Computer (Cyber) Security

Definition and Challenges

Designing Secure Systems 2017/18

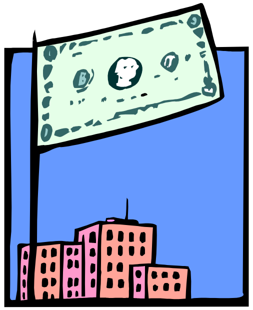
David Galindo

Based on slides by Nicolas Courtois (UCL)

What is security?

Class brainstorm

Security: protect assets



What assets?

- Money [economic security]

But NOT ONLY MONEY

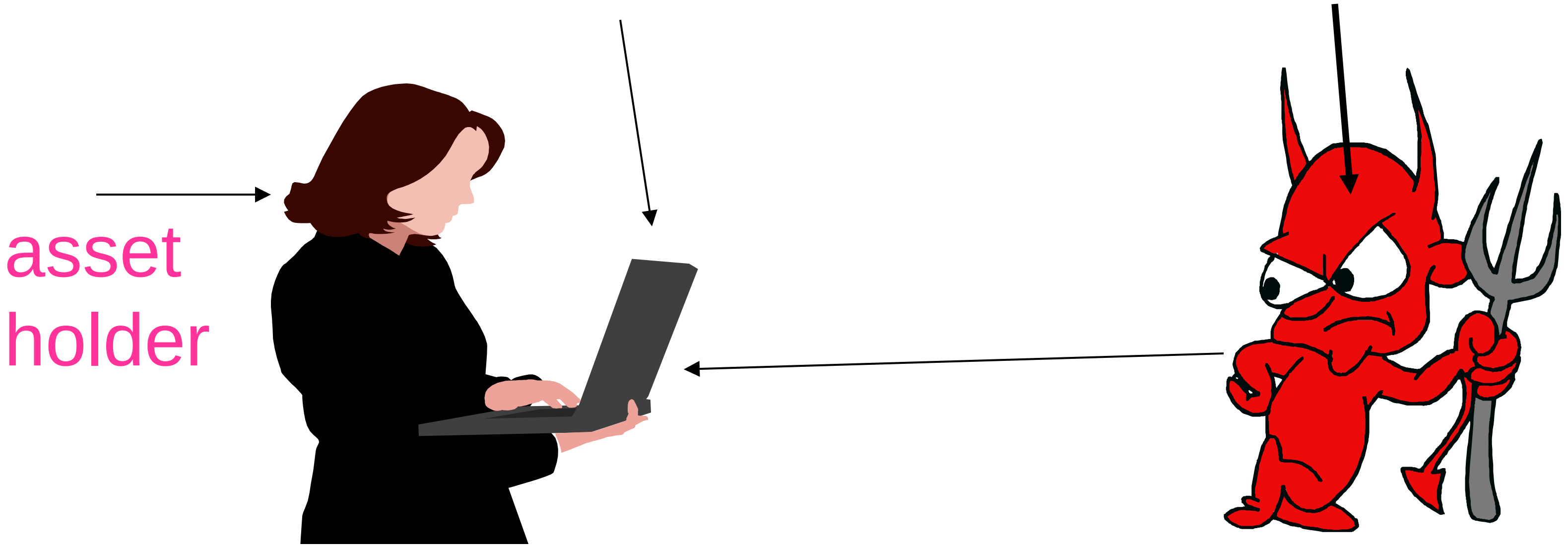
- Life and the quality of life
- Food security
- Freedom, justice, etc…

Computer Security

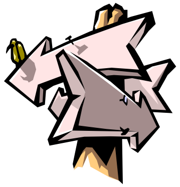
Common Criteria [ISO15408] :

an international standard for computer security certification

Protecting Digital Assets from Threats



asset
holder



Security ≥ Safety

Difference:

security protects against intentional damages...

Notion of an

- Attacker / Adversary
- Attack

Dimensions of Computer Security

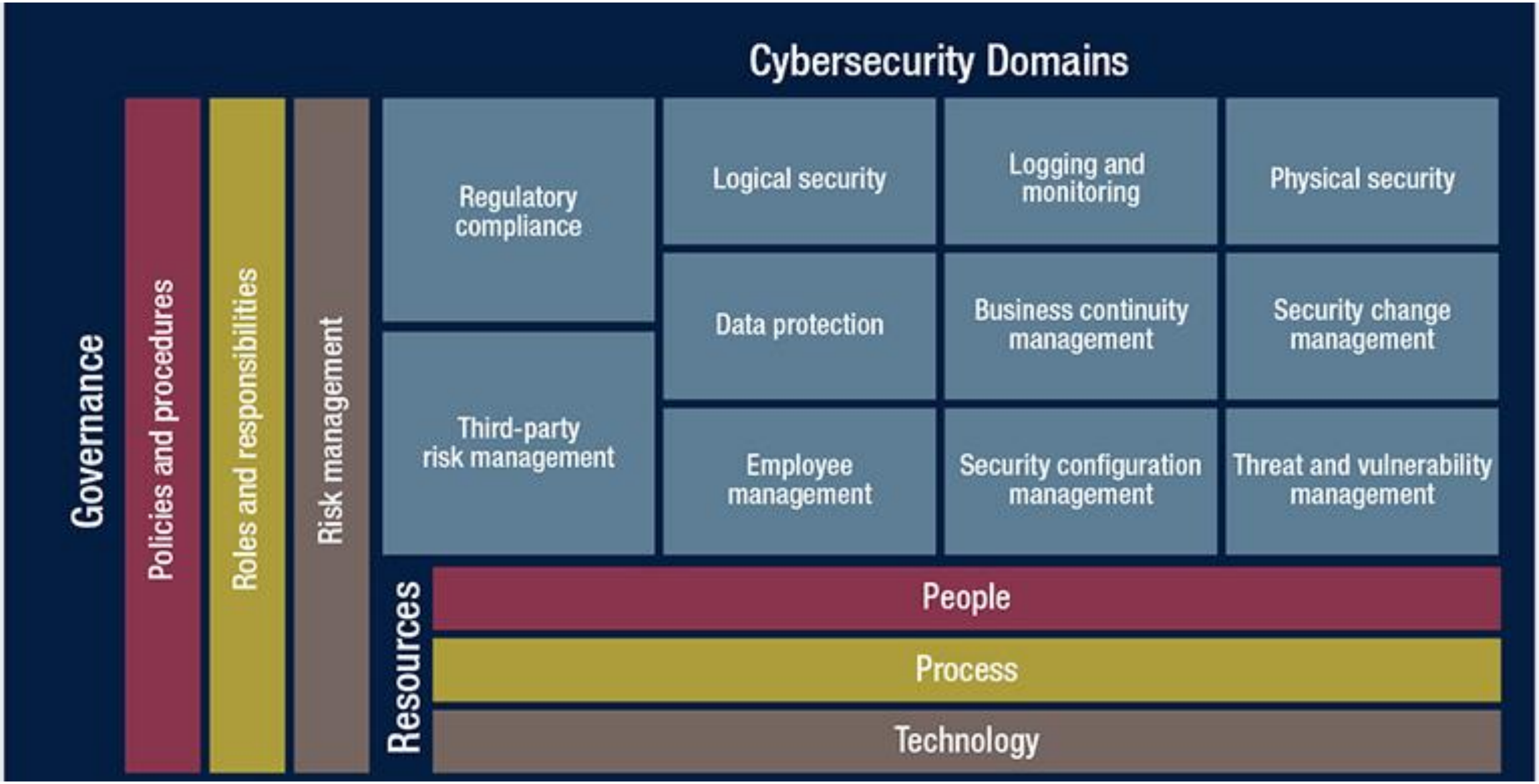
- Physical vs. Logical

- Psychological / Human

very different!

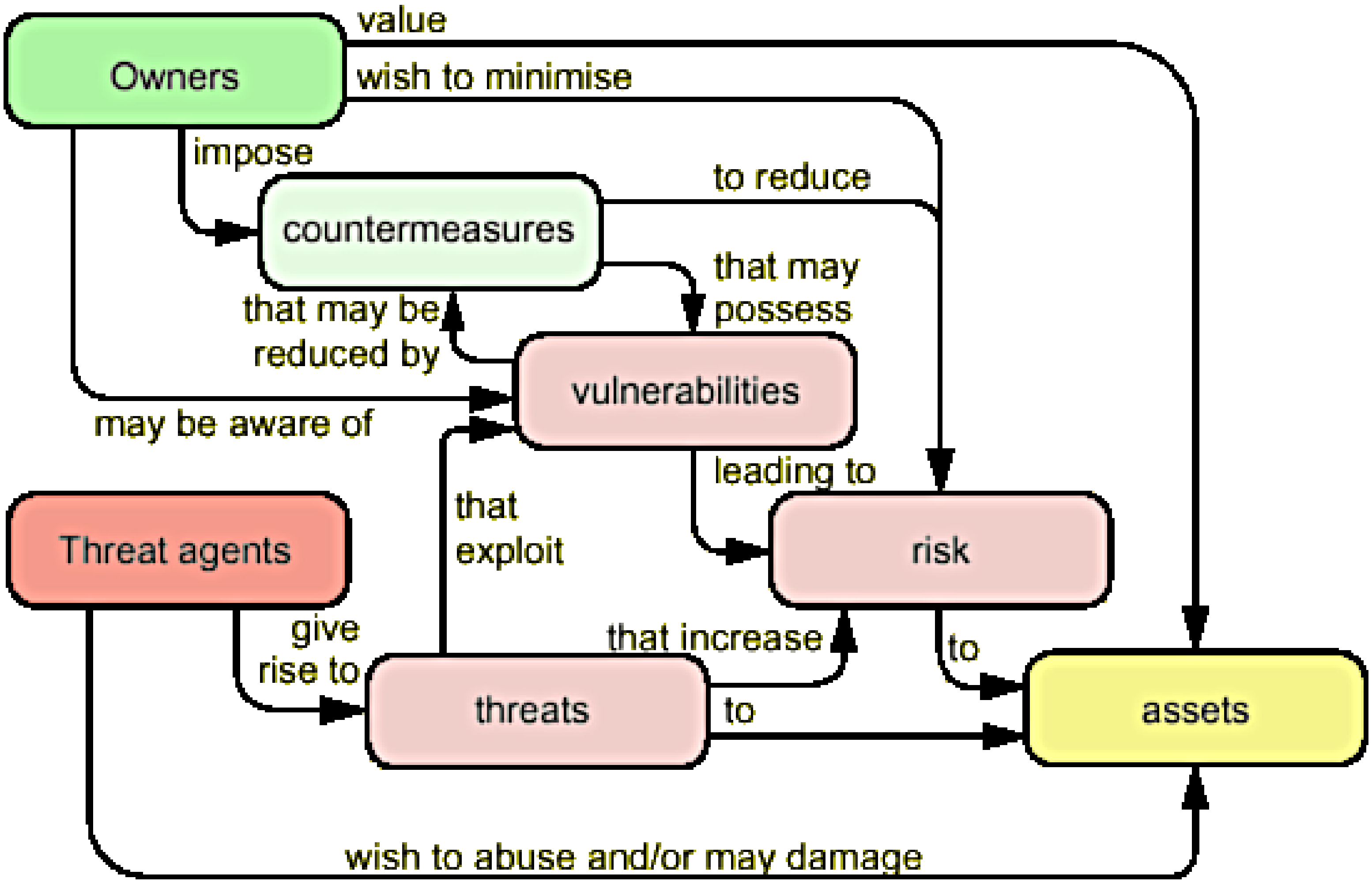
- Organizational / Business

Computer Security Dimensions



Common Criteria

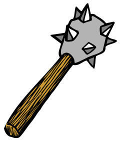
Computer Security on one slide

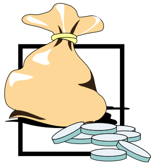


Our Definition of Secure System

Inability for attackers to achieve:

1. Adversarial goal





2. By means of: money, human resources, computing power, memory, risk, expertise... **resources of the adversary**

3. Access to the system

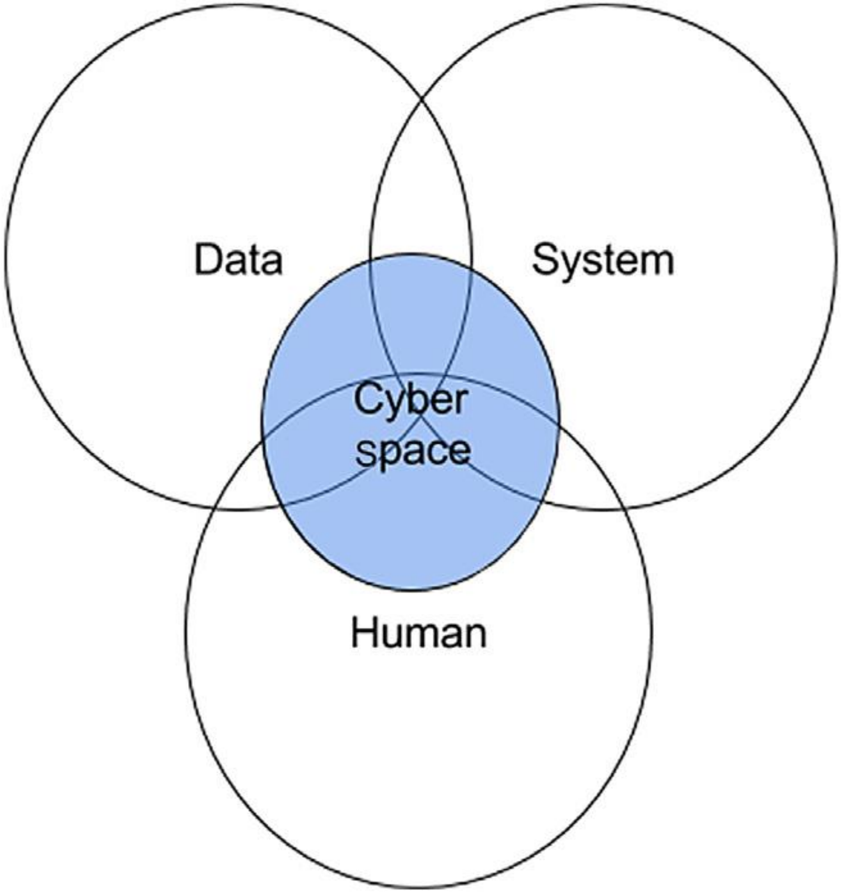
Main Adversarial Goals

Breaching any of:

- Confidentiality
- Integrity
- Authenticity
- Availability
- Accountability

Why is computer security hard?

Class brainstorm



Cyber space at the overlap of data, system, and human

Computer Industry and Security

Tech Background: “Industry Standards” such as:

- Intel CPU
- RAM and hard drives
- C language
- UNIX / Windows
- TCP/IP
- HTTP
- TLS

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-econon background:

Social-econ background:

•software/hardware economics:

  - which industry dominates which
  - free market triumphs and disasters

- **humans that cannot be bothered to obey the policy…**
- bureaucratic organisations that just cannot get their best interest (?) right
- slow adoption of the technology academics/companies are creating
- adoption barriers
- theory vs. practice
- laws / regulations

insecure products!

Attackers

Vocabulary

Attacker / Adversary / Threat Agent

Who are the attackers?

- Adventurous teenagers
- Petty criminals to organized criminals
- Foreign states
- Industrial spies
- Disgruntled employees
- Competitors
- Researchers
- Terrorists
- …

Attacker means

- Software vulnerabilities
  - Buffer overflow attacks
  - SQL injection attacks
  - Javascript attacks (e.g., XSS)
  - Broken authentication, access control, and session management
- Security misconfiguration

Attacker means continued

- Social engineering
  - Phishing attacks
- Traffic interception (e.g. wireless)
- Hardware/physical attacks
- Ingenuity, hard work, good luck, brute force

Attacker motivation

- Profits and other benefits
  - Crime business
  - Reputation damage

- Political activism, terrorism
- Enjoyment, fame
- Development of science and offensive technology:
  - University researchers
  - Security professionals (defenders)
  - Professional hackers, pen testers, etc…

Recent Trend

The industrialization of hacking:

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

Cybercrime actors

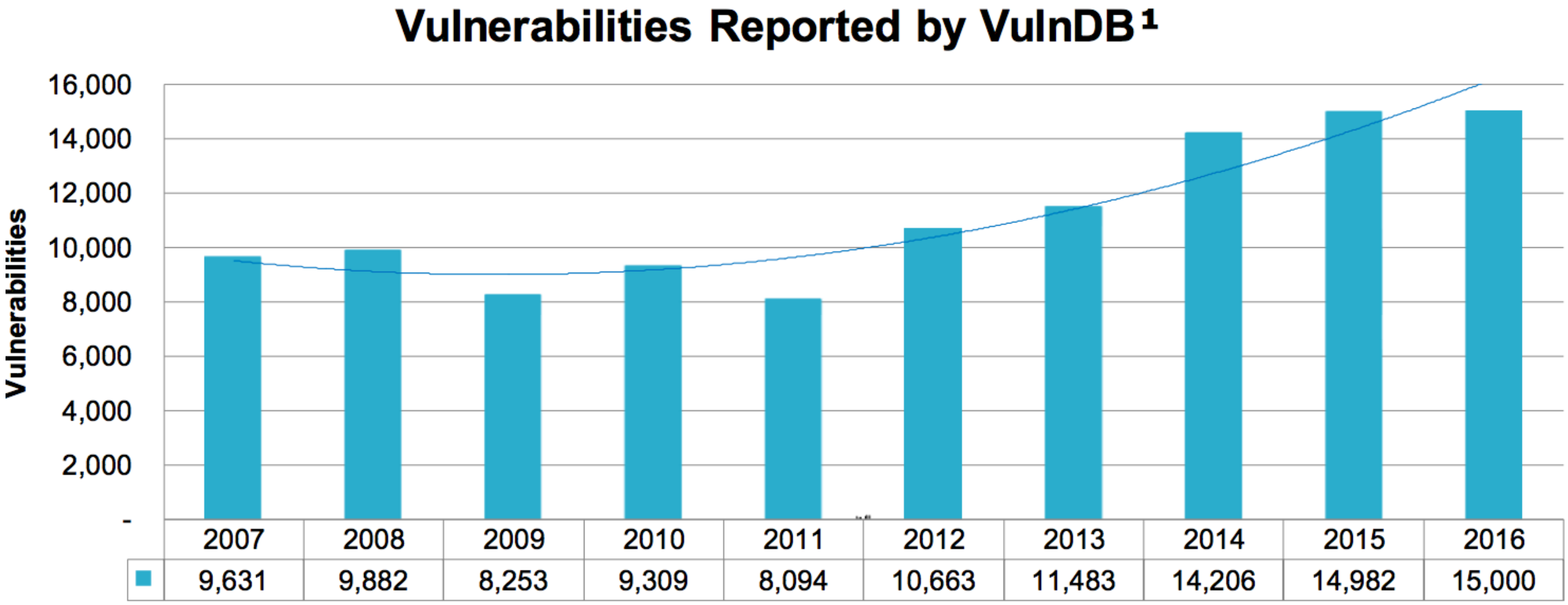
- Exploit developers
  - Very smart people who reverse-engineer software
  - Develop and sell exploits packs and kits
- Botnet masters
  - Develop software and control vast numbers of *zombie machines* (i.e. infected by a bot)
  - Rent out their botnet to other actors
- Spammers
  - Advertise links for other actors
- Phishers
  - Setup scam sites to steal information
  - Work with spammers to spread the attack

Cybercrime actors contd

- Counterfeiters
  - Run websites selling fake goods
  - Must be able to clear credit cards
- “Bulletproof” Hosting Providers
  - Offer dedicated servers to other actors
  - Hosted in lawless parts of the Internet
- Carders, Cashiers, and Mules
  - Turn stolen bank accounts and credit cards into cash
  - Help launder money
- Crowdturfers
  - Create, verify, and manage fake accounts
  - Solve CAPTCHAS for a fee

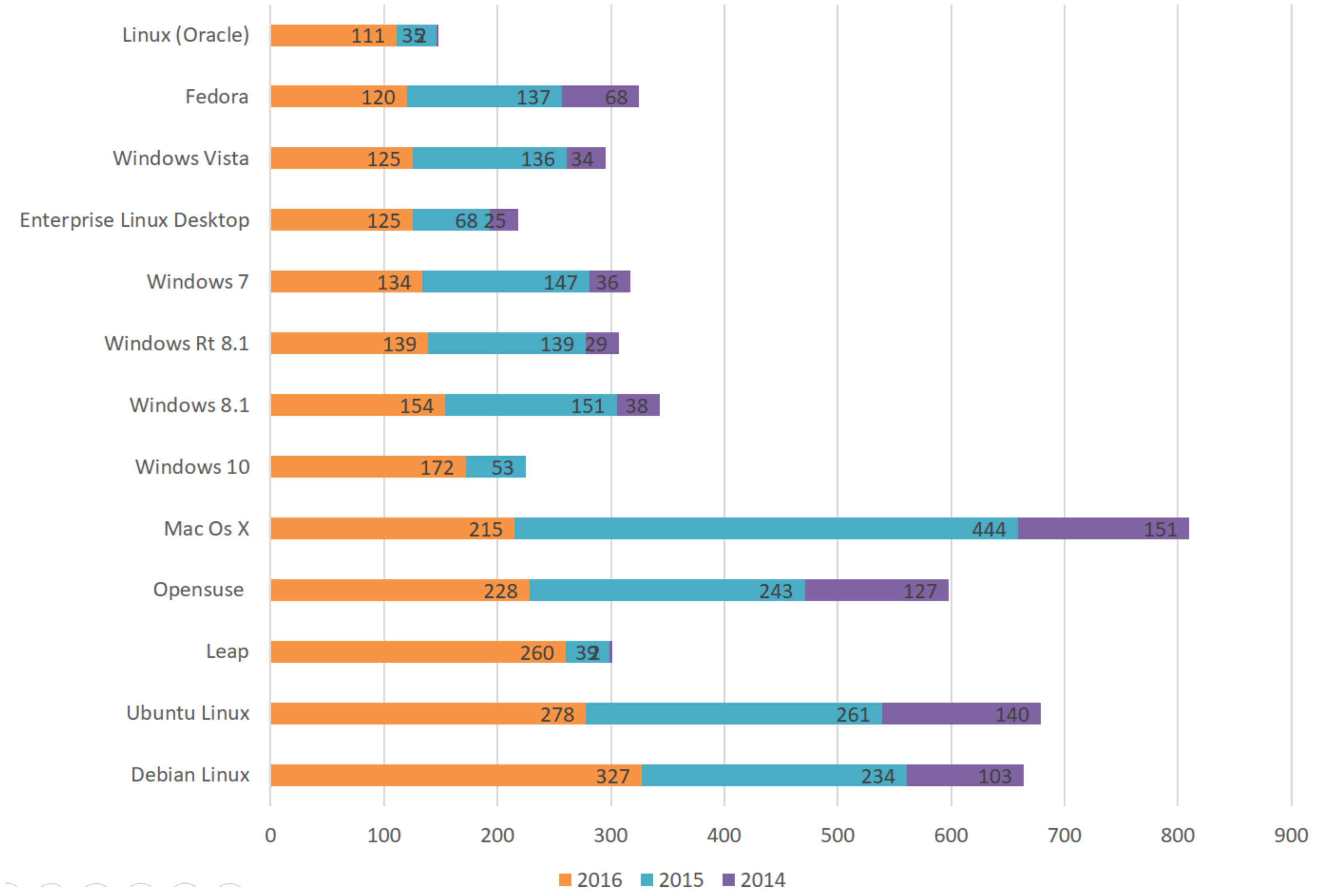
Software vulnerabilities

Reported Vulnerabilities stats


Vulnerabilities Reported by VulnDB[1]

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
■	9,631	9,882	8,253	9,309	8,094	10,663	11,483	14,206	14,982	15,000

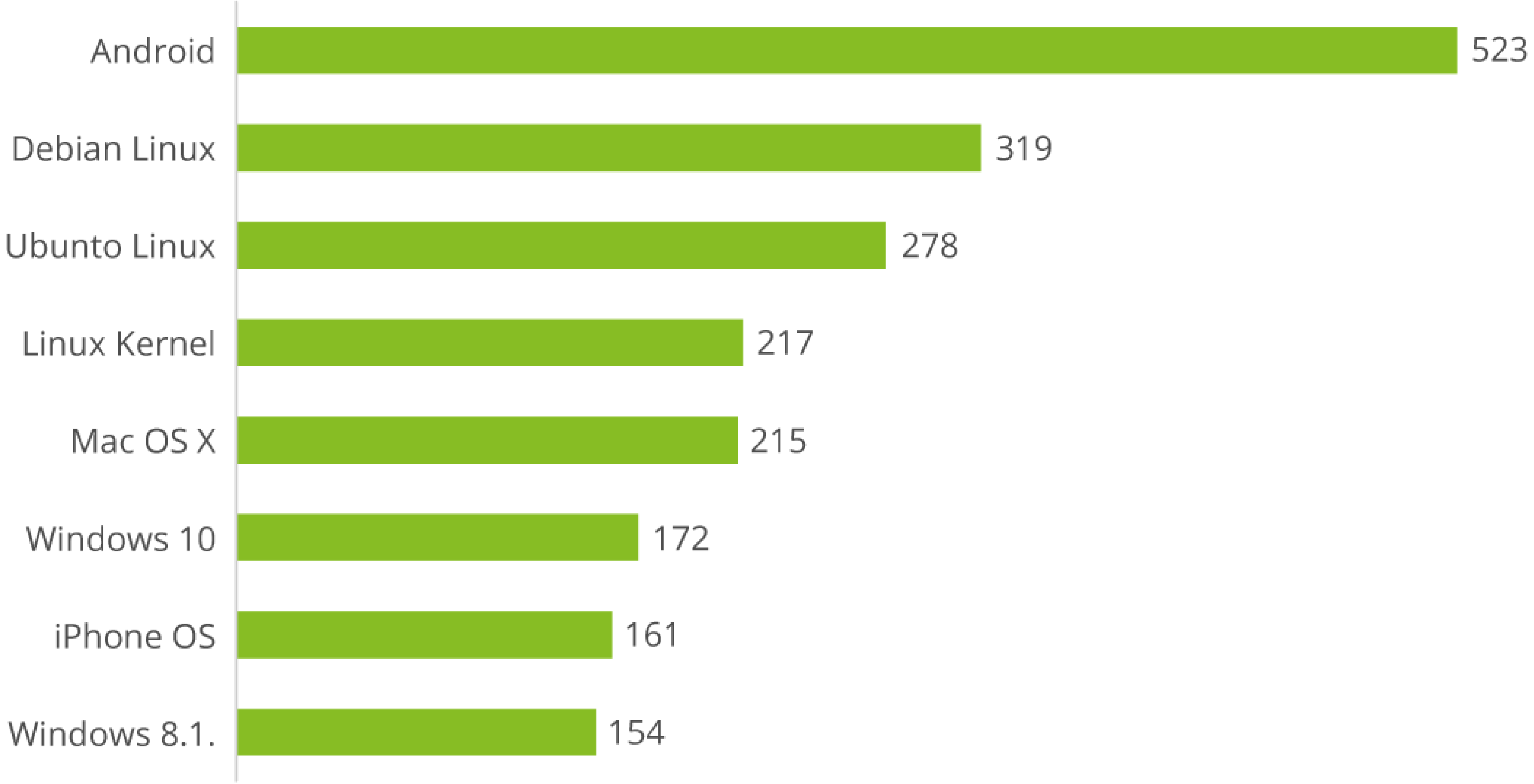
Top vulnerable operating systems in 2016



Tech Chart of the Day

Android Is The Most Vulnerable Operating System

Number of vulnerabilities by operating system in 2016*



* Vulnerability defined as a mistake in software that can be directly used by a hacker to gain access to a system/network

CompSec and Economics

Question

Why do so many vulnerabilities exist in the first place?

Class brainstorm

Why does commercial security fail?

Claim: the link between “money” and security is still frequently broken today:

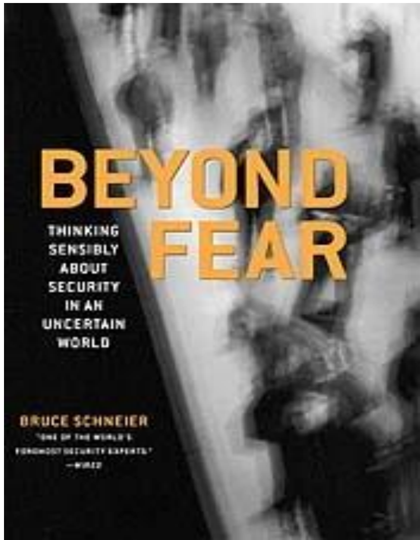
- Security is a public good
  - “private” incentives are weak
- Worse than “market for lemons”:
  - Not only the customer cannot see the difference between good security and bad

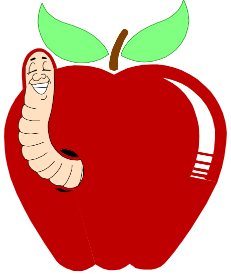
~~Frequently~~ Sometimes the manufacturer cannot either

The Very Nature of Security:

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

Critical to any security decision is the notion of **security trade-offs,** meaning the **costs** – terms of money, convenience, comfort, freedoms, and so on - that inevitably attach themselves to any security system. People make security trade-offs naturally.


BEYOND FEAR
THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD
BRUCE SCHNEIER
"ONE OF THE WORLD'S FOREMOST SECURITY EXPERTS" —WIRED



Why Things Happen?

Bugs…   or don’t care

- Programming with absence of security considerations
  - C/C++ is unsafe
  - Security/cryptography research developed with obsession with security. Both never met
- Economics/business:
  - customers do not see => do not care about security
  - usability: usage burden frustrates users

*Risk

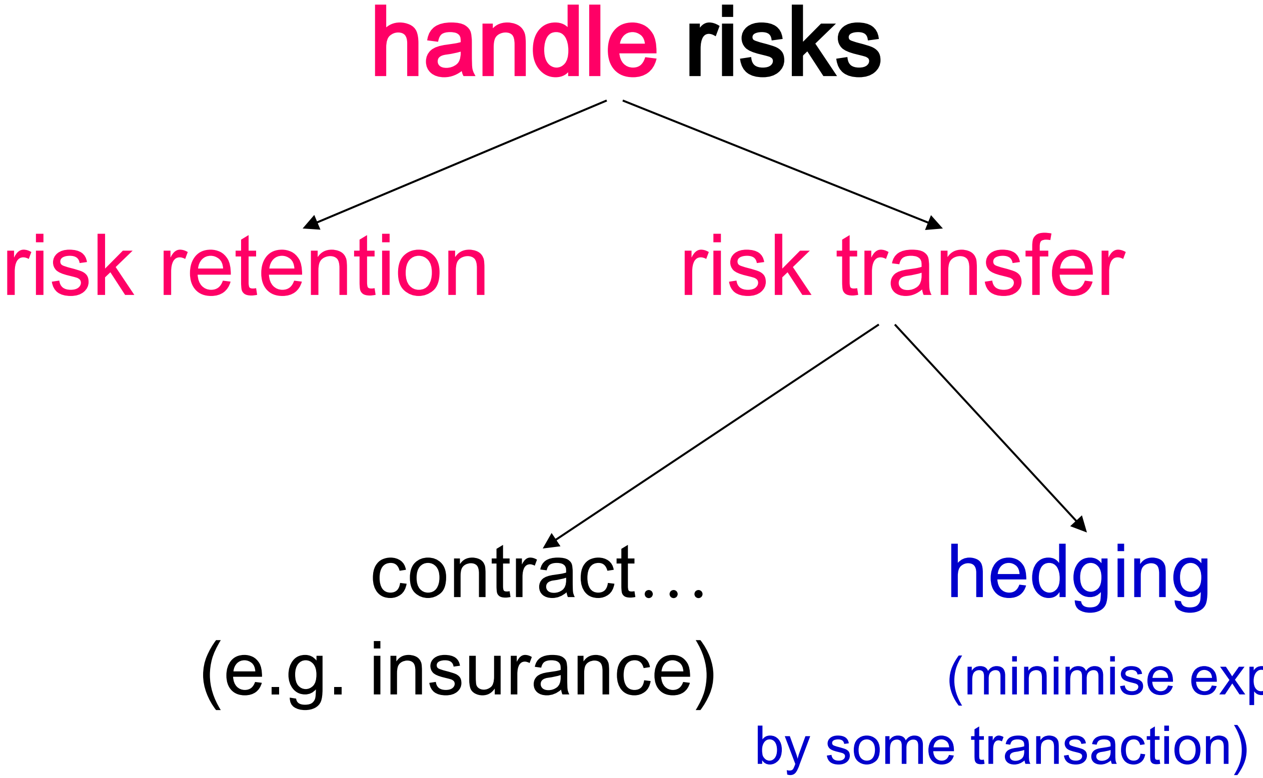
Risk Management = 1+2

A risk is the potential for something unwanted to happen (e.g., loss of C-I-A)

1. Measuring or/and assessing risks

2. Developing strategies and solutions to manage risks:
    - reduce/avoid and
    - handle risks

**Risk Management contd…



handle risks

risk retention

risk transfer

contract…
(e.g. insurance)

hedging

(minimise exposure
by some transaction)

Residual Risk = def

what remains after defences are in place…

Defenders

3 Actions of Defenders

- Prevent
- Detect
- Respond

Types of Prevention

- Deter (discourage)
- Hinder (make harder)

Detection and Recovery

Detect

- Monitoring/logging
- Anomaly analysis

Recover

- Incident management
- Forensics
- Change procedures
- Install new technologies

Reasoning about security

Attack trees

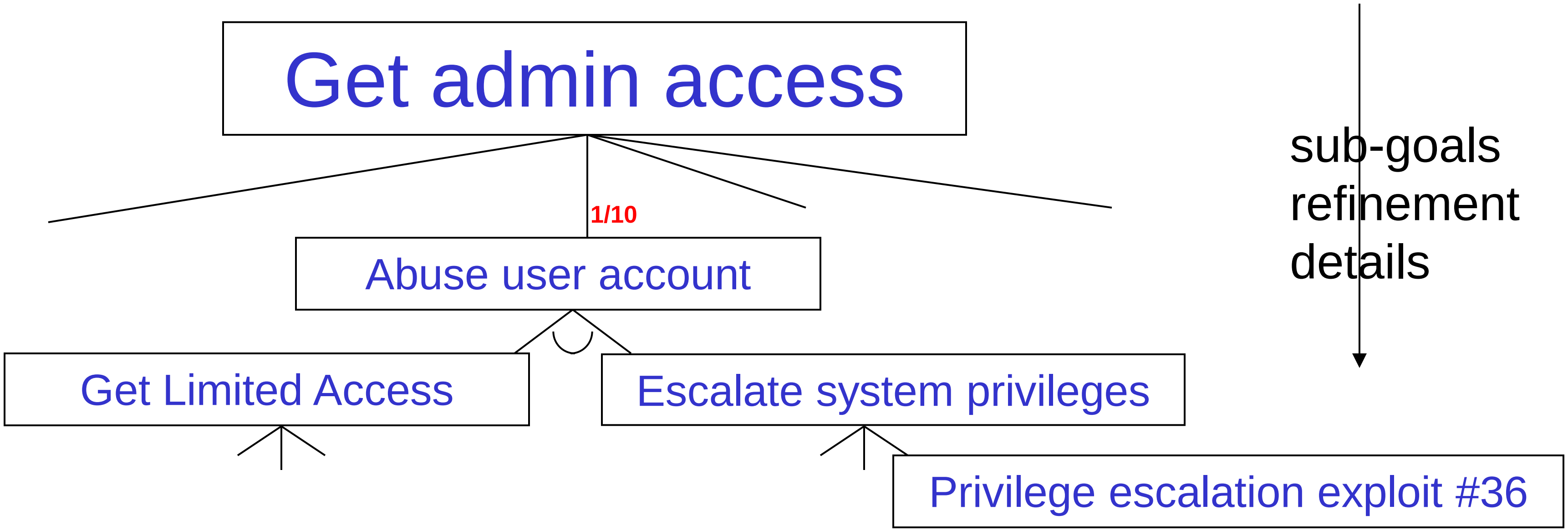
Attack tree

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



Get admin access

1/10

Abuse user account

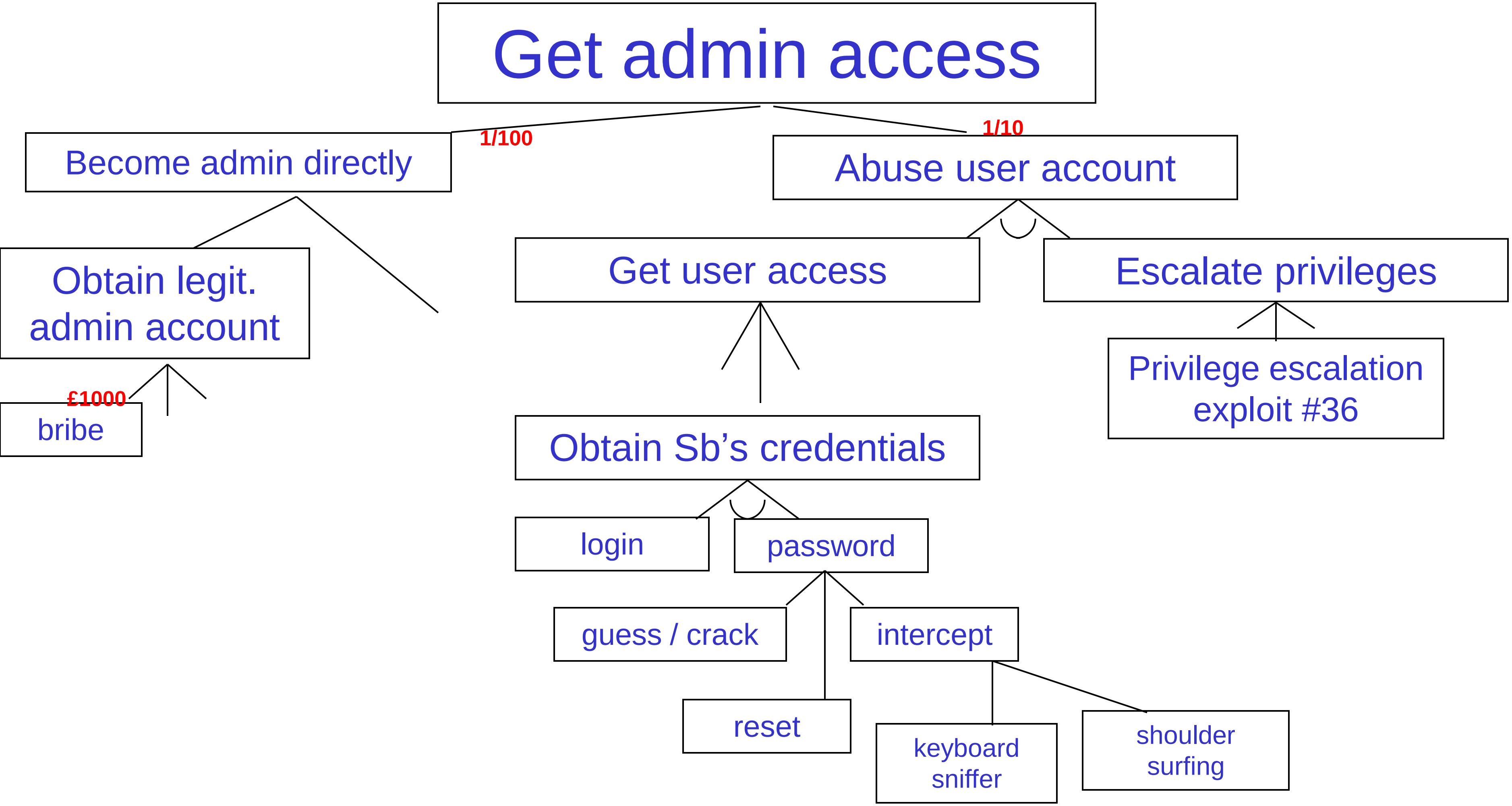
Get Limited Access

Escalate system privileges

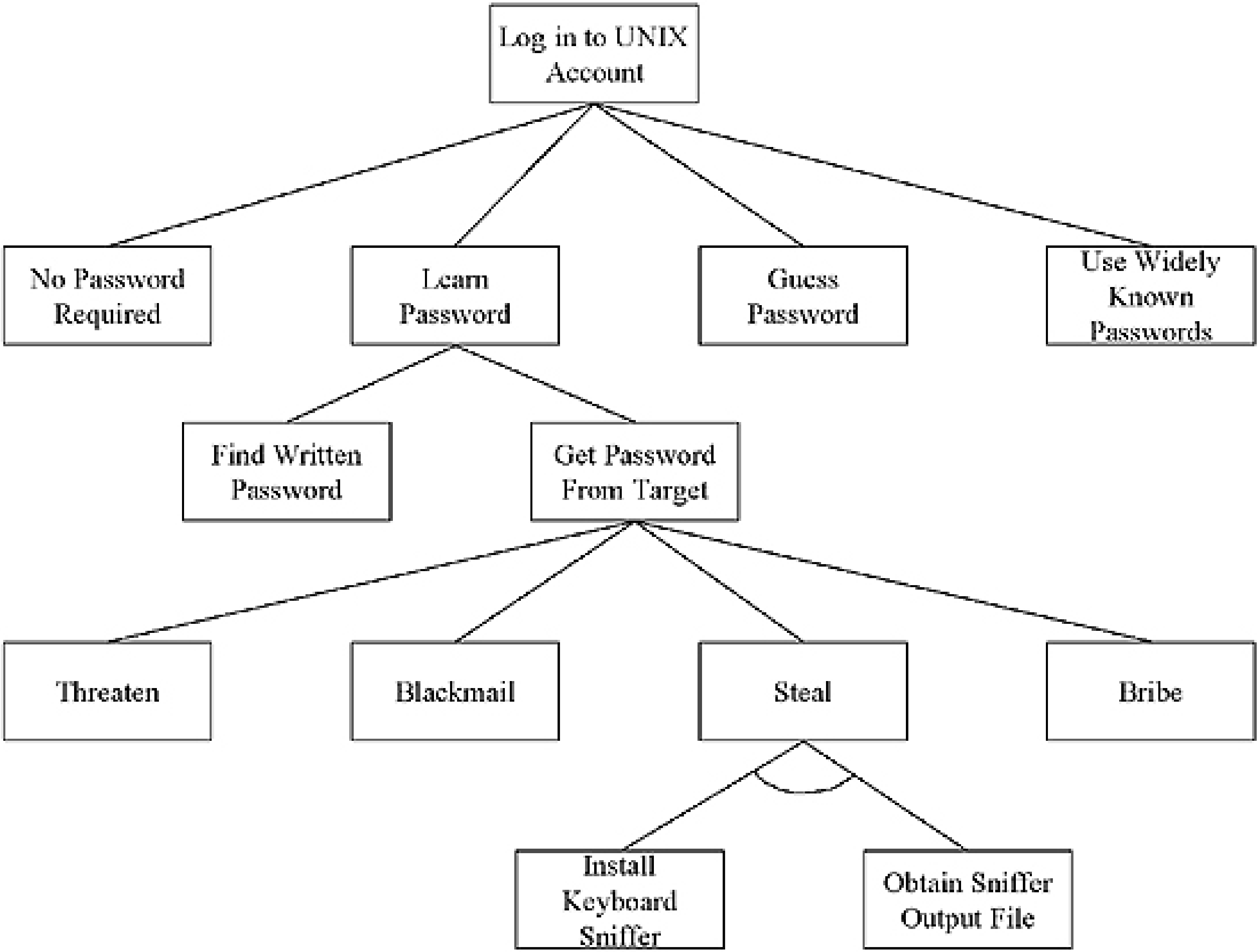
Privilege escalation exploit #36

sub-goals
refinement
details

Expanded Example

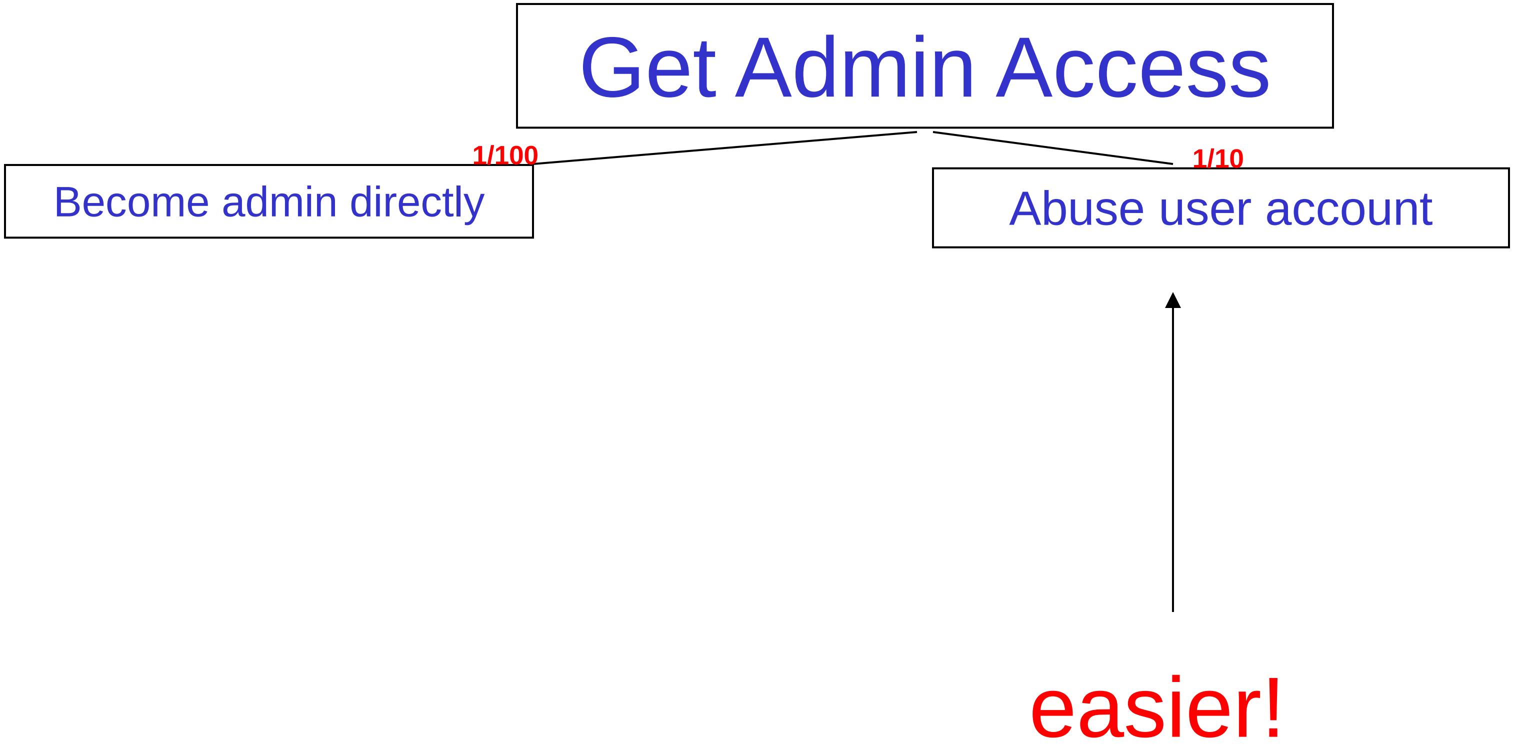


Unix Log In


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

Weakest Link

Security like a chain:



Get Admin Access

1/100

Become admin directly

1/10

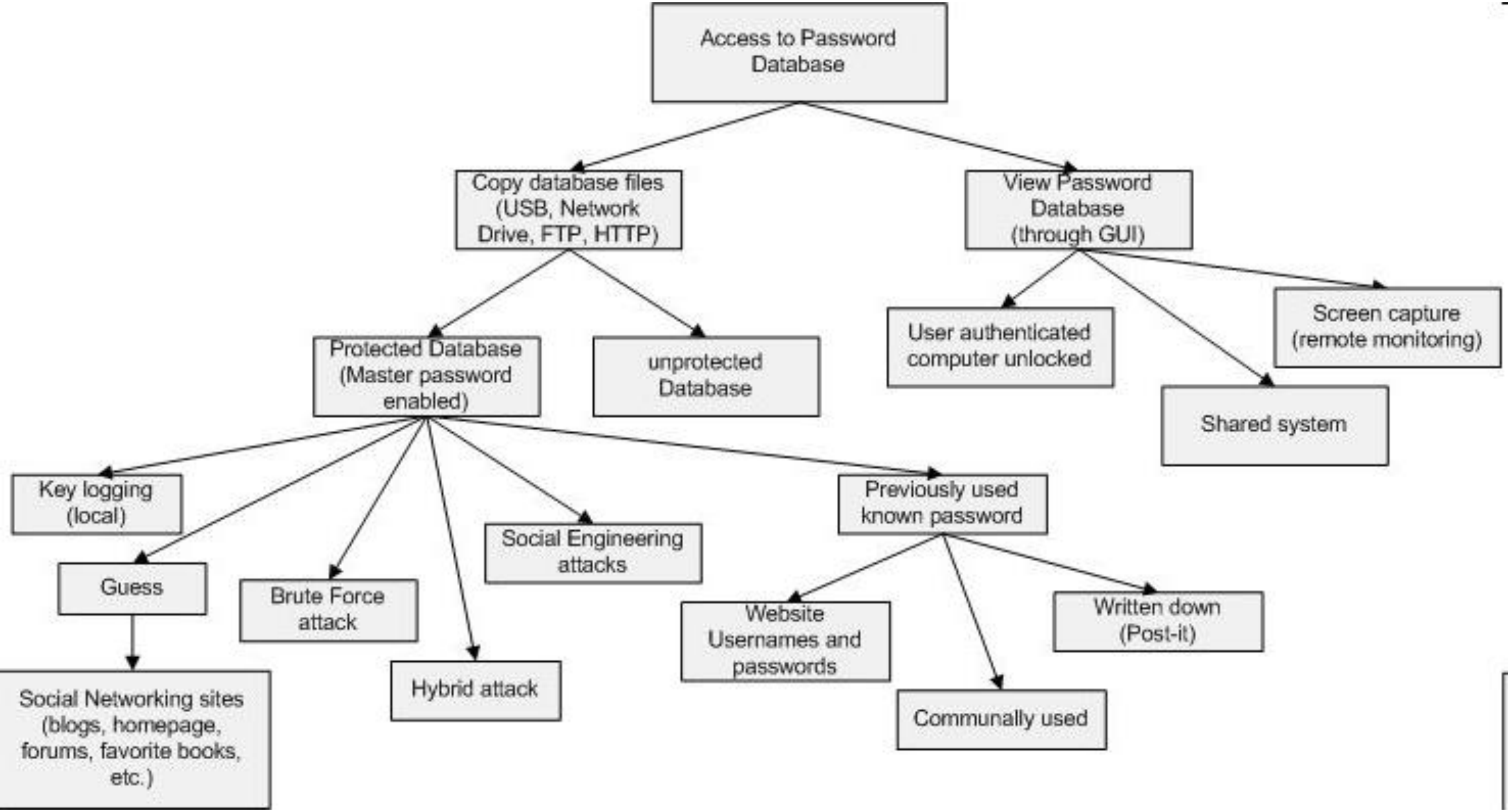
Abuse user account

easier!

Accessing Password Database

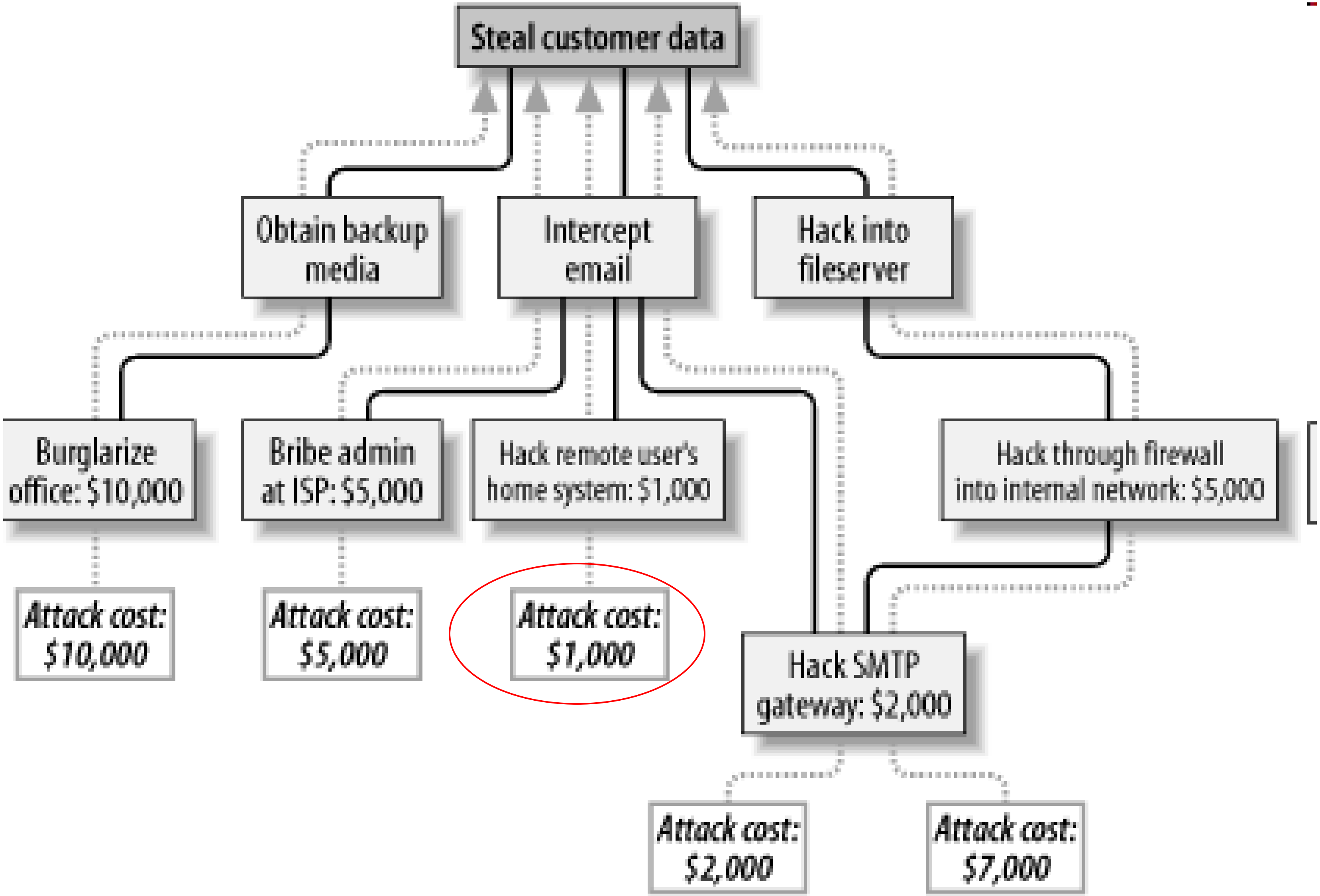
Class brainstorm

Accessing Password Database

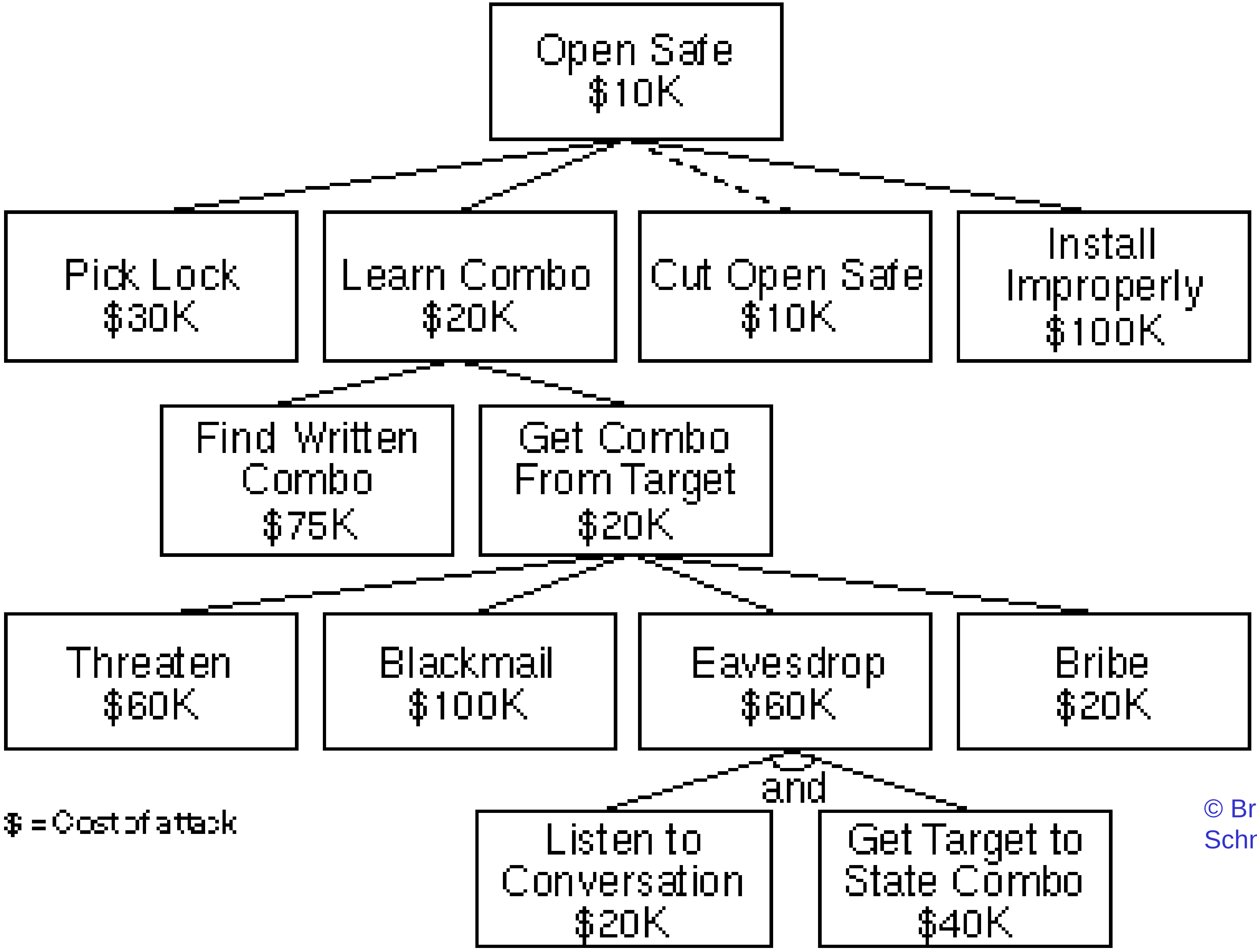


Access to Password Database
Copy database files (USB, Network Drive, FTP, HTTP)
View Password Database (through GUI)
Protected Database (Master password enabled)
unprotected Database
User authenticated computer unlocked
Screen capture (remote monitoring)
Shared system
Key logging (local)
Guess
Brute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

Stealing Data with Costs

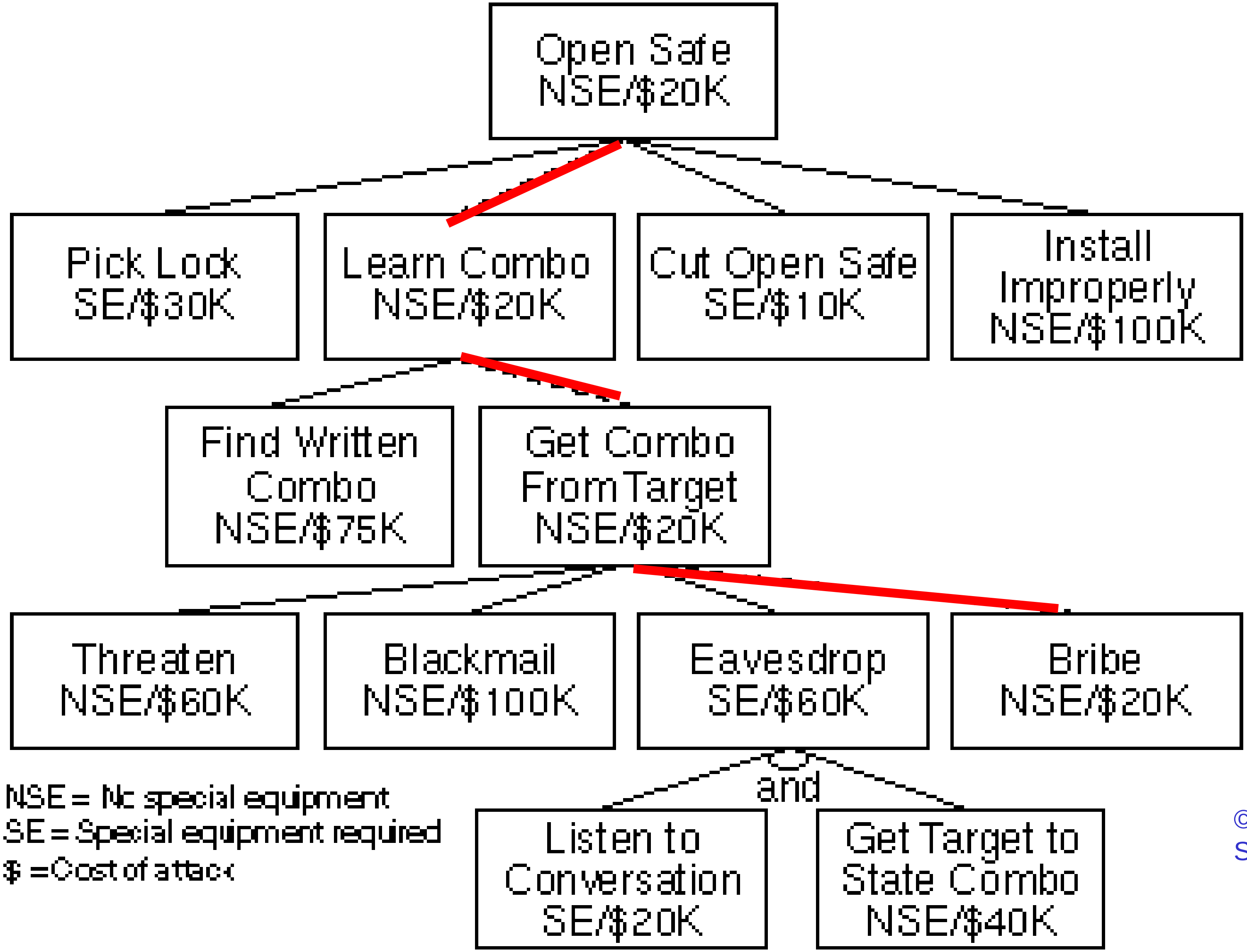


Opening a Safe with Costs



© Bruce Schneier

Cheapest Attack without Special Equipment



Open Safe
NSE/$20K

Pick Lock
SE/$30K

Learn Combo
NSE/$20K

Cut Open Safe
SE/$10K

Install Improperly
NSE/$100K

Find Written Combo
NSE/$75K

Get Combo From Target
NSE/$20K

Threaten
NSE/$60K

Blackmail
NSE/$100K

Eavesdrop
SE/$60K

Bribe
NSE/$20K

and

Listen to Conversation
SE/$20K

Get Target to State Combo
NSE/$40K

NSE = No special equipment
SE = Special equipment required
$ = Cost of attack

© Bruce Schneier

Secrecy vs. Transparency

Open source vs. closed source

and security

Class brainstorm

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.

It doesn’t mean that companies should disclose their designs.

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

When is open source security good?

- Cryptography
  - AES, RSA, SHA256 etc, heavily tested, not yet broken
  - Compare closed-source crypto
    - Oyster card, car immobilisers, broken in months

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

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

Ethics

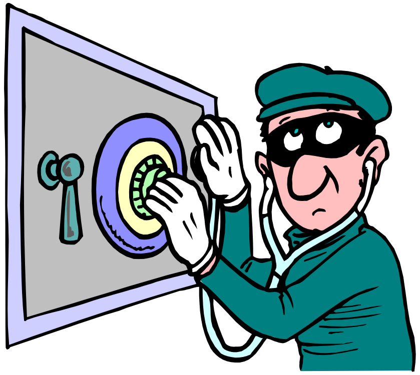
or should Karate classes be legal?

Key Question:

Is actively researching serious security vulnerabilities socially desirable?

- Of Course Yes!

…will tell you every professional hacker and every academic code-breaker…



Bruce Schneier [14 May 2008]:

Problem: A hacker who discovers one [attack] can sell it on the black market, blackmail the vendor with disclosure, or simply publish it without regard to the consequences

Q: […] is it ethical to research new vulnerabilities?

A: Unequivocally, yes. [according to Schneier]

Because:

- Vulnerability research is vital because it trains our next generation of computer security experts

http://www.schneier.com/blog/archives/2008/05/the_ethics_of_v.html

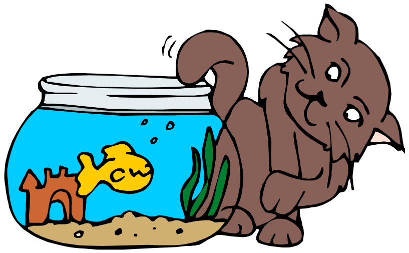
Responsible disclosure

Researchers should disclose vulnerabilities to the system owners, and give them "reasonable time" to fix them

especially if

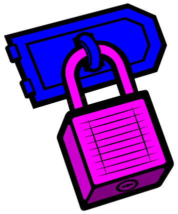
…these vulnerabilities are likely to be rediscovered

Cf. E. Rescorla. "Is finding security holes a good idea?" In 3rd Workshop on the Economics of Information Security (2004)



Benefits:

Disclosure creates incentives
for fixing these vulnerabilities



Companies advertise bounties
= rewards for finding bugs/vulnerabilities

Are people the weakest link in computer security?

“Cybersecurity professionals have spent the last 25 years saying **people are the weakest link**. That’s stupid! They cannot possibly be the weakest link – they are the people that create the value at these organisations”

“What that tells me is that the **technical systems** we’ve built **are not built for people**. Techies build systems for techies, they don’t build technical systems for normal people”

Ian Levy, NCSC Director

The Guardian, 22 Sept 2017