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
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...
### 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)
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
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

1. **Analyse the hacking phenomenon in its several aspects (technological, social, economic) through technical and criminological approaches**

2. **Understand the different motivations and identify the actors involved**

3. **Observe those *true* criminal actions “in the field”**

4. **Apply the profiling methodology to collected data (4W: who, where, when, why)**

5. **Acquire and disseminate knowledge**
The Hackers Profiling Project (HPP)

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

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

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
The Hackers Profiling Project (HPP)

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:

#### 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.

### 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
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.
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
The Hackers Profiling Project (HPP)

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

Hacking career
- Principles of the hacker’s ethics

Motivations
- Crashed or damaged systems

Selected targets
- Perception of the illegality of their own activity

Relationship between motivations and targets
- Effect of laws, convictions and technical difficulties as a deterrent
The Hackers Profiling Project (HPP)

Level of technical skills

- Wannabe Lamer
  Script Kiddie

 + Cracker
  Ethical hacker
  Q.P.S. Hacker
  Cyber-Warrior
  Industrial spy
  Government Agent
  Military Hacker
The Hackers Profiling Project (HPP)

Degree of danger

- Wannabe Lamer  Script Kiddie  Ethical Hacker  Q.P.S. Hacker
+ Cracker  Cyber-Warrior  Industrial spy  Government Agent  Military Hacker
# The Hackers Profiling Project (HPP)

## Detailed analysis and correlation of profiles – table #1

<table>
<thead>
<tr>
<th>PROFILE</th>
<th>RANK</th>
<th>IMPACT LEVEL</th>
<th>TARGET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wanna Be Lamer</td>
<td>Amateur</td>
<td>NULL</td>
<td>End-User</td>
</tr>
<tr>
<td>Script Kiddie</td>
<td></td>
<td>LOW</td>
<td>SME</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specific security flaws</td>
</tr>
<tr>
<td>Cracker</td>
<td>Hobbiest</td>
<td>MEDIUM, HIGH</td>
<td>Business company</td>
</tr>
<tr>
<td>Ethical Hacker</td>
<td></td>
<td>MEDIUM</td>
<td>Vendor</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Technology</td>
</tr>
<tr>
<td>Quiet, Paranoid Skilled Hacker</td>
<td></td>
<td>MEDIUM, HIGH</td>
<td>On necessity</td>
</tr>
<tr>
<td>Cyber-Warrior</td>
<td></td>
<td>HIGH</td>
<td>“Symbol” business company</td>
</tr>
<tr>
<td>Industrial Spy</td>
<td></td>
<td>HIGH</td>
<td>Business company</td>
</tr>
<tr>
<td></td>
<td>Professional</td>
<td></td>
<td>Corporation</td>
</tr>
<tr>
<td>Government agent</td>
<td></td>
<td>HIGH</td>
<td>Government</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Suspected Terrorist</td>
</tr>
<tr>
<td>Military Hacker</td>
<td></td>
<td>HIGH</td>
<td>Government</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Strategic Company</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Individual</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Strategic Company</td>
</tr>
</tbody>
</table>
## Detailed analysis and correlation of profiles – table #2

<table>
<thead>
<tr>
<th>OFFENDER ID</th>
<th>LONE / GROUP HACKER</th>
<th>TARGET</th>
<th>MOTIVATIONS / PURPOSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wanna Be Lamer</td>
<td>GROUP</td>
<td>End-User</td>
<td>For fashion, It's “cool” =&gt; to boast and brag</td>
</tr>
<tr>
<td>Script Kiddie</td>
<td>GROUP: but they act alone</td>
<td>SME / Specific security flaws</td>
<td>To give vent of their anger / attract mass-media attention</td>
</tr>
<tr>
<td>Cracker</td>
<td>LONE</td>
<td>Business company</td>
<td>To demonstrate their power / attract mass-media attention</td>
</tr>
<tr>
<td>Ethical Hacker</td>
<td>LONE / GROUP (only for fun)</td>
<td>Vendor / Technology</td>
<td>For curiosity (to learn) and altruistic purposes</td>
</tr>
<tr>
<td>Quiet, Paranoid, Skilled Hacker</td>
<td>LONE</td>
<td>On necessity</td>
<td>For curiosity (to learn) =&gt; egoistic purposes</td>
</tr>
<tr>
<td>Cyber-Warrior</td>
<td>LONE</td>
<td>“Symbol” business company / End-User</td>
<td>For profit</td>
</tr>
<tr>
<td>Industrial Spy</td>
<td>LONE</td>
<td>Business company / Corporation</td>
<td>For profit</td>
</tr>
<tr>
<td>Government Agent</td>
<td>LONE / GROUP</td>
<td>Government / Suspected Terrorist / Strategic company / Individual</td>
<td>Espionage / Counter-espionage / Vulnerability test / Activity-monitoring</td>
</tr>
<tr>
<td>Military Hacker</td>
<td>LONE / GROUP</td>
<td>Government / Strategic company</td>
<td>Monitoring / controlling / crashing systems</td>
</tr>
</tbody>
</table>
## Detailed analysis and correlation of profiles – table #3

<table>
<thead>
<tr>
<th></th>
<th>OBEDIENCE TO THE “HACKER ETHICS”</th>
<th>CRASHED / DAMAGED SYSTEMS</th>
<th>PERCEPTION OF THE ILLEGALITY OF THEIR OWN ACTIVITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wanna Be Lamer</td>
<td>NO: they don’t know “Hacker Ethics” principles</td>
<td>YES: voluntarily or not (inexperience, lack of technical skills)</td>
<td>YES: but they think they will never be caught</td>
</tr>
<tr>
<td>Script Kiddie</td>
<td>NO: they create their own ethics</td>
<td>NO: but they delete / modify data</td>
<td>YES: but they justify their actions</td>
</tr>
<tr>
<td>Cracker</td>
<td>NO: for them the “Hacker Ethics” doesn’t exist</td>
<td>YES: always voluntarily</td>
<td>YES but: MORAL DISCHARGE</td>
</tr>
<tr>
<td>Ethical Hacker</td>
<td>YES: they defend it</td>
<td>NEVER: it could happen only incidentally</td>
<td>YES: but they consider their activity morally acceptable</td>
</tr>
<tr>
<td>Quiet, Paranoid, Skilled Hacker</td>
<td>NO: they have their own personal ethics, often similar to the “Hacker Ethics”</td>
<td>NO</td>
<td>YES: they feel guilty for the upset caused to SysAdmins and victims</td>
</tr>
<tr>
<td>Cyber-Warrior</td>
<td>NO</td>
<td>YES: they also delete/modify/steal and sell data</td>
<td>YES: but they are without scruple</td>
</tr>
<tr>
<td>Industrial Spy</td>
<td>NO: but they follow some unwritten “professional” rules</td>
<td>NO: they only steal and sell data</td>
<td>YES: but they are without scruple</td>
</tr>
<tr>
<td>Government Agent</td>
<td>NO: they betray the “Hacker Ethics”</td>
<td>YES (including deleting/modifying/stealing data) / NO (in stealth attacks)</td>
<td></td>
</tr>
<tr>
<td>Military Hacker</td>
<td>NO: they betray the “Hacker Ethics”</td>
<td>YES (including deleting/modifying/stealing data) / NO (in stealth attacks)</td>
<td></td>
</tr>
</tbody>
</table>
## Detailed analysis and correlation of profiles – table #4

<table>
<thead>
<tr>
<th>DETERRENCE EFFECT OF:</th>
<th>LAWS</th>
<th>CONVICTIONS SUFFERED BY OTHER HACKERS</th>
<th>CONVICTIONS SUFFERED BY THEM</th>
<th>TECHNICAL DIFFICULTIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wanna Be Lamer</td>
<td>NULL</td>
<td>NULL</td>
<td>ALMOST NULL</td>
<td>HIGH</td>
</tr>
<tr>
<td>Script Kiddie</td>
<td>NULL</td>
<td>NULL</td>
<td></td>
<td>HIGH: they stop after the 1st conviction</td>
</tr>
<tr>
<td>Cracker</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>Ethical Hacker</td>
<td>NULL</td>
<td>NULL</td>
<td>HIGH: they stop after the 1st conviction</td>
<td>NULL</td>
</tr>
<tr>
<td>Quiet, Paranoid, Skilled Hacker</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
</tr>
<tr>
<td>Cyber-Warrior</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL: they do it as a job</td>
</tr>
<tr>
<td>Industrial Spy</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL</td>
<td>NULL: they do it as a job</td>
</tr>
</tbody>
</table>
Age [Total: 471, Null: 915]

- 30% above 45
- 29% 41-45
- 7% 35-40
- 3% 41-45
- 3% 31-34
- 3% 26-30
- 21% 21-25
- 10% 20
Age that you started with hacking [Total: 171, Null: 1212]

- 10% 15 (101)
- 16% 20 (49)
- 21% 25 (10)
- 26% 30 (4)
- More than 40 (1)
- 31% 34 (0)
- 35% 40 (0)
Have you ever practised carding? [Total: 201, Null: 1182]

- No (176) [88%]
- Yes (25) [12%]
Where do you live?

- Big town (215 / 470 / 916)
- Small town (164 / 470 / 916)
- Country (91 / 470 / 916)
Technical skills [Total: 239, Null: 1180]

- Medium (77): 32%
- Expertise (58): 24%
- High (53): 22%
- Low (51): 21%
socio-economic status [Totals: 467, Null: 919]

- **Average high (203)**
- **Average low (182)**
- **Low (47)**
- **High (35)**
Studies [Total: 426, Null: 954]

- University (155)
- Secondary school (113)
- Primary school (66)
- Beyond (46)
- Elementary (12)
Personalities

- Curious (173)
- Happy (103)
- Lazy (98)
- Committed (92)
- Healthy (79)
- Introverted (71)
- Unsatisfied (67)
- Equilibrated (55)
- Paranoid (52)
- Ingenious (47)
- Manipulator (45)
- Depressed (44)
- Anxious (38)
- Extroverted (37)
- Satisfied (35)
- Unscrupulous (25)
The Hackers Profiling Project (HPP)

Are hackers terrorists?

The Threat is Increasing

Source: 1997 DSB Summer Study
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
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.

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.
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 Own a Continent**, (AA.VV), Syngress Publishing, 2004
- **Stealing the Network: How to Own the Box**, (AA.VV.), Syngress Publishing, 2003
- **The Fugitive Game: online with Kevin Mitnick**, Jonathan Littman, Little & Brown, 1997
- **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
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
- **Criminal Profiling Research Site. Scientific Offender Profiling Resource in Switzerland. Criminology, Law, Psychology**, Täterpro
The H.P.P. Project's Authors would like to thank 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), BellUA, Telecom Security Task Force, Phrack, 2600 Magazine, Xcon/Xfocus Team, CONfidence.

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


**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.
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

Thank you  
for your attention
The Hackers Profiling Project (HPP)

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

QUESTIONS?
www.unicri.it