Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 66 (2014) 20920-20923

Elixir ISSN: 2229-712X

Analytical Vs Experimental Approach to Implement Hard Disk Security Architecture

Minal Moharir[1,*] and A V Suresh[2]

[1]Department of Information Science and Engineering, R V College of Engineering, Bangalore, India.
[2]Dean Academics, R V College of Engineering, Bangalore, India.

ARTICLE INFO

Article history:
Received: 5 June 2013;
Received in revised form:
20 January 2014;
Accepted: 22 January 2014;

Keywords
Information Security,
Integrity,
Confidentiality,
Authentication,
Encryption, queuing theory.

ABSTRACT

As of January 2011 the internet connected an estimated 941.7 million computers in more than 450 countries on every continent, even Antarctica (Source: Internet Software Consortium's Internet Domain Survey; www.isc.org/index.pl). The internet is not a single network, but a worldwide collection of loosely connected networks that are accessible by individual computer hosts, in a variety of ways, to anyone with a computer and a network connection.

Introduction

As of January 2011 the internet connected an estimated 941.7 million computers in more than 450 countries on every continent, even Antarctica (Source: Internet Software Consortium's Internet Domain Survey; www.isc.org/index.pl). The internet is not a single network, but a worldwide collection of loosely connected networks that are accessible by individual computer hosts, in a variety of ways, to anyone with a computer and a network connection.

However, along with the convenience and easy access to information come risks. Among them are the risks that valuable information will be lost, stolen, changed, or misused. If information is recorded electronically and is available on networked computers, it is more vulnerable than if the same information is printed on paper and locked in a file cabinet. Intruders do not need to enter an office or home; they may not even be in the same country. They can steal or tamper with information without touching a piece of paper or a photocopier. In this way security of stored information is an important issue. The proposed paper considers the security of Hard Disk Drive which is a fundamental element in computing chain.

Analytical modeling is a powerful tool that can offer accurate performance analysis at the small cost. Analytical models are mathematical representations of a particular computer system [68]. Queuing theory is used to define the relationships between various resources (e.g. CPU, disks, memory, etc.) and their queues [1]. These algorithms are populated (parameterized) using measurements taken from a running system. Once the model is built, parameters can be changed to represent possible changes to the running system [2]. The model can accurately project the impact of these changes.

DisTrust a HDD security system is model using queuing model. The proposed Disktrust system offers storing of sensitive information on the secure partition on the HDD as per Partial Disk Encryption. While storing information on HDD, it gets encrypted on-the-fly (seamlessly). The modeling is done here to calculate the CPU processing time & total response time to process a user's request.

The paper organized as follows. The experimental model is discussed for the proposed hard disk security system in Section 2. The analytical model is discussed for the proposed hard disk security system in section 3. Both the models are tested for different load conditions in section 4. Finally the conclusions are drawn section 5.

Disk Trust Experimental Model

The section proposed a windows based HDD security software labeled as DiskTrust as shown in Fig.1. DiskTrust technology uses PDE, creates authorized invisible volume on HD & implements Symmetric Key Cryptography with Rijndael(AES-128) to secure the data stored on secured volume

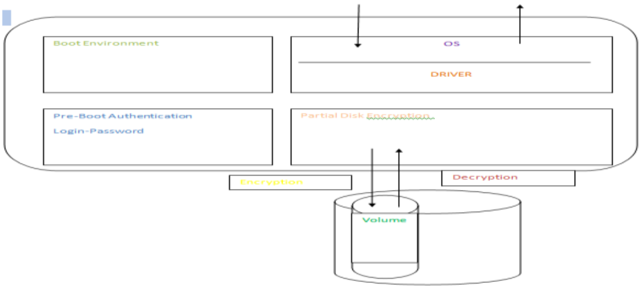

Figure 1. Disktrust Exprimental Architecture

Tele:
E-mail addresses: moharirminal@gmail.com

The technical objectives of the thesis are:

1. Create Hidden partition : A hiddenvolume is created on HDD using window based DiskPart utility.
2. Check authentication: User identity is checked before accessing the contents of created secured volume. Dynamic login-password scheme has been implemented for the user identification.
3. Store/access data from the hidden volume: once the user is identified, can store/ access data. Here the data is encrypted or decrypted on the fly. The encryption is implemented using symmetric key cryptography with AES-128.
4. Execute encryption/decryption algorithm while reading /writing data on Hard Disk Drive.

The above steps are implemented in Java. The model is tested for minimum load, average load and maximum load conditions. (here load specifies number of encryption requests).

DiskTrust Analytical Model

DisTrust a HDD security system is model using queuing model. The basic notations are shown in Fig. 2. In real world, the user needs to secure his personal data. The proposed Disktrust system offers storing of sensitive information on the secure partition on the HDD. While storing information on HDD, it gets encrypted on-the-fly (seamlessly). The modeling is done here to calculate the CPU processing time & total response time to process a user's request.

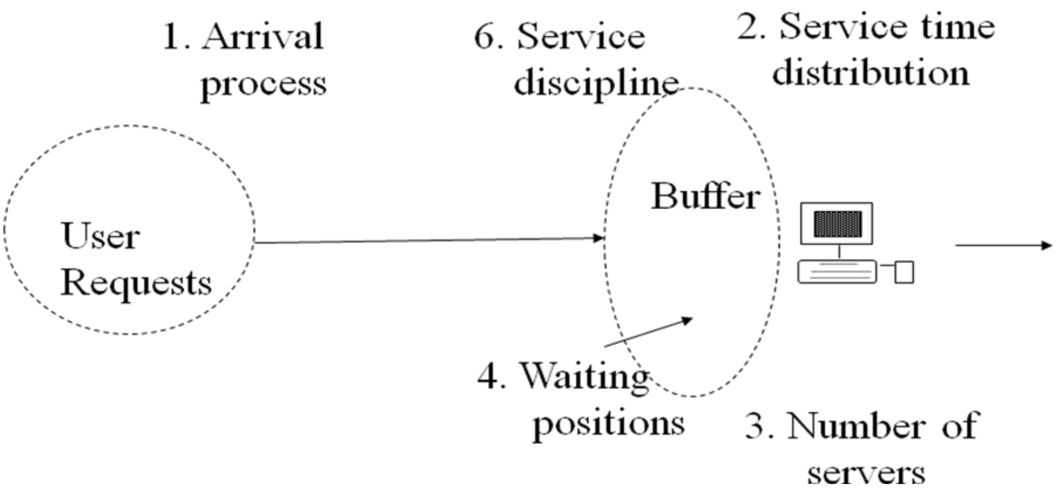

Figure 2. Basic Components of a queue to model DiskTrust

To specify a queuing system, the work needs to specify these six parameters. Queuing theorists, therefore, use a shorthand notation called the Kendall notation [3] in the form A/S/m/B/K/SD, where the letters correspond in order to the six parameters listed above. That is, A is the interarrival time distribution, S is the service time distribution, m is the number of servers, B is the number of buffers (system capacity), K is the population size, and SD is the service discipline.

To model the proposed system, it is assumed that the interarrival time and the service time are exponentially distributed and there is only one processor. There are no buffer or population size limitations and the service discipline is FCFS[2]. So the proposed system to be model can be written as M/M/1 queue.

The state of this queue is given by the number of requests in the system. A state transition diagram for the system is shown in Fig. 3. It is similar to that of the birth-death processes with the following correspondence:

$$\lambda_n = \lambda, \quad n = 0, 1,2,...,\ \infty\ldots\ldots\ldots(1)$$

$$\mu_n = \mu, \quad n = 1, 2\ \ldots\ldots\infty\ldots\ldots\ldots\ (2)$$

Theorem[2] gives us the following expression for the probability [5] of n requests in the system:

$$p_n = \left(\frac{\lambda}{\mu}\right)^n p_0 \qquad n = 1,\ 2,\ \ldots\ldots\infty\ \ \ldots\ldots(3)$$

The quantity λ/μ is called traffic intensity and is usually denoted by symbol ρ. Thus

$$p_n = \rho n\ p_0\ \ldots\ldots\ldots\ldots\ (4)$$

Since all probabilities should add to 1, we have the following expression for the probability of zero jobs in the system:

$$p_0 = \frac{1}{1+\ \rho +\ \rho 2 + \cdots + p\infty} = 1\text{-}\rho\ \ldots\ldots\ldots\ (5)$$

Substituting for ρ_0 in p_n, we get

$$pn\ =\ (1-\rho)\rho^n\ , \qquad n = 0,1,2,...\infty\ \ldots\ldots\ldots(6)$$

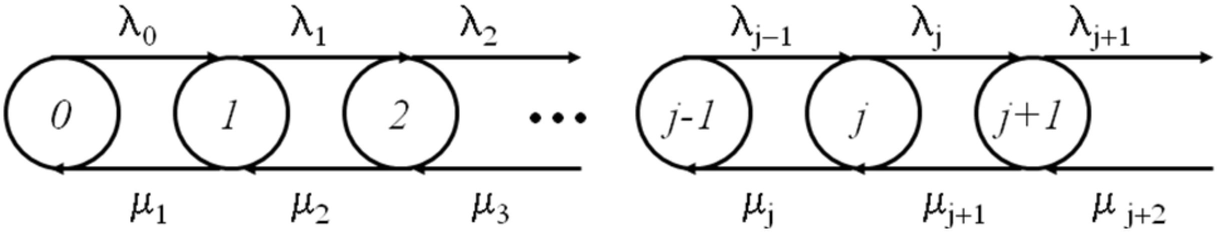

Figure 3. State transition diagram for an M/M/1 queue to model DiskTrust

Notice that n is geometrically distributed [3]. We can now derive many other properties of the M/M/1 queues. For example, the utilization of the server is given by the probability of having one or more requests in the system:

$U = 1 - p_0 = \rho$ ………… (7)

The mean number of requests in the system is given by

$$E[n] = \sum_{n=1}^{\infty} npn = \sum_{n=1}^{\infty} n\left(1-\rho\right)\rho\mathbf{n} = \frac{\rho}{\mathbf{1}-\rho} \text{ ………………………..(8)}$$

The variance of the number of requests in the system is

$$Var[n] = E[n]2 - (E[n])^2 = \qquad - (E[n])^2 = \frac{\rho}{\mathbf{1}-\rho\mathbf{2}} \text{ ……...…..(9)}$$

The probability of n or more requests in the system is

$$p\ (\geq n \text{ jobs in system}) = \sum_{j=n}^{\infty} pj = \sum_{j=n}^{\infty} \left(1-\rho\right)\rho\mathbf{j} = \rho^n \text{ ……………….….(10)}$$

The mean response time can be computed using Little's law, which states that

Mean number in system = arrival rate × mean response time

That is,

$E[n] = \lambda E[r]$ ……………………………………………………….….. (11)

or

$$E[r] = \frac{\mathbf{E[n]}}{\lambda} = \frac{\rho}{\mathbf{1}-\rho}\frac{\mathbf{1}}{\lambda} = \frac{\mathbf{1}/\mu}{\mathbf{1}-\rho} \text{ ……………………………………….. (12)}$$

The cumulative distribution function (CDF) [6] of the response time can be shown to be

$F(r) = 1 - e{-}r\ \mu\ (1{-}\rho)$ …………………………………………………. (13).

Notice that the response time is exponentially distributed. From the distribution, we can also find out its percentiles. For example, the q-percentile of the response time can be computed as follows:

$1 - e\ {-}r_q\mu(1{-}\rho)$……………………………………………………… (14)

or

$$r_q = \frac{\mathbf{1}}{\mu(1-\rho)} \ln\left(\frac{100\rho}{100-q}\right) \text{ ………………………………………..……(15)}$$

When there are no requests in the system, the processor is said to be idle; at all other times the server is busy. The time interval between two successive idle intervals is called busy period.

$$\text{System Throughput} = \frac{\textit{Total number of Request}}{\textit{Total Time}} \text{ ………………………..………….. (16)}$$

Results

The analytical model for proposed 'DiskTrust: HDD security Technique' is implemented and thoroughly tested in section 3. The experimental model for DiskTrust: HDD security Technique is implemented and thoroughly tested in section 4.

For the experimental model, the current work has used a laptop PentiumV 2.4 GHz CPU, in which performance data is collected. In the experiments, the laptop encrypts a different file size ranges from 1MB to 512MB. The performance metrics are collected are:

1- Encryption time

2- CPU process time

The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time [7].

The CPU process time is the time that a CPU is committed only to the particular process of calculations. It reflects the load of the CPU. The more CPU time is used in the encryption process, the higher is the load of the CPU. The CPU clock cycles are a metric, reflecting the energy consumption of the CPU while operating on encryption operations. The following tasks that will be performed are shown as follows:

The performance comparison for the both (analytical, experimental) models is shown in table 5. The comparison is done based on three cases 1) minimum load (5-rquest/second) 2) average load(20-rquest/second) 3) maximum load(50-rquest/second). For analytical model CPU utilization and Response time are calculated according to formula mentioned in chapter 3. For experimental time the CPU usage and response time to process the user request are measured experimentally.

Table 1. DiskTrust Analytical Vs Experimental Model

Load/ Calculation	Analytical Model		Experimental Model	
	CPU Utilization	Response Time	CPU Utilization	Response Time
Minimum Load(5-rps)=125B	0.25	2.66ms	0.1	1.57ms
Average Load(20-rps)=250B	0.5	5.33ms	0.75	5ms
Maximum Load(50-rps)=500B	1	10.78ms	2.45	8ms
Average	5.25	18.77	3.3	14.57

The performance comparison of Analytical Vs. Exprimental Model is graphically plotted as shown Fig. 4

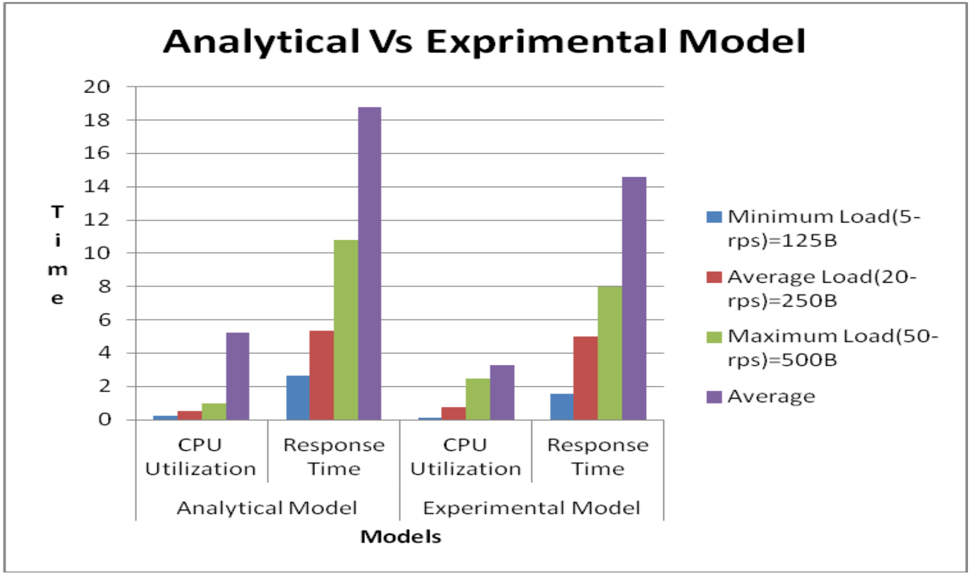

Figure. 4 Analytical Vs. Exprimental Model

Conclusion

The propsed arhitechture implements Hard Disk Security using Partial disk encryption for small scale applications. The analytical and exprimental model are develed. The models are evaluted for minimum, average and maximum load conditions. The variations are more for minimum load conditions. The results are almost similar for average laod conditions. The delta or variaton is 0.25 for CPU utilization for the best case.The delata or variation is 0.33 for response time for the best case.

References

[1] Throughput in Processor-Sharing Queues Na Chen; Scott Jordan Automatic Control, IEEE Transactions on Feb. 2007Volume: 52 , Issue: 2 Digital Object Identifier: 10.1109/TAC.2006.887906, Page(s): 299 – 30.

[2] R. Jain, "The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulatio n, and

[3] Vikas Kaul, S K Narayankhedkar, S Achrekar, S Agarwal, P, Security Enhancement Algorithms for Data Transmission for Next Generation Networks, International Conference & Workshop on Recent Trends in Technology, (TCET) 2012, Proceedings published in International Journal of Computer Applications(IJCA).