Weaknesses of SIP Authentication Scheme for Converged VoIP Networks

Q. Pu

***Abstract*—The Session Initiation Protocol (SIP) is commonly used to establish Voice over IP (VoIP) calls. Mostly recently, Yoon et al. proposed an efficient SIP authentication scheme in a converged VoIP network based on elliptic curve cryptosystem (ECC). In this letter, we first demonstrate that it is insecure against off-line password guessing attacks.**

***Index Terms*—Voice over Internet Protocol; Session Initial Protocol; elliptic curve; authentication.**

I. Introduction

Voice over Internet Protocol (VoIP) is a fast growing technology believed to be the future replacement for traditional Public Switched Telephone Network (PSTN). There are many protocols used in VoIP signaling, but Session Initiation Protocol (SIP)[1] is one of the widely used ones. It has been chosen by the Third-Generation Partnership Project (3GPP) as the protocol for multimedia application in 3G mobile networks. SIP is an application-layer protocol that is capable of handling all the signalling requirements of a VoIP session, i.e. initiating, managing and terminating voice and video sessions across packet networks. It is analogous to the SS7 protocol[2] in traditional telephony. Security and privacy requirements in a VoIP environment are expected to be equivalent to those in PSTN.

SIP is a text-based client-server protocol. When a user requests to use an SIP service, he needs to be authenticated first before getting the service from the server. In SIP specification [1], the authentication mechanism proposed is HTTP digest based authentication[3]. However, it was found vulnerable to the off-line password guessing attacks and the server spoofing attacks[4]. Yang et al. [4] proposed a SIP authentication scheme but it is not suitable for devices with a low computational power because it works only for Discrete Logarithm (DL) settings and involves in costly exponential computation. Unlike many legacy Time Division Multiplex (TDM) voice networks that are physically separated from data-centric networks, the new VoIP networks allow the convergence of networks. Therefore, the services that are enabled by SIP should be equally applicable to mobile and ubiquitous computing [5]. To meet this goal, based on Yang et al.'s scheme, Yoon et al.[5] quite recently proposed a new SIP authentication scheme in a converged VoIP network using elliptic curve cryptosystem (ECC), which has the well-known advantages with regard to processing and size constraints[6]. In this letter, we demonstrate Yoon et al.'s scheme[5] is still vulnerable to off-line password guessing attacks.

E-mail: pqwsh@yahoo.com.cn.
Manuscript received April 15, 2010.

II. Review of Yoon et al.'s Scheme

Yoon et al.'s scheme consists of three phases: the system setup phase, the enrollment phase, and the authentication phase. Here, we just follow the description in [5].

System Setup Phase: The server S choose an elliptic curve $\mathcal{E} : y^2 = x^3 + ax + b$ over a prime finite field F_p and finds a point P in $\mathcal{E}$ with large prime order q. Let G be the cyclic addition group generated by P. Here we believe Elliptic Curve Computational Diffie-Hellman (ECCDH) assumption holds in G: i.e., given uP and vP, where u and v are drawn randomly from Z_q^*, it is computationally infeasible to compute uvP. Then S chooses a one-way hash function $F : \{0,1\}^* \rightarrow \{0,1\}^l$, where l is the security parameter. Finally, S publishes the following system parameters (G, q, P, F). Any user U must agree on these system parameters.

Enrollment Phase: If U with an identity username and password pw wants to register at the SIP server S and become a new legal user, he/she computes $F(pw)$ and sends $\{\text{username}, F(pw)\}$ to S over a secure channel. Then S computes $V = F(pw) \oplus F(\text{username}, k)$ and saves (username, V) in the verification database table, where k is a secret key of S and $\oplus$ is bit-wise exclusive-or(XOR) operation. Here, the purpose of V is to prevent stolen verifier attacks.

Authentication Phase: Yoon et al.'s SIP authentication scheme proceeds as follows.

1) U generates a random integer c, computes $cP \oplus F(pw)$, and then sends it with a request message as REQUEST(username, $cP \oplus F(pw)$) to S.
2) Upon receiving the request message, S extracts $F(pw)$ by computing $V \oplus F(\text{username}, k)$ with his private key k and derives cP by computing $cP \oplus F(pw) \oplus F(pw)$. Then, S generates a random integer s, and computes a common secret session key $sk = scP$ and a message authentication code $F(\text{username}, sk)$. Finally, S sends a challenge message CHALLENGE(realm, sP, $F(\text{username},sk)$) to U.
3) Upon receiving the challenge message, U computes a secret session key $sk = scP$. Then, U computes $F(\text{username}, sk)$ and verifies whether it is equal to the received challenge $F(\text{username}, sk)$. If they are not equal, U rejects the server challenge message. Otherwise, U authenticates S and computes a message authentication code $F(\text{username, realm, } sk)$. Finally, U sends a response message RESPONSE(username, realm, $F(\text{username, realm, } sk)$) to S.
4) Upon receiving the response message, S computes $F(\text{username, realm, } sk)$ and verifies whether it is equal to the received response $F(\text{username, realm, } sk)$. If they

are not equal, S rejects the user response message. Otherwise, S authenticates U and accepts the user's login request. After mutual authentication between U and S, $sk = csP$ is used as a shared session key.

III. Weaknesses of of Yoon et al.'s Scheme

Unfortunately, Yoon et al.'s scheme[5] described above is completely insecure. In this section, we will show it is vulnerable to an off-line password guessing attack.

Off-line password guessing attack succeeds when there is information in communications, which can be used to verify the correctness of the guessed passwords. In [5], Yoon et al. claimed that their scheme can resist the off-line password guessing attack. However, we can show that the off-line password guessing attack, not as they claimed, is still effective. In Yoon et al.'s scheme, since all transcripts are transmitted over an open network, a benign (passive) adversary, can easily obtain the valid message transcript of $cP \oplus F(pw)$. The adversary can guess a password pw^* from the dictionary $\mathcal{D}$ and derive the corresponding $(x^*, y^*) = cP \oplus F(pw) \oplus F(pw^*)$, then verify it by checking $(y^*)^2 \stackrel{?}{=} (x^*)^3 + ax^* + b(\mod p)$. Clearly, if pw^* is not correct, the computation $cP \oplus F(pw) \oplus F(pw^*)$ should result in a random pair (x^*, y^*). Even if $x^*, y^* \in F_p$, the probability that the point (x^*, y^*) falls on $\mathcal{E}$ is no larger than $\frac{2}{p}$. Typically $|\mathcal{D}|$ is much less than p. Therefore, the adversary should be able to identify the correct password pw given one valid message transcript of $cP \oplus F(pw)$ using such a dictionary attack, with a probability of $(1 - \frac{2}{p})^{|\mathcal{D}|-1} \approx 1 - \frac{2(|\mathcal{D}|-1)}{p}$. Please note, the attack is a brute-force method in essence, i.e. the attacker tries offline all possible passwords in a given small set of values. Even though such attacks are not very effective in the case of high-entropy keys, they can be very damaging when the secret key is a password since the attacker has a non-negligible chance of winning.

In addition, we point out that the key derivation phase is deliberately omitted in Yoon et al.'s scheme. Key derivation refers to the process by which an agreed upon large random number, often named master secret, is used to derive session keys to encrypt and authenticate data. As a result, an adversary can obtain some information about the session key although an adversary is unable to obtain the whole key. More specifically, it can reliably distinguish between the session key sk and a randomly chosen string of the expected length simply by checking if sk is a point on elliptic curve or not. In some sense, this is another weakness of the protocol. Indeed, the key derivation phase is a crucial step for theoretical reasons, but also practical purpose, and can not be omitted.

Finally, it is worth of noticing that similar attacks can be applicable to Durlanik et al.'s scheme [10] and Wu et al.'s scheme [11]. Please note Yoon et al. did not find such weaknesses in [5]. Since the rationale for it is the same with the attack described above, the description is omitted here.

References

[1] J. Rosenberg et al., SIP: Session Initiation Protocol, IETF RFC 3261, June2002.

[2] International Telecommunications Union. ITU-T Recommendation Q.700: Introduction to CCITT Signalling System 7. Recommendation Q.700, International Telecommunications Union, March 1993.

[3] J. Franks et al., HTTP authentication: basic and digest access authentication, IETF RFC 2617, June (1999).

[4] C. C. Yang et al., Secure authentication scheme for session initiation protocol, Computer & Security (24) (2005) 381-386.

[5] E-J. Yoon, K-Y. Yoo, C. Kim, Y-S. Hong, M. Jo, H-H. Chen, A Secure and Efficient SIP Authentication Scheme for Converged VoIP Networks, Computer Communications (2010), doi: 10.1016/j.comcom. 2010.03.026.

[6] D. Hankerson, A. Menezes, S. Vanstone. Guide to elliptic curve cryptography. Springer-Verlag, New York, USA, 2004.

[7] Y-P. Liao, S-S. Wang, A New Secure Password Authenticated Key Agreement Scheme for SIP using Self-Certified Public Keys on Elliptic curves, Computer Communications (2009), doi: 10.1016/ j.comcom.2009.10.005.

[8] F. Wang and Y. Zhang , A new provably secure authentication and key agreement mechanism for SIP using certificateless public-key cryptography, Computer Communication, 31.(2008) 2142-2149.

[9] M. Bellare, D. Pointcheval, P. Rogaway. Authenticated key exchange secure against dictionary attacks. Proc. of EUROCRYPT'2000. Berlin, Germany:Springer-Verlag, 2000: 139-155.

[10] A. Durlanik, I. Sogukpinar, SIP authentication scheme using ECDH, World Enformatika socity Transaction on Engineering computing and technology 8 (2005) 350-353.

[11] L. Wu et al., A new provably secure authentication and key agreement protocol for SIP using ECC, Computer Standard & Interfaces, 31 (2) (2009) 286-291.