

A data-centric security architecture for challenged networks

Etienne Lemonnier^{*†}, Lionel Touseau^{*†}, Jamal El Hachem^{*}, Jérémy Buisson[‡], Nicolas Belloir^{*†}, Jean-François Wiorek[§]

^{*} Université Bretagne Sud, UMR CNRS 6074, IRISA, F-56000 Vannes, France

[†] Académie Militaire de Saint-Cyr Coëtquidan, CReC Saint-Cyr, F-56380 Guer, France

[‡] École de l'Air et de l'Espace, F-13300 Salon-de-Provence, France

[§] Thales Group, F-92230 Gennevilliers, France

Abstract—Challenged networks refer to wireless mobile networks operating in infrastructure-less areas, using mesh, ad-hoc or opportunistic networking protocols. Post-disaster emergency networks or tactical networks are instances of such networks where security and data protection is a major concern. Data-centric security (DCS) is a promising approach that brings access control policies directly to the data itself, thereby reducing the security layers on the network. However, DCS solutions rely on centralised architectures that are conflicting with the constraints of challenged networks, which are by nature prone to connectivity disruptions. This paper introduces D3CS, a decentralised and dynamic DCS architecture fitting the dynamic nature of challenged networks. D3CS combines attribute-based encryption and attribute-based signatures with delegation mechanisms to mitigate losses of connectivity with the central authority. An implementation of D3CS has been prototyped and successfully demonstrated on an opportunistic network.

Index Terms—Data-centric security, ABE, decentralisation, Opportunistic Networking

I. INTRODUCTION

Challenged networks encompass all kinds of mobile networks operating in challenging environments where traditional infrastructures may be damaged or unavailable. Disaster-response networks or tactical networks fall into this category. In order to support collaborative operations, they usually rely on ad hoc, mesh or opportunistic networking protocols to enable communications in infrastructure-less environments.

Although these challenged networks are inherently prone to network fragmentation and connectivity disruptions, security remains a major issue that must be addressed despite such connectivity constraints. Even in a post-disaster crisis scenario, emergency response teams should comply with the privacy of medical records whilst providing assistance to victims. Likewise, situational awareness data exchanged in tactical networks should be protected by appropriate levels of security. Supporting the latter case, the North Atlantic Treaty Organization (NATO) advocates for the capability of exchanging classified information among the members of the alliance, across the security domains of each member and regardless of their network security protocols [1].

Different methods can secure exchanges. Among them, Data-Centric Security (DCS) extends defence-in-depth by binding the innermost security layer to the data itself [2]. DCS

adds attaching labels to data and provides attributes to subjects to enable fine-grained access control. Attribute-based access control (ABAC) [3] or attribute-based encryption (ABE) [4] are tools to enact the security policies that define the ability to access data. However, these solutions are unsuitable in the context of challenged networks, because both rely on a centralised authority either for policy evaluation (ABAC) or key management (ABE).

To provide challenged networks with DCS, not only must the decentralisation issue be addressed, but the dynamic nature of such networks must also be taken into consideration. A DCS system should be able to adapt to evolving conditions, and thus support dynamic enrolment or exclusion of members. For these reasons, we propose a decentralised and dynamic DCS (D3CS) architecture tailored to the needs of collaborative systems supported by challenged networks. D3CS leverages ABE and delegation mechanisms to ensure that the data security layer remains operational in spite of connectivity disruptions with authorities. The D3CS architecture has been implemented on an opportunistic network for demonstration.

The remainder of the paper is structured as follows. Section II discusses work related to DCS. Then, Section III presents our decentralised and dynamic DCS architecture (D3CS). Section IV describes the implementation and demonstration of the D3CS architecture on top of an opportunistic network. Eventually, Section V concludes the paper and presents future development perspectives.

II. RELATED WORK

DCS can be implemented using attribute-based access control (ABAC) [3], which enforces access decisions by evaluating subject attributes against predefined policies, through components inserted in the subject-object path to enforce decisions. Zero-Trust Architecture (ZTA) [5] complements ABAC by introducing additional security mechanisms, such as continuous identity verification or end-to-end encryption. Nevertheless, ABAC and ZTA approaches remain centralised, as authorisations are issued by a central entity. If this entity becomes unavailable, subjects cannot obtain access rights. Therefore, decentralisation must be addressed to provide DCS in challenged networks.

To lower centralisation, attribute-based encryption (ABE) [4] could be considered. It is a family of cryptographic schemes that embeds access control into encryption. In the *ciphertext policy* variant (CP-ABE), a subject encrypts an object along with an access policy using a public key. Another subject can decrypt it only if its private key, which is unique and encodes a set of attributes, satisfies the policy embedded within the encrypted object. In contrast with ABAC, subjects with a private key can decrypt objects when permitted by the policy without further action. However, the subjects still need to communicate with a central authority to obtain their private keys.

Porwal and Mittal (P&M) [6] extend CP-ABE with attribute delegation, such that any subject (the *delegator*) can issue a private key for another subject (the *delegatee*). Subjects can thus obtain a private key even when the authority is not available. To ensure soundness, the delegatees inherit only a subset of the delegator attributes, hence the delegatees can access a subset of the objects. To deal with subject exclusion, P&M also provides attribute revocation. To do so, any private key is split in two partial secret keys, a PSKA for the authority, and a PSKS for the subject, with a two-step decryption. Besides, a *trusted mediator* (TM) is introduced to keep the PSKAs secret, while the subjects are only provided with the PSKSs. That way, a subject can decrypt an object only if the TM grants to do so. So, the TM can check whether the PSKA-PSKS pair does not refer to any revoked attribute before accepting to perform the first step of decryption. Trusted mediator is however presented as centralised in P&M's scheme, which is not compatible with decentralised DCS.

Multi-authority ABE architectures [7]–[9], where each authority manages a subset of attributes, have also been proposed to address decentralisation. Spreading the attributes over several authorities contributes to prevent the *key escrow issue*. Yao [9] indicates that each authority can manage specific attributes or security domains. However, this kind of decentralisation does not solve the case of challenged networks, because the authorities still need to be available for key issuance.

While ABE maps the read access check onto the ability to decrypt, it does not integrate attribute claim verification for the object producers, i.e., one cannot verify whether a subject producing an object actually possesses the attributes they claim to have. Attribute-based signature (ABS) [10] can solve this problem, by relying on an authority to issue private keys that confirm the signing subject has the claimed attributes.

Alternative approaches rely on distributed consensus mechanisms. For instance, Blockmesh [11] enforces trust and security in fragmented mesh networks by building on blockchain principles. Another work [12] extended the BATMAN protocol with a blockchain-based trust framework, improving Byzantine Fault Tolerance, and thus security, in MANETs.

In this paper, we propose an architecture that reuses the delegation and revocation of P&M's, while addressing decentralisation by distributing the TM on every entity, and using ABS to certify the subjects' claimed attributes, and adapting the whole to MANETs.

III. D3CS ARCHITECTURE

The proposed D3CS architecture (Figure 1) defines the interactions between the system entities (authority, subject, trusted mediator) through primitives that enable DCS. These interactions then translate into a lightweight protocol at the network layer.

A. Architecture overview: entities

The D3CS architecture defines three kinds of entities. The *Authority* is responsible for managing ABE and ABS master keys from which subjects private keys are derived. The *subject* can label, encrypt, and share data to be decrypted by other authorised subjects (i.e., with the right attributes). The *trusted mediator* (TM), inherited from P&M, is an entity, distributed on each subject or authority, that executes the first decryption step with the PSKA to enact revocation. We assume that each distributed TM is securely isolated from the subject and its operating system, so that its cryptographic material and internal operations cannot be accessed or altered by the user. This isolation could, for instance, be implemented by deploying the TM within a secure element. A compromise of a TM may affect the security guarantees provided by this local instance, but does not compromise the other TMs. Each TM securely stores its own cryptographic material.

B. D3CS primitives: cryptographic features

Our D3CS system relies on six mechanisms to allow interactions between the entities. First, to initialise system parameters and generate the master key, which is required to generate ABE and ABS private keys, the authority must be *setup* (A). Then, *key generation* (B) is performed by the authority upon a subject's key request. If the authority is not available, a subject can request a private key by *delegation* (C). Like P&M, delegation is only possible if the delegator's set of attributes includes the delegatee's attributes. Once subjects have received their private keys, they can label, encrypt and share data. *Encryption* (D) is based on ABE, but it must first be validated by the TM with ABS signature verification to ensure that the claimed attributes match the ones used in the

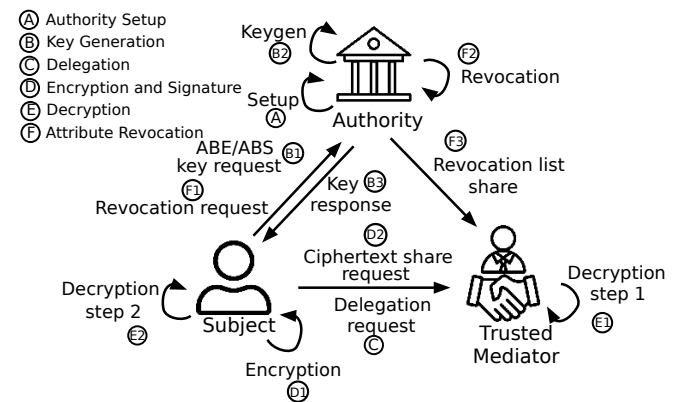


Fig. 1. D3CS architecture overview and interactions between the entities.

object policy. *Decryption* (E) is a two-step process following P&M's scheme. A first step is performed by the TM. The second step is performed by the subject, in order to access the data. Finally, *attribute revocation* (F) is managed by the authority by adding an attribute on the attribute revocation list (ARL). The ARL is replicated on each TM, and is checked by the TM before any D3CS operation (B,C,D,E).

C. D3CS protocol: network layer

The D3CS framework is designed to be network-agnostic, provided that the network layer offers communication primitives through a *network service* to send D3CS messages to the distributed instances of TM (broadcast) or to a specific subject or TM instance or the authority (unicast). In order to implement the previously described D3CS primitives, we propose a protocol relying on different packet types. In the following, we focus on step (B), the key distribution which is essential to enable DCS.

Figure 2 illustrates this step and the role of the distributed TM in a multi-hops scenario. When S3 tries to join the D3CS system, S1 acts as a relay while S2 and the authority can both provide keys for S3, either via authority or via delegation. First, a *KEY_REQUEST* is broadcasted by S3 (the joining subject) in order to ask for ABE and ABS keys. If the authority is available, it will respond with two *KEY_RESPONSE* messages: one for S3 containing the PSKS, one for their TM instance with the PSKA as payload. Other subjects, for instance S2 in Figure 2, can respond with a *DELEGATION_OFFER* message, provided that their attributes allow for a delegation. *DELEGATION_OFFER* are ignored as soon as a *KEY_RESPONSE* is received. Otherwise, if no *KEY_RESPONSE* is issued by the authority, S3 will accept the offer and send a *DELEGATION_ACCEPT* message back to the delegator (S2 in our example). The delegator will then perform a delegation operation and send the keys via a *KEY_RESPONSE*. *KEY_RESPONSE* messages are protected by asymmetric encryption, in order to preserve the confidentiality of the keys, using S3's public key that was previously transferred in the *KEY_REQUEST* payload.

Then, once subjects and their TMs have their PSKS/PSKA pairs of keys, *CT_SHARE* messages are used to carry D3CS encrypted data between subjects. Eventually, upon attribute revocation, the updated ARL is shared with all TMs using a broadcasted *ARL_UPDATE* message.

IV. DEMONSTRATION IN AN OPPORTUNISTIC NETWORK

In order to demonstrate the feasibility of our solution, we developed a proof-of-concept demonstrator to run the D3CS architecture on an opportunistic network, as depicted in Figure 3. We used a network emulation platform to test, and validate qualitatively, each D3CS feature under varying connectivity conditions representative of challenged networks.

A. D3CS proof-of-concept implementation

We implemented the core D3CS components, i.e. the cryptographic primitives and the distributed TM, in a prototype

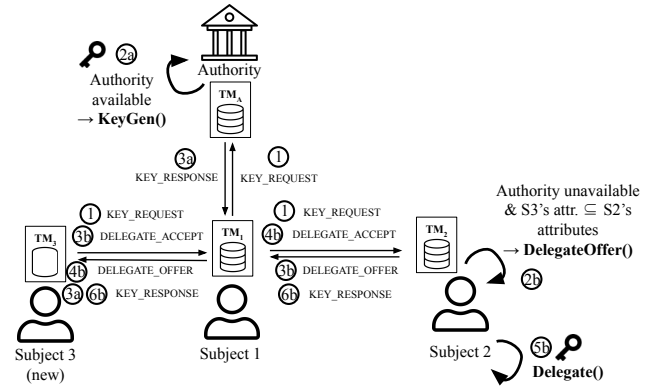


Fig. 2. Distributed TMs handling the multi-hop key request of a new subject.

written in RUST. Cryptographic functions rely on P&M's CP-ABE [6] and Li and Kim [13] ABS primitives.

The NetworkService abstraction provides the network-agnostic interface for the communications. In the proof-of-concept, the NetworkService is operationalised using the DoD-WAN (Document Dissemination in Wireless Ad hoc Networks) [14] open-source middleware¹. DoD-WAN implements an opportunistic networking protocol and provides a network API [15] to the application layer. Opportunistic networking is a commonly accepted solution to tackle challenged networks by enabling disruption-tolerant multi-hop communications. DoD-WAN is based on a store-carry-forward mechanism, where received messages are stored in a local cache and then opportunistically disseminated to other nodes. It follows a publish/subscribe model in which messages are published (i.e., disseminated) on topics, and delivered to the nodes whose subscriptions match the topics. To implement the communication primitives of the network layer (see subsection III-C), specific topics are used for broadcasting within the distributed TM while unicast messages use one topic per entity.

The code developed for this proof-of-concept is available on a public repository.²

B. Demonstration with LEPTON emulation platform

Initial tests of the D3CS prototype implementation were carried out on two computers connected to a WLAN to confirm the correct operation of the D3CS architecture. Yet, in order to test more complex scenarios and network topologies involving connectivity loss or multi-hop delegation, simulation

¹DoD-WAN, <https://casa-irisa.univ-ubs.fr/dodwan/>

²D3CS implementation, <https://gitlab.inria.fr/elemonni/d3cs-prototype>

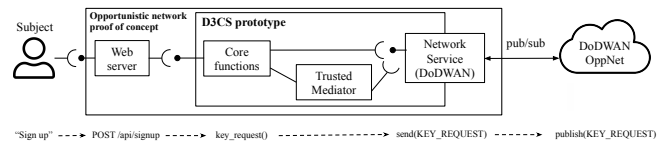


Fig. 3. D3CS proof-of-concept architecture.

tools are required to provide an easily configurable network layer. LEPTON [16] is an emulation platform, designed to emulate a mobile network by managing the connectivity of nodes running actual code (i.e., from the network layer to the application layer). Systems and protocols can therefore be tested in almost actual conditions, in real-time. Moreover, a LEPTON adapter for DoD WAN nodes is already available, and LEPTON features a visual tool that represents the network behaviour as a time-varying graph. For these reasons, we used LEPTON to demonstrate our D3CS implementation in a variety of connectivity and mobility scenarios.

The demonstration setup is composed of 10 nodes representing the authority and nine subjects. LEPTON allowed us to test the D3CS features through different scenarios. LEPTON let us observe the behavior of D3CS in a multihop instable network, in the presence of controlled disconnections, which are representative of challenged networks. An execution was recorded³, showing that the D3CS prototype successfully delivered DCS capabilities, dynamically and in a decentralised way, within a network mimicking challenged networks.

First, we confirm that D3CS behaves at least as well as the P&M baseline. When the authority is reachable by the subjects through the network, key generation upon inclusion of a new subject, encryption, decryption and revocation proceed nominally, evidenced by the recorded execution.

When the authority is not reachable by the subjects, for instance due to network partitioning, the delegation mechanism takes in charge the key generation. Still, DoD WAN keeps the KEY_REQUEST message of the new subject in the caches of the nodes. When the dynamics of the networks reconnect the authority to a node with this message in its cache, the KEY_REQUEST is delivered to the authority, which issues a non-delegated key, including the ABS key that the delegator is unable to issue. The subsequent multihop configuration of the demonstration illustrates that the joining subject ignores the delegated keys when it receives the key from the authority.

The next sequence of the demonstration illustrates the behavior of D3CS when revocation occurs while the network is partitioned. For instance, a delegator disconnected from the authority does not receive ARL updates, and would therefore accept to delegate its key to a delegatee. The subjects that are isolated from the authority can encrypt and decrypt data in such a way that violates the revocation: indeed, their respective TM instances do not know yet the newest revocation list. Revocation can hardly do better than accepting transient ARL inconsistency when we want to tolerate network partitioning and to replicate the ARL for availability purpose. But, as soon as the network reconnects, the ARL is propagated to the TM instances, which start rejecting decryption accordingly.

V. CONCLUSION

Data-centric security (DCS) is a novel approach that consists in embedding security in the data itself, which alleviates the security burden on the network layer. DCS-protected information

could in theory transit on public network channels. DCS solutions are however mainly centralised and do not cope well with network fragmentation and connectivity disruptions which are inherent to challenging infrastructure-less environments such as tactical networks or post-disaster emergency networks. In this paper, we presented a dynamic and decentralised data-centric security (D3CS) architecture that addresses this issue through delegation among other mechanisms. The architecture was evaluated on an opportunistic network, which constitutes a dynamic and partially connected setting, to assess the behaviour of the different D3CS primitives. The first tests yielded promising results and more tests are planned to measure the performance and the scalability of the D3CS solution.

REFERENCES

- [1] K. Wrona, "Towards data-centric security for NATO operations," in *International Conference on Digital Transformation, Cyber Security and Resilience*. Springer, 2020, pp. 75–92.
- [2] J. Bayuk, "Data-centric security," *Computer Fraud & Security*, 2009.
- [3] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to Attribute Based Access Control Definition and Considerations," National Institute of Standards and Technology, Tech. Rep. NIST SP 800-162, 2014.
- [4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology—EUROCRYPT: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 5 2005, pp. 457–473.
- [5] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST, Tech. Rep., 2020.
- [6] S. Porwal and S. Mittal, "A fully flexible key delegation mechanism with efficient fine-grained access control in CP-ABE," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 9, pp. 12 837–12 856, 2023.
- [7] A. Baudet, O.-E.-K. Aktouf, A. Mercier, and P. Elbaz-Vincent, "Decentralized public key infrastructure for autonomous embedded systems," *Proceedings of the 29th C&ESAR*, vol. vol. 99, 2022.
- [8] K. Mrabet, F. E. Bouanani, and H. Ben-Azza, "Generalized Secure and Dynamic Decentralized Reputation System With a Dishonest Majority," *IEEE Access*, vol. 11, pp. 9368–9388, 2023.
- [9] Y.-Q. Yao, Y.-J. Zhang, Z.-Y. Liu, Y.-X. Wang, X.-Y. Tan, and Z. Zhai, "Traceable and revocable multi-authority ABE supporting decryption outsourcing and policy update for cloud data access control," *Frontiers of Computer Science*, vol. 20, no. 4, p. 2004805, Apr. 2026.
- [10] J. Li and K. Kim, "Hidden attribute-based signatures without anonymity revocation," *Information Sciences*, vol. 180, no. 9, pp. 1681–1689, 2010. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0020025510000186>
- [11] J. Luo and A. Velazquez, "Blockmesh data security and trust framework for tactical networks," in *MILCOM 2024-2024 IEEE Military Communications Conference (MILCOM)*. IEEE, 2024, pp. 536–541.
- [12] U. Singh, S. K. Sharma, M. Shukla, and P. Jha, "Blockchain-based batman protocol using mobile ad hoc network (manet) with an ensemble algorithm," *Int. J. Inf. Secur.*, vol. 23, no. 3, p. 1667–1677, Jan. 2024. [Online]. Available: <https://doi.org/10.1007/s10207-023-00804-w>
- [13] J. Li and K. Kim, "Hidden attribute-based signatures without anonymity revocation," *Information Sciences*, vol. 180, no. 9, pp. 1681–1689, 2010.
- [14] J. Haillot and F. Guidec, "A Protocol for Content-Based Communication in Disconnected Mobile Ad Hoc Networks," *Journal of Mobile Information Systems*, vol. 6, no. 2, pp. 123–154, 2010.
- [15] F. Guidec, Y. Mahéo, P. Launay, L. Tousseau, and C. Noûs, "Bringing Opportunistic Networking to Smartphones: a Pragmatic Approach," in *45th Computers, Software, and Applications Conference (COMPSAC)*. Madrid, Spain: IEEE, July 2021, pp. 574–579.
- [16] A. Sánchez-Carmona, F. Guidec, P. Launay, Y. Mahéo, and S. Robles, "Filling in the missing link between simulation and application in opportunistic networking," *Journal of Systems and Software*, vol. 142, pp. 57–72, August 2018.

³<https://gitlab.inria.fr/elemonni/d3cs-prototype/-/blob/main/d3cs.mp4>