Kajian Penggunaan Kriptografi 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

Makalah ini membahas mengenai pengimlementasian kriptografi pada program komunikasi *peer to peer* yang termasuk paling populer saat ini dengan pengguna mencapai jutaan orang di seluruh dunia. Oleh karena begitu besarnya komunitas ini makanya tingkat keamanan sistem juga harus diperkuat dengan berbagai konsep-konsep kriptografi untuk melindungi pengguna serta data yang berlalu lintas dalam jaringan Skype ini. Berdasarkan berbagai laporan evaluasi keamanan pada Skype ini kita bisa mengkaji konsep-konsep kriptografi yang bagaimana yang di implementasikan dalam Skype serta sejauh mana konsep tersebut dapat menjaga berbagai serangan yang dapat masuk ke dalam jaringan yang dapat mengganggu berbagai kepentingan pengguna. Berbagai serangan yang biasa terjadi dalam dunia kriptografi ikut di analisa untuk mencari celah dan kemungkinan di ekploitasinya celah tersebut oleh pihak-pihak yang biasa sangat fokus pada aksi pengayadapan seperti para intelejen. Di samping itu kita juga dapat mengkaji tingkat keamanan pada Skype ini menggunakan data-data hasil pengujian yang telah dilakukan oleh pihak-pihak yang diakui bersifat independen sehingga hasilnya benar-benar objektif. Selain itu juga ada beberapa masalah yang menyangkut kekhawatiran efek samping akibat ketertutupan algoritma dari Skype ini sehingga bukan tidak ada kemungkinan Skype bisa saja berisi aplikasi-aplikasi yang siap memata-mati para pengguna tanpa disadarinya.

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

1. Pendahuluan

Skype memakai kriptografi untuk otentifikasi *user* dan *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. Cita-cita menyediakan pengecekan validitas pengguna dan kepercayaan pada validitas data sudah tercapai.

Skype hanya menggunakan kriptografi standar yang primitive, dengan pendekatan *sound engineering*. Yang ini primitives memasukkan sandi rahasia blok AES, RAS kunci umum cryptosystem, ISO 9796-2 lapisan pengisi tanda-tangan siasat, SHA-1 ganja fungsi, dan RC4 kali sandi rahasia. Saya memandang pelaksanaan Skype masing-masing yang ini, dan dicek bahwa masing-masing pelaksanaan menyesuaikan diri sampai ukurannya dan interoperates dengan pelaksanaan surat keterangan.

Skype menjalankan seorang ahli surat keterangan untuk nama pemakai dan otorisasi.
Tanda-tangan digital yang diciptakan oleh kekuasaan ini adalah dasar untuk identias di Skype. Skype nodes masuk ke dalam sidang dengan benar mencek identias kawan sebaya mereka. Ialah infeasible bagi seorang penyerang untuk lelucon identias Skype di atau di bawah lapisan sidang. (saya tidak memeriksa kode lapisan yang lebih tinggi yang mana pun).

Skype memakai protokol pendirian sidang paten.
Cryptographic maksud protokol ini akan melindungi melawan permainan ulang, untuk mencek menatap identias, dan untuk membolehkan kawan sebaya berhubungan setuju di atas kunci sidang rahasia.
Kawan sebaya berhubungan kemudian mempergunakan kunci sidang mereka untuk mencapai komunikasi rahasia selama seumur hidup sidang.
Saya analyzed protokol ini, dan menemukan bahwa itu mencapainya cryptographic tujuan.
Lebih lanjut, saya menjelajahi kekuatan protokol terhadap tingkat nada beken menyerang, termasuk memainkan kembali menyerang dan laki-laki-di--tengah menyerang.
Saya gigih bahwa masing-masing skenario serangan ialah computationally infeasible.

1.1. Kebijakan Keamanan

A Security Policy menegaskan apa “security” berarti di konteks sistem dan membolehkan orangnya menjawab pertanyaan, “Is sistem ini aman?” A keamanan kebijakan adalah pertolongan luar biasa kepada perancang, implementers, operator, manajer, dan pemakai sistem. Skype Security Policy ialah:

1. Skype usernames unik.
2. Pemakai atau lamaran harus memperkenalkan Skype username dan surat kepercayaan pembuktiannya yang dihubungkan (E. G., kata teguran) sebelum mereka bergerak badan bahwa username’s identias atau hak istimewa.
3. Masing-masing kawan sebaya dengan benar menyediakan bukti untuk yang lainnya username dan hak istimewa setiap kali sidang Skype mapan. Masing-masing mencek other’s bukti di muka sidang dibolehkan memajukan pesan (E. G. , suara, video, berbaris, atau teks).
4. Pesan yang dikirimkan lewat sidang Skype disandikan dari Skype-akhir ke Skype-akhir. Tak ada perantara node, jika yang mana pun ada, mempunyai akses sampai bermaksud pesan ini.

2. Overview of Skype Cryptography

2.1. Pendaftaran

Yang pusat cryptographic rahasia di Skype adalah Server’s tengah pribadi menandatangani pokok, SS. The yang berhubungan verifikasi umum pokok, LAWAN, dan identifier untuk pasang pokok dilantik di setiap klien Skype di waktu tubuh.

Enrolment di Skype cryptosystem mulai dengan pendaftaran pemakai. Pemakai memilih mengingini username, menilpon itu, dan kata teguran, menilpon itu PA. The user’s pelanggan menyebabkan timbulnya pasang pokok RAS, (SA dan VA). Kunci menandatangani yang pribadi, SA, dan pergedel kata teguran, H (PA), disimpan seaman mungkin di panggung pemakai. (di panggung Jendela dilakukan ini memakai Windows CryptProtectData API).

Klien berikutnya memperlihatkan sidang sebanyak 256 bit yang disandikan oleh AES dengan Server Pusat. Kunci untuk sidang ini

terpilih oleh klien dengan bantuan pembangkit tenaga listrik jumlah acaknya yang panggung-spesifik. Kaleng pelanggan dan mencek bahwa benar-benar berbicara dengan server. Klien memberangkatkan server, di antara hal lain,, H (PA) dan VA.

The Central Server mengambil keputusan apakah unik, dan lain dapat diterima di bawah peraturan menamai Skype. Jika oleh sebab itu, toko server (A, H (H (PA))) di database. Membentuk dan menandatangani sehelai Surat Keterangan Identias untuk, ICA, yang berisi, di antara hal lain, Pusat Server's RAS tanda-tangan mengikat dan VA, {, VA} SS dan pokok identifier SS. ICA dikembalikan ke A.

Sebetulnya, diskusi di atas server menandatangani pokok adalah penyederhanaan untuk maksud kejernihan. Sebenarnya, ada dua Central Server pasang pokok, sesuatu dengan modulus 1536 bit dan yang lain dengan modulus 2048 sedikit. Pilihan di antaranya modulus untuk menggunakan dibuat oleh Juru Sita penting.
Bergantung di apakah pemakai mengikuti sudah membeli servis premi Skype yang mana pun, E. G. SkypeOut. Jika oleh sebab itu, yang lebih panjang modulus dipakai. Jika tidak, yang lebih pendek modulus dipakai. Seorang pemakai yang didaftarkan yang membeli servis premi untuk pertama kalinya akan dikeluarkan IC baru, yang ditandatangani dengan kunci yang lebih panjang.

Ada penyederhanaan lain yang berlangsung di diskusi di atas. Server Pusat sebenarnya terdiri atas sejumlah mesin dengan fungsi berbeda, termasuk satu mesin yang melakukan tak lain hanya surat keterangan tanda. Juga, polong Server penting seluruh ditiru beberapa kali lipat untuk kesinambungan kinerja dan perusahaan.

2.2. Peer-to-Peer Key Agreement

mengira sekarang seorang penelpon,, menginginkan untuk berhubungan dengan callee, B, dan tidak ada sidang pra-yang sudah ada Skype di antara mereka. Di kasus ini sidang baru didirikan dan diberikan pokok sidang sebanyak 256 bitnya sendiri, SKAB. This sidang akan ada begitu panjang sewaktu ada lalu-lintas di salah satu dari kedua jurusan di antara dan B, dan untuk suatu waktu tertentu afterward. Sesudah sesi selasai, Sk dipertahankan di kenangan sampai klien tertutup, ketika dinolkan.

Pendirian sidang terlebih dulu memerlukan mendirikan connectivity di antara dan B di seberang awan Skype. Memakai ini connectivity, dan B sekarang menyewa protokol persetujuan pokok selama, di antara hal lain, mereka memeriksa untuk kesegaran, mencek masing-masing other's identias, dan setuju di SKAB.

2.3. Session Cryptography

Semua lalu-lintas di sidang disandikan oleh XORing plaintext dengan pokok kali dihasilkan oleh sebanyak 256 bit AES (juga dikenal sebagai Rijndael) berlari di bilangan bulat membalas mode (ICM). Yang bekas yang pokok ialah saya sudah adalah seorang pemakai Skype sejak Agustus 2004. Karir 35 tahun saya sebagai cryptographer dan keamanan komputer ahli sudah mengajar saya untuk menjadi secara profesional skeptis tentang keamanan hampir segalanya, khususnya sistem yang sama mahirnya dengan Skype di berhasil mengatasi penjagaan jaringan khas. Oleh sebab itu saya mengganti format hard disk di atas komputer serep dan mempersembahkan kotak kepada lamaran Skype. Di balik yang berikutnya sedikit bulan saya mengamati daftar proses yang mengenai mesin, yang melihat untuk apa saja curiga. Saya juga mengadakan sejumlah eksperimen selama saya menangkap dan analyzed bongkos yang mengalir ke dalam dan dari kotak. Saya mencari aktivitas jahat dan mencoba memecahkan bagaimana Skype bekerja. Barangkali anda sudah mengadakan eksperimen mirip sendiri.

Nomor acak dipakai bagi beberapa cryptographic maksud dalam Skype, seperti perlindungan melawan serangan memainkan kembali, pembangkitan pasang pokok RAS, dan pembangkitan AES membagi dua pokok untuk kode rahasia puas.
Keamanan Skype P2P sidang bergantung penting pada kualitas nomor acak yang ditimbulkan oleh kawan sebaya berhubungan.

Pembangkitan jumlah acak berubah-ubah dari panggung ke panggung.
Sampai sejauh ini, saya sudah menilai pembangkitan jumlah acak hanya di panggung Jendela, di mana dilakukan dengan baik. Panggung dengan tenaga mengolah yang lebih terbatas atau lebih terbatas dalam negara bagian bisa diharapkan menantang lingkungan untuk pembangkitan jumlah acak, dan yang ini

mungkin baik secara produktif dinilai di masa mendatang.

Di Jendela yang membedah sistem panggung, Skype membuat Win32 menilpon sistem sampai sejumlah fungsi sistem menjalankan. Sedikit berkumpul dari menilpon ini, dengan suatu pelaut ulung, dikerjakan dengan saksama menggunakan SHA-1. Perintah tinggi sebanyak 64 bit hasil pergedel dikembalikan.

Penggunaan Skype standar cryptographic primitives untuk mencapai cita-cita keamanannya. Tidak ada kode rahasia paten di Skype, yang adalah latihan merencanakan yang baik. Standar primitives mempunyai keuntungan analisa dan evaluasi yang lalu dan terus-menerus di seluruh dunia. Cryptographic primitives dipakai di Skype ialah: sandi rahasia blok AES, RAS kunci umum cryptosystem, ISO 9796-2 lapisan pengisi tanda-tangan siasat, SHA-1 ganja fungsi, dan RC4 kali sandi rahasia.

Saya menilai Skype AES (memajukan Encryption Standard) kode di lingkungan sikap-sendiri.

Skype AES, di Integer Counter Mode (ICM), dipakai sebagai pembangkit tenaga listrik pokok untuk kode rahasia bongkos data. Penetral dengan plaintext (data bongkos) di semua tetapi dua byte terakhir disandikan sebagai berikut: kode Skype yang menguji untuk primality dan menyebabkan timbulnya pasang pokok kelihatannya dilaksanakan dengan benar. Penggunaan kode ganjil kekuasaan variasi standar segi empat-dan-secara lipat ganda algoritme untuk main modular exponentiation, dan juga menggunakan pintar menyelesaikan (yang mematikan jumlah pelaksanaan perkalian di separuh).Lagi, kode melaksanakan bagian-bagian kritis di bahasa perkumpulan di mana mungkin. Ini ialah panggung-tergantung.

Saya mematuhi kesempatan untuk memperbaiki efisiensi primality menguji, dan menceritakan ini kepada tim merencanakan Skype.

Algoritme untuk menghasilkan decryption eksponen (pribadi pokok) adalah variasi metode Montgomery yang dilaksanakan dengan benar modular pembalikan. Metode ini, walaupun memakai perhitungan ekstra, menghapuskan pembagian pemeriksaan pengadilan mahal yang diperlukan oleh metode Euclidian, dan mengganti pembagian biasa yang mahal dengan pembagian yang jauh lebih murahan di samping dua.

Beberapa metode bilangan bulat multi-ketepatan yang dipakai untuk perhitungan RAS menyediakan dan pasang pokok termasuk upacara kode untuk processor khas (LENGAN dan x86) untuk memperbaiki efisiensi.

Saya menguji pembangkitan pasang pokok, kode rahasia, dan decryption proses dan mengetahui bahwa mereka menyebabkan timbulnya hasil benar.

Kode lapisan pengisi tanda-tangan RAS tunduk dengan ISO 9796-2.

Untuk kargo yang lebih kecil, lapisan pengisi mengambil salah satu dari kedua formulir di bawah: kargo yang lebih Besar dibagai-bagi dan masing-masing bagian dilapisi di format berikut: metode verifikasi tanda-tangan memeriksa integritas pesan yang ditandatangani.
Decrypts RAS dan sari dan memeriksa lapisan pengisi. Juga memeriksa pergedel untuk ketepatan. Konsisten dengan ISO 9796-2, setelah blok pertama yang ditandatangani, sisa menandatangani pesan di plaintext, dan ini dicek via SHA-1 petak-petak pergedel.

Kode yang melaksanakan Algoritme Pergedel Aman (SHA-1), indah dan ketat. Sebenarnya, versi ini lebih mudah mengikuti daripada openssh sumber kode SHA-1 pelaksanaan.
Tidak ada ketidakseimbangan macam tampak yang mana pun, masalah penetral, dll.
Kode menyusun dengan bersih dengan tak ada peringatan.

Ada dua interfaces sampai fungsi pergedel.
Kedua yang diuji dengan tak ada masalah.
Skype SHA-1 kode benar. Memberikan vektor tesnya sendiri, dan vektor tes yang diterbitkan lain.Melewati Jim Gillogly’s kata berguling-lebih menguji. Saya menulis naskah untuk memeriksa Skype SHA-1 hasil terhadap Perl 's SHA-1 pelaksanaan untuk beberapa penetral yang dihasilkan secara acak yang besar.
Tidak ada dengan ganjil dikenali selama tes ini.

RC4 algoritme dipakai di Skype untuk menghasilkan diduga menyediakan bagi RSA.
The pelaksanaan RC4 standar. Initialization RC4 dengan sedikit bibit dan penggunaan acak RC4 pokok kali karena menyebabkan timbulnya kunci RAS adalah teknik yang dapat diterima.

Penggunaan mirip ditunjukkan oleh Microsoft di mereka CryptGenRandom () fungsi.

Persetujuan pokok tercapai memakai protokol paten. Saya membuat model resmi protokol, dan analyzed model untuk cacat protokoler. Saya juga dicek bahwa protokol dengan benar dilaksanakan di kode sumber.

Protokol ialah symmetric. Tak satu pun partai di keuntungan; masing-masing ialah equi-ampuh dan mendapat kepastian identik.

Untuk melindungi melawan memainkan kembali, kawan sebaya menantang satu sama lain dengan acak sebanyak 64 bit nonces, dan menjawab dengan membalas tantangan, yang diubah di cara standar, dan ditandatangani dengan responder's pribadi menandatangani pokok.

Untuk mendirikan identias, kawan sebaya tukar-menukar Surat Keterangan Identias mereka (ditandatangani oleh Juru Sita penting) dan mencek bahwa surat keterangan ini berlaku. Karena sehelai Surat Keterangan Identias berisi kunci umum, masing-masing kawan sebaya kemudian bisa mencek tanda-tangan yang terbentuk oleh partai yang lain.

Juga, masing-masing kawan sebaya bisa RAS-menyandikan pesan bagi partai yang lain sendiri. Masing-masing partai menyumbang 128 bit acak toward kunci sidang sebanyak 256 bit. Sumbangan tukar-ditukar sebagai tulisan rahasia RAS. Kedua sumbangan kemudian digabungkan di cryptographically-baik jauh untuk membentuk kunci sidang yang dibagikan.

Satu cara untuk memeriksa kekuatan protokol persetujuan pokok yang mana pun akan menjelajahi kemungkinan berbagai serangan padanya.Saya mempertimbangkan serangan melawan kejadian tunggal protokol, dan juga serangan terhadap lipat ganda kejadian bersamaan protokol.

Cita-cita di serangan ini bagi seorang penyerang perantara, MITM, untuk menirukan penelpon dan/atau callee kepada satu sama lain.
Lalu, informasi akan diberikan dari penelpon kepada penyerang ke callee dan sifat buruk versa. Cita-cita serangan ini adalah akses sampai komunikasi seluruh penelpon dan callee, sama baiknya dengan ketidaktahuan oleh penelpon dan callee bahwa mendengarkan secara diam-diam sudah terjadi.

Untuk melakukan serangan MITM, penyerang harus dapat meyakinkan penelpon bahwa dia callee (dan sifat buruk-versa). Penyerang bisa melakukan ini dengan sehelai surat keterangan yang ditandatangani yang berlaku yang menunjukkannya username callee (resp. Penelpon). Surat keterangan ini juga tidak bisa menjadi surat keterangan benar-benar bekas oleh callee (resp. Penelpon), atau sehelai surat keterangan yang ditempa. Penyerang juga harus dapat untuk menangkap dan/atau menghalangi semua lalu-lintas di antara penelpon dan callee.

Mengambil kemampuan ini, saya menjelajahi beberapa skenario serangan.

Serangan permainan ulang mencari untuk meyakinkan node untuk masuk ke dalam sidang dengan seorang penyerang dengan memainkan kembali data yang direbut oleh penyerang dari sidang sebelumnya antara sasaran dan lain node. Cita-cita mungkin permainan ulang menyerang termasuk menyalin kali pokok yang dipakai dulunya (yang mungkin memungkinkan pemecahan tulisan rahasia-di-dalam), dan menghalangi node dari berhubungan dengan tertentu lain pelanggan.

Pemakai harus pilih apakah ke "remember" kata teguran Skype mereka di panggung mereka sedang menggunakan. Kebanyakan pemakai memilih pilihan ini. Di panggung Jendela, kata teguran diberikan kepada sistem menjalankan untuk melindungi di bawah Jendela CryptProtectData API. seorang pemakai yang bisa nanti login ke Jendela bisa memakai Skype tanpa lebih lanjut memberikan surat kepercayaan yang mana pun.Minoritas pemakai yang pilih itu untuk tidak mengingat kata teguran mereka di atas komputer mereka sedang memakai keapakan login via protokol server pelanggan sebelum mereka bisa memakai Skype. Untuk melindungi terhadap mengira-ngirakan kata teguran atau serangan kamus, paksa Skype Central Server timeout setelah rentetan kata teguran salah.

CRC-macam checksums secara umum dipergunakan di protokol komunikasi untuk dengan dapat diandalkan dan efisien mengetahui kesalahan sedikit. Tetapi, karena mereka linear, mereka mungkin tak cocok agar mengetahui modifikasi disengaja data. Ini adalah satu masalah yang ditemukan di WEP, protokol

keamanan asli bagi IEEE 802.11 tanpa kawat LANs. Beberapa aspek Skype memakai CRC macam checksums di cara mirip WEP dan karenanya dengan beberapa kelemahan sama.

Masalah ini sudah dilaporkan kepada Skype dan dijadwalkan untuk diperbaiki di upcoming melepaskan.

Sedikit tahun yang lalu, sekelompok peneliti Finlandia di Oulu University menemukan jenis keringkihan yang mungkin berbahaya di agen SNMP sejumlah menonjol vendor's produk. Sumber kesukaran ini yang paling kebanyakan di yang ini products' ketidakmampuan untuk dengan selamat dan benar menguraikan ASN1 menyandikan kargo. Tidak secara mengherankan, masalah seperti itu tertunda ke SSL's penggunaan X509 surat keterangan, serta yang dipunyai protokol lain yang mengandalkan suatu cara siasat menyandikan itu.

Protokol Skype tidak menggunakan ASN1, tetapi mereka menggunakan mekanisme mirip dan mengandalkan dengan berat kemampuan mereka untuk dengan benar menguraikan kargo yang disandikan. Dimasukkan di kargo ini adalah bidang yang seorang penyerang mungkin terbenam sampai hampir nilai yang mana pun. Oleh sebab itu penting sekali bahwa kode Skype yang menguraikan kargo ini benar. Saya memeriksa kargo Skype yang menguraikan kode. Saya merasa kesalahan mungkin dihubungkan dengan menguraikan kode bilangan bulat. Kesalahan tidak membahayakan confidentiality komunikasi Skype, tetapi mungkin memimpin ke tak bisa ditebak kelakuan di adanya masukan jahat. Saya menceritakan informasi ini sampai teknik Skype.

Saya mulai sebagai orang skeptis.
Saya berpikir sistem akan mudah untuk mengalahkan. Tetapi, keyakinan saya di Skype bertambah sehari-hari. Lebih banyak saya menemukan ke luar tentang itu, lebih banyak saya suka.

Di 1998 saya mengamati dari mahal ke murah, dari arcane ke biasa, dari sulit ke mudah, dari jarang ke berlimpah. Kolega saya dan saya mencoba meramalkan perbedaan yang mana, jika yang mana pun, ilmu pembacaan sandi berlimpah mungkin membuat di dunia.
Bentuk baru teknik yang mana, bisnis, ilmu ekonomi, atau masyarakat akan mungkin?

Kami tidak meramalkan Skype. Tetapi, sejak saya sadar kembali mengenalnya dengan baik, saya mengaku bahwa Skype adalah contoh awal ilmu pembacaan sandi berlimpah yang mana bisa mengalah.

Perancang Skype tidak ragu-ragu untuk menggunakan ilmu pembacaan sandi secara luas dan baik untuk mendirikan yayasan kepercayaan, keaslian, dan confidentiality untuk mereka kawan sebaya-ke-menatap servis. Implementers Skype melaksanakan cryptographic fungsi dengan benar dan efisien. Akibatnya, confidentiality sidang Skype jauh lebih hebat daripada itu ditawari oleh menelegram atau telepon radio menilpon atau di samping lampiran email dan email.

Kesalahan alam baka di cryptosystem, saya juga sudah mencari pintu punggung, Trojans, melampaui batas "debugging" fasilitas, dll. Saya tidak menemukan petunjuk yang mana pun malware di bagian-bagian kode Skype saya meninjau kembali.

Kebijakan Keamanan menegaskan apa "security" berarti di konteks sistem dan membolehkan orangnya menjawab pertanyaan, "Is sistem ini aman?" A keamanan kebijakan adalah pertolongan luar biasa kepada perancang, implementers, operator, manajer, dan pemakai sistem. Skype Security Policy ialah: kode dengan benar melaksanakan AES yang memakai ukuran blok sebanyak 128 bit dan ukuran pokok sebanyak 256 bit. Standar AES-256 vektor tes dan kunci dibandingkan dengan pertandingan Skype AES. Skype AES hasil yang dihasilkan oleh pelaksanaan lain. Skype menaruh berarti usaha ke dalam membuat Skype AES dikelola dengan cepat. Ialah optimized untuk Integer Counter Mode. Menggunakan macros untuk mempercepatkan perbuatan. Saya membandingkan Skype AES kode ke dua lain optimized C/C++ pelaksanaan. Skype menyandikan fungsi main secara mendukung di syarat-syarat putaran jam per kode rahasia.

1. Skype usernames unik.
2. Pemakai atau lamaran harus memperkenalkan Skype username dan surat kepercayaan pembuktiannya yang dihubungkan (, kata teguran) sebelum mereka bergerak badan bahwa username's identias atau hak istimewa.
3. Masing-masing kawan sebaya dengan benar menyediakan bukti untuk yang lainnya username dan hak istimewa setiap kali

sidang Skype mapan. Masing-masing mencek other's bukti di muka sidang dibolehkan memajukan pesan (, suara, video, berbaris, atau teks).

4. Pesan yang dikirimkan lewat sidang Skype disandikan dari Skype-akhir ke Skype-akhir. Tak ada perantara node, jika yang mana pun ada, mempunyai akses sampai bermaksud pesan ini.

Yang pusat cryptographic rahasia di Skype adalah Server's tengah pribadi menandatangani pokok, S. Kunci verifikasi umum yang mengurus surat-menyurat, V, dan identifier untuk pasang pokok dilantik di setiap klien Skype di waktu tubuh. Enrolment di Skype cryptosystem mulai dengan pendaftaran pemakai. Pemakai memilih mengingini username, menilpon itu, dan kata teguran, menilpon itu P. User's pelanggan menyebabkan timbulnya pasang pokok RAS, (S dan V). Kunci menandatangani yang pribadi, S, dan pergedel kata teguran, H (P), disimpan seaman mungkin di panggung pemakai. (di panggung Jendela dilakukan ini memakai Windows CryptProtectData API). Klien berikutnya memperlihatkan sidang sebanyak 256 bit yang disandikan oleh AES dengan Server Pusat. Kunci untuk sidang ini terpilih oleh klien dengan bantuan pembangkit tenaga listrik jumlah acaknya yang panggung-spesifik. Kaleng pelanggan dan mencek bahwa benar-benar berbicara dengan server. Klien memberangkatkan server, di antara hal lain, H (P) dan V.

Server Pusat mengambil keputusan apakah unik, dan lain dapat diterima di bawah peraturan menamai Skype. Jika oleh sebab itu, toko server (A, H (H (P))) di database. Membentuk dan menandatangani sehelai Surat Keterangan Identias untuk, IC, yang berisi, di antara hal lain, Pusat Server's RAS tanda-tangan mengikat dan V, {, V} dan pokok identifier S. IC dikembalikan kepada A.

Actually, diskusi di atas server menandatangani pokok adalah penyederhanaan untuk maksud kejernihan. Sebenarnya, ada dua Central Server pasang pokok, sesuatu dengan modulus 1536 bit dan yang lain dengan modulus 2048 sedikit. Pilihan di antaranya modulus untuk menggunakan dibuat oleh Juru Sita penting. Bergantung di apakah pemakai mengikuti sudah membeli servis premi Skype yang mana pun.

SkypeOut.

Jika oleh sebab itu, yang lebih panjang modulus dipakai. Jika tidak, yang lebih pendek modulus dipakai. Seorang pemakai yang didaftarkan yang membeli servis premi untuk pertama kalinya akan dikeluarkan IC baru, yang ditandatangani dengan kunci yang lebih panjang.Kira sekarang seorang penelpon,, menginginkan untuk berhubungan dengan callee, B, dan tidak ada sidang pra-yang sudah ada Skype di antara mereka.Di kasus ini sidang baru didirikan dan diberikan pokok sidang sebanyak 256 bitnya sendiri, SK.

Sidang ini akan ada begitu panjang sewaktu ada lalu-lintas di salah satu dari kedua jurusan di antara dan B, dan untuk suatu waktu tertentu afterward. Sesudah sesi selasai, Sk dipertahankan di kenangan sampai klien tertutup, ketika dinolkan.Pendirian sidang terlebih dulu memerlukan mendirikan connectivity di antara dan B di seberang awan Skype.
Memakai ini connectivity, dan B sekarang menyewa protokol persetujuan pokok selama, di antara hal lain, mereka memeriksa untuk kesegaran, mencek masing-masing other's identias, dan setuju di SK
.
Prosedur ini berhasil membuat lipatan pada cukup entropy untuk membalas 64 bit.
Entropy mengumpul dan membaur sedikit mengikuti latihan yang dianjurkan yang standar setergambar di RFC 1750.Metode ialah juga sangat mirip Microsoft CryptoAPI fungsi, CryptGenRandom, yang tergambar di, 2nd Edition, Microsoft Press, pp. 262-269. Tes Penggiling-Rabin di kode pembangkitan bilangan prima termasuk semua kondisi tes perlu Miller-Rabin. Jumlah kelalaian iterations (25) dimasukkan di buatan tes kesempatan salah mengenali jumlah kombinasi seterbaik teramat rendah (kemungkinan < 10). Malah 5 Miller-Rabin iterations akan mengalah kemungkinan = 0,00063 menyetujui jumlah kombinasi.
Ini masih adalah nilai yang dapat diterima dan mengurangi waktu untuk menghasilkan menyediakan di atas mesin pelanggan dengan kecepatan processor terbatas

- Satu skenario mencegah sidang diperlihatkan, tetapi tidak berkompromi confidentiality komunikasi.

- Dua skenario lain menghendaki baik kekalahan dari yang fisik, perangkat keras, dan mekanisme keamanan perangkat halus di seorang kawan

sebaya mengambil bagian atau infeasible pre-perhitungan. Dengan persiapan itu, dua skenario ini kemudian memerlukan beberapa menangkap mengikui menjelang sedetik infeasible post-perhitungan. Jika bisa dilakukan seluruh itu, penyerang bisa berkompromi keamanan tunggal menatap-ke-menatap sidang.

- Skenario lain menghendaki kekalahan dari keamanan di kedua kawan sebaya. Di kasus ini, semua sidang antara pasang kawan sebaya itu bisa dibahayakan.

- Skenario terakhir menghendaki kekalahan dari mekanisme keamanan di Skype Central Server.
- Sewaktu saya menjelaskan di atas, surat keterangan digital yang diciptakan oleh kekuasaan surat keterangan adalah dasar untuk identias di Skype.

Penyerang bisa mematuhi jabatan tangan lipat ganda yang memerlukan sasaran node.
Ini akan memberikan akses kepada tantangan dan jawaban lipat ganda. Penyerang lalu bisa memberangkatkan tantangan sampai sasaran yang berpura-pura menjadi seorang kawan sebaya sebelumnya. Sasaran akan menjawab dengan tantangannya sendiri. Jika tantangan sasaran identik dengan yang sudah dilihat oleh penyerang bagi penelpon ini, penyerang kemudian bisa menjawab tantangan dengan benar dan maju sampai aspek berikutnya protokol penukaran pokok. Tetapi, karena tantangan adalah 64 bit panjang dan dipilih sekenanya, kemungkinan kejadian ini rendah. Kesempatan mendapat pengulangan tantangan dari klien ialah, di kasus sedikit pengamatan, jumlah pengamatan N lebih jumlah kemungkinan, N/2.

Sekalipun peristiwa ini yang tak mungkin terjadi, penyerang masih belum akan mempunyai akses ke kunci AES kecuali kalau peristiwa yang masih lebih tak mungkin terjadi bahwa sasaran memilih sekenanya sumbangan pokok sebanyak 128 bit yang sama sewaktu pilih selama sesi yang direkam oleh penyerang. Ini mungkin terjadi satu kali setiap 2 berusaha, kemungkinan rendah yang lenyap. Dan ini pun adalah pernyataan yang berlebih-lebihan karena tidak mempertimbangkan efek bermanfaat menggarami toonbank Sama Sekali lalu-lintas di sidang disandikan oleh XORing plaintext dengan pokok kali dihasilkan oleh sebanyak 256 bit AES (juga dikenal sebagai Rijndael) berlari di bilangan bulat membalas mode (ICM). Yang bekas yang pokok adalah SK. Sidang Skype berisi kali lipat ganda. Toonbank ICM bergantung pada kali, pada garam, dan sequency dalam kali.

Tenar bahwa pelaksanaan cryptographic pelaksanaan kadang-kadang mungkin meniriskan informasi tentang plaintext atau kunci lewat konsumsi mereka sumber penghasilan yang dibagikan, seperti penyimpanan, waktu CPU atau tenaga. Klien Skype tidak menjadi bek melawan serangan seperti ini. Oleh sebab itu, misalnya, jika program jahat sedang mengenai panggung sama sebagai seorang klien Skype, program jahat itu mungkin dapat memancing sedikit user’s pribadi menandatangani pokok. Ini akhirnya akan membolehkan pemilik program jahat menyamar sebagai pemakai. Saya menganggap ini sebagai masalah kecil, karena berlari program jahat di panggung sama sebagai seorang klien Skype bisa melakukan banyak kerusakan yang lebih luar biasa secara langsung. Sidang SKAB. Skype berisi kali lipat ganda. Toonbank ICM bergantung pada kali, pada garam, dan sequency dalam kali.

3. Detail Kriptografi Skype

3.1. Pembangkitan Bilangan Acak

Random nomor dipakai bagi beberapa cryptographic maksud dalam Skype, seperti perlindungan melawan serangan memainkan kembali, pembangkitan pasang pokok RAS, dan pembangkitan AES membagi dua pokok untuk kode rahasia puas.Keamanan Skype P2P sidang bergantung penting pada kualitas nomor acak yang ditimbulkan oleh kawan sebaya berhubungan.

Pembangkitan jumlah acak berubah-ubah dari panggung ke panggung. Sampai sejauh ini, saya sudah menilai pembangkitan jumlah acak hanya di panggung Jendela, di mana dilakukan dengan baik. Panggung dengan tenaga mengolah yang lebih terbatas atau lebih terbatas dalam negara bagian bisa diharapkan menantang lingkungan untuk pembangkitan jumlah acak, dan yang ini mungkin baik secara produktif dinilai di masa mendatang.

Di Jendela yang membedah sistem panggung, Skype membuat Win32 menilpon sistem sampai sejumlah fungsi sistem menjalankan. Sedikit berkumpul dari menilpon ini, dengan suatu pelaut ulung, dikerjakan dengan saksama menggunakan SHA-1. Perintah tinggi sebanyak 64 bit hasil pergedel dikembalikan.

Prosedur ini berhasil membuat lipatan pada cukup entropy untuk membalas 64 bit. Entropy mengumpul dan membaur sedikit mengikuti latihan yang dianjurkan yang standar setergambar di RFC 1750. Metode ialah juga sangat mirip Microsoft CryptoAPI fungsi, CryptGenRandom, yang tergambar dalam menulis Secure Code, 2nd Edition, Microsoft Press, pp. 262-269.

3.2. Cryptographic primitives

Skype menggunakan standar cryptographic primitives untuk mencapai cita-cita keamanannya. Tidak ada kode rahasia paten di Skype, yang adalah latihan merencanakan yang baik. Standar primitives mempunyai keuntungan analisa dan evaluasi yang lalu dan terus-menerus di seluruh dunia.

Cryptographic primitives dipakai di Skype ialah: sandi rahasia blok AES, RAS kunci umum cryptosystem, ISO 9796-2 lapisan pengisi tanda-tangan siasat, SHA-1 ganja fungsi, dan RC4 kali sandi rahasia.

3.2.1. AES

I menilai Skype AES (memajukan Encryption Standard) kode di lingkungan sikap-sendiri.

Kode dengan benar melaksanakan AES yang memakai ukuran blok sebanyak 128 bit dan ukuran pokok sebanyak 256 bit. Standar AES-256 vektor tes dan kunci dibandingkan dengan pertandingan Skype AES. Skype AES hasil yang dihasilkan oleh pelaksanaan lain. Skype menaruh berarti usaha ke dalam membuat Skype AES dikelola dengan cepat. Ialah optimized untuk Integer Counter Mode. Menggunakan macros untuk mempercepatkan perbuatan. Saya membandingkan Skype AES kode ke dua lain optimized C/C++ pelaksanaan. Skype menyandikan fungsi main secara mendukung di syarat-syarat putaran jam per kode rahasia.

Skype AES, di Integer Counter Mode (ICM), dipakai sebagai pembangkit tenaga listrik pokok untuk kode rahasia bongkos data. Penetral dengan plaintext (data bongkos) di semua tetapi dua byte terakhir disandikan sebagai berikut:

A. Successive blok plaintext ialah XORed ke blok sandi rahasia AES. Yang terakhir ditimbulkan memakai kunci yang didirikan untuk sidang. Masukan (membalas) blok adalah rentetan garam: garam: packet index: block# The packet index adalah nilai sebanyak 48 bit dan block# adalah nilai sebanyak 16 bit.
B. A CRC diperhitungkan di atas isi penetral yang disandikan. Mod 2 jumlah CRC dengan perintah rendah 2 byte packet index disimpan di 2 byte terakhir penetral.
C. Note: Hanya sedikit perintah rendah toonbank AES berganti dari menghalangi untuk menghalangi sedangkan menyandikan penetral.Indeks bongkos berganti dari penetral untuk menahan. Garam disumbang oleh masing-masing kawan sebaya dan adalah nilai acak.

3.2.2. RSA

The Skype kode yang menguji untuk primality dan menyebabkan timbulnya pasang pokok kelihatannya dilaksanakan dengan benar. Penggunaan kode ganjil kekuasaan variasi standar segi empat-dan-secara lipat ganda algoritme untuk main modular exponentiation, dan juga menggunakan pintar menyelesaikan (yang mematikan jumlah pelaksanaan perkalian di separuh).Lagi, kode melaksanakan bagian-bagian kritis di bahasa perkumpulan di mana mungkin. Ini ialah panggung-tergantung.

Tes Penggiling-Rabin di kode pembangkitan bilangan prima termasuk semua kondisi tes perlu Miller-Rabin. Jumlah kelalaian iterations (25) dimasukkan di buatan tes kesempatan salah mengenali jumlah kombinasi seterbaik teramat rendah (kemungkinan < 10-16). Malah 5 Miller-Rabin iterations akan mengalah kemungkinan = 0,00063 menyetujui jumlah kombinasi.
Ini masih adalah nilai yang dapat diterima dan mengurangi waktu untuk menghasilkan menyediakan di atas mesin pelanggan dengan kecepatan processor terbatas saya mematuhi kesempatan untuk memperbaiki efisiensi primality menguji, dan menceritakan ini kepada tim merencanakan Skype.

Algoritme untuk menghasilkan decryption eksponen (pribadi pokok) adalah variasi metode Montgomery yang dilaksanakan dengan benar modular pembalikan. Metode ini, walaupun memakai perhitungan ekstra, menghapuskan pembagian pemeriksaan pengadilan mahal yang diperlukan oleh metode Euclidian, dan mengganti pembagian biasa yang mahal dengan pembagian yang jauh lebih murahan di samping dua.

Beberapa metode bilangan bulat multi-ketepatan yang dipakai untuk perhitungan RAS menyediakan dan pasang pokok termasuk upacara kode untuk processor khas (LENGAN dan x86) untuk memperbaiki efisiensi.

Saya menguji pembangkitan pasang pokok, kode rahasia, dan decryption proses dan mengetahui bahwa mereka menyebabkan timbulnya hasil benar.

3.2.3. *Signature padding*

kode lapisan pengisi tanda-tangan RAS tunduk dengan ISO 9796-2. Untuk kargo yang lebih kecil, lapisan pengisi mengambil salah satu dari kedua formulir di bawah:

4A < data > BC 4B BB…..
BA < data > BC

Larger kargo dibagai-bagi dan masing-masing bagian dilapisi di format berikut:

6A < data memihak > BC

metode verifikasi tanda-tangan memeriksa integritas pesan yang ditandatangani. Decrypts RAS dan sari dan memeriksa lapisan pengisi. Juga memeriksa pergedel untuk ketepatan. Konsisten dengan ISO 9796-2, setelah blok pertama yang ditandatangani, sisa menandatangani pesan di plaintext, dan ini dicek via SHA-1 petak-petak pergedel.

3.2.4. SHA-1

kode yang melaksanakan Algoritme Pergedel Aman (SHA-1), indah dan ketat. Sebenarnya, versi ini lebih mudah mengikuti daripada openssh sumber kode SHA-1 pelaksanaan. Tidak ada ketidakseimbangan macam tampak yang mana pun, masalah penetral, dll. Kode menyusun dengan bersih dengan tak ada peringatan.

Ada dua interfaces sampai fungsi pergedel. Kedua yang diuji dengan tak ada masalah. Skype SHA-1 kode benar. Memberikan vektor tesnya sendiri, dan vektor tes yang diterbitkan lain. Melewati Jim Gillogly's kata berguling-lebih menguji. Saya menulis naskah untuk memeriksa Skype SHA-1 hasil terhadap Perl 's SHA-1 pelaksanaan untuk beberapa penetral yang dihasilkan secara acak yang besar. Tidak ada dengan ganjil dikenali selama tes ini.

3.2.5. RC4

RC4 algoritme dipakai di Skype untuk menghasilkan diduga menyediakan bagi RSA. The pelaksanaan RC4 standar. Initialization RC4 dengan sedikit bibit dan penggunaan acak RC4 pokok kali karena menyebabkan timbulnya kunci RAS adalah teknik yang dapat diterima. Penggunaan mirip ditunjukkan oleh Microsoft di mereka CryptGenRandom () fungsi.

3.3. Peer-to-Peer Key Agreement Protocol

Protokoler persetujuan Pokok tercapai memakai protokol paten. Saya membuat model resmi protokol, dan analyzed model untuk cacat protokoler. Saya juga dicek bahwa protokol dengan benar dilaksanakan di kode sumber.

Protokol ialah symmetric. Tak satu pun partai di keuntungan; masing-masing ialah equi-ampuh dan mendapat kepastian identik.

Untuk melindungi melawan memainkan kembali, kawan sebaya menantang satu sama lain dengan acak sebanyak 64 bit nonces, dan menjawab dengan membalas tantangan, yang diubah di cara standar, dan ditandatangani dengan responder's pribadi menandatangani pokok.

Untuk mendirikan identias, kawan sebaya tukar-menukar Surat Keterangan Identias mereka (ditandatangani oleh Juru Sita penting) dan mencek bahwa surat keterangan ini berlaku. Karena sehelai Surat Keterangan Identias berisi kunci umum, masing-masing kawan sebaya kemudian bisa mencek tanda-tangan yang terbentuk oleh partai yang lain.
Juga, masing-masing kawan sebaya bisa RAS-menyandikan pesan bagi partai yang lain sendiri.

Masing-masing partai menyumbang 128 bit acak toward kunci sidang sebanyak 256 bit.

Sumbangan tukar-ditukar sebagai tulisan rahasia RAS. Kedua sumbangan kemudian digabungkan di cryptographically-baik jauh untuk membentuk kunci sidang yang dibagikan.

3.4. Serangan di Skype Key Agreement Protocol

One jauh untuk memeriksa kekuatan protokol persetujuan pokok yang mana pun akan menjelajahi kemungkinan berbagai serangan padanya. Saya mempertimbangkan serangan melawan kejadian tunggal protokol, dan juga serangan terhadap lipat ganda kejadian bersamaan protokol.

3.4.1. Man-in-The-Middle(MITM)

memecahkan cita-cita di serangan ini bagi seorang penyerang perantara, MITM, untuk menirukan penelpon dan/atau callee kepada satu sama lain. Lalu, informasi akan diberikan dari penelpon kepada penyerang ke callee dan sifat buruk versa. Cita-cita serangan ini adalah akses sampai komunikasi seluruh penelpon dan callee, sama baiknya dengan ketidaktahuan oleh penelpon dan callee bahwa mendengarkan secara diam-diam sudah terjadi.

Untuk melakukan serangan MITM, penyerang harus dapat meyakinkan penelpon bahwa dia callee (dan sifat buruk-versa). Penyerang bisa melakukan ini dengan sehelai surat keterangan yang ditandatangani yang berlaku yang menunjukkannya username callee (resp. Penelpon). Surat keterangan ini juga tidak bisa menjadi surat keterangan benar-benar bekas oleh callee (resp. Penelpon), atau sehelai surat keterangan yang ditempa. Penyerang juga harus dapat untuk menangkap dan/atau menghalangi semua lalu-lintas di antara penelpon dan callee.

Mengambil kemampuan ini, saya menjelajahi beberapa skenario serangan.

- Satu skenario mencegah sidang diperlihatkan, tetapi tidak berkompromi confidentiality komunikasi.
- Two skenario lain menghendaki baik kekalahan dari yang fisik, perangkat keras, dan mekanisme keamanan perangkat halus di seorang kawan sebaya mengambil bagian atau infeasible pre-perhitungan. Dengan persiapan itu, dua skenario ini kemudian memerlukan beberapa menangkap mengikui menjelang sedetik infeasible post-perhitungan.Jika bisa dilakukan seluruh itu, penyerang bisa berkompromi keamanan tunggal menatap-ke-menatap sidang.
- skenario Lain menghendaki kekalahan dari keamanan di kedua kawan sebaya. Di kasus ini, semua sidang antara pasang kawan sebaya itu bisa dibahayakan.
- A terakhir skenario menghendaki kekalahan dari mekanisme keamanan di Skype Central Server.Sewaktu saya menjelaskan di atas, surat keterangan digital yang diciptakan oleh kekuasaan surat keterangan adalah dasar untuk identias di Skype.

3.4.2. Playback Attack

A serangan permainan ulang mencari untuk meyakinkan node untuk masuk ke dalam sidang dengan seorang penyerang dengan memainkan kembali data yang direbut oleh penyerang dari sidang sebelumnya antara sasaran dan lain node. Cita-cita mungkin permainan ulang menyerang termasuk menyalin kali pokok yang dipakai dulunya (yang mungkin memungkinkan pemecahan tulisan rahasia-di-dalam), dan menghalangi node dari berhubungan dengan tertentu lain pelanggan.

Penyerang bisa mematuhi jabatan tangan lipat ganda yang memerlukan sasaran node.
Ini akan memberikan akses kepada tantangan dan jawaban lipat ganda. Penyerang lalu bisa memberangkatkan tantangan sampai sasaran yang berpura-pura menjadi seorang kawan sebaya sebelumnya. Sasaran akan menjawab dengan tantangannya sendiri. Jika tantangan sasaran identik dengan yang sudah dilihat oleh penyerang bagi penelpon ini, penyerang kemudian bisa menjawab tantangan dengan benar dan maju sampai aspek berikutnya protokol penukaran pokok. Tetapi, karena tantangan adalah 64 bit panjang dan dipilih sekenanya, kemungkinan kejadian ini rendah. Kesempatan mendapat pengulangan tantangan dari klien ialah, di kasus sedikit pengamatan, jumlah pengamatan N lebih jumlah kemungkinan, $N/2^{64}$.

Sekalipun peristiwa ini yang tak mungkin terjadi, penyerang masih belum akan mempunyai akses ke kunci AES kecuali kalau peristiwa yang masih lebih tak mungkin terjadi bahwa sasaran

memilih sekenanya sumbangan pokok sebanyak 128 bit yang sama sewaktu pilih selama sesi yang direkam oleh penyerang. Ini mungkin terjadi satu kali tiap 2128 usaha, kemungkinan rendah yang lenyap. Dan ini pun adalah pernyataan yang berlebih-lebihan karena tidak mempertimbangkan efek bermanfaat menggarami toonbank

3.4.3. Password Guessing Attack

Users harus pilih apakah ke “remember” kata teguran Skype mereka di panggung mereka sedang menggunakan. Kebanyakan pemakai memilih pilihan ini. Di panggung Jendela, kata teguran diberikan kepada sistem menjalankan untuk melindungi di bawah Jendela CryptProtectData API. seorang pemakai yang bisa nanti login ke Jendela bisa memakai Skype tanpa lebih lanjut memberikan surat kepercayaan yang mana pun. Minoritas pemakai yang pilih itu untuk tidak mengingat kata teguran mereka di atas komputer mereka sedang memakai keapakan login via protokol server pelanggan sebelum mereka bisa memakai Skype. Untuk melindungi terhadap mengira-ngirakan kata teguran atau serangan kamus, paksa Skype Central Server timeout setelah rentetan kata teguran salah.

3.4.4. Kelemahan penggunaan CRC

CRC-macam checksums secara umum dipergunakan di protokol komunikasi untuk dengan dapat diandalkan dan efisien mengetahui kesalahan sedikit. Tetapi, karena mereka linear, mereka mungkin tak cocok agar mengetahui modifikasi disengaja data. Ini adalah satu masalah yang ditemukan di WEP, protokol keamanan asli bagi IEEE 802.11 tanpa kawat LANs. Beberapa aspek Skype memakai CRC macam checksums di cara mirip WEP dan karenanya dengan beberapa kelemahan sama. Masalah ini sudah dilaporkan kepada Skype dan dijadwalkan untuk diperbaiki di upcoming melepaskan.

3.4.5. Serangan *Side-Channel*

tenar bahwa pelaksanaan cryptographic pelaksanaan kadang-kadang mungkin meniriskan informasi tentang plaintext atau kunci lewat konsumsi mereka sumber penghasilan yang dibagikan, seperti penyimpanan, waktu CPU atau tenaga. Klien Skype tidak menjadi bek melawan serangan seperti ini. Oleh sebab itu, misalnya, jika program jahat sedang mengenai panggung sama sebagai seorang klien Skype, program jahat itu mungkin dapat memancing sedikit user’s pribadi menandatangani pokok. Ini akhirnya akan membolehkan pemilik program jahat menyamar sebagai pemakai. Saya menganggap ini sebagai masalah kecil, karena berlari program jahat di panggung sama sebagai seorang klien Skype bisa melakukan banyak kerusakan yang lebih luar biasa secara langsung.

3.4.6. ASN1 Attack

A Few tahun-tahun yang lalu, sekelompok peneliti Finlandia di Oulu University menemukan jenis keringkihan yang mungkin berbahaya di agen SNMP sejumlah menonjol vendor’s produk. Sumber kesukaran ini yang paling kebanyakan di yang ini products’ ketidakmampuan untuk dengan selamat dan benar menguraikan ASN1 menyandikan kargo. Tidak secara mengherankan, masalah seperti itu tertunda ke SSL’s penggunaan X509 surat keterangan, serta yang dipunyai protokol lain yang mengandalkan suatu cara siasat menyandikan itu.

Protokol Skype tidak menggunakan ASN1, tetapi mereka menggunakan mekanisme mirip dan mengandalkan dengan berat kemampuan mereka untuk dengan benar menguraikan kargo yang disandikan. Dimasukkan di kargo ini adalah bidang yang seorang penyerang mungkin terbenam sampai hampir nilai yang mana pun. Oleh sebab itu penting sekali bahwa kode Skype yang menguraikan kargo ini benar.
Saya memeriksa kargo Skype yang menguraikan kode. Saya merasa kesalahan mungkin dihubungkan dengan menguraikan kode bilangan bulat. Kesalahan tidak membahayakan confidentiality komunikasi Skype, tetapi mungkin memimpin ke tak bisa ditebak kelakuan di adanya masukan jahat. Saya menceritakan informasi ini sampai teknik 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 dank ode 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: 4 Oktober 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: 4 Oktober 2006 pukul 21:00.

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

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