3rd International Conference on
Research in Applied Science
06-08 November 2020
Munich, Germany

IoT Authentication and Security Challenges

Sitalakshmi Venkatraman[1], and Anthony Overmars[2]

[1] School of Engineering, Construction & Design, Melbourne Polytechnic, Victoria, Australia

[2]School of Engineering, Construction & Design, Melbourne Polytechnic, Victoria, Australia

Abstract.

Internet of things (IoT) is an emerging technology becoming integrated into our every day lives as internet enabled devices and humans are getting interconnected seamlessly. However, recent increase in cybersecurity breaches cause severe concerns about gaps in IoT security that could compromise mission critical systems with a severe impact on everyone connected in an IoT network. There is a need to study the requirements of IoT security comprehensively to identify the constraints on the new computing platform where existing security solutions cannot be applied. In this paper, we systematically identify the unique security and privacy requirements of IoT and the associated challenges. We also provide the commonly adopted IoT authentication methods and the limitations in applying such existing schemes by identifying significant security vulnerabilities and possible attacks. In addition, we consider one of the most reliable cryptography based IoT authentication mechanism and demonstrate an encryption key attack using certain properties of prime number theory. These findings provide a deeper understanding and awareness of IoT security risks. Further, our study and recommendations derived thereof open up further research towards the realisation of a more secure IoT landscape of the future.

Keywords: Internet of Things, IoT, authentication, security, encryption, crypto keys, semi-primes, key attacks

1. Introduction

The Internet of Things (IoT) is the ability of the Internet to provide everyday devices with network connectivity, allowing them to identify and communicate with each other for sending and receiving data [1][2]. Today, IoT is beyond hype as the spectrum of application domains available can be categorised under: i) medical IoT of smart hospitals, ii) municipal IoT that provide smart homes, smart cities, and smart grid, and iii) industrial IoT with connected factories, logistics and intelligent automation [3][4][5]. With such devices pervasive and having smart capabilities to collect and analyze data to automate decisions using least human interactions, any security breach could have a severe impact on the IoT ecosystem. Hence, IoT security is of growing interest, and in particular authentication is of supreme requirement. Any possible malicious attack due to a vulnerable unauthenticated device in an IoT network becomes a serious concern [6][7]. Many new devices are being manufactured with old unpatched systems and are hackable. With non-standard methods of IoT authentication of devices, there are various security risks and challenges that lead to issues in data integrity, availability, confidentiality, and trust. These pitfalls can even result in a serious damage to physical networks and businesses [8][9][10]. However, there is a lack of literature on the IoT authentication and security problems of the new computing platform with a focus that this could provide more opportunities towards developing better security solutions [11][12].

The aim of this paper is three-fold: i) Firstly, to provide an overview of the IoT security requirements and the challenges that helps to study and identify the strengths and weaknesses of contemporary IoT authentication methods; ii) Secondly, to create an awareness demonstrate the IoT authentication key attacks that helps, and iii) Thirdly, to propose practical recommendations and possible future research.

The rest of the paper is organised as follows. In Section 2, we identify the unique IoT security requirements that differentiate the security and privacy challenges of IoT from mainstream computer systems. Section 3 provides a review of the commonly adopted IoT authentication methods and their inherent limitations. In Section 4, we describe a cryptography-based encryption keys used for IoT authentication and demonstrate an attack of deciphering the key using certain proven properties of number theory. Finally we provide recommendations based on our findings in Section 5 and conclusions along with future work in Section 6.

2. IoT Security Requirements and Challenges

An IoT device being another computing device, the security issues are similar and require good management of its inherent vulnerabilities, access controls, and system updates/patching [13][14]. In addition, with limited resources available for IoT, standard computer security techniques and solutions are not applicable, and any security attack could have a high impact on millions of IoT devices connected over the Internet [15]. A compromised device could take control of the entire network posing additional risks. It could interfere with critical network devices and consumer services with serious data breaches resulting in wrong decisions that can have an adverse impact on mission critical tasks [8][16].

Recent studies show that IoT Devices are subject to more attacks due to certain contextual constraints such as non-standardised protocols, poor vendor support and system vulnerabilities resulting from open ports or buffer overflows, lack of system updates and insufficient authentication methods [9][17]. With the rise in IoT devices and related incidents, we can clearly say that it is not possible to rely on prompt vendor response to address product lifecycle support issues or system updates that need to also scale well in large environments [18]. Any delay in informing device vulnerabilities to consumers would deprive them from foreseeing possible security issues that could result in a massive malicious attack.

We identify a comprehensive list of IoT security requirements that are uniquely different as compared to traditional computer security requirements. There are challenges in satisfying each of these IoT security requirements and these are provided below:

i. Confidentiality, which can be achieved by providing access rights for only authorised users to a given resource. While such an authorisation process determines whether the authenticated identity has access to the device/data, there are no standard protocols, policies and procedures enforced for all types of devices connected in an IoT network [10][17].

ii. Authentication, which is a process of validating user credentials to verify if the data has originated from a trusted source. However, an authenticated identity could be forged, tampered, subverted, or validation functions replaced maliciously [19].

iii. Integrity, which ensures that the data received is not tampered and remains the same as the original during transmission. Any breaches in data integrity via the Internet could affect the IoT data. Passwords, IoT tokens or encryption leys could be tampered while transfer, affecting data integrity [9].

iv. Relevance, which ensures that both data and key cannot be replayed due to fraudulence. However, replay attacks and denial of service have been on the rise due to maliciousness at the IoT gateway [16].

v. Availability, which guarantees the accessibility of data when required. Network espionage and other distributed denial of service (DDoS) attacks could affect this security requirement of data availability even in the IoT landscape [20].

vi. Robustness, which ensures IoT service despite adversaries and provides normal operations despite any abnormal conditions. This requires network topology robustness against targeted attacks [18].

vii. Resiliency, which ensures the quality of service (QoS) to be maintained at an acceptable level of security even when some nodes in the IoT network are compromised [13].

viii. Energy efficiency, which is very important to consider as minimising IoT energy consumption for encryption, routing and other control overheads are required to maximise network lifetime [21][22].

ix. Assurance, which can be achieved with a system-wide threat assessment and analysis to ensure the ability to disseminate different IoT information [23].

From the above comprehensive set of key IoT security requirements, we find that a combination of different security solutions play a major role in ensuring the entire IoT security. Certain IoT security requirements of QoS such as availability, robustness and resiliency warrant a collaborative approach with other computer security solutions such as intrusion detection systems (IDS) for proactively monitoring and detecting maliciousness before any possible attack. Such solutions are quite complex and expensive for both personal IoT as well as large scale IoT adoption. However, we could consider simple and cost-effective cryptography schemes within the IoT context as the first line to address the challenges faced with IoT security requirements of confidentiality, authentication, integrity, and relevance. Cryptography is employed to protect the device access and data privacy by encrypting messages before transmitting so that only the authenticated user with the right key are able to decrypt and read the messages [25][26]. Using this method, data integrity, confidentiality, and relevance could be maintained as any message transmitted via the IoT network cannot be deciphered without the key. Each step involved in the encryption based IoT authentication methods will require identification of vulnerabilities and security needs so that such schemes can be provisioned carefully to meet all the IoT security requirements.

3. IoT Authentication Methods and Limitations

An IoT authentication method is a set of steps to accept the user credentials and validate them against a trusted authority that results in an authenticated identity [6]. This identity is then used for the authorisation mechanism in determining whether the correct access to a given IoT resource can be permitted. These authentication processes, in general, can be grouped as client and server authentication methods [27]. The type of authentication methods required very much depend on the application such as e-commerce where the server authentication may require digital certificates verified by certificate authorities (CA). Such digital signatures adopt public/private key encryption and many IoT client authentications may not use public/private key cryptography due to their resource intensive verification process and the inconveniences involved in everyday transactions [21]. In addition, the need to consider situations when the authentication methods could fail with adversarial attacks would involve considerable financial implications in large scale IoT deployments for a real-world implementation.

We identify and summarise popular authentication methods, and their limitations below:

- Device passwords - this is the most pervasive and easy to use methods. However, some passwords in digital wallets or smart cards are randomly generated and may require activation [22]. Some IoT network protocols require changing passwords for each communication [24]. Despite high adoptability, passwords could easily be lost or cracked. Further, consumers avoid using a different password for operational convenience and its overheads in maintenance.
- Client certificates - due to the trade-off between usability and security, there is no incentive for adoption of client certificates, which is a major drawback [21].

- Digital signatures - with the difficulty to safely distribute public keys and lack of Public Key Infrastructure (PKI) capabilities with most devices, digital signatures are not practically pervasive [27].
- Biometrics - a unique authenticated identity tied to the individual's features has an advantage of uniqueness. However, the drawbacks vary with the method adopted. Biometrics are quite invasive, tamper-prone and can even be replayed or become non-permanent with physical or biological changes. Certain feature recognition requires complex computations that may otherwise lead to high false positives [28].
- Web-based - due to long active connection requirement that is a limitation with low power IoT devices, web-based popular authentication methods may not be suitable for IoT [12][15].
- Cryptography - public/private key cryptography require expensive computations and server overload. However, cryptographic hashes and authentication tokens are lightweight and portable techniques more suitable for IoT authentication [21][26].

The abovementioned limitations in IoT authentication and lack of security expertise of device developers have resulted in the proliferation of weak authentication schemes [22]. In addition, due to the requirement of minimum user involvement in the scalability of IoT deployments, simplifying password formats and reducing password re-typing are preferred in practical IoT deployments [4][19]. In the case of Web applications, the IoT authentication methods differ depending on the purpose of the service, security and privacy required based on the sensitivity of data. Authentication methods should be tested with different adversaries that include interrogating the servers or user accounts for anomalies, eavesdropping by replaying messages randomly, and active injecting of man-in-the-middle attacks and network traffic [16]. Overall, while cryptography is well suited for communicating IoT authentication keys such as tokens, and security hash methods, it should be chosen well in order to protect from adversaries.

4. Security Attack of IoT Authentication Keys

Cryptography in IoT authentication uses public/private keys where a public key $P_U = (N, e)$ is used to enccrypt the original message, and a private key $P_R = (N, d)$ is used to decrypt the message [19][25]. This is achieved such that two prime numbers, P_1 and P_2 are employed to generate a semi-prime $N = P_1P_2$, and d is derived using Euler's totient function [$\varphi_n = (P_1 - 1)(P_2 - 1)$] along with the extended Euclidean Algorithm $ed \bmod \varphi_n = 1$ [29]. Using cryptography, the IoT security requirements of authentication, confidentiality, integrity and relevnace can be ensured with the property that when a public key is transmitted, the totient φ_n and the two primes P_1 and P_2 remain a secret. If φ_n, P_1 or P_2 can be determined, the private key will be compromised and the cypher-text will no longer be secure [29][30][31].

In this section, we provide a security attack of an IoT authentication key demonstrating how semi-prime could be easily factored and the primes P_1 or P_2 can be determined, thereby

compromising the cypher-text. We show how such a security attack is possible for a small IoT authentication key by using the properties of semi-prime factors from number theory.

Let $N = P_1P_2$ and consider test $N: (N \pm 1) mod 4 = 0$. Previous works have considered certain cases based on the characteristics of the factors of a semi-prime that rely on the property that they are congruent to 1 modulus 4 [32][33][34]. In this work, we consider two cases in the classification of semi-prime and this determines the constructs of the primes used. Note the sign of ± 1 determines the case used and the test is both simple and concise. We first provide mathematical derivations of P_1 and P_2 for the two cases and then apply them to an example of an IoT authentication key attack, when the semi-prime could be factored using our unique simple factorisation technique.

Case (1) $\oplus\ominus\ (N+1) mod 4 = 0,\ \ P_1 = 2(m-n)+1,\ \ \ P_2 = 2(m+n)-1$

Let $m_0 \geq \frac{\sqrt{N}}{2}, m \in \mathbb{N}^+$

Let $n_0 = \frac{\sqrt{4m_0^2 - N + 1}}{2},\ n \in \mathbb{N}^+,\ n \notin \mathbb{N}^+ \Longrightarrow m_x = m_0 + 1$

Let $n = \frac{\sqrt{4m_x^2 - N + 1}}{2},\ n \notin \mathbb{N}^+, \mathrm{m_x} = \mathrm{m_x} + 1 \Longrightarrow n: n \in \mathbb{N}^+$

$P_1 = 2(m-n)+1, P_2 = 2(m+n)-1$

Case (2) $\ominus\ominus\ (N-1) mod 4 = 0,\ \ P_1 = 2(m-n)-1,\ \ \ P_2 = 2(m+n)-1$

Let $m_0 \geq \frac{\sqrt{N}+1}{2}, m \in \mathbb{N}^+$

Let $n_0 = \frac{\sqrt{(2m_0-1)^2 - N}}{2},\ n \in \mathbb{N}^+?,\ n \notin \mathbb{N}^+ \Longrightarrow m_x = m_0 + 1$

Let $n = \frac{\sqrt{(2m_x-1)^2 - N}}{2},\ n \notin \mathbb{N}^+, \mathrm{m_x} = \mathrm{m_x} + 1 \Longrightarrow n: n \in \mathbb{N}^+$

$P_1 = 2(m-n)-1, P_2 = 2(m+n)-1$

Example IoT authentication key with $N = 5959$

Test $(N \pm 1) mod 4 = 0 : (5959 + 1)\ mod\ 4 = 0 \Longrightarrow case\ (1)\ \oplus\ominus$

$m_0 \geq \frac{\sqrt{N}}{2} \Longrightarrow m_0 = \frac{\sqrt{5959}}{2} \Longrightarrow m_0 = 39, n = 6.09, n \notin \mathbb{N}^+$

$m_1 = m_0 + 1 = 39 + 1 = 40$

$n = \frac{\sqrt{4m_1^2 - N + 1}}{2} \Longrightarrow n_1 = \frac{\sqrt{4(40)^2 - 5959 + 1}}{2} = 11, n_1 \in \mathbb{N}^+$

$$P_1 = 2(m-n)+1 \implies P_1 = 2(40-11)+1 = 59, P_2 = 2(m+n)-1 \implies P_2 = 2(40+11)-1 = 101$$
$$N = P_1 P_2 = 59 \text{ x } 101 = 5959$$

This above semi-prime factorisation method demonstrating the key-breaking attack is reasonably quick in the computation for small composites that form typical cryptography keys used for IoT authentication. However, large semi-primes with the above characteristics are practically used for cryptography keys to secure communications within mainstream computer networks. This is because breaking the keys made of very large semi-primes is computationally intractable and tedious [35]. However, small IoT authentication keys using such semi-primes are easily prone to attacks as illustrated above with the simple method that hackers adopt for breaking the encryption keys.

5. Recommendations

On one hand relying on cryptography based secret keys are recommended, understanding the properties and details of crypto primitives used for IoT authentication is essential. Security and privacy considerations should include encryption to be associated with any IoT communications, passwords, data in local and remote storage as well as in transit, etc. It is important to know the mechanism of logging, updating, patching and even offline security features of IoT devices. Further, some of the considerations about the IoT gateway should include how anomalies are detected and what alert mechanisms and interruptions due to any possible attack can be resolved.

Cloud security presents unique security considerations such as ensuring that the web interfaces and applications do not have weak authentication methods. It should also include tracking and updating of third-party components and having appropriate auditing capabilities. Applications should minimize the use of physical external ports of an IoT device. They should intelligently respond to any buffer overflow, fuzzing or other possibilities of security vulnerabilities that malicious attackers could try to exploit.

In order to plan for a continued IoT adoption and growth, we recommend that IoT devices are able to comply with standard practices, procedures and policies along with appropriate consumer awareness and training to be part of every vendor requirement and any future partnership for large scale IoT deployments. Considering the trade-off between usability and complexity of IoT authentication methods, simple evaluation schemes are required to analyze for security vulnerabilities due to default passwords, password leaks, password transfers, hash function truncation, replaying or tampering of authentication tokens, etc. Overall, we recommend simple and well-tested IoT authentication methods with cryptographic protocols wherever possible to protect IoT networks from adversaries.

6. Conclusions and Future Work

IoT is an evolutionary technology envisioning a future for smart homes, smart cities and smart industries. However, security forms the main differentiating factor for consumer adoption of personal IoT devices as well as a successful deployment of any large scale secure IoT infrastructure. In this paper, we first identified the important and unique IoT security requirements and the associated challenges. Next, we considered the most popularly employed IoT authentication methods and their limitations due to the resource constrained context of IoT. While cryptography techniques in IoT authentication methods are recommended, we demonstrated an IoT security attack of an authentication key using semi-prime number theoretic properties that could form an adversary. Finally, we provided practical recommendations based on the findings of this study. However, there are open issues as no single IoT authentication method can effectively and efficiently meet the security and privacy requirements and currently there are no established standard protocols. Our future research would focus on authentication methods towards developing an end-to-end IoT security framework.

Acknowledgment

The authors wish to thank Melbourne Polytechnic for providing the Research and Seed Grant scheme under which this study was conducted as an ongoing research project.

References

[1] Sen, S.; Koo, J.; Bagchi, S. (2018) "TRIFECTA: Security, Energy Efficiency, and Communication Capacity Comparison for Wireless IoT Devices", *IEEE Internet Comput.*, vol. 22, pp. 74–81.

[2] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P. and Sikdar, B. (2019) "A survey on IoT security: Application areas, security threats, and solution architectures", *IEEE Access*, vol. 7, pp. 82721–82743.

[3] Alrawi, O., Lever, C., Antonakakis, M. and Monrose, F. (2019). Sok: Security Evaluation of Home-based IoT Deployments. *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, May 20 - 22, 2019, San Fransisco, CA, USA.

[4] Overmars, A. and Venkatraman, S. (2020) "Towards a Secure and Scalable IoT Infrastructure: A Pilot Deployment for a Smart Water Monitoring System", *Technologies*, vol. 8, 50.

[5] Verdouwab, C., Sundmaeker, H., Tekinerdogana, B., Conzon, D. and Montanaro, T. (2019) "Architecture framework of IoT-based food and farm systems: A multiple case study". *Comput. Electron. Agric*., vol. 165, 104939.

[6] El-hajj, M., Fadlallah, A., Chamoun, M. and Serhrouchni, A. (2019) "A Survey of Internet of Things (IoT) Authentication Schemes", Sensors, vol. 19, 1141.

[7] Khan, F.I. and Hameed, S. (2019) "Understanding security requirements and challenges in internet of things (IoTs): A review", *J. Comp. Netw. Communic*., 9629381:1–9629381:14.

[8] Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C. and Lopez, J. (2018) "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services", *IEEE Commun. Surv. Tuts.*, vol. 20, pp. 3453–3495.

[9] Schmitt, C., Noack, M. and Stiller, B. (2026) "TinyTO: Two-way authentication for constrained devices in the Internet of Things". In *Internet of Things*, Elsevier: Amsterdam, The Netherlands, pp. 239–258.

]10] Tawalbeh, L., Muheidat, F., Tawalbeh, M. and Quwaider, M. (2020) "IoT Privacy and Security: Challenges and Solutions", *Appl. Sci*., vol. 10, 4102.

[11] Kumar, M. T. Katragadda, R. K. Kolli V. S. and Rahiman, S. L. (2019) A Hybrid Approach for Enhancing Security in Internet of Things (IoT), *Proceedings of International Conference on Intelligent Sustainable Systems (ICISS)*, Palladam, Tamilnadu, India, pp. 110-114.

[12] Zhou, L.,; Li,X., Yeh, K.H., Su,C. and Chiu, W. (2019) "Lightweight IoT-based authentication scheme in cloud computing circumstance", *Future Gen. Comput. Syst.*, vol. 91, 244–251.

[13] Anirudh, M., Thileeban, S.A. and Nallathambi, D.J. (2017) Use of honeypots for mitigating DoS attacks targeted on IoT networks. *Proceedings of the 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP),* Chennai, India, 10–11 January 2017.

[14] Abomhara, M. and Koien, G.M. (2015) "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *J. Cyber Secur. Mobil.*, 4, 65–88.

[15] Pammu, A.A., Chong, K.S., Ho, W.G. and Gwee, B.H. (2016) Interceptive side channel attack on AES-128 wireless communications for IoT applications. *Proceedings of the 2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)*, Jeju, Korea, 25–28 October 2016.

[16] Na, S., Hwang, D., Shin, W. and Kim, K.H. (2017) Scenario and countermeasure for replay attack using join request messages in LoRaWAN. *Proceedings of the 2017 International Conference on Information Networking (ICOIN),* Da Nang, Vietnam, 11–13 January 2017.

[17] Tangade, S. and Manvi, S.S. (2016) Scalable and privacy-preserving authentication protocol for secure vehicular communications. *Proceedings of the 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS),* Bangalore, India, 6–9 November 2016.

[18] Neto A. L. M. et al., (2016) AoT: Authentication and Access Control for the Entire IoT Device Life-Cycle, *Proceedings of the 14th ACM Conference on Embedded Network*

Sensor Systems CD-ROM, ser. SenSys '16, New York, NY, USA: ACM, 2016, pp. 1–15.

[19] Chung, Y., Choi, S., Lee, Y., Park, N. and Won, D. (2016) "An Enhanced Lightweight Anonymous Authentication Scheme for a Scalable Localization Roaming Service in Wireless Sensor Networks", Sensors, vol. 16, 1653.

[20] Li, Q. and Cao, G. (2011) "Multicast Authentication in the Smart Grid With One-Time Signature", *IEEE Trans. Smart Grid*, vol. 2, pp. 686–696.

[21] Suárez-Albela, M., Fraga-Lamas, P. and Fernández-Caramés, T.M. (2018) "A Practical Evaluation on RSA and ECC-Based Cipher Suites for IoT High-Security Energy-Efficient Fog and Mist Computing Devices", *Sensors*, vol. 18, 3868.

[22] Huth, C., Zibuschka, J., Duplys, P. and Guneysu, T. (2015) Securing systems on the Internet of Things via physical properties of devices and communications. *Proceedings of the 2015 IEEE Systems Conference (SysCon)*, Vancouver, BC, Canada, 13–16 April 2015.

[23] Kothmayr, T., Schmitt, C., Hu, W., Brünig, M. and Carle, G. (2013) "DTLS based security and two-way authentication for the Internet of Things", *Ad Hoc Netw.*, vol. 11, 2710–2723

[24] Armando, A., et al. (2001) The AVISPA Tool for the Automated Validation of Internet Security Protocols and Applications. In *Computer Aided Verification*; Etessami, K., Rajamani, S.K., Eds.; Springer: Berlin/Heidelberg, Germany, 2005; pp. 281–285.

[25] Rivest, R., Shamir, A. and Adleman, L. (1978) "A Method for Obtaining Digital for Signatures and Public-Key Cryptosystems", Communications of the ACM, vol. 21, 2, pp. 120-126.

[26] Yousefi A. and Jameii, S. M. (2017) Improving the security of internet of things using encryption algorithms, *Proceedings of 2017 International Conference on IoT and Application (ICIOT)*, Nagapattinam, India, 2017, pp. 1-5.

[27] Wen, Q., Dong, X. and Zhang, R. (2012) Application of dynamic variable cipher security certificate in Internet of Things. *Proceedings of the 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, Hangzhou, China, 30 October–1 November 2012.

[28] Thangavelu, V., Divakaran, D.M., Sairam, R., Bhunia, S.S. and Gurusamy, M. (2019) "DEFT: A distributed IoT fingerprinting technique", *IEEE Internet Things J.*, vol. 6, pp. 940–952.

[29] Yan, S.Y. *Factoring Based Cryptography. In Cyber cryptography: Applicable Cryptography for Cyberspace Security*; Springer: Berlin/Heidelberg, Germany, 2018, pp. 217–286.

[30] Ambedkar, B.R. and Bedi, S.S. (2011) "A New Factorization Method to Factorize RSA Public Key Encryption", *Int. J. Comput. Sci. Issues (IJCSI)* 2011, 8, pp. 242–247.

[31] Venkatraman, S. and Overmars, A. (2019) “New Method of Prime Factorisation-Based Attacks on RSA Authentication in IoT.” *Cryptography*, vol. 3, 20.

[32] Zagier D. (1990), "A One-Sentence Proof That Every Prime p ≡ 1 (mod 4) Is a Sum of Two Squares", *The American Mathematical Monthly*, Mathematical Association of America, 97 (2), 144.

[33] Overmars A., Venkatraman S. (2019) “A Fast Factorisation of Semi-Primes Using Sum of Squares” *Math. Comput. Appl.*, vol. 24, 62; doi: 10.3390/mca24020062

[34] Overmars, A., Venkatraman, S. (2020) “Mathematical Attack of RSA by Extending the Sum of Squares of Primes to Factorize a Semi-Prime”. *Math. Comput. Appl.* 2020, vol. 25, no. 63, pp. 1-15.

[35] Traversa, F.L. and di Ventra, M. (2017) “Polynomial-time solution of prime factorization and NP-complete problems with digital memcomputing machines”, *Chaos Interdiscip. J. Nonlinear Sci.*, vol. 27, 023107.