Int. J. Communications, Network and System Sciences, 2016, 9, 603-612
http://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

Extension of Kerberos with X.509 and Integration of Elliptic Curve Cryptography in Authentication

Murat Akkaya

Department of Management Information Systems, Girne American University, Kyrenia, Cyprus
Email: muratakkaya@gau.edu.tr

How to cite this paper: Akkaya, M. (2016) Extension of Kerberos with X.509 and Integration of Elliptic Curve Cryptography in Authentication. *Int. J. Communications, Network and System Sciences*, **9**, 603-612.
http://dx.doi.org/10.4236/ijcns.2016.912046

Received: August 20, 2016
Accepted: December 27, 2016
Published: December 30, 2016

Abstract

Kerberos is one of the solutions for network security problems since it provides strong secret key cryptography over the insecure networks. Through the Kerberos authentication protocol, a client can prove its identity to a server (and vice versa) across an insecure network connection such as on Internet. In this comparative research paper, the Kerberos authentication protocol is extended and strengthened using x.509 with the integration of newer authentication system which is compared with previous authentication systems. In addition to this, RSA encryption mechanism used to provide authentication and security for the most communication systems replaced with Elliptic Curve Cryptography (ECC) encryption in Kerberos during authentication progress through simulation to expose possible efficient alternatives for key generation and to enhance security.

Keywords

Kerberos, Network Security, Authentication, Encryption, X.509, ECC, RSA, Simulation

1. Introduction

Proper authentication is an important aspect of security systems, even in networking. Hence, the Kerberos [1] was developed by Massachusetts Institute of Technology to provide a stronger authentication for both client and server applications irrespective of the communication medium used (secured or not). The protocol can be integrated with an already existing network without the need for additional protocols to secure communication over that network because the Kerberos can use the already existing username and password for users, to perform its authentication processes [2] [3].

In the version 4 of Kerberos, the DES [3] [4] algorithm was used in authentication but the limitations of such methods have led to the Kerberos version 5 which makes provision for any other kind of authentication algorithm to be integrated for better authentication, such as the RSA. Extensions also exist for the Kerberos that allow for this, such as PKINIT [4] [5]. The Kerberos protocol requires an authentication server on which to run as a centralized authentication service. At the host computer running the Kerberos, authentication server is a database of users and their private keys, as well as hosts and their private keys too. Both hosts and users (principals) have unique names and name-type. The x.509 is used to encrypt the principals' names in the database. Currently, there exist several variations of the Kerberos protocol, but the underlying procedure of a classic Kerberos protocol remains the same: client requests the authentication server to confirm the identity of the server; authentication server encrypts server-generated ID + temporary encryption key (session key) using the client's key and relays it back to the client; client encrypts its ticket and the session key using the server's key and transmits it back to the server; authentication server uses this to authenticate client, then to authenticate the server finally. This is a crypto analysis of the Kerberos and x.509 authentication algorithms and research into improving these protocols by uncovering flaws and weak points in the protocols. Work done so far will be reviewed to find unaddressed issues or concerns about the Kerberos and x.509 authentication protocols.

2. Literature Survey

In a formal analysis of Kerberos 5, Frederick Butler *et al.* concluded that the Kerberos was actually structurally sound and took out the over simplification of the protocol in as it is able to grant or deny certain (not all) requests made by the client to the authentication server [5] [6]. Extensible Pre-Authentication in Kerberos or EPAK [6] [7] came into play in 2007 when proposing an extension that allows the Kerberos to be integrated with other authentication methods without changing the underlying workings of Kerberos itself. As the Kerberos became more widely accepted, Saber Zrelli and Yoichi Shinoda in 2007 [8] [9] suggested the Kerberos as an extensible authentication protocol for network access authentication thereby eliminating the need for extra authentication credentials from the users. In 2008, Cervesato *et al.* found a vulnerable spot in the popular PKINIT extension to Kerberos that allows an attacker (man-in-the-middle) to impersonate administrative principals [10] [11]. However, the IETF has changed the specifications of PKINIT to prevent this attack. Sung-Hyun Eum and Hyoung-Kee Choi proposed a new EAP called "EAP-Kerberos II" in 2008 which uses a ticket (key) in Kerberos and thereby increases efficiency by 55% [12] [13], and speed as the key can be downloaded rather than derived. Ahmed Alazzawe *et al.* figured a way to extract Kerberos passwords from the RC4-HMAC encryption used by Microsoft in Kerberos using a method that even reduces the time to crack a single password by about 60% with brute force [13] [14]. Eman El-Emam, Magdy Koutb, Hamdy Kelash, and Osama Farag Allah decided to make the passwords independent of the user's own password when they suggested in their paper in 2009 [14] [15] that a secret key be generated based on each profile, encrypted using Triple-Des, hashed using SHA-256, and Blum BlumShub.

Dahui Hu and Zhiguo Du tried to improve the Kerberos by using a faster RSA algorithm to counter a few mentioned problems [15], such as the speed of the RSA itself and password guessing. However, their approach is still password-based, which has its own vulnerabilities. Hossain, Alamgir *et al.* came up with the idea in 2010 of integrating the user's position in terms of coordinates during the client authentication on Kerberos, to form what they called it N-Kerberos [15] [16]. In addition to this, they modified the BAN [17] [18] logic to create N-BAN so as to reduce the chances of a reply attack by using the N-BAN to confirm the N-Kerberos. In 2011, Sufyan T. Faraj Al-Janabi & Mayada Abdul-salam Rasheed looked at implementing public-key cryptographic approach like PKINIT, PKCROSS, and PKTAPP, at different phases of the algorithm. However, there were performance issues like bottleneck [18] [19] due to this enhancement.

3. ECC vs. RSA

Since most of the communication systems requires reliable infrastructure to provide communication in different fields have used public key cryptography to secure their systems and exchange data. ECC (Elliptic Curve Cryptography) provide secure data exchange and authentication, authorization and identification features. Variety of the studies conducted in the literature contains RSA implementation for security however using 3rd party security mechanisms or algorithms like Kerberos uses requires deep research to expose possible vulnerabilities [20] [21] [22].

However this study focused on the ECC since ECC provides same level of security while providing less key size in contrast to RSA algorithm. The Key sizes of the RSA and ECC are shown and classified into 7 different categories in terms of key size and ratio on Table 1.

4. Simulation Experiment

In this section, a simulation experiment with ASIC simulation package is conducted and the performance of an application that provides encrypted communication with ECC authentication and application that provides only plain text communication is compared. The proposed application examined as how the added ECC security algorithm influences its overall performance.

Table 1. ECC vs RSA key comparison.

Category Type	ECC Key Size	RSA Key Size	Key Size Ratio
A	112	512	1:5
B	163	1024	1:6
C	192	1536	1:8
D	224	2048	1:9
E	256	3072	1:12
F	384	7680	1:20
G	512	15,360	1:30

The ASIC and FPGA are the two most common simulation package to develop ECC algorithm and simulate variety of scenarios by the researchers. The ASIC was used to develop a simulation model for implementation of ECC on Kerberos [23] [24] [25] [26] [27].

The ECC is defined as follows:

$$y_2 = x_3 + \alpha x + \beta \tag{1}$$

where x, $y \in$ GF (p), and $4\alpha_3 + 27\beta_2 \neq 0$ in the GF(p).

The calculation of a public key which is generated by the multiplication of the private key with a point G which is shown as an generator point on the curve. Figure 1 illustrates the simple ECC. In addition to this, Figure 2, Figure 3 and Figure 4 illustrate the comparison between ECC and RSA key size, key generation algorithms and digital signature algorithms.

The algebraic formula used to calculate point addition and point doubling is given as follows (Formula (2) - (5)):

$$X_3 = \lambda_2 - x_1 - x_2 \pmod{p} \tag{2}$$

$$Y_3 = \lambda(x_1 - x_3) - y_1 \pmod{p} \tag{3}$$

$$\text{When } P \neq Q,\ \lambda = (y_2 - y_1)/(x_2 - x_1) \tag{4}$$

$$\text{When } P = Q,\ \lambda = (3x_1^2 + \alpha)/2y_1 \tag{5}$$

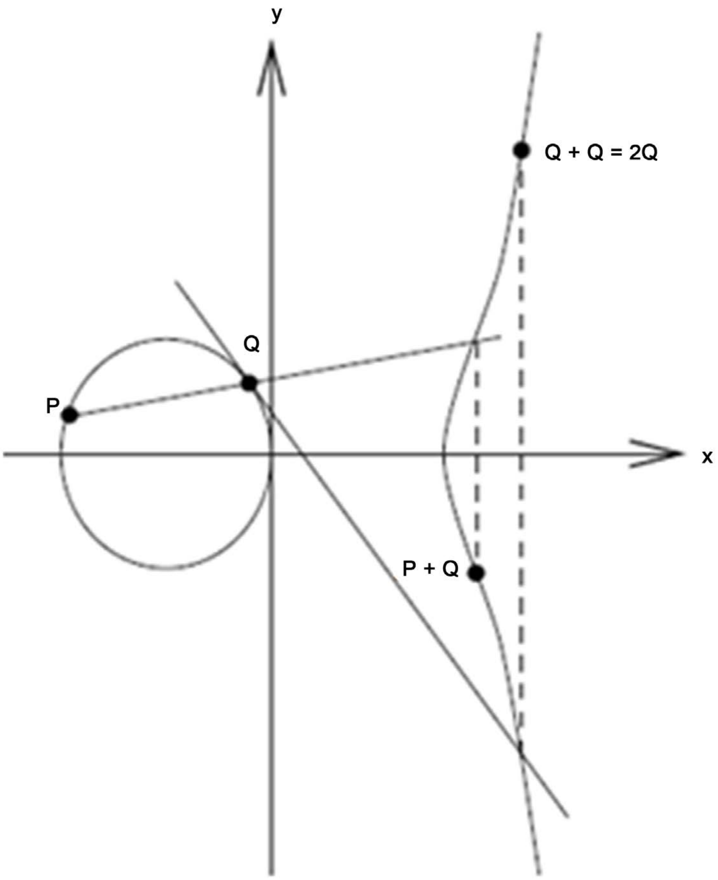

Figure 1. A simple elliptic curve.

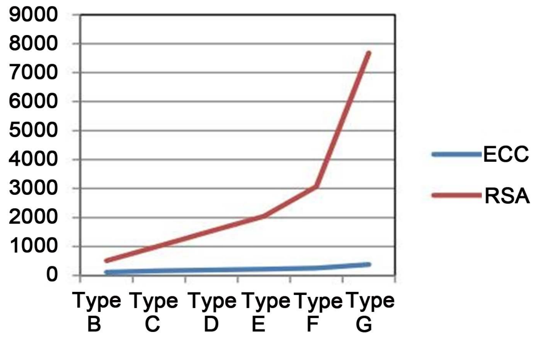

Figure 2. Key size comparison of ECC and RSA in authentication.

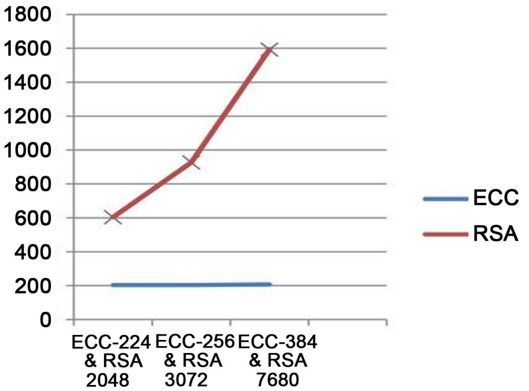

Figure 3. Comparison of key generation algorithm for ECC and RSA (ms).

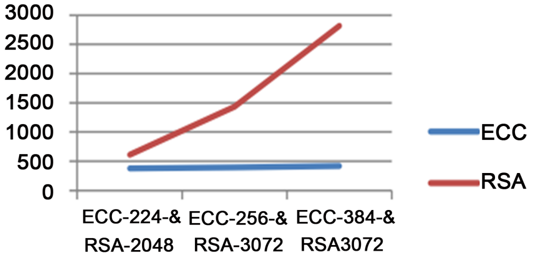

Figure 4. Comparison of digital signature algorithm for ECC and RSA.

5. Findings of DES-RSA-ECC

Much focus have been on extending the Kerberos much like the framework presented by Phillip L. Hellewell *et al.* [28] [29] [30] [31] [32] for integrating new authentication systems (such as RSA) seamlessly with Kerberos without much change to Kerberos itself thereby reducing its limitation being DES-based; support for multiple encryption types negotiable by both client and server [33] [34] [35]; support for anonymous users [34] [36] [37] [38]. Notwithstanding, there are a few potential loopholes I wish to draw attention to and request for comments. First concern is how can the authentication server itself be authenticated and this problem can be solved through concentrating to authentication as well as identification. Another question is whether the Kerberos authentication protocol able to identify an AS much like it identifies the usual principals (client and server)?, or is it impossible to impersonate an AS during a Kerberos authentication? In other words, how it is possible to make sure to trust to "trusted third party authentication server"? Further research would be required to properly analyze Kerberos and check if such vulnerability would indeed be critical or trivial, or even feasible. Second, while Kerberos is used for authentication, what happens between client and server after authentication may be susceptible to further attacks. In theory, a loophole exists such that a form of man-in-the-middle attack is possible, similar to a shoulder attack.

Hence, an attack is proposed on Kerberos to simulate an environment as follows: Assume a man-in-the-middle (MitM) trying to impersonate both the client, and the server at the same time. Also assuming our MitM has found ways to clone or impersonate the client and then simply relays the requests and replies between the legitimate client and server while keeping copies of intercepted date, whether encrypted or in plain view. Next, our MitM attacker simply waits for the legitimate server to authenticate the legitimate client and grants access to the legitimate client. At this point, the MitM cuts off the client from communication with the server and replace the client in the rest of the conversation; now our MitM attacker has access to the server and may then proceed as an authenticated client. In real life, this would be much like waiting for a user to open up a vault and then the attacker sneaks in from behind and locks the user out [25] [26] [27]. Meanwhile, the implementation of ECC on Kerberos protocol and working with combination of Kerberos with ECC provided much better results than RSA encryption. The results exposed that, the total time required to generate key for the corresponding transaction, key size and generation of digital signature required more time than ECC algorithm.

6. Comparison of the Results

Extensible Pre-Authentication in Kerberos or EPAK introduces the advantage of adding new authentication systems easily into Kerberos to increase their usability and performance without changing existing Kerberos-based security frameworks in a way that also allows complex authentication systems with slow performance can leverage Kerberos' SSO capability [39] [40]. EAP-Kerberos allows for scalability while EAP-Kerberos II uses a key in Kerberos which is transported to the client securely rather than being derived, to increase efficiency up to 55% by reducing the number of authentication messages from 18 to 8 thereby increasing its speed. RC4-HMAC used by Microsoft was found to be flawed as Kerberos passwords can be extracted from this encryption method and hence should not be used. Combining PKINIT, PKCROSS, and PKTAPP at several phases in the authentication protocol improved scalability and security but resulted in performance bottlenecks.

The corresponding simulation outcomes indicate that ECC has more practical and efficient in terms of key generation time and key size. Since Kerberos protocol serves vast number of users on the web at given point of time, this becomes a disadvantage for an algorithm which requires more time to generate a key with greater key sizes. The results indicated that signature generation and verification times are almost similar for both algorithms. Once it is considered for large number of users on the web attempts to authenticate, the ECC algorithm becomes more efficient.

7. Conclusions

In conclusion, without considering ECC in authentication progress, the Kerberos has been extended and strengthened using x.509 and with the integration of newer authentication systems. Nevertheless, communication between a once authenticated client and server may still be susceptible to a form of man-in-the-middle/shoulder attack if Kerberos isn't employed during the entire communication between client and server. That's why the deployment and use of ECC algorithm should be more beneficial in Kerberos Authentication protocol.

Hence it is highly recommended that Kerberos can be used to encrypt further communication between clients and servers in order to "guarantee that subsequent messages on the connection originate from the same principal" [41] [42].

First, it is proposed that EAP-Kerberos II is made as standard, and should also be used with the Camellia [41] [42] encryption while maintaining PKINIT. Using a faster algorithm [42], we can further encrypt and authenticate all communications between authenticated principals in order to ensure that after initial authentication, the rest of the communication remains between both legitimate client and server.

Also, further analysis is proposed on a 3-way Kerberos authentication protocol where the client and the server, and the authentication server each has to be identified as legitimate and then authorized to communicate. It is highly recommended to conduct further research on the proposed field in contrast to the necessity of security issues.

References

[1] MIT (2012) Kerberos: The Network Authentication Protocol. http://web.mit.edu/Kerberos/

[2] Zrelli, S. and Shinoda, Y. (2007) Specifying Kerberos over EAP: Towards an Integrated Network Access and Kerberos Single Sign-On Process. 21*st International Conference on Advanced Information Networking and Applications*, Niagara Falls, ON, 2007, 490-497.

[3] Rahnama, B., Sari, A. and Ghafour, M.Y. (2016) Countering RSA Vulnerabilities and Its Replacement by ECC: Elliptic Curve Cryptographic Scheme for Key Generation. In: Singh, D.G.M. and Jayanthi, M., Eds., *Network Security Attacks and Countermeasures*, Information Science Reference, Hershey, PA, 270-312.

[4] Hornquist Astrand, L. and Yu, T. (2012) Deprecate DES, RC4-HMAC-EXP, and Other Weak Cryptographic Algorithms in Kerberos. http://tools.ietf.org/html/rfc6649

[5] Sari, A. and Necat, B. (2012) Securing Mobile Ad Hoc Networks against Jamming Attacks through Unified Security Mechanism. *International Journal of Ad Hoc*, *Sensor & Ubiquitous Computing*, **3**, No. 3.

[6] Thorat, S.S., Sawant, H.K., Gaikwad, S.S. and Chavan, G.T. (2010) Comparative Study of Various PKINIT Methods Used in Advanced Kerberos. *International Journal on Computer Science and Engineering*, **2**, 2337-2344.

[7] Sari, A. and Rahnama, B. (2013) Simulation of 802.11 Physical Layer Attacks in MANET. 2013 *Fifth International Conference on Computational Intelligence*, *Communication Sys-*

tems and Networks, Madrid, 2013, 334-337. https://doi.org/10.1109/cicsyn.2013.79

[8] Butler, F., Cervesato, I., Jaggard, A.D., Scedrov, A. and Walstad, C. (2006) Formal Analysis of Kerberos 5. *Theoretical Computer Science-Automated Reasoning for Security Protocol Analysis*, **367**, 57-87.

[9] Sari, A. (2014) Security Approaches in IEEE 802.11 MANET—Performance Evaluation of USM and RAS. *International Journal of Communications, Network, and System Sciences*, **7**, 365-372.

[10] Hellewell, P.L., van der Horst, T.W. and Seamons, K.E. (2007) Extensible Pre-Authentication Kerberos. *Computer Security Applications Conference*, Miami Beach, FL, 2007, 201-210.

[11] Sari, A. (2014) Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks. *Transactions on Networks & Communications*, **2**, 1-6. https://doi.org/10.14738/tnc.25.431

[12] Cervesato, I., Jaggard, A.D., Scedrov, A., Tsay, J.-K. and Walstad, C. (2008) Breaking and Fixing Public-Key Kerberos. *Information and Computation*, **206**, 402-424. https://doi.org/10.1016/j.ic.2007.05.005

[13] Rahnama, B., Sari, A. and Makvandi, R. (2013) Countering PCIe Gen. 3 Data Transfer Rate Imperfection Using Serial Data Interconnect. 2013 *International Conference on Technological Advances in Electrical, Electronics and Computer Engineering* (*TAEECE*), Konya, 9-11 May 2013, 579-582.

[14] Eum, S.-H. and Choi, H.-K. (2008) EAP-Kerberos II: An Adaptation of Kerberos to EAP for Mutual Authentication. 8*th International Conference on ITS Telecommunications*, Phuket, 24 October 2008, 78-83.

[15] Ahmed, A., Alazzawe, A., Nawaz, A. and Wijesekera, D. (2008) Extracting Kerberos Passwords through RC4-HMAC Encryption Type Analysis. *Proceedings of the* 2008 *IEEE/ACS International Conference on Computer Systems and Applications*, Doha, 31 March-4 April 2008, 679-685.

[16] Shukla, P.K., Mishra, G.S., Girdhar, P.G., Rusia, P. and Kapoor, V. (2009) Implementation Comparison of Kerberos Passwords by RC-5 Encryption Type Analysis with RC-4 Encryption. 6*th International Conference on Information Technology*: *New Generations*, Las Vegas, 27-29 April 2009, 1581-1582.

[17] Sari, A. (2015) Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks. In: Dawson, M. Ed., *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, IGI Global, Hershey, 66-94. https://doi.org/10.4018/978-1-4666-8345-7

[18] El-Emam, E., Koutb, M., Kelash, H. and Allah, O.F. (2009) An Optimized Kerberos Authentication Protocol. *International Conference on Computer Engineering & Systems*, Cairo, 14-16 December 2009, 508-513.

[19] Yilmaz, O., Kirencigil, B.Z. and Sari, A. (2016) VAN Based Theoretical EDI Framework to Enhance Organizational Data Security for B2B Transactions and Comparison of B2B Cryptographic Application Models. *International Journal of Scientific & Engineering Research*, **7**, 1012-1020.

[20] Hu, D. and Du, Z. (2010) An Improved Kerberos Protocol Based on Fast RSA Algorithm. *IEEE International Conference on Information Theory and Information Security* (*ICITIS*), Beijing, 17-19 December 2010, 274-278.

[21] Sari, A. and Karay, M. (2015) Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks. *International Journal of Communications, Network and*

System Sciences, **8**, 567-577. https://doi.org/10.4236/ijcns.2015.813051

[22] Abdelmajid, N.T., Hossain, M.A., Shepherd, S. and Mahmoud, K. (2010) Location-Based Kerberos Authentication Protocol. *IEEE 2nd International Conference on Social Computing (SocialCom)*, Minneapolis, 20-22 August 2010, 1099-1104.

[23] Sari, A. and Rahnama, B. (2013) Addressing Security Challenges in WiMAX Environment. *Proceedings of the 6th International Conference on Security of Information and Networks*, Aksaray, November 26-28 2013, 454-456. https://doi.org/10.1145/2523514.2523586

[24] Fan, K., Li, H. and Wang, Y. (2009) Security Analysis of the Kerberos Protocol Using BAN Logic. *5th International Conference on Information Assurance and Security*, Xi'an, 18-20 August 2009, 467-470.

[25] Al-Janabi, S.T.F. and Rasheed, M.A.-S. (2011) Public-Key Cryptography Enabled Kerberos Authentication. *Developments in E-Systems Engineering (DeSE)*, Dubai, 6-8 December 2011, 209-214.

[26] Sari, A., Rahnama, B. and Caglar, E. (2014) Ultra-Fast Lithium Cell Charging for Mission Critical Applications. *Transactions on Machine Learning and Artificial Intelligence*, **2**, 11-18. https://doi.org/10.14738/tmlai.25.430

[27] Zhu, J.L., Leach, P. and Kerberos, K. (2006) Cryptosystem Negotiation Extension. Internet Engineering Task Force. http://tools.ietf.org/html/rfc4537

[28] Sari, A. (2015) Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks. *International Journal of Communications, Network and System Sciences*, **8**, 19-28. https://doi.org/10.4236/ijcns.2015.83003

[29] Zhu, H.L., Leach, P. and Anonymity, S. (2011) Support for Kerberos. Internet Engineering Task Force. http://tools.ietf.org/html/rfc6112

[30] Sari, A. (2015) A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. *Journal of Information Security*, **6**, 142-154. https://doi.org/10.4236/jis.2015.62015

[31] Neuman, C., Yu, T., Hartman, S. and Raeburn, K. (2005) The Kerberos Network Authentication Service (V5). Internet Engineering Task Force. http://tools.ietf.org/html/rfc4120

[32] Sari, A. (2015) Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite. *International Journal of Communications, Network and System Sciences*, **8**, 29-42. https://doi.org/10.4236/ijcns.2015.83004

[33] Kirencigil, B.Z., Yilmaz, O. and Sari, A. (2016) Unified 3-Tier Security Mechanism to Enhance Data Security in Mobile Wireless Networks. *International Journal of Scientific & Engineering Research*, **7**, 1001-1011.

[34] Obasuyi, G. and Sari, A. (2015) Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. *International Journal of Communications, Network and System Sciences*, **8**, 260-273. https://doi.org/10.4236/ijcns.2015.87026

[35] Certicom Research (2000) SEC 1: Elliptic Curve Cryptography.

[36] Choi, H.-K. and Han C.-K. (2008) An Adoption of Kerberos to 3G Network for Mutual Authentication: Challenges and Evaluations. *International Symposium on Performance Evaluation of Computer and Telecommunication Systems*, Edinburgh, 16-18 June 2008, 448-455.

[37] Blanchet, B., Jaggard, A.D., Scedrov, A. and Tsay, J.-K. (2008) Computationally Sound Mechanized Proofs for Basic and Public-Key Kerberos. *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security*, Tokyo, 18-20 March 2008, 87-99.

[38] Sari, A., Rahnama, B., Eweoya, I. and Agdelen, Z. (2016) Energizing the Advanced Encryp-

tion Standard (AES) for Better Performance. *International Journal of Scientific & Engineering Research*, **7**, 992-1000.

[39] Kamada, K., Sakane, S., Miyazawa, K. and Okabe, N. (2008) Design and Evaluation of a Client-Friendly Cross-Realm Framework for Kerberos 5. *IEEE 6th International Conference on Industrial Informatics*, Daejeon, 13-16 July 2008, 541-546.

[40] Ke, J., Chen, X. and Xu, G. (2008) The Improved Public Key Encryption Algorithm of Kerberos Protocol Based on Braid Groups. *4th International Conference on Wireless Communications, Networking and Mobile Computing*, Dalian, 12-14 October 2008, 1-4.

[41] Karaduman, A., Atasoy, U. and Sari, A. (2016) 21st Century's Developing Technology: "Information Communication Technologies" and "Cyber Security" (21. Yüzyılın Gelişen Teknolojisi "Bilgi İletişim Teknolojileri" ve "Siber Güvenlik"). *International Conference on Research in Education and Science* (*ICRES2016*), Bodrum, Turkey, 19-22 May 2016.

[42] Backes, M., Cervesato, I., Jaggard, A.D., Scedrov, A. and Tsay, J.-K. (2011) Cryptographically Sound Security Proofs for Basic and Public-Key Kerberos. *International Journal of Information Security*, **10**, 107-134. https://doi.org/10.1007/s10207-011-0125-6