UAS KEAMANAN INFORMASI

UMI LATIFATUL ROFI'AH

1310651004

Kelas : A

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH JEMBER

2015

TUGAS 1

BAB 5: Kriptografi

• Cornerstone kriptografi Konsep
• Symmetric Encryption
• Enkripsi asimetris
• Fungsi Hash
• Serangan kriptografi
• Pelaksana Kriptografi

1. KONSEP KRIPTOGRAFI CORNERSTONE

Kriptologi adalah ilmu komunikasi yang aman. Kriptografi menciptakan pesan makna yang tersembunyi, kriptanalisis adalah ilmu membobol pesan yang terenkripsi Sebuah cipher adalah algoritma kriptografi. Sebuah plaintext adalah pesan terenkripsi. Enkripsi mengubah plaintext menjadi ciphertext. Dekripsi sebuah ciphertext akan di ubah menjadi plaintext.

Jeniskriptografi
Ada tiga jenis utama dari enkripsi yang modern: simetris, asimetris, dan hashing.
Enkripsi simetris menggunakan satu kunci: menggunakan kunci yang sama untuk enkripsi dan mendekripsi.
Kriptografi asimetris menggunakan dua kunci: jika Anda mengenkripsi dengan satu tombol, Anda mungkin mendekripsi dengan yang lain.
Hashing adalah transformasi kriptografi satu arah menggunakan algoritma (dan tidak ada tombol).

2. ENCRYPTION SYMMETRIC

Enkripsi simetris menggunakan satu kunci untuk mengenkripsi dan mendekripsi. Simetris enkripsi juga disebut "kunci rahasia" enkripsi: kunci harus dirahasiakan dari Pihak ketiga.
Kekuatan termasuk kecepatan dan kekuatan kriptografi per bit dari kunci.
Kelemahan utama adalah bahwa kunci harus aman bersama sebelum kedua pihak dapat communicate aman.

Vektor inisialisasi dan chaining
Vektor inisialisasi digunakan dalam beberapa cipher simetrik untuk memastikan bahwa pertama blok dienkripsi data acak. Hal ini memastikan bahwa plaintext yang identik mengenkripsi untuk ciphertexts berbeda. Bruce Schneier juga mencatat di Applied Cryptography, "Lebih buruk lagi, dua pesan yang dimulai sama akan mengenkripsi dengan cara yang sama sampai perbedaan pertama. Beberapa pesan memiliki header umum: kop surat, atau 'Dari' line, atau apa pun. "1 vektor Inisialisasi memecahkan masalah ini.
Chaining (disebut umpan balik dalam mode aliran) biji dienkripsi sebelumnya blok ke blok berikutnya yang akan dienkripsi. Ini menghancurkan pola dalam menghasilkan yang ciphertext. Modus DES Elektronik Kode Buku (lihat di bawah) tidak menggunakan initial- isasi vektor atau chaining dan pola dapat terlihat jelas di dihasilkan dalam ciphertext.

DES
DES adalah Data Encryption Standard, yang menggambarkan Data Encryption algoritman rithm (DEA). IBM dirancang DES, berdasarkan lama Lucifer simetris mereka cipher. Menggunakan ukuran blok 64-bit (yang berarti mengenkripsi 64 bit setiap putaran) dan Kunci 56-bit.

Kode Buku Elektronik
Kode Buku Elektronik (ECB) adalah bentuk yang paling sederhana dan paling lemah dari DES. Ini tidak menggunakan inisialisasi vektor atau chaining. Plaintext yang identik dengan kunci identik

mengenkripsi ke ciphertexts identik.

Cipher Block Chaining
Cipher Block Chaining (CBC) Mode adalah mode blok DES yang XORs sebelumnya blok dienkripsi dari ciphertext ke blok berikutnya plaintext yang akan dienkripsi.

3. Enkripsi asimetris

Enkripsi asimetris menggunakan dua kunci: jika Anda mengenkripsi dengan satu tombol, Anda dapat mendekripsi dengan lainnya. Salah satu kunci dapat dibuat publik (disebut kunci publik); asimetris enkripsi juga disebut enkripsi kunci publik. Maka dari itu siapapun yang ingin berkomunikasi dengan anda munngkin cukup download kunci publik anda.
Metode Asymmetric Matematika yang ada di balik terobosan asimetris. Metode ini menggunakan "satu arah fungsi, "yang mudah untuk menghitung" satu cara "dan sulit untuk menghitung di sebaliknya arah.

4. FUNGSI Hash

Sebuah fungsi hash memberikan enkripsi menggunakan algoritma dan tidak ada tombol.
Mereka disebut "Fungsi hash satu arah" karena tidak ada cara untuk membalikkan enkripsi. Sebuah variabel-panjang plaintext "hash" menjadi (biasanya) tetap-panjang nilai hash (sering disebut "message digest" atau hanya "hash"). Fungsi hash terutama digunakan untuk menyediakan integritas: jika hash dari perubahan plaintext, plaintext sendiri telah berubah.

5. SERANGAN KRIPTOGRAFI

Serangan kriptografi digunakan oleh cryptanalysts untuk memulihkan plaintext tanpa kunci. Sebuah serangan brute-force menghasilkan seluruh keyspace, yang setiap kunci yang mungkin. Mengingat waktu yang cukup, plaintext akan pulih. Dikenal plaintext Sebuah serangan plaintext diketahui mengandalkan pulih dan menganalisis plaintext yang cocok dan Pasangan ciphertext: tujuannya adalah untuk mendapatkan kunci yang digunakan.

6. MELAKSANAKAN KRIPTOGRAFI

Simetris, asimetris, dan kriptografi berbasis hash tidak ada dalam ruang hampa: mereka diterapkan di dunia nyata, sering dalam kombinasi, untuk memberikan kerahasiaan, integritas yang rity, otentikasi, dan nonrepudiation.

Tanda tangan digital
Tanda tangan digital digunakan untuk dokumen tanda kriptografi. Tanda tangan digital memberikan nonrepudiation, yang mencakup otentikasi identitas penandatangan, dan bukti integritas dokumen (membuktikan dokumen tidak berubah).
Public Key Infrastructure (PKI) memanfaatkan semua tiga bentuk enkripsi untuk memberikan dan mengelola sertifikat digital. Sebuah sertifikat digital adalah kunci publik ditandatangani dengan tanda tangan digital. Sertifikat digital mungkin berdasarkan server atau client berbasis. Jika dua digunakan bersama-sama, mereka menyediakan saling otentikasi dan enkripsi.

TUGAS 2
Tentang Aplikasi AntiVirus

PCMAV

PCMedia AntiVirus disingkat PCMAV adalah perangkat lunak antivirus buatan PCMedia, sebuah majalah komputer Indonesia. Beroperasi dibawah sistem operasi Microsoft Windows (XP/Vista/7 keatas). PC Media Antivirus (PCMAV) sendiri bukan merupakan satu-satunya antivirus di Indonesia yang mempunyai formula atau teknologi khusus untuk mengatasi virus komputer yang menyebar luas di masyarakat, baik jenis lokal maupun mancanegara (asing), akan tetapi sejauh ini PCMAV digadang-gadang dapat membersihkan infeksi terhadap secara akurat dan tuntas hingga pulih 100%.

Dikarenakan menggunakan bahasa pemrograman Delphi, menjadikannya berbeda dengan antivirus standar industri sejenis yang biasanya menggunakan bahasa pemrograman Microsoft Visual C++. Untuk virus database-nya sendiri dikarenakan virus database internalnya masih sedikit, PCMAV juga memanfaatkan penggunaan alternatif database dari ClamAV sebagai database tambahan eksternal.