

Securing the Madeira Network Management System

Ricardo Marín^{#1}, Julio Vivero^{#2}, Philipp Leitner^{*3}, Andreas Neppach^{*4}, Martin Zach^{*5}, David Ortega^{°6},
Bertrand Baesjou^{°7}, Pablo Arozarena^{°8}

[#]GMV-SGI

Balmes, 268-270, 5, 08006 Barcelona, Spain

{¹rmarin,²jvivero}@gmv.com

^{*}Siemens AG Austria – PSE

Siemenstrasse,92 A-1210 Vienna, Austria

{³philipp.leitner,⁴andreas.neppach,⁵martin.zach}@siemens.com

[°]Telefonica I+D

Emilio Vargas, 6, 28043 Madrid, Spain

{⁶doa,⁷baesjou,⁸pablo}@tid.es

Abstract: In the research project Madeira a meshed network management system based on Peer-to-Peer (P2P) technologies was developed. Up to now, security has always been neglected in this field of research despite the sensitivity of such systems and the high number of security threats that affect them. Madeira incorporates a security solution aimed at minimizing the higher priority risks on all levels. The solution employed in the Madeira project introduces a distributed certification authority based on threshold cryptography, certificate revocation list distribution points and a collaborative accusation protocol aimed at uncovering hosts that exhibit illegal or unwanted behaviour while avoiding false accusations by malicious nodes.

1. INTRODUCTION

The Celtic Madeira project [1] proposes a novel approach to management of meshed and ad-hoc networks [2]. The Madeira management system exploits the inherent capabilities of the Peer to Peer (P2P) paradigm to address the dynamism and self-management characteristics of this kind of networks.

Madeira peers (Madeira Distributed Management system elements or MDMs) automatically self-organize in a logical hierarchy of clusters. At bootstrap, an MDM either joins an existing lower-level cluster or creates a new one (depending on a number of parameters such as the maximum cluster size). Within each cluster an MDM is elected as cluster head. Then, at nth level cluster heads are grouped in clusters at level n-1, and cluster heads are elected also in these n-1 level clusters. This process is iterative until we have a single top-level (level 0) cluster head.

The rationale behind this hierarchy of clusters in our P2P network is guaranteeing the scalability of the system by avoiding massive broadcasts that would otherwise compromise the performance of the network. Hence, the cluster heads behave as a path for management messages (e.g. alarms) to reach the whole infrastructure. This clustering is

completely dynamic and can be changed at any time if necessary.

Additionally, the top-level cluster head runs the Madeira NorthBound Interface (NBI). The NBI offers an interface based on Web Services [3] technology to external Operating Support Systems to manage the Madeira network from the outside.

From a security point of view, the Madeira system exhibits a number of challenges. There is a lack of authentication, confidentiality and data integrity in its communications that potentially allows a malicious entity to eavesdrop management messages (e.g. network topology information), modify messages, spoof the identity of a MDM node or Operation Support System, exchange forged management messages with other peers or respectively manage the network through the NBI. Each of these threats on its own forms a major and unacceptable risk for the whole management infrastructure, compromising its reliability, dependability, availability, privacy and trust.

The design of the Madeira security solution was kicked off after the Madeira Distributed Management system was fully designed and implemented, with the goal of addressing all of the above risks. Hence, the solution was strongly framed by the Madeira system design which delimited the scope of solutions applicable. The chosen base technologies for the solution are an X.509v3 [4] certificate infrastructure and the TLS protocol to provide a X.509v3 certificate-based authentication, confidentiality and integrity. Yet, a classic centralized X.509v3 Certificate Authority (CA) breaks the P2P approach taken in Madeira. Therefore, a distributed CA and Certificate Revocation List (CRL) has been introduced, enhancing both the availability of the CA and the scalability of the whole management system.

However, these measures alone are not enough since two significant security problems are still unaddressed in the Madeira infrastructure:

First of all, there is always the possibility that a “legal” MDM is compromised and an attack on the rest of the infrastructure can be launched from this compromised node. Though this possibility can never be completely eliminated, the Madeira Security system introduces some services aimed at preventing a compromise: Network Intrusion Prevention and Host Intrusion Detection services. Whenever a compromise attempt is detected, independently of whether it was successful or not, the Madeira Accusation Protocol is triggered to report the attack and take corresponding reactive measures.

The second problem roots in the Madeira cluster hierarchy approach. Since cluster heads provide the path for management messages to reach the whole infrastructure, a single malicious or faulty cluster head can block the dissemination of management messages throughout the network, causing serious reliability and availability problems. To avoid this problem, an Advertisement Service is defined that provides reliable multipath routing for management messages.

The rest of the paper is organized as follows: in section 2 a review of the relevant state of the art in P2P security is provided. Section 3 details all security services briefly introduced in the above paragraphs, and finally section 4 finalises the paper by summarizing the main conclusions drawn.

2. RELATED WORK

The distinguishing feature of Peer-to-Peer systems is the lack of a central management entity, which renders P2P systems scalable, fault tolerant and open. Unfortunately this feature also leads to severe security implications: without a central “trusted” entity that has full knowledge of the network it is hard to achieve an equivalent level of security to the one that is standard for client-server applications. The decentralized structure of P2P networks eases attacks on the integrity and security of the network.

Most research in the area of P2P security focuses on the idea of reputation and trust management. Well-known trust models for P2P systems include the Poblano model [5], which has been developed as part of the JXTA [6] P2P middleware, the PACE framework [7] and the reputation-based trust management system proposed by Selcuc et al. [8]. Similarly popular is the “Web of Trust” concept of Pretty Good Privacy [9]. Generally, these trust and reputation-based systems are unsuitable for Madeira for two reasons: Firstly, trust models are usually user-driven and Madeira is a completely automated system without any user interaction. Moreover, trust models are also content-driven, which is again not true for Madeira. Therefore, trust models have not been

considered suitable for building the Madeira security framework.

Another option to address the security challenges is falling back to a centralized security infrastructure as done in the Skype [10] VoIP service. Skype uses a standard RSA-based [11] public key infrastructure (PKI) to provide confidentiality and authentication. The Skype PKI uses a central certification authority (CA) that is controlled by the company behind Skype. The public key of this CA is hardcoded into the Skype software. The certificates are never refreshed. Clearly this central CA forms a single point of failure for the Skype service in general. This philosophy is contradictory with the Madeira focus. Therefore the use of a central CA has also been rejected for the Madeira platform.

A more interesting approach is implementing a distributed CA (dCA) as done in DICTATE [12] (Distributed Certification Authority with probabilistic freshness for Ad Hoc Networks). The general idea of DICTATE is to combine an offline Identification Authority (IA) and an online revocation authority (RA). The RA is implemented in a distributed fashion using threshold cryptography [13] (TC). Therefore the DICTATE system does not provide a single point of failure like a centralized system. However, DICTATE needs a lot of offline configuration to work (basically all IA tasks have to be carried out offline) which makes it inapplicable for Madeira. Yet the Madeira security framework will make use of some of DICTATEs baseline ideas, like the employment of TC to implement a physically distributed online certification authority.

3. MADEIRA SECURITY SYSTEM

Before starting with a detailed description of the important components that form the Madeira security system it is important to have in mind a couple of relevant assumptions taken in Madeira. First, end-user communications were defined to be out of scope for the Madeira project. Consequently, end-users of the Madeira managed network should use their own security mechanisms if they want to protect their data and communications. Second, within the research scope of the project a scenario is envisioned in which all MDM nodes belong to the same domain; hence there is no need for a trust model between operators.

Considering the above assumptions, Figure 1 depicts how the security services have been introduced within the Madeira system. At the lower layer, TLSv1 (with RSA, AES128 and SHA1 ciphersuite) is used to protect all communications of higher-level services. Node certificates are exchanged during the TLS handshake for authentication.

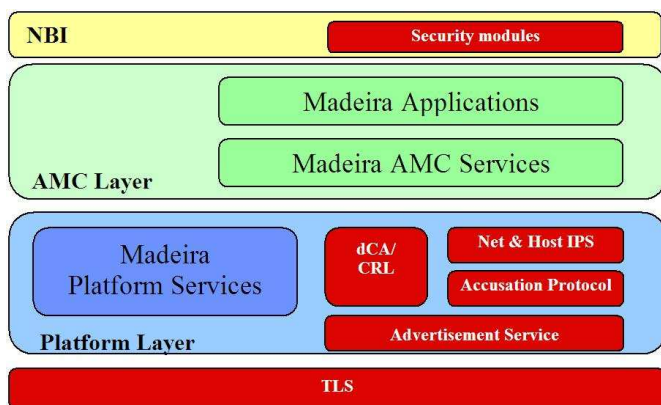


Figure 1 - Madeira security solution architecture

The Madeira platform layer provides basic services for the Madeira Distributed Management system (e.g. lifecycle, communication, neighbourhood information, grouping, ...).

The AMC layer provides, specific application modules (e.g. configuration or fault management modules) as well as services that support application modules functionality (e.g. logging service or policy-based management service).

The NBI provides a management interface for external Operation Support Systems.

In the following sections a detailed description of the security services (boxes with white text in red background in figure 1) included within Madeira is provided.

3.1 Advertisement Service.

The Advertisement Service (AS) is introduced to provide multipath message routing within the hierarchical cluster topology.

The need for multipath routing arises from the tree structure of the Madeira topology, resulting in inter-cluster communications to always be routed through the cluster heads. Hence, it would be very easy for a malicious cluster head to block all relevant messages (for instance certificate revocation requests).

The Advertisement Service algorithm provides a reliable multipath routing through the Madeira hierarchical topology and is detailed in Figure 2.

Simplifying, this algorithm broadcasts advertisements away from the sender until they reach the boundaries of the cluster. Hence, advertisements will follow as many different alternative paths as the number of clusters that borders the originating cluster.

To avoid infinite number of cluster internal broadcasts, advertisements include a Time to Live (TTL) parameter that is decremented in each hop within the source cluster. If the TTL parameter reaches zero, the message is dropped. The TTL parameter is not checked again once the message leaves the source cluster.

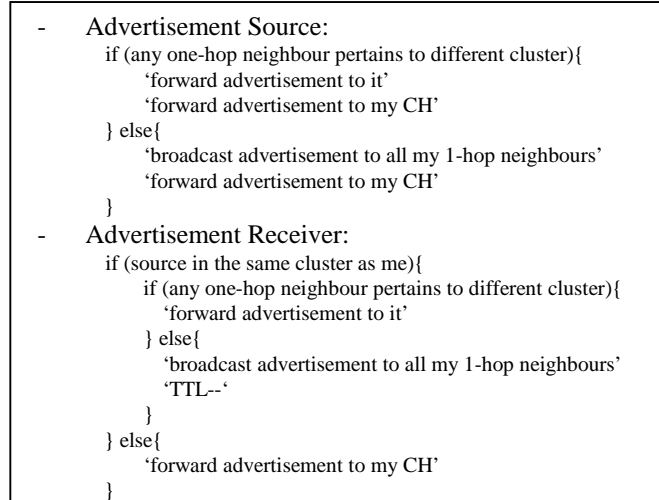


Figure 2 – Advertisement Service algorithm

3.2 Accusation protocol

The goal of the Accusation Protocol is to assure that malicious nodes are detected and neutralized while, at the same time, to protect legal nodes from being neutralized due to false accusations of malicious nodes.

Whenever a MDM detects an attack it sends a signed accusation message. Received accusations are stored by MDMs and counted. If the number of signed accusations from different MDMs reaches a specific threshold the neutralization action is requested, attaching all signed accusations as evidence. The neutralization action might consist on a certificate revocation request using the certificate revocation service described below or network-wide traffic dropping (for instance if the attacker does not even have a valid certificate).

In order to guarantee that the accusation is transmitted through multiple paths to the entire Madeira infrastructure the Accusation Protocol relies on the Advertisement Service to disseminate accusation messages.

3.3 Network and Host IDS

One of the new security services added to Madeira is a Network and Host Intrusion Detection System. Its goal is to detect and avoid attempts on compromising an MDM both from the network and from the host point of view. This service is uses well known IDS tools (i.e. SNORT [14] and AIDE [15]). These tools are integrated and customized to the particular needs of the Madeira system: whenever an intrusion attempt is detected, the accusation protocol is triggered.

3.4 Distributed Certificate Authority

The Madeira security solution uses X.509v3 certificates for authentication and session key establishment during the TLS handshake. Initial certificates are provided directly by the administrator, while most of the further tasks related to the certificate infrastructure, like renewing and revoking

certificates, are carried out by a distributed Certification Authority (dCA). This dCA is based on Threshold Cryptography (TC) and consists of a subset of Madeira peers (in the following called dCA members).

TC is grounded on the following principle: A $(n, k+1)$ TC scheme allows n parties to share the ability to perform a cryptographic operation (e.g. creating a digital signature), so that any $k + 1$ parties can perform this operation jointly, whereas it is infeasible for at most k parties to do so, even by collusion [16]. The dCA implemented for Madeira is independent of the underlying TC scheme, and can be used with each scheme that supports generation of RSA signatures in a distributed way. In our design shareholders have to *cooperate* in order to perform cryptographic operations (cp. [17], [18]).

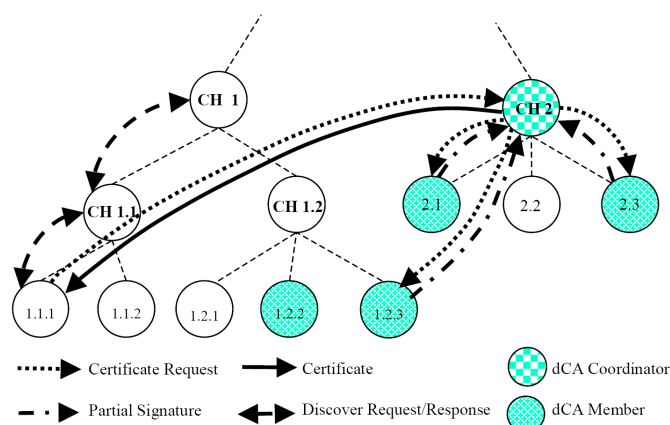


Figure 3 - dCA Certificate Request

The members of the dCA are advertised in the Madeira network using the Advertisement Service. To avoid distribution of false dCA IDs, all IDs are signed by the dCA private key. Additionally, dCA members can be identified using their certificate, which contains a dCA extension. To discover a dCA member, Madeira peers have to send a dCA discovery request by means of the Advertisement Service. With a growing number of peers in the network new dCA members will be required. These new dCA peers get a preinstalled list of known dCAs and introduce themselves to the existing dCA via the Advertisement Service.

Certification Requests. Due to certificate expiration and rekeying, Madeira certificates have to be updated in regular time intervals. This process is detailed in Figure 3. To update a certificate, a PKCS#10 [19] request is sent to a dCA member that initiates the certificate generation. For security reasons, certificate update requests must be sent before the existing certificate expires. This ensures that the requestor can be authenticated.

The dCA member that receives the PKCS#10 request acts as a coordinator for this certification process and arranges a certificate generation group (coalition). Participating dCA members are chosen randomly out of the list of known dCA

nodes. The coordinator sends an invitation together with the original PKCS#10 request to the chosen group. All invited peers check the request and the certificate of the requestor to avoid introduction of foreign peers using compromised dCA members. Additionally the certificate is checked against a recent certificate revocation list (CRL).

If all checks were successful the dCA nodes report their agreement to participate in the certificate generation to the coordinator and finally the list of participating dCA members is redistributed. Then, these dCA members generate partial signatures. These signatures are distributed to all participating shareholders that reconstruct and check the complete signature. If the signature can be reconstructed successfully the coordinator sends the new certificate to the certificate requestor.

3.5 Certificate Revocation List

The certificate revocation approach is based on the x.509v2 CRL extension profile [4]. The dCA is responsible for generating the signed CRLs which are stored at CRL distribution points. CRL distribution points are special dCA members which have the additional responsibility of storing CRL copies.

Certificate Revocation. A revocation request is transmitted to at least one dCA node which again acts as a coordinator (as above) for the certificate revocation process. The request must contain *evidence* against the bearer of the certificate. The evidence consists of signed accusations (cp. the Accusation Protocol) from various peers in the network. The coordinator validates the evidence in the revocation request and, if the evidence provided is adequate, initiates the revocation process to generate a new CRL. The revocation process follows the same steps as the certification process described in the previous section and shown in Figure 3.

Distribution point synchronization. The CRL is stored redundantly on a number of CRL distribution point peers. In order to keep the CRL consistent these peers need to synchronize. The CRL distribution points will therefore send *synchronization messages* to all other distribution points whenever their local CRL version changed (i.e. whenever they added a new node to the CRL as described above). Additional synchronization messages are broadcasted periodically. Whenever a distribution point receives a synchronization message it will try to merge the CRL encoded in the message with its own copy. Since the Madeira CRL does not support removal of certificates (i.e. it is not possible to ‘re-enable’ certificate once they are revoked) this merging is trivial: the node will simply build the union of all certificates on his CRL copy as well as on the one encoded in the synchronization message, and update his CRL copy accordingly.

3.6 NBI Security Modules

Even though the NBI is based on Web Services technology we have chosen TLS [20] for providing host-to-host authentication, confidentiality and integrity instead of a WS-Security [21] approach. The main motivation for this approach is the lower resource consumption of TLS compared to WS-Security.

Different authorization levels to the NBI are provided by the role-based authentication features of the Tomcat [22] application server which runs the NBI.

An Intrusion Detection and Prevention System has been implemented in the NBI: it uses the information available at Axis [23] level and also all information provided by the Madeira system (mainly by the Accusation Service), and analysis this data to detect whether unknown malicious hosts or known Operation Support Systems hosts are trying to perform attacks (e.g. a Denial-of-Service attacks). This component also performs white and black listing checks on incoming authenticated data, discarding messages if needed. Upon detecting such attacks, and based on pre-defined policies, the NBI can undertake actions such as revoking security credentials to misbehaving Operation Support Systems or triggering security alarms.

4. CONCLUSIONS

The Madeira security solution presented in this paper is constrained by the design decisions reached in the Madeira project. Taking into account these limitations we have introduced a number of security mechanisms to minimize the main risks faced by such an infrastructure: temporality of nodes in the network, scalability, mobility, etc. The security mechanisms introduced are grounded on a distributed X.509v3 certificate and CRL infrastructure as well as the use of the TLS protocol for communications. Above this base security layer we have introduced network and host intrusion prevention mechanisms, a collaborative accusation protocol and the Advertisement Service that provides multipath communications within the Madeira hierarchical clusters topology. Although the Advertisement Service has been specifically designed for Madeira, it can be easily applied to obtain multipath communications in any network topology organised in a hierarchy of network domains.

Future work on the Madeira security framework includes the full evaluation of the solution we outlined here. Further research will also include a scalability analysis of the secured Madeira management system to understand the impact that the security framework presented in this paper has on the overall system scalability.

REFERENCES

[1] <http://www.celtic-madeira.org>

- [2] Arozarena, P. et al., Madeira: A peer-to-peer approach to network management, WWRF, April 2006, Shanghai, China.
- [3] Gottschalk, K.D., Graham, et al.: Introduction to Web services architecture, IBM Systems Journal, Volume 41, 2002
- [4] Housley, R. et al.; Internet X509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile; RFC 3280, April 2002. <http://www.ietf.org/rfc/rfc3280.txt>
- [5] Chen, R., Yeager, W.: Poblano – A distributed Trust Model for Peer-to-Peer networks, JXTA White Papers, 2003
- [6] <http://www.sun.com/software/jxta/>
- [7] Suryanarayana, G.; Erenkrantz, J.R.; Hendrickson, S.A.; Taylor, R.N.: PACE: an architectural style for trust management in decentralized applications, Software Architecture (2004)
- [8] Selcuk, A.A., Uzun, E., Pariente, M.R.: A reputation-based trust management system for P2P networks, IEEE Cluster Computing and the Grid (2004)
- [9] Elkins, M.: MIME Security with Pretty Good Privacy (PGP), RFC Editor (1996)
- [10] Berson, T.: Skype Security Evaluation, ALR-2005-031, Anagram Laboratories (2005)
- [11] RSA Laboratories. PKCS #1: RSA Encryption Standard. Redwood City, California, November 1993.
- [12] Luo, J., Hubaux, J.-P., Eugster, P.Th.: DICTATE: Distributed CerTification Authority with probabilisTic frEshness for Ad Hoc Networks. IEEE Transactions on Dependable and Secure Computing (TDSC) (2005)
- [13] Shoup, V.: Practical Threshold Signatures. In Theory and Application of Cryptographic Techniques, S. 207-220, 2000.
- [14] SNORT: <http://www.snort.org/>
- [15] AIDE: <http://sourceforge.net/projects/aide>
- [16] Zhou, L. and Haas, Z.J.: Securing Ad Hoc Networks. IEEE Network Magazine, vol. 13, no.6, December 1999.
- [17] Luo, H., Kong, J., Zerfos, P., et al.: URSA: Ubiquitous and Robust Access Control for Mobile Ad-Hoc Networks. IEEE/ACM Transactions on Networking, October 2004.
- [18] Rabin, T.: A Simplified Approach to Threshold and Proactive RSA. In Proceedings of the 18th Annual international Cryptology Conference on Advances in Cryptology (August 23 - 27, 1998). H. Krawczyk, Ed. Lecture Notes In Computer Science, vol. 1462. Springer-Verlag, London, 89-104, 1998.
- [19] Nystrom, M. Kaliski, B.: PKCS #10: Certification Request Syntax Specification Version 1.7. RFC 2986. November 2000.
- [20] Dierks, T., Rescorla, E.: The Transport Layer Security (TLS) Protocol Version 1.1. RFC 4346. April 2006
- [21] Web Services Security: SOAP Message Security 1.1 (WS-Security 2004) OASIS Standard Specification, 1 February 2006
- [22] Apache Tomcat – <http://tomcat.apache.org>
- [23] Apache Axis – <http://ws.apache.org/axis/>