INFORMATION SECURITY IN AN ORGANIZATION

Author Name: Mohammed Mahfouz Alhassan

Zhejiang Normal University

College of Mathematics, physics & Information Engineering, Jinhua –Zhejiang Province, CHINA.

Email: [mmalhassan@tamalepoly.edu.gh](mailto:mmalhassan@tamalepoly.edu.gh)

*Abstract:* Information security is one of the most important and exciting career paths today all over the world. Information security simply referred to as InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

It is a general term that can be used regardless of the form the data it may take (e.g. electronic, physical data, with knowledge of information security we are confident that our data is protected and also assured of the safety of our data and ensure that the value of our organizations maintained.

But this is not the only explanation experts have given, information security is the life savior of organizations all over the globe.

So people in this field can be considered as the physicians of the computer system, also we can call them the pathologist or better still the cardiologist of the computer system. Let‘s not under-estimate the impact of security incidents, which can lead to data loss, leaks of personal information, wasting of time, and the spread of viruses. We shouldn’t’ think that security incidents that happen to other computers will not affect us. We should take responsibility in managing your own information.

Keep alert to news regarding security threats and equip ourselves and organizations with the latest knowledge. Consult experts and advisors if you are in any doubt.

Keep a contact list of assistance, e.g. public services, application support, and ISP hotlines.

***Keyword:* Defending information from unauthorized access, Key to the future of every organization.**

**ACKNOWLEDGEMENT**

My greatest Thanks, goes to my supervisor Professor, Han Jianmin of Zhejiang Normal University.

College of Mathematics, Physics, and Information Engineering for his excellent supervision and guidance, skills and help, and more importantly guiding me through each and every step of the process with knowledge and support, Thank you for very much your advice.

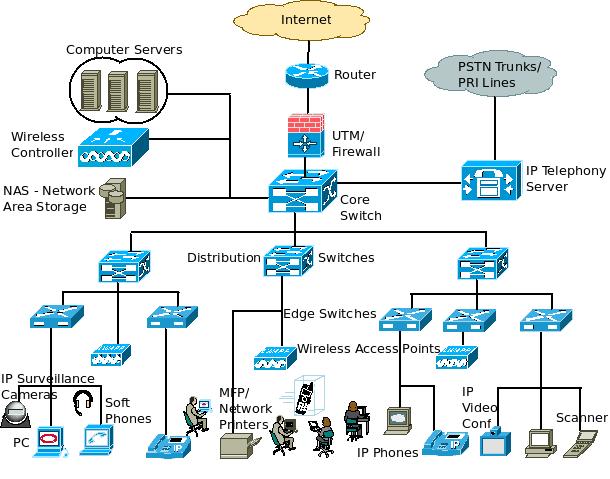
I will always remain grateful. It has been an honor to study under your guidance.

**I. INTRODUCTION**

Information security is of great importance and interest to everybody in the world of technology today, whether you are a mobile phone or a personal computer user, this is why information security is of the most importance in our everyday life, and in the IT technology fields.

The Study of information security has so many concepts and also topics that every IT professionals should master or have some basics of, the knowledge and skills of information security are just some few that is essential for all those that are involved in the IT technology sector. E.g. Cyber-security analyst, forensics analyst, network administrators, systems administrators, application developers. Lack of knowledge in this important field of information security will be more likely to develop applications that are not secure or build networks that are insecure and easier for attackers to penetrate, this is why information security knowledge is very important in our everyday lives. Regardless of the choosing career, you find yourself in the IT technology sector.

**II. Security Knowledge for Network Administrators**



**Fig. 1 Security Architecture - Enterprise Network Architecture Diagram.**

The general term that would refer to these specialists as a webmaster. There are various factors involved in drawing visitors to your site and turning them into customers.

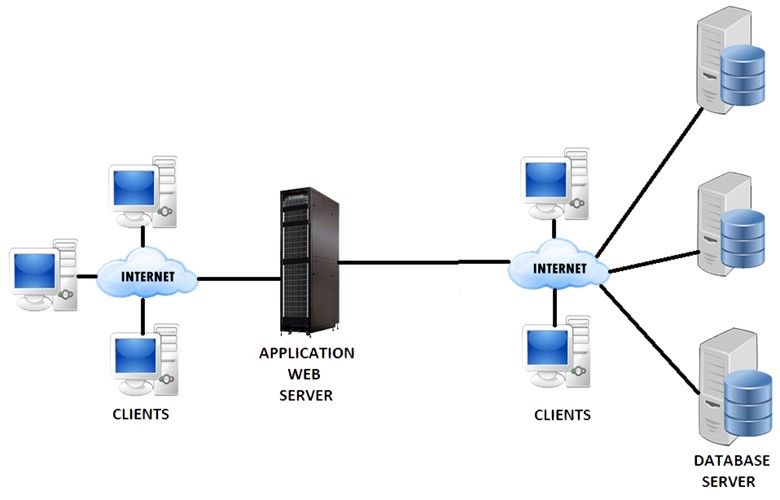
No matter how attractive your site looks like, looks alone are not enough to generate sales. Rather than entrusting your website to inexperienced service providers who may not have a full range of webmaster Skills, it’s extremely important that you enlist the help of proficient webmasters, without basic knowledge of information security, the webmaster or web developer is very likely to design or program a website that will easy to for attackers to penetrate.

The importance of information security in a computer-based environment has resulted in a large stream of research that focuses on the technical defenses (e.g., encryption, access control, and firewalls) associated with protecting information (e.g., Anderson [1972],

**I.T Security Knowledge for Database Administrators**

Database administrators are responsible for the management of our database servers in the organization, databases are used to store our valuable information in the organization's database.

Many professionals have given lots of insight into the core function of a database administrator, one of them is the management of data, but some organizations define different functions for the Data Administrator than those of the Network Administrator. Database Administration concerns the responsibility for serving as the custodian of the firm’s data.



**Fig. 2 *Database Security Architecture***

The Data Administrator: resolves disputes that arise because data are centralized, but shared among system users. Decides where data will be stored and managed. Maintains corporate-wide data definitions and standards. Plans for database usage, analysis, design, implementation, maintenance, and protection. Has a high level of both managerial and technical skills.

Database Administration involves the actual hands-on, physical management of databases. This is a very technical function that focuses on physical database design issues including security enforcement, system performance, and backup/recovery. I know this may sound confusing.

Well there is a difference between a Data Administrator and Database Administrator:

A data administrator (also known as a database administration manager, data architect, or information center manager) is a high-level function responsible for the overall management of data resources in an Organization. In order to perform its duties, the DA must know a good deal of system analysis and

Programming.

These are the functions of a data administrator (not to be confused with database administrator functions):

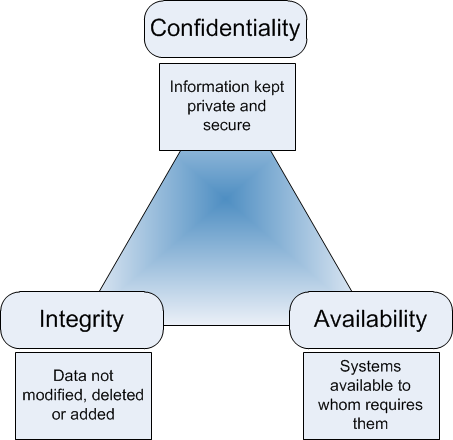
* Data policies, procedures, standards
* Planning- development of organization’s IT strategy, enterprise model, cost/benefit model, the design of database environment, and administration plan.
* Data conflict (ownership) resolution
* Data analysis- Define and model data requirements, business rules, operational requirements, and maintain corporate data dictionary
* Internal marketing of DA concepts
* Managing the data repository.

Database administration -is more of an operational or technical level function responsible for physical database design, security enforcement, and database performance. Tasks include maintaining the data dictionary, monitoring performance, and enforcing organizational standards and security. There is also the database steward, Database stewards- are the people with administrative function responsible for managing data quality and assuring that organizational applications meet the enterprise goals.

It is a connection between IT and business units. Data quality issues include security and disaster recovery, personnel controls, physical access controls, maintenance controls, and data protection and privacy. For example, in order to increase security, the database steward can have control over who can gain access to the database by assigning a specific privilege to users.

**CIA in Information Security**

Does the name CIA or term sound familiar, the core function of the CIA. (Central Intelligence Agency) is a civilian foreign intelligence service of the U.S. Government, tasked with gathering, processing and analyzing national security information from around the world, primarily through the use of human intelligence. Is an arm of the United States secret Service, in fact, a very important arm of The United States secret service o better still one of the most respect security institution in the world? Well the CIA in computer terms or in information security is known as:



**Fig 3. CIA Architecture**

**C-Confidentiality**

**I-Integrity**

**A-Availability**.

Well anybody body who is abreast with the works of the US secret service, knows the core functions of the CIA in the united states well these concept in Information security means having confidence in something, and logically we all know what having confidence in something means, in simple terms it means trusting in the person or a thing. so in information security cycles , confidentiality is to make or ensure that only trusted people are seeing or accessing the information and ensuring that the confidence of the information is maintained Confidentiality- has a lot to do with technology, that helps protect data and also to ensure only the right or trusted people have access to the data. And how do to ensure or be assured that the people we so much trust will not turn against us or abuse the trust we have in them. This is where integrity comes in, it means we should be sure that the person we so much confidence in, is someone or is a person that has integrity and someone that stand up to his words committed individual that is committed to his/her work, this is the same with computer security, it will always be what we knew it to be now or at later time when we return to access the data.

Integrity helps ensure that our data is what it’s supposed to be, anytime we need it, this is where availability comes in.

CIA. Confidentiality, integrity availability. This word keeps being discussed throughout when discussing information security.

**Concept of Triple-An in Information Security**

The term or acronym AAA stands for Authentication, Authorization, and Accounting. (Or better still auditing)

The last A. Authentication -is what helps identify the identity of an individual, and not only that, it helps

Protect our machines and our personal selves until it’s certain or verifies the true identity of the

Individual.

Authorization- then helps control who has access to our systems and whatever it’s in the machine, and it works with the help of authentication, when our authentication is weak, whatever the machine authorizes will be useless or will be very weak, so authorization depends on authentication before it

Can function properly, when the system or the machine, it’s very easy for hackers to attack, by just

Guessing the password and getting access to the data on the machine.

Accounting-well this accounting is not the accounting we know in financial terms, or in financial world, in information security (IT) this is referring to watching what other people do on our network, things they access, when they accessed it, from where they access it, are they running other programs on the machines, like programs that will allow them to sit in another location and still our valuable data. Or reading confidential documents on the systems, or also if the person is creating a new file or modifying a File, this is the accounting that goes on within the computer system, it is for this reason that it’s sometimes referred to as Auditing. Because it performs the functions of audits of whatever is going on the system, be it a single system, or many systems on the network some expert also said the first process in (AAA),

Authentication provides a way of identifying a user, typically by having the user enter a valid username and valid password before access is granted. The process of authentication is based on each user having a unique set of criteria for gaining access. The AAA server compares a user’s authentication credentials

With other user credentials stored in a database. If the credentials match, the user is granted access to the network. If the credentials are at variance, authentication fails and network access is denied.

Following authentication, a user must gain authorization for doing certain tasks. After logging into a System, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Simply put, authorization is the process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted.

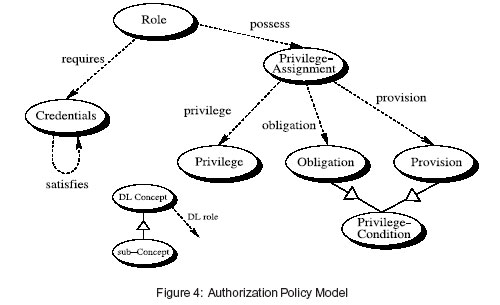
Usually, authorization occurs within the context of authentication. Once you have authenticated a user, They may be authorized for different types of access or activity.

The final plank in the AAA framework is accounting, which measures the resources a user consumes during access.

This can include the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics and usage information and is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

**Least Privileges**

Ensures that the user is not given more capabilities than required to perform his or her responsibilities.

Also known as the principle of minimum necessary access. A process running on a computer can access.

A capacity is a capability or a permission, functions, rights, things that they are allowed to do.

Each user or process has a responsibility. Let’s take, a company CEO, has the responsibilities of his company’s financial matters, and so in that case, so that person should be given the rights to all financial data, so in this case the duties of function or the financial officer doesn‘t include the checking the email because he or her not or does not have that permission. The duty is only to handle the financial matters of the company. And not the management of the email server or checking the staff emails of the company. Least privileges are enforced through proper permission management. Discretionary Access control: when properly implemented is in compliance with least privilege, so discretionary access control is used in deciding what people can access. In simple terms, we can call it controlling what is accessed on the network, and not everyone can access everything but can access what is granted to them, things they need to access.

**Surface Attacks**

Combined points through a system may be attacked. E.g. keyboards, mouse, USB Ports, CD/DVD drives, external drives, firewire and etc. this are able to allow a person to the physical machine. Your attack surface is the sum of your security risk exposure. Put another way, it is the aggregate of all known, unknown and potential vulnerabilities and controls across all software, hardware, firmware and networks. A smaller attack surface can help make your organization less exploitable, reducing risk.

A typical attack surface has complex inter-relationships among three main areas of exposure: software

Attack surface, network attack surface, and the often-overlooked human attack surface. The same

Way, if that machine is on a network, the attack points can be the points, e.g. if the machine is on the web server, it can easily be attacked through the port, like port 80. If the machine is on the SMTP server it’s easier to also gain access to the SMTP services, same with active directory services (LDAP) lightweight active directory protocol.

But the good news is that there is a way we can minimize or reduce the impact of the attack when it occurs on the machine. By simply using attack service reduction, by disabling unneeded services, so we can also do that by simply using a firewall to block the port, though the application might be running on the machine. Another simplest way is to just disconnect the machine from the network. These are the some of the methods used in preventing some Attacks on our network. Even if it happens it will be minimal.

**III. CONCLUSION**

We should take responsibility in managing your own information and security, and also take steps to Protect and secure our data, and help build the capacities of those responsible for the security and investments of our organizations, with the world moving at a faster pace, so are hackers, like Script Kiddies, these kind of cyber criminals normally don’t care about hacking. And the other cyber thieves, that exploit on people's ignorance on information security issues. Information security is a life savior, and the only Cure is to make it affordable for people to take advantage of the tremendous benefits it has in other to help save the world. I believe information security will make the world a better place for all.

And prevent all

People in this world from using the computer and the Internet to hurt innocent people.

**REFERENCES.**

1. *Rigney. al., "Remote Authentication Dial In User Service (RADIUS),"*[*RFC 2865*](ftp://ftp.rfc-editor.org/in-notes/rfc2865.txt)*(Obsoletes RFC 2138, 2058), June 2000.*

*Simpson W., "PPP Challenge Handshake Authentication Protocol (CHAP),"*[*RFC 1994*](ftp://ftp.rfc-editor.org/in-notes/rfc1994.txt)*, August*

*1996.*

*(2) ACM Transactions on Information and System Security, Vol. 5, No. 4, November 2002*

*FINNE, T. 1998. A conceptual framework for information security management. Compute. Sec. 17,*

*4, 303–307.*

*(3)0FRICKE, D. 2000. Balancing cooperation and risk in intrusion detection. ACM Trans. Inf. Syst.*

*Sec. 3, 1 (Feb.), 1–29*.

(4)HOO, K. 2000. How much is enough? A risk-management approach to computer security. Consortium

For Research on Information Security Policy (CRISP) Working Paper. Stanford University, Stanford, Calif., June.

(5)A secure capability computer system. In Proceedings of the IEEE Symposium

On Security and Privacy. IEEE Computer Society Press, Los Alamitos, Calif, pp. 86–94.