Computer Networks 121 (2017) 37–52

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

SPARTA: A survival performance degradation framework for identity federations

Ricardo Macedo[a,*], Leonardo Melniski[a], Aldri Santos[a], Yacine Ghamri-Doudane[b], Michele Nogueira[a]

[a] NR2 - Federal University of Paraná, Curitiba, PR, Brazil Brazil
[b] L3i - University of La Rochelle, La Rochelle CEDEX 1, France

ARTICLE INFO

Article history:
Received 18 March 2016
Revised 18 February 2017
Accepted 7 April 2017
Available online 12 April 2017

Keywords:
Performance degradation
Identity federations
Survivability

ABSTRACT

Identity federations simplify user's access control across different networks, domains or systems. These federations allow users to seamlessly access data from another domain and they avoid the need of a completely redundant user administration. Federations rely on Identity Providers (IdPs) to manage user's identities. However, IdPs are prone to Distributed Denial-of-Service (DDoS) attacks and flash crowd events. Those attacks and events can severely compromise the performance of IdPs, affecting legitimate users. Existing solutions either ignore such events, statically improving the performance of only specific IdP operations, or tolerate a predetermined number of failures, employing extra hardware resources purchased to replicate IdPs services. This article presents SPARTA, a Survival Performance degrAdation fRamework for idenTity federAtions. SPARTA offers identity federation survivability employing the collective intelligence principles. We showcase the framework over a real identity management system. Results from the experiments show the improvements of the system under attacks. We measure improvements by identity authentication latency (i.e., the time interval between the authentication request and its response) and throughput. As future works, we intend to evaluate our solution using large-scale identity federations.

1. Introduction

Wireless networks offer services with the potential to significantly improve people's quality of life. Those networks must manage the service access of a large number of users and devices. These users and devices can freely move across domains, increasing the complexity of the management [1–3]. The identity federation model intends to assist this management. It integrates different administrative domains, preserving local policies and technologies [4]. Identity federations separate resource provisioning service from user management. Hence, federations count on three entities Identity Providers (IdP), Service Providers (SP) and Embedded Discovery Service (EDS) [5]. IdPs manage user's identities. SPs offer services for users, such as Web applications. EDS provides a web interface allowing a user to select which IdP they will use when accessing a SP. The federation simplifies the access in mutiple domains to an authenticated user have access. Once authenticated in a IdP, the user can access services from different SPs. This reduces the management complexity and improves user experience [6].

IdPs are accessible over the Internet. Consequently, they are prone to Distributed Denial-of-Services (DDoS) attacks [7] and flash crowds events. DDoS flooding attacks generate a large number of malicious requests to overload or exhaust hardware capacity. This forces IdPs to consume all memory and processing capacity, which results in service unavailability [8]. A flash crowd event is a sudden increase in simultaneous service requests issued by legitimate users, resulting in low system performance [9]. IdPs have limited memory and processing resources that can be exhausted by a large number of requests. In Identity Management (IdM) systems, an IdP overload can decrease the performance of identification and authentication operations or make them unavailable to legitimate users, thereby impacting service provisioning.

We classify approaches to avoid performance degradation in IdP operations as: (*i*) improvement of identity management operations at large scale [10–13] and (*ii*) failure-tolerance based [5,14,15]. However, the former does not consider DDoS overloads or flash crowds events. The latter tolerate failures up to a pre-established threshold. In other contexts, research interest in survivability has appeared as a promising solution against unexpected attacks

* Corresponding author at: Department of Informatic, Rua Cel. Francisco H. dos Santos, 100 - Centro Politécnico - Jardim das, 81531980 Curitiba, Brazil.
E-mail address: rmacedo@inf.ufsm.br (R. Macedo).

http://dx.doi.org/10.1016/j.comnet.2017.04.033
1389-1286/

[16–18]. Such research has targeted the management of emergent threats, thereby enabling systems to learn and incorporate lessons about the improvement of resistance, recognition, and recovery through adaptation strategies. Thus, survivability of IdP operations remains unexplored.

This work presents a **S**urvival **P**erformance degr**A**dation f**R**amework for iden**T**ity feder**A**tions (SPARTA). To the best of our knowledge, SPARTA is the first framework that promotes identity federation survivability. Hence, SPARTA employs the collective intelligence principle to learn and incorporate lessons about performance degradation. The framework considers primary IdP operations, such as identification, authentication and attribute provision, as essential services from the identity federation, as suggested in the literature [8,14,19]. The SPARTA framework comprises *survival, collaboration*, and *analysis* modules. The survival module can employ different techniques to attain resistance, recognition, recovery, and adaptation of essential services against performance degradation. The collaboration module promotes interaction among IdPs for sharing information about the status of the whole identity federation. It follows the principle of collective intelligence that comprise a form of universally-distributed intelligence that can be constantly improved and coordinated in real time [20]. The analysis module uses shared information to improve the adaptation of essential identity federation services. Following the SPARTA modules, the identity federation can survive to emergent performance degradation events using the collective intelligence of its components, differently from solutions in the literature that tolerate a predetermined number of failures or ignore them.

We have conducted experimental performance evaluations using the framework. A scheme and a tool showcase the framework. The *MoniOptimize* tool employs the framework reorganization concept. Performance evaluations have employed a locally-controlled environment and a real testbed from the Brazilian identity federation. Results show that the tool improved the utilization of federation resources. It increases throughput and decreases authentication latency for both malicious and legitimate requests.

Our major contributions are:

- SPARTA, a framework to provide survivability for identity federations against performance degradations. It employs collective intelligence concept. This framework consists in a full solution to protect, identify, recover and adapt identity federation essential services (IdP operations of identification, authentication, and attribute provisioning) against DDoS attacks and flash crowd events.
- SAMOS, a scheme to mitigate DDoS attacks showcasing the SPARTA framework. The scheme has evolved from different work [8,19,21].
- A tool following the SPARTA framework concepts and its evaluation using a real testbed. We have conducted performance evaluations in the Brazilian IdM CAFe federation. The federation is distributed among different Brazilian States. The results show that the tool improves the latency and throughput of authentications workloads.

This article proceeds as follows. Section 2 describes the related works. Section 3 presents the SPARTA framework. Section 4 showcases the framework concept in a scheme for DDoS attacks mitigation on identity management systems. Section 5 details the experimental performance evaluation. Section 6 concludes the article.

2. Related work

In the last decade, the interest in scalable IdM systems has increased. Initially, the Internet offered services to a small number of users. Across time, the advent of the Web and the increasing number of mobile devices have resulted in high demand to provide services and assist users at a large scale. The new context impacted the management of user's accounts, increasing complexity and demanding more from hardware resources. This also generated the necessity to execute these operations as quickly as possible.

Many studies have attempted to improve the performance of IdM operations at a large scale. Preuveneers and Joosen [10] proposed a scalable framework for context-aware authentication. They employed machine learning techniques to decrease the cost of interactions among users and authentication authorities. Méndez et al. [11] presented a more efficient for providing the single sign-on, *i.e.* a method for authenticating users in heterogeneous computing environment, at large scale. Blazquez et al. [12] analyzed the impact of the OpenID, *i.e.* a protocol that implements the single sign-on method, in providing IdM services to the Internet of Things. *Chard* Chard et al. described an architecture for improving the performance of accounts management user, exploring database techniques [13]. However, these approaches do not consider overloaded scenarios resulting from DDoS attacks or flash crowd events.

The DDoS attacks against clients of Internet Service Provider (ISP) have also attracted attention of the scientific community. Fayaz et al. [22] proposed the Bohatei system to defend ISP consumers providing flexibility and elasticity against DDoS attacks. Bohatei system comprises of four steps. The first identifies the attack through anomaly detection techniques. The second estimates the volume of the suspicious traffic. The third locates virtual machines to process the malicious traffic. The last one configures roles to forward the traffic to virtual machines. The Bohatei's authors assume ISPs equipped with pre-defined libraries to offer the defense strategy against DDoS attacks. However, this approach depends on an intrusion detection system that in general is prone to high rates of false negatives and/or false positives [23].

Other studies have presented failure-tolerant-based solutions to mitigate the effects of DDoS attacks on IdPs. Generally, these studies apply replicas, *i.e.* many instances of the same service, for responding to requests in case of failures or overload by employing external computational resources. Barreto *et al.* presented an intrusion-tolerant IdM infrastructure that uses replication and shared memory [5]. Kreutz *et al.* presented an architecture to make IdPs resilient to arbitrary failures through replication techniques. The architecture can tolerate a predetermined number of failures [14]. Modern IdM frameworks, such as *Shibboleth*, implement IdP clustering feature, where each cluster member acts as a replica [15]. However, these approaches are designed to tolerate only a predetermined number of failures.

Research interest in survivability has appeared in other contexts inspiring approaches against new kind of threats and attacks [16–18]. These approaches adapt the system essential services improving mechanisms of resistance, recognition, and recovery. By the adaptation, the system learn and incorporate lessons about emergent threats and attacks, becoming more reliable. Nogueira et al. [16] presented an architecture to provide essential services on ad hoc and mesh networks under attacks, intrusions and failures. Deshpande et al. [17] presented an architecture that provides survivability for *vetronics, i.e.* electronics vehicles equipped with connected systems, in case of threats and attacks in the military domain. Mehresh and Upadhyaya [18] proposed a architecture to provide survivability against the manipulation of exchanged data among distributed systems components. However, such approaches are designed following specific contexts that differ from IdM.

Recently, the collective intelligence concept has emerged as a new perspective to represent a universal kind of intelligence [20,24–26]. This has motivated innovative designs for complex and self-organized systems. Pierre Lévy defined collective intelligence as a form of universally-distributed intelligence that can be constantly improved and coordinated in real time and results