Comprehensive formal security analysis of Single Sign-On protocols based on the SAML 2.0 standard

Zvonimir Hartl, mag. ing. inf. et comm. techn.

mentor: Asst. Prof. Ante Đerek, PhD

University of Zagreb Faculty of Electrical Engineering and Computing

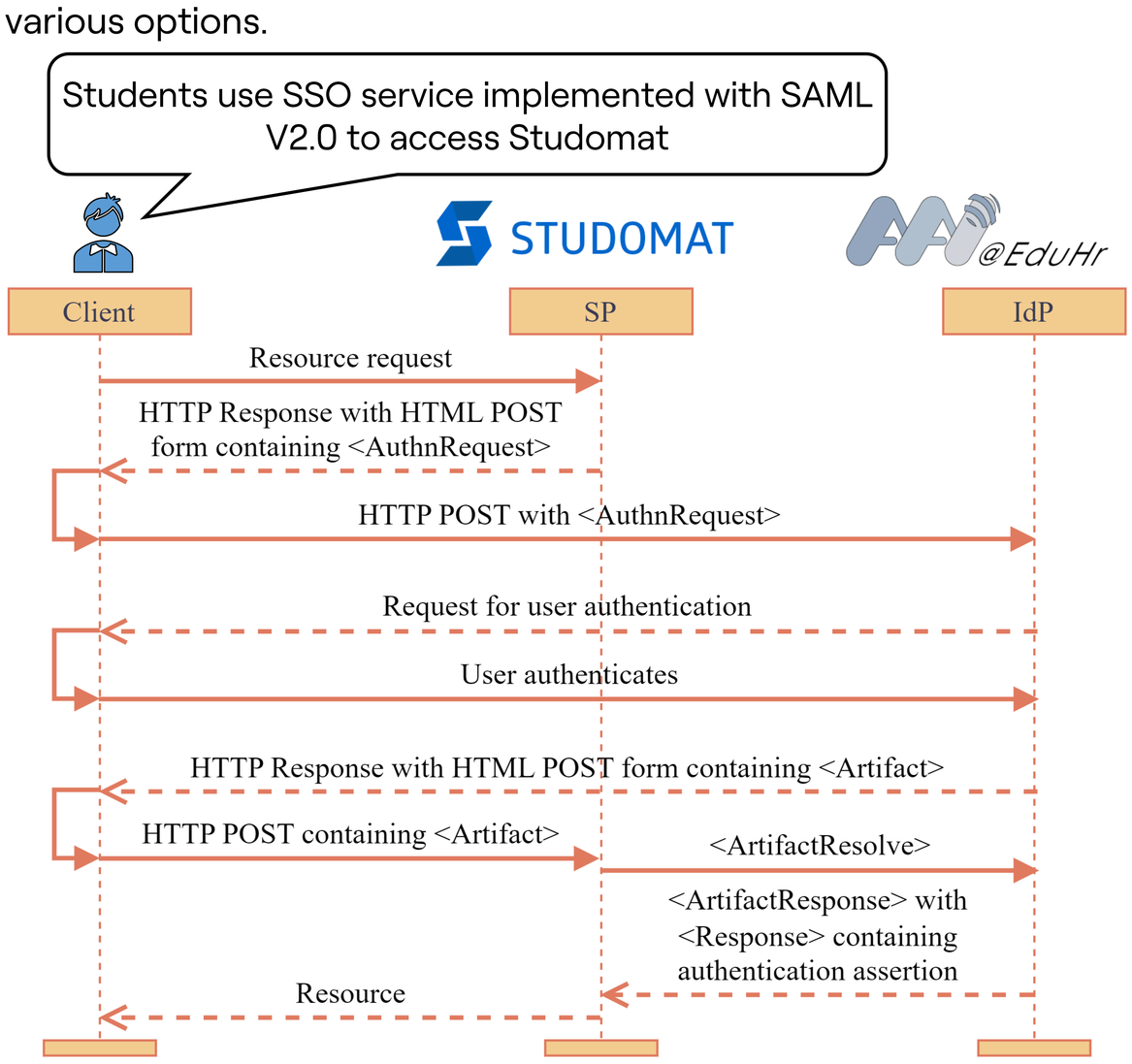
UNIVERSITY OF ZAGREB
Faculty of Electrical Engineering and Computing

1. Introduction

Single Sign-On (SSO) protocols enable exchange of authentication and authorization data between trusted service providers and identity providers, enabling user to have one set of credentials at identity provider and being able to use services at multiple service providers. SAML V2.0 [1] is one of the most used protocols that provide SSO functionality. SAML V2.0 is mostly used by governmental, federal and education institutions. Example implementations are Croatian National Identity and Authentication System (NIAS) and Authentication and Authorization Infrastructure of Science and Higher Education in Croatia (AAI@EduHr).

2. Problem Description

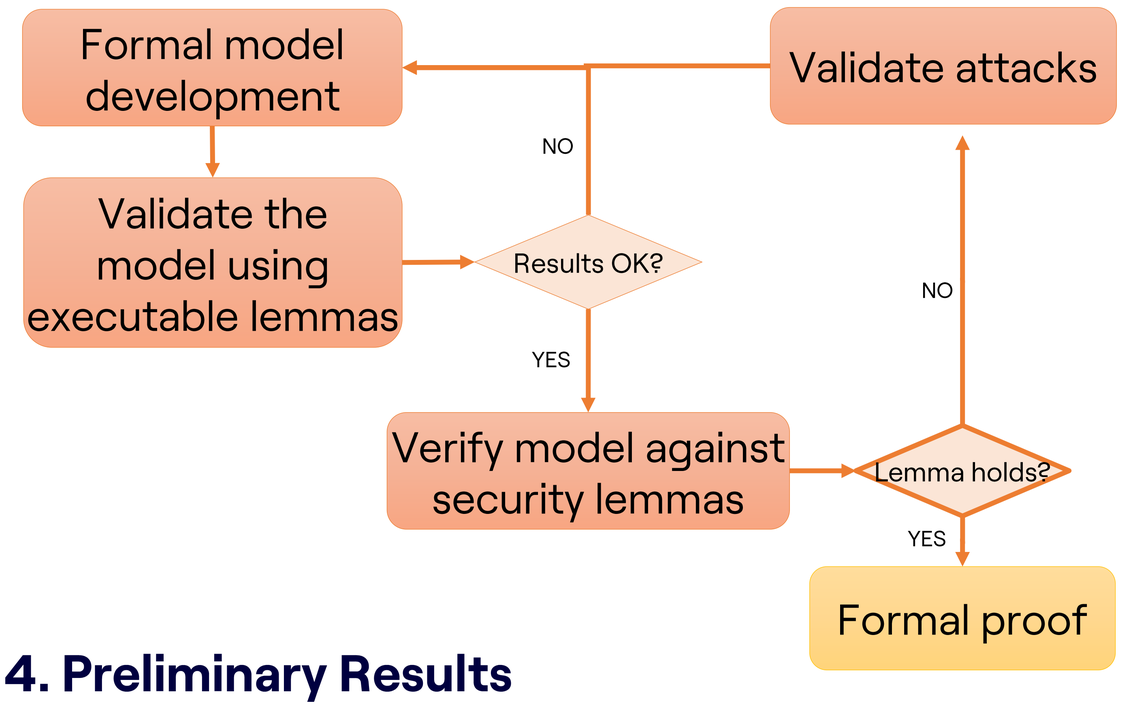
Compromising IdP or braking SSO protocol can allow a malicious actor to access a broad set of services and consequently a broad set of sensitive user data. SSO protocol is single point of failure therefore it would be of much use to have formal proof that it is secure. It is complex to create a formal model of SAML V2.0 SSO Profile since it offers six different use case implementations with various options.



IS THE SAML V2.0 SSO PROTOCOL REALLY SECURE?

3. Methodology

Formal analysis could give us guarantee that SAML V2.0 SSO Profile is secure or can provide us enough knowledge on how to improve the protocol security. **Tamarin Prover** is the state-of-the-art tool for formal analysis of security protocols [2]. We used it to create formal model of the use case SP-initiated SSO with POST/Artifact bindings from SAML V2.0 web browser SSO profile. To build such a model we needed to iterate many times through following process.



4. Preliminary Results

For now we managed to formally model one use case SP-initiated SSO with POST/Artifact bindings from SAML V2.0 web browser SSO profile. We generated 8 different variants of use case in accordance with different possible implementations of secure ID generation, RelayState handling and authentication request signing. Results of analysing broad set of security properties of given use case is shown in following table.

No.	Property	Protocol variant							
		srs	srw	sns	snw	urs	urw	uns	unw
1	sec_Client_Resource_Authenticity	✓	✓	✓	✓	✓	✓	✓	✓
2	sec_Client_Resource_Authenticity_Strong	✓	✓	✓	✓	✓	✓	✓	✓
3	sec_Client_Registered_Resource_Secrecy	✓	✓	✓	✓	✓	✓	✓	✓
4	sec_Client_Registered_Resource_Secrecy_Strong	✗	✗	✗	✗	✗	✗	✗	✗
5	sec_Client_Resource_Secrecy	✓	✓	✓	✓	✓	✓	✓	✓
6	sec_Client_Resource_Secrecy_Strong	✓	✓	✓	✓	✓	✓	✓	✓
7	sec_Client_Resource_Freshness	✓	✓	✓	✓	✓	✓	✓	✓
8	sec_Client_SP_Non_Injective_Agreement	✓	✓	✓	✓	✓	✓	✓	✓
9	sec_Client_SP_Non_Injective_Agreement_Strong	✓	✓	✓	✓	✓	✓	✓	✓
10	sec_Client_SP_Injective_Agreement	✓	✓	✓	✓	✓	✓	✓	✓
11	sec_Client_SP_Injective_Agreement_Strong	✓	✓	✓	✓	✓	✓	✓	✓
12	sec_SP_Client_Resource_Secrecy	✓	✓	✓	✓	✓	✓	✓	✓
13	sec_SP_Client_Resource_Secrecy_Strong	✓	✓	✓	✓	✓	✓	✓	✓
14	sec_SP_Client_Non_Injective_Agreement	✓	✓	✓	✓	✓	✓	✓	✓
15	sec_SP_Client_Non_Injective_Agreement_Strong	✓	✓	✓	✓	✓	✓	✓	✓
16	sec_SP_IdP_Weak_Agreement	✓	✓	✓	✓	✓	✓	✓	✓
17	sec_SP_IdP_Weak_Agreement_Strong	✓	✓	✓	✓	✓	✓	✓	✓
18	sec_SP_IdP_Non_Injective_Agreement	✓	✓	✓	✓	✓	✓	✓	✓
19	sec_SP_IdP_Non_Injective_Agreement_Strong	✓	✓	✓	✓	✓	✓	✓	✓
20	sec_SP_IdP_Authentication_Freshness	✓	✓	✓	✓	✓	✗	✓	✗
21	sec_SP_IdP_Authentication_Freshness_Strong	✓	✓	✓	✓	✓	✗	✓	✗
22	sec_SP_IdP_Assertion_Secrecy	✓	✓	✓	✓	✓	✓	✓	✓
23	sec_SP_IdP_Assertion_Secrecy_Strong	✓	✓	✓	✓	✓	✓	✓	✓
24	sec_IdP_SP_Non_Injective_Pre_Agreement	✓	✓	✓	✓	✗	✗	✗	✗
25	sec_IdP_SP_Weak_Agreement	✓	✓	✓	✓	✓	✓	✓	✓
26	sec_IdP_SP_Non_Injective_Agreement	✗	✗	✗	✗	✗	✗	✗	✗
27	sec_IdP_SP_Injective_Agreement	✗	✗	✗	✗	✗	✗	✗	✗
28	sec_IdP_SP_Assertion_Secrecy	✓	✓	✓	✓	✓	✓	✓	✓

Legend:
first letter of the protocol variant – authorization requests are signed (“s”) or unsigned (“u”)
second letter of the protocol variant – relay state mechanism is used (“r”) or not used (“n”)
third letter of the protocol variant – random IDs are cryptographically strong (“s”) or weak (“w”)
✓– property verified, ✗– property falsified

5. Conclusion

The results of formal verification of security proprieties of SP-initiated SSO with POST/Artifact bindings have shown that most important security properties of resource and assertion secrecy hold in all possible variants of protocol.
In future work we would like to create comprehensive formal models of all possible use cases of Web Browser SAML SSO Profile and to automatically verify presented security properties.

References

[1] Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Std., March 2005. [Online]. Available: https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[2] S. Meier, B. Schmidt, C. Cremers, and D. A. Basin, “The TAMARIN Prover for the Symbolic Analysis of Security Protocols,” in Computer Aided Verification - 25th International Conference, CAV 2013

Contact

Zvonimir Hartl, mag. ing. inf. et comm. techn.
zvonimir.hartl@fer.hr

PhD Day Faculty of Electrical Engineering and Computing, 1 June 2023