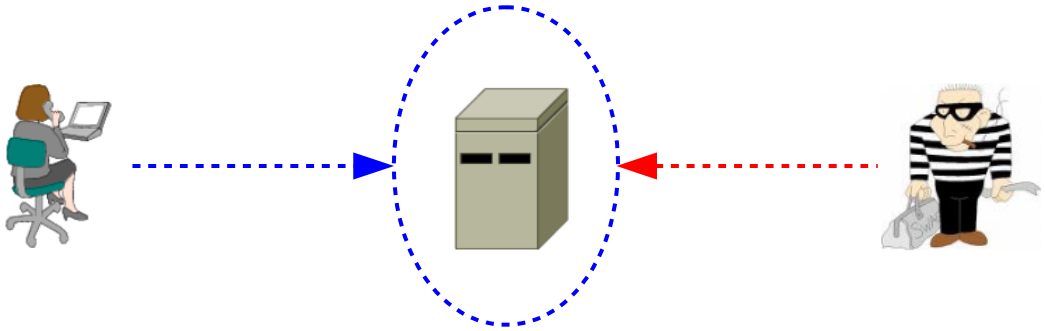
System:
Threats, Vulnerabilities and Risks

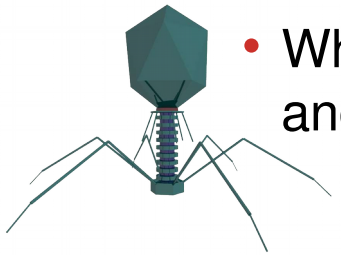


CISSP®
Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Application Issues – Traditional Environment

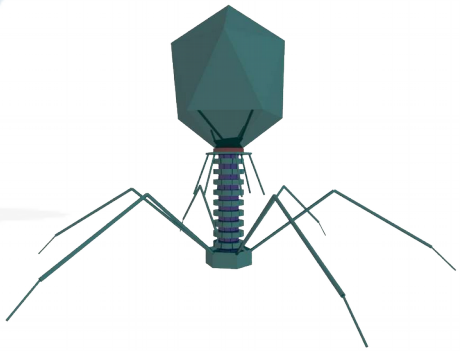
- **Viruses**
  - **MBR/GPT**
    - MBR/GPT viruses make it impossible to start the computer from the hard disk.
  - **File Infector Viruses**
    - Virus copies the file and places into an area where it can be executed. i.e. RAM
    - The malicious code runs first while the infected file remains quiescent.
    - The virus copies itself away from infection area, allowing it to continuously infect files as the user functions other programs.
    - When established, the virus grants control back to the infected file.
    - When a user opens another application, the dormant virus runs and copies itself into files that were previously uninfected, a cycle.



Application Issues – Traditional Environment

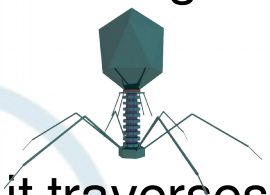
- **Macro Viruses**
  - Virus that is written in a macro language within a software application such as a word processor.

- Anti-virus software and other preventive measures
  - Detect and eliminate known viruses.
    - A list of virus signature definitions or "*signatures*".
    - A heuristic algorithm to find viruses based on common behaviours.
- Importance of regular backups.



Application Issues – Traditional Environment

- **Multipartite Virus**
  - Virus that uses more than one technique to spread itself.
- **Stealth Virus**
  - Virus that write itself into the OS itself to avoid being detected by anti-virus software.
- **Polymorphic Virus**
  - This is a virus that modifies its own code as it traverses systems. This camouflages signatures.
- **Encrypted Virus**
  - Viruses use cryptographic techniques in order to hide their signature from anti-virus software.
- **Hoax**
  - Spam e-mail that warns of a virus that is spread by friend to friend and warns of a virus, real or imaginary that is very destructive.

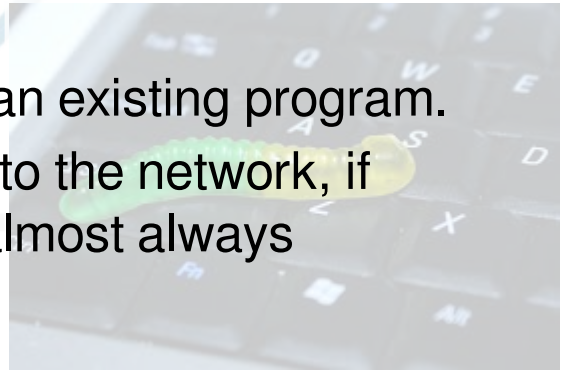


Application Issues – Traditional Environment

- **Trojan Horse**
  - Malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorised access to the user's computer system. Trojan horses facilitate the use of the computer:
    - As part of a Botnet (e.g., to perform DDoS attacks).
    - Data Theft (e.g., passwords, security codes, credit card, ..)
    - Installation of software (including other malware).
    - Downloading of files.
    - Uploading of files.
    - Deletion of files.
    - Modification of files.
    - Keystroke logging.
    - Viewing the user's screen.
    - Wasting computer storage space.

Application Issues – Traditional Environment

- **Logic Bomb**
  - This is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.
    - i.e. A programmer may hide a piece of code that starts deleting files, should they ever be terminated from the company.
  - To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software.
- **Worms**
  - A self-replicating computer program that uses a network to send copies of itself to other nodes and it may do so without any user intervention.
  - Unlike a virus, it does not need to attach itself to an existing program.
  - Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or devour files on a targeted computer.



Application Issues – Traditional Environment

- **Spyware**
  - Spyware is a type of malware that is installed on computers and collects info about users without their knowledge.
  - The presence of spyware is typically hidden from the user and is secretly installed on the computer.
- **Adware**
  - Adware or advertising supported software is any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used.
  - Some types of adware are also spyware and can be classified as privacy invasive software.

Application Issues – Traditional Environment

- **Password Attacks**
  - Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system.
- **Dictionary Attacks**
  - The distinction between guessing, dictionary and brute force attacks is not strict. They are similar in that an attacker goes through a list of candidate passwords one by one, the list may be explicitly enumerated or implicitly defined, can incorporate knowledge about the victim, and can be linguistically derived.
- **Social Engineering**
  - Social engineering is the act of manipulating people into performing actions or divulging confidential information.

Denial of Service (DoS)

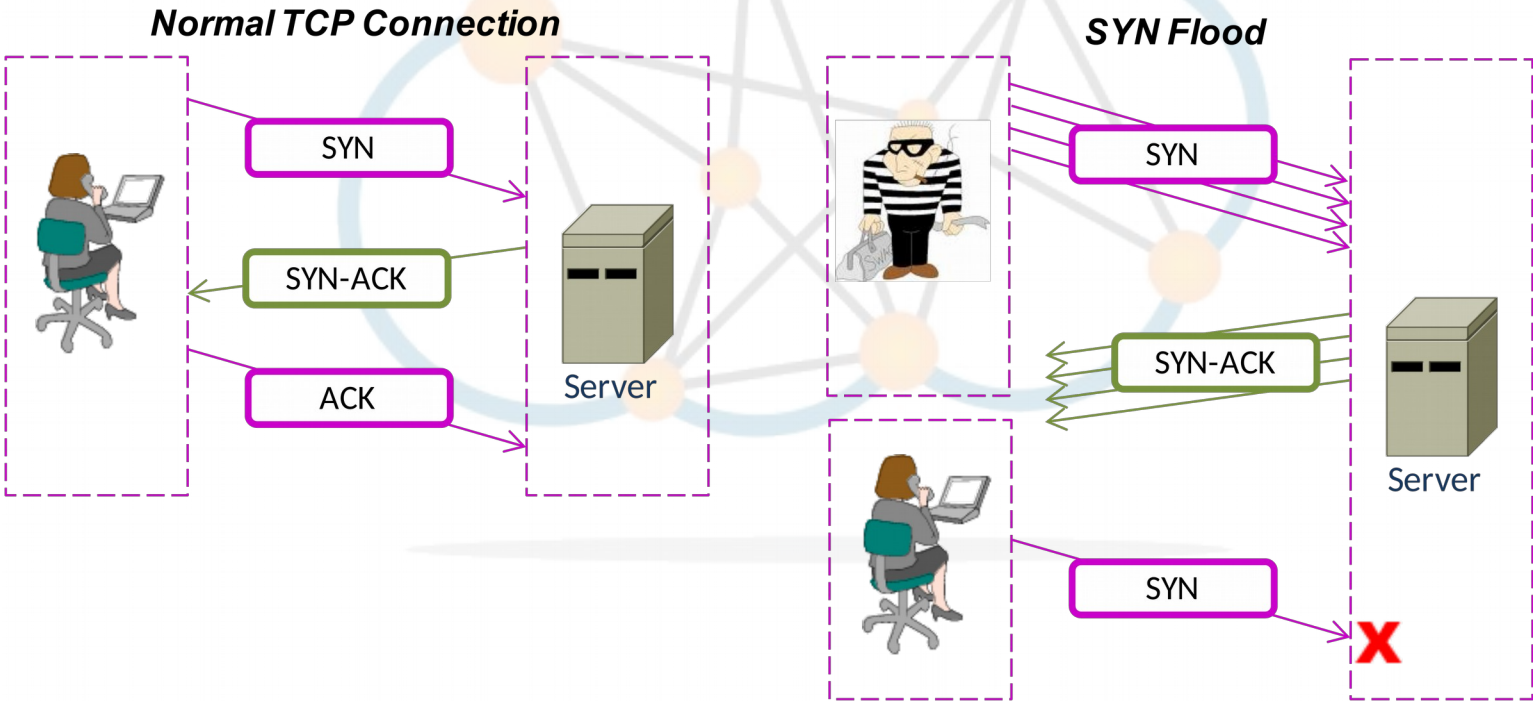
CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Application Issues – Traditional Environment

- **Denial of Service (DoS) Attacks**
  - A DoS attack is an attempt to make a computer resource unavailable to its intended users.
- **SYN Flood Attack**



DoS example - hping

```
Linux:~# sudo apt-get install hping3

Linux:~# sudo hping3 --count 10000 --data 120 --syn --win
64  --destport 21 --flood -rand-source www.attacktarget.com
HPING www.attacktarget.com (lo 127.0.0.1): S set, 40
headers + 120 data bytes
hping in flood mode, no replies will be shown
--- www.hping3testsite.com hping statistic ---
1189112 packets transmitted, 0 packets received, 100%
packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

DoS example - nping

```
Linux:~# sudo apt-get install nmap

Linux:~# nping --tcp-connect --rate=90000
                --count 900000 -reduce-verbosity
                www.attacktarget.com

Starting Nping 0.6.40 ( http://nmap.org/nping ) at
2016-01-21 12:08 EAT
Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
TCP connection attempts: 900000 | Successful
connections: 0 | Failed: 900000 (100.00%)
Nping done: 1 IP address pinged in 260.25 seconds
```

Distributed Environment

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

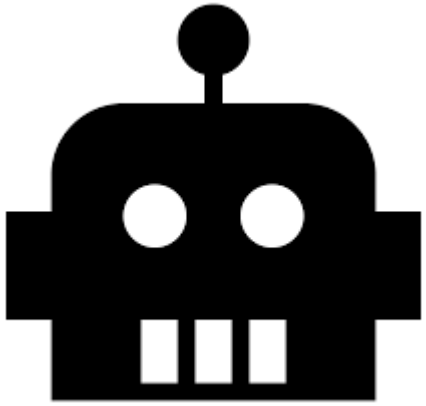
diarmuid@obriain.com

Distributed Computing Environment (DCE)

- Framework and toolkit developed in the early 1990s for developing client/server applications.
  - **Remote Procedure Call (RPC)** mechanism, a naming (directory) service, a time service, an authentication service and a **Distributed File System (DFS)**.
- The largest unit of management in DCE is a cell. Major components of DCE within every cell are:
  - The Security Server that is responsible for authentication. i.e. ***Kerberos***.
  - The Cell Directory Server (CDS) that is the repository of resources and ACLs. i.e. ***Lightweight Directory Access Protocol (LDAP)***.
  - The Distributed Time Server (DTS) that provides an accurate clock for proper functioning of the entire cell. i.e. ***Network Time Protocol (NTP)***.

Agents (bots)

- Software that acts for a user or other program in a relationship of agency.
- "*action on behalf of*" implies the authority to decide which (and if) action is appropriate.
  - i.e. the agents are not strictly invoked for a task, but activate themselves.
  - The largest use of bots is in web spidering.
    - *robots.txt,* containing rules for the spidering.



Malicious Bots (botnets)

- Malicious bots (and botnets) of the following types:
  - **Spambots** - harvest email addresses from internet forums, contact forms or guestbook pages.
  - **Downloader programs** - that suck bandwidth by downloading entire web sites.
  - **Website scrapers** - grab the content of web sites and re-use it without permission on automatically generated doorway pages.
  - Viruses and worms.
  - DDoS attacks.
  - Botnets / zombie computers; etc.
  - File-name modifiers on peer-to-peer file-sharing networks.
    - These change the names of files (often containing malware) to match user search queries.

Application Issues – Distributed Environment

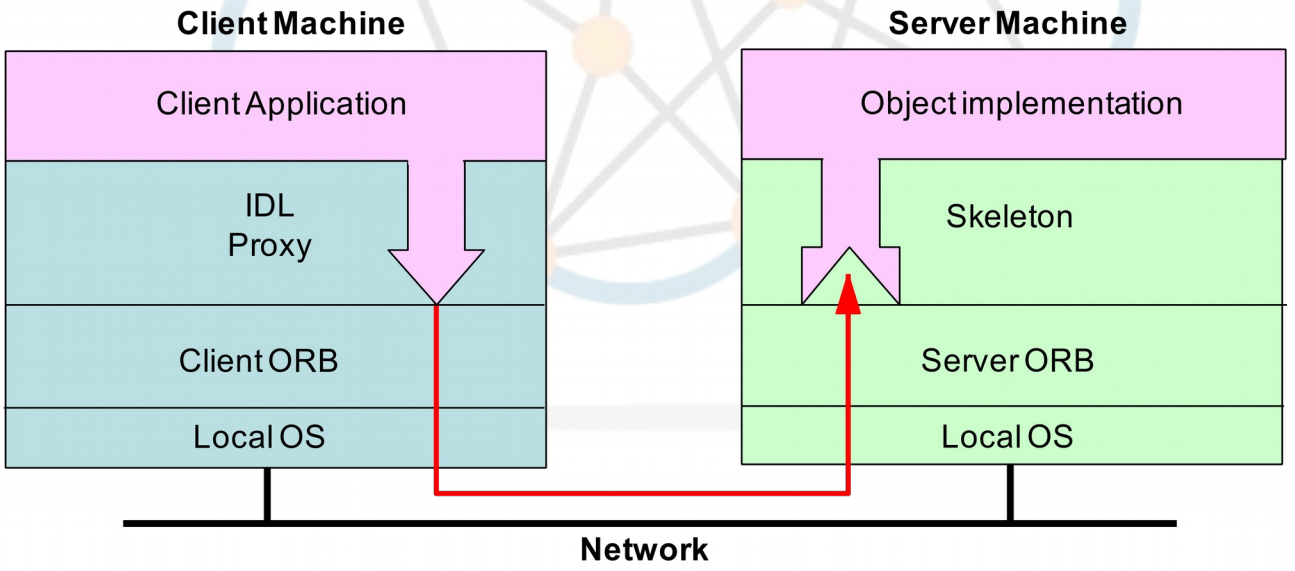
- **Applets**
  - Any small application that performs one specific task, sometimes running within the context a larger program perhaps as a plug-in.
  - The term typically also refers to programs written in the Java programming language which are included in an HTML page to provide interactive features to web apps that cannot be provided by HTML.
  - When a Java technology-enabled web browser views a page that contains an applet, the applet's code is transferred to the clients system and executed by the browser's Java Virtual Machine (JVM).
    - Sandbox.
- **ActiveX**
  - ActiveX is a Microsoft framework for defining reusable software components that perform a particular function or a set of functions. Microsoft Applets.
  - Malware, such as computer viruses and spyware, can be accidentally installed from malicious websites using ActiveX controls.

Application Issues – Distributed Environment

- **Object Request Broker (ORB)**
  - Middleware software that allows programs to make calls from one computer to another via a network.
  - ORBs promote interoperability of distributed object systems because they enable users to build systems by piecing together objects from different vendors that communicate with each other via the ORB.

Application Issues – Distributed Environment

- **Common Object Request Broker Architecture (CORBA)**
  - CORBA uses an Interface Description Language (IDL) to describe the data which is to be transmitted on remote calls.
  - The ORB takes the form of an object with methods enabling connection to the objects being served. After an object connects to the ORB, the methods of that object become accessible for remote invocations.
  - The ORB requires some means of obtaining the network address of the object that has now become remote.



Application Issues – Distributed Environment

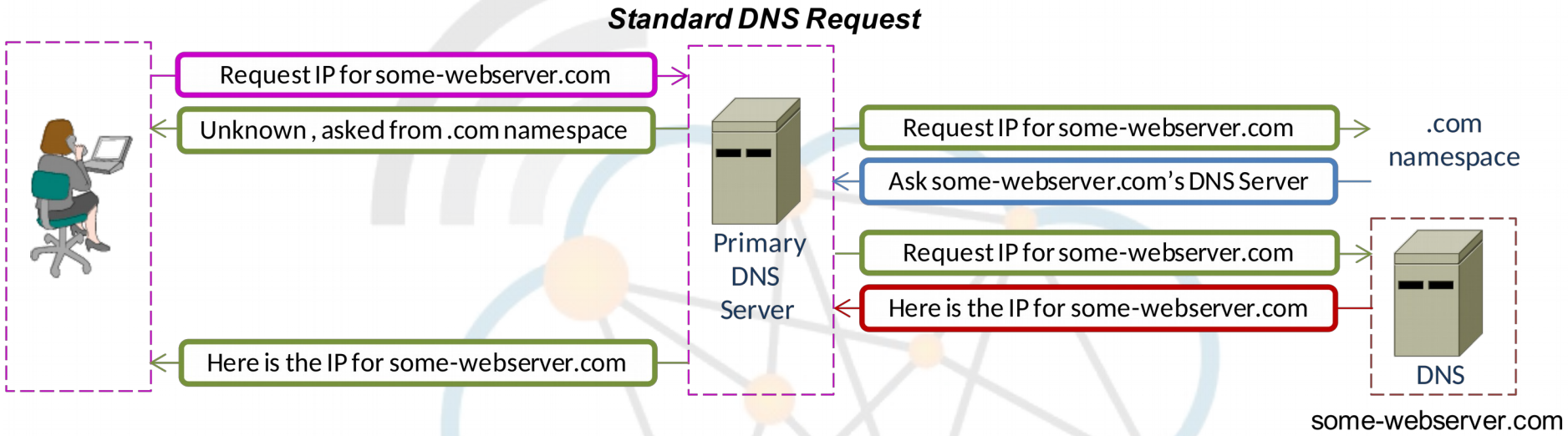
- **Distributed Common Object Model (DCOM)**
  - Proprietary Microsoft technology for communication among software components distributed across networked computers.
  - Originally was called 'Network Object Linking and Embedding (Network OLE) provides the communication substrate under Microsoft's COM+ application server infrastructure.
  - Deprecated in favour of the Microsoft .NET Framework.
- **.NET Framework**
  - Microsoft library of coded solutions to common programming problems and a Virtual Machine (VM) that manages the execution of programs written specifically for the framework.
  - The .NET Framework is intended to be used by most new applications created for the Windows platform.
  - It replaced DCOM.

Distributed DoS (DDoS) – Smurf attack

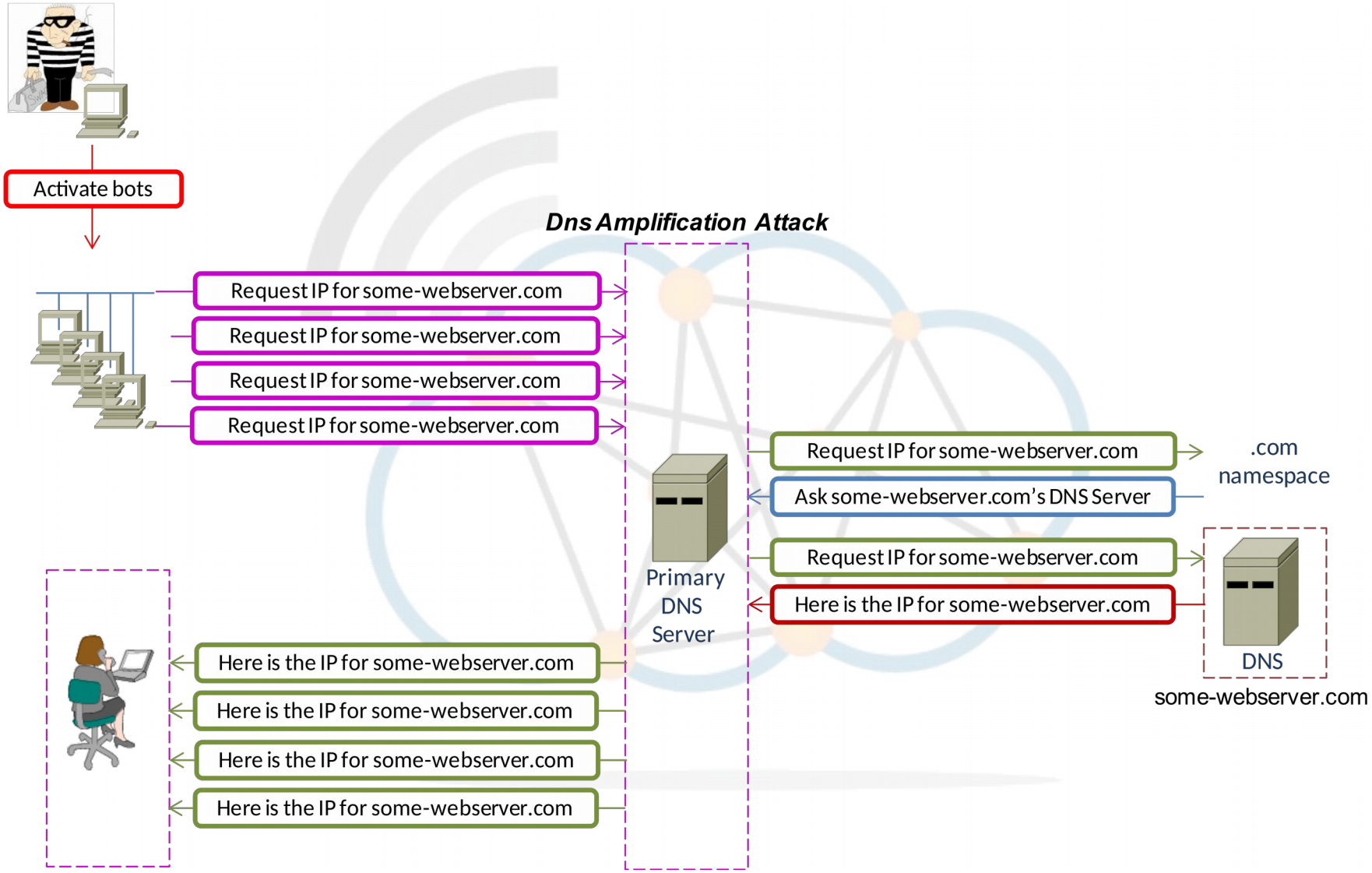
- Perpetrator sends a large volume of ICMP echo request (ping) traffic to IP broadcast addresses, all of which have a spoofed source IP address of the intended victim.
- Responding devices then flood the victim with echo reply packets.
- **Fix**:
  - Configure individual hosts and routers not to respond to ping requests or broadcasts.
  - Configure routers not to forward packets directed to broadcast addresses.
  - Until 1999, standards required routers to forward such packets by default, but in that year, the standard was changed such that the default is not forwarded.
  - Another proposed solution, to fix this as well as other problems, is network ingress filtering which rejects the attacking packets on the basis of the forged source address.
  - To prevent such attacks on a Cisco router add the command:

```
Router(config-if)# no ip directed-broadcast
```

Domain Name System (DNS)



DNS Amplification Attack



Teardrop Attack

- Application which sends Forged IP fragmented Packets that overlap each other and makes it difficult for the receiving host to reassemble them and usually causes a Kernel Panic in the target host.
- Teardrop exploits an overlapping IP fragment which causes the TCP/IP fragmentation re-assembly code to improperly handle overlapping IP fragments.
- In most cases a simple reboot can be best solution but restarting the OS might cause the loss of unsaved data in running applications.
- For machines that run Microsoft Windows:
  - When a Teardrop attack is run against a machine, it will crash or reboot (on Windows machines, a user might experience the Blue Screen of Death).

LAND Attack

- A DoS attack that consists of sending a special poison spoofed packet to a computer, causing it to lock up.
- The attack involves sending a spoofed TCP SYN packet (connection initiation) with the target host's IP address and an open port as both source and destination.
- The reason a LAND attack works is because it causes the machine to reply to itself continuously.
- Definition: "*A LAND attack involves IP packets where the source and destination address are set to address the same device*."
- Other LAND attacks have since been found in services like SNMP and Windows 88/tcp (kerberos/global services) which were caused by design flaws.

DNS Cache poisoning Attack

- Maliciously created or unintended situation that provides data to a caching name server that did not originate from authoritative DNS source.
- This can happen through improper software design, misconfiguration of name servers, and maliciously designed scenarios exploiting the traditionally open-architecture of the DNS system.
- Once a DNS server has received such non-authentic data and caches it for future performance increase, it is considered poisoned, supplying the non-authentic data to the clients of the server.
- A DNS server translates a domain name into an IP Address that Internet hosts use to contact Internet resources, in this case a flawed IP Address.

Ping of Death (POD) Attack

- Attack on a computer that involves sending a malformed or otherwise malicious ping to a computer.
  - A ping is normally 56 bytes in size.
- Sending a Ping which is larger than 65,535 bytes could crash the target computer by causing a buffer overflow, and the system may crash.
- This bug is mostly historical.
- In recent years, a different kind of ping attack has become wide-spread - ping flooding simply floods the victim with so much ping traffic that normal traffic fails to reach the system (a basic DoS attack).

Databases

and

CISSP®

Diarmuid Ó Briain

CEng, FIEI, FIET, CISSP

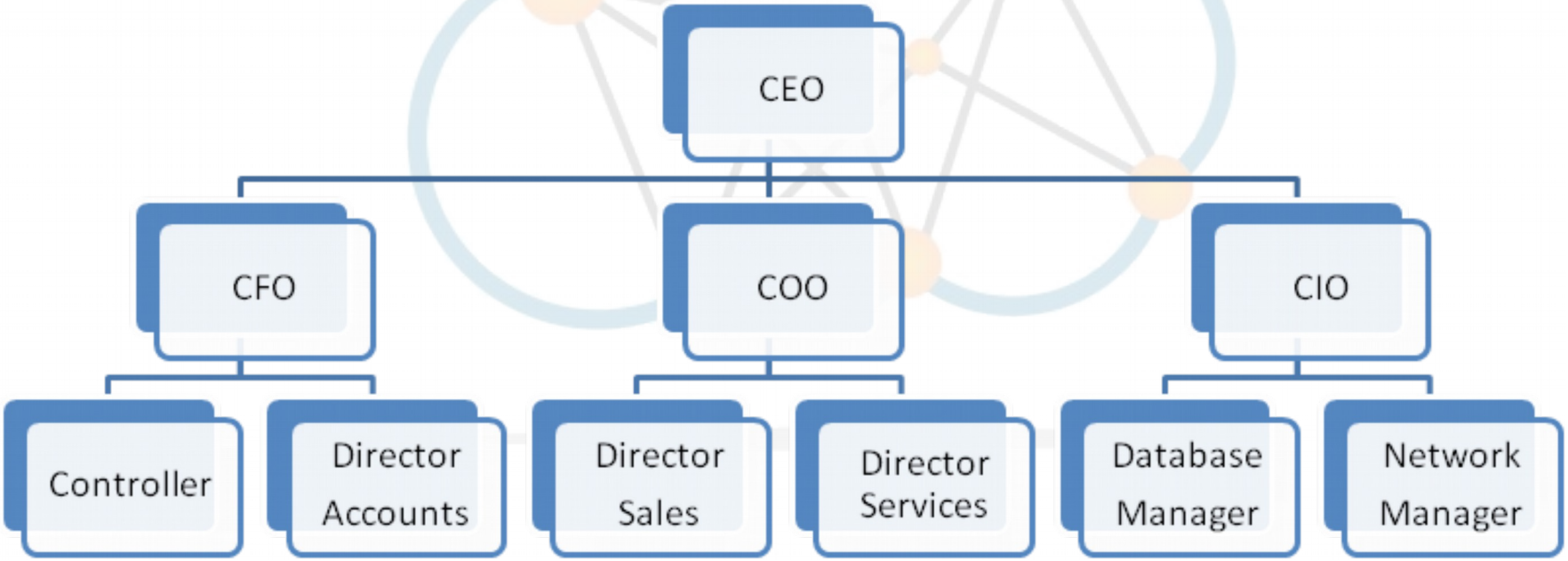
diarmuid@obriain.com

Database Management System (DBMS)

- A system software package that helps the use of integrated collection of data records and files known as databases.
- It allows different user application programs to easily access the same database.
- Instead of having to write computer programs to extract information, user can ask simple questions in a Structured Query Language (SQL).
- Many DBMS packages provide Fourth-generation programming language (4GLs) and other application development features.

Hierarchical Database

- In a hierarchical data model data is organised into a tree-like structure.
- The structure allows repeating information using parent/child relationships: each parent can have many children but each child only has one parent.



Distributed Database

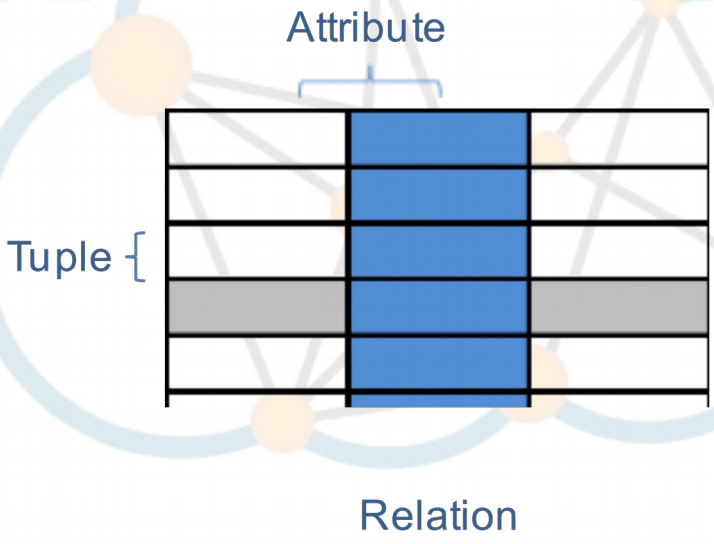
- Database that is under the control of a central DBMS in which storage devices are not all attached to a common CPU.
- Data may be dispersed across multiple computers located in the same physical location, or may be dispersed over a network of interconnected computers.
- To ensure that the distributive databases are up to date and current, there are two processes:
  - **Replication**
    - Software that identifies changes in the distributive database.
    - Distributes these changes across the distributed database.
  - **Duplication**
    - Identifies one database as a master and then duplicates that database.
    - Typically carried out at a set time after hours.
    - Changes to the master database only are allowed.
    - This is to ensure that local data will not be overwritten.

Relational Database

- Matches data using common characteristics found within the data set. The resulting groups of data are organised and are much easier for people to understand.
- Relational databases have become a predominant choice for the storage of information in new databases used for financial records, manufacturing and logistical information, personnel data and much more.
- Relational databases have often replaced legacy hierarchical databases and network databases because they are easier to understand and use, even though they are much less efficient.
- The increase in computer power masks inefficiencies of relational databases, which made them impractical in earlier times, have been outweighed by their ease of use.

Relational Database

- Relation – can be described as a table.
  - A set of tuples that have the same attributes.



Relational Database Keys

- **Candidate Keys**
  - A set of attributes where in all the relations assigned to that variable there are no two distinct tuples (rows) that have the same values for the attributes in this set.
- **Primary Keys**
  - Primary Key is a Candidate Key to uniquely identify each tuple in a table. It is selected by the DBA. A Primary Key comprises a single attribute or set of attributes. No two distinct tuples in a table can have the same value in those attributes. Depending on its design, a table may have arbitrarily many unique keys but at most one Primary Key.
- **Foreign Keys**
  - A foreign key is a reference to a key in another relation, meaning that the referencing tuple has, as one of its attributes, the values of a key in the referenced tuple.

Relational Database Keys

Table 1

FN	LN	AGE	CITY	SPORT
Conor	Ryan	14	**LK**	RUGBY
Cian	Ryan	18	**LK**	RUGBY
Brian	Tobin	13	**CK**	SOCCER
Aoife	Doherty	11	**DU**	SOCCER
Ian	Davies	12	**GW**	GAA
Sinéad	O'Meara	9	**GW**	GAA

Table 2

CITY	CITY_NAME
LK	Limerick
CK	Cork
DU	Dublin
GW	Galway

What city is Cian Ryan from ?

SQL Example

```
mysql> SELECT a.FN, a.LN, b.CITY_NAME
    -> FROM  Table1 a INNER JOIN Table2 b
    -> ON a.CITY = b.CITY
    -> WHERE a.AGE > 11;
+--------+--------+-----------+
| LN     | FN     | CITY_NAME |
+--------+--------+-----------+
| Ryan   | Conor  | Limerick  |
| Ryan   | Cian   | Limerick  |
| Tobin  | Brian  | Cork      |
| Davies | Ian    | Galway    |
+--------+--------+-----------+
4 rows in set (0.00 sec)
```

Conor	Ryan	Limerick
Cian	Ryan	Limerick
Brian	Tobin	Cork
Ian	Davies	Galway

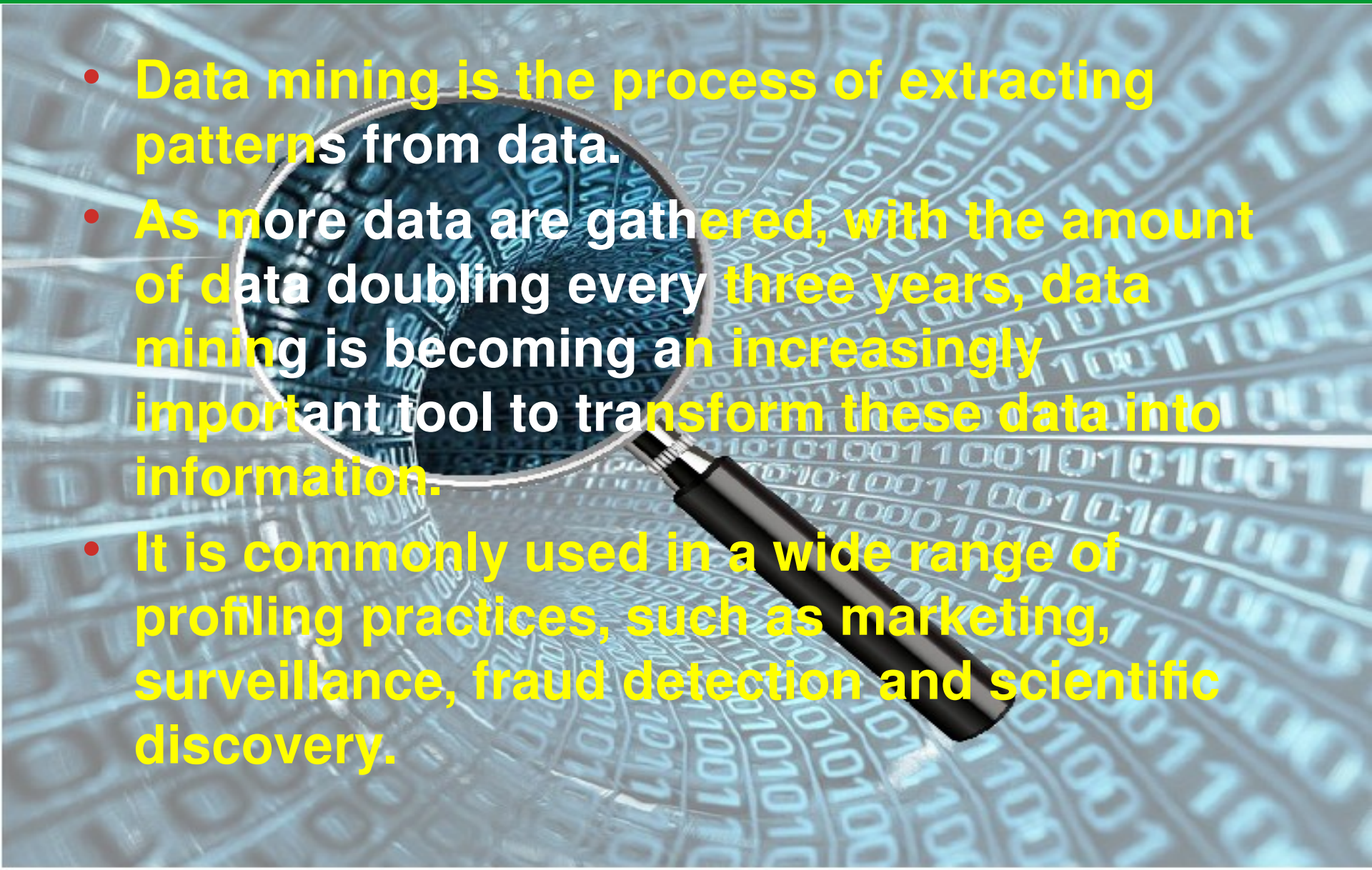
Database transactions

- Data Integrity is very important in database transactions.
- Database transactions have four characteristics called the ACID model.
  - **Atomicity**
    - Ability of the DBMS to guarantee that either all of the tasks of a transaction are performed or none of them are.
  - **Consistency**
    - Ensure that the DBMS remains in a consistent state before the start of the transaction and after the transaction is over (whether successful or not).
  - **Isolation**
    - Requirement that other operations cannot access or see the data in an intermediate state during a transaction.
  - **Durability**
    - Guarantee that once the user has been notified of success, the transaction will persist, and not be undone.

ODBC / JDBC

- **Open Database Connectivity (ODBC)**
  - ODBC provides a standard software API method for using DBMS.
  - The designers of ODBC aimed to make it independent of programming languages, DB systems, and OSs.
  - ODBC uses as its basis the various Call Level Interface (CLI) specifications from the SQL Access Group, X/Open (now part of The Open Group), and the ISO/IEC.
- **Java Database Connectivity (JDBC)**
  - JDBC is an API for the Java programming language that defines how a client may access a database.
  - Provides methods for querying and updating data in a database.

Data mining



- Data mining is the process of extracting patterns from data.
- As more data are gathered, with the amount of data doubling every three years, data mining is becoming an increasingly important tool to transform these data into information.
- It is commonly used in a wide range of profiling practices, such as marketing, surveillance, fraud detection and scientific discovery.

Data Storage

CISSP®

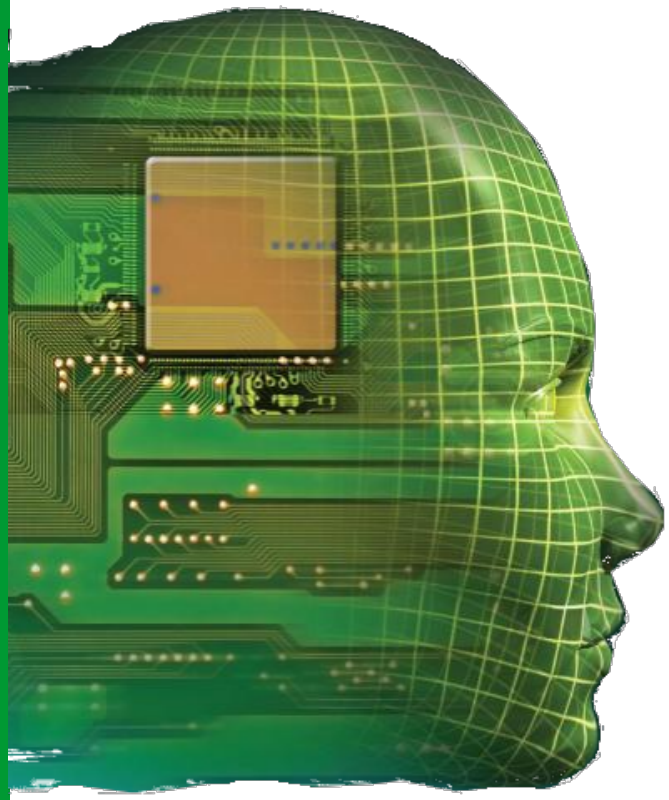
Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Types of Storage

- **Primary Memory -** Random Access Memory (RAM).
- **Secondary Storage**
- **Virtual Memory**
- **Virtual Storage –** RAM Disk
- **Random Access Storage**
  - RAM and Hard-drives are considered Random Access Storage.
  - Such devices are defined as such because any item of stored data can be accessed in the same timeframe as any other item of stored data.
- **Sequential Access Storage**
  - CDs and Tapes fall into this category. It is any device where the disk or tape must be scanned from beginning to end to find items of data.
- **Volatile Storage**
  - Storage where data is lost on power being removed. i.e. RAM
- **Non-volatile Storage**
  - The removal of power does not result in the loss of data.

Knowledge based Systems



CISSP®

Diarmuid Ó Briain

CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Expert System

- Software that attempts to provide an answer to problems.
  - Traditional application and/or subfield of **Artificial Intelligence (AI)**.
- **Knowledgebase**
  - Capture Subject Matter Expert's (SMEx) knowledge.
- **Knowledge engineering**
  - Gathering SMEx knowledge and codifying it.
- Proven by being placed in the same real world problem solving situation as the human SMEx.

Neural Networks

- Neuron's are programming constructs that mimic the properties of biological neurons.
- Used to gain an understanding of biological neural networks, or for solving AI problems.
- Cognitive modelling
  - Simulate some properties of neural networks by build mathematical models of biological neural systems.
- Artificial Intelligence (AI)
  - Based on statistical estimation, optimisation and control theory.
    - Speech recognition
    - Image analysis
    - Adaptive control.

Decision Support System (DSS)

- Information systems that support business and organisational decision-making activities.
- Interactive system intended to help decision makers compile useful information from a combination of raw data, documents, personal knowledge, or business models to identify and solve problems and make decisions.
- Typical information that a decision support application might gather and present are:
  - An inventory of all current information assets (including legacy and relational data sources, cubes, data warehouses, and data marts).
  - Comparative sales figures between one week and the next.
  - Projected revenue figures based on new product sales assumptions.

Application Attacks

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Buffer Overflows

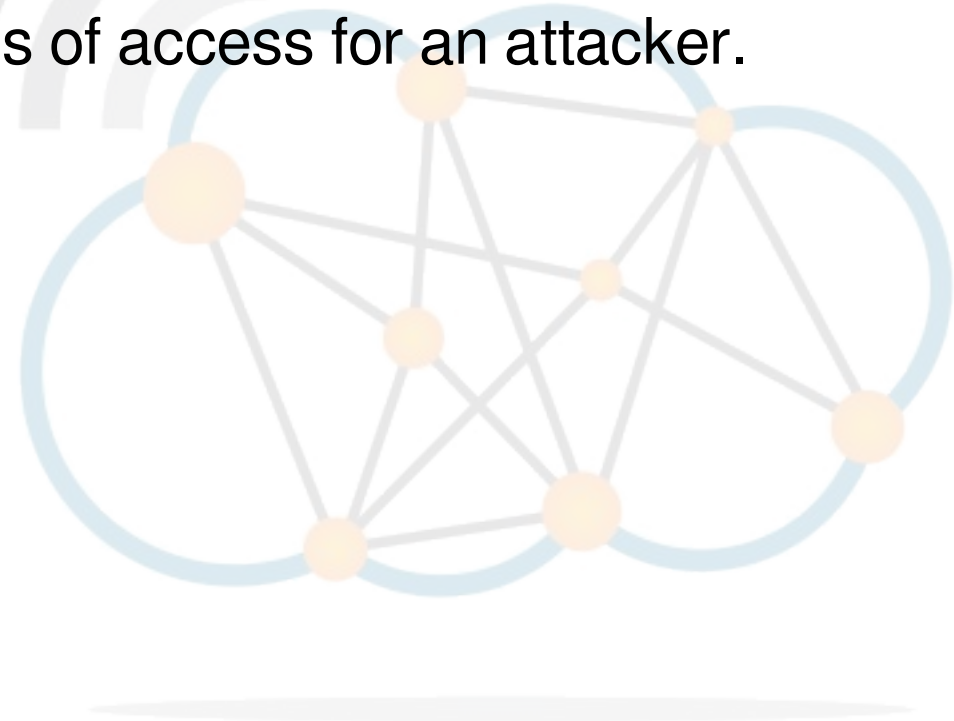
- Anomaly where a process stores data in a buffer outside the memory the programmer set aside for it.
- May overwrite adjacent memory, which may contain other data, including program variables and program flow control data.
- This may result in a crash of the process or the system.
- Basis of many software vulnerabilities and can be maliciously exploited.
- C and C++, provide no built-in protection against accessing or overwriting data in any part of memory and do not automatically check that data written to an array is within the boundaries of that array.

TOCTTOU

- **T**ime **O**f **C**heck **T**o **T**ime **O**f **U**se
- A bug caused by changes in a system between the checking of a condition (such as a security credential) and the use of the results of that check.
- Example
  - Web application that allows a user to edit pages, but allows administrators to lock pages to prevent editing.

Trap doors

- Trap Doors are code sequences that permit access for developers during the write stage.
- If these are not removed before code release they can offer a means of access for an attacker.



Rootkit

- Software system that consists of one or more programs designed to obscure the fact that a system has been compromised.
- An attacker may use a rootkit to replace vital system executables, which may then be used to hide processes and files the attacker has installed, along with the presence of the rootkit.
- Rootkits exist for a variety of operating systems, such as GNU/Linux, UNIX, Mac OS, Solaris and Microsoft Windows aswell as mobile OS like Android.

CISSP®

Diarmuid Ó Briain

CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Cross Site Scripting (XSS)

- Enable malicious attackers to inject client-side script into web pages viewed by other users.
- An exploited XSS vulnerability can be used by attackers to bypass access controls such as the same origin policy.
- XSS carried out on websites were roughly 80% of all documented security vulnerabilities as of 2007.

Cross Site Request Forgery (CSRF)

- Unauthorised commands are transmitted from a user that the website trusts.
- Unlike XSS, which exploits the trust a user has for a particular site, CSRF exploits the trust that a site has in a user's browser.

SQL Injection

- Code injection technique that exploits a security vulnerability occurring in the database layer of an application.

```
SQL> SELECT * FROM transaction WHERE account = '123456789';
A/C 123456789
Date            Sort Code      Account Value          Balance
12/11/2009      99-45-22       98234567       € 2,500         € 8,340
12/11/2009      99-45-22       99876543       € 1,000         € 7,340


SQL> SELECT * FROM transaction WHERE account = '123456789; DELETE
* FROM transaction WHERE account = '123456789'';
A/C 123456789
All transactions deleted !!
```

Reconnaissance Attacks

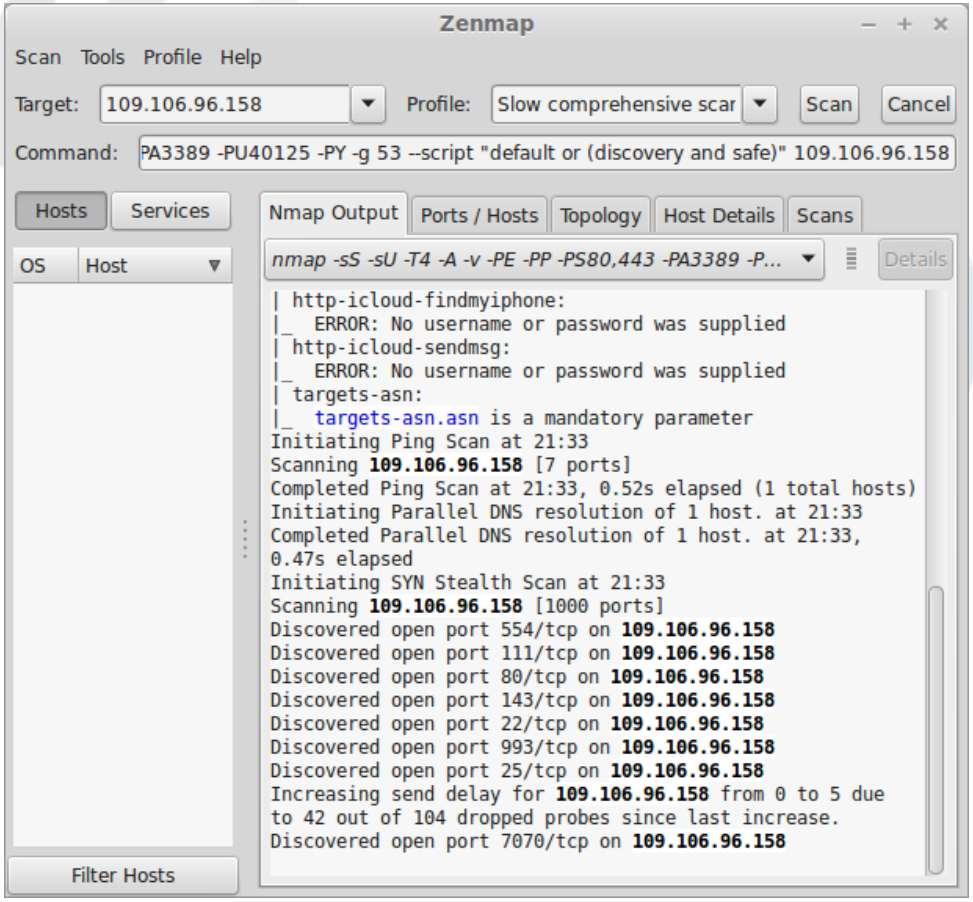
CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

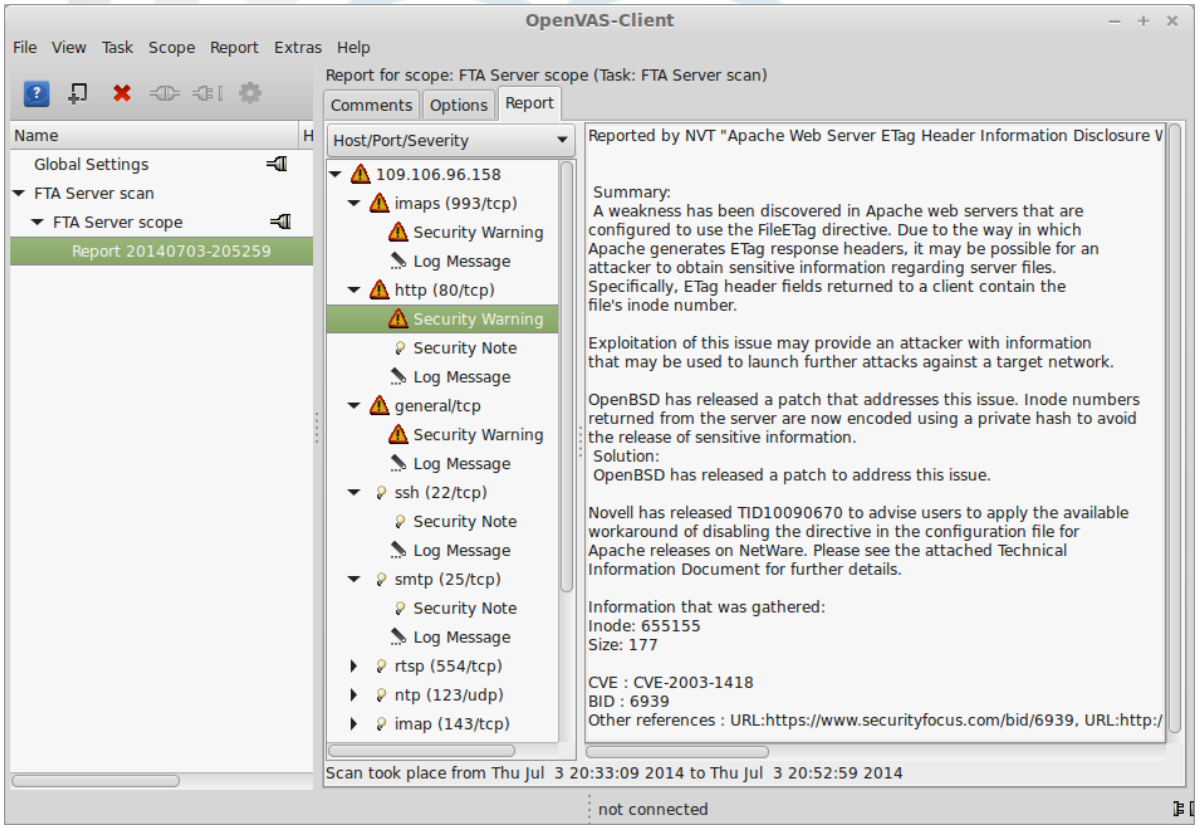
IP Probes and Port Scans

- IP Probes are the initial sweep of a network carried out on a target network.



Vulnerability Scan

- Program designed to search for and map systems for weaknesses in an application, computer or network.



Dumpster diving

- The practice of sifting through commercial or residential trash to find items that have been discarded by their owners, but which may be useful to the dumpster diver.

Masquerade Attacks

CISSP®

Diarmuid Ó Briain
CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

IP Spoofing

- The creation of IP packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system.
- Used in DoS attacks to flood the victim with overwhelming amounts of traffic.
- Ingress filtering is necessary on the gateway to a network to block packets from outside the network with a source address inside the network.
- The gateway should also perform egress filtering on outgoing packets, which is blocking of packets from inside the network with a source address that is not inside.

Session Hijacking

- The exploitation of a valid computer session to gain unauthorised access to information or services.
- It is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. i.e. HTTP cookies.
- TCP session hijacking is when a hacker takes over a TCP session between two machines:
  - Most authentication only occurs at the start of a TCP session.
- A popular method is using source-routed IP packets. This allows a hacker at point A on the network to participate in a conversation between B and C by encouraging the IP packets to pass through its machine.

Decoy Techniques

CISSP®

Diarmuid Ó Briain

CEng, FIEI, FIET, CISSP

diarmuid@obriain.com

Honey pots

- A trap set to detect, deflect, or in some manner counteract attempts at unauthorised use of information systems.
- It consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource of value to attackers.
- These are valuable as a surveillance and early-warning tool.
- Honeypots should have no production value, and hence should not see any legitimate traffic or activity.

Pseudo-flaw

pseudo-flaw.net

Research. Demonstrations. Utilities.

- An apparent loophole or trapdoor that has been inserted into an OS in order to trap unauthorised intruders who access a network.

Thank you