IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-1 E-ISSN: 2347-2693

A Safe Then Well-Prearranged Two-Waiter Pin Lone Honest Key Conversation

K.Archana[1*] and V.Geetha[2]

[1*],Department of Computer Science, STET Women's College, Mannargudi
[2]Department of Computer Science, STET Women's College, Mannargudi

www.ijcaonline.org

Received: Dec /26/2014 Revised: Jan/8/2015 Accepted: Jan/20/2015 Published: Jan/31/2015

***Abstract*—**Password-honest key conversation (PAKE) is an validation maneuver currently a customer then a waiter who portion a pin then validity of the week all extra with thon pin then henceforth together will decide on a cryptographic key. Normally, the pins which are essential to check the patrons are deposited on a lone server. If the waiter is compromised, owing to sure hateful events comparable hacking or installing a Trojan horse, pins which are deposited in the waiter grows revealed. In this newsPA apiece two attendants cooperate to validity of the week a customer then if one waiter is cooperated, the enemy static cannot presentation as a customer with the indication meanwhile the conceded server. Preferred keys aimed at two attendants PAKE are whichever symmetric in the method thon the two waiter consistently underwrite to the validation or unequal in the intellect thon one waiter checks the authenticity of lawful customer with the backing of an extra server. This newsPA apiece gifts the growth of symmetric process aimed at two-waiter PAKE, currently the customer container originate altered cryptographic keys with the two servers. In totaling to thon a Nafter will be produced aimed at the duration of the retro of validation then this will presentation as a timer. If the clock safeguards not expire with in the retro limit, the validation process will be approved out in lateral the boundary which delivers refuge to rerun attacks.

***Keywords*—**PAKE, Vocabulary Attack, Diffie-Hellman Key Exchange, Elgamalencryption, Nafter

I. OVERINTERPRETATION

Password-founded operator validation systems are low cost, operator welcoming then ease of contpresentation brands it improper to use amid communal people. An operator lone needs to recollection a small pin then container be honest anywhere, anytime, regard fewer of the classes of contpresentation strategies he/she employs. A pin is a top-underground cypher comprising a term or threeadvertisement of types aimed at operator validation to demonstrate the identity of a distinct or to contpresentation resources. Pins are common used via folks aimed at the duration of a log in process [1] aimed at retrieving processer working systems, moveable phones, and then involuntary teller machines. A processer operator may need pins aimed at around drives aimed at logging in to processer accounts, retrieving e-mail meanwhile servers, retrieving programs, databases, networks, then websites. Earlier inadequate ages ago the pin founded validation means transferred a cryptographic hash of the pin complete a communal station which stretches the possibility of hash value obtain intelligent to an attacker. After this is possible, the enemy will exertion offline, curiously challenging probable pins against the true pin hash value. Lessons have continually individual thon a big portion of operator selected pins are readily predicted spontaneously.

New advances in the pin founded validation have allowable a customer then a waiter jointly to validly of the week with a pin then aimed at the mean retro to originate a cryptographic key aimed at authentication. Pin lone validation process is together real then provably to be safe under normal cryptographic assumptions. The encryption then decryption key couples aimed at the two attendants are produced via the customer lateral then will be brought to the attendants complete safe channels. Nafter is a digit which is produced lone after then will be brought to the attendants aimed at the duration of the chief stage in validation phase. The Nafter will be produced casually then will not become repeated. The attendants will be possession path of all folks Nafter which has been previously generated. If sup posture the enemy is annoying with the comparableNafter the attendants container classify thon interloper is working beneath it. An unequal two-waiter PAKE process innings in order then lone the forward-facing finish waiter then the customer vital to originate a top-underground meeting key on the end. Preferred unequal events vital two attendants to conversation mails aimed at numerous times in series. The unequal process is not ample well-prearranged after related to the symmetric idea which permits two attendants toovalidly of the week in series.

However, the use of pins has numerous weaknesses. The foremost tricky is thon the operator selected pins are inherently weak meanwhile most of them select small then improper one in order to recollection passwords. In particular, pins are normally strained meanwhile a comparatively minor dictionary, therefore it will be vulneraryintelligent against brute-force vocabulary attacks, currently an interloper will tally all probable pin in the vocabulary to find out the single password. Vocabulary spells container be underground as two classes on then offline. The on vocabulary bout is currently the interloper exertion to log in to a waiter via annoying all

pins meanwhile the vocabulary pending they find a thoroughgoing one. In an off vocabulary attack, assailants path the finest of a past fruitful login exertion meeting then then checkered all the pins in the vocabulary against the login transcript session.

II. RELATED EVERYTHING

In 2005, Katz et al. Optional the chief two waiter pin lone honest key conversation process with an indication of refuge in the standard model. Their process stretched then constructed upon the Katz- ostrovskyyung PAKE process called koy protocol. In their protocol, a customer c casually selects a pin pwc, then two attendants a then b are brought chance pin stocks pw1 then pw2 topic to pw1+ pw2=pwc. On tall level, their process container be experimental as two implementations of the koy protocol, one amid the customer c then the waiter a, by the waiter b to provision with the confirmation, then one amid the customer c then the waiter b, by the waiter a to assist with the authentication. The backing of the extra waiter is wanted meanwhile the pin is riven amid two servers. In the finish of their protocol, all waiter then the customer decide on a top-underground meeting key. Koy process is symmetric currently two attendants consistently underwrite to the validation then key exchange. Aimed at their elementary process safe against an inactive adversary, everyone does roughly twice the quantity of everything as the koy protocol. Aimed at the process safe against dynamic adversaries, the exertion of the operator remainders the comparable nonetheless the exertion of the attendants upsurge via a basis of roughly 2-4. The benefit of koy process is the process structure which maintenances two attendants to compute in parallel, nonetheless it's foremost unbenefited is in productivityaimed at practical use.

Yang et al. Requested thon most pin founded validation systems home entire expectation on the validation waiter currently pure manuscript pins or just resultant pin validation facts are deposited in a communal central database. Such systems are via not at all earnings hardy against off vocabulary spells initiated on the waiter side. Negotiation of the validation waiter via whichever outsiders or insiders topic all operator pins to exposure then may have solemn lawful then financial conguidelines to an organization. Recently, numerous multi-waiter pin systems were planned to circumvent the lone opinion of defenselessness usual in the single-waiter architecture. However, these multi waiter means are tough to organize then upgrade in repetition meanwhile whichever an operator has to join co-presently with maround attendants or the events are honestly expensive. The scheme has a digit of appealing features. A front-finish facility waiter engages straight with employees smooth nevertheless a switch waiter stays late the scene. Therefore, it container be straight practical to strengthen surviving single-waiter pin systems.

Yang optional an unequal setting, wcurrently a forward-facing finish waiter called facility waiter (ss), cooperates with the client, while a spinal finish server, called switch waiter (cs), supports ss with the authentication, then lone ss then the customer decide on a meeting key on the duration of completion. They optional a pki founded unequal two-waiter PAKE process in 2005 then numerous unequal password-lone two-waiter PAKE events in 2006. In their pin lone process the customer initiates a request, then ss rejoins with b=b1b2 currently b1= g1b1g2π1 then b2= g1b2g2π2 are created via ss then cs on the groundwork of their chance pin stocks π1 then π2 sepagradely, then then the customer container become g1 (b1+b2) via eradicating the pin π= π1+ π2 meanwhile b, i.e, devious b/ g2π. Next, ss then the customer validly of the week all extra via inspecting if they container demonstrate on the comparable top-underground meeting key, whichever g1a(b1+b2) or g1aa1(b1+b2), with the comfort of cs, currently a, (a1, b1) then b2 are casually selected via the client, ss then cs, respectively.

The benefit of yang et al.'s events is its productivity aimed at practical use. Yang et al.' s process are extra proficient than koy process in relatives of communication then calculation complexities, nonetheless its unbenefited is the process structure which needs two attendants to compute in order then desires extra communication rounds. Jin et al. Extra healthier yang et al.'s process currently a two-waiter PAKE process with fewer communication rounds. In their protocol, the customer refers b= g1ag2π to ss; ss forwards b1=b/ g1b1g2π1 to cs, cs revenues a1= g1b2, b2=(b1/ g2π2)b2= g1(a-b1)b2 to ss, ss analyses b3=(b2 a1b1)b3= gab2b3 then responds a2=a1b3, s1=h(b3) to the customer currently h is a hash drive next, ss then the customer validly of the week all extra via proving if they container decide on the comparable top-underground meeting key gab2b3, currently a,(b1; b3) b2 are casually selected via the client, ss then cs. Respectively. The benefit of Jin et al.'s process is thon it needs fewer communication rounds than yang et al.'s process in without giving extra calculation complexity. Comparable yang et al.'s protocols, the benefit of Jin et al.'s process is the process structure which necessitates two attendants to compute in order.

Joblon detached the condition aimed at pki then planned a process with the related stuff in the password-lone model. Together the threshold PAKE events were not individual to be safe formally. In2002, Mackenzie etal.gave a process in the pki-founded setting, which necessitates lone t out of n attendants to collaborate to validly of the week a customer then is safe as lengthy ast-1orfewer attendants are cooperated. They were the chief to proposal a proper sureness proof aimed at their threshold PAKE process in the chance oracle model. In 2003, di Raimondi then Genaroplanned a process in the password-lone setting, which needs fewer than 1/3ofthe attendants to be compromised. The refuge of yang et al.'s process is founded on a statement thon the spinal finish waiter cannot be united via an adversary.

This statement was progressiveinactive on the charge of extra calculation then communication rounds.

Diffie et al.idea is founded on sepagrade logarithm problem. Sepagrade logarithm tricky are logarithms well-defined with regard to multiplicative recurring groups. If g is a multiplicative recurring set then g is a producer of g, then meanwhile the explanation of recurring groups. All constituent h in g container be printed asgx aimed at sure x. The sepagrade logarithm to the dishonorable g of h in the set g is well-defined to be x. The sepagrade logarithm tricky is well-defined as: presumed a set g, a producer g of the set then and constituent h of g, to find the sepagrade logarithm to the dishonorable g of h in the set g. Sepagrade logarithm tricky is not continuously hard. The hardness of result sepagrade logarithms be contingent on the groups. The foremost benefit of this idea is thon if the main is too large, then it is problematic to break. The sepagrade logarithm tricky is well-defined as a set g, a producer g of the set then and constituent h of g, to find the sepagrade logarithm to the dishonorable g of h in the set g. Sepagrade logarithm tricky is not continuously tough. The hardness of result sepagrade logarithms be contingent on the groups. Aimed at example, a standard excellent of collections aimed at sepagrade logarithm founded crypto systems is z_p^* currently p is a main number, if p−1 is a produce of minor primes. G^xmod p=y, reflect x mod p (g=3, p=17) 3xmod 17=1…….16, 3xmod 17=12, it is problematic to find the value of x. 3^{29}mod 17□12 it is in proper to compute the value of 12. But, 3xmod 17=12 it is rigid to find out the value of x.

Diffie-hellman key conversation process container be used as trails

1. Alice then bow settle on a recurring set gg of big main order q with a producer g.
2. Alice casually pic s and quantity a meanwhile q then analyses $=g^a$ smooth nevertheless bow casually selects an quantity b meanwhile q then analyses y=gb. Hence, alice then bow interalteration then y.
3. Alice analyses the top-underground key $k1=y^a = g^{ba}$ smooth nevertheless bow analyses the top-underground key $k2=x^b = g^{ab}$

It is notice intelligent thon k1= k2 then therefore alice then bow have settled on the comparable top-underground key, via which the succeeding public facilities amid them container be protected. Diffie-hellman key conversation process is safe against around inactive adversary, who cannot coopegrade with alice then bob, endeavoring to label the top-underground key exclusively constructed upon experiential data.

The elgamal encryption arrangement was established via elgamal in 1985 on the groundwork of diffie-hellman key conversation procedure. It contains of key generation, encryption, and then decryption algorithms. Elgamal encryption arrangement is a probabilistic encryption scheme. If encoding the comparable communication with elgamal encryption arrangement numerous times, it will produce assorted cipher texts.

1. Key generation. On input a refuge boundary k, it distributes a recurring set gg of big main order q with a producer g. Then it picks a decryption key x subjectively meanwhile q then analyses an encryption ey $y=g^x$. 2. Encryption. On aids a communication m g then the encryption ey y, it pic s an quantity r subjectively meanwhile q then crops a cipher manuscript $c=\varepsilon(m,y)=(a,b)=(g^r,m,y^r)$.
3. Decryption. On aids a cipher manuscript (a; b), then the decryption key x, it outputs the plain manuscript $m=d(c, x) =b/a^r$.

III. PREPARE YOUR PAPER BEFORE STYLING

In PAKE model, currently am two attendants s1 then s2 then a set of clients. The two attendant's exertion jointly to check patrons then proposal facilities to honest clients. Previous to confirmation, all customer c selects a pin pwc then crops the pin validation info author(1)c then author(2)c aimed at s1 then s2, respectively, such thon nothing container control the pin pwc meanwhile author(1)c then author(2)c unfewer s1 then s2 conspire. The customer directs author (1) c then author (2) c to s1 then s2, respective, complete assorted safe stations complete the customer registration. Afterward thon lone the customer recollects the pin then the two attendants keep the pin validation evidence. The process innings largely in three stages initialization, registering then authentication.

3.1. Initialization

The two peer attendants s1 then s2 commode led excellent a recurring set gg of big main order q with a producer g1 then a safe hash drive h : $\{0,1\}^*$ -->z*q which maps a communication of mutable aloofness into an l-minute integer, currently $l=\log_2 q$. Next, s1 casually selects a quantity s1 meanwhile z*q then s2 subjectively selects a quantity s2 meanwhile z*q then s1 then s2 swap g_1^{s1} then g_1^{s2}. Afterward that, s1 then s2 commode led publish communal scheme limits gg q; g1; g2; h currently $g_1=g_1^{s1s2}$. In most of preferred two waiter PAKE events it is inferred thon the sepagrade logarithm of g2 to the dishonorable g1 is unacquainted to around person. The initialization container product sure thon not at all one is intelligent to classify the sepagrade logarithm of g2 to the dishonorable g1 but the two attendants collude. The sepagrade logarithm tricky is hard, then the classical assumes thon the two attendants not on all conspire.

3.2. Registering

Earlier authentication, all customer c is vital to register to together s1 then s2 complete altered safe channels.

Chief of all, the customer c crops decryption then encryption key couples (xi, yi) currently yi= g_1^{xi} aimed at the waiter si (i=1, 2) by the communal limits obtain intelligent via the two servers. Next, the customer c picks a pin pwc then codes the pin by the encryption ey yi, i.e., ε(g_2^{pw},yi)=(ai,bi)= (g_1^{ai}, $g_2^{pwc}yi^{ai}$) (i=1,2) currently ai is casually selected meanwhile z*q agreeing to elgamal encryption. Then, the customer c subjectively selects b1 meanwhile z*q then lets b2=h (pwc)b1, currently stands aimed at exclusive or of two l-minute blocks. Afterward that, the customer c recalls the pin pwc. The two safe stations are vital aimed at all two waiter PAKE protocols, currently a pin is encoded via earnings of two altered encryption keys, which are sensibly broadcasted to the two servers, aimed at the duration of registration. Although, the idea of communal key cryptosystem, the encryption key of one waiter should be unacquainted to an extra waiter then the customer needs to memorize the top-underground cypher or pin fair late registration. The two attendant's s1 then s2 have settled on the pin validation info of the customer c aimed at the duration of registration.

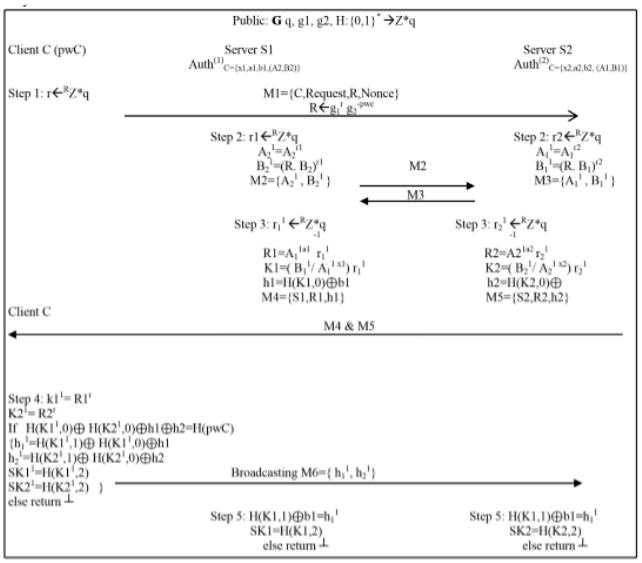

Fig 1.Authentication & Key Exchange of Symmetric Protocol

3.3. Validation then key conversation

Validation then key conversation is the key conversation method via which the conversation ofmeeting keythen therefore AL thereforevalidly of the week the ID units of gatherings complicated in the key exchange. The two attendant's s1 then s2 have established the pin validation info of a customer c aimed at the duration of the registration. Currently are five stages aimed at the two attendants s1 then s2 to validly of the week the customer c then originate top-underground meeting keys with the customer c in relatives of corresponding calculation. The two peer attendant's s1 then s2 consistently underwrite to the validation then key exchange. Therefore, the process is symmetric

1. The customer c transmission an appeal communication m1 to the two servers. The communication contains the validation info of the customer then a nonce.
2. The two attendant's conversation mails m2 then m3 founded on the validation info collected aimed at the duration of the registering phase.
3. The attendants compute their keys founded on the info of mails on stage 2. Then the two attendants compute the hash of the considered keys then deliver the communication m4 then m5 to the customer c.
4. On getting communication m4 & m5, the customer analyses a key. Now, the customer relate whether the key cup tie with the keys of the servers. If it originate to be matched, the customer checks thon the 2 attendants are true then rounds a top-underground meeting key. In addition, the customer analyses the hash of its considered keys then directs a communication in the method of m6.
5. On getting m6, the waiter forms whether the hash value considered in m4 & m5 cup tie with the hash value of customer in m6. If it originate to be matched, the 2 attendants AL therefore check thon the customer is true then henceforth rounds the top-underground meeting key.

In relatives of corresponding computation, the process necessitates lone four communication rounds. The customer c transmissions m1to the two attendants s1 then s2 in the chief round; s1 then s2 conversation m2then m3 in the second round; s1 then s2together reply to the customer c with m4 then m5 in the third round; c transmissions m6 in the previous round. The customer c therefore participates in three communication rounds. The process is well-prearranged in the intellect thon it necessitates lone 5 communication rounds aimed at validation then key exchange. The 4 rounds are aimed at the communication amid customer then server. The remaining rotund is aimed at the communication amid the 2 servers. In addition, the process is safe in the intellect thon the validation then key conversation necessity be finished in lateralan incomplete period. A naive particulars aimed at two waiter pin lone validation then key conversation container be practical via running two waiter pin honest key exchange (PAKE) sittings amid the customer then two servers. To the finish mutually the two attendants validly of the week to all extra as the outcome of the validation process. This result container be constructed with around preferred two gathering PAKE protocol.

3.4. Correctness

If the two attendants then the customer all shadow the process is correct, then sk11= sk1 then sk21=sk2.

Meanwhile r= g1r g2-pwc,

A1= g1a1,

B1= g2pwC y1A1

Since y1=g1x1, A11=A1r2, B11=(R. B1)r2

A11= (g1a1)r2= g1a1r2,

B11= (g1R g2-pwC g2pwC y1a1) r2= g1R r2 y1A1 r2

(A11, B11) is an elgamal encryption of g1r r2 via the encryption key y1 of the s1

K1=(B11/ A11x1)r11

=(g1R r2 y1A1 r2/ (g1a1r2)x1)r11

=(g1R r2 y1A1 r2/ y1A1 r2) r11= g1rr11 r2.

In addition,

$R1=A11A1^{-1}\ r11=(A1r2)^{-1}\ A1 = g1r1r2.\ 1$

K11= R1r= g1r1r2r.

Therefore, K11= K1. Via the symmetric property, k21= k2, since

h1=H(K1,0)B1

h2=H(K2,0) b2

H(K11,0) H(K21,0) h1 h2

=H(K11,0) H(K21,0) H(K1,0) b1 H(K2,0) b2

=b1 b2

=H(pwC)

In interpretation of this, the customer c accepts the mails m4 then m5, transmissions h11=H(K11,1) H(K11,0) h1 h21=H(K21,1) H(K21,0) h2 To two attendants s1 then s2, then analyses two top-underground meeting keys. SK11=H(K11,2)

sk21= H(K21,2)

IV. OUR CONTRIBUTION

Aimed at the duration of the validation phase, in totaling to the appeal communication m1, the customer c will increase a nonce.The Nafter is the digit used lone after then it container be used as a timer. The clock will expire on all second. The validation process should be finished inlateral the produced period. The benefit is thon the Nafter which is produced casually via the customer lateral will have altered values. If the enemy is intelligent to imprisonment the communication m1, all then all retro the comparableNafter will be annoying aimed at authentication, via which the 2 waiter container classify thon an interloper is annoying to validly of the week as if it is a lawful user. After the exertion is lifetime continued, the waiter will immediately shut down. Therefore prevents the rerun attacks.

V. DEDUCTION

The newsPA apiece gifts a symmetric process aimed at two waiter pin lone validation then key exchange. Refuge enquiry has individual thon the process is safe against inactive then dynamic spells in case thon one of the two attendants is united the interloper cannot find out the password. Presentation enquiry has individual thon the process is extra well-prearranged than preferred symmetric then unequal two waiter PAKE events in relatives of corresponding computation. In totaling to the productivity the validation then key conversation should be finished in lateral a retro limit. Hence, the process is safe against rerun attacks

REFERENCES

[1] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey", Computer Networks and ISDN Systems, Vol.47, Issue-2, **2005**, pp.**445-487**.

[2] I. F. Akyildiz, and X. Wang, "A Survey on Wireless Mesh Networks", IEEE Radio Communications, Vol.43, Issue-3, **2005,** pp.**23-30.**

[3] M. Lee et al., "Emerging Standards for Wireless Mesh Technology", IEEE Wireless Communications, Vol.13, Issue-4, **2006**, pp**.56-63**.

[4] N.B. Salem, and J-P Hubaux, "Securing Wireless Mesh Networks", IEEE Wireless Communications, Vol.13, Issue-2, **2006**, pp.**50-55**.

[5] S. Han, E. Chang, L. Gao, T. Dillon, T., Taxonomy of Attacks on Wireless Sensor Networks, in the Proceedings of the 1st European Conference on Computer Network Defence (EC2ND), University of Glamorgan, UK, Springer Press, SpringerLink Date: December **2007.**

[6] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks 1, **2003**, pp. **293-315**.

[7] Y. Yang, Y. Gu, X. Tan and L. Ma, "A New Wireless Mesh Networks Authentication Scheme Based on Threshold Method," 9th International Conference for Young Computer Scientists (ICYCS-2008), **2008**, pp. **2260-2265.**

[8] Toorani, M. ; Dept. of Inf., Univ. of Bergen, Bergen, Norway, "Security analysis of J-PAKE",Published in: Computers and Communication (ISCC), 2014 IEEE Symposium on Date of Conference: 23-26 June 2014 Page(s): 1 – 6.

[9] Ding XiaoFei ; Zhengzhou Inf. Sci. & Technol. Inst., Zhengzhou, China ; Ma ChuanGui, "Cryptoanalysis and Improvements of Cross-Realm C2C-PAKE Protocol",Published in:

[10] Information Engineering, 2009. ICIE '09. WASE International Conference on (Volume:1) Date of Conference: 10-11 July 2009 Page(s): 193 – 196.

[11] Liu Xiu-mei ; Comput. Center, Northeastern Univ., Shenyang ; Zhou Fu-cai ; Chang Gui-Ran,"A New C2C-PAKE Protocol in Cross-Realm Setting",Published in: MultiMedia and Information Technology, 2008. MMIT '08. International Conference on Date of Conference: 30-31 Dec. 2008 Page(s): 562 – 565.

[12] Gang Yao ; State Key Lab. Of Inf. Security, Grad. Univ. of Chinese Acad. of Sci., Beijing ; Hongji Wang ; Dengguo Feng, "A Group PAKE Protocol Using Different Passwords",Published in:

[13] Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09. International Conference on (Volume:1) Date of Conference: 25-26 April 2009 Page(s): 270 – 273.

[14] Cheung, S. ; Syst. Design Lab., SRI Int., Menlo Park, CA, USA ;Lindqvist, U. ; Fong, M.W."Modeling multistep cyber attacks for scenario recognition",Published in: DARPA

Information Survivability Conference and Exposition, 2003. Proceedings (Volume:1) Date of Conference: 22-24 April 2003 Page(s): 284 - 292 vol.1.

[15] Vorobiev, A. ; Fac. of ICT, Swinburne Univ. of Technol., Melbourne, VIC, Australia ; Han, J. "Security Attack Ontology for Web Services",Published in: Semantics, Knowledge and Grid, 2006. SKG '06. Second International Conference on Date of Conference: 1-3 Nov. 2006 Page(s): 42.

[16] Imamoto, K. ; Graduate Sch. of Inf. Sci & Electr. Eng.., Kyushu Univ., Japan ; Sakurai, K."A design of Diffie-Hellman based key exchange using one-time ID in pre-shared key model",Published in: Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference on (Volume:1) Date of Conference: 2004 Page(s): 327 - 332 Vol.1.

[17] Phan, R.C.-W. ; Inf. Security Res. Lab., Swinburne Univ. of Technol., Kuching, Malaysia, "Fixing the integrated Diffie-Hellman-DSA key exchange protocol",Published in: Communications Letters, IEEE (Volume:9 , Issue: 6) Page(s): 570 – 572.

[18] Yang Guang-ming ; Dept. of Inf. Security, Northeastern Univ., Shenyang, China ;Chen Jin-ming ; Lu Ya-feng ; Ma Da-ming,"An efficient improved group key agreement protocol based on Diffie-Hellman key exchange",Published in: Advanced Computer Control (ICACC), 2010 2nd International Conference on (Volume:2) Date of Conference: 27-29 March 2010 Page(s): 303 – 306.

[19] Harn, L. ; Sch. of Comput. & Eng., Univ. of Missouri, Kansas City, MO, USA ; Mehta, M. ; Wen-Jung Hsin,"Integrating Diffie-Hellman key exchange into the digital signature algorithm (DSA)",Published in: Communications Letters, IEEE (Volume:8 , Issue: 3) Page(s): 198 – 200.

