Sistem Kriptografi Dalam Menangani Keamanan Data Pada Skype™

Syahrul Anwar – NIM : 13503061

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail :
if13061@students.if.itb.ac.id

Abstrak

Berdasarkan data dari eBay, Skype menjadi layanan VoIP yang populer, dengan lebih dari 60 juta pelanggan saat ini. Alasan utama populernya Skype karena harganya yang rendah, hampir mendekati nol jika terjadi telepon dari komputer ke komputer. Skype juga dilengkapi dengan layanan suara dan reabilitas yang bagus. Walaupun Skype bisa didapatkan secara cuma-cuma dan dapat menembus jaringan terbuka, namun Skype menjadi hak milik protokol dan infrastruktur, fakta dimana penggunanya dapat diabaikan saat itu juga.

Peningkatan Skype ini menjadi pintu belakang bagi keamanan jaringan. Karena kepemilikan Skype, kita tidak akan mengetahui apa yang terjadi di belakang sana. Skype memiliki beberapa bug yang serius yang membuka protokol dan dapat dieksploitasi oleh *hacker*. Untuk itu sangat perlu diperhatikan langkah-langkah atau solusi yang dapat mengontrol kerja dari Skype ini pada komputer atau jaringan komputer kita.

Selain membahas kriptografi secara umum, untuk lebih memperdalam pemahaman kita mengenai sistem kriptografi yang digunakan maka kita akan membahas kepada yang lebih spesifik terutama mengenai penggunaan dan implementasi dari sistem kriptografi kunci public yang dimiliki oleh aplikasi ini.

***Kata kunci**:* Skype *security*, VOIP, *Advanced Encryption Standard*, *electronic code book*, *cipher block chaining*, *cipher feedback*, *output feedback*, *AESEncryptor*, enkripsi, dekripsi.

1. Pendahuluan

Skype membuat pemakaian kriptografi untuk otentifikasi *user* dan identifikasi *server*, dan untuk melindungi *content* yang ditransmisikan melalui jaringan *peer to peer* ini dari pemakain illegal oleh pihak lain selain pemilik *peer*. Sistem kriptografi yang dikembangkan dalam skype ini didesain dan diimplementasikan dengan baik. Keinginan untuk menyediakan pengecekan validitas pengguna dan kepercayaan pada validitas data sudah tercapai.

Skype hanya menggunakan kriptografi standar yang primitif, dengan pendekatan *sound engineering*. Primitif-ptimitif ini termasuk AES block cipher, RSA public-key cryptosystem, ISO 9796-2 signature padding scheme, SHA-1 hash function, dan RC4 stream cipher. Pengimplementasian dan pengencekan sudah dilakukan sesuai dengan referensi standar masing-masing primitif ini.

Skype mengoperasikan sebuah ototritas yang tersertifikasi untuk *user names* dan otorisasi. Tanda tangan digital yang dibuat dengan ototritas ini adalah basis untuk indentittas pada Skype. Titik-titik Skype masuk ke dalam sebuah sesi yang diverifikasi dengan benar. Tidak memungkinkan bagi penyerang untuk menipu identitas Skype pada atau dibawah *session layer*.

Skype memakai *proprietary session-establishment protocol*. Tujuan kriptografis dari protokol ini adalah melindungi balasan dari lawn bicara, mengecek validitas identitas, dan untuk mengecek persetujuan terhadap kunci sesi yang rahasia. Lawan bicara kemudian mempergunakan kunci sesi mereka untuk keperluan komunikasi rahasia selama waktu hidup sesi tersebut.

1.1. Kebijakan Keamanan

Sebuah kebijakan keamanan menegaskan apa makna “keamanan” dalam konteks sistem dan dapat menjawab pertanyaan, “Apakah sistem ini aman?”. Sebuah kebijakan keamanan adalah bantuan yang sangat berarti kepada perancang, implementer, operator, manajer, dan pemakai sistem. Kebijakan-kebijakan keamanan Skype ialah sebgaia berikut:

1. Usernames Skype unik.
2. Pemakai atau pelamar harus menentukan username dan otentikasi yang berasosiasi dengannya (contohnya

password) sebelum mereka dapat memiliki identitas dan hak aksesnya.

3. Masing-masing *peer* melakukan identifikasi lawan komunikasi setiap sesi Skype terbentuk Masing-masing menverifikasi lawnnya sebelum sesi tersebut mengizinkan terlewatkannya pesan-pesan(contoh, suara, video, file, atau teks).

Pesan yang dikirimkan lewat sebuah sesi Skype disandikan dari Skype-end ke Skype-end. Tak ada node perantara, jika yang mana pun ada, kalaupun ada harus memiliki kepertingan tertentu yang berhubungan dengan pesan yang dikirim.

2. Gambaran dari *Cryptography Skype*

2.1 Registrasi

Inti kerahasiaan penulisan kode rahasia (cryptography) pada skype berada pada server utama penandaan kunci, Ss. koresponding pengujian umum, Vs, dan sebuah pengenal untuk kunci ganda yang diinstal di setiap klien skype pada saat membuatnya.

Pelatihan dalam skype cryptosystem dimulai dengan melakukan registrasi terlebih dahulu. Pengguna memilih nama yang diinginkan, misalkan pengguna memakai nama A, dan sebuah password, misalnya PA. Klien pengguna mengembangkan kunci ganda RSA. Tanda kunci pribadi, SA, dan password cadangan, H(PA\0, disimpan sebagai pengaman pada platform pengguna. Pada platform windows dilakukan menggunakan (windows CryptoProtectData API).

Klien selanjutnay membuat sesi 256-bits AES-sesi encrypted dengan server utama. Kunci untuk sesi ini dipilih oleh klien dalam menolong pengacakan nama penggerak pada platform spesifiknya. Klien dapat menguji apakah platform tersebut sudah terdaftar pada server. Klien mengirim pada server, diantara beberapa kode, A, H(PA) dan VA.

Server utama memilih apakah nama tersebut berbeda dan dapat diterima oleh aturan penamaan dalam skype. Jika ya, server menyimpan (A, H(H(PA))) dalam data base. Ini membentuk dan menandai identitas data untuk A, ICA, yang berisi, diantara kode-kode tersebut, tanda server utama RSA A dan VA,{A, VA} S dan kunci pengenal dari SS.ICA dikembalikan pada A.

Sebenarnya penandaan kunci server yang dijelaskan diatas disederhanakan untuk memperjelas. Pda kenyataanya, terdapat dua kunci ganda server utama, yang satu dengan modulus 1536 bits dan yang lainnya dengan modulus 2048 bits. Pilihan dimana modulus untuk digunakan dibuat dengan server utama. Ini tergantuk pada latihan pengunaan server skype premium yang telah dibeli, contohnya, skypeout. Jika berhasil, service premium untuk pertama kali akan diperkenalkan sebuah IC baru, ditandai dengan kunci yang lebih lama.

Terdapat kesederhanaan lain yang akan terjadi pada penjelasan diatas. Server utama tersebut ternyata membuat sejumlah mesin dengan fungsi-fungsi yang berbeda, termasuk satumesin yang tidak melakukan apapun kecuali menandai data. Juga keseluruhan pada server utama dicopy beberapakali untuk mengulang tampilan dan tugas.

2.2 Tiap detail kecocokan kunci

Misalkan A ingin berkomunikasi dengan B, dan tidak ada keberadaan sesi skype sebelumnya diantara keduanya. Pada kasus ini sebuah sesi baru dibentuk dan dikirim dengan kunci 256 bitsnya, SKAB. Sesi ini akan berlangsung lama selama ada tanda disetiap cara penggunaan A dan B, dan untuk waktu yang sudah pasti setelahnya. Setelah sesi tersebut berakhir, SK disimpan dalam memori hingga klien tersebut ditutup, dimana waktunya menjadi nol.

Pengembangan sesi pertamakali membutuhkan koneksi antara A dan B sepanjang skype yang menggunakan koneksi ini, A dan B sekarang bersatu dalam kesesuaian kunci selama keduanya telah teruji kebersihannya, identitasnya, dan diterima dalam SKAB.

2.2 Sesi Cryptography

Semua tanda dalam sebuah sesi disembunyikan oleh penyensoran teks kosong dengan aliran kunci yang dibentuk 256- bit AS (dikenal sebagai Rijindael) beroperasi dalam interger count mode (ICM). Kunci yang digunakan tersebut telah menjadi pengguna skype sejak agustus 2004. Karier saya selama 35 tahun sebagai cryptographer dan ahli pengamanan computer, telahmengajarkan saya untuk menjadi

skeptokal yang professional dalam segala pengamanan, terutama untuk sebuah system yang terlatih seperti skype dalam melakukan pertahanan network tertentu. Lalu saya memformat kembali hard disk dalam sebagian computer dan memberikan box tersebut pada aplikasi skype. Sebulan kemudian saya mengecek daftar dari proses pengoperasian mesin tersebut, mengecek apapun yang mencurigakan. Saya juga melakukan eksperimen selama mengambil dan menganalisa paket-paket tersebut masuk-keluar box. Saya mencaritahu bagimana skype bekerja. Semoga anda telah melakukan eksperimen yang sama.

Mungkin anda membayangkan bagaimana senangnya saya ketika, pada April 2005, skype menghubungi saya dan mengundang saya untuk melakukan evaluasi sendiri terhadap pengamanan informasi skype, dengan fokus spesial dalam skype cryptosystem. Sya berkunjung ke pusat pengoperasian skype di Tallin, dank e pusat perdagangan skype di London. Di setiap tempat saya mewawancarai orang-orang skype dan diwawancarai oleh mereka. Pertemuan tersebut berjalan dengan lancer, saya memenangkan bisnis tersebut. Sejak 1 Juni ’05 saya telah menganalisa pengamanan property dari software skype dan service-nya, dengan memfokuskan pada penggunaan cryptography yang terbaru saya telah mendapatkan akses pada ahli-ahli skype dan pada kode skype. Sya telah mengetahui banyak mengenai skype. Semakin saya temukan semakin saya senang.

Skype membuat penggunaan cryptography menjadi luas untuk pengguna sebenarnya dan identitas server, dan untuk melindungi isi network p2p dari kemunculannya yang hanya senagian. Sistem pengujian akan menampilkan identitas pengguna dan diterimanya p2p. Saya percaya skype dapat dibanggakan.

Skype hanya menggunakan standar cryptographic yang lama. Cara lama tersebut termasuk AES blok cliper, RSA kunci umum cryptosystem, skema cara penandaan ISO 9796-2, Fungsi SHA-1, dan aliran RCA cliper. Sya melihat implementasi dari tiap skype, dan menguji tiap implementasi tersebut.

Skype mengoperasikan hak penciptaan data untuk nama pengguna. Penandaan digital diciptakan berdasarkan hak ini untuk mengidentifikasikan skype. Skype memulai sesi dengan benar dengan menguji kejelasan identitas.

Skype menggunakan sesipengembangan yang pas. Tujuan cryptographic adalah untuk melindungi replay, untuk menguji identitas, dan untuk membiarkan pengomunikasian untuk menyetujui sesi kunci rahasia. Pengkomunikasian tersebut kemudian menggunakan kunci sesi untuk mendapatkan komunikasi yang tetap. Selanjutnya, saya mengeksplor kekuatan protocol dalam melawan serangan range yang terkenal, termasuk replay attack dan man- in- the-middle-attack.

Informasi ini dihasilkan setelah melakukan evaluasi selama 4 bulan. Lamanya evaluasi dapat memecahkan masalah yang belum terlihat. Pada versi 1.3 kode base diuji. Kode base diulangi untuk membuka snapshot.

Terdapat kesederhanaan lain dari penjelasan diatas. Server utama pada kenyataannya berisi sejumlah mesin dengan fungsi berbeda, termasuk mesin yang tidak melakukan apapun selain menandai data. Termasuk, keseluruhan server pod utama dicopy beberapa kali.

Nomer acak digunakan untuk beberapa tujuan cryptographic dalam skype, seperti perlindungan terhadap serangan playback. Pengamanan skype P2P bergantung pada kualitas nomer acak dengan kejelasan komunikasi.

Nomer acak bervariasi dari satu platform ke platformlain. Sejauh ini, saya telah mengevaluasi nomer acak hanya pada platform windows, yang bekerja dengan baik. Platform dengan processing yang terbatas atau lebih internal dapat diperkirakan menjadi lebih bagus, dan ini dapat dievaluasi dengan amat baik di masa yang akan datang.

Dalam sebuah platform system pengoperasian windows, skype membuat system win 32 memanggil nomer fungsi operasi system. Bits tersebut merespond panggilan ini, menggunakan SHA-1, permintaan yang tinggi pada 64-bits dikembalikan.

Skype menggunakan standar cryptographic yang lama untuk hasil pengamanaanya. Tidak ada kegagalan dalam skype, karena latihan yang baik pada engineering. Standar lama memiliki keuntungan dalam penganalisaan dan pengevaluasiannya di seluruh dunia.

Cryptographic lama yang digunakan di skype adalah: AES blok cipher, RSA kunci umum cryptosystem, penandaan ISO 9796-2, fungsi SHA-1, dan arus RC4 cipher. Saya menguji AES skype dengan kode yang berdiri sendiri.

Skype dalam ICM digunakan sebagai kunci penggerak untuk pemaketan data yang tersembunyi.

Terdapat fungsi-fungsi cadangan . Keduanya diuji tanpa hambatan. Kode SHA-1 skype telah benar. Itu melewati tes vectornya sendiri, dan tes vector yang lain. Saya menulis sebuah skrip untuk mengecek skype SHA-1 melawan implementasi Sha-1 perl, untuk penggerak alat acak besar.

RC4 algoritm digunakan dalam skype untuk menggerakan RSA. Implementasi RC4 telah diketahui secara umum. Proses inisialisasi RC4 dengan acak menggunakan bits dan arus kunci RC4 untuk menggerakan fungsi cryptGenRandom.

Kecocokan kunci diterima mrenggunakan protocol yang cocok. Saya membangun model resmi protocol, menganalisa jalannya model protocol. Saya juga menguji kebenaran implementasi protocol pada sumber kode.

Protocol bersifat simetris.

Untuk mencegah kegagalan, digunakan 64 bit nonces secara acak dan dijawab dengan pengembalian, ditandai dengan penndaan kunci pribadi penjawab.

Untuk mengembangkan identitas, pertukaran identitas pada (ditandai server pusat) dan menguji ke-valid-an data. Karena identitas data mengandung kunci umum, tiap kejelasan data kemudian dapat menguji penandaan pada bagian lain. Selain itu tiap detail dapat menyembunyikan pesan RSA pada bagian tertentu.

Satu cara untuk menguji kekuatan kecocokan kunci protocol adalah dengan mengeksplor serangan yang mungkin terjadi.

3. Detil Dalam Skype Cryptography

3.1 Pembentukann Nomer Random

Nomer acak digunakan untuk beberapa cryptographic yang bertujuan dalam proses yang terjadi pada skype, seperti sebagai perlindungan terhadap serangan balik, pergerakan kunci ganda RSA, dan pergerakan kunci sebagian pada AES dilakukan untuk mengisi cryption. Pengamanan pada sesi skype P2P bergantung sekali pada keselarasan nomer random yang dikgerakan oleh detil komunikasi.

Nomer random bergerak bervariasi dari satu platform ke platform lainnya. Sejauh ini, saya telah menguji nomer random yang hanya bergerak pada platform windows, dimana proses tersebut berjalan dengan baik. Platform dengan kekuatan processing yang terbatas lebih membatasi pergerakan random, dan ini mungkin dapat dievaluasi dengan lebih produktif lagi di masa yang akan datang.

Miller Rabin melakukan tes pada pergerakan nomer termasuk pada kode yang memungkinkan untuk di tes pada aturan kondisi Miller Robin. Yang kemudian dari hasil yang telah diteliti nomer-nomer tersebut sangat efisien dalam pengoperasian tim sengineering.

3.2 Cryptography Primitives

Skype menggunakan standar cryptography promitives untuk mendapatkan hasil pengamanannya. Tidak ada aturan penyembunyian dalam skype. Standar lama memiliki keuntungan pada analisis lama dan baru. Cryptography lama digunakan dalam skype yaitu; AES blok cipher, kunci umum cryptosystem RSA

3.2.1 AES

Saya mengevaluasi kode AES menggunakan ukuran blok 128 bits. Standar AES-256 dibandingkan dengan skype AES. Skype AES mencocokan hasil-hasil buatan implementasi lain. Skype menyimpan usaha yang jelas terhadap pemercepat jalannya AES. Ini menggunakan macros pada kecepatan. Saya membandingkan kode skype AES untuk dua pengoptimalisasian C/CCH implementasi. Skype

tersebut menyembunyikan tampilan fungsi pada jam putar tiap penyembunyian.

Skype AES dalam ICM digunakan sebagai kunci penggerak untuk penyembunyian data. Alat dengan paket data pada semua kecuali 2 bytes disembunyikan sebagaimana yang terlihat pada:

A. Blok paket data yang berhasil adalah XoRed hingga blok AES cipher. Huruf-huruf digunakan menggunakan sesi kunci yang dibentuk;

   Salt: salt: packet-indeks: block #

   The packet- index is a 48-bitvalue& the block # is a 16 bit value.
B. Sebuah CRC dioperasikan dalam bentuk alat tersembunyi.
C. Ket: Hanya permintaan dengan bit rendah pada counter AES mengubah dari blok satu ke blok lain selama menyembunyikan sebuah alat.

3.2.2 RSA

Kode skype yang menguji pergerakan kunci ganada muncul untuk diimplementasikan dengan benar. Kode tersebut menggunakan cara tidak biasa yang bervariasi.

3.2.3 Tanda Pengaman

Kode pengaman RSA digabungkan dengan ISO9796-2. Untuk masukan yang lebih kecil, pengamanan mengambil bentuk:

4A <DATA><SHAL (DATA)> BC.4BB..BA <data><shal(data)>BC

Pemasukan yang lebih besar diamankan dengan format

6A <spartial data><shal (complete-data)>BC

Metode pengujian tanda tersebut mengecek kesatuan tanda pesan. Ini menyembunyikan RSA dan menginteraksikan pengamanan. Ini juga mengecek keakuratan cadangan. Sesuai dengan ISO 9796-2, setelah pemblokan tanda pertama, selanjutnay tanda pesan diketik tersembunyi, dan ini diujimelalui cadangan SHA-1.

3.2.4 SHA

Kode pengimplementasian keamanan SHA-1, amat bagus dan kuat. Kenyataanya versi ini mudah untuk diikuti daripada pengimplementasian sumber kode SHA-1. Tidak terdapat tipe yang tidak sesuai, ataupun masalah-masalah lain. Kode tersebut bersih tanpa peringatan.

Terdapat dua fungsi cadangan. Keduanya telah terbukti tidak bermasalah. Kode tipe skype SHA-1 memiliki kebenaran. Kode tersebut melewati tes vector dan tes lain. Sya menulis skrip untuk mengecek output skype SHA-1 melawan pengimplementasian SHA-1 perl untuk menggerakan alat secara acak.

3.2.5 RC4

RC4 digunakan dalam skype untuk menggerakan RSA. Implementasi RC4 amatlah biasa. Inisialisasi RC4 dengan bits acak dan penggunaan arus kunci RC4 dalam menggerakan kunci RSA merupakan teknik yang dapat diterima. Sebuah penggunaan serupa dilatih oleh Microsoft pada fungsi cryptoGenRandom.

3.3 Detail-detail Kecocokan Kunci Protokol

Kecocokan kunci protocol didpat dengan menggunakan protocol yang cocok. Saya membuat sebuah model protocol resmi dan menganalisa model tersebut untuk berjalannya protocol. Saya juga menguji kebenaran implementasi protocol dalam sumber kode.

Protokol bersifat simetris, detailnya berkemampuan satu sama lain dengan random bit nonces 64, dan dengan pengembalian kemampuan, dimodifikasi pada arah standard an ditandai dengan kunci jawaban pribadi.

Untuk membuat identitas, pertukaran detail dalam data identitas dan pengujian data tersebut harus valid. Karena data identitas memuat kunci umum, tiap detil dapat menguji bentuk tanda oleh bagian lain. Juga, tiap detil dapat mengirim pesan dengan sendirinya.

Bit hingga tiap bagian memiliki kontribusi pada sesi kunci 128 random bit hingga 256- bit.

Kontribusi ditukar sesuai RSA cryptogram. Kedua kontribusi tersebut kemudian tergabung dalam arah suara cryptography untuk membentuk kunci sesi gabungan.

3.4 Serangan Pada Kecocokan Kunci Skype

Satu cara untuk menguji kekuatan tiap kecocokan kunci protocol adalah untuk mengeksplor berbagai serangan. Sya mempertimbangkan serangan langsung protocol dan juga serangan pada penjumlahan protocol.

3.4.1 Man-In-The-Middle(MITM)

Kesuksesan pada serangan ini untuk penyerang pemula, MITM, untuk menyamarkan panggilan. Kemudian untuk informasi akan dilewati dari pemanggil pada penyerang dan sebaliknya. Kesuksesan serangan ini merupakan akses keseluruhan komunikasi panggilan.

Dan tujuan untuk menampilkan serangan MITM, penyerang harus dapat meyakinkan pemanggil bahwa Ialah yang dipanggil, begitupun sebaliknya. Penyerang dapat melakukan ini dengan tanda data valid. Data ini dapat digunakan pemanggil. Pemanggil harus juga dapat memblok semua tanda antara pemanggil dan yang dipanggil.

Saya mengeksplor scenario penyerangan tersebut.

1. Skenario mencegah pembentukan sesi tapi tidak menjajinkan pengkomunikasian yang terpercaya.
2. Skenario yang lain membutuhkan baik serangan fisik, hardware, mekanisme pengamanan software pada detil sebelum dilakukan pengkomputerisasian.
3. Skenario yang lain membutuhkan serangan pada pengamanan detil keduanya.

3.4.2 Penyerangan Balik

Sebuah serangan balik ditemukan untuk menyadarkan sebuah node untuk menyalakan sesi dengan penyerang yang dilakukan dengan membalikan data yang diambil oleh penyerang dari sesi sebelumnya diantara target dan node yang lain. Kemungkinan sesuksesan serangan balik termasuk menduplikat arus kunci yang digunakan sebelumnnya dan membloking sebuah node dari pengkomunikasian dengan klien yang lain.

Serangan tersebut dapat meneliti sebuah target node yang bertambah dengan cepat. Ini akan memberikan akses untuk menjumlahkan jawaban dan kemampuan. Penyerang kemudian dapat mengirim kemampuannya pada target dengan berpura-pura menjadi kejelasan yang sebelumnya. Target tersebut akan menjawab dengan kemampuannya sendiri. Jika kemampuan target diidentifikasikan pada satu penyerang yang telah diteliti sebelumnya untuk panggilan ini, penyerang tersebut kemudian dapat menjawab kemampuan mengulang dari klen merupakan sejumlah penelitian N dalam kemungkinan totalnya, N/2.

Bahkan jika kejadian ini tidak terjadi dengan semestinya, penyerang akan tetap tidak memiliki akses pada kunci AES kecuali kejadian tersebut terjadi dengan target memilih pada random yang sama 128 bit. Ini mungkin terjadi sekali setiap 2 percobaan, kemungkinan resiko hilang kecil.

3.4.3 Serangan Penebakan Password

Para pengguna dapat memilih untuk mengingat password skype dalam platform yang mereka gunakan. Sebagian besar pengguna memilih pilihan ini. Dalam platform windows, password diberikan pada system pengoperasian untuk melindungi dalam perlindungan windows crypprotect Data API. Seorang pengguna yang kemudian masuk pada windows dapat menggunakan skype tanpa posisi apapun. Sedikitnya pengguna yang tidak memilih untuk tidak mengingat password pada computer yang mereka gunakan harus login melalui client-server protocol sebelum mereka menggunakan skype. Untuk melindungi penebakan password pusat server skype terpaksa ‘timeout’ (kehabisan waktu) jika password salah beberapa kali.

3.4.4 Kelemahan Pengguna CRC

Tipe CRC checksums sering digunakan dalam pengkomunikasian protocol untuk pendeteksian kerusakan bit yang dapat dipercaya dan efisien. Bagaimanapun karena mereka seukuran, mereka

mungkin tidak cocok dalam perubahan tujuan pendeteksian data. Ini merupakan satu masalah yang ditemukan WEP, pengamanan protocol asli untuk IEEE 802. Beberapa aspek skype menggunakan checksum tipe CRC dalam cara yang menyerupai WEP dan dengan konsekuensi checksum beberapa kelemahan.
Masalah ini telah dilaporkan pada skype dan direncanakan untuk diperbaiki.

3.4.5 Serangan Sebelah-Channel

Amatlah terkenal bahwa implementasi pengoperasian cryptography terkadang memiliki keterbatasan informasi mengenai teks kosong atau kunci untuk membagi data klien skype membuat tidak adanya pertahanan pada serangan ini. Program bahaya tersebut dapat menyimpulkan tanda kunci pengguna pribadi. Program tersebut berbahaya jika dijalnkan pada platform yang sama dengan klien skype.

3.4.6 Penyerangan ASN1

Beberapa tahun yang lalu sebuah kelompok menyelesaikan penelitian di Universitas OULU ditemukan bermacam-macam bahaya pada sejumlah produk penjualan yang terkenal. Sumber yang umum pada kesulitan ini adalah produk ini tidak mampu memberi kode ASN1 dengan benar. Tidak mengherankan, masalah seperti itu dipindahtangankan pada penggunaan dari X509 SSL, sebaik protocol lain yang menunda cara skema data pengkodean.

Protocol skype tidak menggunakan ASN1 melainkan memperkerjakan sebuah mekanisme yang serupa dengan bergantung penuh pada kemampuannya dalam memberikan kode dengan benar. Dengan demikian pengkodean skype dengan benar amatlah penting. Saya melihat kembali dalam memasukan kode skype. Saya menemukan kemungkinan terjadinya kesalahan yang merupakan gabungan dengan pengkodean intergers. Kesalahan tersebut tidak membahayakan pengkomunikasian skype, tapi mungkin memimpin ketidakpastian perilaku dalam keberadaan input yang berbahaya. Saya mengkomunikasikan informasi ini pada mesin skype.

4. Kesimpulan

Dari analisa di atas dapat kita simpulkan hingga saat ini Skype masih bisa dibilang baik dalam penerapan konsep-konsep kriptografi dalam aplikasi ini karena didukung oleh penggunaan standar enkripsi yang paling popular dan bisa dibilang paling mutakhir yang sudah diakui saat ini paling tidak berdasarkan pengakuan para tim pengembang hingga 12 tahun ke depan. Disamping itu para pengguna justru dikhawatirkan oleh ketertutupan pihak Skype terhadap alogritma dan kode program mereka yang bisa saja di salah gunakan oleh pihak Skype untuk menyelipkan *spyware*, *malware*, dan berbagai aplikasi yang sangat merugikan para pengguna tanpa disadari kehadirannya. Dengan kata lain, penggunaan Skype terpaksa harus dilandasi oleh rasa kepercayaan yang tinggi.

DAFTAR PUSTAKA

[1] Daemen, Joan, Vincent Rijmen. (2004). The *Rijndael* Specification. *http://csrc.nist.gov/encryption/AES/Rijndael/Rijndael.pdf*. Tanggal akses: 20 Desember 2006 pukul 21:00.

[2] Munir, Rinaldi. (2006). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.

[3] *NIST*. (2006). National Institute of Standards and Technology. *http://www.nist.gov*. Tanggal akses: 20 Desember 2006 pukul 21:00.

[4] Skype Official Website. h*ttp://www.skype.com*. Tanggal akses: 20 Desember 2006 pukul 21:00.

[5] Skype Journal. *http://www.skypejournale.com*. Tanggal akses: 4 Oktober 2006 pukul 21:00.