Efficiency of the Single Sign On mechanism in a tactical network environment

Joanna Śliwa, Tomasz Podlasek  
C4I Systems’ Division  
Military Communication Institute  
Zegrze, Poland  
{j.sliwa, t.podlasek}@wil.waw.pl

Robert Matyszkiel, Bogusław Grochowina  
Radiocommunications & Electronic Warfare Division  
Military Communication Institute  
Zegrze, Poland  
{r.matyszkiel, b.grochowina}@wil.waw.pl

Abstract—The article describes tests of efficiency of Web Single Sign On (SSO) solution used to provide authentication and authorization of user requests and responses during web portal invocation in a tactical radio network environment. The software solution was based on Fediz Apache CXF and WS-Federation standard configured with Passive Requestor Profile. There has been created tactical network environment with real PR4G radios configured to work in the IP PASS mode. The article discusses the scenario used for the experiment, results of the response times and success rate of secure web portal invocations on the tactical level. The results of tests may be also important for the Federated Mission Network (FMN) deployment since the solution tested follows FMN configuration template for Web Authentication Services.

Keywords- SSO, WS-Federation, web portal, tactical network environment

I. INTRODUCTION

Modern military operations are supported nowadays by command and control systems implemented with the use of technologies known from the Internet. The information in the current battlefield is of crucial value and therefore its timely and secure transmission is incredibly important, on all levels of command. Especially on the tactical level, where the situation changes dynamically and the time needed for decision making is very short, having access to the information about alarms, threats or location of friendly and foe forces may decide about soldiers life. Having this in mind one needs to remember about the necessity of protection of the information sources form the access of the enemy.

Web resources are usually made available in the form of portals, invoked by the web browsers. This easy to use interface is very useful relieving the need of a dedicated client installation and helpful in multinational scenarios performed by coalitions. However such scenarios impose the need to share resources with different parties posing additional requirements on the exchange of information.

Web portals can be made available with the use of secure Single Sign On (SSO) technology based on WS-Federation standard that supports authorization and authentication of users on the basis of their credentials supporting multi-domain scenarios where users from different domains share valuable resources to each other.

From the other hand realization of web based information sharing processes demands wideband communication means. However, there is still a large number of narrowband communication means in use. The exploitation time planned for them has not expired. For such cases it is necessary to answer the question of the possibility of web based services’ application in networks built with narrowband radios prepared for IP transmission and about the efficiency of secure web resources distribution on the tactical level.

This paper presents result of a limited laboratory test aimed at answering the above questions. For this purpose there has been built a controlled environment using real PR4G radios connecting two computers. The radios operated in the IP PAS mode and offered 19.2 kbps bit rate. The computers were working in a client – server mode. One of them was equipped with a simple web browser and the second one performed a role of the server with a portal up and running, serving web contents – in this case blue force information according to NFFI XML schema. This simple scenario is the part of a more complex case of the NFFI service used in a military patrol operation also presented in this paper. It is assumed that research results of this simple configuration will be the starting point for testing of the reconnaissance patrol scenario.

II. WEB SINGLE SIGN ON (SSO)

A. Introduction to WS-Federation

Secure information sharing in multinational scenarios based on Federation of Systems built with independently operated and managed systems must rely on internal (national) security mechanisms and a relation of trust between the cooperating parties. The notion of “need to share” has given many benefits to soldiers equipped with modern information technology. They could be provided with information supporting their tasks and sometimes even saving their lives.

The security solutions proposed for cross-domain information exchange need to cope with the problem of identity management. It is necessary to allow nations to implement their own authentication mechanisms based on internal Identity Providers, keeping a standard form of the exchange of the confirmations (security assertions) on the intra-domain basis.
Web services’ security standards such as WS-Security, WS-Trust, and WS-SecurityPolicy define a basic model for federation between Identity Providers and Relying Parties. They define mechanisms for representing claims (assertions) about a requestor (as security tokens) which can be then used to protect and authorize web services’ requests in accordance with a valid policy. WS-Federation extends this idea by describing how the claim transformation model inherent in the security token exchanges can enable richer trust relationships and federation of services. This enables scenarios where authorized access to resources managed in one domain can be provided to users whose identities and attributes are created and managed in other domains. WS-Federation includes mechanisms for brokering of identity, attribute discovery and retrieval, authentication and authorization claims between federation partners, and protecting the privacy of these claims across organizational boundaries [4]. These mechanisms are defined as extensions to the Security Token Service (STS) model defined in WS-Trust. Moreover, WS-Federation defines how to map these mechanisms, and the WS-Trust token issuance messages, onto HTTP (easy to use in Web browser environments). The intention is to provide a common infrastructure for performing Federated Identity operations for both web services and browser-based applications.

B. Passive Requestors Profile

As already mentioned the WS - Federation specification defines extensions to the WS - Trust model to enable different styles of the federation [1]. The model, based on HTTP encoding of the WS-Trust messages, can be used from either web service clients directly or from browsers and portals. This approach enables common infrastructure and management tools irrespective of the client application platform being used. Processing of the SOAP requests can be performed with the use of the base HTTP 1.1 mechanisms (GET, POST, redirects, and cookies) and conform as closely as possible to the WS-Trust protocols for token acquisition.

In general, requestors are associated with an, so called, Identity Provider (IP) or Security Token Service (STS) where they authenticate themselves (in their own domains) using the method in accordance with the local security policy. The authentication can be based on different credentials (according to SAML [5]), e.g. the username/password (the username token), X.509 certificates (X.509 Certificate Token). At the time of initial authentication, a cookie is created for the requestor at their Identity Provider so that every request for a resource does not require requestor’s intervention.

In the Web approach, there is a common pattern used when communicating with an IP/STS. In the first step, the requestor accesses the resource, and then is redirected to a local IP/STS operated by the resource provider. In this case we assume that no token or cookie is supplied with the request. This is also the case when the token has not been cached (the requestor hasn’t been authenticated yet). Then a second redirection to the requestor's IP/STS will be performed. The IP/STS in the requestor’s home domain (realm) generates a security token for the use by the federated party.

The figure below illustrates an example flow in a single domain. As depicted, all communication occurs with the standard HTTP GET and POST methods, using redirects (steps 2-3 and 5-6) to automate the communication. When returning non-URL content, HTTP POST is required (e.g. in step 6) if a result reference is not used. In step 2 the resource can act as its own IP/STS so communication with an additional service is not required. Step 3 depicts the resource redirecting directly to the requestor’s IP/STS. In general, this could redirect to an IP/STS for the resource (or any number of chained IP/STS services). It might also redirect to a home realm discovery service.

C. Application of Web Authentication

The aim of the WS-Federation application in Federated Mission Network is to create Federated User Web Application Authentication and allow users from one security domain to access web applications (e.g. claims-aware web portals) in another domain using a web browser. This promotes information sharing in multinational scenarios, and allows users from different domains to collaborate in an integrated fashion. The solution is based on open standards, and therefore is not limited to a single platform or solution. It allows the administrators of federated domains to retain control over their own resources, while selectively making them available to partners.

The simple scenario assumes that each domain is separately managed leaving the mechanism for users’ authentication an internal decision. There is no direct trust between the domains’ authentication mechanisms (such as e.g. Kerberos). In this way it is not necessary to create separate accounts for users from foreign domains in access to the web application in the target domain (which was proven difficult at CWIX exercises in many cases due to the internal national security policies).
D. The mechanism operation – a multidomain example

In a scenario involving two domains mutually trusting each other, the beginning of the process is very similar (see Fig.2). The user invokes the target service by trying to access target domain’s web resource. When trying to access the web application, the user is required to authenticate. By clicking on a control or link on the log-in page, the user is redirected to the Identity Provider in the target domain, which hosts a Security Token Service (STS) [3]. The user is then redirected to their own Identity Provider, in the source domain, where he is able to authenticate (based on inter-domain authentication mechanism). He authenticates to his local STS, and is issued with an XML security token (a SAML Assertion [5]), which proves his identity and indicates the method of authentication, and is then sent to the Identity Provider in the target domain. This Identity Provider then approves SAML token from the trusted party, and issues a new security token which is trusted by the web application. It contains claims about the user (the set defined administratively based on attribute/value pairs that may come from directories, databases or even text files) that the web application trusts, and can use for making authorization decisions (if required). The security token will contain at least one claim that uniquely identifies the user for auditing purposes. The security token is sent to the web application, which then accepts the user as authenticated.

III. EXPERIMENT SCENARIO

A. Operational context

The operational context of web services research is the scenario of reconnaissance patrol (see Fig. 3) that consists of the following phases.

- Phase I – march from base A to village B. Patrol commander reports to base A current position;
- Phase II – search of village B. Troopers in vehicles and outside vehicles report to patrol commander current situation and position. Patrol commander reports to base A current situation and position;
- Phase III – march from village B to road crossing D. Patrol commander reports to base A current position;
- Phase IV – fight in an ambush. Troopers in vehicles and outside vehicles report to patrol commander current situation and position. Patrol commander reports to base A current situation and position; In this phase the soldiers need support of the allied forces that are deployed in a nearby area. For this purpose they need to invoke the coalition member web resource that offers NFFI tracks from a web based interface and get to know the exact positions and status of these forces.
- Phase V march from road crossing D to base A. Patrol commander reports to base A current position.

The reconnaissance patrol uses the following radio networks (see Fig. 4):

- base commander – CNR 1;
- patrol commander – CNR 2;
- squad commanders – CNR 3.

Radio correspondents are:

- base A – node 1;
- patrol commander – node 3;
- squad commanders – nodes 2, 4, 5;
- troopers – nodes 6 ÷ 12.

In case of the lack direct connection data will be retransmitted.

In the research we used the scenario thread from the phase IV when the soldiers need to invoke the web resource of the allied party retrieving friendly forces location and status. Consequently, it was necessary to configure two domains (own and the ally) and provide the data transmission at the application layer.

B. Network environment

The Polish Armed Forces are currently equipped with portable radios type Fast@Net RRC-9210 and vehicle radios type Fast@Net RRC-9310AP. These VHF radios belong to PR4G radios family. They provide IP/TCP compatible data transmission by 25 kHz radio channel in two operation modes:
• **IP MUX** (IP Multiplexed) – prepared for simultaneous voice and data transmission in the same channel. Data transmission is possible with bit rate of 4.8 kbps and is realized in half duplex mode or in triggered TDMA mode. The radio network needs NCS (Network Command Station) radio for its synchronization and triggering IP MUX mode. Synchronization can also be delivered by GPS receivers. Adding additional radios to radio network or removing them is possible at any time and is done by NCS radio with a dedicated command. The newest version of firmware provides the automatic distribution of route changes after the radio network reconfiguration;

• **IP PAS** – prepared only for data transmission with the bit rate of 19.2 kbps. Network synchronization is done in a distributed way and NCS radio is not necessary, however the IP PAS radio network needs Address Server that typically is run in NCS radio so NCS radio is present in the radio network. It is possible to implement five hops (intermediate radios). The network range is enlarged but on the other hand it introduces bigger transmit time delay. This mode is therefore not dedicated for real time data. Maximum number of radios in the network is limited to 32. Each radio automatically updates network topology data (knows the neighborhood). In the case of lack of direct connection between the source and end radios, a connection with an intermediate radios are established.

## IV. EXPERIMENT RESULTS

### A. Network configuration

The laboratory network was built with two Fast@Net RRC-9310AP radios. They were configured to work in the IP PAS mode with bit rate of 19.2 kbps to create transmission channel for the application layer data exchanged between two computers, each of them connected to its own radio. The output power of radio transmitters was established at the level that allowed to achieve neglecting value of Bit Error Rate (BER) and to make measurements in conditions of error free transmission.

The two computers played roles of two domains with the following software components installed:

- **Domain B** – web browser, WIL IdP, WIL STS;
- **Domain A** – Protected service (RP), MCI STS, MCI IdP.

![Laboratory testbed schema](image)

It must be emphasized that Fast@Net radios operated as routers connecting two Wide Area Networks for the two cooperating domains.
B. Test scenarios

The test assumed that the client from domain B (WIL) communicates with domain A (MCI) from his internet browser. The tests were performed based on 2 main scenarios (see Figure 6):

- Scenario 1: Federated authentication and request for resource;
- Scenario 2: Cached authentication token – direct access to resource (request and response messages are sent directly between the client and browser).

The domain MCI makes a web portal available (protected resource – RP) and serves NFFI tracks data according to 3 simple cases (see Table 1) that differ in the size of the message sent: small/medium/big messages. The other parameters and circumstances for both scenarios were the same (the same authentication method, the same kind of connection (TLS)).

In each scenario 20 separate measurements were performed. The authentication in the home domain of the user was based on Username Token - UT, with login and password. SAML token was used to bear credentials between the domains.
### Table I. Data sent back in response to the client

<table>
<thead>
<tr>
<th>Case number</th>
<th>The number of NFFI tracks</th>
<th>NFFI size [kB]</th>
<th>Http size [kB]</th>
<th>Full size [kB]</th>
</tr>
</thead>
<tbody>
<tr>
<td>case 1</td>
<td>1</td>
<td>0.98</td>
<td>0.4</td>
<td>1.4</td>
</tr>
<tr>
<td>case 2</td>
<td>5</td>
<td>9.92</td>
<td>0.4</td>
<td>10.4</td>
</tr>
<tr>
<td>case 3</td>
<td>50</td>
<td>98.7</td>
<td>0.4</td>
<td>100.1</td>
</tr>
</tbody>
</table>

### C. Scenario 1: federated authentication and request for resource

The main aim of this scenario was to test the application response times in the communication among entities involved in the web authentication in the multi-domain scenario. It is assumed that the user does not have the authorization token yet and needs to be provided with it for the purpose of the resource access control.

In the scenario response time for 6 information exchanges was measured (see red example on Figure 6) for 3 cases of the response message size (see Table 1).

### D. Scenario 2: cached authentication – direct access to resource

In the second scenario, there has been measured the application response time between sending the request for the resource, successful authentication/authorization of a user in a federated environment and receiving the response. The credential tokens were held in the browser temporary memory, and were sent through the HTTPS protocol.

In this scenario the response time was measured (see green box on Figure 6) for 3 cases of the response message size (see Table 1).

### E. Results

In this chapter the results of the measurements of application response times during federated web authentication (SSO) in a multi-domain configuration in particular phases of the process of cross-domain authorization (P0-P4 – see also Figure 6) for the 3 proposed cases are almost equal. This is due to the fact that in order to be able to retrieve the actual data from the resource, the requestor needs to be authenticated in his own domain, get a SAML assertion and provide it in the target domain for verification (and this process is the same for any response from the target server). Only after this step, the actual response can be delivered (in P5 – see also Figure 6). The size of the response is dependent on the case (see Table 1). As suspected, the messages with bigger size (especially the 100kB-one) have higher transmission delays resulting from the communications channel throughput (see chapter IV A).

Scenario 2 was aimed at verification of the scenario when the user has already been authenticated in his domain and his web browser has cached SSO tokens to be used for further requests. With this token, the user can directly invoke the target Web Service Provider (see Figure 6 – Scenario 2 P5).

![Figure 8. Transmission delays during cached web authentication in a federated scenario; P5 according to Scenario 2 Figure 6.](image)

In Figure 8 there have been presented results of the transmission delay for cached federated authentication in 3 aforementioned cases (see Table 1). The results resemble P5 transmission delays from the scenario 1 (see the comparison of P5 in the two scenarios in Figure 9). Retrieval of the response takes more time when the actual data has bigger size. However in this case the token is cached and can be sent in request to the target service directly. The overall transmission delay related to the process of the federated web authentication is significantly lower in case of the cached authentication (13 times for the smallest response message, 5,3 times for the medium message and 1,8 times for the biggest response) (see Figure 10).

SSO improves the application response times perceived by the user (requestor) significantly. The exchange of information among particular components of web authentication architecture (IdPs, STSs, WRP) are not visible for him. The user is interested in getting the valuable information back in response as quickly as possible, which is particularly important in case of dynamic operational activities performed at the tactical level. As described in our operational scenario the soldiers need immediate support from the allied forces so that it is necessary for them to be
provided with their direct location and status. Quick delivery of the NFFI tracks can be of a crucial importance for their safety.

![Figure 9](image9.png)

**Figure 9.** Comparison of the transmission delay for the phase 5 of the communications process (P5 in Figure 6) in the two scenarios.

![Figure 10](image10.png)

**Figure 10.** Comparison of the overall transmission delay for the federated authentication in two scenarios.

V. CONCLUSIONS

The article describes results of tests of the Web Single Sign On (SSO) solution efficiency used to provide authentication and authorization of user requests and responses during web portal invocation in a tactical radio network environment. The web resource provider offered 3 types of NFFI messages (one track – small message, 5 tracks – medium message, 100 tracks – big message). The web authentication was configured to work in a federated scenario where the requester belonged to another domain from the web resource provider. Two scenarios were tested. The first one consisted in checking the response time when the full path of interactions between IdPs and STSs in the two domains were performed. The second one was to verify the advantages in terms of the response time when the tokens are cached and SSO is used.

The results proved that the WS-Federation passive requestor’s profile is able to work in a tactical network using narrowband radios configured to work in the IP Pass mode and gives satisfactory results given the effective throughout of the channel equal to 9 kbps. The SSO was even 13 times faster in case of the smallest message when compared to federated web authentication without cache. It is a considerable benefit that needs to be taken into account when designing the time of expiry of the tokens in the national domain during the mission preparation.

The results of tests may be also important for the Federated Mission Network (FMN) deployment since the solution tested follows FMN configuration template for Web Authentication Services [3].

ACKNOWLEDGMENT

This work was supported by European Defense Agency, contract no. B-0882-IAP4-GC, “Military Disruption Tolerant Networks”.

REFERENCES


[6] NATO Friendly Forces Information (STANAG 5527 [NFFI])