MODELLING APPROACHES OF PERFORMANCE EVALUATION OF HIGH QoS OF KERBEROS SERVER WITH DYNAMICALLY RENEWING KEYS UNDER PSEUDO CONDITIONS

Yoney K. EVER [1] Eser GEMIKONAKLI[2] Kamil DIMILILER [3]
[1] Software Engineering Department, Near East University, Nicosia,
North Cyprus, Mersin 10 Turkey
Email: yoneykirsal.ever@neu.edu.tr

[2] Graduate School of Applied Sciences, University of Kyrenia, Girne, Mersin 10 Turkey
E-mail: eser.gemikonakli@kyrenia.edu.tr

[3] Electrical & Electronic Engineering Department, Near East University, Nicosia,
North Cyprus, Mersin 10 Turkey
Email: kamil.dimililer@neu.edu.tr

Abstract: In literature, some existing studies suggested different proposed approaches that interrupt temporary link/server access. Also, in order to find implications in terms of performance degradation, analytical models are used, as well as failures of the servers. Unlike previous studies, the failures of the servers are considered together with link/server interruptions for renewals. In this study, the authors mainly focused to develop a new framework for the existing authentication protocols by considering them in an unusual fashion. The performance degradations that may be caused by service interruptions are discussed with a new framework to model the interactions between the network and the authentication servers.

Keywords: Kerberos variance, Quality of Service, Performability modelling, Queueing analysis

Introduction

Last three decades use of networked computer system has been increased and become popular. Communication and distribution of large, confidential and classified information are also available electronically, which requires challenge to protect system, data as well as resources. The configuration of the system plays an important role in privacy and data integrity that affects the performance of the underlying networks. The system considered should have the ability to perform sufficient and legitimate access to resources, while considering the applied security resources.

Network authentication is one of the vital methods for network and information security communications. Kerberos which is based on Needham-Schroder Authentication Protocol (Needham1978) commonly used for this purpose. As stated in literature, Kerberos architecture is divided into two core elements Key Distribution Centre (KDC) and Ticket Granting Service (TGS) (Brennen2004). The KDC stores authentication information and uses it to securely authenticate users and services while TGS holds digital tickets to identify the network clients and servers. If an attacker can gain administrative access to the KDC, he would have access to the complete resources of the Kerberos realm. A masquerading TGS (any client) can impersonate the TGS of the network (Kirsal2007b). In addition, Kerberos exhibits some other vulnerabilities widely reported in the literature (Brennen2004).

The design of the proposed protocol, combines the properties of Kerberos and Key-Exchange protocols together, which was considered in developing a specific authentication protocol as part of a previously proposed framework (Kirsal2007a). This combined approach had been proposed to shut down external access to an enterprise network for a period of time to enable the distribution of randomly generated keys (Kirsal2007b), (Schneider1998). In research (Kirsal2007b), while authentication protocol was designed, intruder is modelled as well. While the protocol was modelled, renewing keys at various intervals was considered, in order to block potential intruders. Although the intruder had been given the power to attack, the protocol was successful in preventing replay attacks (Kirsal2007b), (Kirsal2008). Security protocols in distributed systems are time-sensitive. That is to say if time of decrypting messages are increased, intruders could be blocked and prevented. In (Kirsal2008), a new protocol is proposed based on the use of timestamps to delay decryption by potential intruders. Considering the key distribution, external network access is restricted for short time intervals (Kirsal2007b), and (Kirsal2008). This affects the performance of the network. For this purpose, an analytical model has been developed to evaluate the

performability of the proposed approach (Kirsal2007b). While key distribution times depend on network characteristics such as size, and speed, the intervals between key renewals can be determined by the mean values of decryption times.

Related Works

In this section, frequent key renewal protocol, challenges of quality of service, and performability modelling for security protocols will be explain in detail.

Frequent Key Renewal Protocol

As stated in (Kirsal-Ever2013) the proposed protocol is based on frequent key renewal under pseudo conditions. the proposed approach was shutting-down external access to an enterprise network for a period of 140 seconds, to enable the distribution of randomly generated keys to users in a relatively secure way. Details are given in (Kirsal-Ever2013).

Quality of Service Challenges

Quality of Service (QoS) refers to the ability of a network to provide better, more predictable service. It is referred as selected network traffic over various underlying technologies, specifically wireless and mobile networks (Lowe1996), (Saravanan2006), (Song2005). Last two decades wireless and mobile networks have gained widespread popularity mainly because of their low cost and relatively high data rates. In this circumstances, issues with QoS becomes extremely important. In recent years, within the use of a wireless communication system, seamless time sensitive movement of audio and video are demanded by enterprises and users. However, interruptions may be caused because of implemented security mechanisms, which can cause degradation of performance for the traffic.

In addition, as stated in (Hua2004), interruptions in wireless and mobile systems cause the packet loss, latency, congestion and jitter, which are important QoS challenges. Latency is the time delay occurred in speech by the end-to-end user communication system. The lower the latency, the better the QoS (Balsamo2003), (Baghaei2004). In order to increase QoS in terms of packet losses, less interruptions, dedicated bandwidth and controlled jitter should be improved. Researches on good QoS showed that greater levels of interruption introduce more delay and require lower network latency (Lowe1996), (Hua2004).

The major constraint is end-to-end interruption. It requires the delay to be reduced through a packet network. To support traffic reliably and enhance the QoS in WLAN, a network must therefore be able to provide packet forwarding latency, jitter, guaranteed network bandwidth and capacity for communication during periods of network congestion (Kirsal-Ever2013).

Necessity of Modelling Security Protocols for Performability Modelling

Implemented security mechanisms in wireless communication systems are one of the main reason of service interruptions (Ever2009). The wireless variants of existing protocols may prefer to shut the communication while the critical key exchange processes are taking place. That would introduce significant delays, and increased number of request awaiting for authentication.

System or server interruptions depend on the system's nature and can have different impacts on the system performance. The system may not support the ongoing process or the packet efficiently due to the interruptions hence performance may degrade. In order to overcome this problem, availability and performance of the system should be considered together (Jiang2005). In (Trivedi1994) a unified performability and reliability analysis by using Markov Reward model (MRM) is presented. In (Kirsal-Ever2013) existing performability evaluation methods are considered for evaluation of security mechanisms from a performance point of view. A new framework has also been discussed for modelling the interactions between the network and the authentication servers.

Framework

The arrivals of jobs are assumed to be independent and follow Poisson distribution with rate λ. The service times of jobs are distributed exponentially with mean $1/\mu$. The Kerberos server considered can serve jobs only during its operative periods, which means that the key distribution is being taken place (the system is not shut) and the server

is active during this process. The Kerberos server may suffer from failures and inter failure times are distributed exponentially with mean 1/ξ. At the end of this period, the server breaks down and requires an exponentially distributed repair time with mean 1/η. The distribution of time intervals between shutdowns are assumed to be exponentially distributed with given mean value 1/δ. When the system is shut, the server does not provide service to incoming request for an exponentially key distribution time which is given by 1/φ. This system can be modelled as follows:

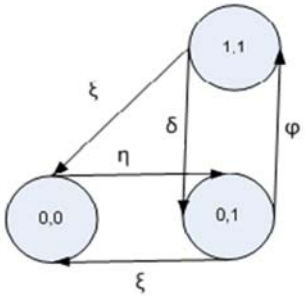

Figure 1. State diagram for availability of standalone Kerberos authentication server

The state (0, 0) denotes the event that the system is shut and the server is broken. In the state (0, 1) the server is not broken and the system is shut. Finally, the state (1, 1) represents the state where the server becomes operative since the system is not shut and the server is active. In case the server is broken in this stage, there is a direct transition from state (1, 1) to the state (0, 0). Therefore, it is assumed that the system is shut and key distribution does not take place while the server is nonfunctional.

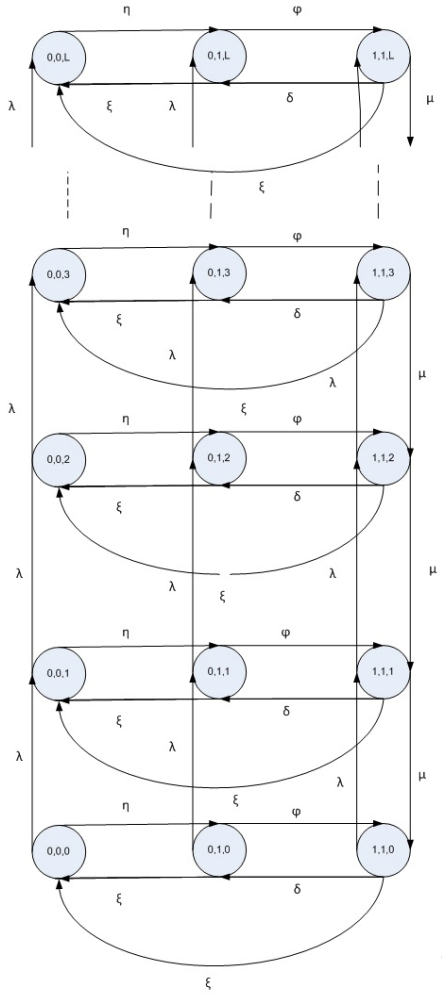

Figure 2. The state transition diagram for the performance and availability model of the system

The system state can be represented by (i, j, k) where i is the system status, j is the number of active server and k

is the number of jobs in the system. Please note that i and j can be maximum 1 since there is only one server considered for the proposed model. Therefore, in Figure 2, as long as jobs keep on arriving to the system, the system state changes one state upward until it reaches maximum number of jobs (L) in the system. The upward transition further than the state (i, j, k) is not possible since the jobs are blocked because of the limitation of L, where $k \leq L$. There is forward lateral transition from state (i, j, k) to the state (i, j+1, k) when the server is repaired. Once the system generates key, there is also forward transition from the state (i, j, k) to the state (i+1, j, k). There are two possible backward lateral transition from the state (i+1, j+1, k) to the state (i+1,j,k) and (i, j, k), when the system is shut and the server is broken respectively. Another backward lateral transition can be possible from the sate (i, j+1, k) to the state (i, j, k) in case the server is broken. Finally, when the server is operative, one job is served with a downward transition from the state (i+1, j+1, k+1) to (i+1, j+1, k).

The two dimensional process considered in (Kirsal-Ever2013) can be used for the Spectral Expansion solution method with the matrices A, B and also C as given below. Please note that the matrix A represents the lateral, the matrix B upward and also the matrix C downward transitions.

$$A = A_j = \begin{bmatrix} 0 & \eta & 0 \\ \xi & 0 & \varphi \\ \xi & \delta & 0 \end{bmatrix} \qquad B = B_j = \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix} \qquad C_0 = (0),\ C = C_j = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \mu \end{bmatrix}$$

Conclusions and Future Work

This paper is concerned with a modelling approach for performability evaluation of Kerberos servers which dynamically renew keys under pseudo-secure conditions as well as security variants over Kerberos authentication protocol as an example to service interruptions in wireless communication systems. As stated earlier, during key distribution, external access to the network is not allowed. The access restrictions happen for short intervals (Kirsal2007), (Kirsal2008). However, any link shut-down costs the network in terms of performance degradation. Therefore, it is essential to evaluate the impact of the proposed approach on system performance. The proposed approach in (Ever2009) also involves temporary interruption to link/server access where it has implications in terms of QoS degradation. Discussions on performance and availability evaluation of some security measures are provided.

Hence in order to enhanced QoS, the existing performance and availability modelling techniques used in the literature can be adapted to modelling of various security protocols considering the server behaviour as well as the characteristics of the networks. In order to evaluate the cost in terms of the degradation of system performance, an analytical method is used. Unlike the previous studies, the server failures are considered as well. Therefore, the approach presented in this study provides more realistic performability measures.

The model developed is highly flexible and it can be used for systems with various failure, repair, and renewal times and times between interruptions. The method can be extended for multiple Kerberos servers and for systems with backup servers especially for the KDC.

References

[1] Balsamo, S., Persone, V. D. N., & Inverardi, P. (2003). *A Review on Queueing Network Models with Finite Capacity Queues for Software Architectures Performance Prediction*. Performance Evaluation. 51(4), pp. 269-288.

[2] Chakka, R. (1998). *Spectral Expansion Solution for Some Finite Capacity Queues*, Annals of Operations Research. 79, pp. 27-44.

[3] Ever, E., Kirsal, Y. & Gemikonakli, O. (2009). *Performability Modelling of a Kerberos Server with Frequent Key Renewal under Pseudo-Secure Conditions for Increased Security*. IEEE International Conference on the Current Trends in Information Technology (CTIT). Dubai Women College, pp. 91 96.

[4] Baghaei, N. & Hunt, R. (2004). *Security Performance of Loaded IEEE 802.11b Wireless Networks*. Computer Communications, Elsevier, UK. 27(17), pp. 1746-1756.

[5] Brennen, V. A. (2004). "Kerberos Infrastructure HOW TO", CryptNET, Guerrilla Technoogy Development.

[6] Chakka, R. & Mitrani, I. (1994). *Heterogeneous Multiprocessor Systems with Breakdowns: Performance and Optimal Repair Strategies*. Theoretical Computer Science. l25, pp. 91-109.

[7] Ever, E., Kirsal, Y. & Gemikonakli, O. (2009), *Performability Modelling of Handoff in Wireless Cellular Networks and the Exact Solution of System Models with Service Rates Dependent on Numbers of Originating and Handoff Calls*. IEEE Proceedings of International Conference on Computational Intelligence, Modelling and Simulation (CSSim 2009), pp. 282-287.

[8] Ever, E., Gemikonakli, O., Kocyigit, A. & Gemikonakli, E. (2013). *A Hybrid Approach to Minimize State*

Space Explosion Problem for the Solution of Two Stage Tandem Queues. Journal of Network and Computer Applications. 36, pp.908-926.

[9] Jiang, Y., Lin, C., Shen, X., & Shi, M. (2005). *Mutual Authentication and Key Exchange Protocols with Anonymity Property for Roaming Services.* NETWORKING, pp. 114-125.

[10] Kirsal, Y. & Gemikonakli, O. (2007). *An Authentication Protocol to Address the Problem of the Trusted 3rd Party Authentication Protocols*. Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics, (CISSE 2006), pp. 523-526.

[11] Kirsal, Y. & Gemikonakli, O. (2007). *Frequent Key Renewal Under Pseudo- Secure Conditions for Increased Security in Kerberos Authentication and its Impact on System Performability*. Proceedings of the 3rd International Conference on Global E-Security, University of East London (UeL), 2007.

[12] Kirsal,Y. & Gemikonakli, O. (2008). *Improving Kerberos Security through the Combined Use of the Timed Authentication Protocol and Frequent Key Renewal,* 7th IEEE International Conference on Cybernetic Intelligent Systems (CIS2008), IEEE Press, pp. 153-158.

[13] Lowe, G. (1996). *Some New Attacks upon Security Protocols*. 9th IEEE Computer Security Workshops, Society Press, pp. 162-169.

[14] Mitrani, I. (2005). *Approximate Solutions for Heavily Loaded Markov- Modulated Queues*. Performance Evaluation, vol.62 (1-4), pp. 117-131.

[15] Needham, R. M. & Schroeder, M. D. (1978). *Using Encryption for Authentication in Large Networks of Computer*. Commun. ACM, ACM Press, vol. 21, pp. 993-999.

[16] Schneider, S. (1998). *Verifying Authentication Protocols in CSP*. IEEE Trans. Sofw. Eng., IEEE Press, vol. 24, pp. 741-758.

[17] Trivedi, K. S., Malhotra, M. & Fricks, R. M. (1994). *Markov reward approach to performability and reliability analysis*, pages 7-11.

[18] Mitrani, I. (2001). *Queues with Breakdowns, Performability Modelling: Techniques and Tools*, Wiley, Chichester.

[19] Trivedi, K. S., Dharmaraja, S. & Ma, X. (2003). *Performability modelling of wireless communication systems*. International Journal of Communication Systems, vol 16, pp. 561-577.

[20] Gemikonakli, O., Mapp, G., Thakker, D., & Ever, E. (2006). *Modelling and performability analysis of network memory servers*, Annual Simulation Symposium, pp.127-134.

[21] Gemikonakli, O., Mapp, G., Ever, E., & Thakker, D. (2007). *Modelling network memory servers with parallel processors, break-downs and repairs*, Annual Simulation Symposium, pp. 11-20.

[22] Kirsal, Y., & Gemikonakli, O. (2009). *Performability Modelling of Handoff in Wireless Cellular Networks with Channel Failures and Recovery*, In IEEE Proceedings of 11th International Conference on Computer Modelling and Simulation (UKSim 2009), pp. 544-547.

[23] Kirsal, Y., Ever, E., Gemikonakli O. & Mapp G. (2011). *Critical Review of Analytical Modelling Approaches for Performability Evaluation of the Handover Phenomena in Mobile Communication Systems.,* The Proceeding of IEEE 11th International Conference on Computer and Information Technology, 2th International Workshop on Dependable Service-Oriented and Cloud computing (DSOC 2011), pp. 132-137.

[24] Kirsal, Y., Gemikonakli, O., Ever, E. & Mapp, G. (2012). *Performance Analysis of Handovers to Provide a Framework for Vertical Handover Policy Management in Heterogeneous Environments*, In 45th Annual Simulation Symposium, (ANSS'12), Orlando, FL, USA, pp. 1-8.

[25] Gowrishankar, S. G.N., & Satyanarayana P.S. (2009). *Analytic Performability Model of Vertical Handoff in Wireless Networks,* Journal of Computer Science, 5(6), pp. 445-450.

[26] Trivedi, K.S. & Ma X. (2002). *Performability Analysis of Wireless Cellular Networks,* Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2002).

[27] Shensheng, T. & Wei, L. (2005). *Performance Analysis of the 3G Network with Complementary WLAN*, Global Telecommunications Conference GLOBECOM '05, vol. 5, pp. 2636-2641.

[28] W. Xia, and, L. Shen (2007). *Modeling and Analysis of Handoffs in Cellular and WLAN Integration*. IEEE International Conference on Communications, ICC '07I, pp. 385-391.

[29] Saravanan, I., Sivaradje, G. & Dananjayan, P. (2006). *QoS provisioning for cellular/WLAN interworking, Wireless and Optical Communications Networks*, 2006 IFIP International Conference, pp. 50-55.

[30] Song, W., Jiang, H., Zhuang, W. & Shen, X. (2005). *Resource Management for QoS Support in Cellular/WLAN Interworking*, IEEE Network, 19(5), pp.12-18.

[31] Hua, Z., Li, M., Chlamtac, I., & Prabhakaran, B. (2004). *A Survey of Quality of Service In IEEE 802.11 Networks*, In IEEE Wireless Communications Journals, 11(4), pp. 6-14.

[32] Kirsal-Ever, Y., Yonal Kirsal, Alberto Polzonetti, Leonardo Mostarda, Clifford Sule, Purav Shah, Enver Ever (2013), "Challenges of Kerberos Variance with High QoS Expectations", *International Conference on Security and Management (SAM), World Congress in Computer Science, Computer Engineering, and Applied Computing (WORLDCOMP)*, Las Vegas, USA.