Journal of Network and Computer Applications 63 (2016) 173–189

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

A cyber-resilient architecture for critical security services ☆

Diego Kreutz [a,b,*], Oleksandr Malichevskyy [b], Eduardo Feitosa [c], Hugo Cunha [c], Rodrigo da Rosa Righi [d], Douglas D.J. de Macedo [e]

[a] SnT/University of Luxembourg, Luxembourg
[b] LaSIGE/FCUL, Portugal
[c] IComp/UFAM, Manaus, Brazil
[d] UNISINOS, São Leopoldo, Brazil
[e] UFS, Aracaju, Brazil

ARTICLE INFO

Article history:
Received 28 December 2014
Received in revised form
26 July 2015
Accepted 11 September 2015
Available online 11 February 2016

Keywords:
Cyber resiliency
Cyber security
System design
Fault and intrusion tolerance
Identification and authentication services
Network access control

ABSTRACT

Authentication and authorization are two of the most important services for any IT infrastructure. Taking into account the current state of affairs of cyber warfare, the security and dependability of such services is a first class priority. For instance, the correct and continuous operation of identity providers (e.g., OpenID) and authentication, authorization and accounting services (e.g., RADIUS) is essential for all sorts of systems and infrastructures. As a step towards this direction, we introduce a functional architecture and system design artifacts for prototyping fault- and intrusion-tolerant identification and authentication services. The feasibility and applicability of the proposed elements are evaluated through two distinct prototypes. Our findings indicate that building and deploying resilient and reliable critical services is an achievable goal through a set of system design artifacts based on well-established concepts in the fields of security and dependability. Additionally, we provide an extensive evaluation of both resilient RADIUS (R-RADIUS) and OpenID (R-OpenID) prototypes. We show that our solution makes services resilient against attacks without affecting their correct operation. Our results also pinpoint that the prototypes are capable of meeting the needs of small to large-scale systems (e.g., IT infrastructures with 800k to 10M users).

1. Introduction

The growth and criticality of Authentication and Authorization Infrastructures (AAIs) is directly related to the fact that users are nowadays allowed to transparently access different services (e.g., Facebook, Google, Twitter, and Amazon), as well as federated network infrastructures (e.g., *eduroam* TERENA Task Force on Mobility, 2011), with a single credential or authentication session. While this is of great value for the users, fostering seamless mobility and simplicity, it also poses new challenges and concerns from a security and dependability point of view. This means that failures on the authentication and authorization services can achieve catastrophic levels. These services rely on Identity Providers (IdPs) or Authentication, Authorization, and Accounting (AAA) protocols to identify and authenticate the user before granting him access to the requested resources or services. OpenID (Recordon and Reed, 2006) and RADIUS (Rigney et al., 2000) are examples of such services, which are widely deployed in enterprise IT infrastructures.

Despite the importance of AAIs for IT infrastructures and systems such as clouds, virtual networks and e-commerce, there are still open questions regarding their availability and reliability. This reality is supported by recent investigations that pinpoint the fact that digital attacks and data breach incidents are growing at a fast pace (Verizon RISK Team, 2013; IBM Security Systems, 2013; McAfee Labs, 2013; Verizon, 2015). For instance, advanced persistent threats (Tankard, 2011) are already classified among the most concerning threats of the World's current cyber warfare (European Commission, 2014; Delgado, 2014; Business, 2014). Even more alarming is the evidence of a growing trend in the number and frequency of targeted attacks in the next few years (McAfee Labs, 2013; Lee and Rotoloni, 2014; SyndiGate.info, 2014; TrendLabs, 2014). As a result, cyber security is arguably becoming a global first class priority for academy, industry and governments

☆This paper is an extended version of our previous paper “System Design Artifacts for Resilient Identification and Authentication Infrastructures” (Kreutz et al., 2014c), which has received a Best Paper Award from the International Academy, Research, and Industry Association.

* Corresponding author. Tel.: +352 46 66 44 5242.

E-mail addresses: diego.kreutz@uni.lu, kreutz@computer.org (D. Kreutz), olexmal@lasige.di.fc.ul.pt (O. Malichevskyy), efeitosa@icomp.ufam.edu.br (E. Feitosa), hugo.cunha@icomp.ufam.edu.br (H. Cunha), rrrighi@unisinos.br (R. da Rosa Righi), dmacedo@ufs.br (D.D.J. de Macedo).

http://dx.doi.org/10.1016/j.jnca.2015.09.014
1084-8045/© 2016 Elsevier Ltd. All rights reserved.

(Lee and Rotoloni, 2014; Whitehouse News, 2014; European Commission, 2014; Moteff, 2014; Johnson et al., 2014).

It is also worth emphasizing, as it has already been stated by research initiatives, security agencies and governments, that security is not anymore only about detecting and preventing, but rather about resiliency, i.e., maintaining the correct operation of systems in adverse circumstances, such as advanced attacks and intrusions (Verissimo et al., 2006; BOYD, 2014; Whitehouse News, 2014; Goche and Gouveia, 2014; O'Rourke, 2009). Some agencies and IT experts are even coining the term “cyber resiliency” (BOYD, 2014; Goche and Gouveia, 2014) as the new norm, instead of cyber security.

The vast majority of critical infrastructures, as well as other systems, rely on AAIs. However, commonly deployed authentication and authorization services, such as RADIUS and OpenID, are still far from being cyber-resilient, i.e., capable of ensuring essential properties such as confidentiality, integrity, and high availability (Niedermayer et al., 2014; Kreutz et al., 2014b; Kreutz and Feitosa, 2014). This can also be observed in the services' online documentation and deployment recommendations (FreeRADIUS, 2012; RADIUS Partnerships, 2008; Juniper Networks, 2010; OpenID, 2010; Clamshell, 2013). Only a few implementations provide basic mechanisms to improve the service's reliability and robustness, such as SSL communications and simple replication schemes to avoid eavesdropping and tolerate crash failures, respectively. This scenario is arguably an open avenue for further research with the ultimate goal of designing and deploying cyber-resilient systems, i.e., capable of dealing with new threats and cyber attacks posed by the current state of cyber warfare.

To best of our knowledge, this paper proposes the first set of system design artifacts and functional architecture for designing, implementing and deploying cyber-resilient AAI architectures. Differently from the existing solutions that provide mostly ad hoc and system-specific repairs (Bau and Mitchell, 2011), making it unclear whether the solution can be applied to solve similar problems in other systems, we propose and evaluate an architecture and system design artifacts that can be reused in a systematic way to solve similar problems in other systems or domains. In order to demonstrate the feasibility and applicability of the proposed system components, we implemented and thoroughly evaluated two distinct prototypes: R-RADIUS and R-OpenID.

Considering the current state of the art, our main contribution is fivefold: (a) the definition of an architecture and essential system design artifacts for building secure and dependable authentication and authorization infrastructures, (b) a step-by-step design and discussion of a resilient architecture for AAIs using as reference two use cases, RADIUS and OpenID, (c) trusted components for ensuring the confidentiality of sensitive data stored in replicated systems subject to malicious faults, (d) experimental evaluation in three different environments, demonstrating that multi-infrastructure deployments (e.g., data centers, clouds) can help to increase the robustness of systems against first class attacks such as large scale DDoS attacks, and (e) higher levels of security and resiliency for AAIs without impairing either the performance (e.g., support 800K users) or the costs (e.g., without requiring huge amounts of computing resources).

The next section introduces the concepts and main motivation of this research. Following, in Section 3 we describe the functional elements and system design artifacts to develop robust and reliable AAI services. In Section 4 some of the deployment scenarios, issues and challenges are analyzed. The implementation of the two prototypes, R-RADIUS and R-OpenID, is discussed in Section 5. Section 6 provides an extensive evaluation with results and discussions regarding throughput, latency, the behavior of the system under faults and attacks, and a security analysis. Lastly, in Sections 7 and 8 we provide an overview of related work and the final remarks.

2. Concepts and state of affairs

AAI solutions are often based on protocols like OpenID and RADIUS (Lutz and Stiller, 2013; Kisin, 2013; Do et al., 2013; Kreutz et al., 2013a). However, both the protocol specification and implementations lack features for providing robust security (e.g., strong confidentiality) and dependability (e.g., high availability), being frequent target of attacks and data theft attempts (e.g., user credentials). We start with the basic concepts of each protocol and then we delve into further details and a discussion regarding their main weaknesses.

OpenID is a framework to build identity providers (Recordon and Reed, 2006). It is based on open Hypertext Transfer Protocol (HTTP) standards, which are used to describe how users can authenticate on third party services through their own IdP. There are two main advantages of this approach. First, it allows identification and authentication protocols to be transported over standard Web protocols. Second, users need only one single credential to access different services provided that service providers accept external IdPs.

RADIUS is an AAA protocol (Rigney et al., 2000) commonly used in corporate and carrier grade networks. The authentication verifies the user identity before granting him access to the network or service. Authorization is used to determine which actions a user can perform after a successful authentication. Finally, accounting provides methods for collecting data about the network or service usage. The collected data can be used for billing, reporting and traffic accounting.

2.1. Vulnerability assessment of RADIUS and OpenID

RADIUS and OpenID have different weaknesses regarding security and dependability (Sun et al., 2012; Kreutz et al., 2013a, 2014c,b), as summarized in Table 1. Current implementations and deployments are highly susceptible to: (i) common vulnerabilities in different parts of the IT stack; (ii) sensitive data leakage due to the fact that keys and certificates are commonly stored in the operating system's file system; and (iii) resource depletion attacks if the VMs are deployed on the same physical server with current virtualization technologies such as the Xen (Kreutz and Feitosa, 2014; Kreutz et al., 2014a) and the KVM hypervisors (see resource depletion attacks in Section 6).

Figures 1 and 2 illustrate the traditional architectures of RADIUS- and OpenID-based services. From a security and dependability point of view, there are several single points of failure on traditional deployments, such as the RADIUS server, the MySQL back-end, the OpenID server and the LDAP back-end.

In order to tolerate simple crash faults, both services use multiple instances and a cluster of back-end services as illustrated

Table 1
Vulnerabilities and properties (Kreutz and Feitosa, 2014; Kreutz et al., 2014a).

Vulnerability/support	RADIUS	OpenID
Tolerates crash faults (using back-end clusters)	Yes	Yes
Tolerates arbitrary faults	No	No
Tolerates infrastructure outages	No	No
Tolerates DDoS attacks	No	No
Risk of common vulnerabilities	High	High
Risk of sensitive data leakage	High	High
Diverse security-related vulnerabilities	Yes	Yes
Susceptible to resource depletion attacks	Yes	Yes