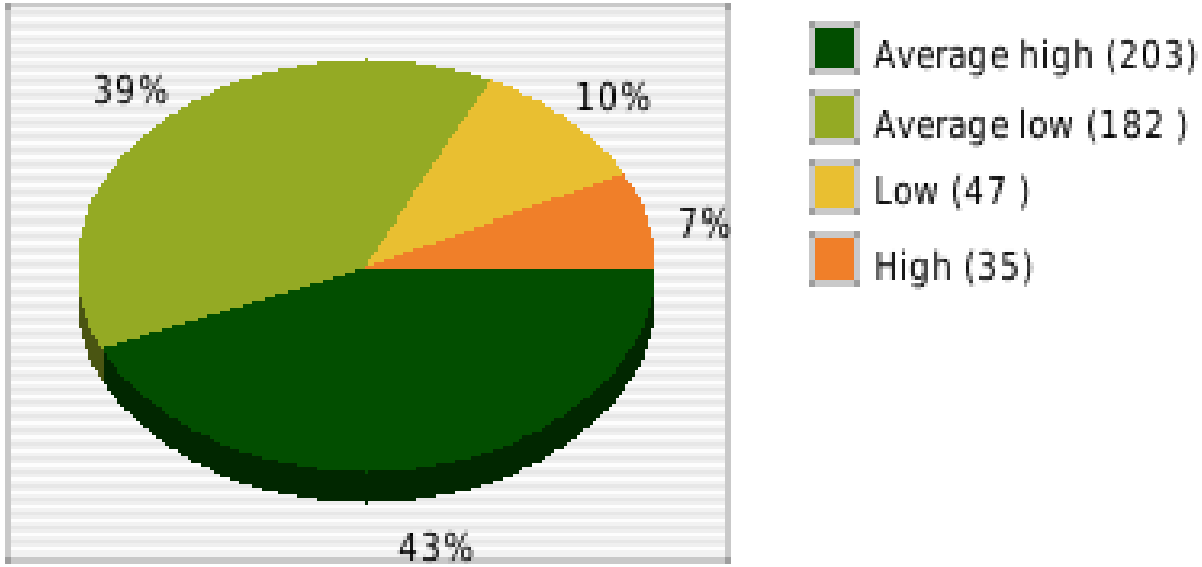
unicri
advancing security, serving justice, building peace




Technical skills [Total: 239, Null: 1180]
22%
21%
24%
32%
Medium(77)
Espertise (58)
High (53)
Low (51)

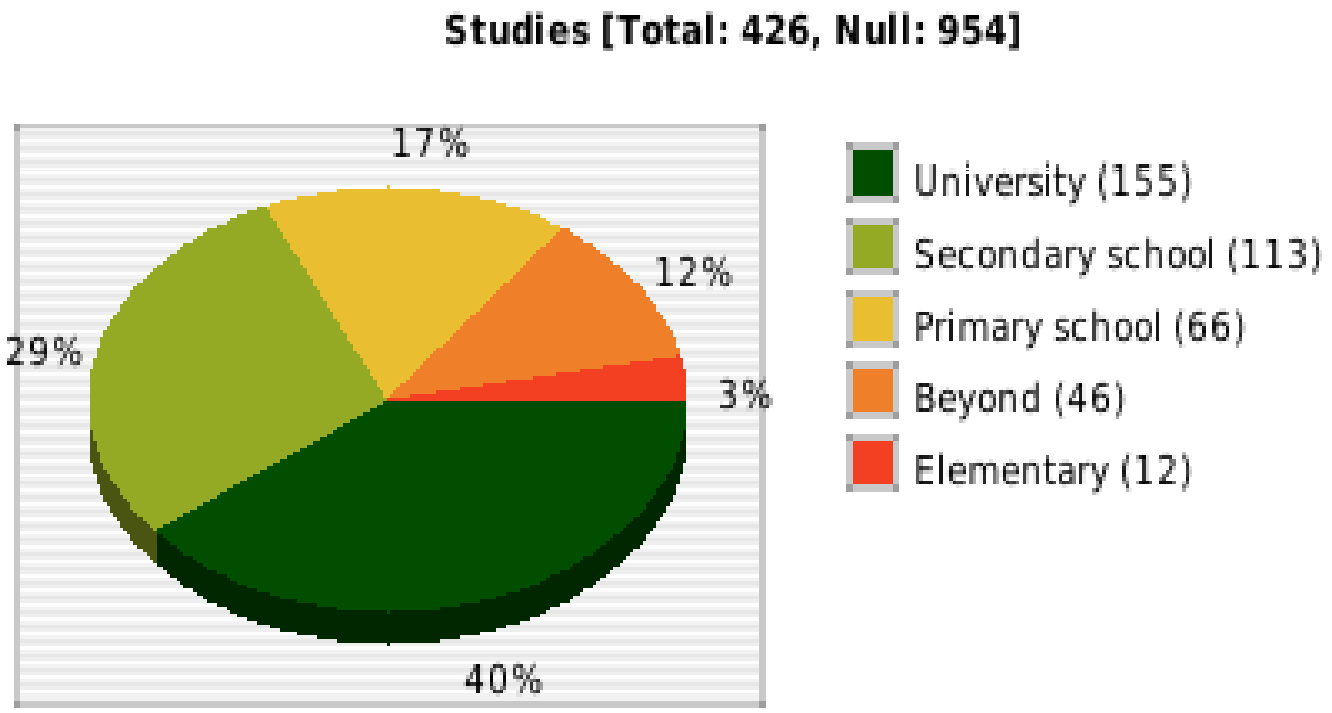
The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace



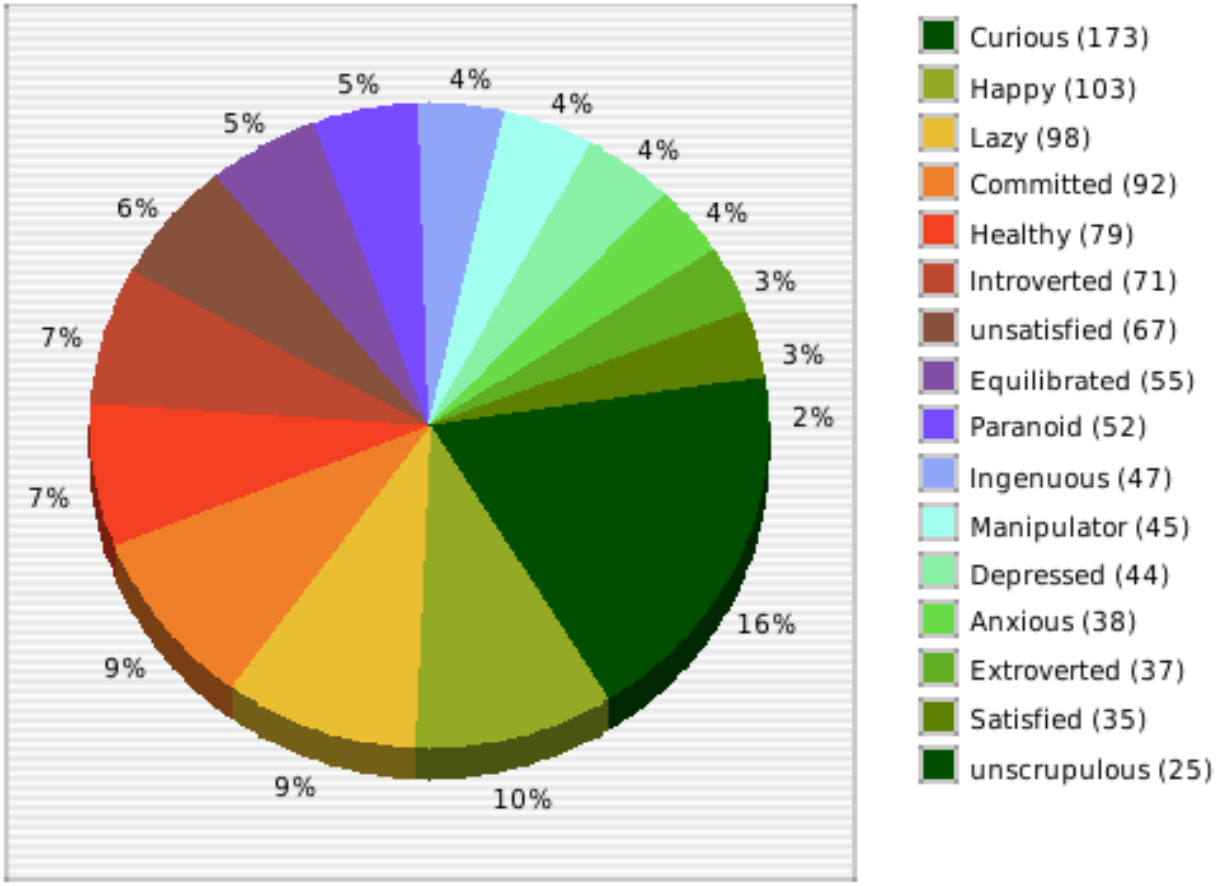
The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace



The Hackers Profiling Project (HPP)

unicri
advancing security, serving justice, building peace



unicri
advancing security, serving justice, building peace

Agenda

- ✓ UNICRI & ISECOM
- ✓ Cybercrime
- ✓ Profiling the enemy
- ✓ Hackers…
- ✓ The Hackers Profiling Project
- ✓ Correlation of the profiles
- ✓ Some stats (hackpies)
- ✓ Conclusions
- ✓ References: books you should read
- ✓ Acknowledgements & Contacts

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 we have been able to reach these results on our own (5 people), imagine what we can do by joining your forces and experiences !
- The H.P.P. Project is **open to partnerships.**

Considerations

- **The whole Project** is self-funded and based on independent research methodologies.
- Despite many problems, we have been carrying out the Project since the last **five years**.
- The final methodology will be released under **GNU/FDL** and distributed through ISECOM.
- It is welcome the **interest on our Project** by research centres, public and private institutions, and governmental agencies.
- We think that we are elaborating something **beautiful**...
- …something that **didn't exist before…**

…something that really seems to **have a sense** ! :)

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

unicri
advancing security, serving justice, building peace

Agenda

- ✓ UNICRI & ISECOM
- ✓ Cybercrime
- ✓ Profiling the enemy
- ✓ Hackers…
- ✓ The Hackers Profiling Project
- ✓ Correlation of the profiles
- ✓ Some stats (hackpies)
- ✓ Conclusions
- ✓ References: books you should read
- ✓ Acknowledgements & Contacts

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 2005-2009**
- **Stealing the Network: How to 0wn a Continent, an Identity, a Shadow** (V.A.), Syngress Publishing, 2004, 2006, 2007
- **Stealing the Network: How to 0wn the Box**, (V.A.), 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 & Joshua Quinttner, Harpercollins, 1995
- **Kevin Poulsen, Serial Hacker**, Jonathan Littman, Little & Brown, 1997
- **Takedown**, John Markoff and 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 & William L. Simon, Wiley, 2002
- **The Art of Intrusion**, Kevin D. Mitnick & William L. Simon, Wiley, 2004
- **@ Large: the Strange Case of the World's Biggest Internet Invasion**, Charles Mann & David Freedman, Touchstone, 1998

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)

The Estonia attack: Battling Botnets and online Mobs, Gadi Evron, 2008 (white paper)

Who is "n3td3v"?, by Hacker Factor Solutions, 2006 (white paper)

Mafiaboy: How I cracked the Internet and Why it's still broken, Michael Calce with Craig Silverman, 2008

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

Cyber Adversary Characterization: auditing the hacker mind, Tom Parker, Syngress, 2004

Inside the SPAM Cartel: trade secrets from the Dark Side, by Spammer X, Syngress, 2004

Hacker Cracker, Ejovu Nuwere with David Chanoff, Harper Collins, 2002

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

Malicious Hackers: a framework for Analysis and Case Study, Laura J. Kleen, Captain, USAF, US Air Force Institute of Technology

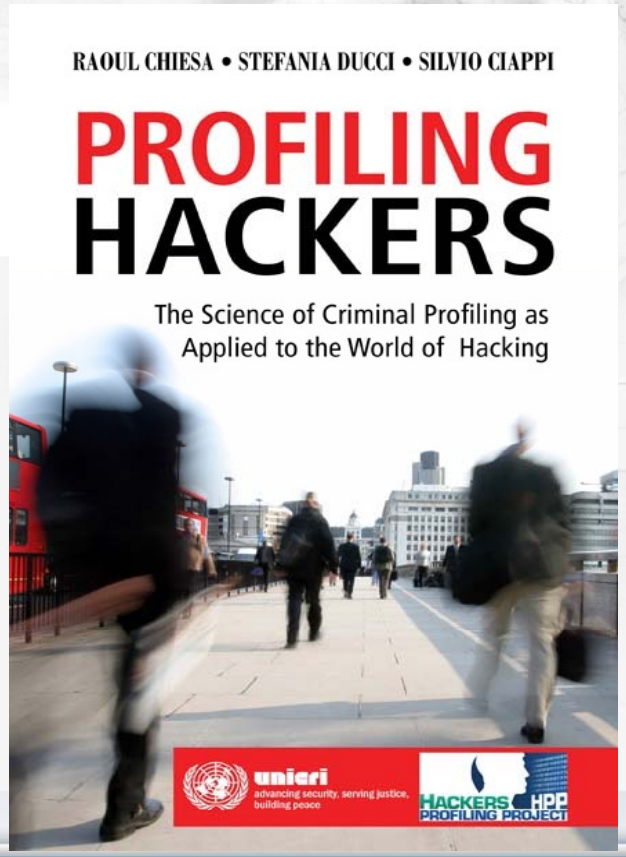
Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology, Täterpro

unicri
advancing security, serving justice, building peace

Biography and References (3)

Profiling Hackers: the Science of Criminal Profiling as applied to the World of Hacking

ISBN: 978-1-4200-8693-5-90000



unicri
advancing security, serving justice, building peace

Contacts, Q&A

Raoul Chiesa

chiesa@UNICRI.it

HPP home page:
http://www.isecom.org/hpp

HPP questionnaires:
http://hpp.recursiva.org

http://www.unicri.it

UNICRI's cybercrime home page:
http://www.unicri.it/wwd/cyber_crime/index.php

Thank you
for your attention

Extra Material

Overview of HPP Training Course

UNICRI offers a unique glimpse into the motivations and lifestyles of hackers with modular HPP Training Courses:

- ✓ Offered in basic (3 days), average (5 days) and advanced (5 days, very in-depth) modules,
- ✓ Covers a wide breadth: basic criminal profiling science, history of the "underground", what motivates hackers, what makes them select specific targets, their "careers" and ethics, deterrents, analysis of the Hackers Profiling book and the questionnaire results, etc…
- ✓ Includes **special guests**: real ethical hackers and their stories.

unicri
advancing security, serving justice, building peace

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

Correlation standards

Gender and age group
Background and place of residence
How hackers view themselves
Family background
Socio-economic background
Social relationships
Leisure activities
Education
Professional environment
Psychological traits
To be or to appear: the level of self-esteem
Presence of multiple personalities
Psychophysical conditions
Alcohol & drug abuse and dependencies
Definition or self-definition: what is a real hacker?
Relationship data
Handle and nickname
Starting age
Learning and training modalities
The mentor's role
Technical capacities (know-how)
Hacking, phreaking or carding: the reasons behind the choice
Networks, technologies and operating systems
Techniques used to penetrate a system

Individual and group attacks
The art of war: examples of attack techniques
Operating inside a target system
The hacker's signature
Relationships with the System Administrators
Motivations
The power trip
Lone hackers
Hacker groups
Favourite targets and reasons
Specializations
Principles of the Hacker Ethics
Acceptance or refusal of the Hacker Ethics
Crashed systems
Hacking/phreaking addiction
Perception of the illegality of their actions
Offences perpetrated with the aid of IT devices
Offences perpetrated without the use of IT devices
Fear of discovery, arrest and conviction
The law as deterrent
Effect of convictions
Leaving the hacker scene
Beyond hacking