Adapting and accelerating the Stream Cipher Algorithm "RC4" using "Ultra Gridsec" and "HIMAN" and use it to secure "HIMAN" Data

Hisham A. Kholidy¹  
 hitcham_dev@yahoo.com

Khaled S. Alghathbar²  
 kalghathbar@ksu.edu.sa

¹ Center of Excellence in Info Assurance, King Saud University, Riyadh, Saudi Arabia
² Faculty of Computers & Information, Fayoum University, Fayoum, Egypt.

Abstract

Masquerade attacks pose a serious threat for cloud system due to the massive amount of resource of these systems. Lack of datasets for cloud computing hinders the building of efficient intrusion detection of these attacks. Current dataset cannot be used due to the heterogeneity of user requirements, the distinct operating systems installed in the VMs, and the data size of Cloud systems. This paper presents a Cloud Intrusion Detection Dataset (CIDD) that is the first one for cloud systems and that consists of both knowledge and behavior based audit data collected from both UNIX and Windows users. With respect to current datasets, CIDD has real instances of host and network based attacks and masquerades, and provides complete diverse audit parameters to build efficient detection techniques. The final statistic tables for each user are built by Log Analyzer and Correlator System (LACS) that parses and analyzes user’s binary log files, and correlates audits data according to user IP address(es) and audit time. We describe in details the components and the architecture of LACS and CIDD, and the attacks distribution in CIDD. Nowadays, a lot of researchers did their best to accelerate the cryptographic algorithms and develop high performance cryptographic schemes by using approaches such as the use of high end computing hardware. Grid computing is one of the most powerful techniques that can achieve a high acceleration for cryptographic algorithms, also it is known that security attributes are pretty difficult to meet but security becomes even a bigger challenge when talking about Grid Computing. So the main focus of this paper is the acceleration of stream cipher algorithm "RC4" using grid technology and also providing secure communication between elements of the Grid system by encrypting data passes between them using the new accelerated RC4 Scheme without affecting the performance of the grid middleware, comparable to the actual execution time. So we will cover two points. First, accelerating RC4 encryption algorithm using our developed Grid Security Scheme "ULTRA GRIDSEC" and our developed "HIMAN" middleware and show that RC4 will be accelerated by about 873.52% comparable to that accelerated by "GRIDCRYPT" Scheme that applied by "Alchemi" middleware developed by Melbourne University. Second, the use of the accelerated RC4 scheme to secure communication between elements of "HIMAN", taking into consideration that the stream ciphering algorithms like RC4 are the most suitable encryption algorithms for applying inside "HIMAN" as we will show.

Keywords: "Ultra Gridsec", HIMAN, Security Scheme, Accelerated RC4, Stream Cipher, GridCrypt, Alchemi

References


A Hierarchical Intrusion Detection System for Clouds: Design and Evaluation

Hisham A. Kholidy ¹²³ Fabrizio Baiardi ² Salim Hariri ¹
hkholiday@ece.arizona.edu, baiardi@di.unipi.it hariri@ece.arizona.edu
hisham_dev@yahoo.com

Esraa M. Elhariri ¹³ Ahmed M. Yousof ¹ Sahar A. Shehata ¹
esraaelhariri@email.arizona.edu amyousof@email.arizona.edu saharabdelfattah@email.arizona.edu

¹ NSF Cloud and Autonomic Computing Center, College of Electrical and Computer Engineering, University of Arizona, USA.
² Dipartimento di Informatica, Università di Pisa, Pisa, Italy
³ Faculty of Computers and Information, Fayoum University, Fayoum, Egypt

Abstract

Security and availability are critical for cloud environments because their massive amount of resources simplifies several attacks to cloud services. This paper introduces a distributed deployment and a centralized one for our Cloud intrusion detection framework, CIDS-VERT. After describing the architectures and the components of the two deployments it describes the experimental results that confirm that the deployments overcome some limitation of current IDSs to detect host, network and DDoS attacks. Lastly, we discuss the integration and the correlation of the host and network IDSs alerts to build a summarized attack report.

Keywords: Cloud Computing, Security, Intrusion Detection, Attacks, DDoS.


References


[12] Abooasaleh Mohammad Sharifi, Saeed K. Amirgholipour1, Mehdi Alirezanejad2, Baharak Shakeri Aski, and Mohammad Ghiami "Availability challenge of cloud system under DDoS attack", Indian Journal of Science and Technology, Vol. 5 No. 6 (June 2012) ISSN: 0974- 6846


ULTRA GRIDSEC: Peer-to-Peer Computational Grid Middleware Security
Using High Performance Symmetric Key Cryptography

Mostafa-Sami M. Mostafa ¹  Safia.H.Deif ²  Hisham A. Kholidy ¹
Mostafa.sami@gmail.com  shdeif@yahoo.com  hisham_dev@yahoo.com

¹ Computer Science Department, Faculty of Computers and Information, Helwan University, Cairo, Egypt
² Computers and Systems Department, National Telecommunication Institute, Cairo, Egypt

Abstract

"ULTRA GRIDSEC" is a high-performance symmetric key cryptography scheme used to secure data passes inside Peer-to-Peer Computational Grid Middleware that we are developing now[1]. This schema is used to accelerate the performance of Triple data encryption standards (TDES) by about 439.7% and this percentage value is changed according to machine capabilities, also it enhances the security of encrypted TDES files. An analysis and comparison of this scheme and its performance is presented in this paper.

Keywords: Cryptography, Security, Grid computing, parallel computation.


References
Enhanced "ULTRA GRIDSEC": Enhancing High Performance Symmetric Key Cryptography Schema Using Pure Peer To Peer Computational Grid Middleware (HIMAN)

Hisham A. Kholidy ¹ Abdulrahman.A.Azab ² Safia.H.Deif ³

¹ Center of Excellence in Information Assurance, King Saud University, Riyadh, Saudi Arabia
² Dept. of Computer Science, University of Stavanger
³ Computers and Systems Department, National Telecommunication Institute, Cairo, Egypt

Abstract

"ULTRA GRIDSEC" is a high Performance Symmetric Key Cryptography Schema used to increase the performance of symmetric key encryption algorithms like DES and TDES by decreasing their execution time and increasing their security by using compression and multithreading techniques and other enhancement points. In this paper we enhancing the performance of a "ULTRA GRIDSEC" by using a pure Peer-to-Peer Computational Grid Middleware called "HIMAN" that we developed before. "ULTRA GRIDSEC" Performance accelerated by about 254.8% when it was applied as an application for "HIMAN" middleware for file with size 55MB and 1MB Block Size, and accelerated by 431.2% for file with size 110MB and 10MB Block Size so every time the size of file is large and choosing the suitable block size and suitable number of threads this can cause a great acceleration for the schema performance regarding to machines capabilities of the running middleware. After that we compared the performance of the Enhanced "ULTRA GRIDSEC" with a developed schema called "GRIDCRYPT" developed by Melbourne University in Australia and run over their middleware called Alchemi, so for file with size 55MB and 1MB Block Size and using 4 workers, "ULTRA GRIDSEC" Performance is faster by about 445.37% than the "GRIDCRYPT" Schema, and for file with size 110MB and 10MB Block Size and using 4 workers, "ULTRA GRIDSEC" Performance is faster by about 708.69% than the "GRIDCRYPT" Schema. An analysis and results of this schema and comparison of this scheme performance with another existing schema are presented in this paper.

Keywords: Cryptography, Security, Grid computing, parallel computation. ULTRA GRIDSEC, High Performance, Symmetric Key Cryptography, Security Schema, Pure P2P, Computational Grid Middleware


References


An Adaptive Decentralized Scheduling Mechanism for Peer-to-Peer Desktop Grids

Abdulrahman.A.Azab ¹  Hisham A. Kholidy ²
abdulrahman.azab@uis.no  hisham_dev@yahoo.com

¹ Dept. of Computer Science, University of Stavanger, Norway
² Computer Science Department, Hurimla Community College, King Saud University, Saudi Arabia

Abstract

P2P Desktop Grid has recently been an attractive computing paradigm for high throughput applications. Desktop Grid computing is complicated by heterogeneous capabilities, failures, volatility, and lack of trust because it is based on desktop computers. One of the important challenges of P2P desktop Grid computing is the development of scheduling mechanisms that adapt to such a dynamic computing environment. This paper proposes an adaptive decentralized scheduling mechanism in which matchmaking is performed between resource requirements of outstanding tasks and resource capabilities of available workers. The matchmaking approach is based on fuzzy logic. Experimental results show that, implementing the proposed fuzzy matchmaking based scheduling mechanism maximized the resource utilization of executing workers without exceeding the maximum execution time of the task.

Keywords: Scheduling Mechanism, fuzzy logic, P2P desktop Grid computing.


References

A New Accelerated RC4 Scheme using "Ultra Gridsec" and "HIMAN" and use this Scheme to secure "HIMAN" Data.

Hisham A. Kholidy¹
hisham_dev@yahoo.com

Khaled S. Alghathbar²
kalgathbar@ksu.edu.sa

¹ Center of Excellence in Info Assurance, King Saud University, Riyadh, Saudi Arabia
² Faculty of Computers & Information, Fayoum University, Fayoum, Egypt.

Abstract

P2P Desktop Grid has recently been an attractive computing paradigm for high throughput applications. Desktop Grid computing is complicated by heterogeneous capabilities, failures, volatility, and lack of trust because it is based on desktop computers. One of the important challenges of P2P desktop Grid computing is the development of scheduling mechanisms that adapt to such a dynamic computing environment. This paper proposes an adaptive decentralized scheduling mechanism in which matchmaking is performed between resource requirements of outstanding tasks and resource capabilities of available workers. The matchmaking approach is based on fuzzy logic. Experimental results show that, implementing the proposed fuzzy matchmaking based scheduling mechanism maximized the resource utilization of executing workers without exceeding the maximum execution time of the task.

Keywords: Scheduling Mechanism, fuzzy logic, P2P desktop Grid computing.

Published In: IEEE Library: The Fifth International conference on Information Assurance and Security (IAS09),

References

HIMAN-GP: A Grid Engine Portal for controlling access to HIMAN Grid Middleware with performance evaluation using processes algebra

Department of Computer Science
Pisa University, I-56126 Pisa, Italy
hkholidy@di.unipi.it, hisham_dev@yahoo.com

Abstract

Grid portal is a secure web environment where user can monitor and execute grid applications, access grid resources, services, and collaborate with other users. A grid portal allows an organization to have a single URL that enables users to gain browser-based access to applications and any customized information in a virtualized, unified and secure way. The main requirement for this grid portal is to be user friendly where it shields the technical and complexity a ways from the users, as the user may does not have any background about technical points inside the grid computing environment like the heterogeneity of operating systems, hardwares, policies and so on. In this paper we propose a new web based grid portal called "HIMAN-GP" that controls access to our previous developed "HIMAN" grid middleware and adapts completely to the functionality of HIM AN, which does not have any user friendly portal to submit its tasks. We focus in this paper on two points: first is the architecture and services of HIMAN-GP, second is evaluating the performance and workload of HIMAN-GP using a performance evaluation process algebra language called "PEPA".

Keywords: Scheduling Mechanism, fuzzy logic, P2P desktop Grid computing.


References


A Study for Access Control Flow Analysis with a Proposed Job Analyzer Component based on Stack Inspection Methodology

Hisham A. Kholidy
hisham_dev@yahoo.com

Department of Computer Science
Pisa University, I-56126 Pisa, Italy
hkholidy@di.unipi.it, hisham_dev@yahoo.com

Abstract

Security problems arise in software systems are very challenging. Using program analysis techniques and some language based security rules can help in enforcing application-level security through control access to program resources and verification of control flow of the information inside the program based on some security properties. This paper presents a new job analyzer component for an intrusion detection system which works inside our developed computational grid system called “HIMAN” to analyze access required by a certain submitted task to the grid resources. This paper consists of three parts. First part is a survey for the previous work for access control, information flow security analyses, and the stack inspection methodology. Second part is a representation for a static analysis study for enhancing the stack inspection methodology in order to optimize the program complexity. Finally, the third part explains how to use the access control flow analysis based on the enhanced stack inspection methodology described in this paper to develop the new job analyzer component.


References

[15] Privileged Operations and their permissions:  
msdn.microsoft.com/enus/library/ff649312.aspx#paght000017_privilegedoperation
Towards Developing an Arabic Word Alignment Annotation Tool with some Arabic Alignment Guidelines

Hisham A. Kholidy
Department of Computer Science
hkholidy@di.unipi.it,
hisham_dev@yahoo.com

N. Chatterjee
Department of Computer Science
Pisa University, I-56126 Pisa, Italy
niladri@di.unipi.it
niladri.iitd@gmail.com

Abstract

Word Alignment is an important supporting task for different NLP applications like training of machine translation systems, translation lexicon induction, word sense discovery, word sense disambiguation, information extraction and the cross-lingual projection of linguistic information. In this paper we study the main rules and guidelines required to build an aligner tool for Arabic language which should help in correcting most of alignment errors. These errors are identified by considering the outputs of some already existing aligner annotation tools.

Keywords: Word Alignment; Annotations; Arabic Corpus Analysis; Arabic Alignment tool

Published In: IEEE Library: The 2010 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp 778-783, Cairo, Egypt

References

Abstract

By impersonating legitimate users, intruders can use the abundant resources of cloud computing environments. This paper develops a framework for "CIDS" a cloud based intrusion detection system, to solve the deficiencies of current IDSs. CIDS also provides a component to summarize the alerts and inform the cloud administrator. CIDS architecture is scalable and elastic with no central coordinator. This paper describes the components, architecture, detection models, and advantages of CIDS.

Keywords: cloud computing, security, intrusion detection, attacks, masquerade.

Published In: IEEE Library: The 9th International Conf. on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA, 2012

References


A Cloud Intrusion Detection Dataset for Cloud Computing and Masquerade Attacks

Hisham A. Kholidy
Department of Computer Science
hkholiday@di.unipi.it,
hisham_dev@yahoo.com

Fabrizio Baiardi
Department of Computer Science
Pisa University, I-56126 Pisa, Italy
biardi@di.unipi.it

Abstract

Masquerade attacks pose a serious threat for cloud system due to the massive amount of resource of these systems. Lack of datasets for cloud computing hinders the building of efficient intrusion detection of these attacks. Current dataset cannot be used due to the heterogeneity of user requirements, the distinct operating systems installed in the VMs, and the data size of Cloud systems. This paper presents a Cloud Intrusion Detection Dataset (CIDD) that is the first one for cloud systems and that consists of both knowledge and behavior based audit data collected from both UNIX and Windows users. With respect to current datasets, CIDD has real instances of host and network based attacks and masquerades, and provides complete diverse audit parameters to build efficient detection techniques. The final statistic tables for each user are built by Log Analyzer and Correlator System (LACS) that parses and analyzes user’s binary log files, and correlates audits data according to user IP address(es) and audit time. We describe in details the components and the architecture of LACS and CIDD, and the attacks distribution in CIDD.

Keywords: attacks, masquerade, dataset, cloud computing, security, intrusion detection

Published In: IEEE Library: The 9th International Conf. on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA, 2012

References