Copyright © September 2023

METODE OTENTIFIKASI

PERTEMUAN 6 - 7

1.1. Metode Otentifikasi

Kata sandi, frasa sandi, atau PIN adalah contoh dari sesuatu yang diketahui pengguna. Kata sandi adalah metode paling populer yang digunakan untuk otentikasi. Istilah frasa sandi, kode sandi, kunci sandi, atau PIN secara umum disebut sebagai kata sandi. Kata sandi adalah serangkaian karakter yang digunakan untuk membuktikan identitas pengguna. Jika rangkaian karakter ini berhubungan kembali dengan pengguna (seperti nama, tanggal lahir, atau alamat), akan lebih mudah bagi penjahat cyber untuk menebak kata sandi pengguna. Sejumlah publikasi merekomendasikan bahwa kata sandi setidaknya terdiri dari delapan karakter. Pengguna tidak boleh membuat kata sandi yang terlalu panjang sehingga sulit untuk dihafal, atau sebaliknya, sangat pendek sehingga rentan terhadap peretasan kata sandi. Kata sandi harus berisi kombinasi huruf besar dan kecil, angka, dan karakter khusus. Klik di sini untuk menguji kata sandi saat ini. Pengguna perlu menggunakan kata sandi yang berbeda untuk sistem yang berbeda karena jika seorang penjahat memecahkan kata sandi pengguna sekali, penjahat akan memiliki akses ke semua akun pengguna. Pengelola kata sandi dapat membantu pengguna membuat dan mengingat kata sandi yang kuat. Klik di sini untuk melihat pembuat kata sandi yang kuat.

Kartu pintar dan fob kunci keamanan adalah contoh dari sesuatu yang dimiliki pengguna.

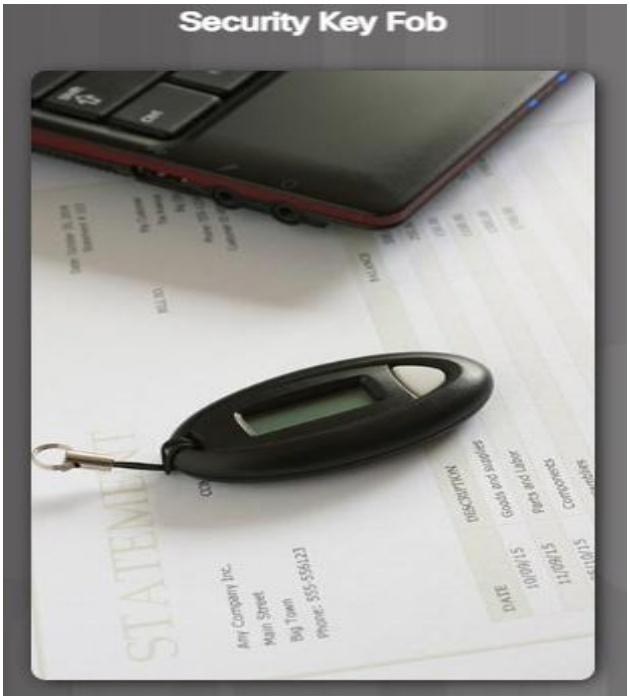
Keamanan Kartu Cerdas (Gambar 1) – Kartu pintar adalah kartu plastik kecil, seukuran kartu kredit, dengan chip kecil yang tertanam di dalamnya. Chip tersebut merupakan pembawa data yang cerdas, mampu memproses, menyimpan, dan menjaga data. Kartu pintar menyimpan

informasi pribadi, seperti nomor rekening bank, identifikasi pribadi, catatan medis, dan tanda tangan digital. Kartu pintar menyediakan otentikasi dan enkripsi untuk menjaga keamanan data.

Gambar 1. Keamanan Smart Card

Security Key Fob (Gambar 2) – Security key fob adalah perangkat yang cukup kecil untuk dipasang ke gantungan kunci. Ini menggunakan proses yang disebut otentikasi dua faktor, yang lebih aman daripada kombinasi nama pengguna dan kata sandi. Pertama, pengguna memasukkan nomor identifikasi pribadi (PIN). Jika dimasukkan dengan benar, fob kunci keamanan akan menampilkan nomor. Ini adalah faktor kedua, yang harus dimasukkan pengguna untuk masuk ke perangkat atau jaringan.

Copyright © September 2023



Gambar 2 Key Fob

Karakteristik fisik yang unik, seperti sidik jari, retina, atau suara, yang mengidentifikasi pengguna tertentu disebut biometrik. Keamanan biometrik membandingkan karakteristik fisik dengan profil yang disimpan untuk mengautentikasi pengguna. Profil adalah file data yang berisi karakteristik individu yang diketahui. Sistem memberikan akses pengguna jika karakteristiknya cocok dengan pengaturan yang disimpan. Pembaca sidik jari adalah perangkat biometrik yang umum.

Ada dua jenis pengenal biometrik:

- Physiological characteristics – ini termasuk sidik jari, DNA, wajah, tangan, retina, atau fitur telinga
- Behavioral characteristics - termasuk pola perilaku, seperti gerak tubuh, suara, ritme mengetik, atau cara pengguna berjalan

Copyright © September 2023

Biometrik menjadi semakin populer dalam sistem keamanan publik, elektronik konsumen, dan aplikasi point-of-sale. Menerapkan biometrik menggunakan pembaca atau perangkat pemindaian, perangkat lunak yang mengubah informasi yang dipindai menjadi bentuk digital, dan database yang menyimpan data biometrik untuk perbandingan.

MULTI-FACTOR AUTHENTICATION

Multi-factor Authentication menggunakan setidaknya dua metode verifikasi. Fob kunci keamanan adalah contoh yang bagus. Kedua faktor tersebut adalah sesuatu yang Anda ketahui, seperti kata sandi, dan sesuatu yang Anda miliki, seperti fob kunci keamanan. Ambil langkah ini lebih jauh dengan menambahkan sesuatu tentang diri Anda, seperti pemindaian sidik jari. Otentikasi multi-faktor dapat mengurangi insiden pencurian identitas online karena mengetahui kata sandi tidak akan memberikan akses penjahat cyber ke informasi pengguna. Misalnya, situs web perbankan online mungkin memerlukan kata sandi dan PIN yang diterima pengguna di ponsel cerdasnya. Seperti yang ditunjukkan pada gambar, menarik uang tunai dari ATM adalah contoh lain dari otentikasi multifaktor. Pengguna harus memiliki kartu bank dan mengetahui PIN sebelum ATM akan mengeluarkan uang tunai.

1.2. Otorisasi

Otorisasi mengontrol apa yang dapat dan tidak dapat dilakukan pengguna di jaringan setelah otentikasi berhasil. Setelah pengguna membuktikan identitasnya, sistem memeriksa untuk melihat sumber daya jaringan apa yang dapat diakses pengguna dan apa yang dapat dilakukan pengguna dengan sumber daya tersebut. Seperti yang ditunjukkan pada gambar, otorisasi menjawab pertanyaan, “Apa hak istimewa membaca, menyalin, membuat, dan menghapus yang dimiliki pengguna?” Otorisasi menggunakan satu set atribut yang menjelaskan akses pengguna

Copyright © September 2023

ke jaringan. Sistem membandingkan atribut ini dengan informasi yang terkandung dalam database otentikasi, menentukan serangkaian batasan untuk pengguna itu, dan mengirimkannya ke router lokal tempat pengguna terhubung. Otorisasi bersifat otomatis dan tidak mengharuskan pengguna untuk melakukan langkah tambahan setelah autentikasi. Terapkan otorisasi segera setelah pengguna mengautentikasi.

Mendefinisikan aturan otorisasi adalah langkah pertama dalam mengontrol akses. Kebijakan otorisasi menetapkan aturan-aturan ini. Kebijakan keanggotaan grup mendefinisikan otorisasi berdasarkan keanggotaan dalam grup tertentu. Misalnya, semua karyawan organisasi memiliki kartu gesek, yang menyediakan akses ke fasilitas tersebut. Jika pekerjaan karyawan tidak mengharuskan dia memiliki akses ke ruang server, kartu keamanannya tidak akan mengizinkannya memasuki ruangan itu. Kebijakan tingkat otoritas menentukan izin akses berdasarkan status karyawan dalam organisasi. Misalnya, hanya karyawan tingkat senior di departemen TI yang dapat mengakses ruang server.

1.3. Akuntabilitas

Akuntabilitas melacak tindakan kembali ke seseorang atau proses yang membuat perubahan ke sistem, mengumpulkan informasi ini, dan melaporkan data penggunaan. Organisasi dapat menggunakan data ini untuk tujuan seperti audit atau penagihan. Data yang dikumpulkan mungkin termasuk waktu masuk untuk pengguna, apakah pengguna berhasil atau gagal, atau sumber daya jaringan apa yang diakses pengguna. Hal ini memungkinkan organisasi untuk melacak tindakan, kesalahan, dan kesalahan selama audit atau investigasi.

Implementasi akuntabilitas terdiri dari teknologi, kebijakan, prosedur, dan pendidikan. File log memberikan informasi rinci berdasarkan parameter yang dipilih. Misalnya, sebuah organisasi

Copyright © September 2023

mungkin melihat log untuk kegagalan dan keberhasilan login. Kegagalan login dapat menunjukkan bahwa seorang penjahat mencoba meretas akun. Keberhasilan masuk memberi tahu organisasi pengguna mana yang menggunakan sumber daya apa dan kapan. Apakah normal bagi pengguna yang berwenang untuk mengakses jaringan perusahaan pada pukul 3:00 pagi? Kebijakan dan prosedur organisasi menguraikan tindakan apa yang harus direkam dan bagaimana file log dibuat, ditinjau, dan disimpan. Penyimpanan data, pembuangan media, dan persyaratan kepatuhan semuanya memberikan akuntabilitas. Banyak undang-undang mengharuskan penerapan langkah-langkah untuk mengamankan tipe data yang berbeda. Undang-undang ini memandu organisasi tentang cara yang benar untuk menangani, menyimpan, dan membuang data. Pendidikan dan kesadaran akan kebijakan, prosedur, dan undang-undang terkait organisasi juga dapat berkontribusi pada akuntabilitas.

1.4. Jenis Kontrol Keamanan

1. Kontrol Pencegahan

Mencegah berarti mencegah sesuatu terjadi. Kontrol akses preventif menghentikan aktivitas yang tidak diinginkan atau tidak sah terjadi. Untuk pengguna yang berwenang, kontrol akses preventif berarti pembatasan. Menetapkan hak khusus pengguna pada suatu sistem adalah contoh dari kontrol preventif. Meskipun pengguna adalah pengguna yang berwenang, sistem memberikan batasan untuk mencegah pengguna mengakses dan melakukan tindakan yang tidak sah. Firewall yang memblokir akses ke port atau layanan yang dapat dieksploitasi oleh penjahat dunia maya juga merupakan kontrol pencegahan.

Copyright © September 2023

2. Kontrol Pencegah

Penghalang adalah kebalikan dari hadiah. Hadiah mendorong individu untuk melakukan hal yang benar, sementara pencegah mencegah mereka melakukan hal yang salah. Profesional dan organisasi keamanan dunia maya menggunakan pencegah untuk membatasi atau mengurangi tindakan atau perilaku, tetapi pencegah tidak menghentikannya. Penghalang kontrol akses mencegah penjahat dunia maya mendapatkan akses tidak sah ke sistem informasi dan data sensitif. Penghalang kontrol akses mencegah sistem menyerang, mencuri data, atau menyebarkan kode berbahaya. Organisasi menggunakan pencegah kontrol akses untuk menegakkan kebijakan keamanan siber.

Pencegah membuat calon penjahat cyber berpikir dua kali sebelum melakukan kejahatan. Gambar tersebut mencantumkan pencegah kontrol akses umum yang digunakan di dunia keamanan siber.

3. Kontrol Detektif

Deteksi adalah tindakan atau proses memperhatikan atau menemukan sesuatu. Deteksi kontrol akses mengidentifikasi berbagai jenis aktivitas yang tidak sah. Sistem deteksi bisa sangat sederhana, seperti pendeteksi gerakan atau penjaga keamanan. Mereka juga bisa lebih kompleks, seperti sistem deteksi intrusi. Semua sistem detektif memiliki beberapa kesamaan; mereka mencari aktivitas yang tidak biasa atau dilarang. Mereka juga menyediakan metode untuk merekam atau memperingatkan operator sistem tentang potensi akses tidak sah. Kontrol detektif tidak mencegah sesuatu terjadi; mereka lebih merupakan ukuran setelah fakta.

Copyright © September 2023

4. Kontrol korektif

Korektif melawan sesuatu yang tidak diinginkan. Organisasi menerapkan kontrol akses korektif setelah sistem mengalami ancaman. Kontrol korektif mengembalikan sistem kembali ke keadaan kerahasiaan, integritas, dan ketersediaan. Mereka juga dapat memulihkan sistem ke normal setelah aktivitas yang tidak sah terjadi.

5. Kontrol Pemulih

Pemulihan adalah kembali ke keadaan normal. Kontrol akses pemulihan memulihkan sumber daya, fungsi, dan kemampuan setelah pelanggaran kebijakan keamanan. Kontrol pemulihan dapat memperbaiki kerusakan, selain menghentikan kerusakan lebih lanjut. Kontrol ini memiliki kemampuan yang lebih canggih dibandingkan kontrol akses korektif.

6. Kontrol Kompensasif

Kompensasi berarti menebus sesuatu. Kontrol akses kompensatif memberikan opsi untuk kontrol lain untuk mendukung penegakan dalam mendukung kebijakan keamanan. Kontrol kompensasi juga bisa menjadi substitusi yang digunakan sebagai pengganti kontrol yang tidak mungkin dilakukan dalam situasi tersebut. Misalnya, sebuah organisasi mungkin tidak dapat memiliki anjing penjaga, jadi alih-alih menggunakan detektor gerakan dengan lampu sorot dan suara gonggongan.

1.5. Obscuring Data

1. Data Masking

Teknologi penyamaran data mengamankan data dengan mengganti informasi sensitif dengan versi yang tidak sensitif. Versi non-sensitif terlihat dan bertindak seperti aslinya. Artinya, suatu

proses bisnis dapat menggunakan data yang tidak sensitif dan tidak perlu mengubah aplikasi pendukung atau fasilitas penyimpanan data. Dalam kasus penggunaan yang paling umum, masking membatasi penyebaran data sensitif dalam sistem TI dengan mendistribusikan set data pengganti untuk pengujian dan analisis. Informasi dapat disembunyikan secara dinamis jika sistem atau aplikasi menentukan bahwa permintaan pengguna untuk informasi sensitif berisiko.

Penyembunyian data dapat menggantikan data sensitif di lingkungan non-produksi untuk melindungi informasi yang mendasarinya. Ada beberapa teknik penyamaran data yang dapat memastikan bahwa data tetap bermakna tetapi cukup diubah untuk melindunginya:

- Substitusi menggantikan data dengan nilai-nilai yang tampak otentik untuk menerapkan anonimitas ke catatan data.
- Pengacakan memperoleh set substitusi dari kolom data yang sama yang ingin disembunyikan pengguna. Teknik ini bekerja dengan baik untuk informasi keuangan dalam database pengujian, misalnya.
- Nulling out menerapkan nilai null ke bidang tertentu, yang sepenuhnya mencegah visibilitas data.

2. Steganography

Steganografi menyembunyikan data (pesan) dalam file lain seperti grafik, audio, atau file teks lainnya. Kelebihan steganografi dibandingkan kriptografi adalah pesan rahasianya tidak menarik perhatian khusus. Tidak ada yang akan pernah tahu bahwa gambar sebenarnya berisi pesan rahasia dengan melihat file baik secara elektronik atau hardcopy. Ada beberapa komponen yang terlibat dalam menyembunyikan data. Pertama, ada data yang disematkan, yaitu pesan rahasia. Cover-text (atau cover-image atau cover-audio) menyembunyikan data tertanam yang

menghasilkan stego-text (atau stego-image atau stego-audio). Stego-key mengontrol proses persembunyian.

Pendekatan yang digunakan untuk menyematkan data pada cover-image adalah menggunakan Least Significant Bits (LSB). Metode ini menggunakan bit dari setiap piksel pada gambar. Piksel adalah unit dasar warna yang dapat diprogram dalam gambar komputer. Warna spesifik suatu piksel adalah perpaduan tiga warna—merah, hijau, dan biru (RGB). Tiga byte data menentukan warna piksel (satu byte untuk setiap warna). Delapan bit membentuk satu byte. Sistem warna 24-bit menggunakan ketiga byte. LSB menggunakan sedikit dari masing-masing komponen warna merah, hijau, dan biru. Setiap piksel dapat menyimpan 3 bit. Gambar tersebut menunjukkan tiga piksel dari gambar berwarna 24-bit. Salah satu huruf dalam pesan rahasia adalah huruf T, dan memasukkan karakter T hanya mengubah dua bit warna. Mata manusia tidak dapat mengenali perubahan yang dibuat pada bagian yang paling tidak signifikan. Hasilnya adalah karakter tersembunyi. Rata-rata, tidak lebih dari setengah bit dalam gambar perlu diubah untuk menyembunyikan pesan rahasia secara efektif.

Gambar 1. Bit Signitifikan

Copyright © September 2023

Steganografi sosial menyembunyikan informasi di depan mata dengan membuat pesan yang dapat dibaca dengan cara tertentu oleh beberapa orang untuk mendapatkan pesan tersebut. Orang lain yang melihatnya dengan cara biasa tidak akan melihat pesan tersebut. Remaja di media sosial menggunakan taktik ini untuk berkomunikasi dengan teman-teman terdekat mereka sambil membuat orang lain, seperti orang tua mereka, tidak menyadari apa arti sebenarnya dari pesan tersebut. Misalnya, frasa "pergi ke bioskop" mungkin berarti "pergi ke pantai". Individu di negara-negara yang menyensor media juga menggunakan steganografi sosial untuk menyampaikan pesan mereka dengan sengaja salah mengeja kata atau membuat referensi yang tidak jelas. Akibatnya, mereka berkomunikasi dengan audiens yang berbeda secara bersamaan.

Steganalisis adalah penemuan bahwa ada informasi tersembunyi. Tujuan dari steganalisis adalah untuk menemukan informasi yang tersembunyi. Pola dalam stego-image menimbulkan kecurigaan. Misalnya, disk mungkin memiliki area yang tidak digunakan yang menyembunyikan informasi. Utilitas analisis disk dapat melaporkan informasi tersembunyi dalam kelompok perangkat penyimpanan yang tidak digunakan. Filter dapat menangkap paket data yang berisi informasi tersembunyi di header paket. Kedua metode ini menggunakan tanda tangan steganografi. Dengan membandingkan gambar asli dengan stego-image, seorang analis dapat mengambil pola berulang secara visual.

3. Data obfuscation

Obfuscation adalah penggunaan dan praktik teknik penyamaran data dan steganografi dalam profesi keamanan siber dan intelijen siber. Kebingungan adalah seni membuat pesan membingungkan, ambigu, atau lebih sulit dipahami. Suatu sistem dapat dengan sengaja mengacak pesan untuk mencegah akses tidak sah ke informasi sensitif.

Copyright © September 2023

Watermarking perangkat lunak melindungi perangkat lunak dari akses atau modifikasi yang tidak sah. Watermarking perangkat lunak menyisipkan pesan rahasia ke dalam program sebagai bukti kepemilikan. Pesan rahasianya adalah tanda air perangkat lunak. Jika seseorang mencoba menghapus tanda air, hasilnya adalah kode yang tidak berfungsi. Kebingungan perangkat lunak menerjemahkan perangkat lunak ke dalam versi yang setara dengan aslinya tetapi lebih sulit untuk dianalisis oleh penyerang. Mencoba merekayasa balik perangkat lunak memberikan hasil yang tidak dapat dipahami dari perangkat lunak yang masih berfungsi.

1.6. Ensuring Integrity

Integritas memastikan bahwa data tetap tidak berubah dan dapat dipercaya oleh siapa pun atau apa pun selama seluruh siklus hidupnya. Integritas data adalah komponen penting untuk desain, implementasi, dan penggunaan sistem apa pun yang menyimpan, memproses, atau mentransmisikan data. Bab ini dimulai dengan membahas jenis kontrol integritas data yang digunakan seperti algoritma hashing, salting, dan kode otentikasi pesan keyed-hash (HMAC). Penggunaan tanda tangan dan sertifikat digital menggabungkan kontrol integritas data untuk menyediakan cara bagi pengguna untuk memverifikasi keaslian pesan dan dokumen. Bab ini diakhiri dengan diskusi tentang penegakan integritas database. Memiliki sistem integritas data yang terkontrol dengan baik dan terdefinisi dengan baik meningkatkan stabilitas, kinerja, dan pemeliharaan sistem basis data.

1. Jenis Kontrol Integritas Data

Hashing

Apa itu Hashing? Pengguna perlu mengetahui bahwa data mereka tetap tidak berubah saat diam atau dalam perjalanan. Hashing adalah alat yang memastikan integritas data dengan mengambil

Copyright © September 2023

data biner (pesan) dan menghasilkan representasi panjang tetap yang disebut nilai hash atau intisari pesan, seperti yang ditunjukkan pada gambar. Alat hash menggunakan fungsi hashing kriptografi untuk memverifikasi dan memastikan integritas data. Itu juga dapat memverifikasi otentikasi. Fungsi hash menggantikan kata sandi teks yang jelas atau kunci enkripsi karena fungsi hash adalah fungsi satu arah. Ini berarti bahwa jika kata sandi di-hash dengan algoritma hashing tertentu, itu akan selalu menghasilkan intisari hash yang sama. Ini dianggap satu arah karena dengan fungsi hash, secara komputasi tidak mungkin untuk dua set data yang berbeda menghasilkan hash digest atau output yang sama. Setiap kali data diubah atau diubah, nilai hash juga berubah. Karena itu, nilai hash kriptografi sering disebut sidik jari digital. Mereka dapat mendeteksi file data duplikat, perubahan versi file, dan aplikasi serupa. Nilai-nilai ini menjaga terhadap perubahan yang tidak disengaja atau disengaja pada data dan kerusakan data yang tidak disengaja. Hashing juga sangat efisien. File besar atau konten seluruh disk drive menghasilkan nilai hash dengan ukuran yang sama.

Properti Hash Hashing adalah fungsi matematika satu arah yang relatif mudah untuk dihitung, tetapi secara signifikan lebih sulit untuk dibalik. Menggiling kopi adalah analogi yang baik dari fungsi satu arah. Sangat mudah untuk menggiling biji kopi, tetapi hampir tidak mungkin untuk menyatukan kembali semua potongan kecil untuk membangun kembali biji aslinya. Fungsi hash kriptografi memiliki properti berikut:

- Inputnya bisa berapa saja.
- Output memiliki panjang tetap.
- Fungsi hash adalah satu arah dan tidak dapat dibalik.
- Dua nilai input yang berbeda hampir tidak akan pernah menghasilkan nilai hash yang sama.

Gambar 2. Hasing Metode

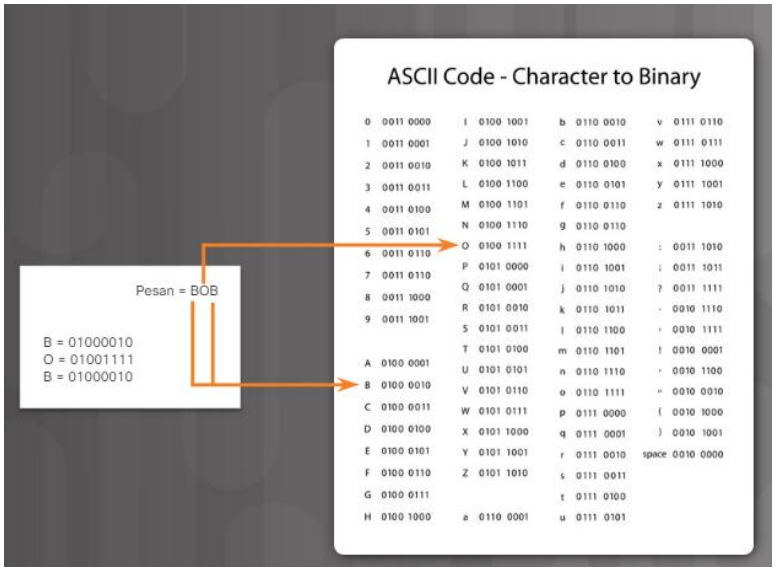
Algoritma Hash Fungsi hash sangat membantu untuk memastikan bahwa pengguna atau kesalahan komunikasi tidak mengubah data secara tidak sengaja. Misalnya, pengirim mungkin ingin memastikan bahwa tidak ada yang mengubah pesan dalam perjalanan ke penerima. Perangkat pengirim memasukkan pesan ke dalam algoritma hashing dan menghitung intisari panjang tetap atau sidik jarinya.

Algoritma Hash Sederhana (Checksum 8-bit)

Checksum 8-bit adalah salah satu algoritma hashing pertama, dan merupakan bentuk paling sederhana dari fungsi hash. Checksum 8-bit menghitung hash dengan mengubah pesan menjadi bilangan biner dan kemudian mengatur string bilangan biner menjadi chuck 8-bit. Algoritma menjumlahkan nilai 8-bit. Langkah terakhir adalah mengonversi hasil menggunakan proses yang disebut komplemen 2. Komplemen 2 mengubah biner ke nilai kebalikannya, dan kemudian menambahkan satu. Ini berarti bahwa nol berubah menjadi satu, dan satu berubah menjadi nol. Langkah terakhir adalah menambahkan 1 menghasilkan nilai hash 8-bit.

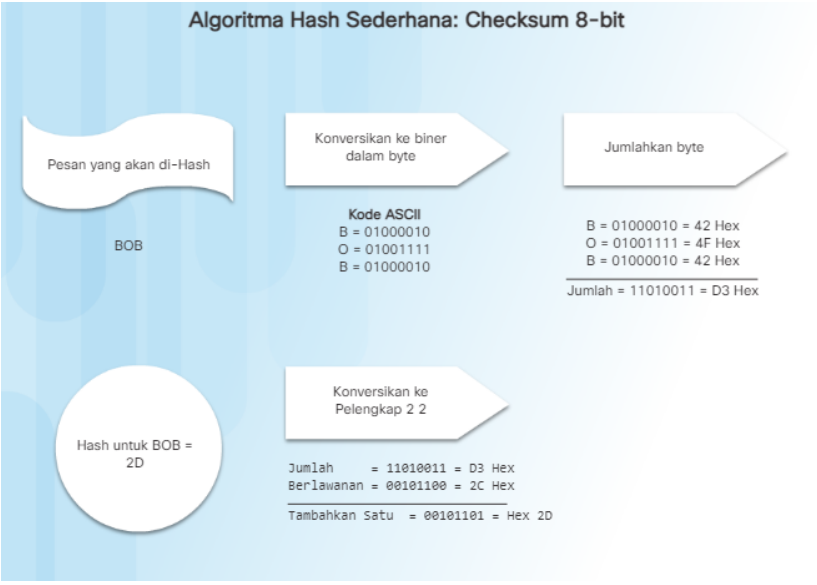
Klik http://easyonlineconverter.com/converters/checksum_converter.html untuk menghitung hash 8-bit untuk pesan BOB .

a. Konversi BOB ke biner menggunakan kode ASCII, seperti yang ditunjukkan pada Gambar 3.



Gambar 3. Ascii Code

b. Konversikan bilangan biner ke heksadesimal, seperti terlihat pada Gambar 4



Copyright © September 2023

Gambar 4. Perhitungan Haseing

c. Masukkan angka heksadesimal ke dalam kalkulator (42 4F 42).

d. Klik tombol Hitung . Hasilnya adalah nilai hash 2D .

Coba contoh berikut:

SECRET = “S”=53 “E”=45 “C”=43 “R”=52 “E”=45 “T”=54

HASH VALUE = 3A

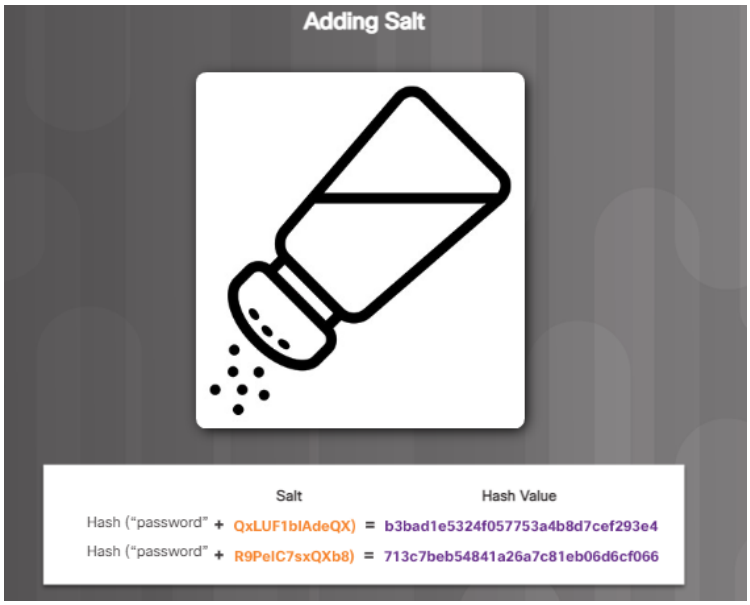
MESSAGE = “M”=4D “E”=45 “S”=53 “S”=53 “A”=41 “G”=47 “E”=45

HASH VALUE = FB

SALTING

Salting membuat hashing kata sandi lebih aman. Jika dua pengguna memiliki kata sandi yang sama, mereka juga akan memiliki hash kata sandi yang sama. Garam, yang merupakan string karakter acak, merupakan input tambahan ke kata sandi sebelum hashing. Ini menciptakan hasil hash yang berbeda untuk dua kata sandi seperti yang ditunjukkan pada gambar. Basis data menyimpan hash dan Salting.

Pada gambar, kata sandi yang sama menghasilkan hash yang berbeda karena Salting di setiap contoh berbeda. Garam tidak harus dirahasiakan karena merupakan angka acak.



Gambar 5. Pemberian Salt

PREVENTING ATTACKS

Salting prevents menggunakan serangan kamus untuk mencoba menebak kata sandi. Pengasinan juga membuat tidak mungkin menggunakan tabel pencarian dan tabel pelangi untuk memecahkan hash.

Lookup Tables, Lookup Tables menyimpan hash kata sandi yang telah dihitung sebelumnya dalam kamus kata sandi bersama dengan kata sandi yang sesuai. Tabel pencarian adalah struktur data yang memproses ratusan pencarian hash per detik. Klik di sini untuk melihat seberapa cepat tabel pencarian dapat memecahkan hash.

Reverse Lookup Tables, Serangan ini memungkinkan penjahat dunia maya meluncurkan kamus atau serangan brute force pada banyak hash tanpa tabel pencarian yang telah dihitung sebelumnya. Penjahat dunia maya membuat tabel pencarian yang memplot setiap hash kata sandi dari basis data akun yang dilanggar ke daftar pengguna. Penjahat dunia maya meng-hash setiap

Copyright © September 2023

tebakan kata sandi dan menggunakan tabel pencarian untuk mendapatkan daftar pengguna yang kata sandinya cocok dengan tebakan penjahat dunia maya, seperti yang ditunjukkan pada gambar. Karena banyak pengguna memiliki kata sandi yang sama, serangan itu bekerja dengan baik.

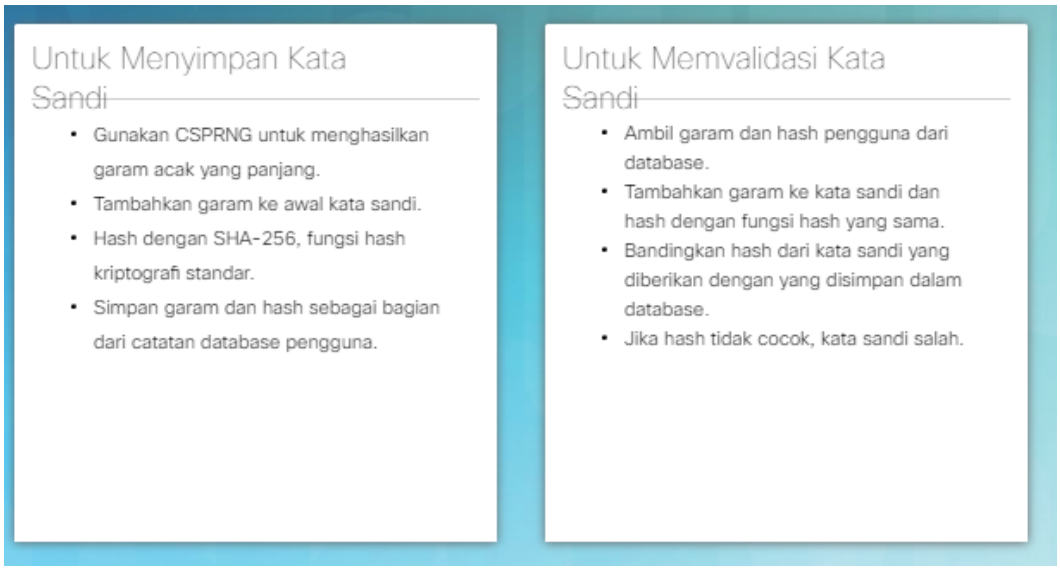
Rainbow Tables , Rainbow Tables mengorbankan kecepatan peretasan hash untuk membuat tabel pencarian lebih kecil. Tabel yang lebih kecil berarti tabel tersebut dapat menyimpan solusi ke lebih banyak hash dalam jumlah ruang yang sama.

MENERAPKAN SALTING

Sebuah Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) adalah pilihan terbaik untuk menghasilkan garam. CSPRNG menghasilkan nomor acak yang memiliki tingkat keacakan yang tinggi dan sama sekali tidak dapat diprediksi, sehingga aman secara kriptografis. Untuk menerapkan penggaraman dengan sukses, gunakan rekomendasi berikut:

- Salting harus unik untuk setiap kata sandi pengguna.
- Jangan pernah menggunakan kembali Salting.
- Panjang Salting harus sesuai dengan panjang keluaran fungsi hash.
- Selalu hash di server dalam aplikasi web.

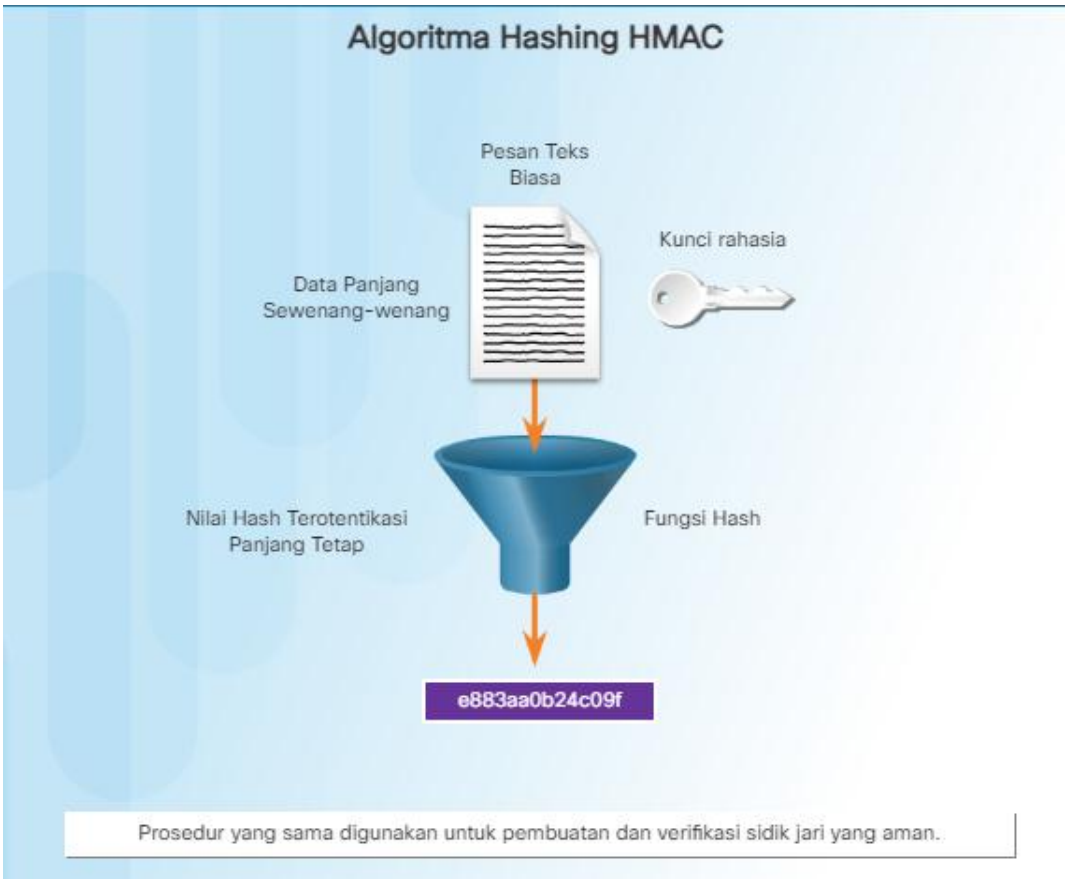
Menggunakan teknik yang disebut peregangan kunci juga akan membantu melindungi dari serangan. Peregangan kunci membuat fungsi hash sangat lambat. Ini mencegah perangkat keras kelas atas yang dapat menghitung miliaran hash per detik menjadi kurang efektif. Langkah-langkah yang digunakan aplikasi database untuk menyimpan dan memvalidasi kata sandi yang diasinkan ditunjukkan pada gambar berikut



Gambar 6 implemnetasi Salting

HMAC

Langkah selanjutnya dalam mencegah penjahat dunia maya meluncurkan kamus atau serangan brute force pada hash adalah dengan menambahkan kunci rahasia ke hash. Hanya orang yang mengetahui hash yang dapat memvalidasi kata sandi. Salah satu cara untuk melakukannya adalah dengan memasukkan kunci rahasia dalam hash menggunakan algoritma hash yang disebut kode otentikasi pesan hash-kunci (HMAC atau KHMAC). HMAC menggunakan kunci rahasia tambahan sebagai input ke fungsi hash. Penggunaan HMAC melangkah lebih jauh dari sekedar jaminan integritas dengan menambahkan otentikasi. HMAC menggunakan algoritma khusus yang menggabungkan fungsi hash kriptografis dengan kunci rahasia, seperti yang ditunjukkan pada gambar. Hanya pengirim dan penerima yang mengetahui kunci rahasia, dan output dari fungsi hash sekarang bergantung pada data input dan kunci rahasia. Hanya pihak yang memiliki akses ke kunci rahasia tersebut yang dapat menghitung intisari dari fungsi HMAC. Karakteristik ini mengalahkan serangan man-in-the-middle dan menyediakan otentikasi asal data.

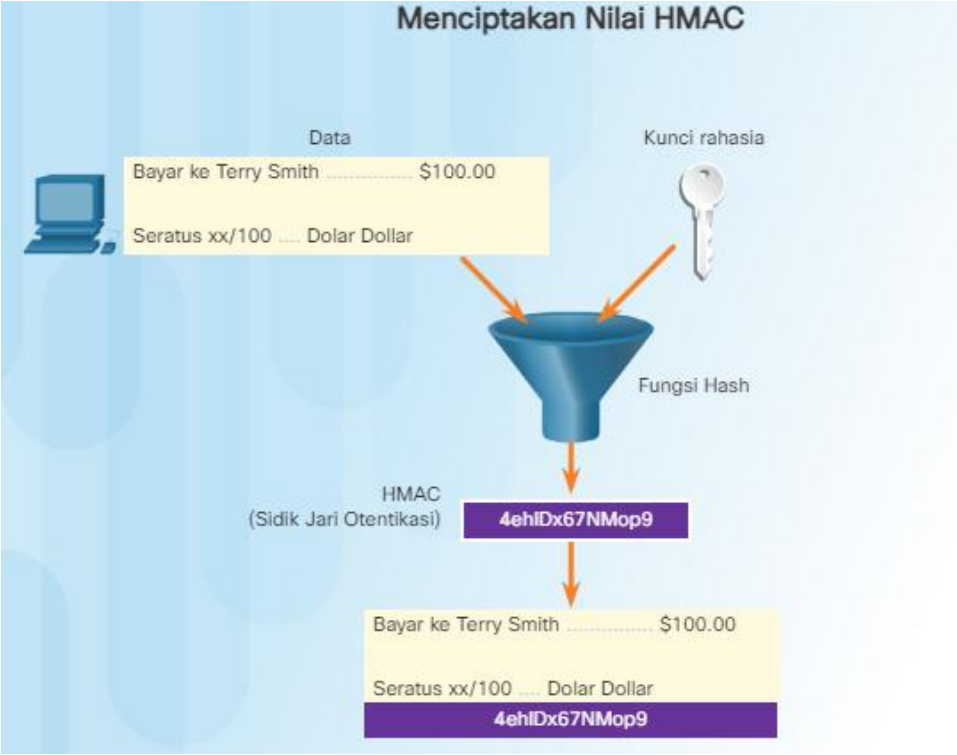


Gambar 7. Algoritma HMAC

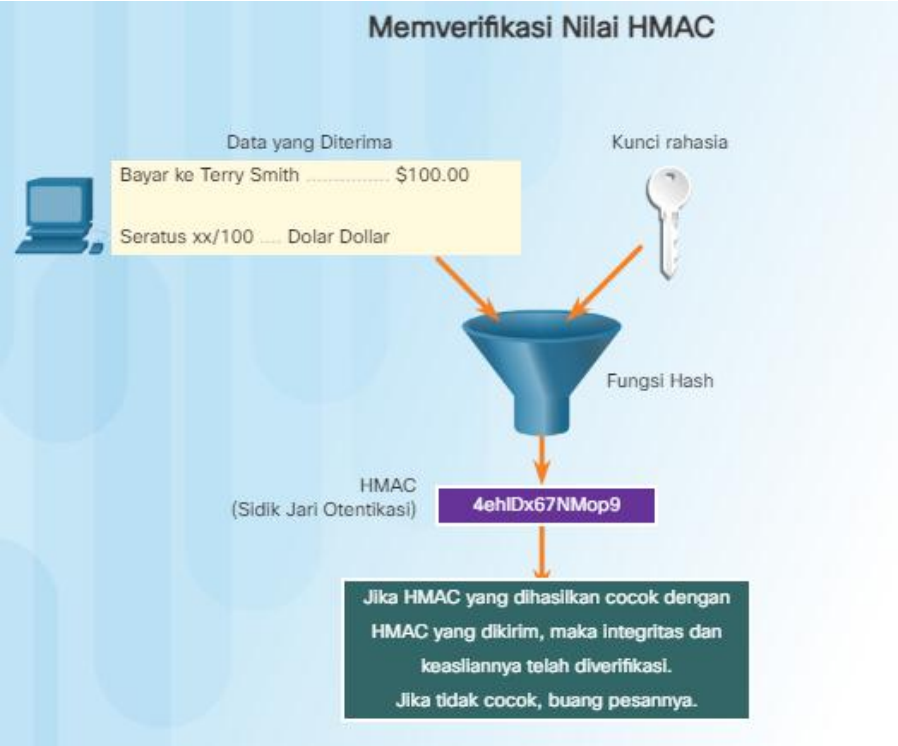
OPERASI HMAC

Pertimbangkan contoh di mana pengirim ingin memastikan bahwa pesan tetap tidak berubah dalam perjalanan dan ingin menyediakan cara bagi penerima untuk mengotentikasi asal pesan. Seperti yang ditunjukkan pada Gambar 8, perangkat pengirim memasukkan data (seperti gaji Terry Smith sebesar $100 dan kunci rahasia) ke dalam algoritma hashing dan menghitung intisari HMAC atau sidik jari dengan panjang tetap. Penerima mendapatkan sidik jari yang diautentikasi yang dilampirkan pada pesan. Pada Gambar 9, perangkat penerima menghapus sidik jari dari pesan dan menggunakan pesan teks biasa dengan kunci rahasianya sebagai input ke fungsi hashing yang sama. Jika perangkat penerima menghitung sidik jari yang sama dengan sidik jari

yang dikirim, pesan tersebut masih dalam bentuk aslinya. Selain itu, penerima mengetahui asal pesan karena hanya pengirim yang memiliki salinan kunci rahasia bersama. Fungsi HMAC membuktikan keaslian pesan.



Gambar 8. Menciptkan Nilai HMAC



Gambar 9. Verifikasi HMAC

PENERAPAN HMAC

HMAC juga dapat mengotentikasi pengguna web. Banyak layanan web menggunakan otentikasi dasar, yang tidak mengenkripsi nama pengguna dan kata sandi selama transmisi. Menggunakan HMAC, pengguna mengirimkan pengidentifikasi kunci pribadi dan HMAC. Server mencari kunci pribadi pengguna dan membuat HMAC. HMAC pengguna harus cocok dengan yang dihitung oleh server. VPN yang menggunakan IPsec mengandalkan fungsi HMAC untuk mengotentikasi asal setiap paket dan menyediakan pemeriksaan integritas data. Seperti yang ditunjukkan pada gambar, produk Cisco menggunakan hashing untuk otentikasi entitas, integritas data, dan tujuan keaslian data:

- Router Cisco IOS menggunakan hashing dengan kunci rahasia dengan cara seperti HMAC untuk menambahkan informasi otentikasi ke pembaruan protokol perutean.
- Gateway dan klien IPsec menggunakan algoritma hashing, seperti MD5 dan SHA-1 dalam mode HMAC, untuk memberikan integritas dan keaslian paket.
- Gambar perangkat lunak Cisco di Cisco.com memiliki checksum berbasis MD5 yang tersedia sehingga pelanggan dapat memeriksa integritas gambar yang diunduh.

Gambar 10. Penggunaan Hashing

TANDA TANGAN DIGITAL

Tanda tangan tulisan tangan dan stempel stempel membuktikan kepengarangan isi dokumen. Tanda tangan digital dapat memberikan fungsi yang sama seperti tanda tangan tulisan tangan. Dokumen digital yang tidak terlindungi sangat mudah diubah oleh siapa saja. Tanda tangan digital dapat menentukan apakah seseorang mengedit dokumen setelah pengguna

menandatanganinya. Tanda tangan digital adalah metode matematika yang digunakan untuk memeriksa keaslian dan integritas pesan, dokumen digital, atau perangkat lunak. Di banyak negara, tanda tangan digital memiliki kepentingan hukum yang sama dengan dokumen yang ditandatangani secara manual. Tanda tangan elektronik mengikat untuk kontrak, negosiasi, atau dokumen lain yang memerlukan tanda tangan tulisan tangan. Jejak audit melacak sejarah dokumen elektronik untuk tujuan pertahanan peraturan dan hukum. Sebuah tanda tangan digital membantu untuk membangun keaslian, integritas, dan non-penolakan. Tanda tangan digital memiliki properti khusus yang memungkinkan otentikasi entitas dan integritas data. Tanda tangan digital adalah alternatif untuk HMAC

Gambar 11. Properti Tanda Tangan Digital

Copyright © September 2023

Menolak berarti menyangkal. Non-repudiation adalah cara untuk memastikan bahwa pengirim pesan atau dokumen tidak dapat menyangkal telah mengirim pesan atau dokumen dan penerima tidak dapat menyangkal telah menerima pesan atau dokumen.

Tanda tangan digital memastikan bahwa pengirim menandatangani pesan atau dokumen secara elektronik. Karena tanda tangan digital adalah unik bagi individu yang membuatnya, orang tersebut nantinya tidak dapat menyangkal bahwa dia memberikan tanda tangan tersebut.

PROSES MEMBUAT TANDA TANGAN DIGITAL

Kriptografi asimetris adalah dasar untuk tanda tangan digital. Algoritma kunci publik seperti RSA menghasilkan dua kunci: satu pribadi dan yang lainnya publik. Kuncinya berhubungan secara matematis. Alice ingin mengirimi Bob email yang berisi informasi penting untuk peluncuran produk baru. Alice ingin memastikan bahwa Bob tahu bahwa pesan itu berasal darinya, dan bahwa pesan itu tidak berubah setelah dia mengirimnya. Alice membuat pesan bersama dengan intisari pesan. Dia kemudian mengenkripsi intisari ini dengan kunci pribadinya seperti yang ditunjukkan pada Gambar 1. Alice menggabungkan pesan, intisari pesan terenkripsi, dan kunci publiknya bersama-sama untuk membuat dokumen yang ditandatangani. Alice mengirimkan ini ke Bob seperti yang ditunjukkan pada Gambar 2. Bob menerima pesan itu dan membacanya. Untuk memastikan bahwa pesan tersebut berasal dari Alice, dia membuat intisari pesan dari pesan tersebut. Dia mengambil intisari pesan terenkripsi yang diterima dari Alice dan mendekripsinya menggunakan kunci publik Alice. Bob membandingkan intisari pesan yang diterima dari Alice dengan yang dihasilkannya. Jika mereka cocok, Bob tahu bahwa dia dapat

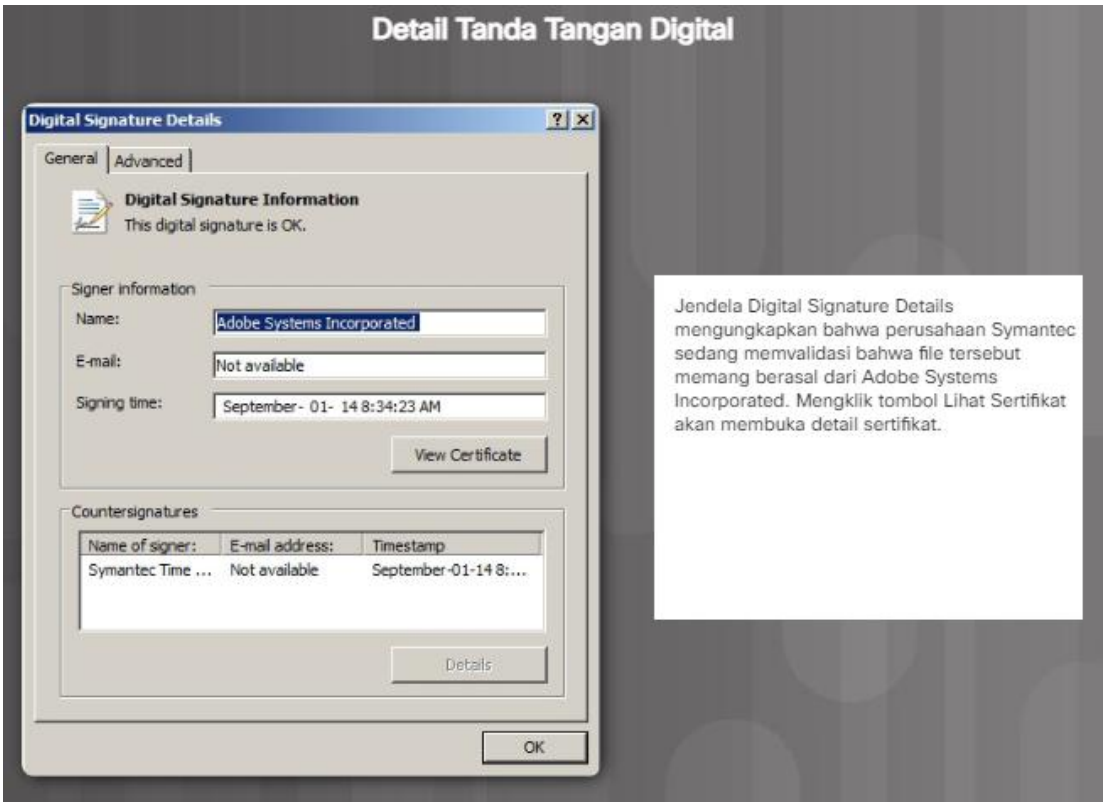
mempercayai bahwa tidak ada yang merusak pesan seperti yang ditunjukkan pada Gambar 3. Klik di sini untuk melihat video yang menjelaskan proses pembuatan sertifikat digital.

Gambar 12. Tanda Tangan Digital

MENGGUNAKAN TANDA TANGAN DIGITAL

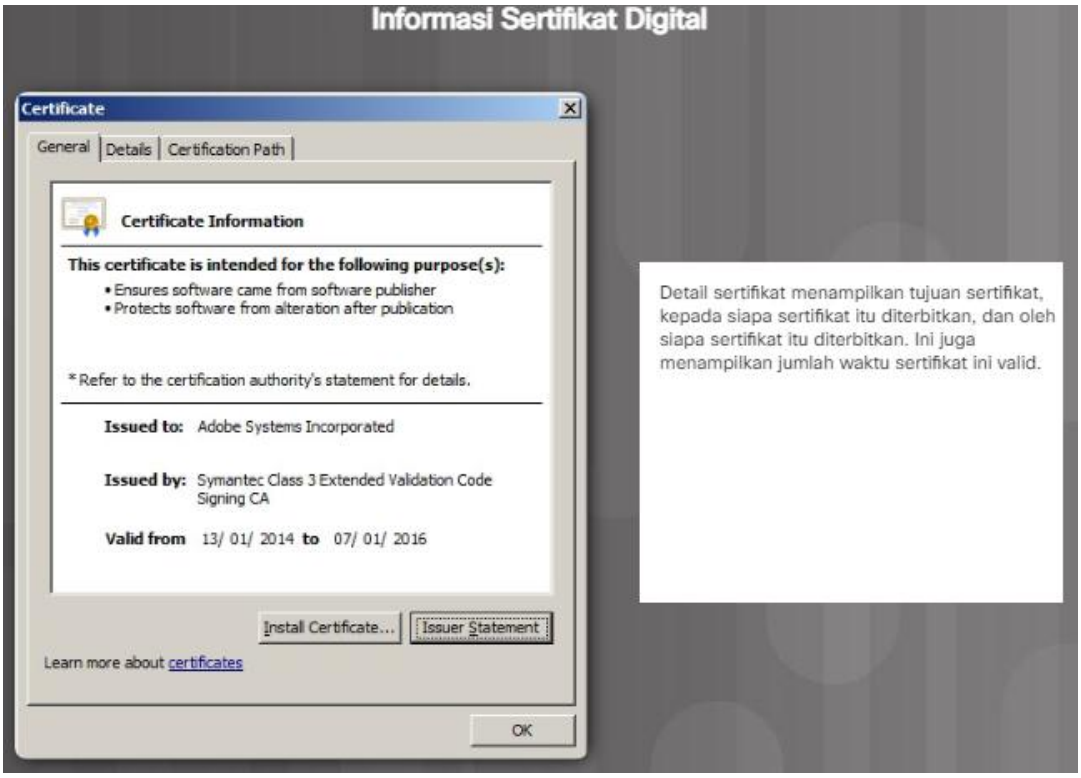
Menandatangani hash alih-alih seluruh dokumen memberikan efisiensi, kompatibilitas, dan integritas. Organisasi mungkin ingin mengganti dokumen kertas dan tanda tangan tinta dengan solusi yang memastikan dokumen elektronik memenuhi semua persyaratan hukum. Dua situasi berikut memberikan contoh penggunaan tanda tangan digital:

- Penandatanganan kode - Digunakan untuk memverifikasi integritas file yang dapat dieksekusi yang diunduh dari situs web vendor. Penandatanganan kode juga menggunakan sertifikat digital yang ditandatangani untuk mengotentikasi dan memverifikasi identitas situs (Gambar 13).



Gamba 13. Detail tanda tangan Resmi

- Sertifikat digital - Digunakan untuk memverifikasi identitas organisasi atau individu untuk mengotentikasi situs web vendor dan membuat koneksi terenkripsi untuk bertukar data rahasia (Gambar 14).



Gambar 14 Informasi Tanda Tangan Digital

MEMBANDINGKAN ALGORITMA TANDA TANGAN DIGITAL

Tiga algoritma tanda tangan digital yang umum adalah Digital Signature Algorithm (DSA), Rivest-Shamir-Adleman (RSA), dan Elliptic Curve Digital Signature Algorithm (ECDSA). Ketiganya menghasilkan dan memverifikasi tanda tangan digital. Algoritma ini bergantung pada enkripsi asimetris dan teknik kunci publik. Tanda tangan digital memerlukan dua operasi:

- Pembuatan kunci
- Verifikasi kunci

Kedua operasi memerlukan enkripsi dan dekripsi kunci.

DSA menggunakan faktorisasi bilangan besar. Pemerintah menggunakan DSA untuk menandatangani untuk membuat tanda tangan digital. DSA tidak melampaui tanda tangan ke

Copyright © September 2023

pesan itu sendiri. RSA adalah algoritma kriptografi kunci publik yang paling umum digunakan saat ini. RSA dinamai berdasarkan individu yang menciptakannya pada tahun 1977: Ron Rivest, Adi Shamir, dan Leonard Adleman. RSA bergantung pada enkripsi asimetris. RSA mencakup penandatanganan dan juga mengenkripsi konten pesan. DSA lebih cepat dari RSA sebagai layanan penandatanganan untuk dokumen digital. RSA paling cocok untuk aplikasi yang memerlukan penandatanganan dan verifikasi dokumen elektronik dan enkripsi pesan. Seperti kebanyakan bidang kriptografi, algoritma RSA didasarkan pada dua prinsip matematika; modulus dan faktorisasi bilangan prima. Klik di sini untuk mempelajari lebih lanjut tentang bagaimana RSA menggunakan modulus dan faktorisasi bilangan prima. ECDSA adalah algoritma tanda tangan digital terbaru yang secara bertahap menggantikan RSA. Keuntungan dari algoritma baru ini adalah dapat menggunakan ukuran kunci yang jauh lebih kecil untuk keamanan yang sama dan membutuhkan perhitungan yang lebih sedikit daripada RSA.