STUDENT DETAILS

Name: Chintamani Masthanaiah
Reg.No.: 191CS115
Class: 2nd year, Sem-4

PAPER DETAILS

Title of the paper: **Securing Database Management Systems using RAM Serial Numbers**

Author names: Sapan Noori Azeez
Department of Software Engineering, Firat University, Elazig, Turkey
Serkan Varol
Engineering and Technology, Southeast Missouri State University, Cape Girardeau, Missouri, USA

Conference Name: 2019 7th International Symposium on Digital Forensics and Security (ISDFS)
Year of Publication: 2019
Reference Link: https://doi.org/10.1109/ISDFS.2019.8757496

SUBMITTED TO: MR. ANNAPPA

Submitted Date: 10th April,2021

ANALYSIS REPORT ON THE SELECTED PAPER.

Abstract in your own words

For any database management system, protection and security are two important elements of any newly launched product to prevent copyright principles. Protection is important for identifying the system faults which would lead to system failures and also prevent from the unauthorized people. Security is to defend against the hackers/malware when they try to access the source code. This can be implemented in many ways. But this paper explains one of these methods i.e... using the RAM serial number to encrypt the software and hardware, which is easier and simpler for the developers in future use.

Problems addressed in the paper and Solutions suggested/implemented

How the encryption security on ITC (Information Technology Computer) can be used to protect DBMS when ENCRYPTION strategies are employed?

Sol. There are two types of encryption. One is hardware encryption, another software encryption. Software encryption is done through the external programming language by generating the unique program through the software tools created by the vendors. When any program is installed these tools create a unique id using the tools.

But there can be an attack from internet where anti-malwares fail to protect in some case of these software encryptions. These pull the extra method for encryptions which can be satisfied by the hardware. Hardware-based encryption is the use of computer hardware to assist software.

Using encryption in the targeted system and form connection between program application and RAM (random access memory) of the Personal Computer (PC) by using the serial number for the PC, which is installed in order to prevent the databases from being copied by other parties.

Hence, Protection and security are foremost important to sustain in this competitive world. Some companies knowingly target the growing companies.

How to check the Serial Number of RAM when accessing with the help of another programming language? How to fetch the serial number to check?

Sol. This facility is provided by the WMI, Windows Management Instrumentation. With the help of the following three, we can able to access the information of any device/driver.

1. Win32_PnPentity
2. Win32_Systemdriver
3. Win32_PnPSigneddriver

The above 3 files are sufficient to fetch the RAM serial number. But we need another

programming language to implement the check.

CAS, Code Access Security power to monitor the authorizations that is associated with an individual. It is one of the 2 kinds of security in ICT (Information and Communication Technology).

How attackers are prevented from accessing the vulnerable.?

Sol. When the program code is accessed, the application will check the RAM of the requested computer, if it matches correctly, the access is given, else denied. .NET framework shields the source code, with the help of WMI, its cross check the RAM value. The genuine method of ensuring security from robbery is to construct the basic parts of your electronic application to provide every one of your clients with a unique ID while communicating with the administration. This may seem hard or even impossible; however, to be completely forthright, there is no other feasible way.

Problems arises due to overemphasis on the accessibility

Sol. Excessive attention on one goal can create issues with the meeting other targets like data availability, data protection, data reliability.

Overemphasis on high accessibility can prompt issue with information safeguard (like when we account for more accessibility, the data need to be redundant which create chaos during system crash). In any case, for applications that require high accessibility, the greater part of the important segments of the IT framework should be tuned to a similar relative level of security.

As the accessibility increases, cost increases quickly. Interest in accessibility can usually enhances information conversation. Venture are likely advantages if the minimal cost increment is proposed. So many companies don’t fully depend on accessibility, which put other aspects of data in trouble.

Future work proposed

No future work is proposed in the paper.

Related problems which are not addressed

Failure of RAM functioning is not addressed.

It is challenging to practice information security while ensuring unique protection tendencies and securing personal data.

Your solution (thought of / implemented fully or partially) to the problem addressed / Future work proposed / Related problems which are not addressed / Issues in the proposed solution)

There need to be multiple RAMs. If one fails to function, other can serve and protect the information meanwhile the former is replaced.

Conclusions

Most of the data is present in the database. Security and protection are important. DBMS internally has 2 more things aside data i.e., data motor (permits data to be lock) and DB pattern (coherent structure) which is responsible for the concurrency, security, independent data. CAS is used to secure our programs and the RAM as plugged into computers' ports. To increase the security protection, the serial number of the RAM must be taken and put into the program that has been created. Nevertheless, programming encryption cannot able to defend against the client mistakes.

Additional References

Hardware-based encryption - Wikipedia
Windows Management Instrumentation - Wikipedia
5 Symptoms of a RAM Problem and How to Fix It - TurboFuture

Plan (if any) for continuation of this work (which may lead to implementation, results and possible publication).

Have a thought to research how we can secure the information through hardware and software more effectively these days. Since the world is moving to digital, we need to find more easier, stronger ways to protect us from threats.

Security is the place I would like to research. This led me to choose this paper as starter.

~~THANK YOU~~