Overcoming the Risks of the Perimeter-based Security with Strong Federated Identification Mechanisms

Wellington Silva de Souza
Prog. de Pós-Grad. em Eng. Elétrica e de Computação
Universidade Federal do Rio Grande do Norte
Natal/RN, Brazil
Email: wellsouz@gmail.com

Sergio Vianna Fialho
Prog. de Pós-Grad. em Eng. Elétrica e de Computação
Universidade Federal do Rio Grande do Norte
Natal/RN, Brazil
Email: fialho@pop-rn.rnp.br

***Abstract*—Nowadays, corporate networks appear completely unprepared to deal with threats from new technologies of communication, risk behavior of users, interoperability with third-party systems and outsourcing. The perimeter-based traditional security approach (model of the "castle and the moat") hinders the development of enterprise systems and creates the delusion of protection in both administrators and users. To overcome these threats, a new data-safety oriented paradigm called 'deperimeterisation' appeared in the last decade. However, it depends on an effective federated identity mechanism to reach the goal of a borderless network. The main contribution of this work is to fill this gap with a proposal of a strong federated identification mechanism, based on the SAML protocol and smart-cards.**

Keywords-network security*; *de-perimeterisation*; *federated identity*; *smart-cards*; *SAML.

I. INTRODUCTION

The revolution brought by the ICT (Information and Communication Technology) to modern society carries within it a set of new threats enterprise networks are not prepared to face, creating resistance in adopting new tecnologies, like Wi-Fi, peer-to-peer, cloud computing, outsourcing and home-office.

Such resistance stems from the traditional "Rings of Trust" [1] approach of security, adopted in the corporate world, shown in Figure 1. In this approach, security is viewed as a protection effort that must be centered in the division of layers (rings), focusing especially in the upper strata.

In this model, the protection of information is "guaranteed" through a physical/logical perimeter that separates the enterprise network (internal network) of the Internet (external network). According to [2], the term "castle and moat" is thus commonly used in analogy to traditional defense mechanisms in computer networks: firewall, proxy, IDS (Intrusion Detection System), IPS (Intrusion Prevention System).

This view of security, however, is inadequate to deal with threats from the current context in which corporate networks are in. Maintaining this model hinders development of enterprise systems and creates the delusion of protection in both administrators and users. So, a new approach of security is necessary in nowadays corporate networks.

In Section II, the risks of maintaining a perimeter-based security will be presented. Section III shows the de-perimeterisation paradigm, its goals and lacks. Section IV presents a proposal of a strong federated identification mechanism, aimed to fill one of the lacks of the de-perimeterisation paradigm, being the main contribution of this work. Section V shows the implementation aspects of the mechanism and the results obtained. Finally, Section VI defines the conclusion obtained from the work and will present the correlated future work.

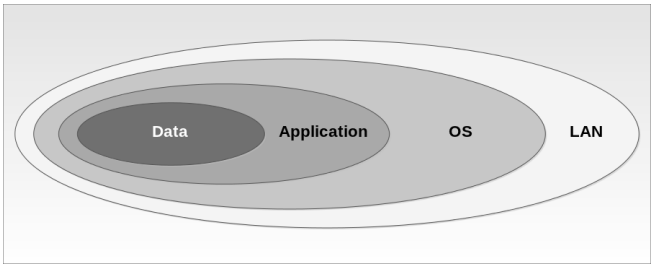

Figure 1. Conventional "Rings of Trust" Model of Security [1].

II. RISKS OF THE PERIMETER-BASED SECURITY

According to [3], after the 16th century, the castle began to decline as a defense, mainly due to the invention and development of heavy guns and mortars. Today, likewise, perimeter-based security systems face new threats for which they are not prepared:

1) Mobile conectivity: Smartphones and 3G/4G modems are becoming common belongings. Nothing prevents an employee from connecting them in the office computer to access content blocked by the enterprise security policy.

2) Wi-Fi hotspots: If there isn't a security protection at the link layer of the network (like IEEE 802.1X [4]) Wi-Fi access points can be connected to the network, providing internal network access to "wardrivers". The same threat occurs when using deprecated security protocols (WEP, for instance) or in the leakage of the shared password

 ISBN: 978-1-61208-249-3

in the WPA/WPA2 (if 'personal' mode is used instead of 'enterprise', RADIUS-based).

3) Using VPN to bypass network security policy: Software like OpenVPN™ [5] enables the user to establish a connection with a remote point over the network perimeter, bypassing it, like shown in Figure 2. Also, these software can perform encryption and HTTP encapsulation, masquerading their traffic like a regular HTTPs connection.

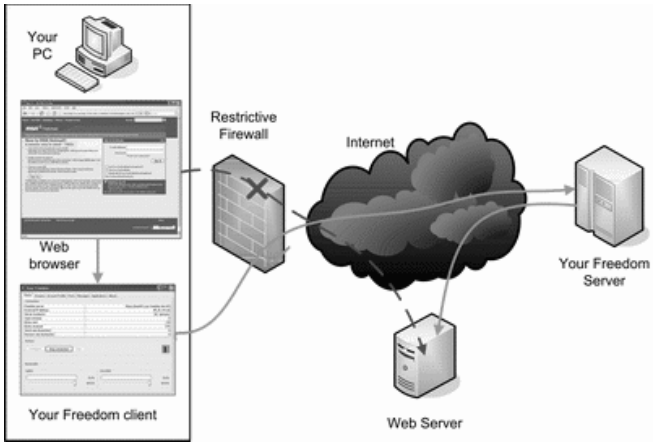

Figure 2. Bypassing Security Policy through VPN [6].

4) Malware: Malware can also perform encryption and HTTP encapsulation. A *trojan*, for instance, can estabilish a connection to a bot-net, delivering full-control of the host to the attacker. The traffic can also be encrypted, hiding it from detection of the network administrator.

5) BYOD: The BYOD ("Bring Your Own Device") [7] trend will presents a new defy to corporations in the next years. Nowadays, it is increasing the number of personal gadgets (smartphones, tablets, notebooks) connected to the corporate network. Generally, these devices are outside the scope of the enterprise configuration management, needing specific rules to be in compliance with the corporate security policy.

6) Mobility of the information: Even if the perimeter were perfect, it assumes that all assets remain inside. However, with the use of laptops, smartphones and pen-drives, valuable information leaves the organization all the time, in a totally unprotected way, bypassing both physical and electronic perimeter.

III. DE-PERIMETERISATION

In order to deal with the risks ignored by perimeter-based security, a new approach began to be investigated in the last decade. In this approach the security is brought close to the data, which are, ultimately, what we want to protect.

Figure 3 outlines the 'De-perimeterised' [1] model of security, which can be compared to the 'Rings of Trust' model showed in Figure 1. In the conventional model each ring establishes a perimeter that protects the interior of what is around them, providing communication from the "secure" to the "insecure". On the other hand, in the de-perimeterised model data is considered independent of context and does not depend on the application, operating system or network to remain safe.

It this in this scope emerges, based on studies of the Jericho Forum [8], a new vision of network security, centered in the concept of de-perimeterisation: it breaks up the traditional view of the network as a finite space, with interior and exterior sides and a perimeter separating them. According to the Jericho Forum, modern computer networks face a so wide variety of threats that the only reliable security strategy is to protect the information itself, rather than the network or the rest of the ICT infrastructure of the organization.

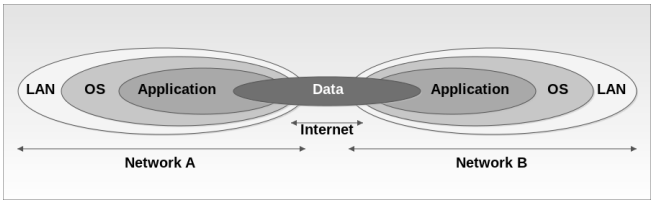

Figure 3. De-perimeterised Model of Security [1].

A. The "four-phases" toward de-perimeterisation

According to the Jericho Forum, all organizations must go through four stages to reach the point where they can develop their business processes safely in a completely de-perimeterised environment:

- **Phase 1**: Start leaving the perimeter. The first step of de-perimeterisation is making web applications leave the border of the corporate network, approaching people who will use them.
- **Phase 2**: Relaxing the perimeter. At this stage, one abandons claim to increasingly strengthen the perimeter, focusing on the availability of transport schemes of encrypted data and authenticated access to organization internal data.
- **Phase 3**: The perimeter ceases to exist. At this point, the encryption has already reached the data level and an authentication mechanism is already implemented in the connection level - thus eliminating the need for perimeters.
- **Phase 4**: Communication without borders. Business processes are already operating in a totally de-perimeterised environment. Data presents global security properties, which are directly handled in the endpoints. Mechanisms for identity management, authentication and authorization are distributed through a network of federated trust.

B. Missing items to accomplish a borderless network

Despite of being an interesting proposal to improve security in nowadays computer networks, the de-perimeterisation

paradigm lacks most of the parts needed to accomplish its four phases. Mechanisms such as authentication at data level and federated identity management are still in the conceptual universe.

Phases '1' (start leaving the perimeter) and '2' (relaxing the perimeter) could be immediately applied, if systems were equipped with an effective validation tool for identity checking. This is one of the items present on stage '4' (communication without borders), which states the need for mechanisms of federated identity, authentication and authorization. Only then stage '3' (the perimeter ceases to exist) could commence.

We conclude, therefore, that the path to de-perimeterisation necessarily involves the adoption of a safe and efficient mechanism for federated identity, which is studied in the following.

IV. A Strong Federated Identification Mechanism

A. Opting for smart-cards

Remote user authentication using smart cards is a good solution for many e-based applications [9]. Comparing different authentication mechanisms used for Internetbanking [10], smart-cards based on a PKI infrastructure (X509 certificates) earned the highest evaluation in the security category (along with SIM chips), although they present less economic and convenient features when compared to other traditional methods (user/password pairwise, for instance).

Considering the corporate world, smart-cards could easily be adopted. In fact, many companies are replacing traditional name tags with smart-cards, providing a value-added badge - their adoption, thus, wouldn't create a considerable economic impact. Unlike the Internetbanking enviroment, the use of smart-cards could be extremely convenient, given that porting id-badges is a common practice in the corporate environment (often a rule of the company).

B. Using SAML to provide federated identification

The SAML (Security Assertion Markup Language) [11] is a XML-based framework designated to provide mechanisms of authentication and authorization. It defines an open data format for creating and exchanging security information between online partners.

For the purposes of this work, SAML was chosen as it enables SSO (Single-Sign-On) and the separation between the authentication process and the service access, delivering federated identification in a WebService manner. Also, SAML is a recommended standard in the e-PING [12], the official brazilian interoperability pattern for e-government.

As stated by SAML, three participants take place in the authentication/authorization process:

- **Subject:** the entity to be authenticated. It can be a person, a computer, an organization. Also known as 'principal'.
- **IdP:** the Identity Provider, which performs the authentication process and generate assertions about the 'principal'. It is the *asserting party*.
- **SP:** the Service Provider, the system which the 'principal' intends to access. In the SAML context it acts as the *relying party*, consuming assertions generated by the IdP. One SP can rely and trust in different and independent IdPs, thus creating a federated identity network surrounding that service.

The UML (Unified Modeling Language) sequence diagram of the federated identification mechanism proposed is shown in Figure 4.

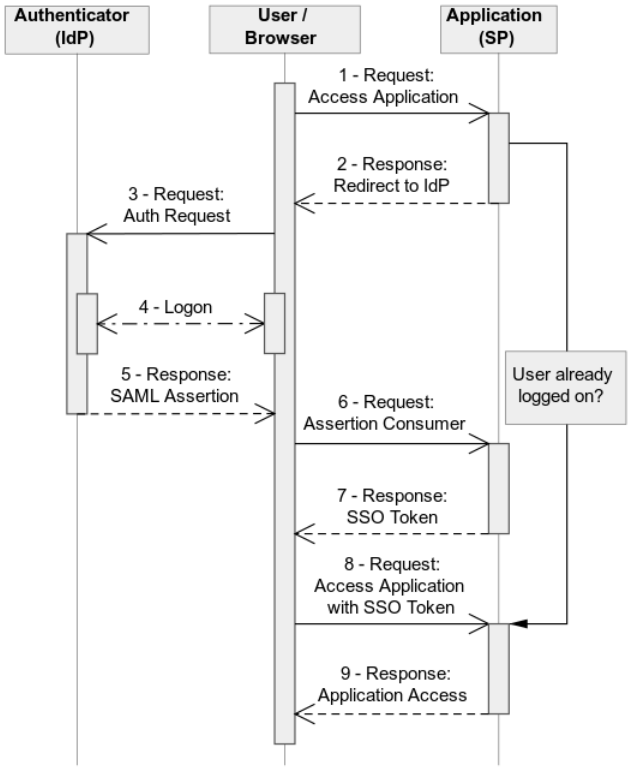

Figure 4. Sequence Diagram of SAML Federated Single-Sign-On.

C. The Logon Process

As shown in Figure 4, the logon process acts apart the entire SAML SSO process. The SAML framework does not defines *per se* a specific implementation for the credential validation of the principal, as it depends on specific enviroment issues (legal restrictions, institutional requirements, users database, directory model, and others).

Figure 5 shows the UML sequence diagram of the logon process for SAML identification through smart-cards.

V. Implementation and Results

The proposed federated identification mechanism was implemented in Java language, through a combination of an applet and a servlet.

 ISBN: 978-1-61208-249-3

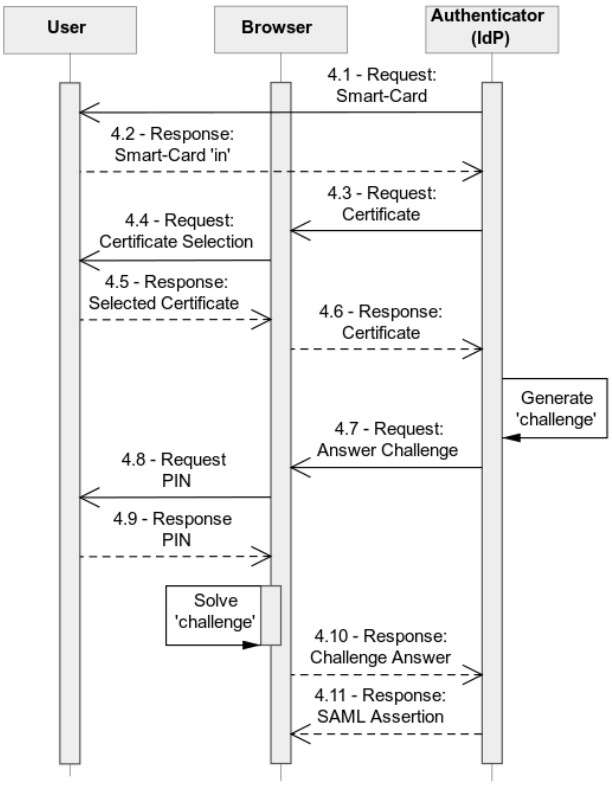

Figure 5. Sequence Diagram of Smart-Card Logon Process.

Since the operation with smart-cards needs communication with PKCS#11 libraries in the local computer file system, a signed applet was designed to interface with the user and his smart-card. The servlet, by his turn, is responsible for dealing with the SAML protocol. This design increases performance and security, because reduce the size of the applet (speeding up the loading process) and protects the IdP private key (stored on the server running the servlet), used to sign the SAML assertions.

The applet is loaded when an application compatible with SAML (SP) redirects the browser to the identification mechanism (IdP), carrying a <samlp:AuthnRequest> element in the URL (steps 2 and 3 of Figure 4). After initialization, the applet performs the logon process (Figure 5), asking for the user certificate and PIN code to access the cryptographic functions on the smart-card. The applet loads the "User Alternative Names" (present in the user certificate) and send then to the servlet.

The servlet, by his turn, receives the "User Alternative Names" and creates a signed <samlp:Response> element, which contains an SAML assertion with the user attributes. The browser is redirected to the application assertion consumer, which validates the <samlp:Response> and creates a SSO Token, allowing access to the service.

A. Tests

The mechanism was tested with third party tools and implementations of the SAML protocol. For tracking the SAML messages, it was used the SAMLTracer [13], a plugin for the Mozilla Firefox browser.

To validate the IdP feature of the mechanism, two SP reference implementations were used: SimpleSAMLphp [14] and TestShibTwo [15]. In both cases, the proposed federated identification mechanism sucessfully was able to receive and process the <samlp:AuthnRequest> from the SP, perform the user authentication, and generate the <samlp:Response>, which was validated by the application assertion consumer.

VI. Conclusion and Future Work

This work presented the problems of the traditional perimeter-based security view, exploring the risks of maintaining this approach in a corporate environment. It was shown that a new paradigm, called de-perimeterisation, has been studied in recent years, and is designed to deal with problems ignored by the perimeterised security model. However, this new approach of security lacks certain parts to be implemented, especially a safe and effective mechanism for federated identity. For this goal, a proposal was presented, using the SAML framework and smart cards, being the main contribution of this work.

This proposal was implemented using Java language, through a combination of an applet and a servlet. This design aimed to improve perfomance and security to the developed mechanism.

It was performed a set of tests using third party reference implementantions of service providers (SP), proving the effectiveness of the mechanism.

As future work, it is intended to apply the the proposed authentication architecture in a real corporate network, accomplishing phases '1' and '2' of the de-perimeterisation process.

References

[1] J. Fritsch, "No borders - de-perimeterization and life after the firewall," *Linux Magazine*, vol. 89, no. 1, pp. 60–63, Jan. 2008.

[2] "O que é um firewall?" One Linea Telecom, Tech. Rep., Nov. 2012. [Online]. Available: http://www.onelinea.com.br/pdfs/bto-firewall.pdf

[3] C. Freudenrich, "How castles work," How Stuff Works, Tech. Rep., Aug. 2012. [Online]. Available: http://history.howstuffworks.com/historical-figures/castle7.htm

[4] T. Jeffree, N. Jarvis, M. Seaman, L. Bell, A. Chambers, M. Cochran *et al.*, *802.1X - Port-Based Network Access Control*, IEEE-SA Standards Board, 3 Park Avenue, New York, NY 10016-5997, USA, Feb. 2010.

 ISBN: 978-1-61208-249-3

[5] "Openvpn - open source vpn," OpenVPN Technologies, Inc, Tech. Rep., Aug. 2012. [Online]. Available: http://openvpn.net

[6] "Yourfreedom - bypass firewalls and proxies, stay anonymous," YourFreedom, Tech. Rep., Aug. 2012. [Online]. Available: https://www.your-freedom.net/

[7] R. G. S. Junior, E. P. Souza, and A. C. A. Nascimento, "Desafios para a universalização do uso de certificados digitais no contexto da icp-brasil," in *CertForum*, Florianópolis, SC, Brazil, Sep. 2012, in press.

[8] "Jericho Forum's homepage," The Open Group, Tech. Rep., Aug. 2012. [Online]. Available: http://www.opengroup.org/getinvolved/forums/jericho

[9] R. Ramasamy and A. P. Muniyandi, "An efficient password authentication scheme for smart card," in *International Journal of Network Security*, vol. 14, no. 3, May 2012, pp. 180–186.

[10] R. S. Guimarães, "Análise comparativa de sistemas de autenticação utilizados em internetbanking," Master's thesis, Instituto de Pesquisas Tecnológicas do Estado de São Paulo, São Paulo, SP, Brazil, 2006.

[11] N. Ragouzis, J. Hughes, R. Philpott, E. Maler, H. Lockhart, T. Wisniewski, S. Cantor, and P. Mishra, *Security Assertion Markup Language (SAML) V2.0 Technical Overview*, OASIS Committee Draft, Mar. 2008.

[12] H. Correia, J. Rodrigues, and P. M. da Costa, *e-PING - Padrões de Interoperabilidade de Governo Eletrônico*, Comitê Executivo de Governo Eletrônico, Nov. 2011.

[13] O. Morken, "Saml tracer :: Add-ons for firefox," Tech. Rep., Nov. 2012. [Online]. Available: https://addons.mozilla.org/firefox/addon/saml-tracer

[14] "Simplesamlphp," Tech. Rep., Nov. 2012. [Online]. Available: http://simplesamlphp.org

[15] "Testshib two," Internet2, Tech. Rep., Nov. 2012. [Online]. Available: https://www.testshib.org

 ISBN: 978-1-61208-249-3