Cybercrime, Privacy & Ethics

Chapter 19

Dr Naveed Khan

n.khan@ulster.ac.uk

COM398

Introduction

- Cybercrimes and computer crimes
- Intellectual Property
- Privacy
- Ethics

Cybercrime and Computer Crime

Categories of Computer Crime (D.O.J.)

1. Computers as Targets

2. Computers as storage devices

3. Computers as Communications Tools

Cybercrime and Computer Crime

Law Enforcement Challenges

- The deterrent effect of law enforcement on computer and network attacks correlates with the success rate of criminal arrest and prosecution
    - Prosecution is difficult for cybercrime…
        - Requires sophisticated grasp of tech
        - Lack of resources
        - Cybercrime is global, enforcement is often local
            - Initiatives such as “International Convention on Cybercrime” aim to help

Cybercrime and Computer Crime

International Convention on Cybercrime (for reference only)

Table 19.1 **Cybercrimes Cited in the Convention on Cybercrime**

Article 2 Illegal access
The access to the whole or any part of a computer system without right.

Article 3 Illegal interception
The interception without right, made by technical means, of non public transmissions of computer data to, from, or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

Article 4 Data interference
The damaging, deletion, deterioration, alteration, or suppression of computer data without right.

Article 5 System interference
The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.

Article 6 Misuse of devices

a. The production, sale, procurement for use, import, distribution, or otherwise making available of:
   i. A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
   ii. A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5; and

b. The possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Cybercrime and Computer Crime

International Convention on Cybercrime (for reference only)

Article 7 Computer-related forgery

The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Article 8 Computer-related fraud

The causing of a loss of property to another person by:

a. Any input, alteration, deletion, or suppression of computer data;

b. Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Article 9 Offenses related to child pornography

a. Producing child pornography for the purpose of its distribution through a computer system;

b. Offering or making available child pornography through a computer system;

c. Distributing or transmitting child pornography through a computer system;

d. Procuring child pornography through a computer system for oneself or for another person; and

e. Possessing child pornography in a computer system or on a computer-data storage medium.

Article 10 Infringements of copyright and related rights

Article 11 Attempt and aiding or abetting

Aiding or abetting the commission of any of the offences established in accordance with the above Articles 2 through 10 of the present Convention with intent that such offence be committed. An attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

Intellectual Property

Types of Property

- The US legal system distinguishes between three primary types of property:

1. Real Property
   - Land, things attached to land (trees, buildings, stationary homes)
2. Personal Property
   - Personal effects, moveable property and goods (cars, bank accounts, furniture, pets, etc)
3. Intellectual Property
   - **Any tangible asset that consists of human knowledge and ideas**

Intellectual Property

Types of Intellectual Property

- There are three kinds of intellectual property for which legal protection is available:

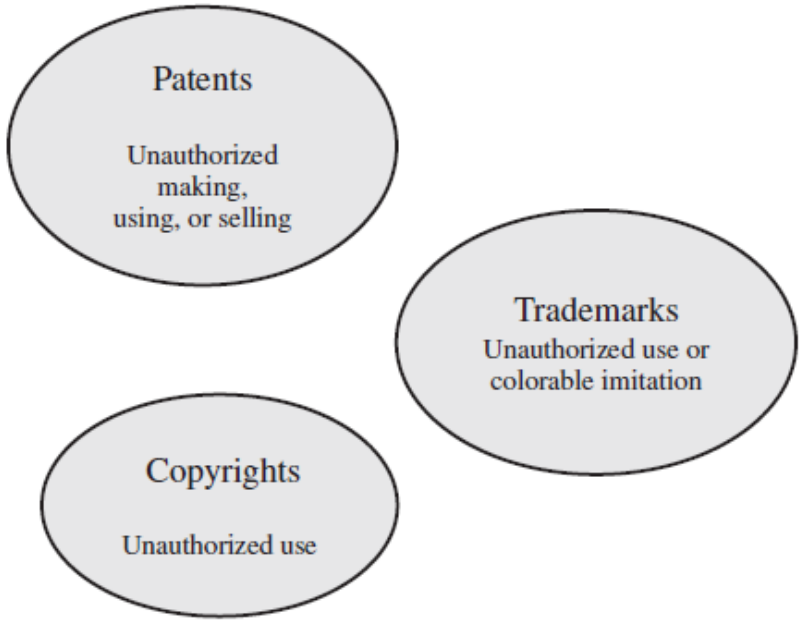


Figure 19.1 **Intellectual Property Infringement**

Intellectual Property

Patent Law

- A patent for an invention is the grant of a property right to the inventor
- The right to “exclude others from making, using, offering for sale or selling”
- There are three types of patents:
  - Utility patents
    - Useful process, machine, article of manufacture
  - Design patents
    - New design for an article of manufacture
  - Plant patents
    - discovery or invention of new and distinct reproduceable plants e.g., hybrid seeding, mutants and cultivations

Intellectual Property

Trademark Law

- A word, name, symbol or device that is used in trade with goods to indicate the source of the goods and distinguish them from the goods of others

Intellectual Property

Copyright Law

- Protects the tangible or fixed expression of an idea
- The creator has put this idea into a concrete form, such as a hard copy, software or multimedia form
- Examples of items which may be copyrighted:
  - Literary works
  - Musical works
  - Dramatic works
  - Motion pictures
  - Sound recordings
  - Software-related works
    - *i.e. Software, documentation, training manuals…*

Intellectual Property

Intellectual Property in the Context of Computing

- Software
  - Operating systems, utility programs and applications
- Databases
  - Data that is collected and organized in such a fashion that it represents commercial value
- Digital Content
  - Audio, video, multimedia, courseware, website content and original digital work that can be presented in some fashion using computers and digital devices
- Algorithms
  - E.g., RSA public-key cryptosystem

Intellectual Property

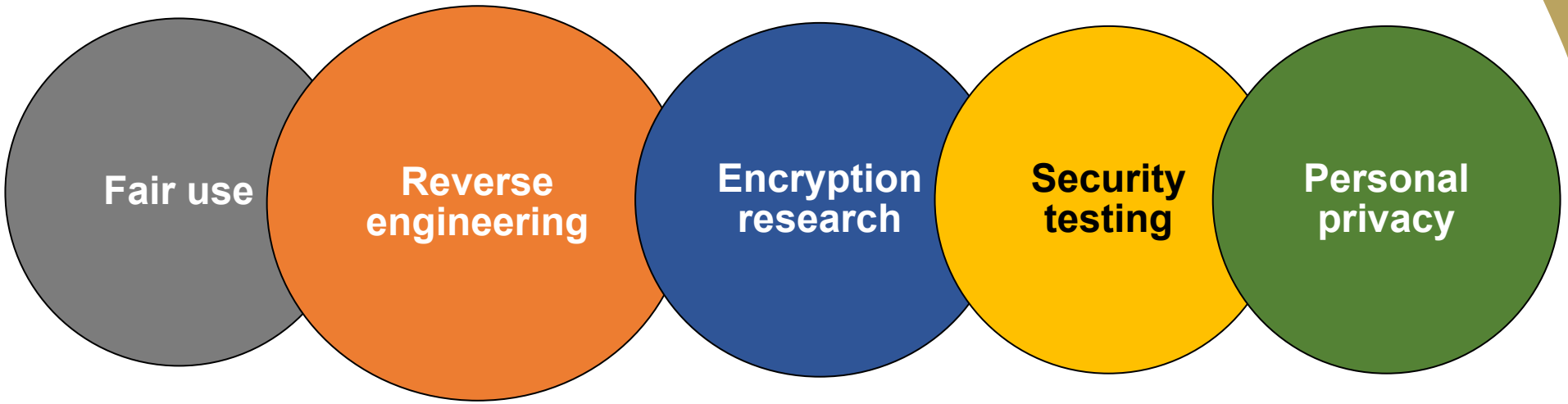
Digital Millennium Copyright Act (1998)

- Signed into law in 1998
- Implements WIPO (World Intellectual Property Organization) treaties to strengthen protections of digital copyrighted materials
- Encourages copyright owners to use technological measures to protect their copyrighted works
  - Measures that prevent access to the work
  - Measures that prevent copying of the work
- Prohibits attempts to bypass the measures
  - Both criminal and civil penalties apply to attempts to circumvent

Intellectual Property

Digital Millennium Copyright Act (1998)

- Certain actions are exempted from the provisions of the DMCA and other copyright laws including:



- Considerable concern exists that DMCA inhibits legitimate security and encryption research
  - Feel that innovation and academic freedom is stifled and open source software development is threatened

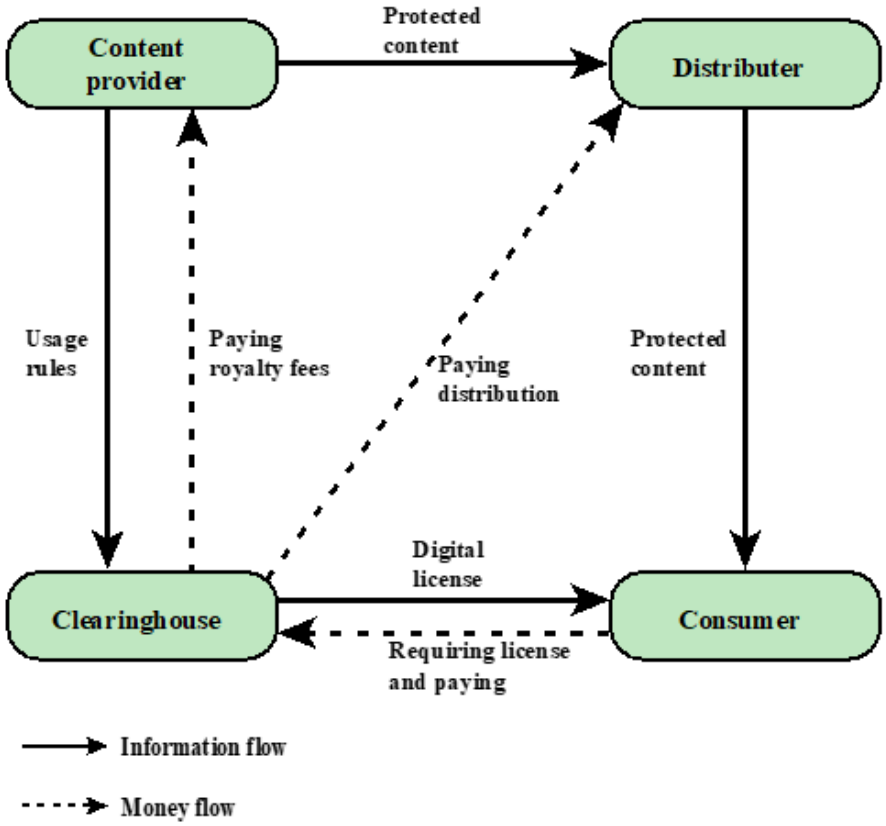
Intellectual Property

Digital Rights Management

- Systems and procedures that ensure that holders of digital rights are clearly identified and receive stipulated payment for their works
  - May impose further restrictions such as inhibiting printing or prohibiting further distribution
- No single DRM standard or architecture
- Objective is to provide mechanisms for the complete content management life cycle
- Provide persistent content protection for a variety of digital content types/platforms/media

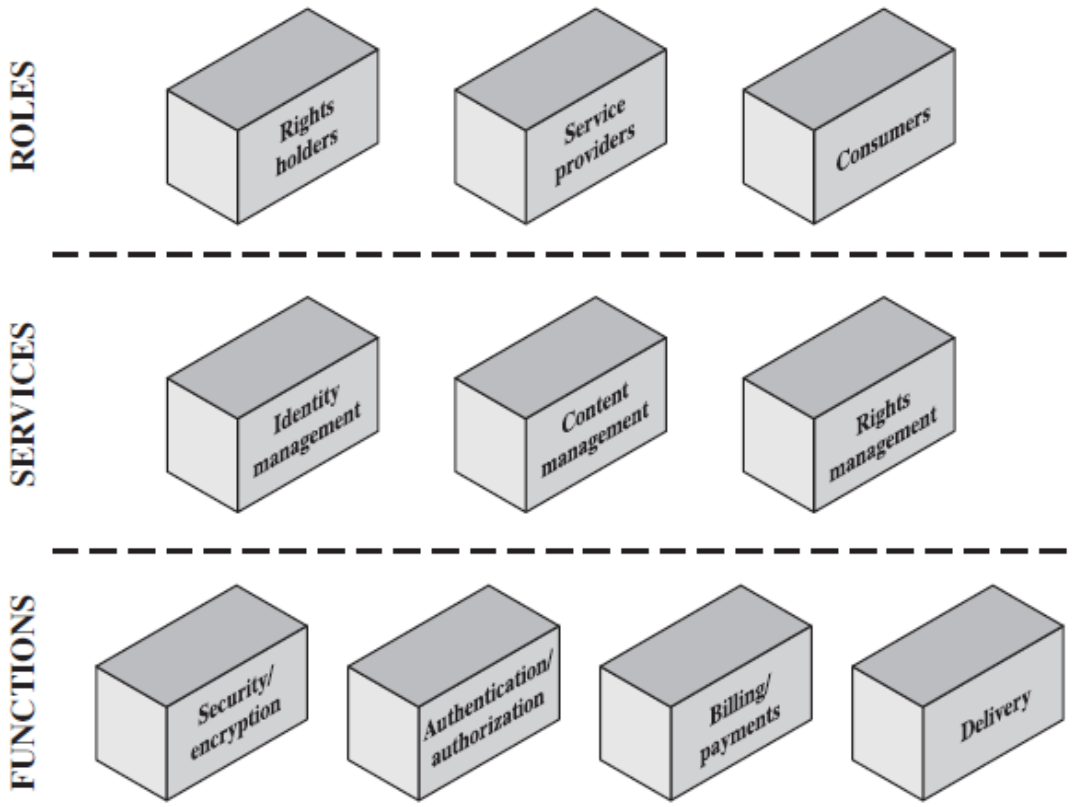
Intellectual Property

Digital Rights Management



Intellectual Property

Digital Rights Management



Privacy

Overview

- Overlaps with computer security
- Dramatic increase in scale of information collected and stored
  - Motivated by law enforcement, national security, economic incentives
- Individuals have become increasingly aware of access and use of personal information and private details about their lives
- Concerns about extent of privacy compromise have led to a variety of legal and technical approaches to reinforcing privacy rights

General Data Protection Regulation

GDPR and Privacy

- Single set of rules for all EU nations
- Supersedes the Data Protection Act 1998

- Protect personal data & strengthen privacy rights of EU individuals
- Give users control over their data

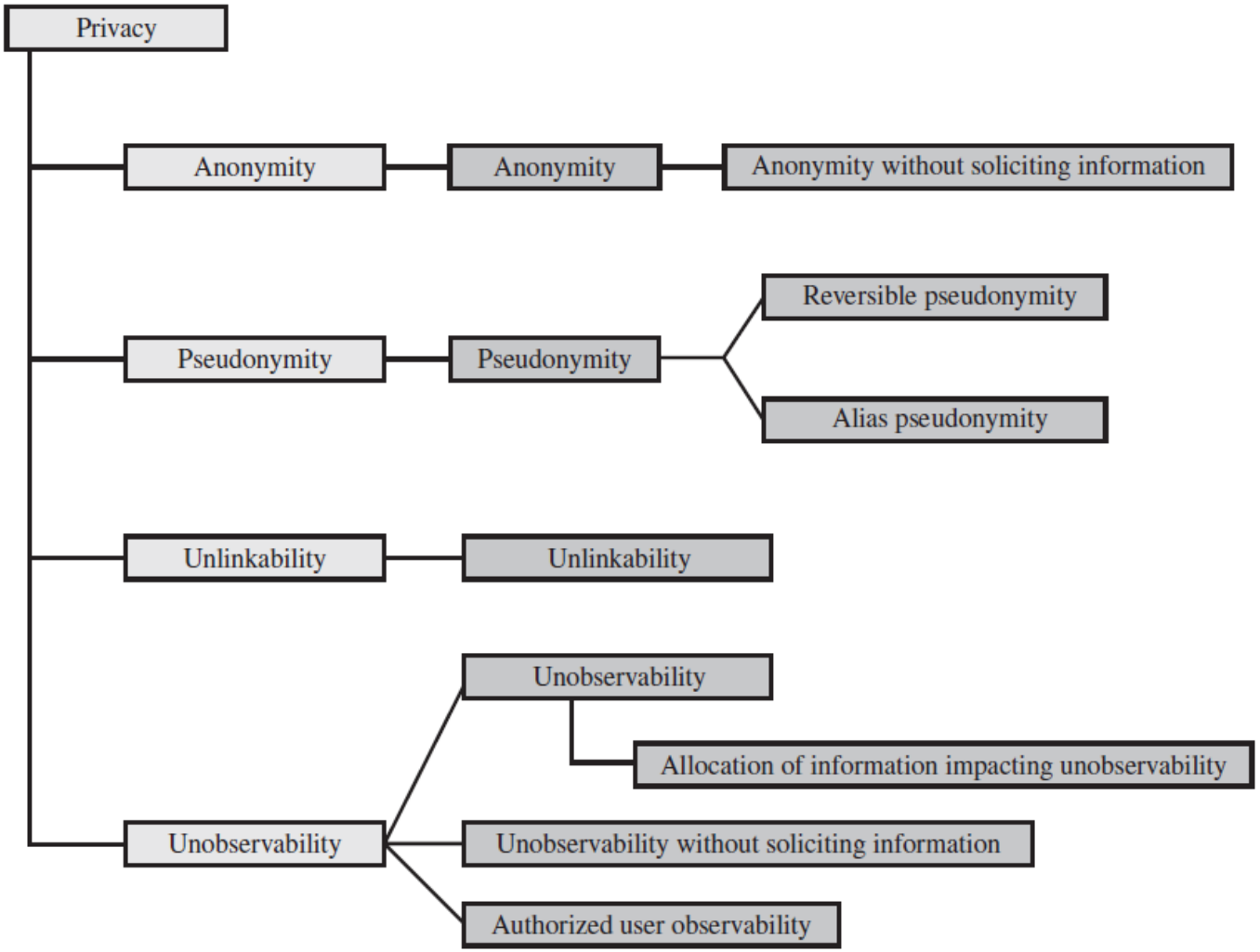
Privacy

ISO 27002 Satement (For Reference)

"An organization's data policy for privacy and protection of **personally identifiable information** should be developed and implemented. This policy should be **communicated to all persons involved in the processing of personally identifiable information**. Compliance with this policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of personally identifiable information requires appropriate management structure and control. Often this is best achieved by the **appointment of a person responsible**, such as a privacy officer, who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personally identifiable information and ensuring awareness of the privacy principles should be dealt with in accordance with relevant legislation and regulations. **Appropriate technical and organizational measures to protect personally identifiable information should be implemented."**

Privacy

Common Criteria Specification (CCPS12b)



Privacy

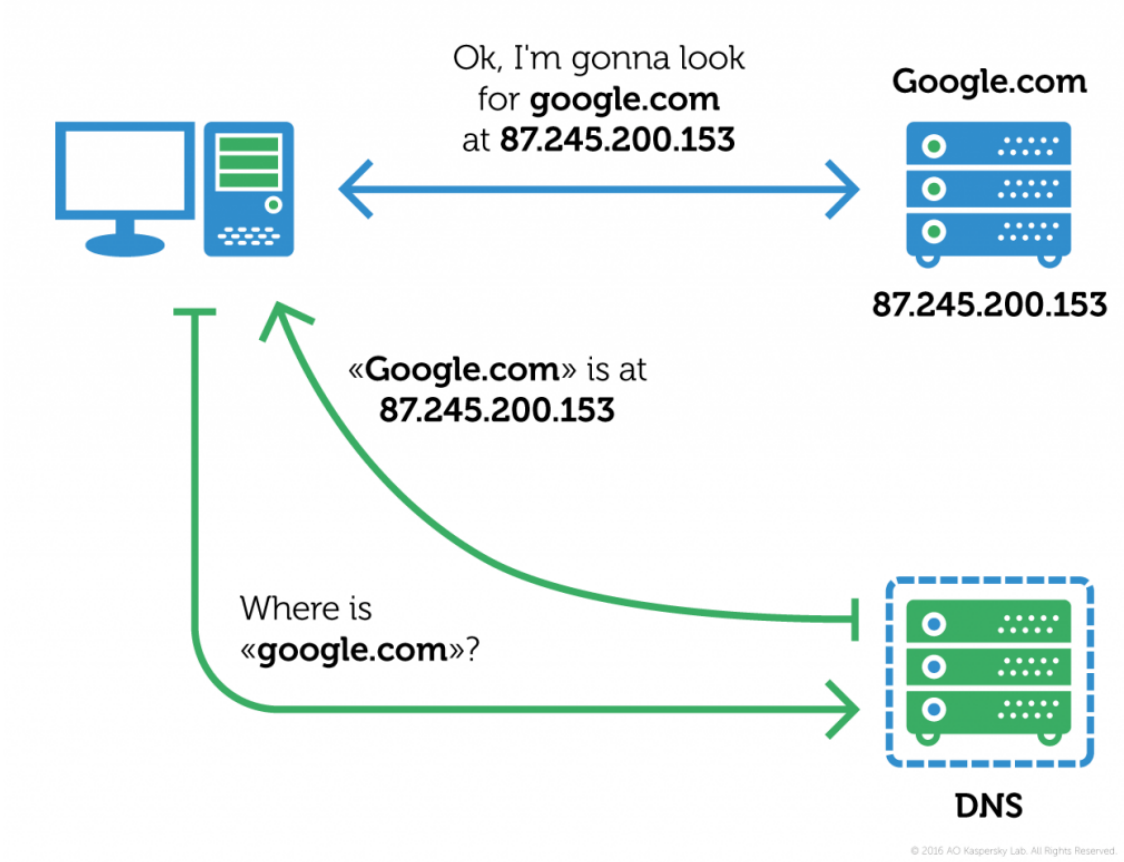
ISP Privacy Concerns

https://www.youtube.com/watch?v=RMpK8Nws5CI&t=6s&ab_channel=Eazl

Privacy

DNS over HTTPS (DoH)

- Traditional DNS is as follows:



Privacy

DNS over HTTPS

- DoH is presented as a potential panacea to privacy issues with ISPs
- DNS requests are typically plaintext
- DoH encrypts the DNS queries and sends them as HTTPS requests
- The encrypted DoH requests are then sent to special DoH resolvers, rather than DNS resolvers
- This is therefore advertised as a way to keep DNS activity private from ISPs

Privacy

DNS over HTTPS - Problems

On closer inspection, DoH causes a number of problems:

1. It doesn't actually prevent ISP tracking
   - Several other parts of HTTPS traffic will still reveal activity in an unencrypted manner

2. Creates difficulty in enterprise networks
   - Traditional blacklists are DNS based
   - Employers may find it difficult to monitor traffic

3. Potentially creates scope for criminal activity

4. DNS traffic is then centralized at a few DoH resolvers.

Ethics

Definition & Context

- Many potential misuses and abuses of information and electronic communication that create privacy and security problems
- Basic ethical principles developed by civilizations apply
  - Unique considerations surrounding computers and information systems
  - Scale of activities not possible before
  - Creation of new types of entities for which no agreed ethical rules have previously been formed

Ethical Issues Related to Computers and Information Systems

- Some ethical issues from computer use:
  - Repositories and processors of information
    - e.g., Data Privacy: Ethical concerns arise when entities that store or process information fail to protect the privacy of individuals. Unauthorized access or data breaches can lead to the misuse of personal information, such as identity theft, financial fraud.
  - Producers of new forms and types of assets
    - e.g., Intellectual Property Rights: Ethical dilemmas may arise when creators or producers of new forms of assets, such as software, digital content, or other digital products, violate intellectual property rights. Such as Copyright infringement, plagiarism or unauthorized use of patented technologies,

Ethical Issues Related to Computers and Information Systems

- Instruments of acts
  - **E.g.,** Cybercrime and Hacking: Computers can be misused as instruments for criminal activities such as hacking, cyber-attacks, or the spread of malicious software.
- Symbols of intimidation and deception
  - E.g., Cyberbullying**:** Computers and digital communication platforms can be used as tools for cyberbullying, which can have severe psychological and emotional impacts on individuals, especially children and teenagers. This raises ethical concerns regarding the use of technology for harassment, intimidation, or manipulation.
- Those who understand, exploit technology, and have access permission, have power over these assets.

Ethics

Professional/Ethical Responsibilities

- Concern with balancing professional responsibilities with ethical or moral responsibilities
- Types of ethical areas a computing or IT professional may face:
  - Ethical duty as a professional may come into conflict with loyalty to employer
  - “Blowing the whistle”
  - Expose a situation that can harm the public or a company’s customers
  - Potential conflict of interest
- Organizations have a duty to provide alternative, less extreme opportunities for the employee
  - In-house ombudsperson coupled with a commitment not to penalize employees for exposing problems
- Professional societies should provide a mechanism whereby society members can get advice on how to proceed

Ethics

Professional/Ethical Responsibilities

- Ethics are not precise laws or sets of facts
- Many areas may present ethical ambiguity
- Many professional societies have adopted ethical codes of conduct which can:

1. Be a positive stimulus and instill confidence
   - As a positive stimulus for ethical conduct on the part of the professional, and to instill confidence in the customer or user of using product or service
2. Be educational
   - To educate managers on their responsibility to encourage and support employee ethical behavior and on their own ethical responsibilities.
3. Provide a measure of support
   - provides a measure of support for a professional whose decision to act ethically in a situation may create conflict with an employer or customer.
4. Be a means of deterrence and discipline
   - A professional society can use a code as a justification for revoking membership or even a professional license. An employee can use a code as a basis for a disciplinary action.
5. Enhance the profession's public image
   - A code can enhance the profession’s public image, if it is seen to be widely honored.

Ulster University

Thanks!