

The H word

About hacking, and therefore... hackers

A humble attempt by Pierre 'khorben' Pronchery,
Olivier 'zitune' André & Serge 'praagma' Humpich
from Bearstech, France

For Microsoft France, September 11th 2009



bearstech

--=(DISCLAIMER)=--

The definition of hacking and hackers is highly subjective. I do not even remotely pretend to be in a good position to tell you about it. However, I'll let you know my perception of the different ways that some may indeed claim to be one, or have been called this way.

Etymology ...and misconceptions

- Not universally approved, but something about chopping wood with an axe
- By extension, the technical aspect: its “kung-fu”
- In the computer world, a creative mind, often a programmer
- For the media, the bad guys who break into machines for profit

...who's right?

It doesn't matter

Let's focus on:

- 1.The culture
- 2.The programmers
- 3.The “bad guys”

In the culture

- 1960s, MIT:
 - MIT Tech Model Railroad Club, Artificial Intelligence Laboratory
 - Free Software movement
 - Hobbyist home computing community, Homebrew Computer Club: Steve Jobs, Steve Wozniak and Bill Gates
 - Internet and the World Wide Web

In the culture

- 1983, WarGames:
 - Hollywood thriller
 - Ally Sheedy as Jennifer Katherine Mack
 - Still draws a cult



In the culture

- 1983, Cyberpunk by Bruce Bethke:
 - Science-fiction legacy
 - Isaac Asimov
 - William Gibson
 - Neil Stephenson...



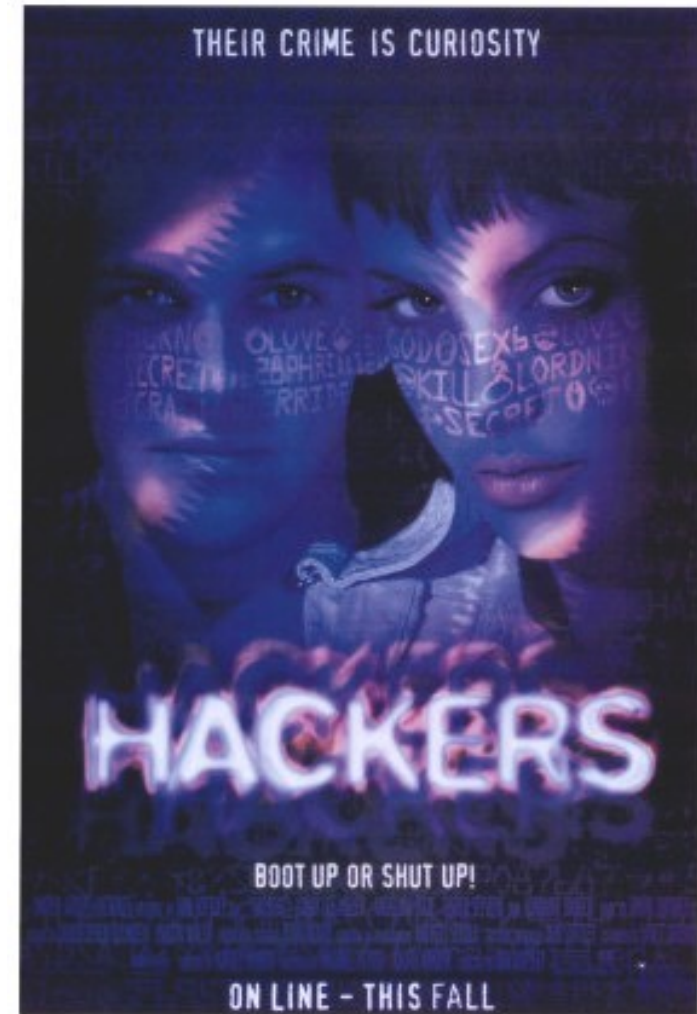
In the culture

- **January 1993: RFC 1392**

A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where "cracker" would be the correct term.

In the culture

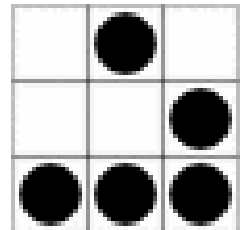
- 1995, Hackers:
 - Hollywood thriller
 - Angelina Jolie
 - *“Their crime is curiosity”*
 - Quite extravagant and inaccurate
 - Still a cult



In the culture

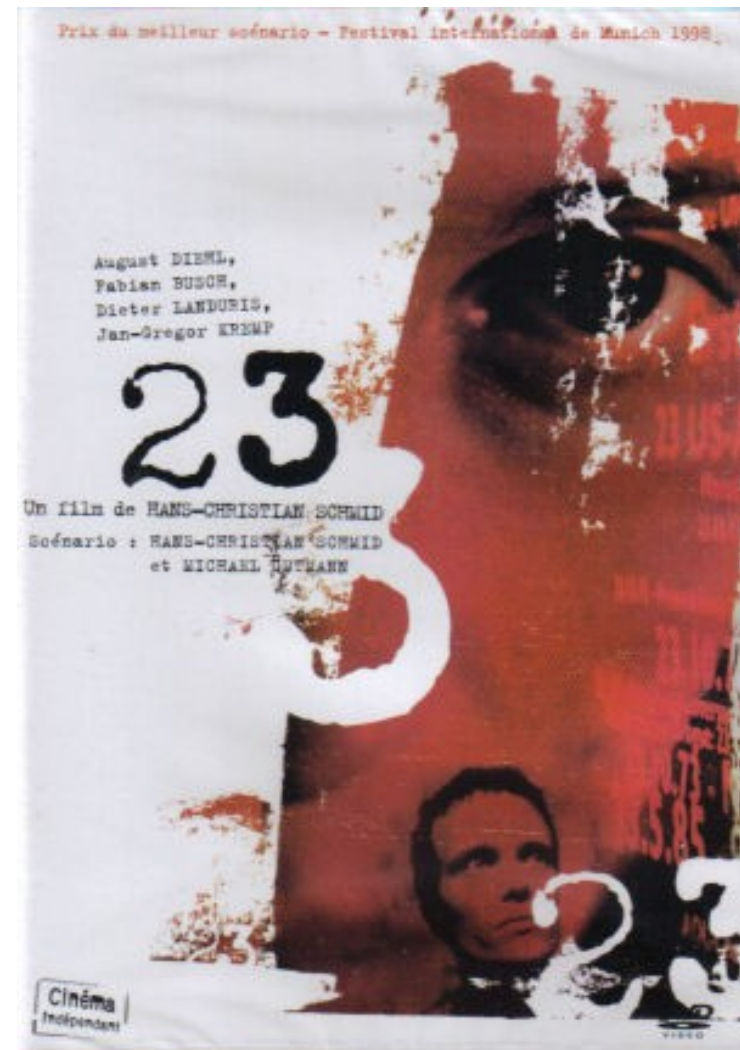
- **1996, Eric S Raymond:**

Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers run Usenet. Hackers make the World Wide Web work. If you are part of this culture, if you have contributed to it and other people in it know who you are and call you a hacker, you're a hacker.



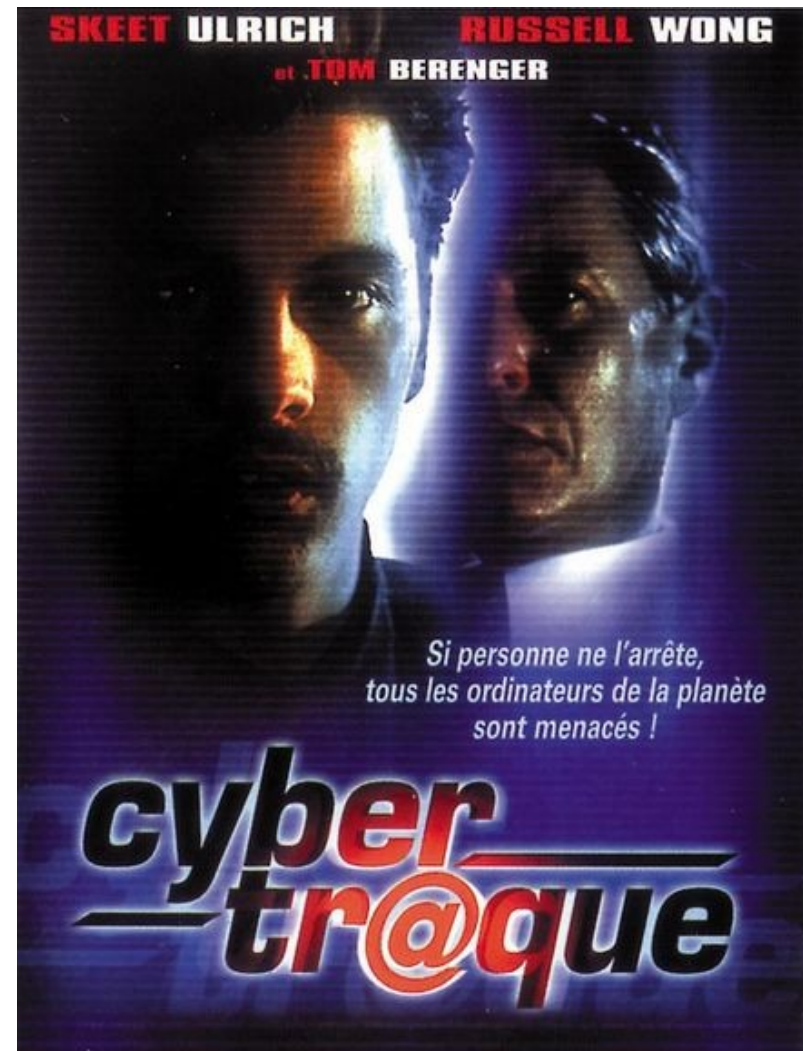
In the culture

- 1998, 23:
 - German movie
 - Story of Karl Koch
 - KGB, Chaos Computer Club...
 - Much more revealing



In the culture

- 2000, Takedown:
 - Hollywood thriller
 - Kevin Mitnick
 - Inaccurate about his real story
 - Interesting for the facts and mind-set



In the culture

- 2001, Antitrust:
 - SCNR!
 - Hollywood thriller
 - Ryan Phillippe
 - “entertaining”



In the culture

- 2001, Operation Swordfish:
 - Yet another Hollywood thriller
 - Halle Berry and John Travolta
 - Mostly fantasy



In the culture

- More movies:
 - Jurassic park's "I know this, it's UNIX" by a little girl,
 - Enemy of the state,
 - The Matrix trilogy, featuring nmap and SSH
 - Die Hard 4...
- Manga animes:
 - Ghost in the shell, Lain...
- More books...

The programmers

Famous examples:

- Richard Stallman (GNU)
- Linus Torvalds (Linux)
- Alan Cox (Linux)
- Miguel de Icaza (GNOME)
- Theo de Raadt (OpenBSD)
- Andrew Doran (NetBSD)

Sharing knowledge

- Scientific approach (OK, not really)
- Intuition matters
- Open Source, copyleft...
- Sort of a meritocracy: you are called a hacker by your fellow hackers
- You've certainly heard about most of this
- It can be boring so let's skip it :)

The “bad guys”

- From fun to organized crime
- The underground
- The scene
- The color of your hat
- The security industry...

A starting point

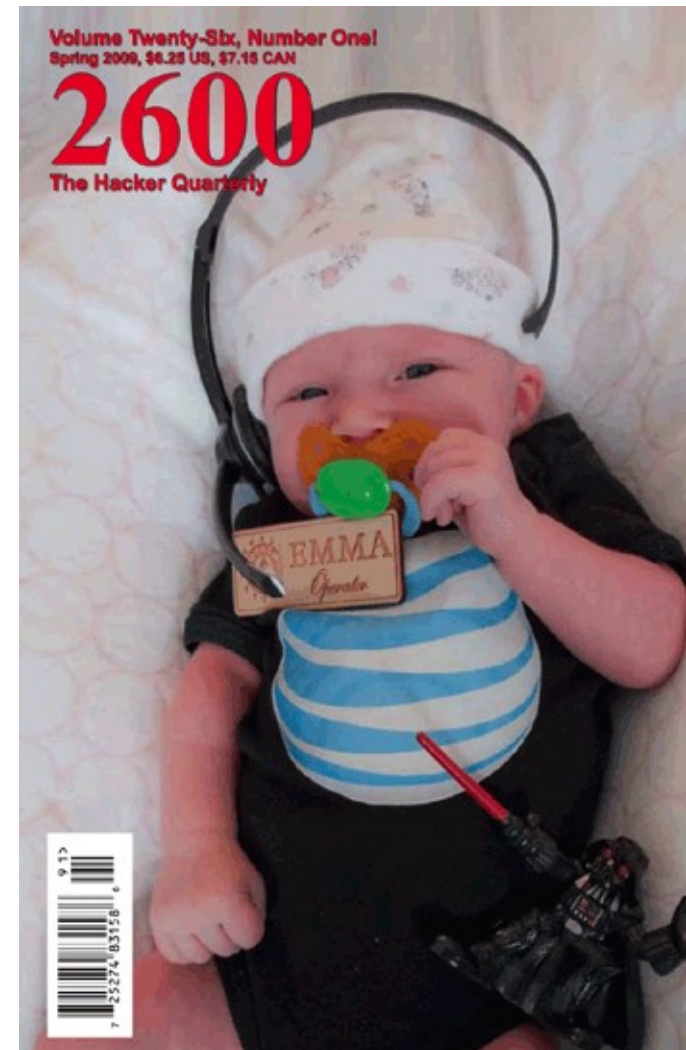
- John Draper AKA Captain Crunch
- Devising access to a local telephone switchboard ...with a cereal box gift
- A toy whistle packaged in Cap'n Crunch cereal emitted a tone at 2600 Hz—the frequency used by AT&T to indicate that lines were ready to route a new call
- Creation of the Blue Box, many followed...
- Then acquainted to... Steve Wozniak and Steve Jobs

Phreaking

- Subculture for the study, experimentation or exploration of telecommunication systems, like the public phone networks
- Early occurrence of unauthorized access through electronic means
- Originally for fun and (mild) personal gain: calling home for free from his military base
- Also among the first hackers caught: sentenced to 5 years probation

2600: The Hacker Quarterly

- Dozens of magazines, or “ezines” appeared on the net
- The surface of the “underground”
- In Europe: CCC, Hacktik...



The underground

- Everything that happens, basically
- Individual and private research
- Network of said researchers, often constituted of “hacker groups”, over IRC, SILC...
- Incidentally, authors of the ezines, like PHRACK and his “Hacker Manifesto”, or “Smashing The Stack For Fun And Profit”

Physical security

- Phreaking becomes closer to computer hacking as the infrastructure gets more complex
- Network security relies on medium access
- Other fields of hacking worth mentioning:
 - Lockpicking
 - Tempest
 - Tapping...
- And then it reaches software...

Software security

Injecting code or otherwise acquire privileges through:

- Buffer overflows, or memory corruption:
 - Stack smashing
 - Heap overflow
 - Off by one byte can be enough!
- Format strings
- Integer overflows
- Uninitialized pointers...

More software security

For proprietary software:

- Cracking
- Serial numbers

As tools get easier to access:

- A crowd of “script-kiddies”
- Emergence of the “scene”
- Things are getting serious...

The security industry

- Money is in the balance:
 - Companies are interconnected
 - Networks and software are vulnerable
- The black art becomes a business:
 - Security consulting
 - Network pentests
 - Source code audits
 - Black-box testing
- Hackers can be hired

The color of your hat

- Security researchers, the “good guys”, are called “white hats”
- Crackers and “bad guys” alike, are called “black hats”
- You'll see many shades of grey



The disclosure dilemma

- Security mailing-lists: Bugtraq, full-disclosure...
- Full disclosure: details of a bug are released directly
- Responsible disclosure: bugs are submitted upstream, the fix and updates coordinated with the vendor
- No disclosure: hacking as a black art

War is on

- The “white hats” (or otherwise disclosers) break the tools of the “black hats”
- The “black hats” retaliate by exposing the “white hats”
- Hacking used against hackers (PayTV...)
- Political and religious wars
- Information and economical warfare...

The scene

- Some (truly skilled) people sharing their work and ideas
- Some looking for fame
- Companies prospecting customers
- Many stories: some funny, some scary, some impressive, some pitiful, some really good
- Picture a circus :)

Deception techniques

- Social-engineering, powered by:
 - Trashing
 - Information warfare and exposed privacy
- Brute-force attacks, thanks to:
 - Weak passwords, keys or design
 - Validation errors...
- Distributed Denial Of Service
 - Kidnapping and taking down entire networks
- Spam, phishing...

More engineering

Reverse-engineering:

- Network protocols
interpreting data exchange
- Firmware images
backdoors, signatures, bugs...
- Software in general
also cracking, checking updates...

Many other ways to hack...

- Anything creative, really
- Hardware hacking is increasingly popular: make, hackaday, hackcenters...
- We'll be contributing soon with “hackable:Devices”
- Follow-up about hardware security :)