TUGAS 3

“RESUME KEAMANAN SISTEM KOMPUTER”

DI SUSUN OLEH :

NAMA : ANDI AMANDA ANDI T.

NIM : F551 22 034

KELAS : TI A

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS TADULAKO

PALU

2023

A. User Authentication

Dalam sebagian konteks keamanan komputer autentikasi pengguna adalah blok bangunan fundamental dan garis pertahanan utama, dimana otentikasi penggunan adalah dasar untuk sebgagian besar jenis kontrol akses dan akuntabilias pengguna, yang mana RFC 4949 mendifinisikan autentikasi pengguna

1. ELECTRONIC USER AUTHENTICATION PRINCIPLES

   NIST SP 800-63-2 (panduan Otentikasi Elektronik, Agustus 2013) mendefinisikan otentikasi pengguna secara elektronik sebagai proses membangun keperayaan pada identitas pengguna yang disajikan secara eletronik ke sistem informasi, dimana sistem tersebut dapat menggunakan identitas yang diautentikasi untuk menetukan apakah individy yang diautentikasi memiliki wewenang untuk melakukan fungsi tertentu, seperti basis data atau akases ke sumber daya sistem

   a. Model For Electronic User Authentication

      SP 800-63-2 mendefiniskan model umum untuk autentiasi pengguna yang melibatkan sejumlah entitas dan prosedur, persayaratan awal dalam melakukan autentikasi pengguna adalah bahwa pengguna harus terdaftar pada sistem, dimana urutan mendaftarnya adalah pemohon doharapkan untukmendaftar ke otoritas pendaftaran (RA) untuk menjadi pelanggan dari penyedia layanan kepercyaan (CSP), dalam model inin RA adalah entitas terpercaya yang menetapkan dan menjamin identitas pemohon kepada CSP, lalu CSP melakukan pertukaran dengan pelanggan nanyinya semua bergantung pada datil sistem otentikasi keseluruhan dan CSP mengeluarkan semacam kredensial, kredensial merupakan struktur data yang secara otomatis mengikat identitas dan atrinut tambahan ke token yag dimiliki oleh elanggan dan diapat diverifikasi ketika dipresentasikan

   b. Means of Authentication

      Terdapat 4 cara umum untuk mengautetikasi identitas pengguna yaitu :

      1. Sesuatu yang diketahui individy : contohnya adalah kata sandi, nomor identifikasi pribadi(PIN), atau jawaban atas serangkaian pertnayaan yan sebelumnya telah diatur sebelumnya

2. Seuatu yang dimiliki oleh individu contohnya adalah termasuk kartu pintar, dan kunci fisik, yang jenis pengautentikaskannya diebut sebagai token
3. Sesuatu yang dimiliki oleh individu(biometrik ststis) contohnya yaitu pengenalan dengan sidik jari retina dan wajah
4. Sesuatu yang dilakukan individu(biometrik dinamis) contohnya termasuk melalui pola suara, karaktersitik tulis tangan dan ritme mengtik

Apabila semua metode ini dilakukan dan digunakan dengan benar maka dapat memberikan autentikasi pengguna yang aman. Namun setiap metode memiliki masalah dengan hal ini ada beberapa contoh spesifik yang berhubungan dengan autentikasi pengguna yaitu :

1. Tingkat, dimana tingkat kepastian yang menggambarkan tingkat kepastian organisisi bahwa penguna telah memberikan kardensial yang mengacu pada identitasnya SP 800-63-2 mengakui empat tingkat jaminan yaitu :
   • Level 1: Sedikit atau tidak ada kepercayaan terhadap keabsahan identitas yang dinyatakan. Contoh di mana tingkat ini sesuai adalah konsumen yang mendaftar untuk berpartisipasi dalam diskusi di papan diskusi situs web perusahaan. Teknik otentikasi yang umum digunakan pada tingkat ini adalah ID dan kata sandi yang disediakan pengguna pada saat transaksi.
   • Tingkat 2: Beberapa keyakinan terhadap keabsahan identitas yang dinyatakan. Kepercayaan tingkat 2 sesuai untuk berbagai macam bisnis dengan publik di mana organisasi memerlukan pernyataan identitas awal (rinciannya diverifikasi secara independen sebelum melakukan tindakan apa pun). Pada tingkat ini, beberapa jenis protokol autentikasi yang aman perlu digunakan, bersama dengan salah satu cara autentikasi yang telah dirangkum sebelumnya dan dibahas di bagian selanjutnya.

• Level 3: Keyakinan tinggi terhadap keabsahan identitas yang diberikan. Tingkat ini sesuai untuk memungkinkan klien atau karyawan mengakses layanan terbatas yang bernilai tinggi namun bukan yang tertinggi. Contoh yang sesuai dengan level ini: Seorang pengacara paten secara elektronik mengirimkan informasi paten rahasia ke Kantor Paten dan Merek Dagang AS. Pengungkapan yang tidak tepat akan memberikan keunggulan kompetitif bagi pesaing. Teknik yang perlu digunakan pada tingkat ini membutuhkan lebih dari satu faktor otentikasi; yaitu, setidaknya dua teknik otentikasi independen harus digunakan.

• Tingkat 4: Keyakinan yang sangat tinggi terhadap keabsahan identitas yang diberikan. Tingkat ini sesuai untuk memungkinkan klien atau karyawan mengakses layanan terbatas yang bernilai sangat tinggi atau yang jika diakses secara tidak benar akan sangat berbahaya. Sebagai contoh, seorang pejabat penegak hukum mengakses database penegakan hukum yang berisi catatan kriminal. Akses yang tidak sah dapat menimbulkan masalah privasi dan/atau membahayakan penyelidikan. Biasanya, autentikasi level 4 memerlukan penggunaan beberapa faktor serta pendaftaran secara langsung.

2. Potensial Impact

   Sebuah konsep yang terkait erat dengan tingkat jaminan adalah dampak potensial. FIPS 199 (Standar Kategorisasi Keamanan Informasi dan Sistem Informasi Federal, 2004) mendefinisikan tiga tingkat dampak potensial pada organisasi atau individu jika terjadi pelanggaran keamanan (dalam konteks kami, kegagalan dalam otentikasi pengguna):

   - Rendah: Kesalahan autentikasi dapat diperkirakan memiliki efek buruk yang terbatas pada operasi organisasi, aset organisasi, atau individu. Secara lebih spesifik dimana kesalaha tersebut dapat dikatakan sebagai penyebab degradasai dalam misi kemampuan sampai pada tingkat

dan durasi tertentu sehingga organisasi dapat menjalankan fungsi utamanya, mengakibatkan kerusakan kecil pada aset organisasi, mengakibatkan kerugian finansial kecil pada organisasi atau individu, dan yang terakir mengakibatkan kerugian kecil pada individu

- Sedang: Kesalahan otentikasi dapat diperkirakan akan menimbulkan dampak buruk yang serius. Lebih khusus lagi, kesalahan tersebut dapat: (1) menyebabkan penurunan yang signifikan dalam kemampuan misi sampai pada tingkat dan durasi dimana organisasi dapat menjalankan fungsi utamanya, namun efektivitas fungsi tersebut berkurang secara signifikan; (2) mengakibatkan kerusakan yang signifikan pada aset organisasi; (3) mengakibatkan kerugian finansial yang signifikan; atau (4) mengakibatkan kerugian yang signifikan terhadap individu yang tidak melibatkan hilangnya nyawa atau cedera serius yang mengancam jiwa.
- Tinggi: Kesalahan otentikasi dapat diperkirakan akan menimbulkan dampak buruk yang parah atau sangat parah. Kesalahan tersebut dapat: (1) menyebabkan degradasi yang parah atau hilangnya kemampuan misi hingga pada tingkat dan durasi tertentu sehingga organisasi tidak dapat menjalankan satu atau lebih fungsi utamanya; (2) mengakibatkan kerusakan besar pada aset organisasi; (3) mengakibatkan kerugian finansial yang besar bagi organisasi atau individu; atau (4) mengakibatkan kerusakan parah atau bencana pada individu yang melibatkan hilangnya nyawa atau cedera serius yang mengancam jiwa.

3. Areas Of Risk

Pemetaan antara potensi dampak dan tingkat asurans yang sesuai dan juga memuaskan untuk menangani potensi dampak tergantung pada konteksnya. Dimana pemetaan yang memungkinkan untuk berbagai risiko yang mungkin dihadapi oleh organisasi. Tabel ini menunjukkan teknik untuk melakukan penilaian risiko. Untuk sistem informasi atau aset layanan tertentu dari sebuah organisasi, organisasi perlu menentukan tingkat dampak jika terjadi kegagalan otentikasi, dengan menggunakan kategori dampak, atau area risiko, yang menjadi perhatian.

	Profil Dampak Tingkat Jaminan			
Kategori Dampak Potensial untuk Kesalahan Otentikasi	**1**	**2**	**3**	**4**
Ketidaknyamanan, tekanan, atau kerusakan pada kedudukan atau reputasi	Rendah	Mod	Mod	Tinggi
Kerugian finansial atau kewajiban organisasi	Rendah	Mod	Mod	Tinggi
Membahayakan program atau kepentingan organisasi	Tidak	Renda	Mod	Tinggi
	ada	h		
Pelepasan informasi sensitif yang tidak sah	Tidak ada	Rendah	Mod	Tinggi
Keamanan pribadi	Tidak ada	Tidak ada	Rendah	Mod/ Tinggi
Pelanggaran perdata atau pidana	Tidak ada	Rendah	Mod	Tinggi

Sebagai contoh, dapat dipertimbangkan potensi kerugian finansial jika terjadi kesalaha autentikasi yang menyebabkan akses tidak sah ke basis data, diaman terdapat beberapa dampak yaitu :

- Rendah: Paling buruk, kerugian finansial yang tidak signifikan atau tidak penting yang tidak dapat dipulihkan kepada pihak mana pun, atau paling buruk, tanggung jawab organisasi yang tidak signifikan atau tidak penting
- Sedang: Paling buruk, kerugian finansial serius yang tidak dapat dipulihkan kepada pihak mana pun, atau tanggung jawab organisasi yang serius.
- Tinggi: kerugian finansial yang parah atau bencana yang tidak dapat dipulihkan kepada

pihak mana pun; atau tanggung jawab organisasi yang parah atau bencana.

2. Password-Based Authentication

Garis pertahanan yang banyak digunakan untuk melawan penyusup adalah sistem kata sandi. Hampir semua sistem multiuser, server berbasis jaringan, situs e-commerce berbasis Web, dan layanan serupa lainnya mengharuskan pengguna untuk memberikan tidak hanya nama atau pengenal (ID), tetapi juga kata sandi. Sistem membandingkan kata sandi dengan kata sandi yang telah disimpan sebelumnya untuk ID pengguna tersebut, yang disimpan dalam file kata sandi sistem. Kata sandi berfungsi untuk mengautentikasi ID individu yang masuk ke sistem. Pada gilirannya, ID memberikan keamanan dengan cara berikut:

- ID menentukan apakah pengguna berwenang untuk mendapatkan akses ke sistem. Pada beberapa sistem, hanya mereka yang telah memiliki ID yang diajukan pada sistem yang diizinkan untuk mendapatkan akses
- ID menentukan hak istimewa yang diberikan kepada pengguna. Beberapa pengguna mungkin memiliki status pengawas atau "superuser" yang memungkinkan mereka untuk membaca file dan melakukan fungsi yang secara khusus dilindungi oleh sistem operasi. Beberapa sistem memiliki akun tamu atau anonim, dan pengguna akun ini memiliki hak istimewa yang lebih terbatas daripada yang lain.
- ID digunakan dalam apa yang disebut sebagai kontrol akses diskresioner. Sebagai contoh, dengan mencantumkan ID pengguna lain, seorang pengguna dapat memberikan izin kepada mereka untuk membaca file yang dimiliki oleh pengguna tersebut.

a. Kerentanan kata sandi

Dapat diidentifikasikan startegi serangan dan tindakan pencegahan berikut:

- Serangan kamus offline
- Serangan akun terentu
- Serangan kata sandi populer
- Menebak kata sandi terhdapap pengguna tunggal
- Pembajakan stasiun kerja
- Mengeksploitasi kesalahan pengguna
- Mengekspliotasi penggunaan kata sandi ganda

- Pemantauan elektronik

b. Penggunaan kata sandi ter-hash

Teknik keamanan kata sandi yang banyak digunakan adalah penggunaan kata samdi terh-hash, skeman ini ditemukan pada hampir setiap varian UNIX dan sejumlah sistem operasi lainnya. Untuk memasukkan password batu ke dalam sistem pengguna harus memeilih atau diberi pasword, kata sandi digabungkan dengan nilai garam denngan tetap panjang [MORR 79] , dan ketika pengguna mencoba masuk ke sistem UNIX, pengguna harus memnerikan ID dan password yang tujuan untuk mengindeks kedalam tabel

Garam memiliki tiga dungsi yaitu:

- Hal ini mencegah kata sandi duplikat terlihat di file kata sandi. Bahkan jika dua pengguna memilih kata sandi yang sama, kata sandi tersebut akan diberikan nilai salt yang berbeda. Oleh karena itu, kata sandi ter-hash dari kedua pengguna akan berbeda.
- Ini sangat meningkatkan kesulitan serangan kamus offline. Untuk garam dengan panjang b bit, jumlah kata sandi yang mungkin bertambah dengan faktor 2 b , meningkatkan kesulitan menebak kata sandi dalam serangan kamus
- Hampir tidak mungkin untuk mengetahui apakah seseorang yang memiliki kata sandi di dua atau lebih sistem telah menggunakan kata sandi yang sama di semua sistem tersebut

c. Implementasi UNIX

Awal dari perkembangan UNIX sebagian besar implemntasi mengandalkan skema kata sandi , setiap pengguna memilih kata sandi hingga 8 karakter dari 8 karakter ini dikonversi menjadi nilai 56 bit menggunakan ASCII -bit yang berfungsi untuk input kunci untuk rutinitas enkripsi. Dan rutinitas I I dikenal sebagai cryot yang didasari oleh DES. Lalu sebuah nilai garam 12-bit digunakan maka algoritma DES yang dimodifikasi akan dieksekusi dengan input data yang terdiri dari sebuah blok 64-bit yang dihasilkan kemudian diterjemahkan kedalam urutan 11 karakter, karena modifikasi DES maka akan mengubahnya

menjadi senuah fungsi hash satu arah. Hash yang direkomndasikan yaitu linux, solaris, dan FreeBSD

3. Token-Based Authentication

Benda yang dimilik oleh pengguna yang tujuannya untuk otentikasi pengguna disebut token

a. Kartu Memori

Kartu memori dapat menyimpan tetapi tidak dapat memproses data, dimana kartu yang paling umu adalah kartu bank dengan strip magnetik di bagian belakangnya

Jenis Kartu	Fitur Penentu	Contoh
Timbul	Hanya karakter yang dibesarkan, di bagian depan	Kartu kredit lama
Strip magnetik	Bilah magnet di belakang, karakter di depan	Kartu bank
Memori	Memori elektronik di dalam	Kartu telepon prabayar
Kontak Pintar Tanpa Kontak	Memori elektronik dan prosesor di dalam Kontak listrik yang terpapar di permukaan Antena radio tertanam di dalam	Kartu identitas biometrik

Kartu memeori dapat digunakan pro=ibadi untuk akses fisik seperti kamar hotel, untuk autentikasi pengguna memberikan kartu memori dan beberapa bentuk sandi atau nomor identifikasi pribadi

b. Kartu pintar

Berbagai macam perangkat memenuhi syarat sebagai token pintar. Ini dapat dikategorikan dalam empat dimensi yang tidak saling terpisah:

• Karakteristik fisik: Token pintar memiliki mikroprosesor tertanam. Token pintar yang terlihat seperti kartu bank disebut kartu pintar. Token pintar lainnya dapat terlihat seperti kalkulator, kunci, atau benda portabel kecil lainnya.

• Antarmuka pengguna: Antarmuka manual termasuk keypad dan tampilan untuk interaksi manusia/token.

• Antarmuka elektronik: Kartu pintar atau token lainnya memerlukan antarmuka elektronik untuk berkomunikasi dengan pembaca/penulis yang kompatibel. Sebuah kartu dapat memiliki salah satu atau kedua jenis antarmuka berikut ini:

- Kontak: Kartu pintar kontak harus dimasukkan ke dalam pembaca kartu pintar dengan koneksi langsung ke pelat kontak konduktif pada permukaan kartu (biasanya berlapis emas). Transmisi perintah, data, dan status kartu berlangsung melalui titik kontak fisik ini.

-Tanpa kontak: Kartu nirkontak hanya memerlukan kedekatan dengan pembaca. Baik pembaca maupun kartu memiliki antena, dan keduanya berkomunikasi menggunakan frekuensi radio. Sebagian besar kartu nirkontak juga mendapatkan daya untuk chip internal dari sinyal elektromagnetik ini. Kisarannya biasanya satu setengah hingga tiga inci untuk kartu yang tidak bertenaga baterai, ideal untuk aplikasi seperti pintu masuk gedung dan pembayaran yang membutuhkan antarmuka kartu yang sangat cepat.

• Protokol otentikasi: Tujuan dari smart token adalah untuk menyediakan sarana autentikasi pengguna. Kita dapat mengklasifikasikan protokol otentikasi yang digunakan dengan smart token ke dalam tiga kategori:

-Statis: Dengan protokol statis, pengguna mengautentikasi dirinya sendiri ke token dan kemudian token mengautentikasi pengguna ke komputer. Paruh terakhir dari protokol ini mirip dengan pengoperasian token memori

4. Biometric Authentication

Sistem autentikasi biometrik mencoba mengautentikasi seseorang berdasarkan karakteristik fisiknya yang unik, dan karakteristik ini merupakan statis seperti sidik jari, geomteri tangan, karakteristik wajah, serta pola terina dan iris mata sementara karakteristik dinamis seperti sidik suara, dan tanda tangan

a. Karakteristik fisik yang digunakan dalam aplikasi biometrik
   - Karakterisiktik wajah
   - Sidik jari
   - Geomtri tangan
   - Pola retina
   - Iris
   - Tanda tangan
   - Suara

b. Pengoprasian sistem otentikasi biometrik

Setiap individu yang akan dimasukkan ke dalam basis data pengguna yang berwenang harus terlebih dahulu terdaftar dalam sistem, hal ini serupa dengan memberikan kata sandi kepada pengguna Tergantung pada aplikasinya, autentikasi pengguna pada sistem biometrik melibatkan verifikasi atau identifikasi. Verifikasi dianalogikan dengan

pengguna yang masuk ke sistem dengan menggunakan kartu memori atau kartu pintar yang digabungkan dengan kata sandi atau PIN. Untuk verifikasi biometrik, pengguna memasukkan PIN dan juga menggunakan sensor biometrik. Sistem mengekstrak fitur yang sesuai dan membandingkannya dengan template yang disimpan untuk pengguna ini. Jika ada kecocokan, maka sistem akan mengautentikasi pengguna ini. Untuk sistem identifikasi, individu menggunakan sensor biometrik tetapi tidak memberikan informasi tambahan. Sistem kemudian membandingkan templat yang disajikan dengan kumpulan templat yang tersimpan. Jika ada kecocokan, maka pengguna tersebut diidentifikasi. Jika tidak, maka pengguna ditolak

c. Akurasi Biometrik

Dalam skema biometrik apa pun, beberapa karakteristik fisik individu dipetakan ke dalam representasi digital. Untuk setiap individu, satu representasi digital, atau template, disimpan dalam komputer. Ketika pengguna akan diautentikasi, sistem membandingkan template yang tersimpan dengan template yang ditampilkan. Mengingat kompleksitas karakteristik fisik, kita tidak dapat berharap bahwa akan ada kecocokan yang tepat antara kedua template. Sebaliknya, sistem menggunakan algoritme untuk menghasilkan skor pencocokan (biasanya berupa angka tunggal) yang mengukur kesamaan antara input dan templat yang tersimpan. Untuk melanjutkan pembahasan, kami mendefinisikan istilah-istilah berikut ini. Tingkat kecocokan palsu adalah frekuensi sampel biometrik dari sumber yang berbeda dinilai secara keliru berasal dari sumber yang sama. Tingkat ketidakcocokan palsu adalah frekuensi sampel dari sumber yang sama dinilai secara keliru berasal dari sumber yang berbeda. Sebagai contohnya dalam kasus sidik jari, hasilnya dapat bervariasi karena kebisingan sensor, perubahan sidik jari karena membengkak atau kering, penempatan jari dan lainnya oleh karena itu setiap individu memili skor pencocokan yang jauh lebih rendah

5. Remote User Authentication

a. Protokol kata sandi

Dimana dalam pembahasan ini menyediakan contoh sedrahana yaitu tentang protokol tantangan-respons untuk

autentikasi melalui kata sandi, dimana protokol yang sebenarnya lebih kompleks seperti kerberos yan membahas pengguna pertama-tama mengirimkan identitasnya ke remote host, dan selanjutnya hist menghasilkan angka acak r yang diesebut nonce dan nantiya akan mengembalikan nonce kepada pengguna

b. Protokol biometrik statis

Dalam cara kerjanya sama sperti sebelumnya dimana pengguna mengirimkan ID ke host yang merespon sebuah angak acak r dan dalam hal ini pengenal untuk enkripsi E(), dalam sisis oengguna terdapat sebuah sistem kilen tem yang mengontrol pernagkat biometrik

c. Protokol Biometrik Dinamis

Dimana melihatkan protokol autentikasi pengguna yang menggunakan biomterik dinamis, perbedaan utama dari kasusu biometrik stabil adalah bahwa host menyediakan urutan acak serta nomor acal sebagai tantangan , tatangan tersebut harus menyuarakan verifikasi pembicara, mengetik, atau menulis dan uurtan tersebut akan menghabsilkan sinyal biometrik BS'(x')

6. Security Issues For Usesr Authentication

Seperti hal nya layanan keamanan lainnya autentikasi pengguna terutama autentikasi pengguna jarak jauh dpaat diserang dengan berbagai macam serangan , autentikasi pengguan tanpa akses ke host jarak jauh atau ke jalur komunikasi yang mengintervensi, musuh mencoba untuk menyamar sebagai pengguna yang sah. Untuk sistem bebrasis kata sandi, musuh mengkin mencoba menebak kata sandi. kata sandi seperti itu memiliki entropi yang besar; yaitu, banyak bit yang diperlukan untuk mewakili kata sandi. Tindakan pencegahan lainnya adalah dengan membatasi jumlah percobaan yang dapat dilakukan dalam periode waktu tertentu dari sumber tertentu. Sebuah token dapat menghasilkan sebuah kode sandi dengan entropi tinggi dari PIN atau kata sandi dengan entropi rendah, sehingga menggagalkan pencarian yang mendalam. Musuh mungkin dapat menebak atau mendapatkan PIN atau kata sandi, namun juga harus mendapatkan token fisik untuk berhasil. Serangan host diarahkan pada file pengguna di host tempat kata sandi, kode sandi token, atau templat biometrik disimpan. Dalam cara kerjanya

membahas pertimbangan keamanan sehubungan dengan kata sandi. Untuk token, ada pertahanan tambahan dengan menggunakan kode sandi satu kali, sehingga kode sandi tidak disimpan di file kode sandi host. Fitur biometrik dari seorang pengguna sulit untuk diamankan karena merupakan fitur fisik dari pengguna. Untuk fitur statis, o t e n ti k a si perangkat biometrik menambahkan ukuran perlindungan. Untuk fitur dinamis, protokol respons-tantangan meningkatkan keamanan. Menguping dalam konteks kata sandi mengacu pada upaya musuh untuk mempelajari kata sandi dengan mengamati pengguna, menemukan salinan tertulis dari kata sandi, atau beberapa serangan serupa yang melibatkan kedekatan fisik antara pengguna dan musuh. Bentuk lain dari penyadapan adalah pencatatan keystroke (keylogging), di mana perangkat keras atau perangkat lunak berbahaya dipasang sehingga penyerang dapat menangkap keystroke pengguna untuk dianalisis kemudian. Sebuah sistem yang bergantung pada beberapa faktor (misalnya, kata sandi plus token atau kata sandi plus biometrik) tahan terhadap jenis serangan ini. Untuk sebuah token, ancaman yang serupa adalah pencurian token atau penyalinan fisik token. Sekali lagi, protokol multifaktor lebih tahan terhadap jenis serangan ini daripada protokol token murni. Ancaman analog untuk protokol biometrik adalah menyalin atau meniru parameter biometrik untuk menghasilkan template yang diinginkan. Biometrik dinamis tidak terlalu rentan terhadap serangan semacam itu. Untuk biometrik statis, otentikasi perangkat adalah tindakan pencegahan yang berguna. Serangan replay melibatkan musuh yang mengulangi respons pengguna yang ditangkap sebelumnya. Penanggulangan yang paling umum untuk serangan semacam itu adalah protokol respons tantangan. Dalam serangan Trojan horse, sebuah aplikasi atau perangkat fisik menyamar sebagai aplikasi atau perangkat otentik dengan tujuan menangkap kata sandi, kode sandi, atau biometrik pengguna. Musuh kemudian dapat menggunakan informasi yang ditangkap untuk menyamar sebagai pengguna yang sah. Contoh sederhana dari hal ini adalah mesin bank jahat yang digunakan untuk menangkap kombinasi ID pengguna/kata sandi. Serangan penolakan layanan mencoba untuk menonaktifkan layanan otentikasi pengguna dengan membanjiri layanan dengan banyak percobaan otentikasi. Serangan yang lebih selektif menolak layanan untuk pengguna tertentu dengan mencoba masuk sampai ambang batas tercapai yang menyebabkan penguncian pada pengguna ini

karena terlalu banyak percobaan masuk. Protokol autentikasi multifacet yang menyertakan token menggagalkan serangan ini, karena musuh harus mendapatkan token terlebih dahulu.