Studi dan implementasi tanda tangan digital untuk mendeteksi serangan pada data link layer IEEE 802.3

Catur Wirawan Wijiutomo– NIM : 13505020
Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if15020@students.if.itb.ac.id

Abstrak
makalah ini membahas mengenai studi teknik tanda tangan digital dan algoritma-algoritma kriptografi yang dipergunakannya. Selain itu teknik tanda-tangan digital ini akan dipergunakan untuk melakukan deteksi serangan pada jaringan. Dua hal ini dicoba untuk digabungkan dengan alasan teknik tanda tangan digital dapat dipergunakan untuk melakukan verifikasi. Hal ini dapat digunakan untuk memberikan keamanan pada protokol data link layer IEEE 802.3 yang memiliki protokol yang nir-authentifikasi. Penggunaan teknik tanda tangan digital ditujukan untuk memberikan suatu fitur authentifikasi dan verifikasi.

Jaringan komputer saat ini bermula dari jaringan komputer sederhana untuk menghubungkan antar civitas akademis. saat ini jaringan komputer telah menghubungkan banyak orang di seluruh dunia dan menjelma menjadi sesuatu yang kita sebut internet. Berita buruk bagai para pengguna internet adalah protokol dasar yang digunakan di internet merupakan protokol yang sama dengan yang digunakan untuk menghubungkan jaringan yang dijalankan atas dasar saling percaya. Padahal diketahui dengan banyak orang yang memanfaatkan internet ada kemungkinan internet digunakan tidak hanya untuk tujuan baik namun juga tujuan jahat. Terlebih saja kejahatan jaringan mengintai para pengguna di jaringan komputer terkecil dan terdekat dari mereka yaitu LAN(*Local Area Network*). LAN secara umum dihubungkan menggunakan protokol data-link layer IEEE 802.3 yang jika dilihat dari jurnal-jurnal ilmiah merupakan protokol yang tidak dirancang atas dasar keamanan.

Dianalisa dari penyusaun terkecilnya dapat kita simpulkan bahwa internet secara murni tidak pernah aman. Hal ini dikarenakan protokol dasar nya sendiri dirancang dengan tidak aman terlebih dengan merujuk pada desain lapisan yang digunakan OSI atau pun TCP-IP tidak memberikan keuntungan apa pun. Hal ini diakinatakan protokol tersebut berda lapisan terbawah yang akan memberikan dampak ke aplikasi yang berjalan di atasnya sehingga membuat pengamanan di lapisan atas seperti firewall atau antivirus tidak berguna .

Kata kunci: data-link layer, protokol, IEEE 802.3

1 Pendahuluan

Protokol nir-authentifikasi yang digunakan pada jaringan komputer di data-link layer merupakan titik keamanan paling lemah yang menyusun jaringan komputer. Hal ini sudah menjadi rahasia umum. Bahkan banyak juga pakar jaringan yang telah memperingatakan bahaya ini baik dalam jurnal ilmiah maupun forum komunitas.

Namun orang-orang tentu saja tidak bisa menghindari untuk tidak menggunakan jaringan pada saat ini. Bagai orang awam meungkin mereka akan merasa aman saat telah memasang antivirus atau firewall di komputer masing-masing. Akan tetapi hal itu tentu saja tidak berguna untuk serangan pada data-link layer. Hal ini mungkin akan sulit dijelaskan kepada orang awam. Hal ini terkait penjelasan teknis yang sulit diterima.

Dengan menyadari situasi ini maka admin jaringan dapat digambarkan sebagai seorang petarung yang dimasukkan ke sungai penuh buaya untuk melindungi tuannya mngarungi sungai, tentu saja ini hanya sebuah analogi.

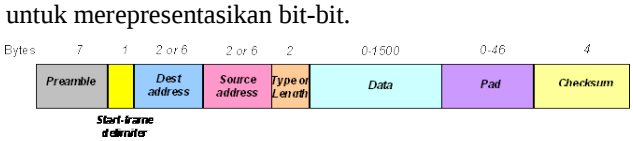
Tentu saja hal ini sangat merepotkan. Sehingga karena admin jaringan harus terus memantau jaringan. Bahkan solusi IDS(*Intrusion Detection System*) sekalipun masih membutuhkan sentuhan manusia. Sehingga pada beberap jurnal ilmiah perlu diimplementasi sub protokol untuk menambal lubang pada protokol asli di data-link layer.

Ilmu kriptografi merupakan salah satu ilmu yang dapat diimplementasikan untuk mengurangi lubang keamanan pada jaringan. Jika seringkali hanya digunakan untuk lapisan yang lebih atas. Maka makalah ini akan mencoba untuk menjelaskan teknik kriptografi yang mungkin yang dapat diimplementasi untuk menambal lubang keamanan di protokol data-link layer.

Salah satu teknik yang akan dicoba dipakai utnuk meningkatkan keamanan di data link layer pada makalah ini adalah teknik tanda-tangan digital. Teknik ini yang ditujukan untuk memeriksa validitas dokumen atau file akan dicoba dipergunakan untuk memeriksa validitas dari paket data link layer.

2 Paket data ethernet

Struktur data pengiriman paket pada ethernet dinamakan ethernet frame. Struktur data ini merupakan susunan untuk merepresentasikan bit-bit.



Ethernet frame IEEE 802.3 terdiri dari:

1. *preamble* sepanjang 7 bytes yang semunaya berisi 10101010. digunakan oleh receiver untuk melakukan sinkronisasi bit.
2. *start of frame* sepanjang 1 bytes berisi 10101011. merupakan flag frame yang mengindikasikan awal dari frame.
3. *destination address* sepanjang 6 bytes berisikan alamat mac pengirim.
4. *source address* sepanjang 6 bytes yang berisikan alamat mac penerima
5. *length* sepanjang 2 bytes
6. *data* yang maksimalnya 1500 bytes berisikan bit-bit data yang dikirimkan atara komputer
7. *pad* yang maksimal 46 bytes
8. *cheksum* sepanjang 4 bytes

struktur data ini merupakan batasan untuk menerapkan solusi keamanan pada data-link layer. Struktur data ini tidak mungkin untuk diubah-ubah karena hal ini merupakan standard yang dikenali sistem. Sehingga pengubahan sturktur data berarti pengubahan data-link layer di luar IEEE 802.3.

Dalam implementasi solusi. Bagian dari struktur data yang menarik untuk dijadikan sebagai informasi modal untuk keamanan adalah pada *destination address*, *source address* dan *data*.

Destination address dan *source address* dapat digunakan sebagai salah satu cara untuk mengindentifikasi pengirim dan penerima sedangkan data dapat dijadikan penampung dari bit-bit hasil kriptografi yang akan dicoba untuk diimplementasikan.

2.1 Protokol data link layer

Selain struktur data dari ethernet frame perlu diperhitungkan protokol yang berjalan pada layer ini. Pada makalah ini akan dibatasi pada IPV4 sehingga protokol yang utama di data-link layer ini adalah protokol ARP.

Protokol ARP ini digunakan sebagai protokol untuk melakukan pencarian host tujuan, protokol ini juga merupakan jantung utama dari cara kerja IEEE 802.3. Cara kerja dapat dijelasakan secara singkat:

1. keadaan awal host pengirim belum memiliki informasi
2. host pengirim mengirimkan pesan tersebar yang diterima keseluruhan host yang tersambung, menanyakan apakah ada yang merupakan tujuan
3. jika ada, host tujuan akan menjawab dan memabalas pesan ke pengirim dengan memberikan informasi alamat
4. tabel di sisi penerima dibentuk
5. pesan diterima oleh pengirim, tabel informasi alamat dibentuk di sisi pengirim
6. pengiriman data dilakukan
7. Tabel tidak selamanya valid. Dalam suatu periodik langkah 1-6 akan berulang lagi

Cara kerja protokol ARP lah yang menjadi lubang keamanan dari IPV4 dan menjadi sasaran eksplotitasi yang mudah. Dari penjelasan kerja protokol ARP dapat diidentifikasikan ada yang kurang dari prokol imi jika ditinjau dari ilmu kriptografi. Yaitu authentifikasi, tidak ada sama sekali pendistribusian kunci privat, publik bahkan yang sederhana sperti mekanisme kunci seperti diffie-Helman.

Hal ini merupakan lubang keamanan terbesar dari protokol ethernet yang tidak berevolusi bahkan setelah jaringan menjadi daerah yang tidak aman. Protokol ini terlanjur menjadi urat nadi internet dan belum dapat digantikan secara menyeluruh.

2.2 Serangan di data link layer

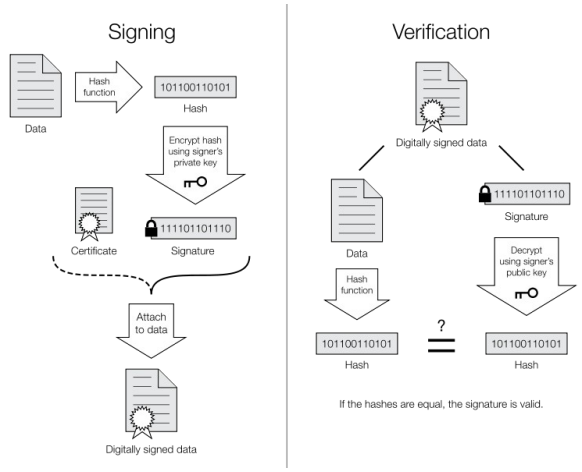
Secara umum ada lima serangan utama yang memiliki dampak cukup signifikan di data-link layer. namun ada satu serangan yang cukup fatal dan ironisnya mudah untuk dilakukan. Serangan ini dinamakan *man in the middle attack (MITM)*. Serangan ini dilakukan dengan memanfaatkan kelemahan ARP, penyerang akan menyamar seakan-akan menjadi komputer perantara dengan cara memberikan infromasi ARP yang salah ke kedua host. sehingga dapat dilakukan penyadapan, bahkan pengubahan data sekalipun.

Pada makalah ini akan difokuskan pada penanganan serangan paling fatal tersebut

3 Teknik tanda tangan digital

Secara umum teknik tanda tangan digital digunakan untuk melakukan verfikasi dokumen. Salah satu algoritma yang dapat dipakai di tanda tangan digital antara lain RSA. Selain algoritma kriptografi digunakn juga fungsi hash, antar lain yang dapat digunakan adalah MD5 dan SHA1.

Secara umum cara kerja tanda tangan digital dijelaskan pada gambar:



pada proses penanda tangan digunakan suatu hash function untuk mendapatkan nilai hash dari suatu dokumen. Nilai hash ini selanjutnya diencrypt

menggunakan kunci private. Selanjutnya hasil enkripsi akan ditempelkan ke dokumen yang selanjutnya menjadi arsip bertanda tangan.

Pada proses verifikasi, arsip yang bertanda tangan dipisahakan antara data dan tanda tangan. Data lalu dibangkitkan nilai hash nya dan tanda tangan didekripsi dengan kunci publik. Kedua nilai ini lalu dicek apakah sama. Jika sama maka dokumen tersebut valid. Jika tidak maka dinilai dokumen telah diubah dan dinyatakan tidak valid.

3.1 Algoritma

Untuk algoritma enkripsi dan dekripsi digunakan RSA. Algoritam RSA merupakan kriptografi yang termasuka kunci publik asimetris. RSA memilki dua pasang algoritma yaitu (E,D). E adalah algortima enkripsi public dan D adalah algoritma deckripsi. RSA mmenuhi

1. Enkripsi mengikuti dekripsi: jika c= E(m) dan cipherteks berkorespoodensi dengan beberapa palintext m, maka m=D(c). dengan kata lain m= D(E(m)) untuk plainteks m apapun
2. dapat mengeksripsi dengan efisien, untuk plainteks m apapun terdapta algorima untuk mengkalkulasi E(m).
3. dapar mendekripsi dengan efisien untuk plainteks atau cipherteks x, terdapat algoritma yang efisien untuk mengkalkulasi D(x).
4. kunci privat dan publik tidak berubah. Dengan mengetahui E tidak dapat ditemukan cara untuk memeproleh D.
5. tanda tangan diikuti dengan verifikasi. Set dari pesan m akan saam dengan set dari cipherteks c = E(m). sehingga algoritam dekripsi dan diapliaksiakn ke pesan, menghasilkan apa yang disebut pesan tertandatangan. Jika s= D(m) dan tanda tangan berkorespodensi dengan beberapa plainteks m, maka m= E(s). dengan kata lain, m = E(D(m))

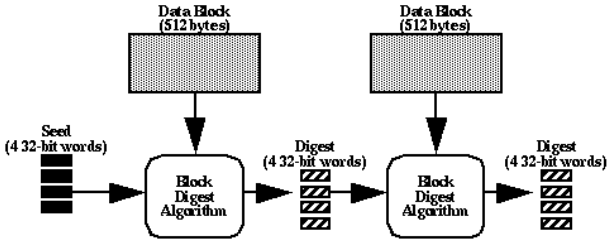
konstruksi RSA:

1. memilih p dan q yaitu bilangan prima acak besar yang memilki ukuran yang sama namun tidak salaing berdekatan nilainya.
2. Menghitung n = p*q
3. memilih eksponen enkripsi e acak yang kurang dari n dan tidak memilki faktor dari p-1 atau q-1
4. mengkalkulasi deksripsi eksponen yang memenuhi ed mod (p-1)(q-1) = 1
5. fungsi enkripsi adalah $E(m) = m^e \bmod n$
6. fungsi dekripsi adalah $D(c) = c^d \bmod n$
7. public key yang dipublish adalah pasangan (n,e)
8. private key adalah pasangan 3 bilangan (p,q,d)

3.2 Fungsi Hash

Untuk fungsi hash digunakan MD5, MD5 adalah fungsi hash satu-arah yang dibuat oleh Ron Rivest. MD5 merupakan perbaikan dari MD4 setelah MD4 berhasil diserang oleh kriptanalis. Algoritma MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan message digest yang panjangnya 128 bit.

Kehandalan dari MD5 untuk kebutuhan protokol terlihat dari banyaknya protokol internet yang menggunakan fungsi hash ini, antara lain: SNMP v2, IPv6/SIPP,OSPF,RIPing



Langkah-langkah pembuatan message digest secara garis besar:

1. Penambahan bit-bit pengganjal (padding bits).
2. Penambahan nilai panjang pesan semula.
3. Inisialisasi penyangga (buffer) MD.
4. Pengolahan pesan dalam blok berukuran 512 bit

4 Implementasi

Dalam implementasi kita perlu mempertimbangkan beberapa pertimbangan

1. proses dekripsi dan enkripsi tidak boleh terlalu memberatkan dan memakan bayak resource komputasi baik bagi PC pengirim maupun penerima
2. proses dekripsi dan enkripsi harus cepat. Hal ini terkait dengan komunikasi. Lag sedapat mungkin harus dihindari
3. kedua faktor tersebut tidak mengurangi tujuan dari keamanan.

Jika pada tujuan awal dari tanda tangan digital adalah menandatangani dan mengecek validitas dari dokumen. Maka pada penandatangan frame tujuan yang ingin dicapai adalah mengecek apakah penerima dan pengirim sesuai. Hal ini dikarenakan serangan MITM adanya pihak ketiga yang melakukan penyadapan sehingga teknik tanda tangan digital digunakn untuk menverifiaksi apakah frame berasal dari satu pengirim dan penerima yang dimaksudkan.

Dari tujuan diatas akan digunakan bagian struktur data *destination*, *source address* dan data. Struktur data ini akan digunakan sebagai data-data yang akan ditandatangai dan dilakukan verifikasi.

Secara umum proses tanda tangan dan verifikasi akan berkerja layaknya proses tanda tangan digital pada dokumen. Paket ditandatangani dan dilakukan verfikasi dengan melakukan proses hash, enkripsi, dekripsi dan penocokan hasil hash data dan hasil dekripsi.

4.1 Kebutuhan device tambahan

Namun melihat dari proses enkripsi, dekripsi dan hash, maka poin 1 dan poin 2 tidak dapat dipenuhi karena proses dekripsi, enkripsi sangat memboroskan resource bahkan untuk ukuran kunci yang pendek sekalipun. Akan tetapi kunci yang pendek tentu saja tidak dapat menjadi pilihan karena jika terlalu pendek maka poin ke-3 yang mengarah ke faktor keamanan justru tidak dapat diperoleh.

Dari berbagai pertimbangan dan solusi. maka cara yang paling baik adalah dengan menambahkan fungsi tersebut di sebuah device antara pengirim dan penerima yaitu switch.

Switch yang digunakan juga bukan switch sederhana seperti yang mungkin berbasi crossbar dan diatur dengan mikrokontroller seedrhana. Swithc yang akan digunakan untuk kebutuhan ini paling tidak harus memilki kemampuan komputasi yang baik. Saat jika mengikuti trenda adalah dengan menggunakn Salah satu prosessor embedded berbasis MIPS 32 bit pada kecepatan sekitar 200-500 mhz. Salah satu faktor pemilihan prossesor adlah perbandingan kecepatan pemrosesan MD5 yang jika diuji pada kecepatan 33 mhz dapat mmberikan angka pemrosesan md5 yang cukup baik dengan mencapai 16.5 mbs.

						In-Cache MD5 Rate	
Host	CPU	CPU (Mhz)	Caches External / Internal	MD5 Rate [no cache] (Mb/s)	Optimized MD5 Rate [no cache] (Mb/s)	External Cache (Mb/s)	Internal Cache (Mbps)
Dec 5x33	MIPS 3000	33	128 KB / -	16.5	17.9	18.2	-
Dec 4000 / 710	Alpha	190	4 MB / 8 KB	58.0	86.6	95.3	99.3
HP 712	PA 7100lC	60	64 KB / 1 KB	29.9	32.3	33.2	32.8
HP 9000 / 730	PA 1.1	66	256 KB / -	29.9	32.7	33.7	-
IBM RS6000 / 410	PPC 601	80	512 KB / 32 KB	47.5	47.4	48.8	49.1
IBM RS6000 / 3AT	POWER2	59	64 KB / 32 KB	53.4	54.9	56.1	56.1
IBM RS6000 / 590	POWER2	66.6	256 KB / 32 KB	61.2	63.0	63.4	63.3
Intel	486	66	- / 8 KB	19.0	30.9	-	33.3
Intel	Pentium	90	512 KB / 8 KB	32.5	43.8	45.5	46.7
SGI	MIPS 4400	150	1 MB / 16 KB	48.1	51.2	55.0	55.6
Sun 2	SPARC	40	64 KB / -	12.3	13.2	13.8	-
Sun 10/51	Super-SPARC	50	1 MB / 16 KB	34.7	36.8	37.9	38.3
Sun 20/61	Super-SPARC	60	1 MB / 16 KB	35.9	37.9	39.1	39.5
Sun 20/71	Super-SPARC2	75	1 MB / 16 KB	53.7	57.0	58.5	58.9

Untuk kebutuhan lingkungan implemntasi pemrogramana langung ke prosessor tentu memberikan level abstraksi yang kurang nyaman ke pengembang. yang dapat diusahakan untuk mengatasi masalah ini dengan menggunakan switch yang dipasang sistem operasi linux embedded. Hal ini dimungkinkan karena ukuran kernel linux paling tidak hanya 1 mb. Sehingga selain prosessor kita memerlukan RAM sekitar 1 mb untuk kebutuhan kernel. Terlebih dari kebutuhan prosessor Linux sudah mamapu berjalan di semua arsitektur embedded yang ada di pasaran.

Penggunaaan Linux tentu akan menguntungkan dari pemrosesan stack network. Tools yang dapat dipakai adalah iptables untuk mengatur rule frame. Proses tanda tangan digital dipakai sebagai rule tambahan untuk proses yang akan melewati switch tersebut.

Cara kerja iptables sebagai framework yang mengatur aliran data jaringan yang melewati linux. Pada iptables terdapat beberapa timing location untuk melakukan pengecekan data. Timgin location yang tepat untuk melakukan verifikasi adalah pada timing location forward. Di timing location ini akan dilakukan pengecekan dengan teknik tanda tangan digital. Baik public key, private key dan r menjadi masukan di modul ini. Aksi dilakaukan dengan melakukan tenkink tanda tanga digital dari frame, jika valid frame akan diteruskan jika tidak frame akan didrop.

5 Kesimpulan

Dari pembahasan makalah ini dapat ditarik beberapa kesimpulan

1. protokol ethernet merupakan lubang kemanan dasar dari internet
2. teknik tanda tangan digital dapat digunakan untuk melakukan verifikasi frame ethernet
3. untuk mengimplementasikan solusi tanda tangan digital diperlukan sebuah device tambahan berupa linux embedded.

Secara umum kesimpulan pada poin ke-3 terlihat memperbesar budget untuk menamabah infrastruktur namun hal ini menjadi faktor penting untuk kecepatan jaringan. Terlebih kemampuan prosessor embedded saat ini cukup cepat untuk melakukan komputasi kriptografi paling tidak dengan panjang 128 bit.

Solusi ini terlihat merepotkan namun untuk sebuah jaringan yang membutuhkan keamanan, solusi ini dapat diusulkan.

6 Daftar Pustaka

Schneier, Bruce. *Applied Cryptography 2nd Edition protocols, algorithm and source code in C.* John Willey & sons. 1996

Menezes, A, P. Van Ooschot, dan S. Vanstase. *handbook of Applied Cryptography.* 1996

Schiffman, Mike D. *Building Open Source Network Security Tools: Components and Techniques*. John Willey & sons. 2003

Wehrle Klaus. *The Linux® Networking Architecture: Design and Implementation of Network Protocols in the Linux Kernel.* Prentice hall 2004

Hall, eric. *Internet Core Protocol the definitive guide.* O'reilly 2000