Send Orders for Reprints to reprints@benthamscience.ae

The Open Cybernetics & Systemics Journal, 2015, *9*, 363-366 363

Open Access

The Enhanced Outgoing Test Theorem of Authentication Tests

Deng Zhenrong*, Zhang Xi, Deng Xing, Dai Kai and Huang Wenming

Guangxi Key Laboratory of Trusted Software, Guilin, China

Abstract: Through the research process of Yahalom protocol by using authentication test, the problem of authentication tests cannot always available when there are not only one transform occurs in one transform path. Has this problem mainly is as a result of the authentication test theorems aimed at testing component which is merely once transformation, but the analytical ability of several transformations is not strong enough. After analyzing the authentication test theorems, I proposed an enhanced outgoing test theorem which enhanced capability of the completeness, in order to carry out authentication when the above-mentioned problems happen, the proof for theorem is given. Finally this method is used to authenticate Yahalom protocol and prove Yahalom protocol can fulfill the authentication property.

Keywords: Authentication test, enhanced, outgoing test theorems, yahalom.

Authentication test method [1, 2], which based on strand space [3-6], is proposed by the Guttman *et al.* in 2000, people use it to judge the agreement property of authentication protocols, and it has been widely used. After analyzing this method, I find it can't prove the authentication party be able to complete a full authentication communication when the authentication protocol have a third party involved and the test component occurs several times transformation in the conversion path, even if it can proof that, the process is complex, such as Yahalom protocol [7] B authentication for A.

This article briefly describes the authentication test methods and theorems, Then analyzed why original protocol authentication test theorem can't authentication Yahalom protocol simply and effectively, Then strengthened the outgoing test theorem of authentication test methods, and Prove the strengthened theorem, at last use strengthened Theorem to authenticate Yahalom protocol, and make a comparation with the original authentication test theorems for the degree of completion and the simplicity of the authentication process.

1. INTRODUCTION OF AUTHENTICATION TEST METHODS

Guttman proposed authentication test methods, which is the one of two major events in space string theory. Although the establishment of authentication test methods requires complex theoretical derivation and proof procedure, but when using the method to analysis security protocols, the proving process is simpler and intuitive. The authentication test methods are briefly introduced as follow.

A term t0 is a component of t if t0[t, t0 is not a concatenated term, and any t1≠t0 meet t0[t1[t is a concatenated term. A term t is new at n=<s, i> if t is a component of term (n), but t is not a component of node<s, j> for every j< i.

A term t={h}k is a test component for a in n if: (1)a[t, and t is a component in n; (2) t is not a proper subterm of a component of any regular node n′∈∑.

The edge n1⇒+n2 is a transformed edge for a∈A if n1 is positive(negative) and, n-2. is negative(positive), a[termn1, and there is a new component, t2 of n2. such that a[t2.

The edge n0⇒+n-1 is a test for a if a uniquely originates at n0 and n0⇒+n1 is a transformed edge for a.

The edge n0⇒+n1 is a outgoing test for a in t={h}k. if it is a test for a and K−1∉Kp, Kp represent the unsafe key set. a only occur in t, and t is a test component for a in n0.

The edge n0⇒+n1 is a incoming test for a in t1={h}k if it is a test for a and K∉Kp. and t1 is a test component for a in n1.

A negative node n is an unsolicited test for t={h}k if t is a test component for any a in a and K∉Kp.

Theorem 1.1 Outgoing Test Theorem: Let C be a bundle with n′∈C and let n⇒+n′ be an outgoing test for a in t.(1). There is regular nodes m, m'∈∈C, such that t is a component of m and m⇒+m' is a transforming edge for a.(2). Suppose that a occurs only in component t1={h1}k1. of m′ and t1 is not a proper suberm of any regular component, and K1−1∉Kp. Then there is a negative regular node m″ with t1 as a component.

Theorem 1.2 Incoming Test Theorem: Let C be a bundle with n′∈C and let n⇒+n′ be an incoming test for a in t′. Then there exist regular nodes m, m′∈C such that t′ is a component of m′ and m⇒+m′ is a transforming edge for a.

Theorem 1.3 Unsolicited Test Theorem: Let C be a bundle with n∈C, and let n be an unsolicited test for t={h}k. Then there exists a positive regular node m∈C such that t is a component of m.

1874-110X/15 2015 Bentham Open

2. THE DISADVANTAGE OF AUTHENTICA -TION TEST THEOREM

Authentication test Theorems are composited by three theorems mention above, such as Theorem 1.1, Theorem 1.2 and Theorem 1.3, it has its advantages in agreement certification, such as simple and intuitive features, but also has its shortcomings.

The analysis revealed that the authentication test theorems are valid only when test component occur only one transform in the transformation path, but if there are several times transformation, the authentication test theorems can't draw the right conclusions or verification steps are too complicated.

Next, make the authentication process of Yahalom protocol for example to describe the lack of authentication test theorem.

2.1. Yahalom Protocol

Yahalom protocol, which was proposed at 1988, is a typical classical authentication protocol, as shown in Fig. (**1**). Participant in the communication protocol is subject A, B and the authentication server S, which aims to distribute the session keys between communicating parties.

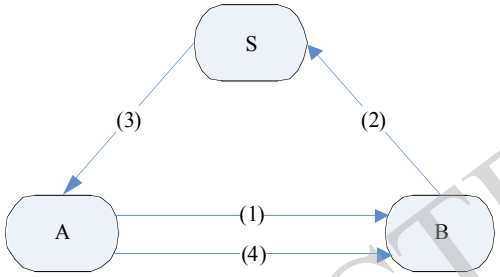

Fig. (1). Yahalom protocol.

(1) A→B:ANa

(2) B→S:B{ANaNb}Kbs

(3) S→A:{BKabNaNb}Kas{AKab},Kbs.

(4) A→B:{AKab}Kbs{Nb}Kab.

Yahalom protocol strand space is composed by three kind strands as follow:

(1) Initiator strand, Protocol trace is showed as follow: <+ANa−{BKabNaNb}KasH+H{Nb}Kab>, *Si*∈ Init[A,B,Na, Nb,Kab].

(2) Responder strand, Protocol trace is showed as follow:<-ANa,+BANaNbKbs,-AKabKbsNbKab>, Sr∈ Resp,A, B,Na,NbKab.

(3) Server strand, Protocol trace is showed as follow: is :<-B{ANaNb}Kbs+{BKabNaNb}Kas{AKab}Kbs>, S∈ Serv [A,B,Na,Nb,Kab].

Here, H represents the encrypted message which participant can't be identified. Supposed A,B∈ Tname, Kbs∉ Kp,Kas∉ Kp, Kab∈ TnameNaNb∈ T\Tname,Na and Nb uniquely originate at ∑.

Yahalom protocol bundle diagram shown in Fig. (**2**).

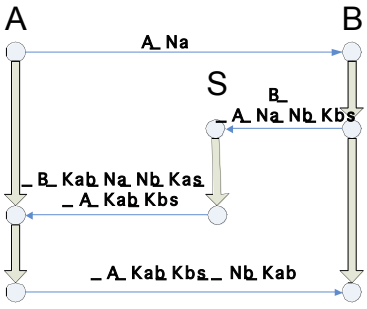

Fig. (2). Yahalom protocol bundle diagram.

2.2. Using Original Outgoing Test Theorem Prove Yahalom Protocol

Proposition 2.1 Suppose that C is a bundle in Σ which is a Yahalom strand space, A≠BKasKbs∉ KpSr∈ Resp [ABNaNbKab] with C-height 3. Then there exist S ∈ Serv [AB,Na,Nb,Kab] with C-height 2, and exist Si∈ Init [A,B,Na,Nb,Kab] with C-height 2.

Proof. ① {AKab}Kbs is an unsolicited test, according to unsolicited test Theorem, there exist a regular node m∈ C in C, t is a components of m, and A≠B, {AKab}Kbs can occurs only at <S, 2> of strand S∈ Serv[A,B,**,Kab].

② <Sr,2>⇒<Sr,3> is a outgoing test and {ANaNb}Kbs is the test component, according to outgoing test theorem, there exist a regular transforming edge for Nb. According to the type of message in bundle C, the transforming edge only occurs in S-'. ∈ Serv[A,B,Na,Nb,Kab']with C-height 2. According to the second term of outgoing test theorem, {B,Kab,NaN-b}Kas only occurs in Si∈ Init[A,B,Na,Nb, Kab] with C-height 2.

Because the original outgoing test can't prove Si is finished, so it can't prove Yahalom protocol satisfy Agreement property.

2.3. Using The Incoming Test Prove Yahalom Protocol

Proposition 2.2 Suppose that C is a bundle in Σ which is a Yahalom strand space, A≠B, Kas,Kbs∉ Kp, S ∈ Serv[A,B,Na,Nb,Kab] with C-height 1. Then there exist Sr∈ Resp[A,B,N-a,Nb*]with C-height 2.

Proof. {ANaNb}Kbs is an unsolicited test, according to unsolicited test theorem, there exist a regular node m∈C in C, and t is component of m A≠B, {ANaNb}Kbs only occurs at node<,S-r.,2> in strand Sr∈ Resp[ABNaNb*].

Proposition 2.3 Suppose that C is a bundle in Σ which is a Yahalom strand space, A≠B,Kas∉Kp, Si. ∈ Init[A,B,Na,Nb,Kab] with C-height 2, there exist stand S ∈ Serv[A,B,Na,Nb,Kab] with C-height 2.

Proof. <Si,1>⇒<Si,2> is an incoming test for Na ,{BKab,Na,Nb},Kas is the test component,according to incoming test theorem, there exists a transforming edge for ,N-a.. According to the type of message in bundle C, the transforming edge only occurs in S ∈ Serv[A,B,Na,Nb,Kab] with C-height 2.

Proposition 2.4 Suppose that C is a bundle in Σ which is a Yahalom strand space, A≠B, Kas∉Kp,Si∈ Init,A,B,Na,

Nb,Kab with C-height 2,there exists strand Sr∈ Resp [A,B,Na,Nb,*] with C-height 2.

Proof. If there is a strand Si.∈ Init[A,B,Na,Nb,Kab] with C-height 2,according to Proposition 2.3 only prove there exist a strand S ∈ Serv,A,B,Na,Nb,Kab with C-height 2. And because Proposition 2.2, Indirect proof there exists strand Sr ∈ Resp[A,B,Na,Nb*] with C-height 2.

Proposition 2.5 Suppose that C is a bundle in Σ which is a Yahalom strand space, A≠B, Kbs∉Kp, Sr.∈ Resp[A,B,Na,Nb,Kab] with C-height 3,then there exists a strand Si.∈ Init[A,B,Na,Nb,Kab] with C-height 3.

Proof. <Sr,2>⇒<Sr,3> is an incoming test for Nb, {Nb}Kab is the test component, according to incoming test theorem, there exists a regular transforming edge for Nb. According to the type of message in bundle C, the transforming edge only occurs in Si. ∈ Init[A,B,Na',Nb,Kab] with C-height 3. Because the parameters A and B did not reach directly consistent for Na and Nb unique origin in B, use Proposition 2.4 on ,S-i.,prove that there exist Sr'∈ Resp[A,B,Na',Nb*] with C-height 2. According to form of the responder strand, N-b. originates at <Sr',2> and because Nb is uniquely originates,so <Sr',2>=<Sr,2>, and Sr'=Sr, Na'=Na. Thus, there exists a strand Si.∈ Init [A,B,Na,Nb,Kab] with C-height 3.

3. ANALYSIS FOR AUTHENTICATION TEST THEOREMS SHORTCOMINGS

When Authenticator party Authenticate the authenticated party, only if Authenticator parties to confirm the authenticated party finish the last message being sent steps, Authenticator will just finish the Authentication [8].

Proposition 2.1 shows that when using the outgoing test theorem authentication Yahalom, B only confirmation A execution to step 2 in the for Authentication (*e.g.* the last step before the release of information), this can't guarantee that A can execute completly (*e.g.* completion of three nodes), so the certification can't complete.

But it proves that Authentication for B to A is can be completed in the BAN logic certification, and reach agreement on the parameters on each other [9, 10]. Analyze the causes, there are several transformation occur on the test component ,{A,N-a.,N-b.}-,K-bs.. in the transform path, Outgoing test can verify A execution to the second step(application the second term of the outgoing test theorem), the third step can't guarantee be executed (outgoing test theorem has its advantages at parameters certification, but not as good as on the degree of done in agreement on input test theorem).

The last section shows that use the incoming test theorem authentication Yahalom protocol [11, 12], you can ensure B execute to the third step, But to prove the consistency of the parameters needed complicated indirectly certificate chain such that B certification S, and S certification A. (This Process must follow the order that S to B, A to S, B to A for authentication, and the needs of every party ensure the consistency of the parameters Nb of the only origin from B).

When using the input test theorem proving Protocol, the process is too complicated and degree of completion of the Protocol have no room for improvement, so this paper mainly strengthened the completion of the outgoing test theorem.

4. ENHANCED OUTGOING TEST THEOREM

Theorem 4.1 Let C is bundle, n′∈ C n⇒+n′ is outgoing test for a in t(1)So there exists regular nodes m, m′∈ C, make t is component of m, and m⇒+.m′ is the transforming edge for a;(2)Besides that,if the test component t1={h1}k1 of m' in the transforming edge is not as the same as the one(t') of the n' in the transformed edge ,then there exist a transforming edge between m' and n', and the two nodes l, l' of the edge are all regular. If the test component t2={h2}k2 of l' is different from t', and a only occurs in the component t2 of l', and t2 is not a subset of any regular component, and K2-1 not belong to Kp, then between l' and n' there exist a transforming edge, and the two nodes o, o' of the edge are regular. And so on, until tx = t', then the outgoing test end.

This theorem enhance the second term of the outgoing test theorem, make degree of completion of it more powerful and there is no any additional assumptions on the original outgoing test theorems.

5. THE PROVEMENT OF THE ENHANCED OUTGOING TEST THEOREM

To prove Theorem 4.1, we introduce the following three important definition and propositions, all of them can be found in the literature [1].

Definition 5.1 A transformation path is a path for which each node ni is labeled by a component Li of ni in such a way that Li=Li+1 unless ni⇒+ni+1 and Li+1 is new on the strand of ni+1.

Proposition 5.1 Suppose (p, L) is transformation path traversing no key edges such that p1 and l(p) are regular and L1≠L|p|(l(p) is the last node of p, and L|p| is the test component of l(p)).Let L1 beof the form {h1}k1.Suppose that L1 is not a proper subterm of any regular component, and suppose that k1-1∉Kp,then pa is regular.Moreover, pa⇒+pa+1 is a transforming edge.

Propositions 5.2 Suppose p is a transformation path such that a∉Li for every ni and L1≠Ln. Then p has a transforming edge for a.

Proof for Theorem 4.1 From Lm' ≠Ln', according to the definition 5.1 there is a transformation path between m' and n'. according to Proposition 5.2 there is a transforming edge for a between m' and n', and, from the outgoing test Theorem, we know m ' and n' are regular nodes , the form of Lm'={h1}k1, and Lm' is not a proper subterm of any regular component , and k1-1∉P. Based on the proposition 5.1, we know that there is a regular node pa which makes La≠La+1, and pa⇒+pa+1 is the transforming edge. Now we have prove pa is a regular, then prove pa+1 is a regular node too. Since pa⇒+pa+1 is transforming edge, so pa+1's symbol term is positive, because bundle is a causal relationship with partial order , then pa+1 existence depends only on pa exists because there exist pa and it is a regular node, so pa+1 also exists and is a regular node. If the test component t2={h2}k2 of pa+1 is different from t ', and a only appearing in compo-

nent t2, and t2 is not a proper subterm of any regular component , and k2-1 ∉ Kp, then the we can use proposition 5.1 to prove that there must have a transforming edge between pa+1 and n' , and the two nodes o, o' of the transforming edge are regular. And so on, until tx=t', there must be no transforming edge between px and n', then the outgoing test end.

6. USING ENHANCED OUTPUT TEST THEOREM AUTHENTICATE YAHALOM PROTOCOL

Proposition 6.1 Suppose that C is a bundle in Σ which is a Yahalom strand space, A≠B,Kas,Kbs∉ Kp,Sr∈ Resp[A,B,,N-a,Nb,Kab] with C-height 3. Then there exist S∈ Serv[A,B,Na,Nb,Kab] with C-height 2, and exist Si∈ Init[A,B,Na,Nb,Kab] with C-height 3.

Proof. ① {AKab}Kbs is an unsolicited test, according to unsolicited test Theorem, there exist a regular node m∈ C in C, t is a components of m, and A≠B, {AKab}Kbs can occurs only at <S,2> of strand S∈ Serv, A, B,**, K-ab.

② <Sr, 2>⇒<Sr, 3> is a outgoing test and {ANa, Nb.}Kbs is the test component, according to enhanced outgoing test theorem, there exist a regular transforming edge for ,N-b.. According to the type of message in bundle C, the transforming edge only occurs in S' ∈ Serv[AB,Na,Nb,Kab'] with C-height 2. Because the node's(<S, 2>) test component t1≠t′, according to enhanced outgoing test theorem, there is another transforming edge for ,N-b.. According to the type of message in bundle C, the transforming edge can only occurs at S-i. ∈ Init[A, B, Na, Nb, Kab'] with C-height 3.

③ For ② is valid when Kab=Kab', if Kab≠Kab' then {Nb}Kab is H which can't be recognized by B, outgoing test is not valid, and Sr is not executed, which conflict the assume that there is a strand Sr with C-height 3, so Kab=Kab′. Thus, from ② we know there is a strand S ∈ Serv[A,B,Na,Nb,Kab] with C-height 2,and because ① there exist Si∈ Init[A, B, Na, Nb, Kab] with C-height 3.

7. CONCLUSION

Enhanced outgoing test theorem can authenticate the protocol that there are multiple transformations occurring in the transformation certification path for test component, it overcome the deficiencies of the original outgoing test theorems on degree of completion, and significantly reduce prove step over the incoming test theorems.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work is supported by Guangxi key Laboratory of Trusted Software (No: kx201317), by the Postgraduate's Innovation Project of Guilin University of Electronic Technology under (No: GDYCSZ201470), by the 2014 Guangxi University of Science and Technology Research Projects (NO: LX2014149), by the Nature Science Foundation of Guangxi (No: 2013GXNSFAA019350).

REFERENCES

[1] J.D. Guttman, and F.J. Thayer, "Authentication tests and the structure of bundles", *Theoretical Computer Science*, vol. 283, no. 2, pp. 333-380, 2002.

[2] J.D. Guttman and F.J. Thayer, "Authentication Tests", In: *IEEE Symposium on Security and Privacy*, 2000, pp. 96-109.

[3] F.J. Thayer, J.C. Herzog, and J.D. Guttman. "*Strand spaces:Why is a Security Protocol Correct*", IEEE Computer Society Press, Los Alamitos, 1998, pp. 160-171.

[4] Q. Sihan, *Security Protocol*, Tsinghua University Press, Beijing, 2005, pp. 82-83.

[5] F.J.T. Fabrega, J.C. Herzog, and J.D. Guttman, "Strand spaces: proving security protocols correct", *Journal of Computer Security*, vol. 7, no. (2-3), pp. 191-230, 1999.

[6] F.J. Thayer, J.C. Herzog, and J.D. Guttman,. "Mixed strand spaces", In: *Proc. of the 12th IEEE Computer Security Foundations Workshop*, Mordano, 1999, pp. 72-82.

[7] F. J. Thayer, J. C. Herzog and J. D. Guttman, "Strand Spaces: Why is a Security Protocol Correct", In: *IEEE Symposium on Security and Privacy,* IEE Complete Society Press, Oakland, 1998.

[8] G.A. Lowe, *Hierarchy of Authentication Specifications*, IEEE Computer Society Press, Los Alamitos, 1997, pp. 6-7.

[9] Q. Sihan, *Security Protocol*, Tsinghua University Press, Beijing, 2005, pp. 124-127.

[10] C. Liqiong, *The Extension and Application of Strand Space*, Shanghai Jiao Tong University, Shanghai, 2008.

[11] L. Jing, and Z. Shixiong. "Strand space model of yahalom protocol and its analysis", *Mini-Microsystems*, vol. 27, no. 5, pp. 788-792, 2006.

[12] C. Chunling and Z. Yanchun, "Analysis and improment of yahalom protocol", *Computer Applications and Software*, vol. 25, no. 7, pp. 266-268, 2008.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014