# Internet Crime

**2-3 hours**

**Ernst L. Leiss**
**Department of Computer Science**
**University of Houston**
coscel@cs.uh.edu

**Support of this research under NSF grants 0313880, 0453498, 0519316 and 1241772 is acknowledged**

Any opinions, findings, conclusions, or recommendations expressed herein are those of the authors and do not reflect the views of the National Science Foundation

# Contents

1. Introduction (~15 min)
2. Common Crimes Facilitated by the Internet (~15 min)
    - 2.1 Common crimes with economic purposes or motivation
    - 2.2 Vandalism
3. Internet Crimes (~30 min)
4. What Is a Crime? (~15 min)
5. Two Case Studies (~30 min)
6. Child Pornography (~15 min)
7. Protections Against Internet Crime (~30 min)
8. Conclusion

# 1. Introduction

## Crime

### Will use a more general definition than the legal one:

Activities that are either considered criminal in a significant number of countries where the Internet is used, or that are generally considered to be extremely undesirable and detrimental to society at large.

### No universality implied

Legal standards are local, the Internet is a global commodity

### Core of tension

between local and global standards/norms

# 2. Common Crimes Facilitated by the Internet

## 2.1 Common crimes with economic purposes or motivation

**Crimes that have existed before the Internet**
**The Internet is a tool that facilitates their commission**
**Generally recognized by most jurisdictions as legal crimes**

**Theft of funds through electronic means**
**Espionage**
**Theft of intellectual property (IP)**

**Detection often harder, delayed**

things exist uniquely, electronic IP can be copied freely;
thus, a thing that is taken is gone, but a file that is taken/copied is not

**Immediacy** once detected, measures can be taken immediately

**Familiarity of law enforcement with ordinary crime but not with crime within electronic context**

## Theft of funds through electronic means

- **Subverting EFT systems** (Electronic Funds Transfer)
- **Subverting ATMs and the PINs involved** (Automatic Teller Machines, Personal Identification Number)

## Industrial espionage

- **Stealing trade or company secrets**
  - **Using memory sticks or CD-ROMs** (Compact Disk Read-Only Memory)
  - **Using network facilities**
- **Using viruses/worms to scan files for key words and post those files somewhere**

## Theft of IP

- **Pirated software**
- **Pirated movies**
- **File sharing of videos and music** copying is an infringement of IP rights

## 2.2 Vandalism

No direct enrichment objective (although vandalism is sometimes used to blackmail targets)

- Viruses and worms
- Denial of service

## Viruses and worms

Have existed since at least 1983 (Fred Cohen)

Internet greatly facilitated their spread

All are able to change information, but most just destroy

## Denial of service (DoS)

Caused indirectly by the destruction of files by viruses

More often, attempts to overwhelm sites by excessive traffic

Today, all successful DoS attacks are distributed

# 3. Internet Crimes

## Crimes specifically related to and dependent on the Internet

Distributed denial of service
Spy ware
Spam
Spoofing, phishing
Violation of copyrights of IP
Distribution of undesirable material of information

## Distributed denial of service (DDoS)

DDoS extends DoS

Install attacking programs (bots) at thousands of (unsuspecting) systems (bot nets)

Upon a prompt, all programs send many spurious service requests in a coordinated way to the targeted site

# Spy ware

**Major threat to people's privacy**

**Software that monitors a computer user's activities**

**Installed without the user's knowledge**

- Via viruses or unguarded downloads

**Reports actively or is queried remotely about recorded activities**

**Collects confidential information, e. g.,**

- Credit card numbers
- PINs
- Passwords

**Collects information about visited web sites, etc.**

**ActiveX**

# Spam

**No universal definition**

**Somebody's spam may be someone else's useful information**

**Challenge-response schemes**

- Allow to distinguish between programs spewing out spam and humans (application of artificial intelligence)

# Spoofing, phishing

## IP spoofing, ARP spoofing (for man-in-the-middle attacks), e-mail spoofing

**IP spoofing** is the creation of Internet Protocol packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system

In **ARP spoofing,** an attacker sends fake Address Resolution Protocol (ARP) messages onto a Local Area Network with the aim of associating the attacker's MAC address with the IP address of another host, causing any traffic meant for that IP address to be sent to the attacker instead.

**E-mail spoofing** is the creation of email messages with a fake sender address, facilitated because protocols do no authentication. Spam and phishing emails typically use such spoofing to mislead the recipient about the origin of the message

## Social engineering

Attacker fools victim to provide confidential information
Often uses spam
Often redirects to a fake bank web site
Requires users to be unguarded (stupid)

## Major source of identity theft

Successful attacker obtains credit cards or opens bank accounts in the victims' name and uses their credit lines

## No technical means for preventing human stupidity

# Bullying

**Social media**

Play major role in bullying

Anonymity

Difficulties in prosecution:

What crime? First Amendment.

How to identify unequivocally the perpetrator

# Internet Business Model

**Spam has existed well before the Internet but required a higher hit rate (about 2-3 per 100) to be economically viable**

**No charge to transmit files on Internet (low fixed cost, virtually no variable cost)**

**Free spam messages = very low success rate ok (1 hit per million)**

# Possible solutions (controversial):

**Charging for transmission (perhaps per MByte)**

**Required registration/certification of senders**

# Violation of copyrights of IP

**Peer-to-peer (P2P) file sharing**

Distributed, BitTorrent

**Extensive discussion of morality of copyright in the digital era**

**WIPO (UN's World Intellectual Property Organization)**

# Distribution of undesirable material of information

**Clashes between jurisdictions and 'netizens' (citizens of the net)**

States wish to enforce their laws, the Internet is 'everything goes'

**Banning vs. permissiveness**

Local laws vs. information superhighway

**Which state is to define Internet behavior?**

# 4. What Is a Crime?

**Legally requires existence of a law**
**Laws are creations of states :: fundamentally local**

**Internet**

**Spans every inhabited time zone**
**Touches many, very different cultures, societies, and states**
**Is not governed by any single country**

**Is used in the transmission of digital objects that states wish to regulate or ban according to their local laws (jurisdictions)**

**If two jurisdictions are involved for sender and receiver, which rules?**
**What about points, through which the transmission passes?**

**Very controversial for one country to apply its laws to residents of another**

# 5. Two Case Studies

**In both:**

**Regulation vs. Freedom of Speech**

**Local laws Anchored in US Constitution**

## Pornography

**No global definition: community standards**

Issue of different jurisdictions with differing standards

Even true within the US (different states/localities have different standards), but more so among different countries

**(1) A sends B a digital object Vid using the Internet**

**In A's jurisdiction: Vid is not pornographic**

**In B's jurisdiction: Vid is pornographic**

**Whose jurisdiction applies? A, B?**

**Kansas court case: B applies to receiver (obvious) and sender (not as obvious)**

**(2) A sends B a digital object Vid using the Internet, transmission passes through C**

**In A's and B's jurisdictions: Vid is not pornographic**

**In C's jurisdiction: Vid is pornographic**

**Whose jurisdiction applies? A, B, C?**

**No known US precedent as of early 2014**

# Cryptographic methods

Many countries regulate cryptographic algorithms (state secrets)
Within US, Freedom of Speech greater good

Export limitations :: US Constitution does not apply outside US!

In view of the dual use of cryptography (both military and civilian), in the US restrictions only apply to ‘strong encryption’ (long keys)

Import is not restricted
Re-export of a just imported algorithm is!

# 6. Child Pornography

Generally considered unacceptable, prosecuted by most jurisdictions, with generally draconian penalties

Ostensible motivation: Protecting minors

However, child pornography laws have been applied to drawings as well.

## Complicating factor: Aging software

Software that ages subjects using general image processing techniques
These techniques are usually employed to depict missing children how they would look years later.
Problem: This software can be "run backwards", i. e., instead of increasing the age of the subject, the age can be decreased.

Using aging software run backwards, one can start with legal depictions of sexual activities involving consenting adults and obtain images that constitute child pornography.

Moral dilemma: The initial motivation, protecting minors, is no longer valid.

Many jurisdictions in the USA have held this type of depictions illegal.

Even cartoons depicting sexual activities involving minors have been found in violation of child pornography statues.

This presents a significant challenge to computer scientists.

Clearly, the software itself cannot be considered illegal.

Conceptually, the aging software could be applied in real time. Thus there would be no permanent depiction nor storing of illegal content, only the ephemeral production of images which exist about 30-40 ms before being overwritten.

# 7. Protections Against Internet Crime

## Legal 'protections' don't protect

**Laws only punish carrying out prohibited activities, but do not prevent them (except perhaps through deterrence)**

## Technical protections

**Do prevent prohibited activities** (they are impossible to carry out)

**Encryption**

**Authentication techniques**

**Digital watermarks**

## Cryptography

**Classical or symmetric**

**Public-key**

**Can be used to achieve security and integrity (with some protocols)**

# Authentication techniques

## Passwords

**Pro**: Compact (tens of bytes), easily changed

**Con**: No connection to owner, non-unique

**Exact match required**

## Biometric measurements

**Examples**: Finger prints; Hand geometry; Iris or retina scans; Voice or face recognition

**Pro:** Indesolvable connection to owner

**Con:** Large size, impossible to get new ones when data lost/stolen

**Similarity function**

No two measurements of the same person are identical

**Too lax: false-positive (bad guy gets in)**

**Too restrictive: false-negative (good guy is kept out)**

**Difficult to get no false-positives and few false-negatives**

# Digital watermarks

**Safeguard the integrity of a digital object**

Not applicable to security

**Do not affect its use in any perceptible way**

Invisible to human eye (video) / not audible to human ear (audio)

Human senses are not very acute/can be fooled easily

The information is present and the object is modified, but the human viewer/listener does not perceive the modification

**Mark copies of same object uniquely**

Permits tracing when object passes through various hands

**Copied whenever a watermarked object itself is copied**

Can determine from which legitimate watermarked copy an illegal copy was made

## Safe software

Attackers exploit software vulnerabilities, e. g., buffer overflows

## Buffer overflows

A data structure designed for a certain amount of data is filled with more than that amount of data

Exploited to subvert computer systems (viruses, worms)

Easy to test for, but not done (so-called efficiency == stupidity)

Vulnerabilities can never be completely eliminated, only reduced through good programming practises

<u>Software is the most complex human creation</u>

Operating systems have tens of millions of lines of code
(e. g., MS Vista 65 M loc); not even hundreds of experts are able
to explain every aspect of these complex software suites

# 8. Conclusion

Individuals have responsibilities for preventing cyber crime

- Prudent programming practises
  - Never forego buffer overflow checks and range checks
- General use of protection mechanisms
  - Cryptography, authentication schemes, watermarks
- Prompt installation of patches
- Consistent use of virus detection software
- Use of audit facilities and appropriate follow-up