Approach to Secure Distributed Data Storing by Quasi-Random FAT Network Mapping

Yuri Dobush, Ivan Demydov

Abstract – **The conception of secure distributed data storing system is described. Quasi-random approach for data-flow routing into different encrypted flows to distributed network FAT at servers' databases is proposed.**

Keywords – **data storing network, secure data storage, distributed data storage, data flow routing.**

I. The Method Description

There is actual problem existing of secure data storing for different kind of applications such as commercial and non-commercial databases. The prospective effect of these techniques lays on the independent financial informational security with strong spatial distributed defense of every informational data flows from main access Host to 1...N Servers, which held special dedicated data storage space (Fig. 1). We accept that initial data flow division into File router of the main access Host to the N independent flows, routed to data Servers' dedicated storage spaces quasi-randomly, in accordance with sequence, generated into Key maker module. This sequence could be also saved into secure data Storage and describes Network Map (NetMAP) for File Allocation Table (FAT), in order to route initial data flows to DB Servers and reverse it to Host properly when required.

Different mechanisms should be implemented to generate reliable and strong key sequence, such as biometric-based attractors, special encrypting algorithms with strong physical insulation of the used key carrier to secure the flow routing and FAT mapping, NetMAP access processes [1].

The robust network configuration in corporative or public networks, which deal with secure distributed data, provides perfect data accessibility and inability to detect and identify a content of each independently stored data flow stream, generated by routing according to quasi-random generated network FAT map [2, 3].

II. Practical Implementation Features

Fig. 1 describes basic relations between components of the secure distributed data-storing system. It is necessary to provide reliable key generating and keeping it into proper key storage and, if possible, to use other identification mechanisms, that, for example, providing access by biometric authorization subsystem. External interfaces to network "cloud" of the main access Host should be secured by author's technique [1], where properties of each Host Ethernet line are controlled electrically to prevent unauthorized access or data theft.

In order to store data reliably and provide necessary accessibility each flow must be duplicated to the different servers simultaneously. Data packing and de-packing into/from data-flows before/after routing could be realized by appropriate encryption algorithms.

Ivan Demydov – Ph.D., Lviv Polytechnic National University, Telecommunications Dept., 12, St. Bandery Str., 79013, Lviv, Ukraine. E-mail: web@post.su, demydov@lp.edu.ua
Yuri Dobush – Ph.D. student, Lviv Polytechnic National University, Telecommunications Dept., 12, St. Bandery Str., 79013, Lviv, Ukraine. E-mail: mklimash@lp.edu.ua

Dedicated databases (DB) at Servers should use data recovery information to guarantee accessibility of data in case of the one or more network servers will be unreachable. These additional volume of the information could be generated by the main access Host instantly at the process of data encryption.

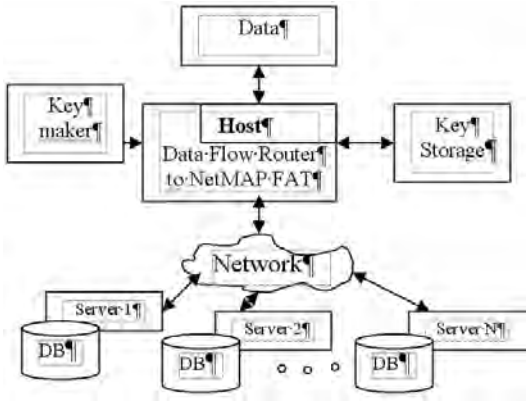

Fig. 1. The basic component relations for proposed secure data storing system.

Conclusion

Proposed secure distributed data storing system could find application at the financial data-centers, national secure data storing services and other. The effective data division to different flows increases network database system security more, than every encryption algorithms, makes network system more emergent.

Further investigations could be defined as loosen segment of DB servers logical recovery, routing inside network "cloud" improvement [3], such as multi-path routing.

Reference

[1] Добуш Ю.Д. Захист від несанкціонованого доступу до структурованих кабельних систем з використанням технології Power Over Ethernet / Ю.Д. Добуш // Збірник наукових праць «Спеціальні телекомунікаційні системи та захист інформації». - Вип. №2(18).- К.: 2010. – С. 122-125.

[2] Добуш Ю.Д. Підхід до оцінки ефективності захищеної мультисервісної мережної системи передавання / [Ю.Д. Добуш, М.М. Климаш] // Матеріали 4-ої Міжнародної науково-технічної конференції «Проблеми телекомунікацій-2010» (ПТ-10): Збірник тез. – К.: НТУУ «КПІ», 2010, – С.31-32.

[3] Demydov I., Kryvinska N., Strauss C., Klymash M., Ivanochko I. Enterprise Distributed Service Platforms - an Approach to the Architecture and Topology // Emerging Research and Projects Applications Symposium (ERPAS 2009), in conjunction with 7th International Conference on Advances in Mobile Computing and Multimedia (MoMM2009), 14-16 December 2009, Kuala Lumpur, Malaysia, ACM ISBN: 978-1-60558-659-5 (electronic), pp. 417-421.