# Intelligent Campus Single Sign-on System using Novel Software Architecture

Yao FU

*Chongqing Industry Polytechnic College,* Chongqing, China 401120

***Abstract* — Federated identity management technology has been used by more and more users, which supports cross-domain work and supplies single sign-on capability when accessing network service. However, as common users cannot understand server certificate, which makes spoofing attack more likely. This paper proposes one joint identity management bi-direction authentication protocol based on server, with human perceptual authentication code being adopted to verify identity authority server in TLS conversation. The purpose of bi-directional protection of token is reached through binding client certificate and strengthening same original policy. Finally, we analyze the safety with formalized model and prove that protocol can provide safe authentication.**

***Keywords - identity management; identity authentication; single sign-on; software system structure***

## I. INTRODUCTION

Federated Identity Management (FIM) is to let the users use the same identity data to attain all the access permit of service participated in federation and this technology can decrease the difficulty of identity management of service provider and decrease the cost and risk of user identity management. In the framework of FIM protocol, the users take browser as user agent to interact with service provider and identity authority. When users visit service, authorization of authentication is requested and service provider will transfer authentication to trusted identity authority. Identity authority verifies the user and produces a security token for user and the user provides it to service provider for authorization of authentication. Main FIM products include Passport of Microsoft as well as the following products Cardspace and Cardspace2.0 (name updated as U-Prove), Athens and its replacement Shibboleth, liberty alliance project based on security assertion markup language (SAML).

At present, the security of these FIM methods can't be guaranteed adequately and a great number of articles have reported the numerous possible attacks that FIM may suffer (see chapter two), especially some problems based on server in reality:

1. Related researches have shown that common internet users can't understand server certificate and can't identify the safety indicator of server in a better way.

2. All the data sent by service is saved in document object model of server (DOM), which is only protected by same origin policy (SOP). However, SOP can be easily cheated by related attacks for domain name resolution, which include cross site attack and domain deception attack etc. and make all the data may possibly be visited by malicious script.

3. Server can only produce tokens through identity authority and transfer data through TLS encryption protection, so these tokens can't be combined with legal client through encryption method and then can be used easily by attacker used above attack method to steal tokens.

This paper has proposed one Bi-directional Authentication Protocol for Federated Identity Management (BBFIM), whose contents include:

- Bi-direction authentication of user perceived and identity authority: considering about reducing the dependence of users on fixed server and external equipment as well as the insecurity of static password, the user verification method is one time password (OTP), (combined with static password is optional), the verification of identity authority needs to provide a human perceptible authenticator (HPA) reserved by user, such as text, voice and image etc.
- Through strengthening the authentication of SOP for server: identity authority produces one token, in addition, it also provides the pair of all service providers (server, public key) within federation for browser, which has been taken as the source factor of SOP to strengthen the verification of the server.
- Binding of token and legal client: identity authority provides a client certificate for browser and bines token with public key certificate. Considering about that attackers can't visit the private key of certificate, so even if the attackers attain tokens, they can't prove their legal possession of client certificate and can't use the tokens normally.

The organization structure is this paper is as following: the second chapter introduces related researches, the third chapter offers formal security model of authentication protocol based on browser, the fourth chapter describes and analyzes the proposed protocol and finally summarizes.

## II. FORMAL SECURITY MODEL OF SOFTWARE SYSTEM STRUCTURE

### *A. Participant of Protocol and Corresponding Ability and Secret key*

The participants of protocol include server of identity authority $I$, provider of service $S$, client $C := (U, B)$, in which $B$ is browser and $U$ is user. The model of $U$ is probabilistic machine with limited calculation ability, which can recognize HPA and can make use of one out of band means (such as short message or password card) to attain one time password.

Define the secrete keys of $U$ as long-term secret keys $LL_U := (uname, OTP(k), w \in W)$, which include username of $I$ registered through one out of band means, HPA as wlel as OTP acquisition method, in which $k \in \square$ is the security parameter of protocol and $W$ is HPA space. $B$ is a machine of probabilistic polynomial time (PPT) exchanging protocol information with server. Browser is responsible for processing the received message $m \in M$ based on the status of browser $\psi \in \{0,1\}^{\lambda_1(k)}$, which includes presenting HPA to user and saving token information, in which $M \in \{0,1\}^{\lambda_2(k)}$ refers the massage space of all web objects, $\lambda_i : \square \to \square, i \in [1,2]$ is a polynomial, $\psi$ refers to the configuration of browser for message processing can be revised by DOM model of browser. In addition, browser $B$ can receive user input with different device interfaces, such as mouse and keyboard etc. Define its secret key as short-term secret key $SL_B^{Aftaut} := (cert_B, sk_B, token^*, \{(S, pk_S) \mid S \in FS\})$, including certificate of user generated after certified by $I$, cryptographic token as well as pair of $S$ (domain name, public key) within all federations, users delete when exit (optional) and exist some term of validity. Identity authority server $I$ is common PPT machine and define its secret key as long-term secret key $LL_I := (cert_I, sk_I, (uname, OTP(k), w), \{(S, pk_S) \mid S \in FS\})$, including certificate and corresponding private key, long-term secrete key shared with user, all pairs of $S$ (domain name, public key) with federation $FS$. Service provider is common PPT machine and defines its secret key as long-term secret key $LL_S := (cert_S, sk_S, cert_I)$, including certificate and corresponding private key and public secret certificate of $I$.

### B. Ability of Attacker

Opponent $A$ can control all communication process and can make the user accept the forged server certificate through controlling domain name resolution and then enable $A$ visit the DOM model of browser.

Considering about the malicious software attack of operation system can destroy the security of all encryption protocol, this paper did not consider about the malicious software attack of opponent $A$ to browser $B$ as well as the platforms of server $I$ and $S$, therefore, $A$ can't steal the secret information stored in platform, such as certificate private key. At the same time, opponent attaining the secret key of user through physical means has not been considered.

Define $A$ to participate the execution of protocol through following requests:

- $Execute(C, P)(P \in \{I, S\})$: wire tap the execution of protocol conversation and attain corresponding conversation copy;
- $Invoke(C, P)(P \in \{I, S\})$: implement one new protocol case and attain the first protocol message through $B$;
- $Send(P, m)(P \in \{C, I, S\})$: send a message to one protocol participant and receive corresponding response;
- $RevealDOM(C)$: steal the stored information in server DOM.

### C. Attack Game

To differentiate different cases, each protocol participant uses one $cid \in \square$ to express communication identifier. When $cid_C = cid_S$ or $cid_C = cid_I$, we believe that two cases belong to one conversation, called as two cases matching. If the two make successful authentication during execution, then mutually accept, or else cases suspense. Definition is given as following:

Definition 1: when each $Execute(C, P)(P \in \{I, S\})$ request result produces two matching cases and mutually accepted, we regard $\Pi$ of BBFIM protocol correct.

Definition 2: presume $\Pi$ of BBFIM protocol is correct, $Game_{\Pi}^{BBFIM}(A, k)$ is the cases of $C$, $I$, $S$ and complies with the interaction process of $A$, the opponent of above ability presumption.

1. Case $[S, cid_S]$ with one case $[C, cid_C]$ accepts but without matching, or on the contrary;
2. Case $[I, cid_I]$ with one case $[C, cid_C]$ accepts but without matching, or on the contrary.

For all PPT opponents operating with security parameter $k$, define the biggest possibility of wining attacking game as:

$$Succ_{\Pi}(A, k) = \max_A \mid \Pr[A.wins.in.Game_{\Pi}^{BBFIM}(A, k)] \mid$$

When this function is the negligible function of $k$, we say protocol $\Pi$ can provide safe authentication.

## III. SECURITY PROTOCOL

### A. Encryption Module

The main component of BBFIM is TLS protocol, which accomplishes authentication after secret key negotiation. This paper uses the most common encryption component based on RSA in the protocol specifications, including the following (to construct the negligible function of $k$, the protocol transfers the following encryption module form into probabilistic turing machine operating on the polynomial time of $k$, that is construct difference lengths with different parameters with polynomial $p_i : \square \to \square, i \in [1,5]$ )

- Pseudo random function $PRF_i : \{0,1\}^{p_i(k)} \times \{0,1\}^* \to \{0,1\}^*, i \in [1,4]$, this function is used to derive the secret key of different lengths. Use $Adv_{PRF}^{prf}(k)$ to define the biggest advantage of all PPT opponents in recognizing $PRF$ output.
- Provide CUF-CPA security function $MAC\text{-}Enc$ and corresponding verification function $Dec\text{-}MAC$, this function first calculates message verification code and then make symmetric encryption, define the symmetric encryption algorithm as $(sEnc, sDec)$, message verification code function as $MAC$, and then $Dec\text{-}MAC_{k_1,k_2}(m^*, m) := (sDec_{k_1}(m^*) == m \mid MAC_{k_2}(m))$, $MAC\text{-}Enc_{k_1,k_2}(m) := sEnc_{k_1}(m \mid MAC_{k_2}(m))$, in which $m$ is transmission message. Use $Adv_{MAC\text{-}Enc}^{cuf\text{-}cpa}(k)$ to define the biggest advantage of all PPT opponents in destroying the security of CUF-CPA. On the basis of literature [6], regard message verification code function and symmetric encryption function as one function, because the message transmission always calculates message verification code first and then makes encryption; its security is determined by both [13].
- Provide asymmetric encryption algorithm of IND-CPA security. Use $Adv_{(asEnc,asDec)}^{ind\text{-}cpa}(k)$ to define the best advantage

of all PPT opponents destroyed $(asEnc, asDec)$ IND-CPA security.

- Anti-conflict harsh function $Hash: \{0,1\}^* \to \{0,1\}^{p_2(k)}$. Use $Succ^{coll}_{Hash}(k)$ to define the biggest possibility of all PPT opponents in finding a harsh conflict successfully.
- Provide digital signature function $Sig$ of EUF-CMA security and corresponding verification function. Use $Succ^{euf\text{-}cma}_{(Sig,Ver)}(k)$ to define the biggest possibility of all PPT components with signature oracle in finding a forged signature successfully.

### B. Protocol Description

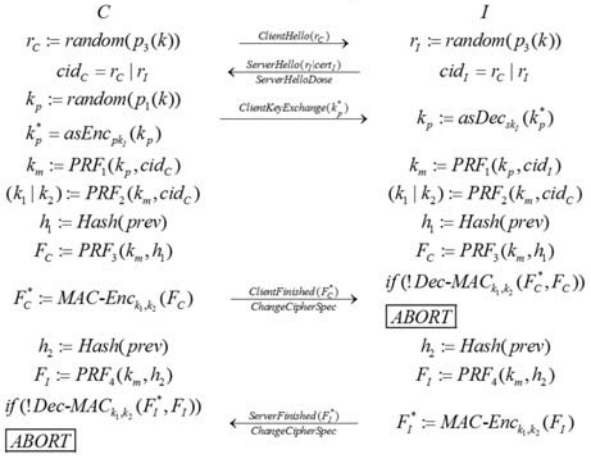
(1) Initialization stage.

Before protocol execution, it needs some registration process to accomplish following interaction or registration (these interaction processes are generally some out of band mechanisms or ensuring the safety of internet channel through other ways, such as supervision software etc):

- $C$ registers username and HPA to $I$ and attains the attaining method $OTP(k) \in \{0,1\}^{p_4(k)}$ of one time password out of band, such as password cark or registration mobile phone number. To simplify protocol, here presume to attain directly with password card.
- $C$ and $S$ register own private key and certificate pair, here presume that the corresponding public key can be attained from certificate.
- Interaction $(S, pk_S)$ between $C$ and $S$ as well as $cert_I$.

(2). Interaction between $C$ and $I$.

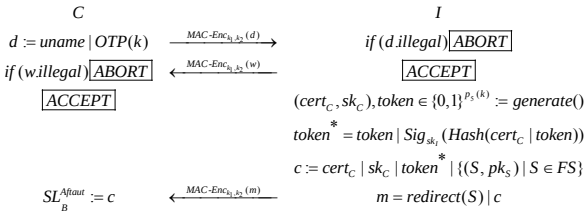
When $C$ requests service to $S$ through URL, if $B$ exists $SL^{Aftaut}_{B}$, then the protocol enters 4.2.3 directly, or else $S$ makes $C$ interact with $I$ first through redirection code.




Picture 1. secret key negotiation between $C$ and $I$

During request stage, both parties exchange own random number and calculate to attain communication identifier $cid_C = r_C \mid r_I$, at the same time, $I$ sends certificate to $C$. During secret key negotiation stage, conversation secret key (including symmetric secret key $k_1$ and MAC secret key $k_2$) is produced through main secret key $k_m$, $k_m$ is produced by pre-main key $k_p$, $k_p$ is selected by $C$ randomly and transmit to $I$ encrypted through $pk_I$. $C$ and $I$ start from all former processed message, first hash, and then calculate PRF, encrypted through conversation secret key and accomplish the confirmation of mutual conversation secret key. As shown in picture 1.

At encryption transmission stage, $C$ sends username and one-time password to $I$ for verification, $I$ sends corresponding $w$ to $C$ after successful authentication. After mutual authentication between $C$ and $I$, $I$ generates token and certificate for client and send them and $(S, pk_S)$ to $C$, in which it needs to bind token and certificate public key and make encryption through symmetrical secret key $k_{IS}$, $C$ save it in browser, that is $SL^{Aftaut}_{B}$. As shown in picture 2, in which omit the default authentication of $Dec\text{-}MAC_{k_1,k_2}$.



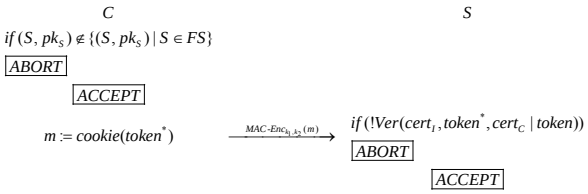

Picture 2. Mutual authentication between $C$ and $I$

(3) Interaction between $C$ and $S$.

The request stage and secret key negotiation stage is the same as 4.2.2, which only increases the authentication for client certificate. Realize through certificate private key signature and the signature content is the hash of all former processed message, as shown in picture 3:


Picture 3. Client certificate authentication between $C$ and $S$

Encryption transmission stage, $C$ judge if $(S, pk_S)$ pair is in $SL^{Aftaut}_{B}$, for legal $S$, $C$ send cookie with $token^*$ to $S$, or else send one empty cookie, $S$ adopts $k_{IS}$ to decrypt and verifies its $pk_C$, as shown in picture 4, in which omit the default authentication of $Dec\text{-}MAC_{k_1,k_2}$.




Picture 4. mutual authentication between $C$ and $S$

### C. Security Analysis

We will analyze the security of BBFIM protocol in the following, make $q$ as the biggest number of protocol conversation of opponent $A$ in participating $Game^{BBFIM}_{\Pi}(A,k)$ execution.

(1) Attack for $C/I$ interaction.

1) When inject on pseudo server certificate to $A$, the security of protocol depends on the mutual authentication

method in the protocol, which includes one time password and HPA guessing. Presume the attaining method of OTP is random for $A$ and $A$ can't forge HPA not registered by user while not be discovered by user, then the upper probability limit destroyed by $A$ is $Succ_{CI}^{InjCert}(A,k) \le \frac{q}{2^{p_4(k)}} + \frac{q}{|W|}$

2) Or else, the security of protocol depends on whether TLS protocol is destroyed by $A$. For the destroy of each secret calculation of TLS in protocol (including random number and encryption module), construct a series of attack games (this paper will not list the details), apply the simultaneous method in [10], and then attain the upper probability limit of TLS protocol destroyed by $A$ is:

$$Succ_{CI}^{NoInj}(A,k) \le \frac{2q^2}{2^{p_3(k)}} + \frac{q^2}{2^{p_1(k)}} + 4qAdv_{PRF}^{prf}(k) + 4qAdv_{MAC\text{-}Enc}^{cuf\text{-}cpa}(k) + qAdv_{(asEnc,asDec)}^{ind-cpa}(k) + 2qSucc_{Hash}^{coll}(k)$$

(2). Attack for $C/S$ interaction

1) When inject one pseudo server certificate to $A$, the security of protocol depends on the mutual authentication method in the protocol, which includes token guessing and forge of $(S, pk_S)$ pair, its upper probability limit destroyed by $A$ is $Succ_{CS}^{InjCert}(A,k) \le \frac{q}{2^{p_5(k)}} + qAdv_{(sEnc,sDec)}^{ind-cpa}(k) + q_{CI}^{NoInj} + q_{CI}^{InjCert}$.

2) Or else, whether the security of protocol based on TLS protocol will be destroyed by $A$. At the same time, the upper probability limit of TLS protocol destroyed by $A$ is as following:

$$Succ_{CS}^{NoInj}(A,k) \le \frac{2q^2}{2^{p_3(k)}} + \frac{q^2}{2^{p_1(k)}} + 4qAdv_{PRF}^{prf}(k) + 3qAdv_{MAC\text{-}Enc}^{cuf\text{-}cpa}(k) + qAdv_{(asEnc,asDec)}^{ind-cpa}(k) + 3qSucc_{Hash}^{coll}(k) + qSucc_{(Sig,Ver)}^{euf-cma}(k)$$

Finally we can draw the following conclusion: if $PRF$ is standard pseudo random function, $(MAC\text{-}Enc, Dec\text{-}MAC)$ is with CUF-CPA security, $(asEnc, asDec)$ is with IND-CPA security, $Hash$ anti-conflict, $(Sig, Ver)$ is with EUF-CMA and then protocol $\Pi$ provides the safe authentication in definition 2. In fact, these security presumptions under TLS protocol specification are effective, because RSA encryption （PKC#1 or RSA-OAEP）regulated in protocol already has been verified with IND-CPA security under ROM [11]. RSA signature regulated in protocol （PKCS#1 or RSA-PSS） has been verified with EUF-CMA security[12] under ROM, in addition, Krawczyk has proven that the structure with MAC first and then encryption in TLS is with CUF-CPA security[13].

## IV. CONCLUSION

Authentication based on browser has become the attack target of various attacks due to is universality and vulnerability. This paper has introduced a authentication protocol based on browser and federated identity management and made the weakest security presumption for user: can't understand server certificate, evaluate webpage only through easily recognizable indicator, but can identify human perceptual authentication code and can use some offline safety authentication method, including dynamic password token and external security certificate etc. The protocol strengthens the security model of browser; strengthen the authentication for server through realizing SLSO strategy, at the same time, bind security token and client public key certificate together to ensure the legitimacy of client. Finally analyzed the security of protocol and verified that the protocol can provide safe authentication under DOM attack.

## REFERENCES


[1] Fett D, Sters R, Schmitz G. SPRESSO: A Secure, Privacy-Respecting Single Sign-On System for the Web[C]// ACM Sigsac Conference on Computer and Communications Security. ACM, 2015:1358-1369.

[2] Zhang M H. Design and Implementation of a Succinct Single Sign on System[J]. Computer Programming Skills & Maintenance, 2014.

[3] Li W, Zhu Y B, Zou M. Applied Research of Single Sign on Technology in Cloud Services[J]. Applied Mechanics & Materials, 2014, 602-605:3552-3555.

[4] Yang S, Yao X. Implementation of CAS Server as Authentication Protocol on Single Sign-On (SSO) Network With PHP Programming[C]// Icetia. 2014:815-834.

[5] Jinyu Hu and Zhiwei Gao. Distinction immune genes of hepatitis-induced heptatocellular carcinoma[J]. Bioinformatics, 2012, 28(24): 3191-3194.

[6] Liu, Y., Yang, J., Meng, Q., Lv, Z., Song, Z., & Gao, Z. (2016). Stereoscopic image quality assessment method based on binocular combination saliency model. Signal Processing, 125, 237-248.

[7] Jinyu Hu, Zhiwei Gao and Weisen Pan. Multiangle Social Network Recommendation Algorithms and Similarity Network Evaluation[J]. Journal of Applied Mathematics, 2013 (2013).

[8] Yishuang Geng, Jin Chen, Ruijun Fu, Guanqun Bao, Kaveh Pahlavan, Enlighten wearable physiological monitoring systems: On-body rf characteristics based human motion classification using a support vector machine, IEEE transactions on mobile computing, 1(1), 1-15, Apr. 2015

[9] Lv, Z., Halawani, A., Feng, S., Ur Réhman, S., & Li, H. (2015). Touch-less interactive augmented reality game on vision-based wearable device. Personal and Ubiquitous Computing, 19(3-4), 551-567.

[10] Jinyu Hu and Zhiwei Gao. Modules identification in gene positive networks of hepatocellular carcinoma using Pearson agglomerative method and Pearson cohesion coupling modularity[J]. Journal of Applied Mathematics, 2012 (2012).

[11] Jiang, D., Ying, X., Han, Y., & Lv, Z. (2016). Collaborative multi-hop routing in cognitive wireless networks. Wireless personal communications, 86(2), 901-923.

[12] Songprasop P. Integrated Single Sign-On System on Open Nebula[J]. Universiti Teknologi Petronas, 2014.

[13] Suoranta S, Manzoor K, Tontti A, et al. Logout in single sign-on systems: Problems and solutions[J]. Journal of Information Security & Applications, 2014, 19(1):61-77.

[14] Kim S, Oh H T. System and method for single-sign-on in virtual desktop infrastructure environment[J]. 2016.

[15] Sharaga A, Luft A. Multi-hop single sign-on (SSO) for identity provider (IdP) roaming/proxy: WO, US9258344[P]. 2016.

[16] Fett D, Kusters R, Schmitz G. An Expressive Model for the Web Infrastructure: Definition and Application to the Browser ID SSO System[J]. Computer Science, 2014:673-688.

[17] Yang S, Yao X. Implementation of CAS Server as Authentication Protocol on Single Sign-On (SSO) Network With PHP Programming[C]// Icetia. 2014:815-834.

[18] Hope P, Zhang X. Examining user satisfaction with single sign-on and computer application roaming within emergency departments.[J]. Health Informatics Journal, 2015, 21(2):107-19.

[19] Xie Q R. Design and Implementation of Campus Culture Service Module on Library Unified Information System[J]. Applied Mechanics & Materials, 2014, 687-691:2780-2783.

[20] Lv, Z., Réhman, S. U., & Chen, G. (2013, November). Webvrgis: A p2p network engine for vr data and gis analysis. In International Conference on Neural Information Processing (pp. 503-510). Springer Berlin Heidelberg.

[21] Li, X., Lv, Z., Zheng, Z., Zhong, C., Hijazi, I. H., & Cheng, S. (2015). Assessment of lively street network based on geographic information system and space syntax. Multimedia Tools and Applications, 1-19.

[22] Zhang, X., Han, Y., Hao, D., & Lv, Z. (2015, November). ARPPS: Augmented reality pipeline prospect system. In International Conference on Neural Information Processing (pp. 647-656). Springer International Publishing.

.