PROSIDING KOMMIT 2012
(KOMPUTER DAN SISTEM INTELIJEN)

Volume 7 – 2012

TEKNOLOGI INFORMASI DAN KOMUNIKASI (TIK) UNTUK KETAHANAN NASIONAL

ISSN: 2302-3740

PENERBIT
Lembaga Penelitian Universitas Gunadarma

Alamat Editor:
Lembaga Penelitian Universitas Gunadarma
Jl. Margonda Raya 100 Pondok Cina
Depok, 16424
Telp. +62-21-78881112 ext. 455
Fax. +62-21-7872829
e-Mail: kommit@gunadarma.ac.id
Laman: http://penelitian.gunadarma.ac.id/kommit

Prosiding KOMMIT, Volume 7 - 2012

Editor:
Tety Elida, Moh. Okki Hardian, Wahyu Rahardjo, Fitrianingsih, Tri Wahyu Retno Ningsih

Disain sampul: Wira Catur

Penerbit: Lembaga Penelitian Universitas Gunadarma

ISSN: 2302-3740

DEWAN REDAKSI

PENERBIT

Lembaga Penelitian Universitas Gunadarma
Jl. Margonda Raya 100 Pondok Cina
Depok, 16424
Telp. +62-21-78881112 ext. 455
Fax. +62-21-7872829
e-Mail: kommit@gunadarma.ac.id
Laman: http://penelitian.gunadarma.ac.id/kommit

PANITIA PELAKSANA SEMINAR

Penasehat:
Prof. Dr. E.S. Margianti, S.E., MM.
Prof. Suryadi Harmanto, SSi., M.MS.I.
Agus Sumin, S.Si., MM.

Penanggung Jawab:
Prof. Dr. Yuhara Sukra, MSc.
Prof. Dr. Didin Mukodim, MM.

Ketua Pelaksana:
Dr. Ir. Hotniar Siringoringo, MSc.

Wakil Ketua Pelaksana:
Dr. Bertalya

Sekretariat:
Ida Ayu Ari Angreni, ST., MMT.
Dr. Jacobus Belida Blikololong
MS. Harlina, S.Kom., MM.

Sarana Prasarana:
Drs. Hardjanto Sutedjo, MM.
Rino Rinaldo, SE., MM
Riyanto, ST.

KATA PENGANTAR

Pertukaran informasi merupakan kebutuhan masyarakat modern, sehingga Teknologi Informasi dan Komunikasi (TIK) menjadi hal yang sangat penting. Secara kasat mata, setiap orang dapat menyaksikan perkembangan TIK yang sangat pesat. Perkembangan TIK sampai saat ini masih didominasi oleh negara-negara maju. Kondisi ini harus direposisi.

Indonesia memiliki sumber daya manusia yang handal dan banyak, di antaranya berada di perguruan tinggi. Sumber daya manusia ini terkesan bekerja masih sendiri-sendiri. Penelitian di lingkungan perguruan tinggi maupun litbang sering disalahartikan sebagai pemuas akademis, sementara di kalangan industri lebih tertarik pada penyelesaian ekonomis jangka pendek. Permasalahan ini dapat diatasi dengan memulai kolaborasi antara dunia pendidikan, litbang, industri dan pemerintah.

KOMMIT merupakan seminar nasional di bidang komputer dan teknik yang mendukung pengembangan teknologi komputer maupun aplikasi komputer dalam berbagai bidang. Seminar ini bertujuan menyediakan wadah bagi peneliti, akademisi dan praktisi untuk saling bertukar informasi, berdiskusi dan berkolaborasi sehingga dapat menghasilkan produk siap pakai di dalam bidang sistem informasi.

Topik yang menjadi pembahasan pada KOMMIT ke 7 ini adalah: sistem informasi manajemen, sistem informasi geografis, sistem informasi medis, *enterprise resource planning*, *information retrieval*, matematika aplikasi, sistem keamanan, aplikasi multimedia, pengolahan sinyal dan citra, *computer vision*, *open source & open content*, *e-government, e-business, e-education*, data semantik, *information system interoperability*, *distributed, parallel, grid, P2Pp, mobile information management, mobile tecnology, green computing*, telekomunikasi dan jaringan komputer, sistem kontrol, instrumentasi dan diagnosis, mekanika dan elektronika, energi terbarukan, *cognitive science*, *soft computing, perceptual science*, bioinformatika dan geoinformatika, *collaborative network, dan electron devices*.

Artikel yang disajikan pada seminar ini setelah melalui proses *peer review*, berjumlah seratus satu, yang berasal dari 15 Perguruan Tinggi di Indonesia. Beberapa artikel yang terpilih akan di publikasikan pada Jurnal Ilmiah yang diterbitkan oleh Universitas Gunadarma.

Semoga seminar ini dapat memberikan masukan bagi pengembangan teknologi informasi dan komunikasi di negara kita. Kami ucapkan terima kasih kepada para reviewer yang telah bersedia melakukan review, juga kepada pembicara tamu dan nara sumber yang telah berkontribusi pada acara ini, serta kepada semua pihak yang telah membantu proses produksi prosiding ini.

Ketua Pelaksana
Dr. Ir. Hotniar Siringoringo, MSc.

DAFTAR ISI

PROTOKOL AUTENTIKASI BERBASIS ONE TIME PASSWPORD UNTUK BANYAK ENTITAS

Avinanta Tarigan[1]
D.L. Crispina Pardede[2]

[1,2]*Pusat Studi Keamanan Sistem Universitas Gunadarma, Jakarta*
[1]*avinanta@gmail.com*

Abstrak

One-time-password (OTP) adalah salah satu metode autentikasi yang aman untuk dua entitas, tetapi menjadi tidak efisien ketika diterapkan kepada banyak entitas. Beberapa penelitian telah menghasilkan protokol autentikasi berbasis OTP yang efisien, tetapi verifikasi formal tidak dilakukan sehingga tidak diketahui adanya kelemahan dalam protokol tersebut. Penelitian ini menghasilkan sebuah protokol autentikasi berbasis OTP yang lebih efisien dan dapat digunakan untuk proses autentikasi banyak entitas. Dengan menggunakan 3 (tiga) langkah autentikasi dan tanpa menggunakan kriptografi yang memerlukan daya komputasi tinggi, autentikasi antara entitas dapat tercapai. Protokol ini diverifikasi secara formal untuk membuktikan keamanan dan tidak adanya kelemahan dalam protokol tersebut.

***Kata Kunci**: One-time-password, autentikasi.*

PENDAHULUAN

One-time-password (OTP) atau one-time-pad adalah metode autentikasi antara dua entitas, dimana serangkaian password digunakan oleh entitas tersebut untuk saling mengautentikasi dengan metode *challenge-and-response* (Pomeranz, 2000). OTP banyak digunakan dalam transaksi elektronik di dunia perbankan karena penggunaan password yang hanya sekali setiap transaksi dianggap jauh lebih aman dibandingkan penggunaan satu password yang sama di setiap transaksi (Kim dkk., 2008), tetapi lebih efisien dibandingkan dengan menggunakan infrastruktur kunci publik yang kompleks.

Kesederhanaan dan keamanan OTP tersebut mulai digunakan dalam sistem autentikasi banyak entitas. Kelemahannya adalah bahwa n entitas memerlukan $n^2 - n$ buah daftar OTP sehingga tidak efisien. Beberapa penelitian mengusulkan protokol autentikasi berbasis OTP untuk banyak entitas, tetapi tidak melakukan verifikasi formal terhadap protokol yang diusulkan. Verifikasi formal terhadap sebuah protokol penting dilakukan agar diketahui apakah protokol tersebut mengandung kelemahan atau tidak (Tarigan dan Hilbert, 2005). Salah satu pendekatan formal untuk verifikasi protokol autentikasi yang banyak digunakan adalah BAN *logic* (Burrows, Abadi, dan Needham, 1990). Penelitian ini mengusulkan sebuah protokol autentikasi berbasis OTP untuk banyak entitas berbantuan *Trusted Third Party* (TTP), yang efisien terhadap penggunaan kata-kunci, dan aman karena telah dianalisis menggunakan metoda formal BAN *logic*.

METODE PENELITIAN

Telaah pustaka dan perbandingan antara protokol telah dilakukan oleh dan diketengahkan dalam (Yulianti, 2009) yang berfokus pada efisiensi protokol. Pada penelitian ini, kinerja dan kriteria dari

skema autentikasi dibandingkan dengan memperhatikan parameter berikut:

1. Tidak ada tabel verifikasi (P1): Penyedia Layanan (*service provider*) tidak memerlukan kamus dari tabel verifikasi untuk melakukan autentikasi dari sebuah entitas.
   a. Jika P1 = 'Ya', berarti tidak ada informasi yang disimpan dalam tabel verifikasi,
   b. Jika P1 = 'Tidak', berarti ada informasi yang disimpan dalam tabel verifikasi.
2. *Password* dipilih secara bebas (P2): Entitas dapat memilih *password* secara bebas.
   a. Jika P2 = 'Ya', berarti entitas dapat memilih *password* secara bebas.
   b. Jika P2 = 'Tidak', maka entitas tidak dapat memilih *password* secara bebas dan tidak dapat mengunggah setiap *password*.
3. Autentikasi mutual (P3): Entitas dan penyedia layanan dapat melakukan autentikasi satu sama lain.
   a. Jika P3 = 'Ya', berarti setiap entitas dapat mengidentifikasi entitas lainnya,
   b. Jika P3 = 'Tidak', berarti setiap entitas tidak dapat mengidentifikasi entitas lain dan membutuhkan *value* lain untuk mengidentifikasi entitas lain.
4. Biaya komunikasi dan komputasi yang lebih rendah (P4) : Biasanya, oleh karena keterbatasannya, perangkat yang digunakan tidak mendukung biaya komunikasi dan *bandwidth* yang lebih tinggi.
   a. Jika P4 = 'Rendah', berarti hanya memerlukan sedikit komputasi,
   b. Jika P4 = 'Tinggi', berarti komputasi dibutuhkan dalam setiap proses meminta dan menjawab di antara *client* dan *server*, *server* dan *client*, dan sebagainya
5. Persetujuan *session key* (P5): Sebuah *session key* yang disetujui oleh entitas dan penyedia layanan, dibangkitkan pada setiap sesi.
   a. Jika P5 = 'Ya', berarti sebuah *session key* dibutuhkan untuk mendapatkan persetujuan di setiap sesi,
   b. Jika P5 = 'Tidak', berarti tidak dibutuhkan sebuah *session key* untuk mendapatkan persetujuan di setiap sesi,
6. Tidak ada sinkronisasi waktu (P6): *Timestamp* diabaikan untuk mengatasi masalah sinkronisasi waktu.
   a. Jika P6 = 'Ya', berarti tidak dibutuhkan penambahan *server* untuk memberikan atau membangkitkan *time-stamp* dan hal ini mengurangi biaya komputasi
   b. Jika P6 = 'Tidak, berarti dibuthkan penambahan *server* untuk memberikan atau membangkitkan *time-stamp* dan hal ini menambah biaya komputasi.
7. Perlunya enkripsi (P7): Konversi sebuah pesan ke dalam karakter rahasia dengan menggunakan pasangan *public/secret key*.
   a. Jika P7 = 'Ya', berarti diperlukan sebuah cara pengamanan data dengan mengubah pesan menjadi karakter rahasia.
   b. Jika P7 = 'Tidak', berarti tidak diperlukan sebuah cara pengamanan data dengan mengubah pesan menjadi karakter rahasia.
8. Jumlah prinsipal (entitas) (P8): banyaknya entitas yang diperlukan dalam proses autentikasi.
   a. Jika P8 = 'Rendah', berarti hanya memerlukan sampai dengan tiga entitas.
   b. Jika P8 = 'Tinggi', berarti memerlukan lebih dari tiga entitas.

Protokol yang Diusulkan

Tujuan dari protokol ini adalah untuk menetapkan autentikasi antara dua entitas: *A* sebagai inisiator autentikasi, dan *B* sebagai penyedia layanan, dengan

memanfaatkan pihak ketiga terpercaya *TTP* yang menjadi fasilitator. Setiap entitas mempunyai daftar (*list*) dari *one time password* yang hanya diketahui oleh entitas tersebut dengan TTP. Daftar OTP yang dipunyai oleh entitas *A* dan *TTP* adalah P^a dimana $P^a = \{P_1^a, P_2^a, \ldots, P_n^a\}$ dan setiap kata kunci dalam daftar tersebut adalah bilangan bulat positif $P_i^a \in N$. Sedangkan daftar OTP yang dipunyai entitas *B* dan TTP adalah $P^b = \{P_1^b, P_2^b, \ldots, P_n^b\}$. Dalam satu sesi autentikasi, salah satu password dalam daftar tersebut digunakan dan tidak akan digunakan lagi dalam sesi berikutnya.

Protokol ini tidak menggunakan proses enkripsi dan dekripsi dengan tujuan efisiensi komputasi, dan yang digunakan adalah *one-way-hash* h = hash(m), dimana m adalah pesan dan h adalah *digest* dari pesan tersebut. Penggunaan *one-way-hash* memerlukan daya komputasi yang lebih rendah daripada kriptografi, serta dapat digunakan untuk mengetahui integritas dari pesan yang diterima.

Protokol ini mengambil asumsi bahwa TTP dan setiap entitas sudah mempunyai daftar OTP dan jika OTP habis digunakan maka dapat dibuat kembali daftar OTP baru. Selain itu, protokol ini mengambil asumsi bahwa ada semua entitas mempunyai jam (*clock*) setiap entitas dan TTP yang tersinkronisasi dengan server waktu (*time server)* dan setiap pesan yang dikirimkan akan mendapatkan balasan (*acknowledgement*) bahwa pesan telah diterima atau ditolak. Berikut ini adalah penjelasan protokol yang diusulkan.

Fase 1: Autentikasi antara A dan TTP

Tujuan fase pertama adalah agar *A* terautentikasi oleh TTP dengan menggunakan salah satu password dalam P^a yang belum digunakan dalam sesi autentikasi sebelumnya, serta memberitahukan dengan entitas mana *A* hendak melakukan interaksi (*B*).

$$\text{M1 : A} \rightarrow \text{TTP : } A;B;\ \text{x};\ t_1;\ \text{hash}\ (P_x^a \oplus t_1)$$

Dalam pesan ini *A* mengirimkan identifikasi dirinya, identifikasi *B* sebagai penyedia layanan, x adalah indeks dari *password* yang digunakan dalam sesi tersebut, dan t_1 adalah waktu terkini pada waktu M_1 dikirimkan. Selain itu A mengirimkan hasil *one-way-hash* dari P_x^a yang dijalinkan dengan t_1 (dalam tulisan ini $\oplus$ adalah simbol untuk *concate-nation*).

Setelah menerima pesan ini, TTP membandingkan waktu terkini dengan t_1 untuk mengetahui apakah pesan yang diterima masih baru atau terkini (*freshness*), dan membandingkan antara hash ($P_x^a \oplus t_1$) yang dikalkulasi dari t_1 yang diterima dari pesan dan P_x^a yang ada dalam P^a yang dipunyai TTP. Jika hasilnya sama, maka TTP berkesimpulan bahwa autentikasi dengan A adalah berhasil, jika sebaliknya, maka TTP beranggapan bahwa M_1 bukan berasal dari *A* dan membatalkan jalannya protokol (*abbort*).

Fase 2 : Autentikasi antara TTP dengan B dan pemufakatan kata-kunci

Tujuan fase kedua adalah tercapainya autentikasi TTP oleh *B*, dan juga memberitahukan *B* bahwa *A* hendak melakukan interaksi dengan *B*. Selain itu pemufakatan kata-kunci ρ dengan *B* juga dilakukan dalam fase ini.

$$\text{M2 : TTP} \rightarrow \text{B : } A;B;\ \text{y};\ \theta;\ t_2;\ hash(P_y^b \oplus \theta \oplus t_2\ )$$

Setelah menerima pesan M_2, *B* memeriksa keterkinian pesan dengan menggunakan t_2 serta integritas dan autentikasi pesan dengan menggunakan hasil hash. Jika nilai hash sama, maka *B* berkesimpulan bahwa autentikasi dengan TTP adalah berhasil, jika tidak maka *B* akan membatalkan jalannya protokol. Sedangkan $\theta \in N$ adalah bilangan acak bulat positif yang digunakan untuk memberitahu *B* nilai $\rho \in N$ dimana $\rho = P_y^b + \theta$. Nilai ρ pada fase ini hanya

diketahui oleh *B* dan TTP karena nilai P_y^b hanya diketahui oleh keduanya.

Fase 3: Pemufakatan kata-kunci ρ antara *A* dan *B*

Tujuan fase ketiga ini TTP mengirimkan nilai ρ yang digunakan pada fase kedua, tetapi tersamar dalam nilai $\lambda \in N$, dimana $\lambda = \rho - P_x^a$.

$$\text{M3} : \text{TTP} \rightarrow A : A,B,\lambda,t_3, \text{hash}\ (P_x^a \oplus \lambda \oplus t_3)$$

Setelah menerima pesan M3, *A* memeriksa keterkinian pesan dan autentikasi bahwa pesan dari TTP seperti prosedur pada fase-fase sebelumnya. Perlu diperhatikan bahwa P_x^a adalah kata kunci yang dipilih oleh *A* pada fase pertama. Pada akhir protokol, *A* mengetahui nilai ρ yaitu dengan menambahkan λ yang diterima dengan P_x^a sehingga $\rho = P_x^a + \lambda$, sehingga *A* dan *B* mempunyai informasi ρ yang tidak diketahui entitas lain.

Autentikasi Pesan

Setelah protokol selesai pada fase 3, maka nilai ρ yang hanya diketahui *A* dan *B* dapat digunakan untuk melakukan autentikasi pesan antara kedua entitas tersebut. Misalnya dalam interaksi ke-*I*, *A* mengirimkan pesan m_i kepada *B*, maka pesan yang dikirim dapat diformulasikan sebagai berikut:

$$\text{Mi} : A \rightarrow B : A,B,m_i, t_i, \text{hash}\ (P_x^a \oplus \lambda \oplus m_i \oplus t_i)$$

atau dalam interaksi ke-*j*, *B* mengirimkan pesan m_j kepada *A*, maka pesan diformulasikan sebagai berikut:

$$\text{Mj} : B \rightarrow A : A,B,m_j, t_j, \text{hash}\ (P_x^b \oplus \lambda \oplus m_j \oplus t_j)$$

dimana *A* dan *B* dapat memeriksa keterkinian dari pesan m_j dan m_i dengan menggunakan t_j dan t_i serta memeriksa integritas dan autentikasi dengan membandingkan nilai *hash* yang dikirimkan dengan ρ yang telah diketahui masing-masing entitas yang merupakan capaian dari protokol ini.

HASIL DAN PEMBAHASAN

Protokol yang diusulkan di sini memungkinkan lebih dari tiga entitas dapat melakukan autentikasi antara satu dengan yang lainnya. Protokol ini lebih efisien dibandingkan protokol lain yang bertujuan sama, karena protokol ini hanya memerlukan 3 langkah. Jumlah kata kunci yang diperlukan hanya *n* buah untuk *n* entitas. Komputasi yang diperlukan lebih murah mengingat tidak digunakannya kriptografi. Tabel 1 menunjukkan perbandingan beberapa skema otentikasi yang menggunakan OTP berdasarkan parameter-parameter yang telah diuraikan pada bagian sebelumnya.

Tabel 1.
Efektivitas Skema Otentikasi

SKEMA	P1	P2	P3	P4	P5	P6	P7	P8
(Jeong, dkk., 2008)	Ya	Ya	Ya	Sangat Rendah	Ya	Ya	Ya	Tinggi
(Jeong, dkk., 2006])	Tidak	Tidak	Ya	Tinggi	Ya	Ya	Ya	Tinggi
(Wang dan Chang, 1999)	Ya	Ya	Tidak	Sedang	Tidak	Tidak	Tidak	Rendah
(Yang dan Shieh, 1999)	Ya	Ya	Tidak	Sedang	Tidak	Ya	Ya	Rendah
(Hwang dan Li, 2000)	Ya	Tidak	Tidak	Sedang	Tidak	Tidak	Tidak	Rendah
Shun	Ya	Tidak	Ya	Sangat Rendah	Tidak	Tidak	Tidak	Rendah
(Chien, dkk., 2002)	Ya	Ya	Ya	Sangat Rendah	Tidak	Tidak	Tidak	Rendah
(Hwang, 2002)	Ya	Ya	Tidak	Sangat Rendah	Tidak	Tidak	Tidak	Rendah
(Yuliyanti dan Tarigan, 2009)	Tidak	Ya	Ya	Sangat Rendah	Tidak	Tidak	Tidak	Rendah
Protokol yang Diusulkan	Tidak	Ya	Ya	Sangat Rendah	Tidak	Tidak	Tidak	Rendah

SIMPULAN

Protokol yang diusulkan dalam tulisan ini dapat memungkinkan banyak entitas untuk dapat melakukan pembuktian keaslian atau otentikasi satu dengan lainnya dengan efisien dibandingkan dengan protokol lain yang bertujuan sama. Efisien dalam konteks ini berarti memerlukan jumlah langkah yang sedikit (3 langkah), daftar OTP yang sedikit (*n* daftar kata-kunci untuk *n* entitas), serta tidak memerlukan daya komputasi yang berarti karena tidak menggunakan kriptografi. Keamanan dapat dicapai oleh protokol ini karena hal sebagai berikut: (1) penggunaan *timestamp* pada setiap langkah memungkinkan entitas untuk memeriksa kekinian pesan, (2) dicapainya kemufakatan atas kata-kunci memungkinkan otentikasi yang berlanjut pada satu sesi komunikasi, dan (3) penggunaan *one-way-hash* menjamin integritas pesan dan secara keseluruhan menjamin otentikasi pesan. Protokol ini masih mempunyai kelemahan, yaitu harus menggunakan *global timestamp server* untuk mensinkronkan semua entitas. Oleh karena itu perlu dipikirkan penggunaan *nonce* dalam protokol tersebut, tetapi tetap efisien. Kelemahan kedua adalah bahwa pengiriman nilai θ dan λ masih terlihat sehingga *A* dapat mengetahui P_y^b dan sebaliknya *B* dapat mengetahui P_x^a. Untuk itu diperlukan cara atau metode agar pemufakatan kata-kunci dapat dilakukan tanpa membuka komponennya.

DAFTAR PUSTAKA

Burrows, M., Abadi, M., and Needham, R. 1990 "A logic of authentication" *ACM Transactions on Computer Systems* vol 8pp 18-36.

Chien, H.Y., Jan, J.K., and Tseng, Y.M. 2002 "An efficient and practical solution to remote authentication: Smart cards" *Computers and Security* vol 21 pp 372-375.

Hwang, M.S. 2002 "A simple remote user authentication scheme" *Mathematical and Computer Modelling* vol 36 pp103-107.

Hwang, M.S., and Li, L.H. 2000 "A new remote user authentication scheme using smart cards" *IEEE Transaction on Consumer Electronics* vol 46 pp 28-30.

Jeong, J., Chung, M.Y., and Choo, H. 2006 "Secure user authentication mechanism in digital home network" *Lecture Notes in Computer Science* vol 4096 pp. 345-354.

Jeong, J., Chung, M.Y., and Choo, H. 2008 "Integrated OTP-based user authentication scheme using smart cards in home networks" *Proceedings* of the 41st Hawaii International Conference on System Sciences. pp. 294-300.

Kim, H.C., Lee, H.W., Lee, K.S., and Jun, M.S. 2008 A design of one time password mechanism using public key infrastructure *Proceeding* 4th NCM. IEEE Computer Society vol 1 pp 18-24.

Pomeranz, H. 2000 *One time password* Deer Run Associates.

Tarigan, A. and Hilbert, M. 2005. *Introduction to formal method for ensuring cryptographic protocol* (English Version).

Wang, S.J., and Chang J.F. 1999 "Smart card based secure password authentication scheme" *Computers and Security* vol 5 pp 231-237.

Yang, W.H., and Shieh, S.P. 1999 "Password authentication schemes with smart cards" vol 18 pp 727-733.

Yuliyanti, A., and Tarigan, A. 2009 A lightweight authentications protocol based on one-time-password *Thesis* Universitas Gunadarma.