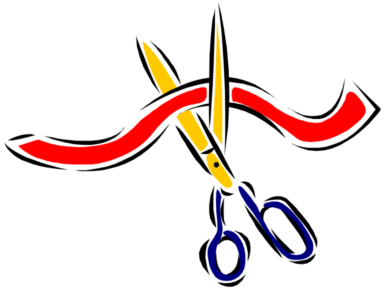
“always” at the exam

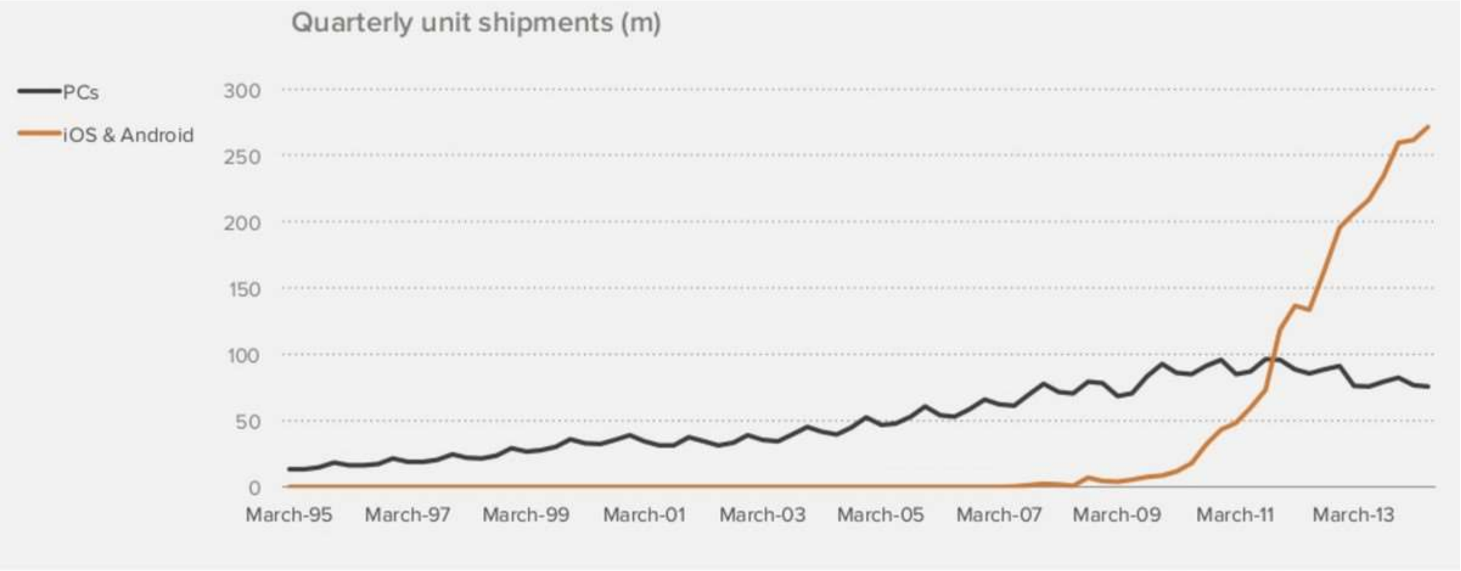
Computer Security Foundations and Principles



Nicolas T. Courtois

- University College London

Computers, PCs ?
Tablets, Mobile Phones, Smart Watches,…



Source: Gartner, Apple, Google, a16z

Computer Industry and Security

Tech Background: “Industry Standards” such as:

- CPU + chipset,
- RAM + SSD,
- C language,
- UNIX / Windows
- TCP/IP, HTTP,
- TLS,
- I/O tech: touch screen etc.

Social-Econ Background:

Science background:

Computer Industry and Security

"Industry Standards"

Social-Econ Background:

Science background:

- What technology "enablers"(computers) and "disablers" (cryptology,HWSec) can/cannot achieve?
- How to define / classify security problems and find "good" solutions

Computer Industry and Security

"Industry Standards"

Science background:

Social-Econ Background: things exist for a reason. "Nice or unpleasant" facts of life:

- software/hardware economics:
  - which industry dominates which
  - free market triumphs and disasters
- these stupid humans that cannot be bothered to obey the security policy…
- these bureaucratic organisations that just cannot get their best interest(?) right
- nobody is buying/using the wonderful(?) technology, adoption barriers
- theory vs. practice
- crime war terrorism…
- laws / regulations
- etc…

hackable
insecure rubbish!

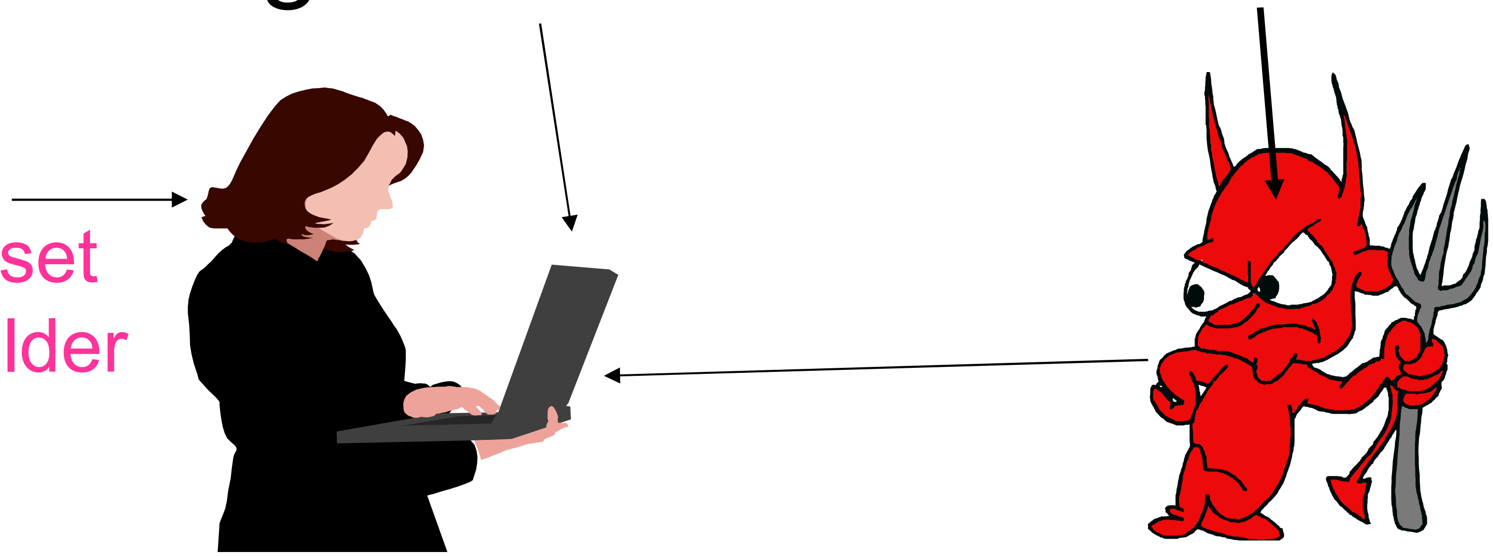
What is Security?

Security: Definition

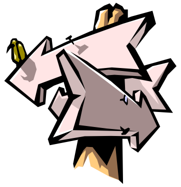
Common Criteria

[ISO15408]

Protecting Assets from Threats



asset holder



Security ≥ Safety

Difference:

protect against intentional damages...

Notion of an

Attacker / Adversary.

Notion of an Attack.

Attacker

Attacker = Adversary = Threat Agent

Main Goals:

- Confidentiality
- Integrity
- Authenticity

Accountability

Availability

Security Science

1.2.3.

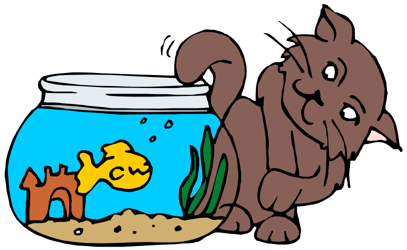
Claim [Courtois, Schneier]:

Computer Security and real-world security are governed by the same laws !!!

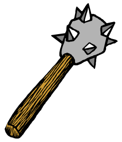
The Security ? 3-point Formal Approach

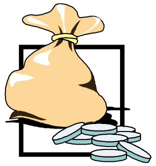
What is Security ? Inability to achieve:

1. Security against what: Adversarial Goal.



2. Against whom: resources of the Adversary: money, human resources, computing power, memory, risk, expertise, etc..





3. Access to the system.

1. Adversarial Goals

- Enjoyment, fame, ego, role models
- Develop science and offensive technology:
- $$$ profits and other benefits

2. a. Who Are the Attackers

- bored teenagers,
- petty => organized criminals,
- rogue states,
- industrial espionage,
- disgruntled employees, …

- pure legitimate use
- Inadvertent events, bugs, errors,
- ourselves (forgot the d… password!),
- our family / friends / co-workers,

2. b. Their Means

- computers (MIPS) / other hardware (antennas, liquid Nitrogen, etc…)
- knowledge / expertise
- risk/exposure capacity

3. Access to a Computer

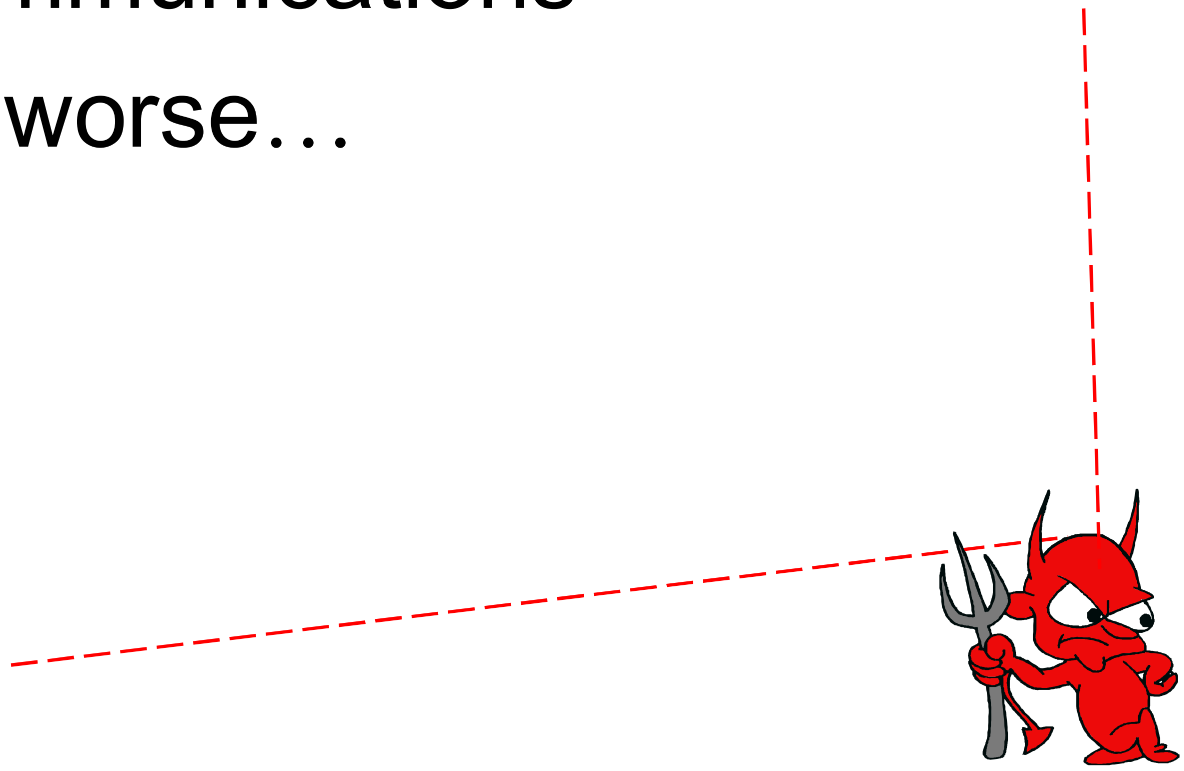
- Remote location, not connected to Internet
- Remote location, somewhat connected…
- Physical proximity…
- Access to USB ports.
- Access (alone) for a few seconds…
- Take it home and hack it…

*3. Access

Internet

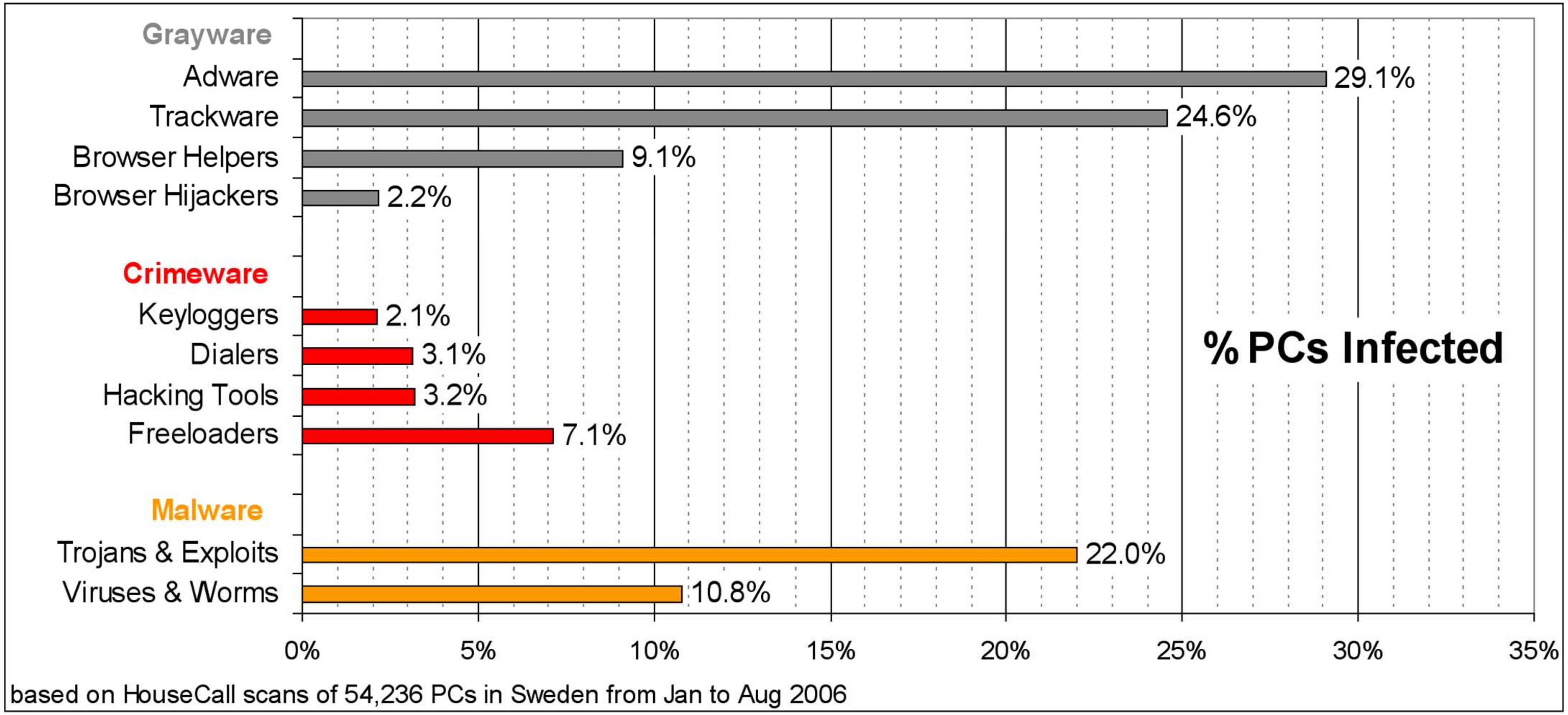
+wireless communications

made things worse…



Is My PC Infected = 2006.

- Long time ago:



based on HouseCall scans of 54,236 PCs in Sweden from Jan to Aug 2006

Since 2006:

- Malicious software strains:

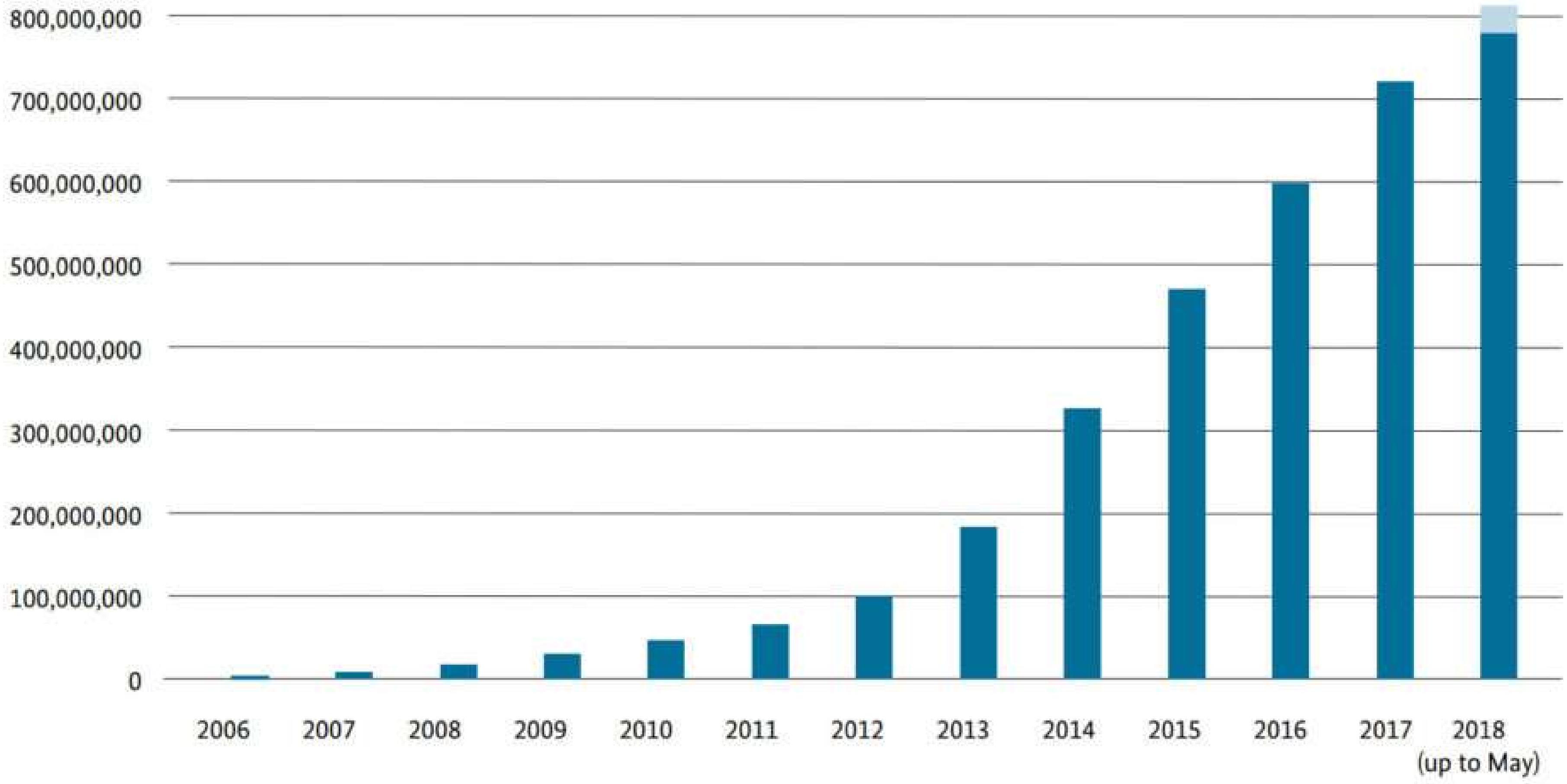
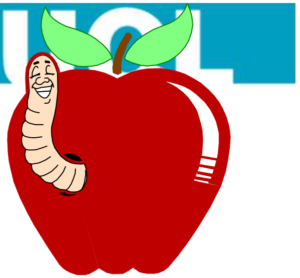


Figure 12 Known malware (2018 up to May), source AV-Test



Why Things Happen?

Bugs… or don’t care.

- Programming developed with absence of security.
  - C/C++ is unsafe (Microsoft has blacklisted big chunks of standard C, could have happened 30 years ago).
  - Security/cryptography research developed with obsession with security. Both never met.
- Economics/Business:
  - many things just don’t matter!

Security and Economics

- Security is about
  [sensible] security trade-offs.
- Closely related to economics: How to allocate resources efficiently.

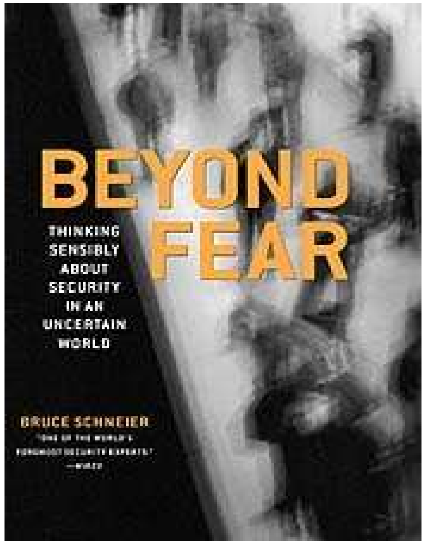
Security and Economics

Bruce Schneier “Beyond Fear” book [2003], p.1:

Critical to any security decision is the notion of

[security] trade-offs,

meaning the costs in terms of money,
convenience, comfort, freedoms, and so on –
that inevitably attach themselves
to any security system.



Failures

Types of Failures

- Failure in design
- Failure in implementation
- Failure in operation

Hacking A.D. 2015-2020

The industrialization of hacking:

- division of labour, clear definition of roles
- forming a supply chain
- professional management
- state actors

Do You Know…

Q1.

Can in Windows/Linux a process run by an administrator access the system/kernel memory?

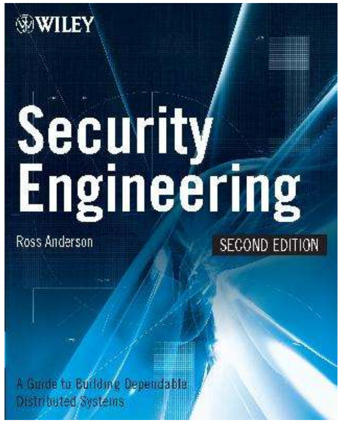
Q2.

Why do we must press Ctrl+Alt+Del when we log to a PC under many versions of Windows?

Principles of Security Engineering

Security Engineering

Definition: [Ross Anderson]



building systems
to remain dependable
in face of malice, error or mischance.

Magic Formulas…

or "Security Mantras":

- repeat after me: C.I.A. C.I.A.

In fact we have no silver bullet.

on the contrary:

Security is about conflicting requirements,

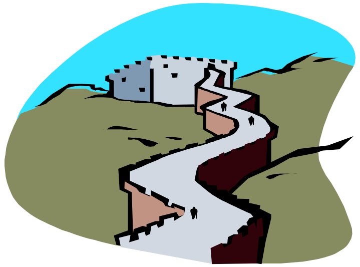
conflicting engineering criteria,

Overcoming human,
technology and market failures.

insecure rubbish!

Proportionality Principle

Maximize security???



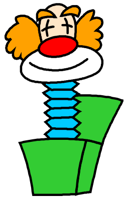
Maximize “utility” (the benefits)
while limiting risk
to an acceptable level
within reasonable cost…

» all about economics…

Efficiency and Effectiveness

Security measures must be:

- Efficient and effective…



Design Principles for Protection Mechanisms

[Saltzer and Schroeder 1975]

Least Privilege [or Limitation] Principle

Every "module" (such as a process, a user or a program)
should be able to access only such information and resources
that are necessary to its legitimate purpose.

Security Goals For the OS+Hardware

Goal 1A.

allowing multiple users securely share a computer.

Goal 1B.

allowing multiple processes securely share a computer.

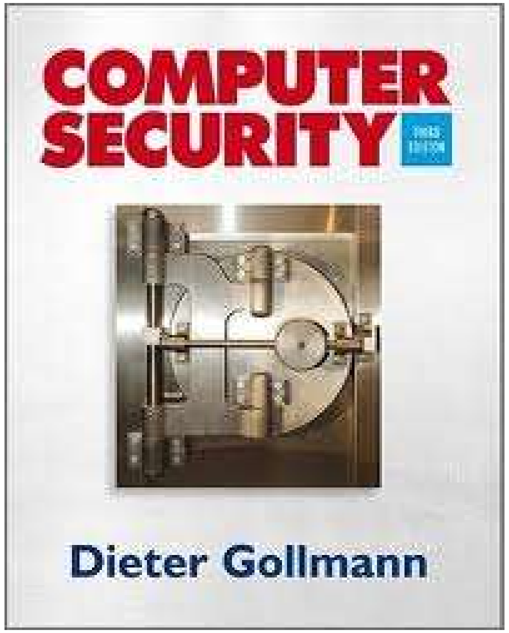
Goal 1ab – Means to Achieve It

multiple users / processes securely sharing a computer.

- authentication of users, cf. part 05 in

http://www0.cs.ucl.ac.uk/staff/n.courtois/compsec.html

- file access control and (drive/file) encryption and auth. Cf. part 04



- memory protection
- processor modes
  - Cf. Chapter 6.3.5.
- logging & auditing

Kernel space vs. User space

- Kernel space: the OS kernel, some kernel extensions, some device drivers
  - they run in the most privileged CPU mode = system mode = ring 0.
  - Privileges to access special registers, MMU, privileged instructions, hardware interruptions etc…
  - typically cannot be swapped to disk

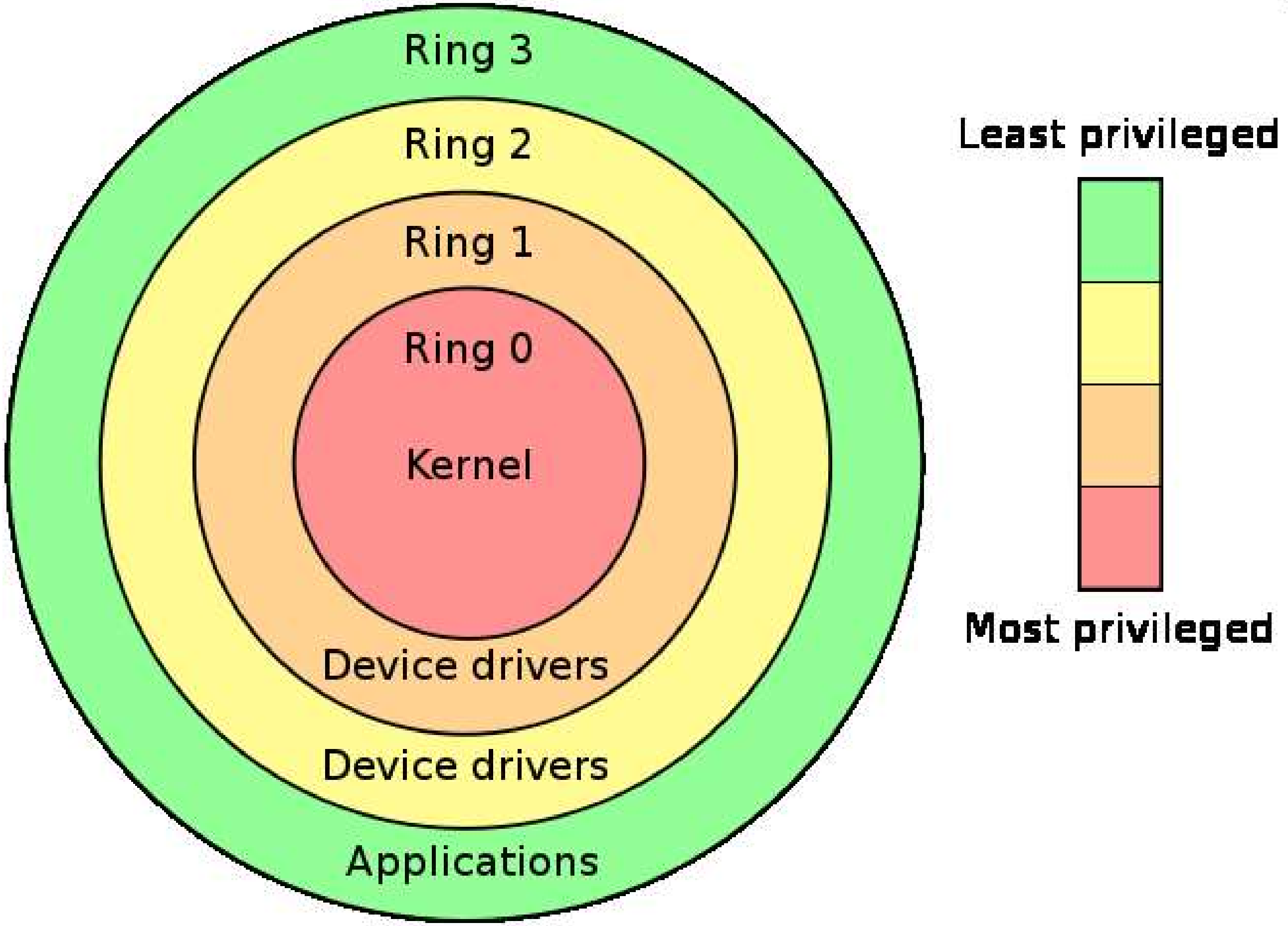
- User space, Userland: other parts of the OS that

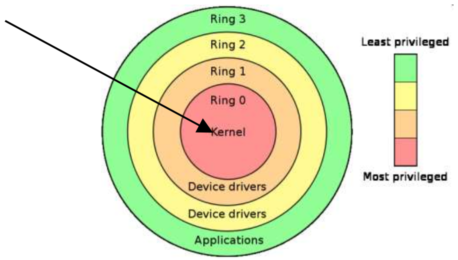
  run as processes or services/daemons in the user mode.
  - I/O and components
  - manipulating the filesystem
  - Shell

Quiz: Unix: Process running as Admin=User space,
Windows: process with user=system?

Rings – Hardware @ CPU

Different CPU architectures define several Rings.



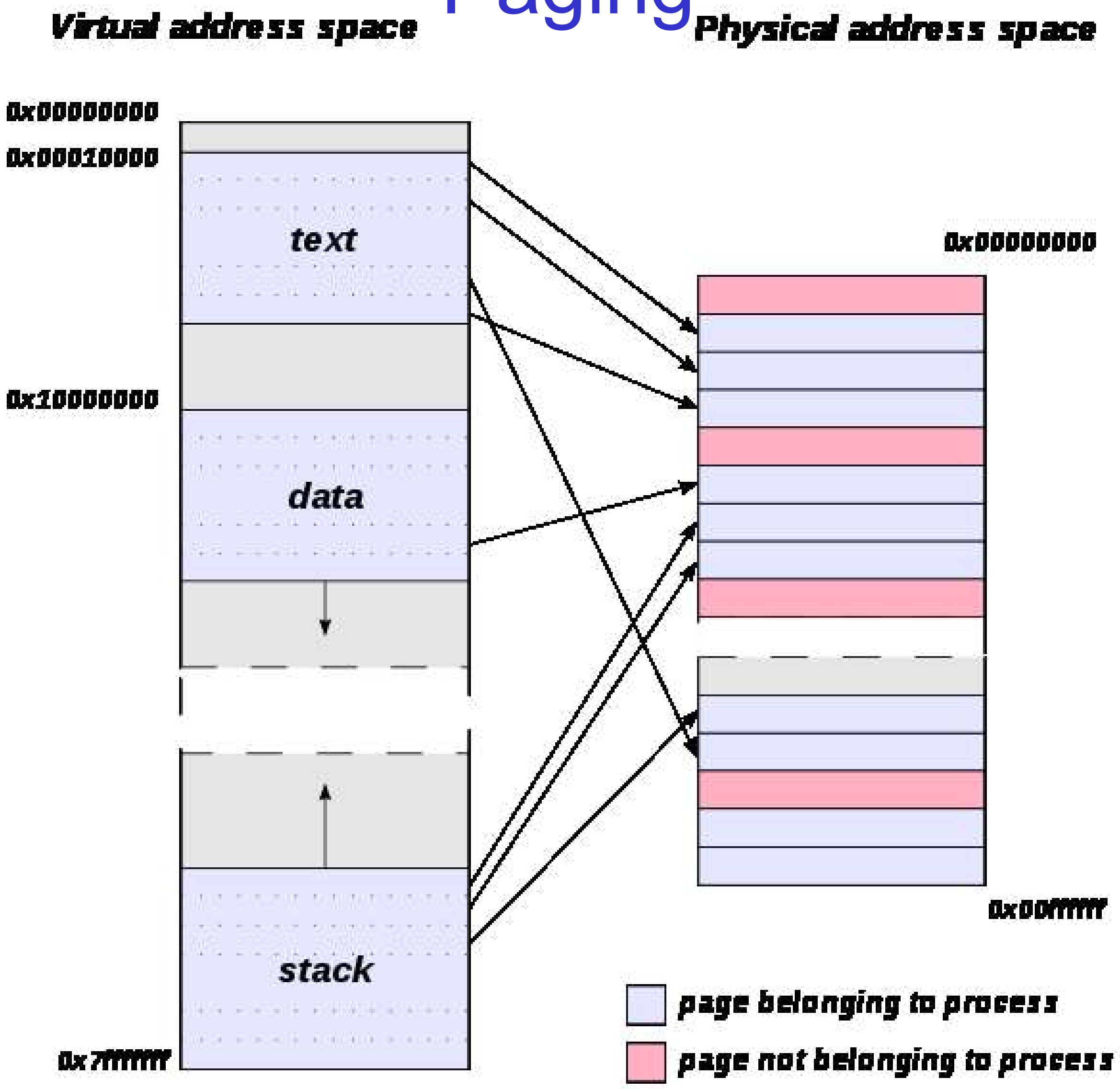


How to Penetrate to Ring 0?

boot loader!

- critical and privileged access point in all PCs.
  - Would allow to disable some hardware securities such as DEP…
  - Could allow a virus to be so stealth that no anti-virus would detect it.
- Beware of boot sector viruses!
- Good news: most motherboards have a hardware mechanism that prevents the OS from writing the boot sector of the hard drive. No access from the O/S level.

Paging


Virtual address space
Physical address space
0x00000000
0x00010000
text
0x10000000
data
stack
0x7fffffff
0x00000000
0x00ffffff
page belonging to process
page not belonging to process

Default Deny

There are two basic attitudes:

- Default permit
- Default deny –

Improves security, harder to things to work

Windows DEP = Data Execution Prevention

By default code CAN be executed (backwards compatible old versions of Windows).

Except when pages are marked as NX = Never Xecute (only recent programs have it).

Hardware mechanism. Both Intel and AMD implement it but Intel was the last to deliver this benefit to large-public CPUs, since P4 Prescott.

- Windows - Since XP SP2.
  - PAE mode needed: 64-bit page tables. Bit 63 is used.
- Also active in Linux with x64 CPUs, works also if you install 32-bit Linux on x64 CPU

Fail-safe Defaults

Secure by default,

Example:if we forget to specify access, deny it.

Economy of Mechanism

A protection mechanism should have a simple and small design.

- small and simple enough to be build in a rigorous way,
  - and fully tested and analysed

Separation of Privileges

Split into pieces with limited privileges!

Implementation in software engineering:

Have computer program fork into two processes.

- The main program drops privileges (e.g. dropping root under Unix).
- The smaller program keeps privileges in order to perform a certain task.
- The two halves then communicate via a socket pair.

Benefits:

- A successful attack against the larger program will gain minimal access.
  - even though the pair of programs will perform privileged operations.
- A crash in a process run as nobody cannot be exploited to gain privileges.

Additional possibilities:

obfuscate individual modules and/or make them tamper resistant through software.
Or burn them into a dedicated hardware module, and burn the fuse that allows to read the firmware.

Least Common Mechanism

Mechanisms used to access resources should not be shared.

Why? Not so obvious.

- If everybody depends on it, failure will have a higher impact.
- One user can do a DOS attack.
- Shared service [or resource such as CPU cache] can provide side channels.
- A mechanism serving all users must be designed to the satisfaction of every user, harder than satisfying more specialized requirements.

Saltzer and Schroeder 1975:

- Psychologically Acceptable

Think Ahead

Pro-active security design:

- Design the security in,
  - built-in from the start.
- Allow for future security enhancements.

[Morrie Gasser 1988]

also

- Fail securely:

if sth. goes wrong, yes,
make sure it “fails securely”.

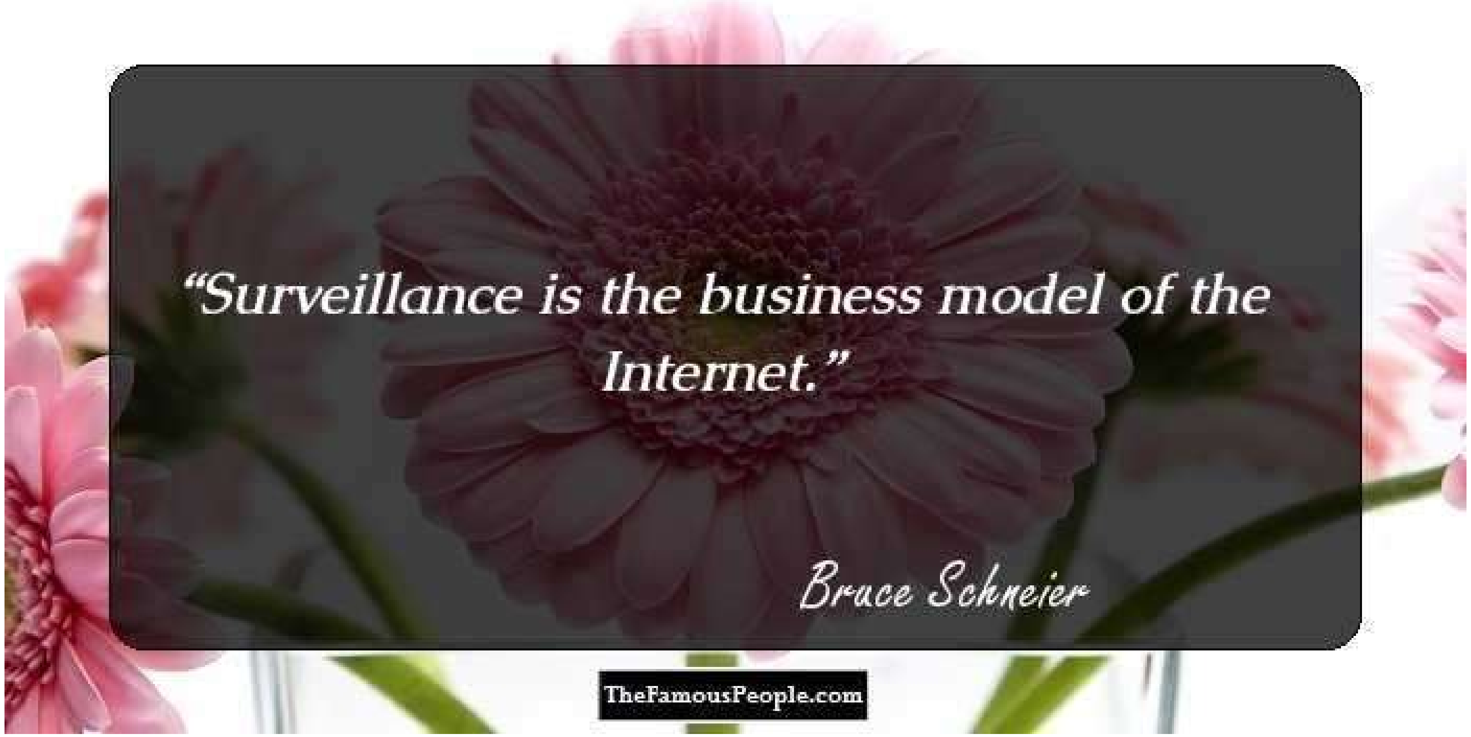
Trust

Following Ross Anderson and US Dept of Defence definitions:

- Trusted system [paradoxical definition]:
  one that can break the security policy (in theory, risk).
- Trustworthy system: one that won't fail us (0 risk).
  we can be assured that the security policy will not be violated

An employee who is selling secrets
is trusted and NOT trustworthy at the same time.

Secrecy vs. Transparency



"Surveillance is the business model of the Internet."

Bruce Schneier

TheFamousPeople.com

Open Design Principle

[Saltzer and Schroeder 1975]

Frequently incorrectly understood
and confused with “open source”
[cf. also Kerckhoffs principle in crypto].

Examples:

- Linux!
- DES S-boxes
- cryptography such as SHA256 (used in bitcoin) is open source BUT was designed behind closed doors at the NSA.

The False Principle:

Open Source [Collaborative Economy]

Minimalistic focus:

- forget being paid for your work

Open Source vs.
Closed Source
and Computer Security

Secrecy:

Very frequently
an obvious
business decision.

- Creates entry barriers for competitors.
- But also defends against hackers.

Kerckhoffs' principle: [1883]

"The system must remain secure should it fall in enemy hands ..."

Kerckhoffs’ principle: [1883]

Most of the time: incorrectly understood.

Utopia:

Who can force companies to publish their specs???

No obligation to disclose.

- Security when disclosed.
- Better security when not disclosed.

Which Model is Better?

Open and closed security are
more or less equivalent…

more or less as secure: opening the system
helps both the attackers and the defenders.

Cf.

Ross Anderson: Open and Closed Systems are Equivalent (that is, in an ideal world). In Perspectives on Free and Open Source Software, MIT Press 2005, pp. 127-142.

The False Principle:

The Weakest Link

Weakest Link

Chain metaphor:

Schneier: www.schneier.com/blog/archives/2005/12/weakest_link_se.html

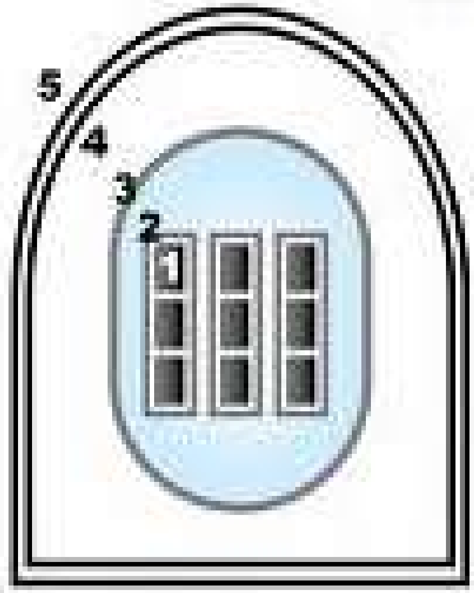
“security is only as strong as the weakest link.”

Two Cases

Security can be like a chain:

or, <u>better</u>

Security can be layered

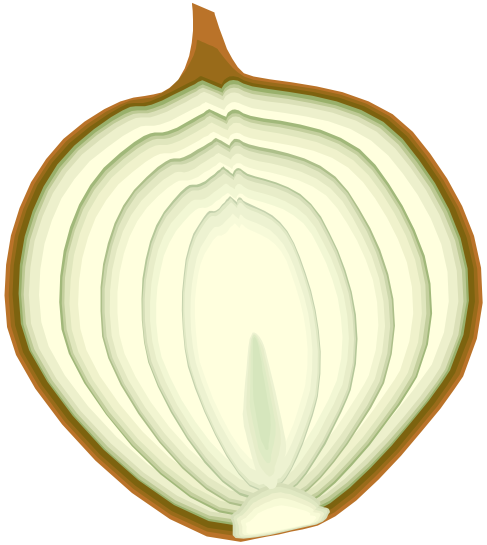


Military: Defence in Depth

Layers

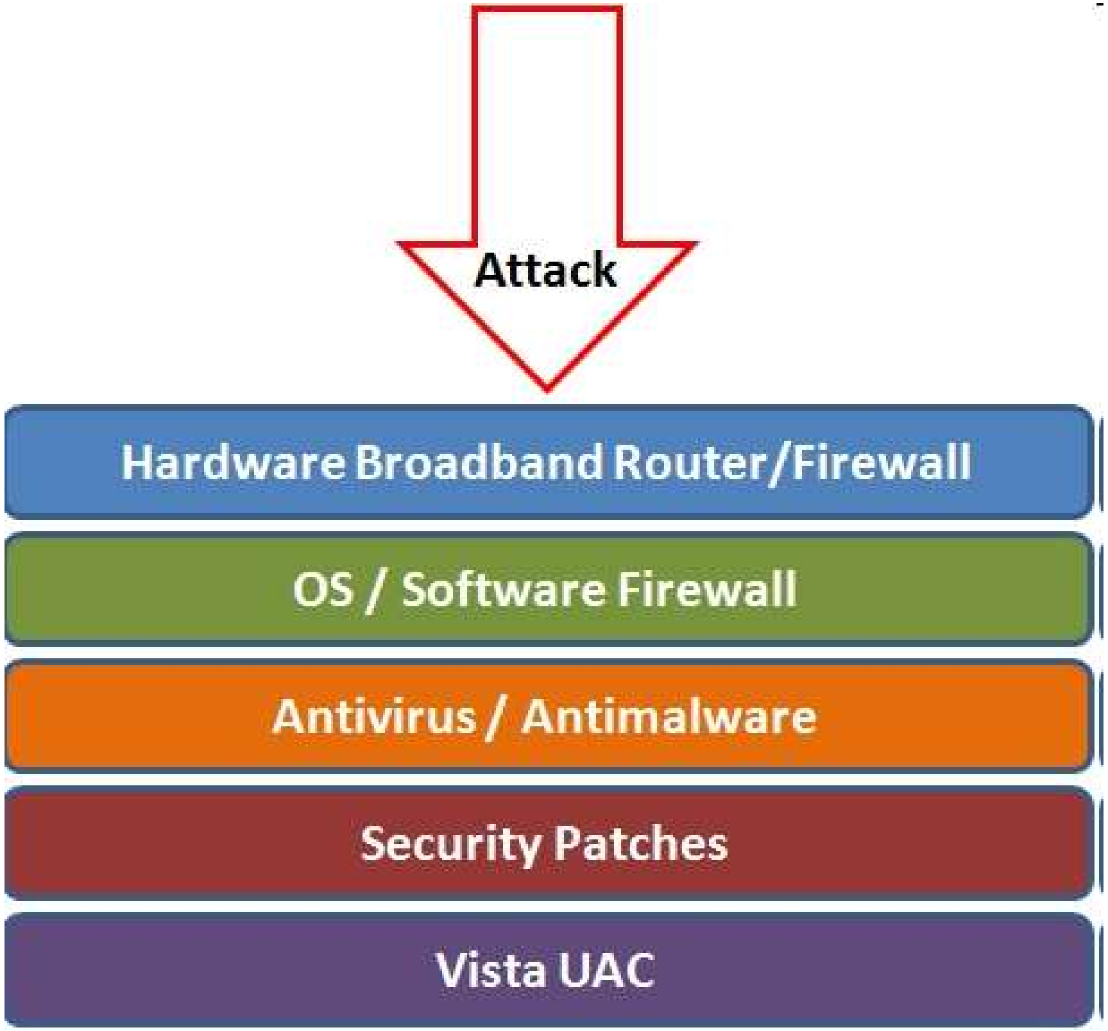
Computer systems have multiple layers, e.g.

- HW components
- Chipset/MB
- OS
- TCP/IP stack
- HTTP application
- Secure http layer
- Java script
- User/smart card interface



Example 1:

assuming
1000 little details…



Attack

Hardware Broadband Router/Firewall

OS / Software Firewall

Antivirus / Antimalware

Security Patches

Vista UAC

Another False?? Or True?? Principle:

Assume the Worst

Famous Schneier Quote

www.schneier.com/essay-005.html

“It's always better to assume the worst.
Assume your adversaries are better than they are.
Assume science and technology will soon be able to do things they cannot yet.
Give yourself a margin for error.
Give yourself more security than you need today.
When the unexpected happens,
you'll be glad you did.”

BUT… this is rubbish (or is it?)

Worst Case Defences? Criticism

Cormac Herley [Microsoft research]:

- Most security systems are build
  to defend against the worst case.
- In reality, the average case losses are insignificant or small,
  - e.g. actually computer crime worldwide is very small…
  - and many security technologies are maybe -- from the economics point of view -- totally useless
    - but it depends,
      we cannot judge security technologies by present losses,
      because there are also losses that have been avoided or deterred by this technology, and also that losses evolve over the time with highly chaotic pattern (they are 0 then suddenly they may explode)

Attack Trees

– a nice tool

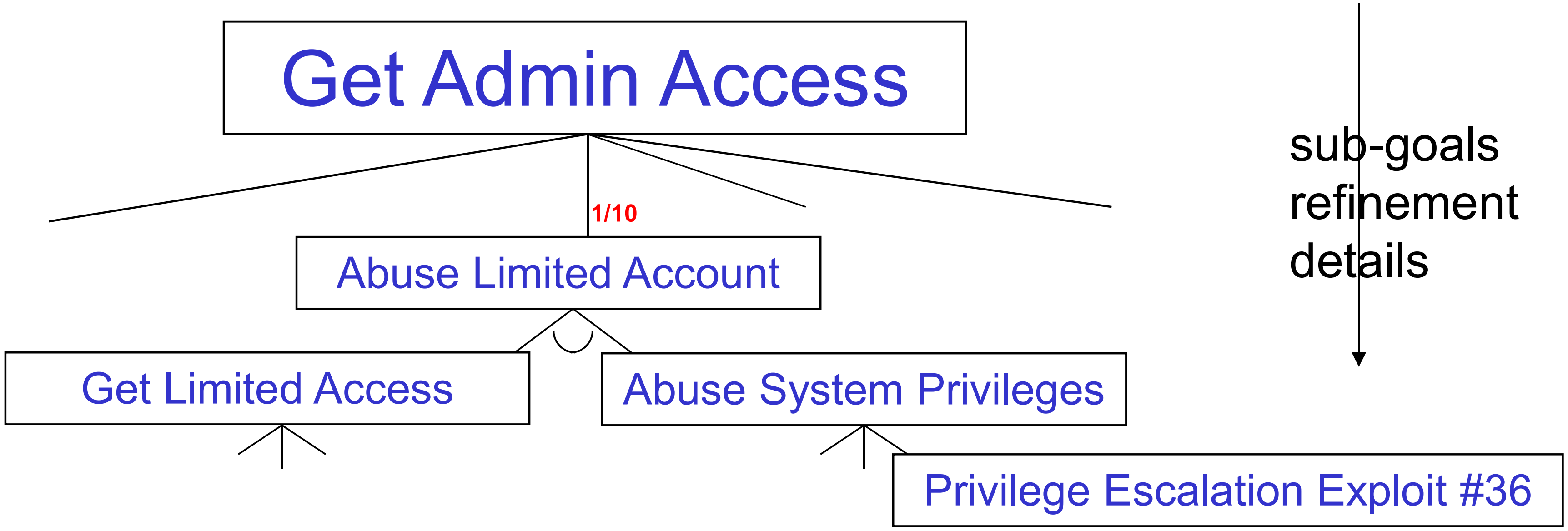
Attack Tree [Schneier 1999]

Formal analysis of all known attack avenues.

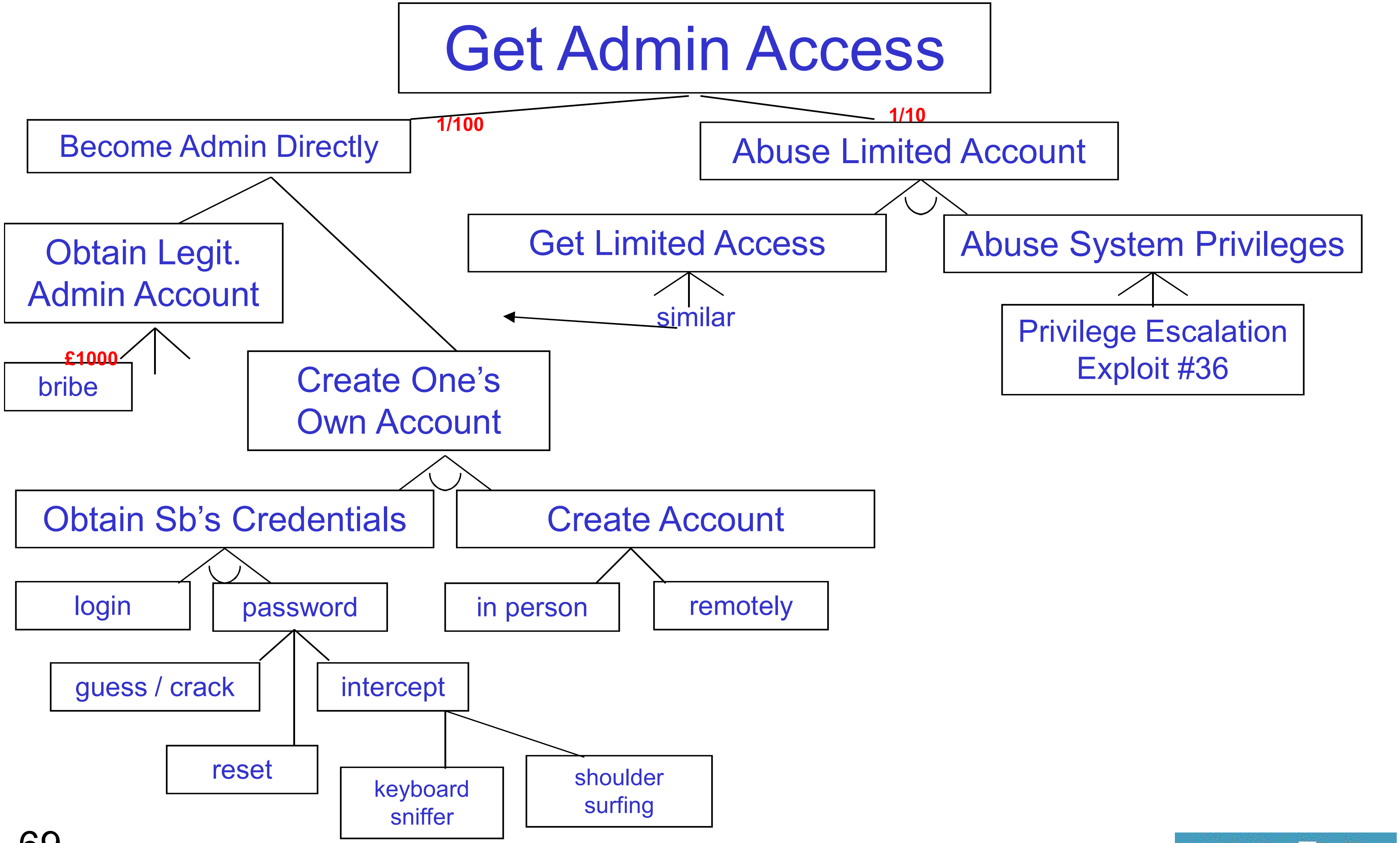
but what about unknown attacks?

A tree with OR nodes and AND nodes.

nodes can be labeled with probabilities or cost estimates

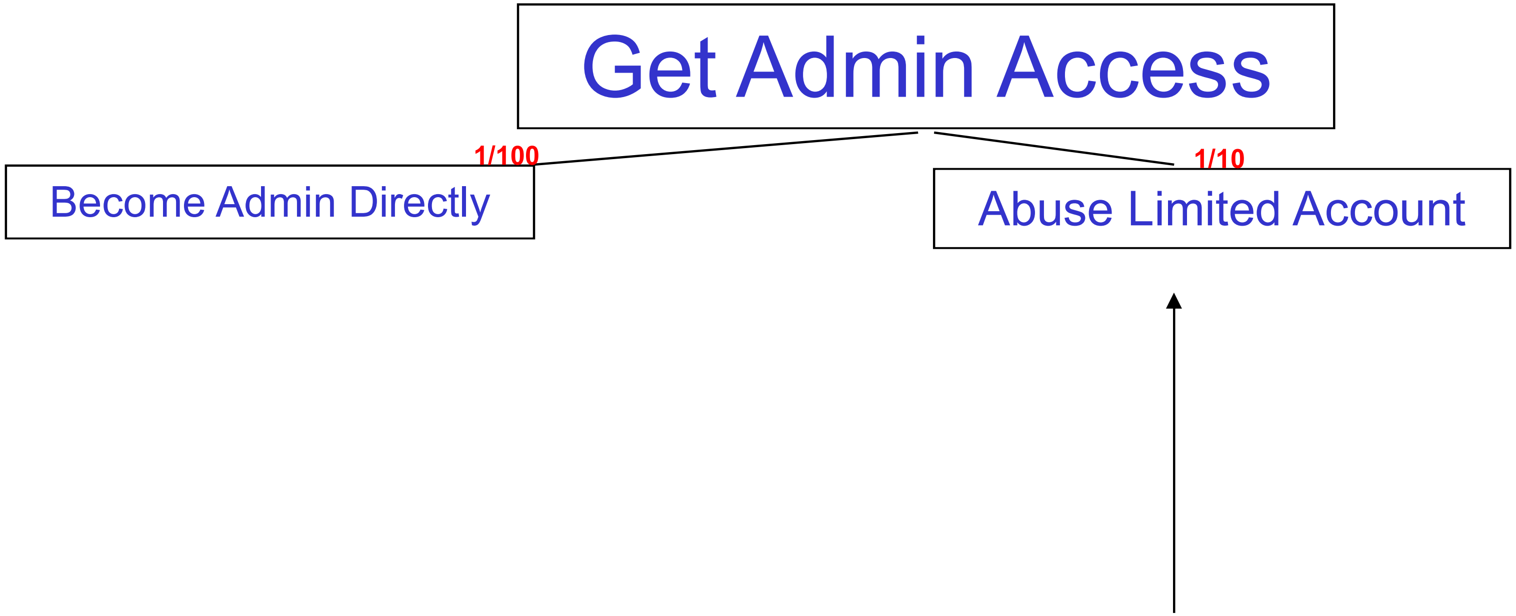


Expanded Example



Weakest Link

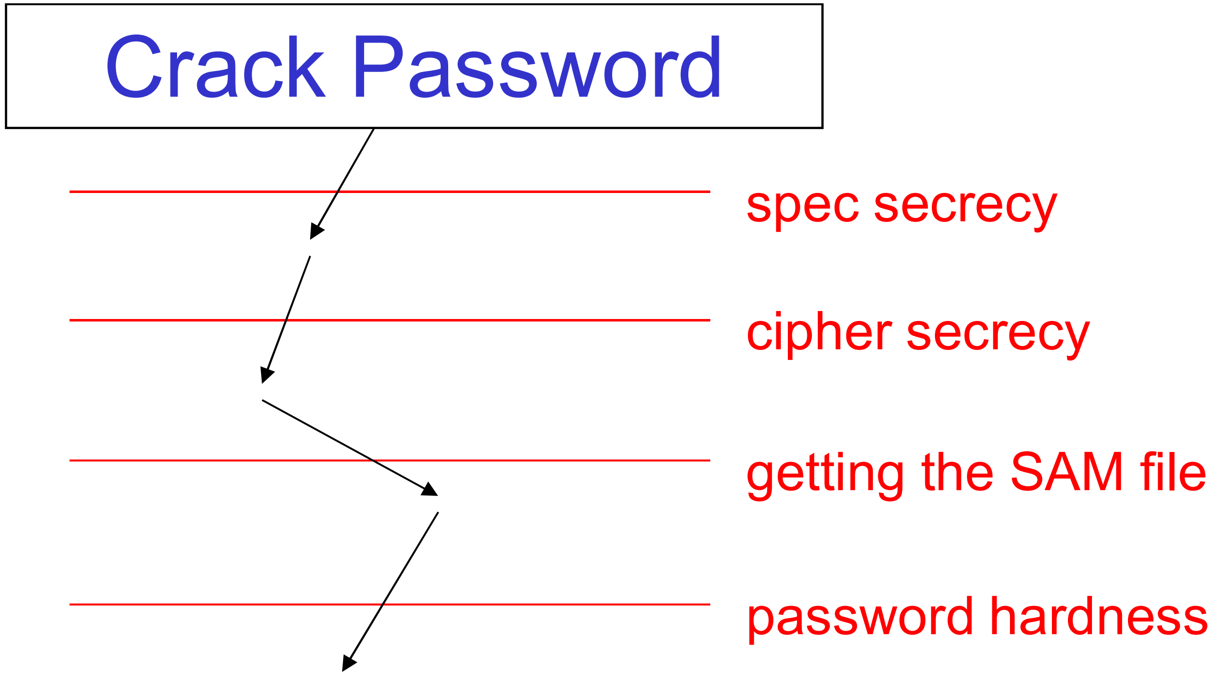
Security like a chain:



easier!

Defense in Depth

also appears in attack trees…



Crack Password

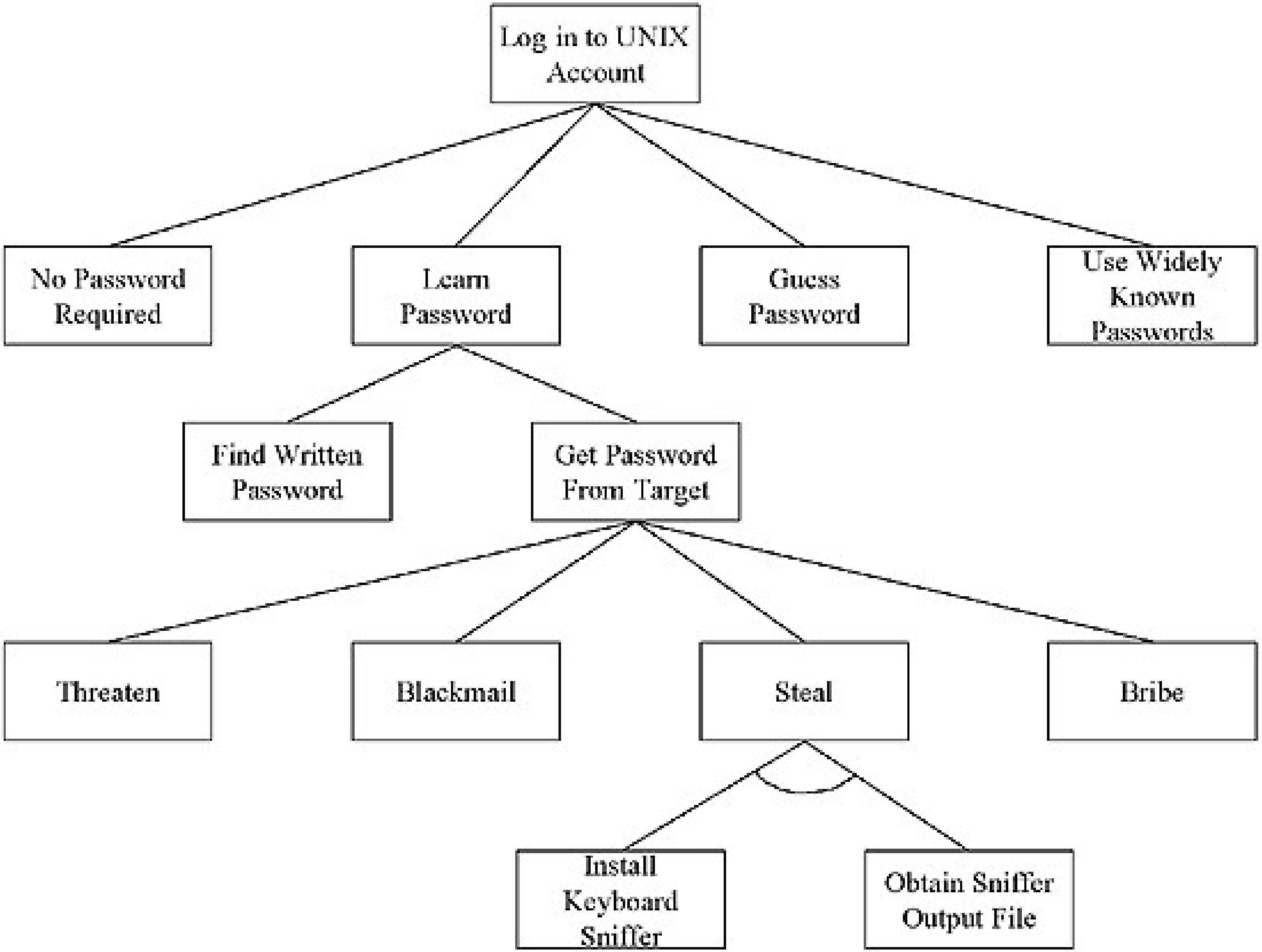
spec secrecy

cipher secrecy

getting the SAM file

password hardness

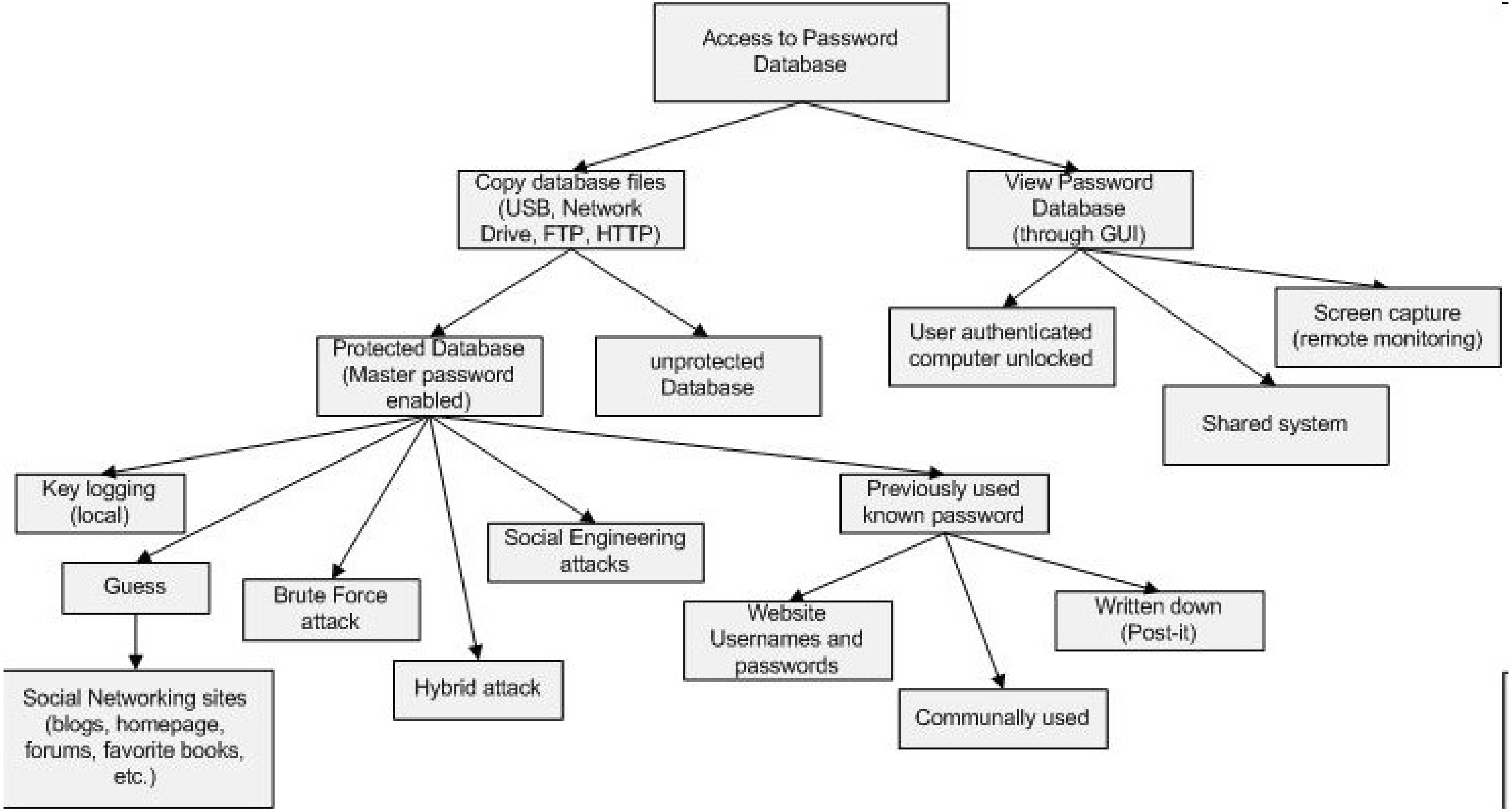
**Unix Log In


Log in to UNIX Account
No Password Required
Learn Password
Guess Password
Use Widely Known Passwords
Find Written Password
Get Password From Target
Threaten
Blackmail
Steal
Bribe
Install Keyboard Sniffer
Obtain Sniffer Output File

Conclusion:

In complex systems, the principles of weakest link and defence in depth will occur simultaneously!

Accessing Password Database


Access to Password Database
Copy database files (USB, Network Drive, FTP, HTTP)
View Password Database (through GUI)
Protected Database (Master password enabled)
unprotected Database
User authenticated computer unlocked
Screen capture (remote monitoring)
Shared system
Key logging (local)
Guess
Brute Force attack
Hybrid attack
Social Engineering attacks
Previously used known password
Social Networking sites (blogs, homepage, forums, favorite books, etc.)
Website Usernames and passwords
Written down (Post-it)
Communally used

Security Dystopia

“Security” - for Whom?

Do Computers belong to us? Work for us?

- Best case, they work for your boss and your banker [increased productivity].
- Worst case: Mass surveillance with rogue businesses and criminals.