Introduction to the security of ICT systems

Antonio Lioy
< lioy @ polito.it >

Politecnico di Torino
Dip. Automatica e Informatica

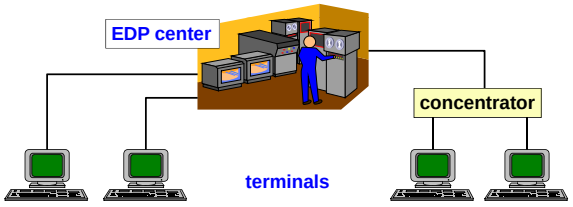
Agenda

- **introduction to information security:**
  - evolution of ICT systems and the security problem
  - problems and vocabulary of ICT security
  - technological attacks (sniffing, spoofing, …)
  - non-technological attacks (social engineering)

Why security is "hot" today?

Traditional paradigms

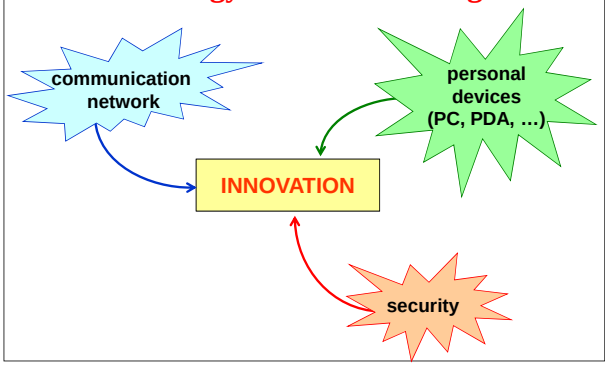
- **centralised information and processing**
- **access to data from "dumb" terminals**
- **"unicast" communication over dedicated lines**



New paradigms

- **distributed information and processing**
- **access from distributed intelligent terminals**
- **"broadcast" communication and/or shared lines**
- **new application paradigms (web, SMS, …)**

Technology as innovation engine



A definition of ICT security

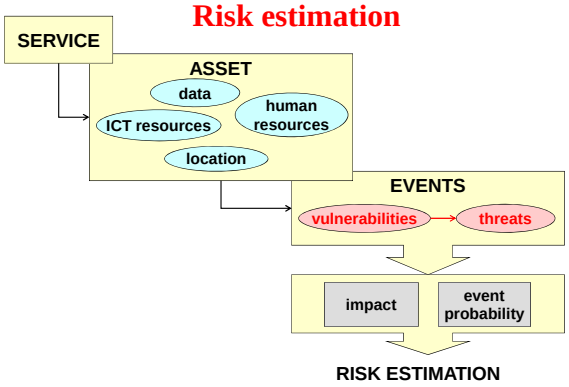
It is the set of products, services, organization rules and individual behaviours that protect the ICT system of a company.

It has the duty to protect the resources from undesired access, guarantee the privacy of information, ensure the service operation and availability in case of unpredictable events (C.I.A. = Confidentiality, Integrity, Availability).

The objective is to guard the information with the same professionalism and attention as for the jewelry and deposit certificates stored in a bank caveau.

The ICT system is the safe of our most valuable information; ICT security is the equivalent of the locks, combinations and keys required to protect it.

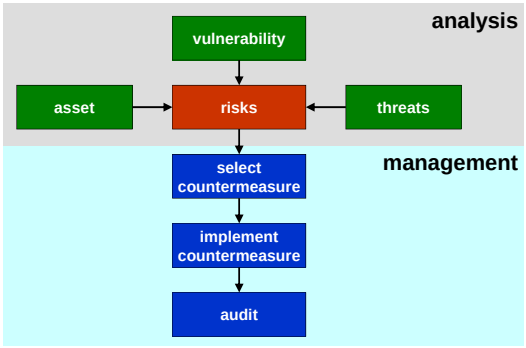
Risk estimation



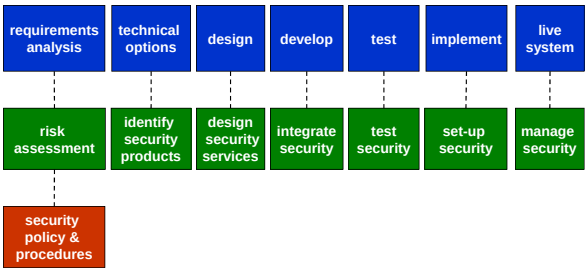
Terms

- ASSET = the set of goods, data and people needed for an IT service
- VULNERABILITY = weakness of an asset
  - e.g. pwd = login; sensible to flooding
- THREAT = deliberate action / accidental event that can produce the loss of a security property exploiting a vulnerability
- ATTACK = threat occurrence (deliberate action)
- (NEGATIVE) EVENT = threat occurrence (accidental event)

Analysis and management of security



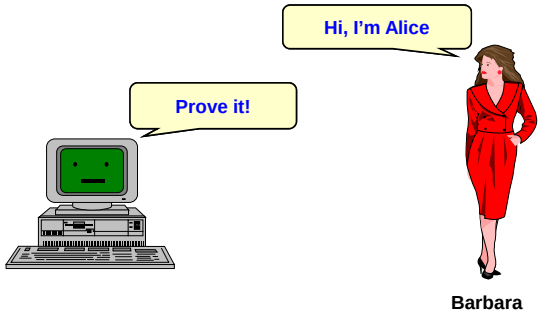
Security in the lifecycle of a system



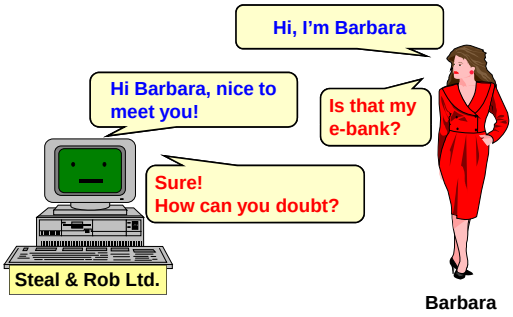
(abstract) security properties

autenticazione (semplice / mutua)	*authentication (simple / mutual)*
autenticazione della controparte	*peer authentication*
autenticazione dei dati	*data / origin authentication*
autorizzazione, controllo accessi	*authorization, access control*
integrità	*integrity*
riservatezza, confidenzialità	*confidentiality, privacy, secrecy*
non ripudio	*non repudiation*
disponibilità	*availability*
tracciabilità	*accountability*

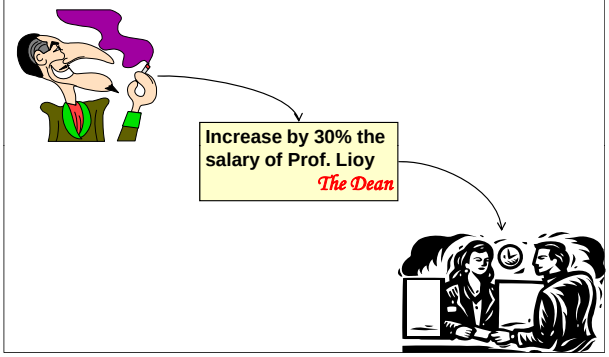
Peer authentication



Mutual peer authentication



Data authentication



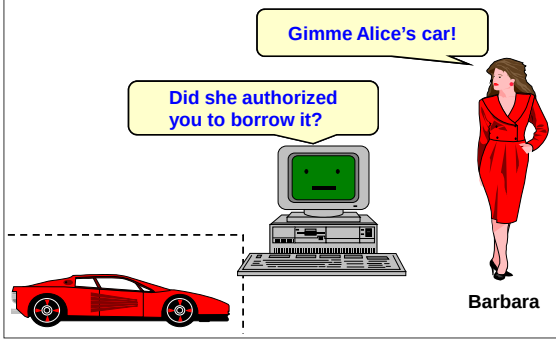
Non repudiation

- **formal proof – acceptable by a court of justice – that gives undeniable evidence of the data creator**
- **several facets:**
  - (sender/author) authentication
  - integrity
  - (sender/author) identification
  - . . .

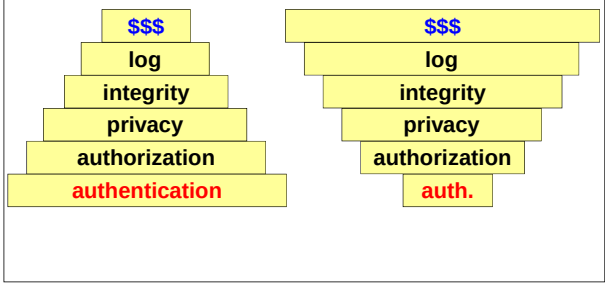
Non repudiation - example

- **let's consider non-repudiation of an electronic signature:**
  - syntax (is that your signature?)
  - semantics (did you understand what you were signing?)
  - will (have you signed voluntarily?)
  - identification (was really YOU the signer?)
  - time (when did you sign?)
  - place (where did you sign?)

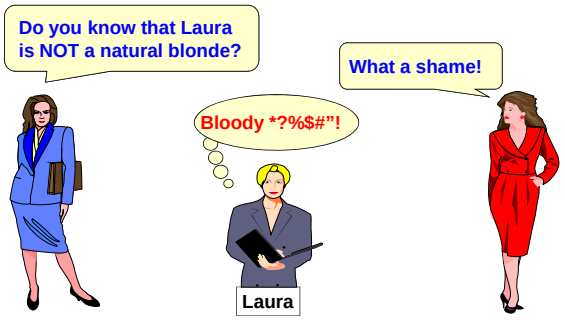
Authorization (access control)



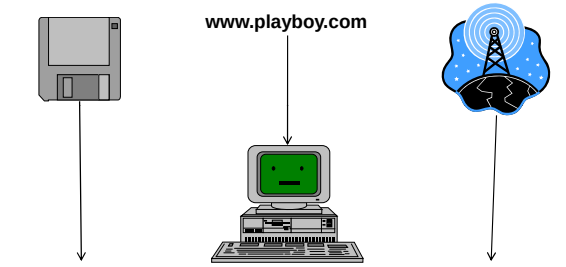
Pyramid of security



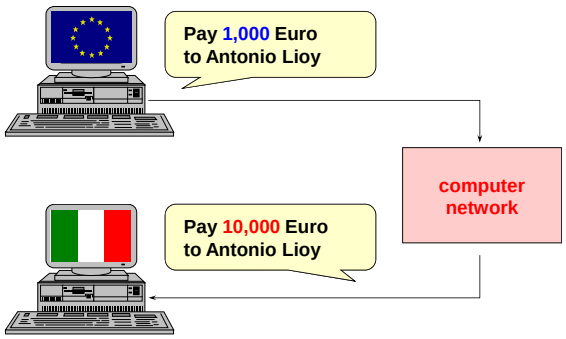
Privacy (communication)



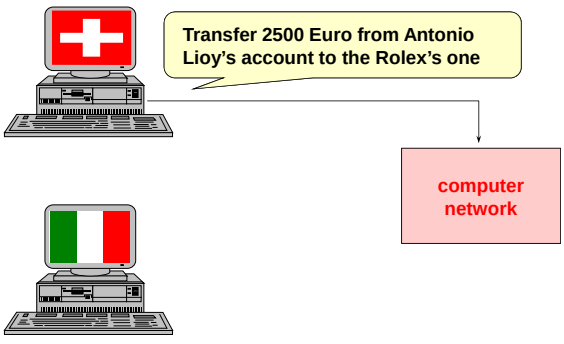
Privacy (data, actions, position)



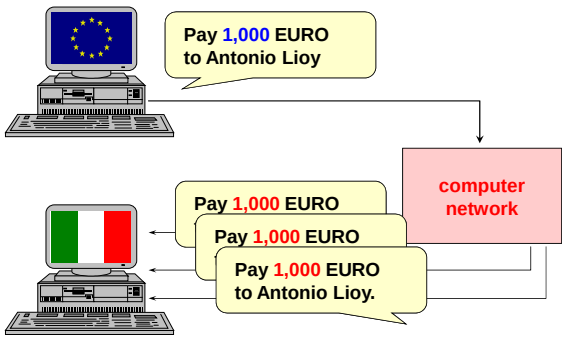
Integrity (data modification)



Integrity (data filtering)

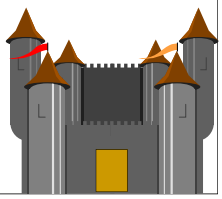


Replay attack



Where is the enemy?

- **outside our organization**
  - boundary / perimeter defense (firewall)
- **outside our organization, with the exception of our partners**
  - Extranet protection (VPN)
- **inside our organization**
  - LAN / Intranet protection (?!)
- **everywhere!**
  - application-level protection



Where does the attack come from? (2006)

- **Internet (50% of the sample)**
- **internal system (50%)**

(from an analysis made by CSI/FBI in 2006 on a sample of 536 USA firms)

Consequences of an attack (2006)

- **virus (65% of sample)**
- **theft of laptop/PDA (47%)**
- **network abuse by insiders (42%)**
- **unauthorized data access by insiders (32%)**
- **denial-of-service (25%)**
- **penetration of systems (15%)**
- **abuse of wireless networks (14%)**
- **theft of sensitive information (9%)**
- **financial frauds (9%)**
- **TLC frauds (8%)**
- **web defacement / web app misuse (6%)**

Stolen laptop / PDA

- **not only an economic loss to replace the stolen device …**
- **but also the loss of data that become unavailable (backup?) …**
- **or the spreading of restricted information**

Scoop of a Global Post reporter in the town between Pakistan and Afghanistan

US PCs sold at the Peshàwar market

Computers of the US army with restricted data sold for 650$ along the road where Nato troops are attacked by the talebans. … Still full of classified informations, such as names, sites, and weak points. (corriere.it, 9/2/09)

Insecurity: the deep roots (I)

- **"Attack technology is developing in a open-source environment and is evolving rapidly"**
- **"Defensive strategies are reactionary"**
- **"Thousands - perhaps millions - of system with weak security are connected to the Internet"**
- **"The explosion in use of the Internet is straining our scarse technical talent. The average level of system administrators … has decreased dramatically in the last 5 years"**

Insecurity: the deep roots (II)

- **"Increasingly complex sw is being written by programmers who have no training in writing secure code"**
- **"Attacks and attack tools trascend geography and national boundaries"**
- **"The difficulty of criminal investigation of cybercrime coupled with the complexity of international law means that … prosecution of computer crime is unlikely"**

from "Roadmap for defeating DDOS attacks" (feb. 2000, after Clinton meeting at White House) updates on www.sans.org/dosstep/roadmap.php

Basic problems (technological)

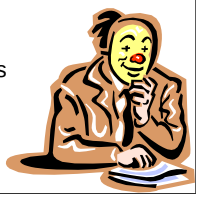
- **the networks are insecure:**
  - (most) communications are made in clear
  - LANs operate in broadcast
  - geographical connections are NOT made through end-to-end dedicated lines but:
    - through shared lines
    - through third-party routers
- **weak user authentication (normally password-based)**
- **there is no server authentication**
- **the software contains many bugs!**

Some classes of attacks

- **IP spoofing / shadow server**
  someone takes the place of a (legitimate) host
- **packet sniffing**
  passwords and/or sensitive data are read by (unauthorized) third parties
- **connection hijacking / data spoofing**
  data inserted / modified during their transmission
- **denial-of-service (distributed DoS)**
  the functionality of a service is limited or disrupted (e.g. ping bombing)

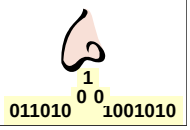
IP spoofing

- **forging the source network address**
- **typically the level 3 (IP) address is forged, but it is equally easy to forge the level 2 address (e.g. ETH, TR, ...)**
- **a better name would be *source address spoofing***
- **attacks:**
  - data forging
  - (unauthorized) access to systems
- **countermeasures:**
  - do NEVER use address-based authentication



Packet sniffing (eavesdropping)

- **reading the packets addressed to another network node**
- **easy to do in broadcast networks (e.g. LAN) or at the switching nodes (e.g. router, switch)**
- **attacks:**
  - allows to intercept anything (password, data, ...)
- **countermeasure:**
  - non- broadcast networks (!?)
  - encryption of packet payload



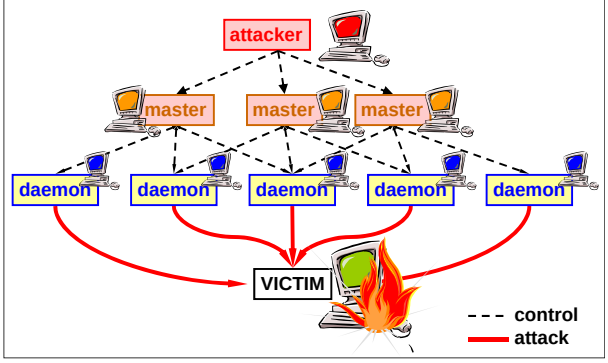
Denial-of-service (DoS)

- **keeping a host busy so that it can't provide its services**
- **examples:**
  - mail / log saturation
  - ping flooding ("ping bombing")
  - SYN attack
- **attacks:**
  - block the use of a system / service
- **countermeasures:**
  - none!
  - monitoring and oversizing can mitigate the effects

Distributed denial-of-service (DDOS)

- **software for DoS installed on many nodes (named daemon, zombie or malbot) to create a Botnet**
- **daemons remotely controlled by a master (often via encrypted channels) and have auto-updating feature**
- **effect of the base DoS attack multiplied by the number of daemons**
- **examples of DDoS attack networks:**
  - TrinOO
  - TFN (Tribe Flood Network)
  - Stacheldraht (=barbed wire)

DDoS attack



Feb 8th 2000, 10.30am (PST) @ Yahoo Server Farm

- **"the initial flood of packets, which we later realized was in excess of 1G bits/sec, took down one of our routers …"**
- **"… after the router recovered we lost all routing to our upstream ISP …"**
- **"… it was somewhat difficult to tell what was going on, but at the very least we noticed lots of ICMP traffic …"**
- **"… at 1.30pm we got basic routing back up and then realized that we were under a DDoS attack"**

http://packetstorm.decepticons.org/distributed/yahoo.txt

The lawyer said ...

"There is a distinct probability that if your site has been hijacked for a denial of service attack, then you could be liable for damages.

I would definitely advise clients they have grounds to sue."

Nick Lockett, e-commerce lawyer at Sidley & Austin

"Be Secure or Be Sued"
Silicon.com, 16 Nov 2000

http://www.silicon.com/a40900

Shadow server

- **host that manages to show itself (to victims) as a service provider without having the right to do so**
- **requires address spoofing and packet sniffing**
- **shadow server must be faster than the real one, or the real one must be unable to respond (due to a failure or because is under attack, e.g. DoS)**
- **attacks:**
  - issue wrong answers, providing thus a "wrong" service to victims instead of the real one
  - capture victim's data provided to the wrong service
- **countermeasures:**
  - server authentication

Connection hijacking

- **also named *data spoofing***
- **attacker takes control of a communication channel to insert, delete, or manipulate the traffic**
- **logical or physical MITM (Man In The Middle)**
- **attacks:**
  - reading, insertion of false data and modification of data exchanged between two parties
- **countermeasure:**
  - authentication, integrity and serialization of each single network packet

Software bug

- **even the best software (either off-the-shelf or custom) contains bugs that can be used for various aims**
- **easiest exploit: DoS**
- **example: WinNT server (3.51, 4.0)**
  - telnet to TCP port 135
  - send 10 random characters, then CR
  - server unavailable! (CPU load at 100% even though no useful work is done)
  - solution: install SP3

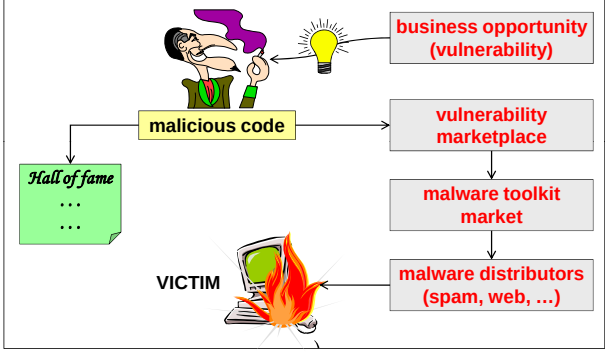
Some typical application-level problems

- **buffer overflow**
  - allows the execution of arbitrary code injected through a specially crafted input
- **store sensible information in the cookies**
  - readable by third parties (in transit o locally on the client)
- **store passwords in clear in a DB**
  - readable by third parties (e.g. backup operator)
- **"invent" a protection system**
  - risk of inadequate protection

Virus and worm (malware)

- **virus = does damage then replicates itself**
- **worm = does damage because replicates itself**
- **requires complicity (may be involuntary) from:**
  - the user (gratis, free, urgent, important, …)
  - the sys manager (wrong configuration)
  - the producer (automatic execution, trusted, …)
- **countermeasures:**
  - user awareness
  - correct configuration / secure sw
  - install antivirus (and keep updated!)

Malware food chain



Basic problems (non technological)

- **low problem understanding (awareness)**
- **mistakes of human beings (especially when overloaded, stressed, …)**
- **human beings have a natural tendency to trust**
- **complex interfaces / architectures can mislead the user and originate erroneous behaviours**
- **performance decrease due to the application of security measures**
- **…**

Social engineering

- **ask for the (involuntary) user's partecipation to the attack action**
- **usually naive users are targeted (e.g. "do change immediately your password with the following one, because your PC is under attack") ...**
- **… but experienced users are targeted too (e.g. by copying an authentic mail but changing its attachment or URL)**
- **via mail, phone or even paper**

Social engineering: examples

- **phishing (~ fishing):**
  - "dear Internet banking user, please fill in the attached module and return it to us ASAP according to the privacy law 675 …"
- **psychological pressure:**
  - "help me, otherwise I'll be in troubles …"
  - "do it, or I'll report it to your boss …"
- **showing acquaintance with the company's procedures, habits and personnel helps in gaining trust and make the target lower his defenses**

A mail from CIA …

```
From: Post@cia.gov
Date: Tue, 22 Nov 2005 17:51:14 UTC
X-Original-Message-ID: <1e3c8.15d13bbb95@cia.gov>
Subject: You_visit_illegal_websites

Dear Sir/Madam,
we have logged your IP-address on more than 30 illegal Websites.
Important: Please answer our questions!
The list of questions are attached.

Yours faithfully,
Steven Allison

++++ Central Intelligence Agency -CIA-
++++ Office of Public Affairs
++++ Washington, D.C. 20505
++++ phone: (703) 482-0623
++++ 7:00 a.m. to 5:00 p.m., US Eastern time
```

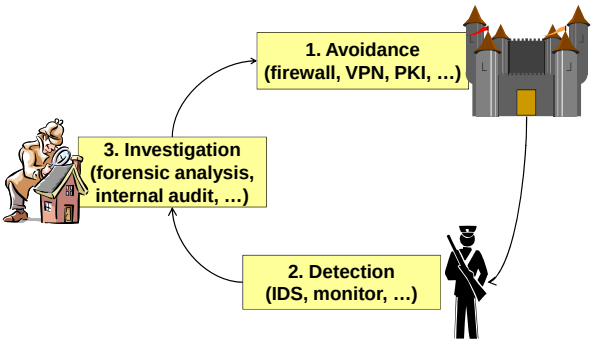
Phishing

- **using mail or IM to attract a network service user to a fake server (shadow server) for:**
  - acquiring her authentication credentials or other peronal information
  - persuading her to install a plugin or extension which actually is a virus or a trojan
- **specialized variants:**
  - spear phishing (include several personal data to disguise the fake messagge as a good one, e.g. mail address, name of Dept/Office, phone no.)
  - whaling (targeted to VIP such as CEO or CIO, e.g. the 20,000 hit on april 08 that then installed a trojan related to the servers of Piradius)

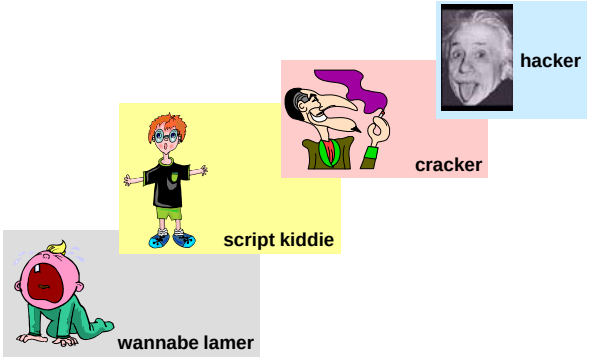
Pharming

- **term of controversial use**
- **set of several tecnicquea to re-direct an user towards a shadow server**
  - changing the "host" file at the client
  - changing the nameserver pointers at the client
  - changing the nameservers at a DHCP server (e.g. an ADSL / wireless router)
  - poisoning the cache of a nameserver
- **via:**
  - direct attack (vulnerability or malconfiguration)
  - indirect attack (virus or worm)

The three pillars of security



Hacker & C.



Hacker (I)

hacker: /n./ [originally, someone who makes furniture with an axe]

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.

2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.

3. A person capable of appreciating {hack value}.

4. A person who is good at programming quickly.

Hacker (II)

5. An expert at a particular program, or one who frequently does work using it or on it; as in "a Unix hacker". (Definitions 1 through 5 are correlated, and people who fit them congregate.)

6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.

7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.

8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence "password hacker", "network hacker". The correct term for this sense is {cracker}.

Cracker

cracker: /n./ One who breaks security on a system. Coined ca. 1985 by hackers in defense against journalistic misuse of {hacker} (q.v., sense 8). An earlier attempt to establish "worm" in this sense around 1981-82 on Usenet was largely a failure.

Kevin Siers, NC, USA (cartoon from the Charlotte Observer)