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

ANALISIS DAN VERIFIKASI FORMAL PROTOKOL NON-REPUDIASI ZHANG-SHI DENGAN LOGIKA SVO-CP

Hanum Putri Permatasari[1]
Avinanta Tarigan[2]
D. Lucia Crispina Pardede[3]

[1]Jurusan Sistem Informasi, [2]Jurusan Teknik Informatika
[3]Jurusan Sistem Komputer
Universitas Gunadarma
Jl. Margonda Raya No. 100 Depok – 16424
[1,2,3]{hanum, avinanta, pardede}@staff.gunadarma.ac.id

Abstrak

Protokol non-repudiasi adalah protokol keamanan yang memberikan layanan Non-Repudiation of Origin (NRO) dan Non-Repudiation of Receipt (NRR). Protokol non repudiasi yang memenuhi kedua layanan tersebut tanpa memberi keuntungan lebih kepada satu prinsipal daripada prinsipal lain merupakan protokol yang memenuhi aspek fairness. Protokol [Zhang and Shi, 1996] adalah protokol yang seharusnya mengamankan transaksi elektronik dalam konteks non-repudiasi. Berdasarkan penelitian terdahulu mengenai verifikasi protokol non-repudiasi ZS dengan metode formal logika [Coffey and Saidha, 1997] yang dilakukan oleh [Ventuneac, 2004] menunjukkan bahwa hasil verifikasi protokol tidak dapat digunakan untuk menguji ketercapaian tujuan akhir (goal) serta tidak menguji fairness. Tujuan utama dari penelitian ini adalah melakukan analisis dan verifikasi formal terhadap protokol non-repudiasi Zhang-Shi dengan menggunakan logika SVO-CP untuk mengetahui kehandalan protokol tersebut dalam memenuhi sifat non-repudiasi, yaitu NRO, NRR, dan fairness. Prosedur penelitian dilakukan dalam empat tahap dan hasil menunjukan bahwa protokol non-repudiasi Zhang-Shi mencapai kebenaran semua tujuannya (NRO dan NRR) serta penerapan logika SVO-CP kepada verifikasi protokol non-repudiasi Zhang-Shi menunjukkan protokol tersebut mencapai fairness.

Kata Kunci: *non-repudiasi, fairness, logika SVO-CP*

PENDAHULUAN

Peningkatan pemanfaatan layanan berbasis internet seperti e-mail bersertifikasi dan pembayaran elektronik dari suatu barang menjadikan non-repudiasi dituntut dalam pengembangan protokol keamanan sebagai pertukaran pesan yang adil (*fair)*. Non-repudiasi adalah salah satu layanan keamanan yangmengawasi peristiwa penyangkalan (*repudiation*) oleh satu dari sejumlah pihak(entitas) yang terlibat dalam sebuah komunikasi, bahwa ia telah berpartisipasi dalam semua atau sebagian komunikasi. Untuk menegakkan akuntabilitas setiap partisipan atas aksi yang dilakukan, dibutuhkan layanan *Non-repudiation of Origin* (NRO) dan *Non-repudiation of Receipt* (NRR). Secara formal, *fairness* dinyatakan sebagai keadaan dimana NRO dan NRR dipenuhi atau NRO dan NRR keduanya sama sekali tidak dipenuhi. Non-repudiasi dianalisis melalui tujuan NRO dan NRR. *Fairness* dianalisis dengan melakukan pemeriksaan tercapainya tujuan NRO dan NRR.

Protokol non-repudiasi yang ditawar-

kan oleh (Zhang and Shi, 1996) dan (Zhou and Gollmann, 1996) merupakan protokol non-repudiasi yang menggunakan *online* TTP. Protokol Zhang-Shi (ZS) memiliki kelebihan dibanding protokol Zhou and Gollmann (ZG), yaitu menyediakan kerahasiaan ganda (*double confidentiality*) yang ditandai dengan pesan cipher di bawah kunci sesi serta pemanfaatan fungsi hash pada setiap transmisi pesan ke setiap partisipan.

Keamanan sebuah sistem tidak dapat hanya diukur melalui desainnya saja. Verifikasi atas implementasinya harus dilakukan juga. Verifikasi terhadap layanan non-repudiasi dapat dilakukan dengan menggunakan metode formal. Salah satu upaya pertama untuk menerapkan metode formal dalam verifikasi protokol non-repudiasi Zhang-Shi (Zhang and Shi, 1996) dengan menggunakan logika CS (Coffey and Saidha, 1997), yaitu oleh (Ventuneac, 2004). Verifikasi menggunakan logika CS menguji ketercapaian tujuan dari setiap langkah protokol dan tidak menguji ketercapaian tujuan akhir dari protokol non-repudiasi serta tidak menguji *fairness* dari protokol non-repudiasi yang diverifikasi.

Logika SVO yang merupakan unifikasi dari logika BAN, GNY, vO, dan AT telah digunakan untuk verifikasi protokol non-repudiasi (Zhou and Gollmann, 1998), namun pengujiannya dilakukan untuk membuktikan keyakinan hakim (*adjudicator*) yang merupakan pihak yang tidak terlibat dalam komunikasi yang diatur oleh protokol non-repudiasi. Pembuktian sifat *fairness* tidak hanya memeriksa bukti di akhir perjalanan protokol, melainkan harus memperhatikan tahap-tahap pengumpulan bukti oleh setiap prinsipal. Keterbatasan SVO membuatnya tidak dapat digunakan untuk membuktikan *fairness*.

Pembuktian *fairness* terhadap protokol non-repudiasi ZG tercapai oleh (Pardede, 2012) dalam penelitian disertasinya dengan menggunakan logika SVO yang diperluas, yang kemudian disebut dengan logika SVO-CP. Dengan demikian dalam penelitan ini, penulis melakukan verifikasi terhadap protokol non-repudiasi ZS dengan menggunakan logika SVO-CP untuk mengetahui kehandalan protokol tersebut dalam memenuhi sifat non-repudiasi, yaitu *Non-Repudiation of Origin* (NRO), *Non-Repudiation of Receipt* (NRR) dan *fairness*.

Logika SVO

Logika SVO (Syverson and van Oorschot, 1994) mencakup empat logika pendahulunya, yaitu GNY, BAN, AT, dan vO. Logika GNY, AT dan vO merupakan perluasan dari logika BAN, dengan demikian logika SVO juga mencakup logika BAN.

Logika SVO mempunyai dua aturan inferensi, yaitu modus ponen dan *Necessitation*. Modus Ponen: Dari φ dan $\varphi \supset \psi$ memberikan ψ. Necessitation: Dari $\vdash \varphi$ memberikan $\vdash$ P belief φ. Logika SVO mengandung dua puluh aksioma :

Believing untuk sembarang prinsipal P dan formula φdan ψ

AX1. (P believes $\varphi \wedge$ P believes $(\varphi \supset \psi)) \supset$ P believes ψ.

AX2. P believes $\varphi \supset$ P believes (P believes φ).

Source Association

AX3. $P \overset{K}{\leftrightarrow} Q \wedge$ R received $\{X^Q\}_K) \supset$ (Q said X $\wedge$ Q sees K)

AX4. PK_σ(Q,K)$\wedge$ R received X $\wedge$ SV (X, K, Y)) $\supset$ Q said Y, dimana PK_σ(Q,K) berarti K merupakan kunci verifikasi *public signature* bagi prinsipal Q.SV(X, K, Y) berarti bahwa jika diberikan pesan X yang ditandatangani, dengan menerapkan kepadanya kunci verifikasi tandatangan K maka terbukti bahwa Y adalah pesan yang ditandatangani dengan kunci privat yang sesuai.

Key Agreement

AX5. $((PK_\delta(P,K_p)) \wedge (PK_\delta(Q,K_q))) \supset P \overset{FO(Kp,Kq)}{\longleftrightarrow} Q$

AX6. $\varphi \equiv \varphi\ [F_0(K,K')/F_0(K',K)]$
Receiving
AX7. P received $(X_1, ..., X_n) \supset$ P received X_i
AX8. (P received $\{X\}_K \wedge$ P sees K) $\supset$ P received X
AX9. P received $[X]_K \supset$ P received X
Seeing
AX10. P received X $\supset$ P sees X
AX11. P sees $(X_1, ..., X_n)$ P sees X_i
AX12. (P sees $X_1 \wedge ... \wedge$ P sees $X_n) \supset$ P sees $F(X_1, ..., X_n)$
Comprehending
AX13. P believes (P sees F(X)) $\supset$ P believes (P sees X)
Saying
AX14. P said $(X_1, ..., X_n) \supset$ (P said $X_i \wedge$ P sees X_i)
AX15. P says $(X_1, ..., X_n) \supset$ (P said $X_1, ..., X_n \wedge$ P says X_i)
Jurisdiction
AX16. (P controls $\varphi \wedge$ P says $\varphi) \supset \varphi$

Prinsipal P mengatakan formula φ dimana P memiliki wewenang atas φ, maka φ benar adanya.
Freshness
AX17. fresh$(X_i) \supset$ fresh $(X_1, ..., X_n)$
AX18. fresh$(X_1, ..., X_n) \supset$ fresh$(F(X_1, ..., X_n))$
Nonce-verification
AX19. (fresh(X) $\wedge$ P said X) $\supset$ P says X)

Freshness mengubah pesan yang pernah dikatakan pada waktu lampau menjadi pesan yang segar yang baru saja dikatakan.
Symmetrics Goodness of Shared Key

AX20. $P \overset{K}{\leftrightarrow} Q \equiv Q \overset{K}{\leftrightarrow} P$

Logika SVO-CP

Penelitian yang dilakukan oleh (Pardede, 2012) dalam disertasinya yakni memperluas logika SVO agar dapat digunakan untuk verifikasi sifat *fairness* dari sebuah protokol non-repudiasi. CP melakukan perluasan terhadap logika SVO dengan menambahkan notasi dan aksioma yang dibutuhkan untuk verifikasi protokol non-repudiasi.

Notasi yang diajukan untuk perluasan logika SVO adalah:
1. MR(P, L, X): Pesan X ditujukan bagi prinsipal P pada sesi L.
2. P knows X: Prinsipal P mengetahui pesan X. Pengetahuan P akan Xdapat diperoleh melalui pesan yang diterima oleh P atau pesan yangmemang berasal dari P.

Aksioma yang diajukan adalah:
1. P says X $\supset$ P knows X.
2. P knows $(x_1, x_2, ..., x_n) \supset$ P knows x_i.
3. P believes Q said X and P believes MR(Q, L, X) $\supset$ P believes Q knowsX.
4. P believes (Q controls φ) $\wedge$ P believes (Q said φ) $\supset$ P believes φ.
5. P believes $PK_\psi(Q,K) \wedge$ P receives $\{X\}_K \supset$ P believes Q said X.

METODE PENELITIAN

Pada tahap awal yaitu melakukan identifikasi terhadap bukti NRO dan NRR dari protokol Zhang-Shi. Penelitian ini dilakukan dalam empat tahap utama, yaitu (1) tahap pertama, spesifikasi langkah-langkah protokol. Pada langkah pertama ini dilakukan spesifikasi protokol dalam bahasa logika dengan mengekspresikan setiap pesan di dalam protokol sebagai sebuah formula logika. Langkah pertama ini dikenal sebagai formalisasi protokol, (2) tahap kedua, spesifikasi asumsi-asumsi awal. Asumsi-asumsi yang diterapkan mencerminkan keyakinan (*belief*) dan milik (*possession*) dari setiap prinsipal, di awal perjalanan protokol, (3) tahap ketiga, tujuan yang diinginkan oleh protokol dinyatakan dalam bahasa logika. Tujuan-tujuan tersebut dinyatakan dalam hal keyakinan dan milik dari setiap prinsipal, di akhir perjalanan protokol. Verifikasi protokol keamanan dilakukan untuk memeriksa apakah tujuan-tujuan tersebut tercapai, dan (4) tahap keempat, langkah akhir verifikasi adalah penerapan

postulat-postulat logika. Penerapan postulat-postulat logika dilakukan untuk menurunkan keyakinan dan milik prinsipal-prinsipal, dari keyakinan awal (asumsi-asumsi) hingga mencapai tujuan protokol.

HASIL DAN PEMBAHASAN

Langkah-langkah dalam protokol Non-Repudiasi Zhang-Shi adalah

(T_1) A $\rightarrow$B : $\{PC_A || \{M\}K_{AB}\}PK_B || S_A(H(\{M\}K_{AB}) || N_A)$

(T_2) B $\rightarrow$A : $S_B(H(\{M\}K_{AB}) || N_A || N_B || t_B)$

(T_3) A $\rightarrow$SS : $\{PC_A || Label || t_B\}PK_{SS} || S_A(H(\{M\}K_{AB}) || K_{AB} || t_B)$

(T_4) B $\leftrightarrow$SS : Label, I_A

(T_5) A $\leftrightarrow$SS : Label, I_A

Dimana

Label = $f(N_A, N_B, t_B)$ dan

I_A = Label $||$ $PC_{SS} || S_{SS}$(Label $||$ $S_A(H(\{M\}K_{AB}) || K_{AB} || t_B)$)

Untuk kelengkapan, daftar item data dari setiap prinsipal A, B dan SS yang harus disimpan dalam basis data untuk keberhasilan kelengkapan protokol, yang dirangkum sebagai berikut

- A menyimpan: $S_B(H(\{M\}K_{AB})) || N_A || N_B || t_B)$, I_A, M (atau $\{M\}K_{AB}$),PC_B, yang kemudian disebut bukti *NRR*,
- B menyimpan: $S_A(H(\{M\}K_{AB} || N_A)$, N_B, t_B, I_A, M (atau $\{M\}K_{AB}$), PC_A,yang kemudian disebut bukti *NRO*,
- SS menyimpan: $\{PC_A || Label || t_B\}PK_{SS}$, $S_{SS}(t_{SS})$, S_{SS}(Label $||S_A(H(\{M\}K_{AB}) || K_{AB} || t_B)$), yang kemudian disebut bukti *NRD*.

Analisis Protokol Zhang-Shi

Pada bagian ini diaplikasikan logika SVO-CP (Pardede, 2012) untuk verifikasi protokolnon-repudiasi Zhang-Shi (ZS). Protokol ZS dianalisis untuk verifikasi apakah tujuan akhir (*goal*) serta *fairness* tercapai. Langkah pertama adalah menet-apkan spesifikasi protokol non-repudiasi ZS secara formal.

Spesifikasi Protokol Secara Formal

- (T_1) A$\rightarrow$B : $\{PC_A$, $\{M\}K_{AB}\}PK_B$, $S_A(H(\{M\}K_{AB}), N_A)$
- (T_2) B $\rightarrow$A : $S_B(H(\{M\}K_{AB})$, N_A, N_B, $t_B)$
- (T_3) A $\rightarrow$SS : $\{PC_A$, Label, $t_B\}PK_{SS}$, $S_A(H(\{M\}K_{AB}), K_{AB}, t_B)$
- (T_4) B $\leftrightarrow$SS : S_{SS}(Label, $S_A(H(\{M\}K_{AB}), K_{AB}, t_B)$)
- (T_5) A $\leftrightarrow$SS : S_{SS}(Label, $S_A(H(\{M\}K_{AB}), K_{AB}, t_B)$)

Spesifikasi Asumsi Awal

P1 A believes $PK_\sigma(B, S_B)$

P5 A believes $PK_\sigma(SS, S_{ss})$

P2 B believes $PK_\sigma(A, S_A)$

P6 B believes $PK_\sigma(B, PK_B)$

P3 SS believes $PK_\sigma(A, S_A)$

P7 B believes $A \overset{KAB}{\longleftrightarrow} B$

P4 B believes $PK_\sigma(SS, S_{ss})$

P8 B believes fresh (N_A)

P9 A believes f resh (t_B, N_B)

Asumsi P1 sampai dengan P5 menyatakan bahwa prinsipal yakin akan kunci verifikasi tanda tangan publik dari prinsipal lain yang mengirimkan pesan kepadanya. Sebagai contoh: A *believes* PK_{SV} (B, S_B) berarti prinsipal A yakin bahwa S_B adalah kunci publik untuk verifikasi tanda tangan B. Asumsi-asumsi ini bersama dengan aksioma yang relevan digunakan untuk menunjukkan asal-usul pesan yang dikirimkan kepada resipien, juga untuk menunjukkan keyakinan re-sipien atas prinsipal yang mengatakan pesan.

P10 A believes MR(B, L, $H\{M\}K_{AB}$
P11 A believes MR(SS, L, K_{AB})

Asumsi P10 menyatakan bahwa prinsipal A sebagai originator pesan M yakin bahwa pesan M ditujukan bagi prinsipal B pada sesi L. Asumsi P11 menyatakan bahwa prinsipal A sebagai originator pesan K yakin bahwa pesan K ditujukan bagi SS pada sesi L.

P12 A believes SV($S_B(H(\{M\}K_{AB}))$, N_B, t_B), S_B, ($H(\{M\}K_{AB})$)
P13 B believes SV($S_A(H(\{M\}K_{AB}))$), S_A, ($H(\{M\}K_{AB})$)
P14 SS believes SV($S_A(H(\{M\}K_{AB}))$, K_{AB}, t_B), S_A, ($H(\{M\}K_{AB})$)
P15 B believes SV(S_{SS}(L, $S_A(H(\{M\}K_{AB})$, K_{AB}, t_B))), S_{SS}, ($H(\{M\}K_{AB}$, K_{AB},t_B))
P16 A believes SV(S_{SS}(L, $S_A(H(\{M\}K_{AB})$, K_{AB}, t_B))), S_{SS}, ($H(\{M\}K_{AB}$, K_{AB},t_B))

Asumsi P12 sampai dengan P16 mengasumsikan keyakinan prinsipal akan kunci verifikasi tanda tangan publik dari prinsipal yang berkomunikasi dengannya.

P17 B *believes* SS *controls* $PK_{\psi}(A, K_{AB})$
P18 SS *said* (A, B, L, K_{AB}) $\supset$A *said* (A, B, L, K_{AB})$\wedge$B *receives* (A, B, L,K_{AB})

Asumsi P17 menyatakan bahwa prinsipal B sebagai resipien pesan dari A yakin bahwa SS mempunyai wewenang atas kunci publik K_{AB} yang dimiliki oleh A. Asumsi P18 menyatakan bahwa bila SS said (A, B, L, K_{AB}) maka sebelumnya A mengatakan (A, B, L, K_{AB}) dan prinsipal B menerima (A, B, L,K_{AB})

Spesifikasi Tujuan

P19 B receives {PC_A, $\{M\}K_{AB}\}PK_B$, $S_A(H(\{M\}K_{AB}), N_A)$
P20 A receives $S_B(H(\{M\}K_{AB}), N_A, N_B, t_B)$
P21 SS receives {PC_A, Label, $t_B\}PK_{SS}$, ($S_A(H(\{M\}K_{AB}), K_{AB}, t_B)$)
P22 B receives $S_{SS}(L, S_A(H(\{M\}K_{AB}), K_{AB}, t_B))$
P23 A receives $S_{SS}(L, S_A(H(\{M\}K_{AB}), K_{AB}, t_B))$

Premis P19 sampai dengan P23 adalah anotasi langkah-langkah spesifikasi tujuan dalam protokol ZS.Pada setiap langkah, prinsipal diasumsikan menerima pesan yang ditujukan kepadanya sesuai protokol.

Asumsi Pemahaman Penerimaan Pesan

P24 B believes B receives {PC_A, $\{M\}K_{AB}\}PK_B$, $S_A(H(\{M\}K_{AB}), N_A)$
P25 A believes A receives $S_B(H(\{M\}K_{AB}), N_A, N_B, t_B)$
P26 SS believes SS receives {PC_A, L, $t_B\}PK_{SS}$, ($S_A(H(\{M\}K_{AB}), K_{AB}, t_B)$)
P27 B believes B receives S_{SS}(L, $S_A(H(\{M\}K_{AB}), K_{AB}, t_B)$)
P28 A believes A receives S_{SS}(L, $S_A(H(\{M\}K_{AB}), K_{AB}, t_B)$)

Keyakinan setiap prinsipal bahwa ia menerima pesan perlu diasumsikan untuk dapat menurunkan keyakinan prinsipal akan pesan yang ia yakin diterimanya.

Tujuan *Fairness*

Protokol dianalisis untuk melihat apakah protokol menjamin *fairness*. Protokol dikatakan mencapai *fairness* bila memenuhi B *believes* A *said* M (*NRO*) and A *believes* (B *said* NRR *and* SS *said* NRD).

Penerapan Postulat Logika

Sebagai langkah akhir dari verifikasi protokol keamanan, dilakukan penerapan aksioma-aksioma dan aturan inferensi secara berulang untuk memperoleh hasil yang diharapkan.

Berangkat dari premis [P20] dan dengan menerapkan aksioma [AX7] diperoleh [R4]. A *receives* $S_B(H(\{M\}K_{AB})$,

N_A, N_B, t_B) ⊃ A *receives* $S_B(H(\{M\}K_{AB}))$. Dengan penerapan MP pada [P25] dan [R4] diperoleh [R5]. A *believes* A *receives* $S_B(H(\{M\}K_{AB}))$. Penerapan MP dan [AX4] kepada premis [P1], [P12], dan hasil [R5] memberikan [R6]. A believes B said $(H(\{M\}K_{AB}))$. [R6] menyatakan bahwa prinsipal A yakin bahwa pesan $(H(\{M\}K_{AB}))$ yang diterima berasal dari prinsipal B. $(H(\{M\}K_{AB}))$ adalah tanda terima pesan (NRR) yang merupakan bukti bahwa B telah menerima pesan yang sebelumnya dikirimkan oleh A.

Penerapan aksioma [AX7] pada [P22] diperoleh [R11]. B *receives* $S_{SS}(L, S_A(H(\{M\}K_{AB}), K_{AB}, t_B))$ ⊃ B *receives* $S_{SS}(L,S_A(H(\{M\}K_{AB})))$. Dengan penerapan MP pada [P27] dan [R11] diperoleh [R12]. B *believes* B *receives* $S_{SS}(L, S_A(H(\{M\}K_{AB})))$. Penerapan [MP] dan [AX4] kepada premis [P4], [P15] dan hasil [R12] memberikan [R13]. B believes SS said $(L, S_A(H(\{M\}K_{AB})))$ yang menyatakan B yakin bahwa pesan $(L, S_A(H(\{M\}K_{AB})))$ berasal dari SS. Pesan tersebut merupakan tanda konfirmasi dari SS bahwa ia telah menyediakan kunci K_{AB} untuk dapat diakses secara bebas oleh B.

Hasil penerapan MP pada [R13] dan premis [P18] memberikan [R14]. B *believes* A *said* (A, B, L, K_{AB}) yang menyatakan bahwa prinsipal B yakin bahwa (A, B, L, K_{AB}) yang memuat kunci K_{AB} berasal dari A. Hasil penerapan MP pada AX15 kepada [R13] memberikan [R15]. B *believes* SS *said* K_{AB}, dimana $K_{AB}= PK_{\psi}(A, K_{AB})$. Dengan memperhatikan [P17] dan [R15], aksioma [AT4] memberikan [R16]. B believes $PK_{\psi}(A, K_{AB})$. Penerapan aksioma [AT5] pada [R2a] dan [R16], dimana $M = \{M\}K_{AB}$, $K_{AB}= PK_{\psi}(A,K_{AB})$ memberikan [R17]. B *believes* A *said* M. Prinsipal B telah menerima $\{M\}K_{AB}$ dan yakin bahwa K_{AB} adalah kunci publik dari A, yakin bahwa pesan M berasal dari A. Prinsipal B dapat membuka pesan M menggunakan kunciK_{AB}.

Berangkat dari premis [P23] dan dengan menerapkan aksioma [AX7] pada [P23] diperoleh [R18]. A receives $S_{SS}(L, S_A(H(\{M\}K_{AB}), K_{AB}, t_B))$ ⊃ A receives $S_{SS}(L,S_A(H(\{M\}K_{AB})))$. Penerapan MP pada [P28] dan [R18] memberikan [R19]. A believes A receives $S_{SS}(L, S_A(H(\{M\}K_{AB})))$. Penerapan [MP] dan [AX4] kepada premis [P5], [P16] dan hasil [R19] memberikan [R20]. A *believes* SS *said* $(L, S_A(H(\{M\}K_{AB})))$. Prinsipal A yakin bahwa SS telah meletakkan kunci K_{AB} pada direktori yang bisa diakses oleh B. Hal tersebut ditunjukkan oleh keyakinan A bahwa pesan $(L, S_AH(\{M\}K_{AB}))$ berasal dari SS. Pesan tersebut merupakan bukti konfirmasi (NRD) bahwa SS telah menerima K_{AB} dari A dan telah menyediakannya untuk dapat diakses oleh B.

Diskusi

Berdasarkan analisis dengan penerapan logika SVO-CP pada protokol Zhang-Shi menunjukkan resipien B yakin pesan M berasal dari originator A. Hal tersebut ditunjukkan oleh [R17] B *believes* A *said* M. Keyakinan originator A bahwa pesan telah diterima oleh resipien B dan SS telah menyediakan kunci K_{AB} di sebuah tempat yang bisa diakses oleh B tercapai dan ditunjukkan oleh [R6] A *believes* B *said* $(H(\{M\}K_{AB}))$ dan [R20] A *believes* SS *said* $(L, S_A(H(\{M\}K_{AB})))$. $(H(\{M\}K_{AB}))$ adalah tanda terima pesan (NRR). $(L, S_A(H(\{M\}K_{AB})))$ adalah konfirmasi bahwa SS menyediakan kunci K_{AB} untuk dapat diakses oleh B (NRD). Kedua hal tersebut di atas menunjukkan dipenuhinya B *believes* A *said* M *and* A *believes* (B *said* $(H(\{M\}K_{AB}))$ and A *believes* SS *said*$(L, S_A(H(\{M\}K_{AB})))$). Dengan demikian, analisis protokol menggunakan logi-

ka SVO-CP menunjukkan bahwa tujuan *fairness* B *believes* A *said* M *and* A *believes* (B *said* NRR *and* SS *said* NRD) dipenuhi.

SIMPULAN

Penerapan metode formal logika SVO-CP dalam analisis dan verifikasi protokol non-repudiasi Zhang-Shi menunjukan bahwa protokol tersebut memiliki kehandalan yang dipenuhinya kebenaran atas semua tujuannya (*Non-Repudiation of Origin* (NRO) dan *Non-Repudiation of Receipt* (NRR)).

Tujuan *fairness* dalam penelitian ini adalah B believes A said M and A believes (B said NRR and SS said NRD). Penerapan logika SVO-CP kepada veryfikasi protokol non-repudiasi Zhang-Shi menunjukkan protokol tersebut mencapai *fairness*.

DAFTAR PUSTAKA

Coffey, T. and Dojen, R. 2009 “A Formal Verification Centred Development Process for Security Protocols” chapter XIV, pages 165-178. IGI Global.

Coffey, T. and Saidha, P. 1997 “Logic for verifying public-key cryptographic protocols” *IEEE Proceedings Computer Digital Technology*, 144(1):28 –32.

.

Pardede, D. L. C. 2012 *Perluasan Logika SVO Untuk Analisis Dan Verifikasi Formal Protokol Non-Repudiasi* PhD thesis of Information Technology Gunadarma University Depok.

Syverson, P. F. and Van Oorschot, P. C. 1994 “On unifying some cryptographic protocol logics” *IEEE Symposium on Research in Security and Privacy* pages 14-28.

Tarigan, A., Rechnernetze, A., Systeme, V., and Bielefeld, U. 2002 *Survey in formal analysis of security properties of cryptographic protocol*.

Ventuneac, M., C. T. N. T. 2004 “Reasoning on properties of non-repudiation security protocols” *WSEAS Transactions on Information Science and Applications*, 1(5):1262–1267.

Zhang, N. and Shi, Q. 1996 “Achieving non-repudiation of receipt” *The Computer Journal* 39(10):844–853.

Zhou, J. and Gollmann, D. 1996 “A fair non-repudiation protocol” In *IEEE Symposium on Security and Privacy Research in Security and Privacy* pages 55–61 IEEE Computer Society Press.

Zhou, J. and Gollmann, D. 1998 “Towards verification of non-repudiation protocols” *In Proceedings of 1998 International Refinement Workshop and Formal Methods Pacific* pages 370–380 Springer-Verlag