Aspetos Socio Profissionais da Informática

Security in the Internet: Issues, Challenges and the Way Forward

Departamento de Informática da

FCT/UNL

Lecture Outline

- The Internet Security Architecture, its Flaws and Cons
- Security and Examples of Ethical Challenges
- The Way Forward: How to Deal With These Challenges

These slides are (very partially) based on slides from Chapter 7 of Michael J. Quinn, "Ethics for the Information Age"

Internet Security Architecture

Flaws and Cons

Driving Goals of The Internet Project

- Communication should continue despite failures
  - Survive equipment failure or physical attack
  - Traffic between two hosts continue on another path
- Support multiple types of communication services
  - Differing requirements for speed, latency, & reliability
  - Bidirectional reliable delivery vs. message service
- Accommodate a variety of networks
  - Both military and commercial facilities
  - Minimize assumptions about the underlying network

Open to all types of applications and innovation

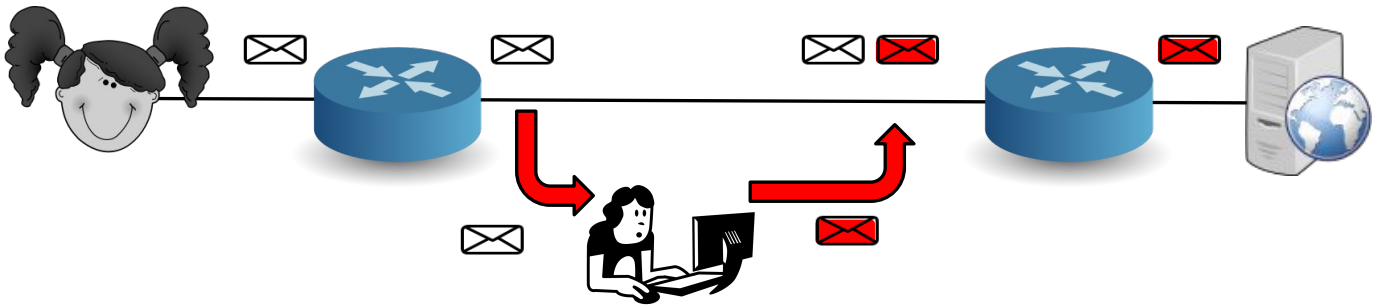
Driving Goals not Met or Absent

- Permit distributed management of resources
  - As many nodes are managed by different institutions, this is still rather challenging
  - Inside each separated network management may be simpler
- Accountability for use of resources
  - Inside each separated network management may be simpler
  - Complex and unsolved problem at large
  - solutions still fairly limited and immature
- Trustable
  - Can we trust a system made of many parts and managed by different institutions ?
  - are the end-to-end arguments enough ?

Security and Accountability

- Security was considered an end-systems problem
  - It has become a mess and a big challenge
  - In the end it requires careful trade-off analysis

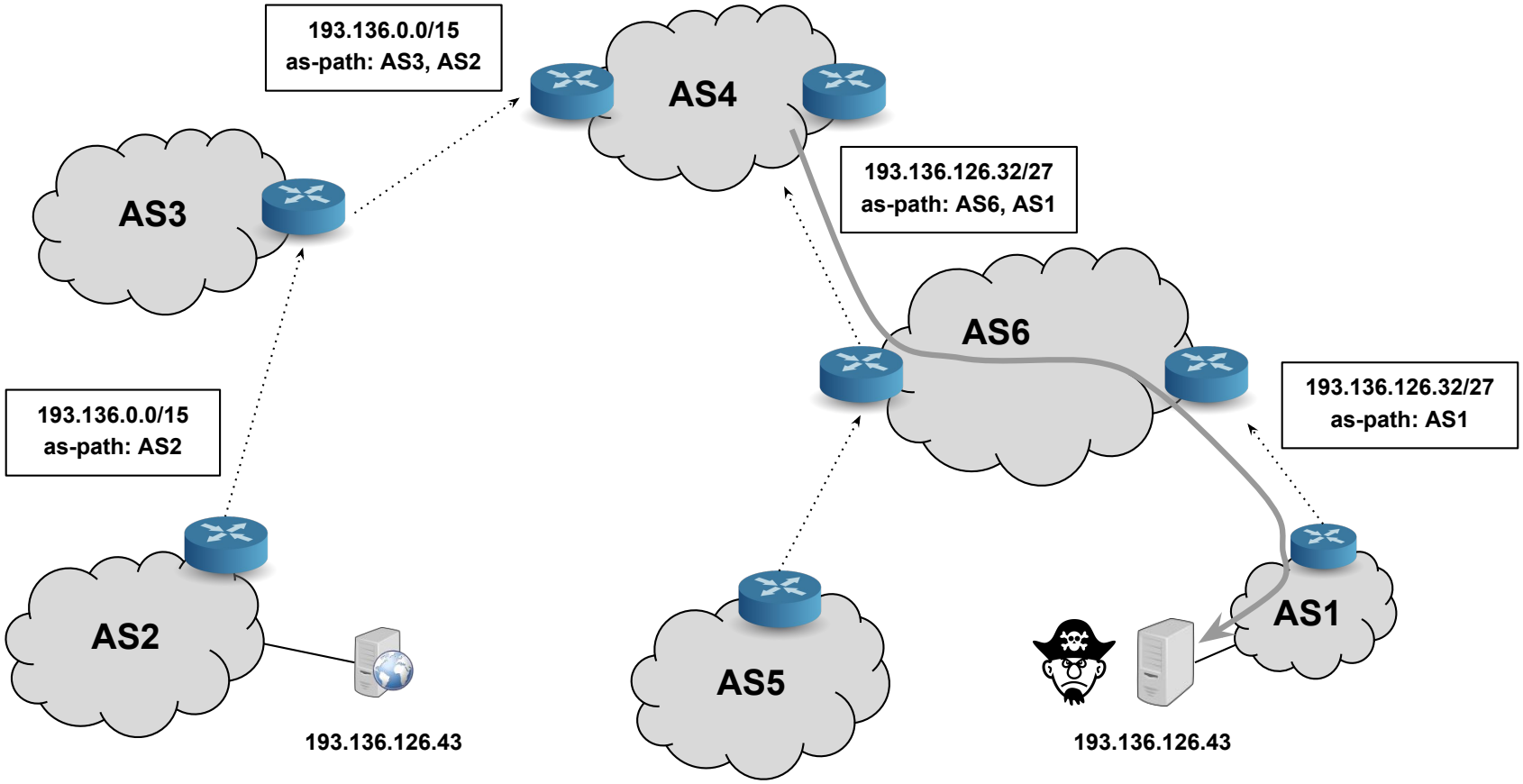
- Accountability is a distributed problem and becomes extremely complex at scale
  - Nodes and resources managed by different institutions



Source Address: What if Source Lies?

- Source address should be the sending host
  - But, who's checking, anyway?
  - You could send packets with any source you want
- Why would someone want to do this?
  - Launch a denial-of-service attack
  - Evade detection by "spoofing"
    - But, the victim could identify you by the source address
    - So, you can put someone else's source address in the packets
  - Also, an attack against the spoofed host
    - Spoofed host is wrongly blamed
    - Spoofed host may receive return traffic from the receiver

BGP Security (BGP Hijacking)



Internet Security Architecture

A Curse or a Blessing?

Higher Level Attacks

- Malware
  - Virus, Worms, Many forms of attacks using HTTP + servers and browsers software weakness, Trojan horses, Spyware, …
- Hacking
  - Modern meaning of hacker: someone who gains unauthorized access to computers and computer networks (it is common but against the law)
  - Bots: transform a user computer in an unsuspected attack machine remotely controlled (DDoS, Spam, …)

Hackers, Past and Present

- Original meaning of hacker: explorer, risk taker, system innovator
- 1960s-1980s: Focus shifted from electronics to computers and networks
- Modern meaning of hacker: someone who gains unauthorized access to computers and computer networks
- "Ethical hacking" using hackers' tools, but not the methods, to increase systems resilience to security attacks – hard to correctly implement

Ethical Case Study: Sidejacking

- Sidejacking: hijacking of an open Web session by capturing a user's cookie
- Sidejacking possible on unencrypted wireless networks because many sites send cookies "in the clear"
- Internet security community complained about sidejacking vulnerability for years, but ecommerce sites did not change practices

Firesheep

- October 2010: Eric Butler released Firesheep extension to Firefox browser
- Firesheep made it possible for ordinary computer users to easily sidejack Web sessions
- More than 500,000 downloads in first week
- Attracted great deal of media attention
- Early 2011: Facebook and Twitter announced options to use their sites securely

Utilitarian Analysis

- Release of Firesheep led media to focus on security problem
- Benefits were high: a few months later Facebook and Twitter made their sites more secure
- Harms were minimal: no evidence that release of Firesheep caused big increase in identity theft or malicious pranks
- **Conclusion: Release of Firesheep was good**

Kantian Analysis

- Accessing someone else's user account is an invasion of their privacy and is wrong
- Butler provided a tool that made it much simpler for people to do something that is wrong, so he has some moral accountability for their misdeeds
- Butler was willing to tolerate short-term increase in privacy violations in hope that media pressure would force Web retailers to add security
- He treated victims of Firesheep as a means to an end

It was wrong for Butler to release Firesheep — he should find alternatives

Case Study: The Internet Worm

- Worm
  - Self-contained program
  - Spreads through a computer network
  - Exploits security holes in networked computers

The Internet Worm

- Robert Tappan Morris, Jr.
  - Graduate student at Cornell
  - Released worm onto Internet from MIT computer
- Effect of worm
  - Spread to significant numbers of Unix computers
  - Infected computers kept crashing or became unresponsive
  - Took a day for fixes to be published
- Impact on Morris
  - Suspended from Cornell
  - 3 years' probation + 400 hours community service
  - $150,000 in legal fees and fines

Ethical Evaluation

- Kantian evaluation
  - Morris used others by gaining access to their computers without permission
- Social contract theory evaluation
  - Morris violated property rights of organizations
- Utilitarian evaluation
  - Benefits: Organizations learned of security flaws
  - Harms: Time spent by those fighting worm, unavailable computers, disrupted network traffic, Morris's punishments

Morris was wrong to have released the Internet worm

Bots

- Bot: A kind of backdoor Trojan that responds to commands sent by a command-and-control program on another computer
- First bots supported legitimate activities
  - Internet Relay Chat
  - Multiplayer Internet games
- Other bots support illegal activities
  - Distributing spam
  - Collecting person information for ID theft
  - Denial-of-service attacks

Rootkits

- Rootkit: A set of programs that provides privileged access to a computer
- Activated every time computer is booted
- Uses security privileges to mask its presence

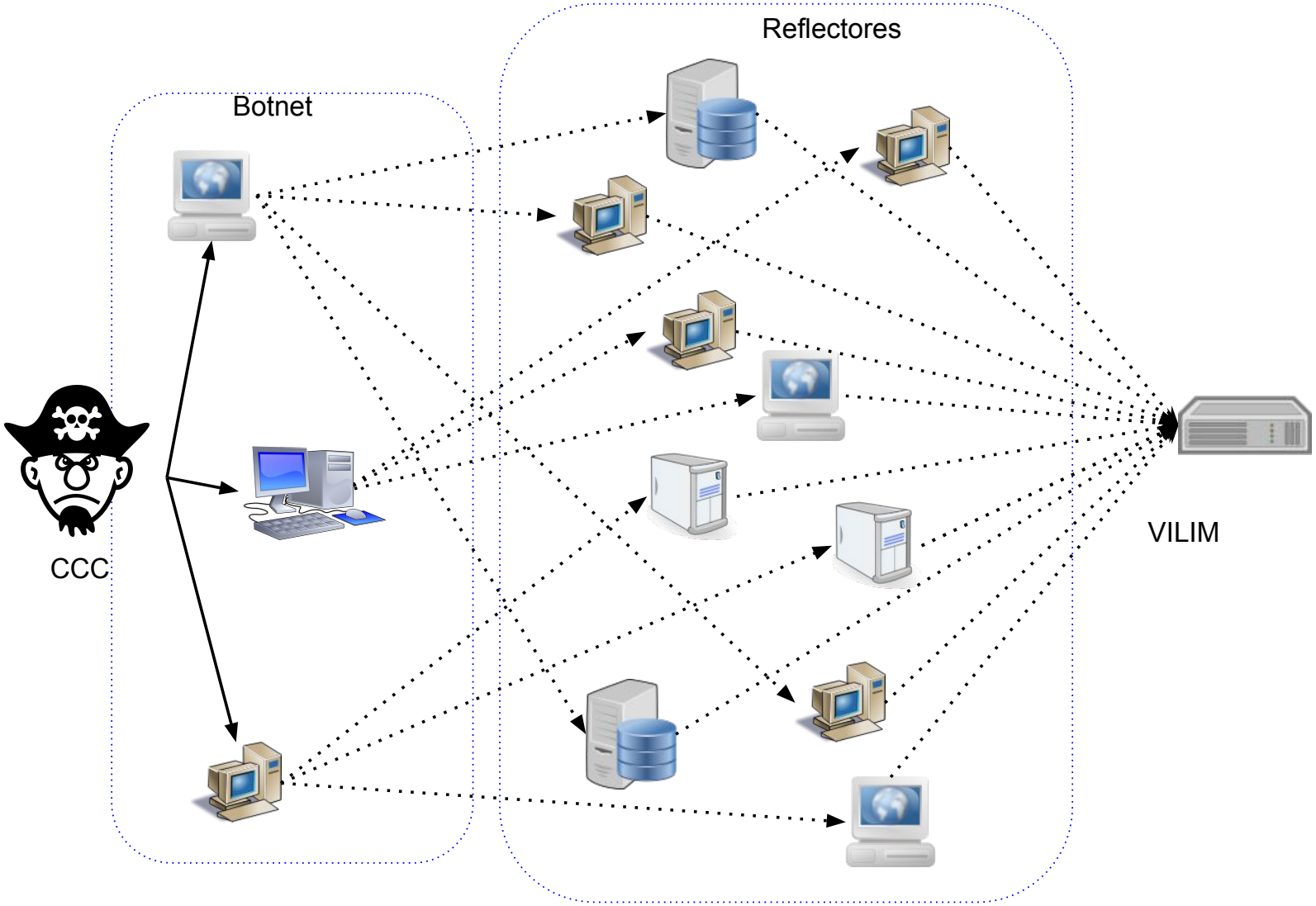
Botnets and Bot Herders

- Botnet: Collection of bot-infected computers controlled by the same command-and-control program
- Some botnets have over a million computers in them
- Bot herder: Someone who controls a botnet
- IoT botnet: a botnet made of IoT devices (e.g. Mirai botnet specialized in networked devices running Linux, like IP cameras, home routers, …)

Denial-of-service and Distributed Denial-of-service Attacks

- Denial-of-service attack: Intentional action designed to prevent legitimate users from making use of a computer service
- Aim of a DoS attack is not to steal information but to disrupt a server's ability to respond to its clients
- Distributed denial-of-service attack (DDoS): DoS attack launched from many computers, such as a botnet

Reflection DDoS Attacks



The Rise and Fall of Blue Security
Part I: The Rise

- Blue Security: An Israeli company selling a spam deterrence system
- Blue Frog bot would automatically respond to each spam message with an opt-out message
- Spammers started receiving hundreds of thousands of opt-out messages, disrupting their operations
- 6 of 10 of world's top spammers agreed to stop sending spam to users of Blue Frog

The Rise and Fall of Blue Security Part II: The Fall

- One spammer (PharmaMaster) started sending Blue Frog users 10-20 times more spam
- PharmaMaster then launched DDoS attacks on Blue Security and its business customers
- Blue Security could not protect its customers from DDoS attacks
- Blue Security reluctantly terminated its anti-spam activities

Lessons

- It is hard to fight attackers by usng their own methods

- Example: figthing a bot net using another bot net

Politically Motivated Cyber Attacks

There is evidence that many take place using all kinds of technics, including DDoS

Attacks on Social Networking Sites

- Massive DDoS attack made Twitter service unavailable for several hours on August 6, 2009
- Three other sites attacked at same time: Facebook, LiveJournal, and Google
- All sites used by a political blogger from the Republic of Georgia
- Attacks occurred on first anniversary of war between Georgia and Russia over South Ossetia

Anonymous

- Anonymous: loosely organized international movement of hacktivists (hackers with a social or political cause)
- Various DDoS attacks attributed to Anonymous members

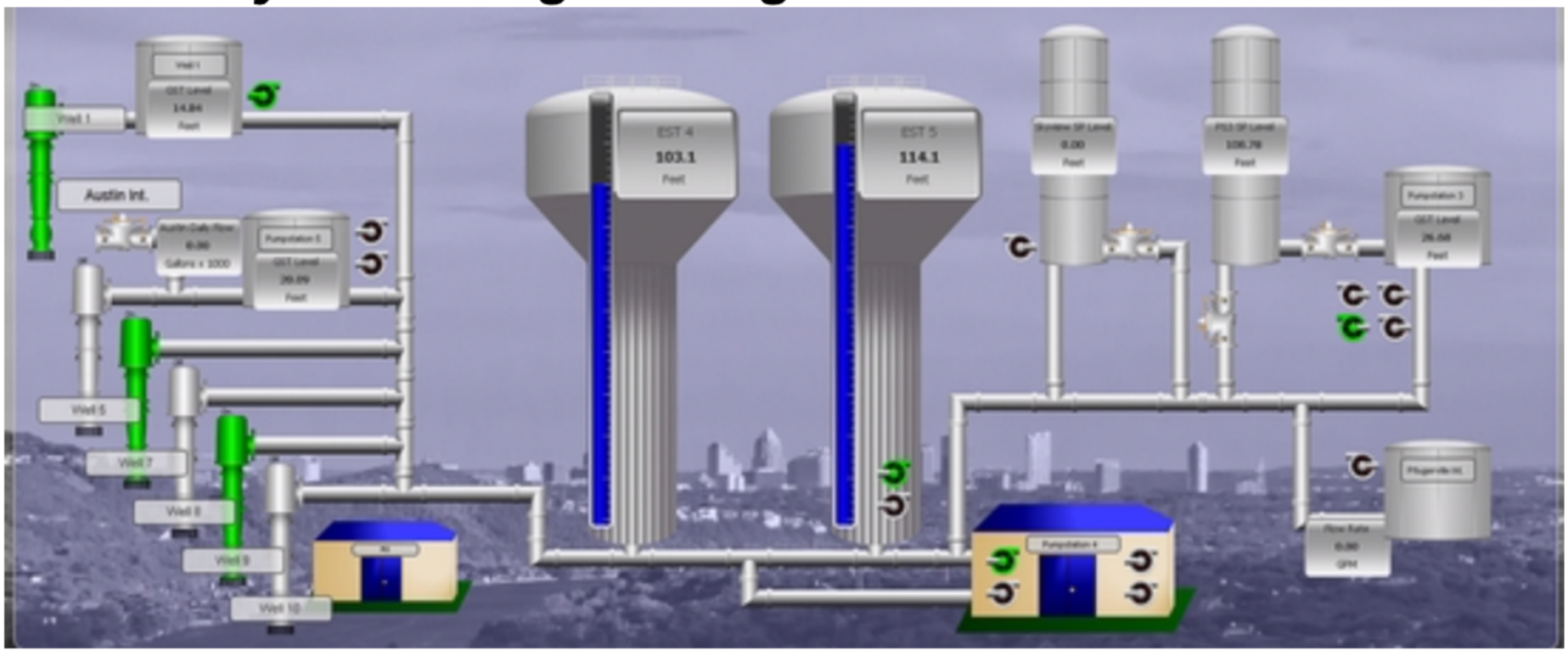
Year	Victim	Reason
2008	Church of Scientology	Attempted suppression of Tom Cruise interview
2009	RIAA, MPAA	RIAA, MPAA's attempt to take down the Pirate Bay
2009	PayPal, VISA, MasterCard	Financial organizations freezing funds flowing to Julian Assange of WikiLeaks
2012	U.S. Dept. of Justice, RIAA, MPAA	U.S. Dept. of Justice action against Megaupload

Supervisory Control and Data Acquisition (SCADA) Systems

- Industrial processes require constant monitoring
- Computers allow automation and centralization of monitoring
- Today, SCADA systems are open systems based on Internet Protocol
  - Less expensive than proprietary systems
  - Easier to maintain than proprietary systems
  - Allow remote diagnostics
- Allowing remote diagnostics creates security risk

SCADA Systems Carry Security Risks

SCADA Systems Engineering



Siemens SCADA System

Stuxnet Worm (2009)

- Attacked SCADA systems running Siemens software
- Targeted five industrial facilities in Iran that were using centrifuges to enrich uranium
- Caused temporary shutdown of Iran's nuclear program
- Worm may have been created by Israeli Defense Forces

Innovation and Ethical Analysis

- Sometimes it is very tempting to introduce new innovative ways of doing something
- It may result in an high level of productivity increase and extra convenience for users
- Does it may have any ethical implications?

(Besides destroying jobs)

Risks of Online Voting

- Gives unfair advantage to those with home computers
- More difficult to preserve voter privacy
- More opportunities for vote selling
- Obvious target for a DDoS attack
- Security of election depends on security of home computers
- Susceptible to vote-changing virus
- Susceptible to phony vote servers
- No paper copies of ballots for auditing or recounts

Utilitarian Analysis

- Suppose online voting replaced traditional voting
- Benefit: Time savings
  - Assume 50% of adults actually vote
  - Suppose voter saves 1 hour by voting online
  - Average pay in U.S. is $21.00 / hour
  - Time savings worth $10.50 per adult American
- Harm of DDoS attack difficult to determine
  - What is probability of a DDoS attack?
  - What is the probability an attack would succeed?
  - What is the probability a successful attack would change the outcome of the election?

Kantian Analysis

- The will of each voter should be reflected in that voter's ballot, otherwise why vote? (first categorical imperative)
- The integrity of each ballot is paramount
- Ability to do a recount necessary to guarantee integrity of each ballot
- There should be a paper record of every vote
- Eliminating paper records to save time and/or money is wrong if the new voting system doesn't have the exact same features as the paper one

Dealing With The Challenges of Security

- Education and Training
- Moral and Ethical Awareness
- The Law mainly deals with the attacker
- And sometimes includes indemnities for the offended

- Are software companies made responsible by the weaknesses of their products?
  - In general they only face reputational consequences

The Applicable Laws in Portugal (1)

- Regime Jurídico da Segurança do Ciberespaço - Lei n.º 46/2018, de 13 de Agosto
  - Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (muito dirigido à segurança das infraestruturas)

- Decreto - Lei n.º 81/2016, de 28 de Novembro
  - Cria a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (https://www.policiajudiciaria.pt/unc3t)

- Que tem por objetivos combater os crimes previstos:
  - Lei nº 109/2009, de 15 de Setembro
  - Código dos direitos de autor, leis da proteção de dados pessoais, e ainda outras figuras de crimes tecnológicos.

The Applicable Laws in Portugal (2)

- Lei do Cibercrime (Lei n.º109/2009 de 15 de Setembro)
  - Decorre da Convenção de Budapeste

- Estratégia Nacional de Segurança do Ciberespaço (RCM 36/2015 de 12 de junho)
  - Está em processo legislativo nova versão da ENSC

- EU Cybersecurity Act (13/09/2017)
  - https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en/

Security by Design

The OWASP (Open Web Application Security Project) security design principles are as follows:

- Asset clarification. ...
- Understanding attackers. ...
- Core pillars of information **security**. ...
- **Security** architecture. ...
- Minimise attack surface area. ...
- Establish **secure** defaults. ...
- The **principle** of Least privilege. ...
- The **principle** of Defence in depth

The Cost of Security

1. Security is Expensive
2. Therefore it must be imposed by regulations and laws
3. To be insecure should be made more expensive than being secure

Conclusion

- For good, the Internet is a fully decentralized infra-structure
- For bad, its inner layers have none or very reduced support for security and accounting
- Security is end-systems responsibility
- Current Law makes attackers responsible for their acts
- But leaves professionals and software manufacturers exempt of their responsibility
- We need regulation making software vendors liable for their products