A Generic Framework for Three-Factor Authentication

Jiangshan Yu[1] Guilin Wang[2] Yi Mu[2] Wei Gao[3]

[1]School of Computer Science
University of Birmingham, UK

[2]School of Computer Science and Software Engineering
University of Wollongong, AU

[3]Department of Mathematics and Informatics
Ludong University, China

March, 2013

Outline of Topics

Password Based Authentication

- 1st Factor: something the client knows.
  e.g. Password, PIN number.
- Applications: TSB Internet banking, Google mail, Dropbox, ConfiChair, Facebook etc.
- Problems: lower entropy, poor selection of password.
- Common powerful attacks: off-line dictionary attack, phishing attack.

Two-Factor Authentication

- 1st+2nd Factor: something the client has.
  e.g. smart card, YubiKey, iTwin, mobile phone, etc.
- Applications: some Internet banking services, on-line games, etc.
- Problems: hardware token may be stolen or lost.
  Data stored in it can be extracted.

Biometric Based Authentication

- 3rd Factor: something the client is.
  e.g. fingerprint, iris, etc.
- Applications: Gate access control, laptop, etc.
- Example: 'fuzzy commitment' [1]
- Problem: biometric features are **totally public**.

[1] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," *ACM CCS, 1999, pp. 28-36.*

Three-Factor Authentication

Three-Factor Authentication

Three-Factor Authentication

Three-Factor Authentication

Still secure even when (any) two factors are corrupted.
Example:

C.-I. Fan and Y.-H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics," *IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, pp. 933-945, 2009.*

Four-Factor Authentication

- 4th Factor: somebody the client knows[2].
- Example: Web of Trust.

[2] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, M. Yung, "Fourth Factor Authentication: Somebody You Know", *ACM CCS, 2006.*

Motivation

Problems:

- Error tolerance has not been considered properly in the existing 3-factor schemes.
- Most existing 3-factor authentication schemes have security problems and privacy issues. [2, 3, 4, 5, 6, 7, 8, 9, 10, 11]

Motivation Cont.

- Goal: provably secure 3-factor authentication schemes.
  - Privacy (i.e. user biometric features) should be protected at least against remote adversaries (e.g. untrusted servers).
  - Errors of biometric data are able to be tolerated.
- Hint A: there are many provably secure two-factor authentication schemes.
- Hint B: there exist secure biometric identification schemes which support error tolerance.
- Solution: Hint A + Hint B $\Longrightarrow$ framework of 3-factor authentication.

Framework A[3]

- Two-factor authentication scheme: PWD + SC
- 'Fuzzy extractor' [12]
  - Gen(BioData)$\longrightarrow$ (sk,pk)
    sk: (nearly) random string
    pk: Auxiliary String
  - REP(BioData',pk) $\longrightarrow$ sk if they are in an error tolerance.
- Run twice two-factor authentication scheme
  - 1^{st} run: PWD+SC
  - 2^{nd} run: reproduce sk, then sk+SC

[3] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. Deng, A generic framework for three-factor authentication: Preserving security and privacy in distributed systems," *IEEE Transactions on Parallel and distributed systems, vol. 22, no. 8, pp. 1390-1397, Aug.2011.*

Framework A Cont.

Problems:

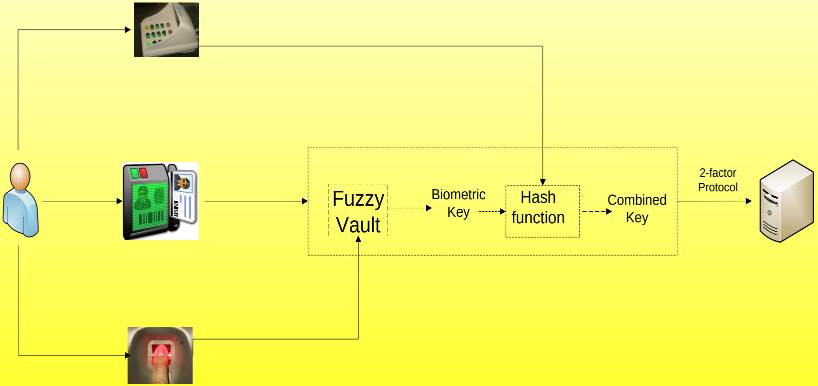
- Error tolerance: Hamming distance, set difference and edit distance.
  These distance measures are less accepted than the Euclidean distance measurement in real biometric applications [13].
- The 'fuzzy extractor' has not been implemented.
- Twice run is neither efficient nor necessary.

Framework B

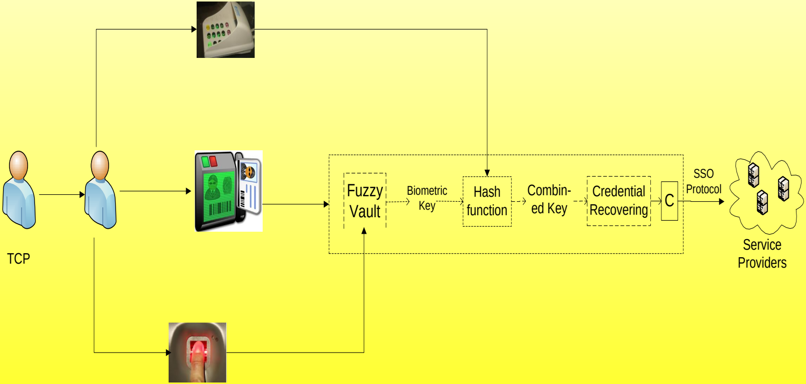
- Two-factor authentication scheme: PWD + SC
- 'Fuzzy vault' [4]
  Unlock(BioData',Lock(BioData,K)) $\longrightarrow$ K, if BioData and BioData' are close.

[4] A. Juels and M. Sudan, "A fuzzy vault scheme," *International Symposium on Information Theory (ISIT), 2002, p. 408.*

Framework B Cont.A



Framework B Cont.B



Analysis

- Error tolerance is guaranteed by employing ‘fuzzy vault’.
- Security relies on 2-factor scheme & ‘fuzzy vault’.
- Privacy is preserved according to ‘fuzzy vault’.

A little more

A concrete authentication scheme is presented with

- a comparison with other 6 three-factor authentication schemes;
- usability analysis;
- security proof (game based model);
- privacy discussion.

A concrete scheme

1. G. Yang, D. S. Wong, H. Wang, and X. Deng, "Two-factor mutual authentication based on smart cards and passwords," *J. Comput. Syst. Sci., vol. 74, pp. 1160-1172, November 2008.*
2. A. Nagar, K. Nandakumar, and A. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," *19th International Conference on Pattern Recognition, Dec. 2008, pp. 1-4.*
   K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance." *IEEE Transactions on Information Forensics and Security, vol. 2, no. 4, pp. 744-757, 2007.*

A concrete scheme cont.A

Registration

We assume the communication channel in this phase is secure.

1. User U chooses a finger, a password PW_1, a long random bit string PW_2, and calculates $PW = h(PW_1||PW_2)$.
2. $U \rightarrow S$: $V = Lock(X, PW_2)$, where X is the biodata of the chosen finger.
3. $S \rightarrow U$:$SC = (ID, B = C \oplus PW_{Init}, V)$, where $C = PRF_k(h(ID))$.
4. U updates B in SC by computing $B = C \oplus PW_{init} \oplus PW$.

A concrete scheme Cont.B

Login-and-Authentication Phase

1. User inserts smart-card, enters password PW_1', scans fingerprint, runs $Unlock(V, X') = PW_2'$ and calculates $C' = B \oplus PW'$, where $PW' = h(PW_1'||PW_2')$
2. $U \rightarrow S$: $M_1{=}(ID, sid, g^a)$;
3. $S \rightarrow U$: $M_2{=}(SID, sid, g^b, Sig_{SK}(SID, ID, sid, g^a, g^b))$
4. $U \rightarrow S$: $M_3{=}(ID,\ sid,\ CT)$, where $CT{=}E_{PK}(C', ID, SID, sid, g^a, g^b)$
5. S checks C' and believes that they share the same session key g^{ab} if C' is valid.

Comparison

Properties / Name of scheme	Store Password or Biodata in DB	Cost		Change password freely	Biometrics privacy	Key Exchange	Security
		Registration phase	Login-and-Authentication phase				
Li and Hwang's scheme [9]	×	L1	L1	√	×	×	Vulnerable to man-in-the-middle attack
Li *et al.*'s scheme[10]	×	L1	L1	√	×	√	Fails to provide strong authentication
Das's scheme[11]	×	L1	L1	√	×	√	Vulnerable to Off-line guessing password attack
Kim-Lee-Yoo scheme [2]	×	2 Exp	4 Exp	√	√	×	Vulnerable to impersonation attack
Bhargav -Spantze *et al.*'s scheme[7, 6]	√	3 Exp	5 Exp	×	√	×	Secure under three-factor requirements
Fan and Lin's scheme [8]	√	L1&L2	1 E/D	×	√	√	Secure under three-factor requirements
Proposed scheme	×	L1	1 DH; 1 Sig; 1 E/D	√	√	√	Secure under three-factor requirements

X: False
√ : Truce
L1: The phase only contains the hash operation and exclusive operation
L2: The phase employs symmetric key encryption/decryption
E/D: The phase compute once asymmetric key encryption and decryption
Exp: The phase calculate once large exponentiation computation
Sig: The participator signs and verifies once digital signature
DH: The plain Diffie-Hellman key exchange operation

Table: Comparison of Schemes

Adversary Model (AM)

1. $Register(\prod, S)$
2. $Execute(U, S, sid)$
3. $Send(U, S, sid, M_i, i)$
4. $Send(S, U, sid, M_j, j)$
5. $Reveal(\prod, U, S, sid)$
6. There are three corrupt queries:
   1. $Corrupt(U, pw, SC)$.
   2. $Corrupt(U, pw, Bio)$.
   3. $Corrupt(U, SC, Bio)$.

   In a concrete attack, A can only make one corrupt query on the target user.
7. $Test(U, S, sid)$

Definitions (A)[5]

Definition

(Matching Conversations): Fix number of moves $R = 2\rho - 1$ and R-move protocol $\prod$. Run $\prod$ in the presence of adversary A in the AM and consider two oracles $\prod_{S,U}^{sid}$ and $\prod_{U,S}^{sid}$ that engage in conversations K and K', respectively. (τ, β, α) denotes that α is answered according to message β at time τ. If $\beta = \lambda$, then it means that protocol $\prod$ starts a new session. Let $*$ denotes the final decision of R-move protocol $\prod$.

1. *We say that K' is a matching conversation to K if there exist $\tau_0 \prec \tau_1 \prec \ldots \prec \tau_R$ and $\alpha_1, \beta_1, \ldots, \alpha_\rho, \beta_\rho$ such that K is prefixed by $(\tau_0, \lambda, \alpha_1)$, $(\tau_2, \beta_1, \alpha_2)$, … , $(\tau_{2\rho-4}, \beta_{\rho-2}, \alpha_{\rho-1})$, $(\tau_{2\rho-2}, \beta_{\rho-1}, \alpha_\rho)$ and K' is prefixed by $(\tau_1, \alpha_1, \beta_1)$, $(\tau_3, \alpha_2, \beta_2)$, …, $(\tau_{2\rho-3}, \alpha_{\rho-1}, \beta_{\rho-1})$.*
2. *We say that K is a matching conversation to K' if there exist $\tau_0 \prec \tau_1 \prec \ldots \prec \tau_R$ and $\alpha_1, \beta_1, \ldots, \alpha_\rho, \beta_\rho$ such that K' is prefixed by $(\tau_1, \alpha_1, \beta_1)$, $(\tau_3, \alpha_2, \beta_2)$, …, $(\tau_{2\rho-3}, \alpha_{\rho-1}, \beta_{\rho-1})$, $(\tau_{2\rho-1}, \alpha_\rho, *)$ and K is prefixed by $(\tau_0, \lambda, \alpha_1)$, $(\tau_2, \beta_1, \alpha_2)$,…, $(\tau_{2\rho-4}, \beta_{\rho-2}, \alpha_{\rho-1})$, $(\tau_{2\rho-2}, \beta_{\rho-1}, \alpha_\rho)$.*

Let $No - Matching^{A,U}(k')$ (or $No - Matching^{A,S}(k)$) be the event that user U (or server S) believes that server S (or user U) is engaged in a matching conversation, but in fact, it is adversary A who impersonates server S (or user U).

[5] M. Bellare and P. Rogaway, "Entity authentication and key distribution," *CRYPTO*, 1993, pp. 232-249.

Definitions (B)

Definition

Secure Three-Factor Mutual Authentication (STMA)
We say that $\prod$ is a secure mutual authentication protocol if for any probabilistic polynomial time (PPT) adversary A in the AM, the following properties are satisfied.

1. *If oracles $\prod_{U,S}^{sid}$ and $\prod_{S,U}^{sid}$ have matched conversations, then they accept each other.*
2. *$\prod_{U,S}^{sid}$ accepted implies a matching conversation: the probability of $No - Matching^{A,U}(k)$ is negligible. (Secure server authentication)*
3. *$\prod_{S,U}^{sid}$ accepted implies a matching conversation: the probability of $No - Matching^{A,S}(k)$ is negligible, where U should not be registered by A. (Secure user authentication)*

Definitions (C)

Definition

Secure Three-Factor Authenticated Key Exchange (STAKE)
A Protocol $\prod$ is called STAKE if the following properties hold for any adversary A in the AM:

- *$\prod$ is a STMA protocol;*
- *if both $\prod_{U,S}^{sid}$ and $\prod_{S,U}^{sid}$ complete matching conversations, then they have shared the same session key;*
- *in a fresh session, the advantage $Adv^{A}(k)$ is negligible.*

Note that:

$Adv^{A}(k){=}|GoodGuess^{A}(k)] - \frac{1}{2}|$, where the GoodGuess is the event such that A wins $Test(U, S, sid)$;

Lemma

Lemma

Secure User Authentication
In the proposed protocol $\prod$*, if the pseudo-random function (PRF) is replaced by an ideal random function, the public key encryption (PKE) scheme is secure against CCA2 attack, and* $\prod_{S,U}^{sid}$ *has accepted, then for any PPT adversary A in the AM, the probability of* $No - Matching^{A,S}(k)$ *is negligible.*

Lemma

Secure Server Authentication
In proposed protocol $\prod$*, if the signature scheme is unforgeable against adaptive chosen message attacks, and* $\prod_{U,S}^{sid}$ *has accepted, then for any PPT adversary A in the AM, the probability of* $No - Matching^{A,U}(k)$ *is negligible.*

Theorem

Theorem

Secure Three-Factor Mutual Authentication (STMA)
In proposed protocol $\prod$*, if: (A) the PRF is replaced by an ideal random function and PKE scheme is secure against CCA2 attack; (B) the signature scheme is unforgeable against chosen message attack; (C) at least one of* $\prod_{U,S}^{sid}$ *and* $\prod_{S,U}^{sid}$ *has accepted; then for any PPT adversary A in the AM, the probabilities of both* $No-Matching^{A_U}(k)$ *and* $No-Matching^{A_S}(k)$ *are negligible.*

Theorem

Secure Three-Factor Authenticated Key Exchange (STAKE)
In proposed protocol $\prod$*, if (A) the PRF is replaced by an ideal random function and the PKE scheme is secure against CCA2 attack; (B) the signature scheme is unforgeable against chosen message attack; then for any PPT adversary A in the AM, STMA is achieved with shared session key and the advantage* $Adv^{A}(k)$ *is negligible.*

Václav Matyás Jr. and Zdenek Ríha, "Toward reliable user authentication through biometrics," *IEEE Security & Privacy,* vol. 1, no. 3, pp. 45-49, 2003.

H.-S. Kim, S.-W. Lee, and K.-Y. Yoo, "ID-based password authentication scheme using smart cards and fingerprints," *SIGOPS Oper. Syst. Rev.,* vol. 37, pp. 32-41, October 2003.

M. Scott, "Cryptanalysis of an id-based password authentication scheme using smart cards and fingerprints," *SIGOPS Oper. Syst. Rev.,* vol. 38, pp. 73-75, April 2004.

U. Uludag, S. Member, S. Pankanti, A. K. Jain, S. Member, S. Prabhakar, Anil, and K. Jain, "Biometric cryptosystems: Issues and challenges," *Proceedings of the IEEE,* 2004, pp. 948-960.

A. K. Jain and D. Maltoni, *Handbook of Fingerprint Recognition*, Inc. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003.

A. Bhargav-Spantzel, A. C. Squicciarini, and E. Bertino, "Privacy preserving multi-factor authentication with biometrics," *Digital Identity Management,* 2006, pp. 63- 72.

A. Bhargav-Spantzel, A. C. Squicciarini, S. K. Modi, M. Young, E. Bertino, and S. J. Elliott, "Privacy preserving multi-factor authentication with biometrics," *Journal of Computer Security,* vol. 15, no. 5, pp. 529-560, 2007.

C.-I. Fan and Y.-H. Lin, "Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics," *IEEE Transactions on Information Forensics and Security,* vol. 4, no. 4, pp. 933-945, 2009.

C.-T. Li and M.-S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications,* vol. 33, no. 1, pp. 1 - 5, 2010.

X. Li, J.-W. Niu, J. Ma, W.-D. Wang, and C.-L. Liu, "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications,* vol. 34, no. 1, pp. 73 - 79, 2011.

A. K. Das, "Cryptanalysis and further improvement of a biometric-based remote user authentication scheme using smart cards," *International Journal of Network Security Its Applications (IJNSA)*, vol. 3, no. 2, 2011.

Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97-139, 2008.

Y. Wu and B. Qiu, "Transforming a pattern identifier into biometric key generators," *ICME*, 2010, pp. 78-82.

A. Nagar, K. Nandakumar, and A. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," *19th International Conference on Pattern Recognition, 2008. ICPR 2008.*, dec. 2008, pp. 1-4.

M. Bellare and P. Rogaway, "Entity authentication and key distribution," *CRYPTO*, 1993, pp. 232-249.

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!

Thank You!!!