

Overview

- Command Injection
- Validating Input
- Input Fuzzing
- Cybercrime

FLITTERIN = FACEBOOK + TWITTER + LINKEDIN



HubSpot

CHECK THIS OUT. WITH **FLITTERIN** I CAN CONNECT TO MY FUTURE BOSS, MY PAST FLAMES AND MY CURRENT OBSESSION ALL IN ONE PLACE!

Source: <http://mashable.com>

perl finger CGI script

- CGI:
- Finger:
- This CGI script **retrieves the desired info** from the server, based on what is passed to it as the value of **user** as a parameter
- From where is the value of user passed?

```
1  #!/usr/bin/perl
2  # finger.cgi - finger CGI script using Perl5 CGI module
3
4  use CGI;
5  use CGI::Carp qw(fatalsToBrowser);
6  $q = new CGI;          # create query object
7
8  # display HTML header
9  print $q->header,
10         $q->start_html('Finger User'),
11         $q->h1('Finger User');
12  print "<pre>";
13
14  # get name of user and display their finger details
15  $user = $q->param("user");
16  print ` /usr/bin/finger -sh $user `;
17
18  # display HTML footer
19  print "</pre>";
20  print $q->end_html;
```

Finger Form (for example)

```
<HTML>
<HEAD><TITLE>Finger User</TITLE></HEAD>
<BODY>
<H1> Finger User</H>
<FORM METHOD = POST action = "finger.cgi">
<B>Username to finger</b>: <input type = text name = user value = "">
<p><input type = submit value = Finger User">
</FORM>
</BODY>
</HTML>
```

- Invokes cgi script
- Takes user as input
- User is passed as parameter to finger.cgi

Command Injection

- If the user is legit – then it's all good ...
- But instead if a **command** is the input – this will be passed to finger.cgi ...
 - e.g. list all the users in this directory (finger.cgi thinks the command is coming from a Web server)
- metacharacters often used in commands

```
14 # get name of user and display their finger details
15 $user = $q->param("user");
16 die "The specified user contains illegal characters!"
17     unless ($user =~ /^\w+$/);
18 print `/usr/bin/finger -sh $user`;
```

a solution: to add a test that ensures that the user input contains only expected tokens (e.g. alphanumeric and not metacharacters)

Recall (SQL Injection)

- Data may be altered to conform to what is expected – by ‘escaping’ metacharacters – and thus rendering the input safe (making the input usable)

```
$name = $_REQUEST['name'];  
$query = "SELECT * FROM suppliers WHERE name = '" . $name . "'";  
$result = mysql_query($query);
```

```
$name = $_REQUEST['name'];  
$query = "SELECT * FROM suppliers WHERE name = '" .  
    mysql_real_escape_string($name) . "'";  
$result = mysql_query($query);
```

Validating Input

- Given that the programmer cannot control the content of input data, it is necessary to ensure that such data conform with any assumption made about the data
 - e.g. for textual, data contain only alphanumeric data or
 - for numeric, only int and double

- 2 possible principles can be followed:
 - compare input data with known dangerous values
 - accept only known safe data

Which is better and why?

Input Fuzzing

- good alternative is called **fuzzing**
- developed by Dr. Barton Miller (U of Wisconsin, Madison) in 1989
- software testing technique that uses randomly generated data as inputs to a program
- range of inputs may be very large (textual, graphic, random network requests , random parameter values passed to system functions etc.)
- the intent is to determine where the program/ function
 - correctly handles all such abnormal inputs
 - crashes
 - fails to respond appropriately
 - identifies reliability (or lack of) and security deficiencies
- Fuzzing – simple, (but effective) and low costs (to generate these inputs)
- Limitations?

Computer Crime vs. Cybersecurity

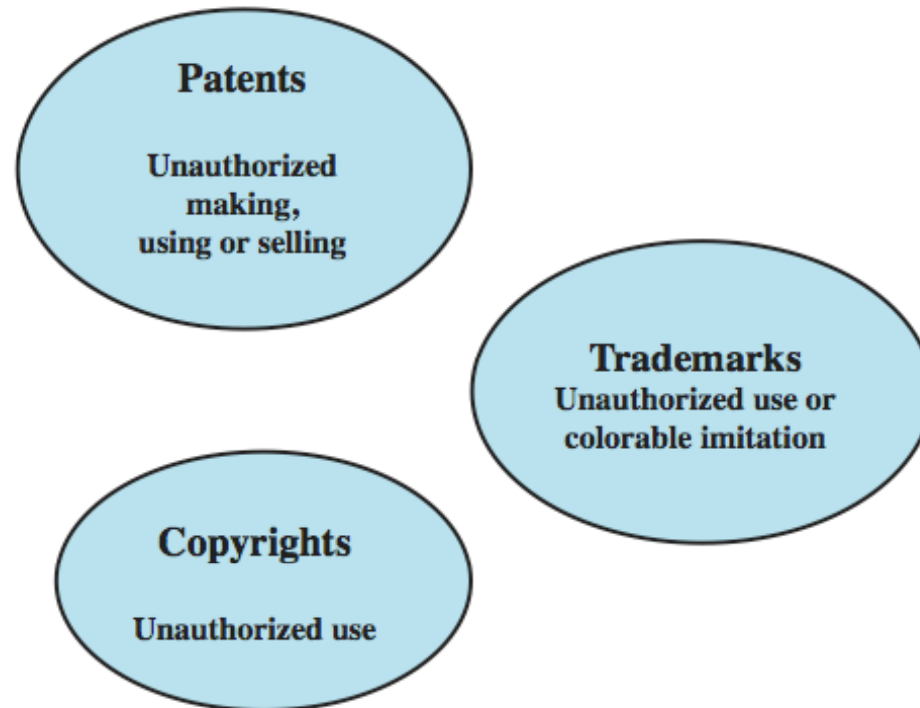
- The term *cybercrime* has a connotation of the use of networks specifically, whereas *computer crime* may or may not involve networks.
- The U.S. Department of Justice categorizes computer crime based on the role that the computer plays in the criminal activity, as follows:
 - **Computers as targets:** to acquire information stored on that computer system without authorization or payment (theft of service)
 - **Computers as storage devices:** as a passive storage medium, e.g. for stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or "warez" (pirated commercial software).
 - **Computers as communications tools:** often traditional crimes committed online, e.g. the illegal sale of prescription drugs, controlled substances, alcohol, etc..

Examples of Cybercrime

- theft of intellectual property
- theft of other (proprietary) info including customer records, financial records
- DOS attacks
- virus, worms, and other malware attacks
- fraud (over the Net)
- illegal generation of spam email
- webpage defacement
- intentional exposure of private or sensitive info
- spyware (but not including adware)
- others

Intellectual Property

- **Intellectual property** is any **intangible asset** that consists of **human knowledge and ideas**



- The legal protection is against **infringement**, which is the invasion of the rights secured by copyrights, trademarks, and patents.
- The right to seek civil recourse against anyone infringing his or her property is granted to the IP owner.

Intellectual Property

- Relevant to Computer and Network Security (misuse of)
 - software
 - all programs produced by vendors
 - databases
 - all data and db protected by copyright
 - digital content
 - audio, video files, multimedia, courseware, website content and other original content
 - Algorithms
 - improvement of software or function

Privacy

- considerable overlap with computer security
- in a global information economy, the **most economically valuable electronic asset is likely the aggregations of information on individuals**
- individuals are becoming increasingly aware (or maybe not) of the extent to which government agencies, businesses, and even Internet users have access to their personal information and private details about their lives and activities
- concerns about the extent to which personal privacy has been and may be compromised have led to a variety of legal and technical approaches to reinforcing privacy rights
 - **COPPA, HIPPA, Sarbanes-Oxley**
- **FB: Zuckerman email for Nov 2009**

EU Privacy Law

- European Union Data Protection Directive was adopted in 1998, to both (1) ensure that member states protected fundamental privacy rights when processing personal information, and (2) prevent member states from restricting the free flow of personal information within the EU. The Directive is organized around the following principles of personal information use:
 - **Notice:** organizations must notify individuals what personal information they are collecting, the uses of that information, and what choices the individual may have.
 - **Consent:** individuals must be able to choose whether and how their personal information is used by, or disclosed to, third parties. They have the right not to have any sensitive information collected or used without express permission, including race, religion, health, union membership, beliefs, and sex life.
 - **Consistency:** organizations may use personal information only in accordance with the terms of the notice given the data subject and the choices the make on its use.
 - **Access:** individuals must have the right and ability to access their information and correct, modify, or delete any portion of it.
 - **Security:** organizations must provide adequate security, using technical and other means, to protect the integrity and confidentiality of personal information.
 - **Onward transfer:** third parties receiving personal information must provide the same level of privacy protection as the organization from whom the information is obtained.
 - **Enforcement:** grants a private right of action to data subjects when organizations do not follow the law.

US Privacy Law

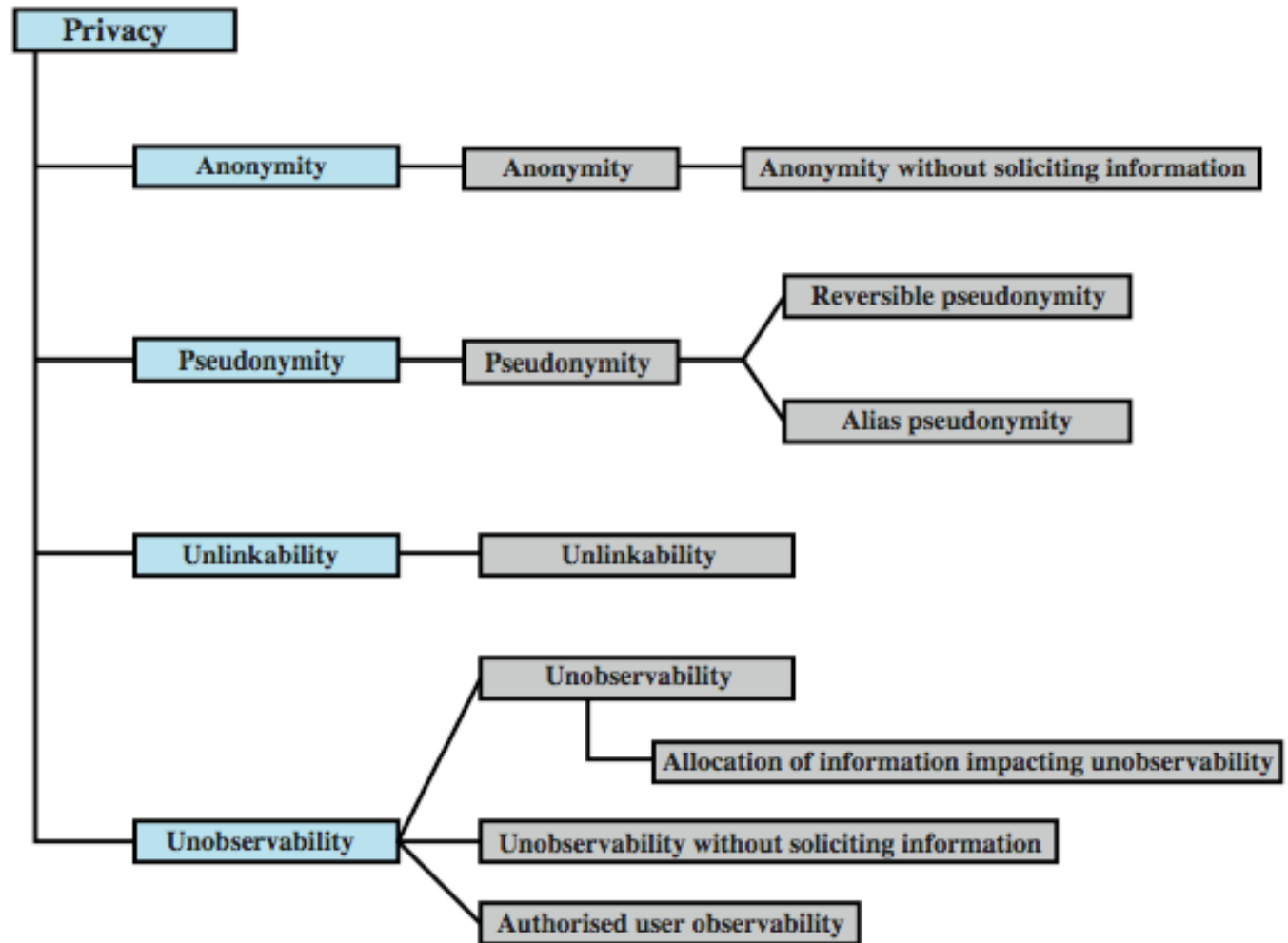
- The first comprehensive privacy legislation adopted in the United States was the Privacy Act of 1974, which dealt with personal information collected and used by federal agencies. The act is intended to:
 - 1. Permit individuals to determine what records pertaining to them are collected, maintained, used, or disseminated
 - 2. Permit individuals to forbid records obtained for one purpose to be used for another purpose without consent
 - 3. Permit individuals to obtain access to records pertaining to them and to correct and amend such records as appropriate.
 - 4. Ensure that agencies collect, maintain, and use personal information in a manner that ensures that the information is current, adequate, relevant, and not excessive for its intended use.
- As with all privacy laws and regulations, there are exceptions and conditions attached to this act, such as criminal investigations, national security concerns, etc.
- While the 1974 Privacy Act covers government records, a number of other U.S. laws have been enacted that cover other areas, including: Banking and financial records, Credit , Medical and health insurance records, Children's privacy, Electronic communications.

Common Criteria Privacy Class

The purpose of the privacy functions is to provide a user protection against discovery and misuse of identity by other users.

It is primarily concerned with the privacy of an individual with respect to **their use of computer resources**, rather than the privacy of their personal information.

This specification is a useful guide to how to design privacy support functions as part of a computer system.



The 4 Major Areas of Privacy (advantages and disadvantages)

- **Anonymity:** Ensures that a user may use a resource or service without disclosing the user's identity
 - Anonymity need not conflict with authorization and access control functions, which are bound to computer-based user IDs, not to personal user information e.g. web email address
- **Pseudonymity:** ensures that a user may use a resource or service without disclosing its user identity, **but can still be accountable for that use**. The system shall provide an alias to prevent other users from determining a user's identity but the system shall be able to determine the user's identity from an assigned alias e.g. company email address nh@MU.edu
- **Unlinkability:** ensures that a user may make multiple uses of resources or services without others being able to link these uses together
- **Unobservability:** ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.