ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/331320033

Network Security: A Brief Overview of Evolving Strategies and Challenges

Article *in* International Journal of Science and Research (IJSR) · February 2019

DOI: 10.21275/ART20194980

CITATIONS
2

READS
7,145

1 author:

Francis Ruambo
Huazhong University of Science and Technology
13 PUBLICATIONS **58** CITATIONS

SEE PROFILE

All content following this page was uploaded by Francis Ruambo on 08 July 2019.

The user has requested enhancement of the downloaded file.

International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor (2018): 7.426

Network Security: A Brief Overview of Evolving Strategies and Challenges

Francis Aidan Ruambo

Mbeya University of Science and Technology (MUST), Information and Communication Technology (ICT) Department

Abstract: ***Network Security strategies evolve parallel with the advancement and development of computer systems and services. The ubiquity of ICT devices and services offers undeniable efficiency in executing our daily routine activities. Challenges in the aspects of security and continuous availability of the ICT resources and services, trigger the evolution of network security strategies. In this review paper, a brief overview of evolving strategies adopted within the dynamic paradigm of network security is highlighted and challenges are reviewed. Additionally, interesting areas for future research in securing the computer network ecosystem are suggested. The review finds that, as long as computer systems and services are dynamically evolving, then the network security strategies will also continue to be an evolving and volatile paradigm. In order to enhance network security, there is a need for incorporating new innovative strategies whilst embracing network security best practices and principles to mitigate appropriately the evolving threats within the computer network ecosystem.***

Keywords: Network Security, Computer Networks, Security Management, Internet of Things

1. Introduction

Network security comprises of all the techniques that intend to maintain, repair and guarantee the protection of information within computer systems from malicious attacks. Security within computer networks has always been a major issue. The computer network technologies are developing quickly, and the development of internet technologies is more rapid. The increasing reliance on the use of the network-connected technologies in our daily activities has grown faster than the approach to secure it. For example, within the internet of things (IoT), the IoT devices are becoming of great importance in playing a part in our daily activities and fortunately promising a bright future in innovation of networking systems and services.

IoT which is the best example of evolving trends within networking systems and services, it refers to the connection of devices and systems with principal physical goals (e.g. Sensing, motor actuation, heating/cooling, and lighting) to data communication networks (including the Internet) through interoperable protocols, frequently incorporated with embedded systems [1]. As time goes on, awareness of the network security importance among people increases. Thus, the society cannot tolerate an era of the functioning evolving networking ecosystem with little attention for security whilst its impact is so high. By securing the ecosystem, can guarantee the protection and security of delicate information generated and stored by the participating devices, hence curbing threats that can be posed to critical infrastructures and services such as smart cities, cars, homes et cetera.

Network security has become the main concern in the development and deployment of computer network systems and services as several kinds of attacks is increasing day after day. The critical issue is how to protect these computer network systems and services from malicious nodes, which create several problems within the network ecosystem such as unavailability of services, loss of data and privacy in communications et cetera. As threats becoming more complex, moving from basic attacks against one device to complicated attacks against several devices in the computer network ecosystem, traditional security strategies are simply not enough in the digitalization era [2]. These challenges have been the driving force that triggers the evolution of various network security strategies, for mitigating the aforesaid problems. This paper emphases on providing a brief overview of evolving network security strategies in addressing the aforementioned issues.

The organization of this review paper is as follows. Firstly, a background on security services and challenges in computer networks is presented in Section II, then the evolution of network security strategies and their challenges are described in section III, in Section IV a classification of evolving strategies is described. Section V discusses some insights for improving security in evolving networking systems and services and finally, the paper is concluded in Section VI.

2. Background on Security Services and Challenges

a) Security Services

Network security is any action designed to shield the integrity and usability of data and network [3]. It includes software and hardware technologies. Effective network security controls access to the resources and services on the network. It marks and prohibit a variety of threats and halts them from spreading or entering into the network. Recently, security threats such as leakage of personal data and economic espionage, identity theft and infection of critical computer systems are given high concerns within mass media and the society at large. Generally, security within computer networks and information systems, must deliver the following services [3]:

Confidentiality: It guarantees that information is unintelligible, upon its accessibility by unauthorized individuals, processes, and entities.

Integrity: It makes sure that data has not been changed

Licensed Under Creative Commons Attribution CC BY

accidentally or intentionally by a third party.

Authentication: It confirms that the data source is the intended identity.

Non-repudiation: It guarantees that the sender of the message cannot dispute its authorship in the future.

Availability: It guarantees that system services are available for users who are legitimate.

Privacy: It guarantees both users' identities unidentifiability and untraceability from their manners and performed actions within the system.

Numerous cryptographic mechanisms have been developed to mitigate different security threats and ensure the provision of the aforementioned security services is achieved. Table 1, provides some of the mechanisms.

Table 1: Security services and strategies

Security services	Security Strategies	Examples
Confidentiality	Message encryption/sign -encryption	Symmetric cryptographic mechanisms (AES, CBC, etc); asymmetric mechanisms (RSA, DSA, IBE, ABE, etc).
Integrity	Hash functions, message signature	Hash functions (SHA-256, MD5, etc.); Message Authentication Codes (HMAC)
Authentication	Chain of hash, Message Authentication Code	HMAC, CBC-MAC, ECDSA
Non-repudiation	Message signature	ECDSA, HMAC
Availability	Pseudo-random frequency hopping, Access control, Intrusion prevention systems, firewalls	Signature-Based Intrusion Detection, Statistical anomaly-based intrusion detection
Privacy	Pseudonymity, unlinkability, k-anonymity, Zero Knowledge Proof (ZKP)	EPID, DAA, Pedersen Commitment

b) Challenges

Nowadays, modern IT technologies are used to enhance the customers' quality of experience and also to optimize performance of critical applications in different fields. Communication networks enable to improve several applications in many fields, such as, smart homes, healthcare, smart grids, smart cities plus other industrial applications. Nevertheless, the role of communication networks as the core in the fundamental infrastructure for delivering of such sensitive applications leads to new security and privacy challenges. In this section, the challenges in implementation of network security in evolving network systems and services are highlighted as illustrated in Figure 1 and explained thereafter.

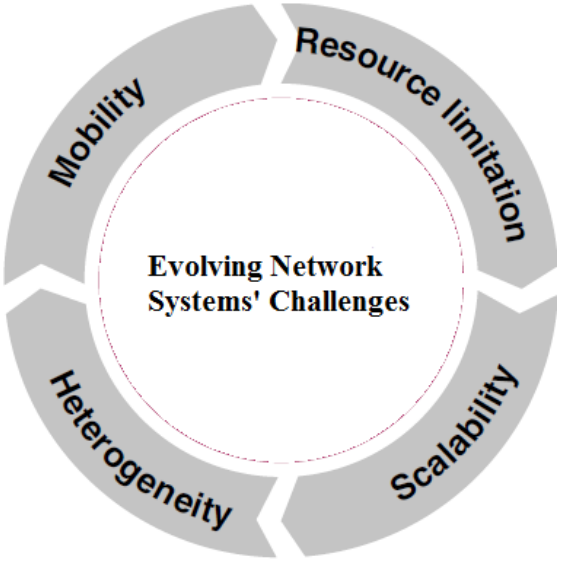

Figure 1: Security challenges

Heterogeneity

Heterogeneity of communication standards and information system technologies in a distributed networked ecosystem is the critical issue in securing the ecosystem. For example, the communication between sensor nodes and servers or CPU units from various applications (which are heterogeneous in terms of units of measurements and delivery frequencies) generally are carried out over the Internet where networks, communication mediums and protocols are also heterogeneous and have different security configurations. The diversity of the entities involved in evolving networks provides a broad surface for attacks from any of those entities (e.g. Attacks such as Distributed Denial of Service are inevitable).Hence, developing (coming up with) an adaptive security solution that works in heterogeneous environments is very challenging.

Scalability

As the population and the reliance on the use of the network-connected technologies gradually increase, the number of smart devices continues to grow daily posing another serious scalability challenge on development of security solutions

Resources limitations

Most of evolving devices participating in modern networks such as embedded sensors and wearable have restricted resources in terms of memory, computation and battery. As the most of cryptographic strategies are expensive in terms of computation, adjusting them to ensure a high security level whilst minimizing consumption of energy is a hard and serious challenge.

High mobility

From embedded sensors and actuators in human bodies to smart vehicles, implementing security solutions that are reliable is a critical challenge. Taking in consideration mobility within highly dynamic environments, where network topology changes frequently are a bit challenging for security solution deployment.

Licensed Under Creative Commons Attribution CC BY

3. Evolution of Network Security Strategies

Evolution in network security strategies is the result of the evolution in ubiquitous interconnectivity between users, devices, and distributed networks (i.e. Networked ecosystem, for instance the Internet of Things). The traditionally security strategies such as defending a single place within the network are gradually ineffective in the networked ecosystem. Additionally, several conventional standards in security and best practices cannot address the evolved security challenges within the ecosystem are not as effective.

The evolution of security strategies encompasses the traditional security pillars: integrity, confidentiality, and availability. But it must increasingly go further than these requirements in order to address also the emerging requirements covering both physical environment, health as well as safety issues. The addition of several interconnected devices and services to the ecosystem requires addressing of critical issues such as physical safety, disaster recovery for such things like smart or driverless cars, connected HVAC systems, business continuity, and online medical devices including pacemakers and infusion pumps, or city networks which are interconnected.

In order to mitigate the evolving security challenges, adopted security strategies are dynamically adding some security functionalities to match the new security requirements. For instance, from basic security requirements Table 2 illustrates additional areas that can be incorporated in enhancing security within the modern networked ecosystem.

Table 2: Evolving additional security requirements

Functionality	Description
Identification	Understanding risk profile and current state
Protection	Applying prevention strategies to mitigate vulnerabilities and threats
Detection	Detecting anomalies and events
Response	Incident response, mitigation, and improvements
Recovery	Continuous life cycle improvement

4. Classification of Evolving Security Strategies

a) Conventional Strategies

This category comprises the cryptographic based strategies that are specifically designed for the Internet of Things which is the evolved paradigm interconnecting several electronic devices and services. The focus is principally on guaranteeing: confidentiality, privacy and availability of services. In evolving networked ecosystem, we need to protect data exchanged between objects from malicious actors through encryption mechanisms. Therefore, only legitimate users are allowed to unveil encrypted data. Data confidentiality is achieved by cryptographic tools, nevertheless, in most cases, these tools are ineffective or even inappropriate in devices with high resource constraints. This resulted from cryptographic algorithms' nature which require a lot of storage and computation.

Privacy preserving is mandatory in a networked ecosystem as data issued by smart objects are very sensitives and inherently linked to real life of users. The main objective of privacy techniques is to guarantee the following requirements:

- Anonymity: Property ensures that a third entity is unable to identify the person's identity among other identities in the system.
- Unlinkability: Impossibility to cover the person's identity from the information they produce.
- Untraceability: Difficulty to track actions and information issued from an entity's behavior within the system.

The privacy strategies intend to protect sensitive data and similarly providing mechanisms to hide users' identities so that the intruders can't identify their behaviors.

Lastly, the availability of the network systems and services is one of the most significant security services needs to be protected against malicious attacks (such as DoS/DDoS) or accidental failures. Very frequently, the damages associated with violation of the availability are tremendous which range from economical losses (i.e. In manufacturing systems) to safety damages (i.e. In transportation systems) or altogether. Additionally, guaranteeing the availability has been a very challenging task since that for attackers to break the system exploit entirely a range of vulnerabilities' types at different levels (i.e. Software, network design, cryptographic algorithms, and etcetera.).

Most of the conventional strategies ensure proper functioning of the security services involving central trusted entities (i.e. in centralized environments).

b) Confidentiality Enablers

Symmetric key strategies offers confidentiality whereby, each entity in the system has to distribute cryptographic keys with all other entities within the system. Symmetric based cryptographic strategies are advantageous for their efficiency (as they are less-computational) and also are easy to implement in hardware platforms. In practice, AES (Advanced Encryption Standard), 3DES and RC4 are only few examples commonly used. Though Symmetric key strategies provide efficiencies, they still suffer from key management and scalability issues. The key distribution tactics adopted is either probabilistically or deterministically. In deterministic tactics, each entity has to form a secure link with all other entities in order to establish a complete secure connectivity coverage. Whilst in Probabilistic key distribution, sharing of a secure key of each node in the network amongst all other nodes is not assured, nevertheless the nodes distribute keys with their neighbors as per some probabilities which establish secure paths amongst all entities within the network.

Traditional Asymmetric strategies comprise all methods rely on public keys and need the authority to issue certificates to various system's users. It includes RSA, DSA, NTRU, ECC cryptosystems, et cetera. The key advantages of the asymmetric strategies are scalability, flexibility, and key management efficiency. Nevertheless, these strategies are not appropriate for constrained devices in the energy-consuming aspect. NTRU comprises of the much less computational

Licensed Under Creative Commons Attribution CC BY

asymmetric strategy which is based on the shortest vector problem within a lattice [4], though it needs more memory space for storing the keys.

Attribute based encryption (ABE) introduces an expressive way to control private data accessibility through policy access structure that describes relationships between attribute set used to encrypt data. Within the ABE system, for each legitimate user a private key based on its attributes is generated by Key Generation Server (KGS) .Additionally, based on predefined policy, a public key is used to encrypt data. A legitimate user is able to decrypt data only if it has the necessary attributes that fulfil the policy. Can be either Key Policy ABE (KP-ABE) or Cipher-text Policy ABE (CP-ABE).

- **Key Policy ABE (KP-ABE):** In **KP-ABE**, the data owner creates an access structure *A* and uses a set of attributes *I* to encrypt the data. Then, a user in order to decrypt the cipher-text is required to have the attributes that fulfil the access structure *A.* In such a manner a user will be able to derive the private key for decrypting the cipher-text [5].
- **Cipher-text Policy ABE (CP-ABE):** In CP-ABE, the encryption relies on the access structure *A*. Whereby, a user is legitimate only if has a set with sufficient attributes *I* that fulfills the access structure (policy A) which has been attached to the cipher text [6].

Identity based encryption (IBE) Transitional public key cryptosystems suffer in scalability issues. This is due to their dependency on the issuing of certificates from the authority for each user in the system which is necessary in dealing with identity usurpation and spoofing. Identity Based Encryption tools deal successfully with the scalability and complexity by using unforgeable string associated with the identity of the user (such as users' email address, phone number and et cetera.) as public key for data encryption and thus no need of certificates. Though IBE strategy is expensive and incur resource consumption, hence not very suitable for evolving networked ecosystem with many under constrained devices.

Privacy Enablers

Data tagging ensures privacy of data flows by incorporating additional labels known as tags, to data flows which allows trusted computing entities to associate with the flows of private data, hence identities of individuals who responsible for the data is hidden[7]. However, tagging mechanisms might suffer the computations issues depending on the size of data. In [8], the authors provided the lightweight code templates devoted to resource-constrained devices to prove the applicability of tagging mechanism for programmable micro-controller (PIC) under constraint.

Zero Knowledge Proof (ZKP) is an effective mechanism mostly used to guarantee the users' identities privacy. The ZKP works by allowing one party (prover) to authenticate to another party (verifier) some property by proving its information possession without disclosing it [9]. This concept is very useful in developing security protocols whilst maintaining the privacy aspect regarding data and properties of the users. In [9] basing on the Discrete Logarithm Problem, an evaluation of some ZKP protocols on elliptic curves (ECC) for resource-constrained devices were proposed. With the same level of security settings, the results found that using ECC (with 1024 key's length) comparing to RSA offers much less execution time and memory. Notably, the energy associated with the communication is minimal for small message sizes. Nevertheless, beyond some threshold, messages' fragmentation causes overloading within ZKP protocols.

The K - anonymity model is another likely promising method to assure data privacy in evolving network services such as the Internet of Things' applications. Bearing in mind the case whereby a set of homogenous data (comprising sensitive information such as ages, the phone numbers, the addresses, and et cetera.) stored in a table. If the table column represents a record of the data owned by some specific users. The K-anonymity models intend to shield each record within the table and make it fuzzy from at least $k-1$ records within the same table through hiding the owner's sensitive information [10]. In cloud and big data applications, k-anonymity model is mostly adopted to protect data streams privacy given out by different users. Principally, in IoT applications, there are several efforts to implement k-anonymity models [11, 12, and 13].

Availability Enablers

DoS/DDoS countermeasure strategies such as IP Trace back methods are effective mechanisms mostly implemented in IP based networks like the Internet to identify in real-time DoS and IP flooding attacks. These methods emphasize primarily to improve the security of IP based lightweight protocols principally designed as versions of the traditional TCP/IP protocols in the evolving networked ecosystem such as IoT. IPv6 Low power Wireless Personal Area Networks (6LoWPAN), Datagram Transport Layer Security (DTLS 9), IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL))are just a few examples amongst other protocols widely implemented in it to support secure end-to-end exchange of information between IoT devices by providing confidentiality and integrity [14] . Though, these protocols are not pre-designed to mitigate the common IP based DoS/DDoS attacks. Several security solutions have been examined to enhance RPL based 6LoWPAN routing protocol and DTLS based transport layer with the aim of increasing robustness and security against DoS attacks. Within the existing solutions, IP routers and IoT gateways play the main role by inspecting and analyzing packets in order to identify malicious behaviors and consequently take appropriate actions [2].

On the other hand, in the network layer of TCP/IP and particularly within the routing level, several security enhancements of RPL and 6LoW- PAN based IoT architectures are suggested. In contrast, Kasinathan et al. [15] suggested an architecture to shield IoT devices based on 6LoWPAN from DoS attacks as well as tampering and jamming attacks in the European project termed *ebbits.* They contributed in designing of Intrusion detection manager that dedicated to secure constrained devices from DoS attacks. For monitor 6LoWPAN packets, they also provide a design of the Intrusion Detection System (IDS), that in case of any misbehavior it raises alerts. The IDS operates in promiscuous

Licensed Under Creative Commons Attribution CC BY

mode.

Artificial intelligence strategies like Artificial Neural Networks (ANN) are regarded as one of the most influential strategy used in designing of efficient IDS. As an instance, in [16], the authors examined the use of ANN in IoT to identify DOS attacks. In order to verify which one is more satisfactory as an IDS in evolving networked systems, they evaluated two types of ANNs, namely: Multilayer Perceptron with Limited Weights and Multilayer Perceptron with Normal Weights. The results found that under training process both of ANN techniques lessen false positive detection, nevertheless their consumption of memory is high, thus limiting their suitability within an ecosystem with constrained devices. The possibility of using Cumulative Sum (CUMSUM) DDoS attacks detection in the context of evolving networks such as IoT was examined by other researchers [17]. The main intention of CUSUM algorithm is real time detection of changes within the statistic process given out by data streams. Through network traffic analysis and its statistical computation, the DDoS are detected. Continuously, the algorithm handles the statistics and finally detects variations which are linked to any misbehavior within the network traffic.

c) Modern Strategies

This category comprises security solutions that are based totally on new evolving techniques rather than the existing cryptographic tools. They are more suitable to address the scalability issues compared to the conventional strategies. In general, the solutions belonging to this category are decentralized. Some of the two promising technologies are emerging:

1) *Software Defined Networking (SDN),* is a new network paradigm which transforms the computer network functionalities by providing a conducive environment for developing network solutions, which are more flexible and simplify network resources management through centralized SDN controllers. There are numerous security solutions based on SDN within the literature that target evolving network services.

   SDN deployment parallel with Network function Visualization (NFV) as a result can enhance the resource allocation in constrained devices within the evolved networked ecosystem. Hence, SDN provides many opportunities for overcoming some evolving challenges of security, scalability, reliability and QoS in flexible and more efficient way [18].
   In [19] contributed a new SDN based IoT architecture with multi-domains which supports all networks with or without infrastructure. Also to manage security policies among multiple SDN domains, they designed a distributed security model. The conflict issues due to security policy enforcement of the several domains, is solved by security paradigm grid that purposely used to solve security heterogeneity issues. Hence, each SDN controller pushes security policies within its domain and outside the domain coordinates with other SDN controllers.

Challenges

Primarily, the SDN based security strategy addresses security issues within the operations of centralized architectures. Therefore, the centralized SDN controllers become particular critical points of attacks. This is the main challenge as centralized SDN controllers need to be protected against evolving common attacks such as DDoS. Also dealing efficiently with the large number of devices in the underlying data plan network poses scalability issues.
Additionally, the southbound interface between data plan and

SDN controller is the threats vulnerable point for efficiency in network performance. For instance, in [20] sited integrity issues within Openflow protocol.

Centralized SDN strategy is not effective in highly dynamic environments where numerous messages are exchanged between devices and network topology changes regularly such as in vehicular networks. In such environments, SDN strategies might take a lot of time to implement security policies and configurations.

It's true that SDN strategy is more suitable in some applications and deal efficiently with the quality of service and heterogeneity issues. Nevertheless, their centralized architecture limits the scalability aspect in the most cases.

2) *Blockchain technology*, promises to provide security within an evolving network ecosystem as its application has already proved successful within cryptocurrency tools (for instance Bitcoin). It simply facilitates transactions between entities in a distributed manner (peer to peer architecture without referring to any central trusted server). Additionally, in its operation no requirement of entities to trust each other is needed. With this technology, it is practically impossible to dispute performed transactions after they are validated. There are evolving security solutions that researchers have put the light on this technology in order to mitigate security threats in evolving network systems and services through the provision of security functionalities such as data privacy, access control, et cetera.

   Some vivid examples of application of blockchain within an evolving networked ecosystem are as follows:
   Alliance on IoT Blockchain (Guardtime and Intrinsic-ID)
   Intrinsic-ID is a company that suggests cryptographic solutions to authenticate embedded devices, though technology termed as a Physical Unclonable Function (PUF) which is mostly used to protect sensitive operations such as payments and data associated with governments. The aim of Guardtime is to offer a security solution using fundamentally Keyless Signature Infrastructure (KSI) platform which comprises a scalable blockchain solution. [2]

Chronicled.com: It is a new startup offering blockchain based solutions. It is primarily focusing on solving security related problems, specifically the authenticity and the identification of IoT devices. They appealed that blockchain might solve several existing security issues credited to its tamper-resistant feature. Especially at the moment when current protection tools such as barcodes, QR codes are effortlessly forged.

Benefits

Licensed Under Creative Commons Attribution CC BY

Blockchain technology can bring some values within security domains [21] in the evolution of networking services. The following are blockchain features that can be incorporated to benefit the security domain of evolving network services:

Security of transactions: Before being sent to the blockchain network, all transactions are signed by the node, and must be validated and verified by miners. After validation, the transactions kept on the blockchain are virtually impossible to forge or do any modification. This offers within the system, a proof of traceable events.

Decentralization: The decentralized architecture of evolving network system and services, favors blockchain as an appropriate security strategy within the ecosystem. Scalability achieved through blockchain decentralized architecture can improve security by avoiding single point of failure thus increasing robustness against DoS attacks.

Pseudononymity: The pseudonyms within blockchain offers unlinkability between information and participating node's identity. Public keys or public keys are used to identify the nodes in blockchain.

Challenges

Regardless of the highlighted blockchain's benefits above, there are still several challenges to be addressed for adapting the blockchain technology in modern networks. Here are some of the challenges:

Computation and storage issues: Miniaturization of devices within evolving networked ecosystem limit capabilities with respect to computation and resources storage. Therefore, to suffice the security need of evolving networking systems and services, the blockchain has to be customized to address the computation and storage issues. In [21] the problem of adaptability is addressed by Proof of Work (PoW) implementation whereby a new application level is added, for the sole purpose of hiding the blockchain details. In this way resource-constrained devices within a networked ecosystem can participate without computing the PoW.

Time latency: Real time applications can suffer security issues if the same transaction validation period of 10 minutes with the bitcoin blockchain, will be adopted within evolving networking systems and services.

Scalability issues: According to Cisco, by 2020, in the Internet there will be more than 20 billion connected IoT objects [22].Although the incredible success that bitcoin blockchain has achieved, with the exponentially increasing of users with time, blockchain technology is still cannot guarantee scalability within the networked ecosystem such as IoT.

Bandwidth consumption: Large in number of transactions generated by numerous devices within the networked ecosystem poses bandwidth consumption problems upon necessity of validating each of the devices' transactions.

The anonymity: Though, from blockchain transactions is impossible to extract the identity of the person from its pseudonym but still doesn't guarantee a fully anonymous transaction. This is due t the fact that the peers within blockchain are identified by pseudonyms which can be tracked [23].

The summary of the classification of evolving network security strategies is illustrated in Figure 2.

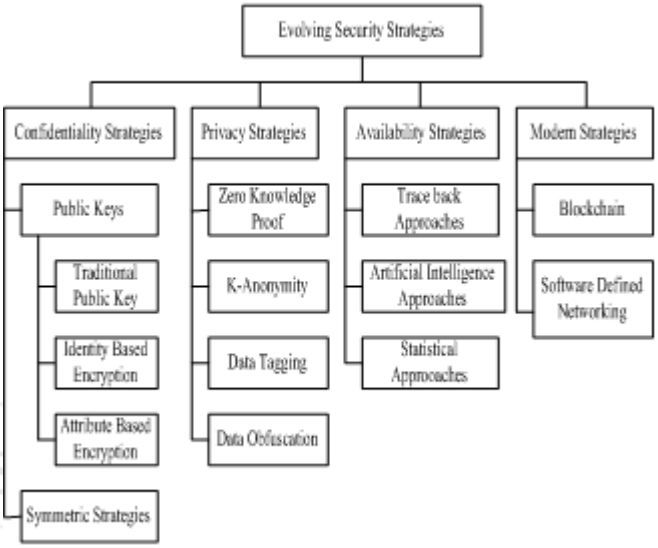

Figure 2: classification of evolving network security strategies

Generally, vital challenges such as resource limitations and scalability are still not convenient enough in dynamic and modern networks such as vehicular networks where the context changes regularly. Often, the context groups several pieces of information about the devices' locations, their battery levels, the number of their neighboring objects, et cetera. These chunks of information can be relevant and hence very important in enhancing the security and additionally they can be applied to design more flexible and context-aware security solutions without referring to cryptographic approaches. For instance, considering a heavy cryptographic algorithm to authenticate a single IoT device A. In some circumstances, sometimes it is interesting: to avoid using a cryptographic algorithm to authenticate device A as it lacks adequate energy to complete the heavy cryptographic processes and consequently saves its battery whilst it is located in a safe zone. Can be a matter of great advantage upon considering other information associated with the device A to identify it without depending on cryptographic strategies. The information could be the date of its last authentication, the location of A, the owner of A, and et cetera.

The context plays an important role to better address security challenges in dynamic IoT environments. Overall, the solutions in this category meet efficiently performance requirements such as power consumption, computation, memory occupation and quality of service. However, compared to other techniques, these solutions remain less developed in the literature, especially in the context of IoT. Therefore, more research efforts should be devoted to fill the gap and enhance the existing solutions by taking advantage of the environment where IoT devices evolve.

Licensed Under Creative Commons Attribution CC BY

5. Discussion

Though several of the security challenges prevailing in digital transformation are new, they can still be managed through a combination of proven best practices and implementation of better security framework. High-speed authentication parallel with monitoring plays the core role in securing the highly distributed ecosystems. Additionally, internal segmentation designed for monitoring and protecting distributed computing and networking whilst enforcing and coordinating distributed and cloud-based security services that can track and secure data and devices distributed across the network ecosystem. Security must tie together the entire networked ecosystem.

Security within evolving network systems and services requires automated visibility from end to end points, equipped with innovative detection capabilities, driven by the threat intelligence permitting orchestration of responses to alleviate threats at machine speed. What is required is an integrated and distributed, framework-based security approach that can cover the whole networked ecosystem, increase and guarantee resilience, and protect computing resources. This strategy can effectively enable monitoring legitimate traffic, checking authentication and credentialing, and imposing access management across the distributed ecosystem through a security architecture that is integrated, synchronized, and automated.

6. Conclusion

In this review paper, a brief overview of evolving network security strategies is highlighted and challenges are reviewed. Additionally, principle strategies in securing the network ecosystem are suggested. The review finds that, as long as computer systems and services are dynamic, evolving phenomena, consequently the evolution in network security strategies will also be a continually evolving and volatile paradigm. In order to enhance network security, there is a need of incorporating new innovative strategies and embracing network security best practices and principles to mitigate appropriately the evolving threats within the network ecosystem.

References

[1] IDC, “Worldwide Internet of Things Forecast,” 2015-2020,May 2015,
[2] D.E. Kouicem, A.Bouabdallah , H. Lakhlef Internet of things security: A top-down survey, Computer Networks 141(2018)199-221.doi.org/10.1016/j.comnet.2018.03.012
[3] H. Noura , Adaptation of Cryptographic Algorithms According to the Applications Requirements and Limitations : Design, Analyze and Lessons Learned, University of Pierre & Marie Curie -Paris VI, 2016 HDR dissertation .
[4] K.T. Nguyen, M. Laurent, N. Oualha, Survey on secure communication protocols for the internet of things, Ad Hoc Netw. 32 (2015) 17–31, doi: 10.1016/j. adhoc.2015.01.006.
[5] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in: Proceedings of the 13th ACM conference on Computer and communications security, ACM, 2006, pp. 89–98.
[6] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption, in: IEEE Symposium on Security and Privacy, 2007. SP’07, IEEE, 2007, pp. 321–334.
[7] P.J. Bruening, K.K. Waterman, Data tagging for new information governance models, IEEE Secur. Priv. 8 (5) (2010) 64–68, doi: 10.1109/MSP.2010.147.
[8] D. Evans, D.M. Eyers, Efficient data tagging for managing privacy in the in- ternet of things, in: 2012 IEEE International Conference on Green Computing and Communications (GreenCom), IEEE, 2012, pp. 244–248.
[9] I. Chatzigiannakis , A. Pyrgelis , P.G. Spirakis , Y.C. Stamatiou , Elliptic curve based zero knowledge proofs and their applicability on resource constrained devices, in: 2011 IEEE 8th International Conference on Mobile Adhoc and Sensor Systems (MASS), IEEE, 2011, pp. 715–720 .
[10] L. Sweeney, K-anonymity: a model for protecting privacy, Int. J. Uncertainty Fuzziness Knowl. Based Syst. 10 (05) (2002) 557–570.
[11] X. Huang, R. Fu, B. Chen, T. Zhang, A. Roscoe, User interactive internet of things privacy preserved access control, in: 2012 International Conference for Internet Technology and Secured Transactions, IEEE, 2012, pp. 597–602.
[12] W. Huo-wang, Z. Cheng, Parallel clustering-based k-anonymity algorithm in internet of things, Inf. Technol. 12 (2013) 003.
[13] B. Niu , Q. Li , X. Zhu , G. Cao , H. Li , Achieving k-anonymity in privacy-aware location-based services, in: INFOCOM, 2014 Proceedings IEEE, IEEE, 2014, pp. 754–762 .
[14] S. Sahraoui, A. Bilami, Efficient hip-based approach to ensure lightweight end-to-end security in the internet of things, Comput. Networks 91 (2015) 26–45, doi: 10.1016/j.comnet.2015.08.002.
[15] P. Kasinathan, C. Pastrone, M.A. Spirito, M. Vinkovits, Denial-of-service detection in 6lowpan based internet of things, in: 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2013, pp. 600–607.
[16] F.M. de Almeida, A. de RL Ribeiro, E.D. Moreno, C.A. Montesco, Performance evaluation of an artificial neural network multilayer perceptron with limited weights for detecting denial of service attack on internet of things, Training 1112.
[17] P. Machaka , A. McDonald , F. Nelwamondo , A. Bagula , Using the cumulative sum algorithm against distributed denial of service attacks in internet of things, in: International Conference on Context-Aware Systems and Applications, Springer, 2015, pp. 62–72.
[18] P. Hu, A system architecture for software-defined industrial internet of things, in: 2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), IEEE, 2015, pp. 1–5, doi: 10.1109/ICUWB.2015.7324414.

Licensed Under Creative Commons Attribution CC BY

[19] O. Flauzac, C. GonzÃ! ‘lez, A. Hachani, F. Nolot, Sdn based architecture for iot and improvement of the security, in: 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, IEEE, 2015, pp. 688–693, doi: 10.1109/WAINA.2015.110.
[20] S. Brief, Sdn security considerations in the data center, 2013.
[21] M. Conoscenti, A. Vetrò, J.C. De Martin, Blockchain for the internet of things: a systematic literature review (2016) 1–6.
[22] D. Evans, The Internet of Things How the Next Evolution of the Internet Is Changing Everything, Technical Report, 2011.
[23] J. Brygier , M. Oezer , Safety and security for the internet of things, 8th European Congress on Embedded Real Time Software and Systems (ERTS 2016), 2016 .

www.ijsr.net
IJSR
ISSN (Online): 2319-7064

Licensed Under Creative Commons Attribution CC BY

View publication stats