Authentication, Authorization, and Accounting (AAA)
&
Access Control

Agung Brastama Putra

- AAA merupakan singkatan yang diakui secara universal dalam keamanan informasi dunia.
- Masalahnya adalah bahwa banyak orang sering keliru tentang apa tiga A.
- 3 A adalah Otentikasi, Otorisasi, dan Akuntable.
- Banyak orang berpikir 3 A adalah Otentikasi, Otorisasi, dan Access Control.
- Akses kontrol erat terkait dengan otentikasi dan otorisasi, tetapi bukan bagian dari triple A keamanan informasi.

Authentication

- Sebelum Anda memberikan akses pengguna ke lingkungan Anda, pertama anda ingin pastikan, Anda tahu siapa pengguna yang masuk.
- Otentikasi digunakan untuk memverifikasi identitas pengguna.
- Otentikasi dapat dibagi menjadi dua komponen: identifikasi dan verifikasi.

Pengertian Secara Harfiah

- Otentikasi adalah verifikasi apakah seseorang itu adalah orang yang berhak.
- Biasanya melibatkan username dan password, tapi dapat menyertakan metode lain yang menunjukan identitas, seperti kartu pintar, sidik jari, dll.

- Jenis-Jenis Otentikasi

1. Mutual Authentication
2. Multifactor Authentication
3. Claims-Based Authentication

Mutual Authentication

- Umumnya, dalam sistem otentikasi, Anda dapat mempertimbangkan satu sistem klien dan sistem lain server. Biasanya, server mengotentikasi klien.
- Tapi bagaimana dengan server? Bagaimana klien yakin bahwa server yang dikatakannya itu?
- Jika identitas server tidak diverifikasi, maka mungkin server dapat dipalsukan.
- Kemudian, klien dapat mengirimkan mandat untuk sebuah entitas berbahaya.
- Di sinilah saling otentikasi masuk dalam skenario otentikasi bersama, baik klien dan server yang dikonfirmasi.

Multifactor Authentication

- Ada tiga otentikasi faktor yang dapat digunakan: sesuatu yang Anda tahu, sesuatu anda miliki, dan sesuatu yang melekat dengan anda.
- Sesuatu yang Anda tahu akan menjadi password, ulang tahun atau beberapa informasi pribadi lainnya.
- Sesuatu yang anda miliki akan menjadi satu kali penggunaan token, kartu pintar atau beberapa artefak lain yang mungkin anda miliki di fisik Anda.
- Sesuatu yang melekat dengan anda akan menjadi identitas biometrik Anda, seperti sidik jari atau pola bicara

- Agar dianggap otentikasi multifaktor, maka harus menggunakan setidaknya dua dari tiga faktor yang disebutkan tadi.

Claims-Based Authentication

- Berbasis Klaim otentikasi adalah metode untuk menyediakan cross-platform otentikasi dan single sign-on.
- Seorang pengguna untuk mengotentikasi satu penyedia otentikasi, dan identitas nya kemudian dibawa ke sebuah aplikasi atau layanan yang mungkin menggunakan otentikasi penyedia yang berbeda.

- Contohnya
- Aplikasi yang melakukan verifikasi keaslian produknya menggunakan Token/donggel, apabila tidak ada token maka aplikasi tersebut tidak bisa dipakai.

Compatible with:
USB B type and Parallel port (IEEE 1284 Port).

www.sjtweb.net

Advanced Authentication Types

- Berikut ini adalah beberapa metode otentifikasi

PAP

- PAP Password Authentication Protokol. sebelum otentikasi terjadi, PAP menggunakan hubungan untuk membuat sambungan
  antara klien dan server.
- Setelah koneksi telah ditetapkan, username dan password kemudian dikirim melalui koneksi dalam bentuk teks.
- Transmisi ini jelas teks username dan password adalah salah satu alasan mengapa PAP dianggap oleh sebagian besar menjadi sebuah protokol tidak aman.
- password ditransmisikan dalam bentuk teks dapat dicuri menggunakan sniffer jaringan dasar.
- Jadi Anda harus berhati-hati jika Anda memilih untuk menggunakan PAP di lingkungan Anda.

CHAP

- CHAP is the Challenge Handshake Authentication Protocol
- CHAP dianggap lebih aman daripada PAP.
- CHAP menggunakan threeway sebuah hubungan saat membuat koneksi.
- Setelah link dibentuk, server akan mengirim tantangan kembali ke klien.
- Klien kemudian merespon dengan nilai hash. Server akan kemudian memeriksa nilai ini terhadap nilai yang dihitung dengan menggunakan hash. Jika nilai adalah sama, maka sambungan dibuat.
- Karena nilai hash yang dikirim bukan yang sebenarnya password, proses koneksi dianggap lebih aman.

EAP

- EAP is the Extensible Authentication Protocol
- EAP digunakan dalam dial-up, point-to-point, dan koneksi LAN.
- Bagaimanapun EAP, sebagian besar adalah terlihat saat ini pada sambungan LAN nirkabel. EAP lebih dari sekedar sebuah protokol, melainkan lebih dari kerangka kerja.
- Kerangka EAP terdiri dari beberapa metode otentikasi.
- Beberapa yang paling sering digunakan adalah EAP-TLS, PEAP, dan LEAP.

LDAP

- LDAP is the Lightweight Directory Access Protocol.
- Ada beberapa kesalahpahaman ketika membahas LDAP dalam konteks otentikasi.
- LDAP sebenarnya adalah protokol yang digunakan untuk query direktori.
- Ketika LDAP digunakan untuk otentikasi, apa yang sebenarnya terjadi adalah bahwa LDAP digunakan untuk mengakses direktori di mana kepercayaan pengguna disimpan.

- Aplikasi atau sistem yang otentik kemudian akan melakukan yang sebenarnya otentikasi.
- Kadang-kadang, ada kekhawatiran atas keamanan menggunakan LDAP untuk komunikasi dengan direktori.
- Untuk mengatasi masalah ini, Anda dapat menggunakan LDAP melalui SSL atau LDAPS.
- Dengan LDAPS, LDAP komunikasi ke direktori dienkripsi menggunakan SSL.
- Dengan LDAPS, Anda harus memastikan struktur sertifikat tidak di tempat.

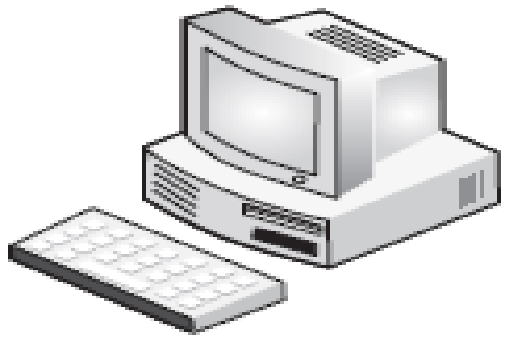
Karberos

- Kerberos adalah sistem otentikasi tiket berbasis.
- Hal ini didasarkan pada penggunaan kunci simetrik.
- Kerberos menggunakan tiket untuk menyediakan otentikasi ke sumber daya, bukan password.
- tiket ini membantu menyelesaikan ancaman mencuri password melalui jaringan sniffing. Untuk membantu menyediakan lingkungan yang aman, Kerberos menggunakan saling
  otentikasi.
- Dalam Otentikasi Reksa, baik server dan klien harus disahkan. Ini membantu mencegah serangan menengah dan spoofing.
- Komponen utama dalam sistem Kerberos adalah Kunci Distribusi Center, Layanan Tiket-Pemberian, dan tiket-Pemberian tiket.

- Key Distribution Center : The Key Distribution Center (KDC) adalah pusat dari proses Kerberos.
- KDC ini memiliki database tombol yang digunakan dalam proses otentikasi. KDC ini terdiri dari dua utama bagian: Layanan Otentikasi dan Tiket Layanan

- Layanan Otentikasi adalah apa mengotentikasi klien.
- Layanan Pemberian-Tiket adalah apa yang menyediakan tiket dan Pemberian-Tiket ke sistem klien. Pemberian-Tiket berisi ID klien, alamat jaringan klien, masa berlaku tiket, dan Pemberian-Tiket kunci Session Server

- Langkah-langkah berikut menguraikan proses Otentikasi Kerberos,
  1. Pengguna memasukkan nama pengguna nya dan password di sistem klien.
  2. Klien menggunakan hash satu arah untuk menutupi password. hash ini satu arah dianggap sebagai rahasia klien.



Client

Username sent to Auth Server

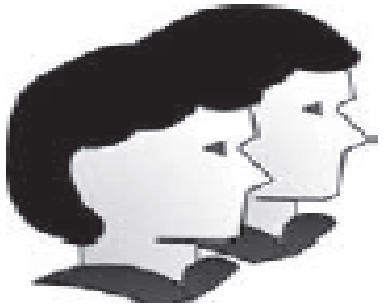
TGS session key and TGT sent to client

Authentication Server

User enters username and password

AS retrieves user credentials

User



Credential Store

- 3. Klien mengirimkan username ke Server Authentication.
  4. Server Otentikasi mengambil password pengguna dari penyimpanan credential dan membuat hash satu arah.
  5. Server Otentikasi memeriksa untuk memastikan bahwa klien adalah disetujui database klien.
  6. Jika klien disetujui, Authentication Server akan mengirimkan kembali kunci Pemberian-Tiket Session Server dan Pemberian-Tiket.
  7. Klien kemudian dikonfirmasi ke server Pemberian-Tiket .

Langkah-langkah berikut menguraikan proses Kerberos permintaan sumber daya

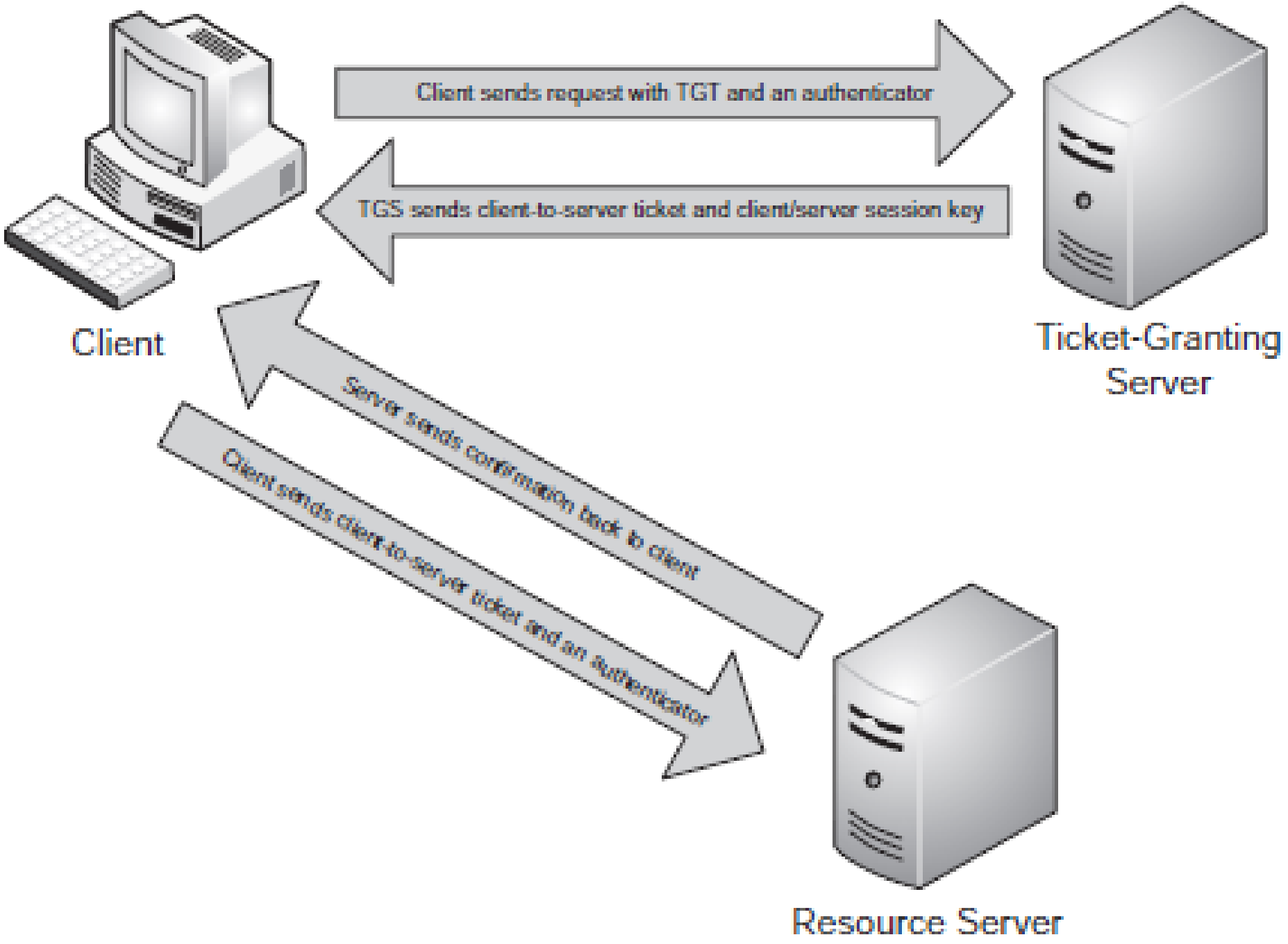
1. Client mengirimkan permintaan ke Layanan Pemberian-Tiket. permintaan itu berisi Tiket Pemberian-Tiket dan authenticator sebuah dienkripsi menggunakan kunci Pemberian-Tiket Session Server.

2. Layanan Tiket-Pemberian mengirimkan tiket klien-ke-server dan kunci session klien/server.

3. Klien mengirimkan tiket klien-ke-server dan authenticator baru ke server di mana sumber daya berada.

4. Server kemudian mengirimkan pesan konfirmasi kembali ke klien.

5. Klien menegaskan server dan mulai mengirim permintaan.


Client sends request with TGT and an authenticator
TGS sends client-to-server ticket and client/server session key
Client
Ticket-Granting Server
Server sends confirmation back to client
Client sends client-to-server ticket and an authenticator
Resource Server

- Kerberos pada Windows Sistem: Kerberos adalah sangat umum di lingkungan windows.
- In fact, Windows 2000 and later use Kerberos as the default method of authentication

Authorization

- Otorisasi adalah proses menentukan apa yang pengguna perbolehkan.
- kebijakan keamanan menentukan pengguna sumber daya apa di lingkungan Anda yang diijinkan untuk diakses.
- Anda harus juga menentukan apa setiap user yang diperbolehkan untuk dilakukan dengan sumber daya tersebut.
  Kebijakan keamanan akan diimplementasikan menggunakan otorisasi sistem Anda
  dan diteruskan menggunakan akses sistem kontrol Anda.

- ada dua konsep untuk memastikan lingkungan Anda aman :

1. *Principle of Least Privilege*
2. *Principle of Separation of Duties*

Principle of Least Privilege

- Prinsip ini setidaknya mengacu pada konsep memberikan mengguna hak minimal yang dibutuhkan untuk melakukan fungsi pekerjaan nya.
- Hal ini membantu mencegah pengguna dari sengaja atau tidak sengaja melakukan hal-hal mereka tidak seharusnya.
- Sebagai contoh, Claudine di Departemen akuntansi tidak harus diberi wewenang untuk melakukan fungsi dalam sistem pengiriman

Principle of Separation of Duties

- Mungkin ada tugas penting atau proses dalam organisasi Anda, bahwa Anda ingin mengambil tindakan ekstra untuk melindungi terhadap penipuan atau kejahatan lainnya.
- Sebuah pemisahan tugas dapat membantu Anda melindungi tugas atau proses.
- Anda mulai dengan memecah proses menjadi tugas yang lebih kecil atau proses.
- Anda kemudian mengotorisasi orang yang berbeda untuk melakukan tugas-tugas yang lebih kecil atau proses.

Accounting

- Accounting adalah proses melacak siapa yang mengakses sumber daya yang di lingkungan Anda.
- Informasi ini dapat digunakan untuk beberapa tujuan. Anda dapat menggunakannya untuk melacak dan memverifikasi masalah keamanan

Product AAA

- RADIUS

RADIUS

- RADIUS is the Remote Authentication Dial-In User Service.
- RADIUS adalah salah satu protokol AAA tertua.
- Awalnya, RADIUS hanya digunakan dalam sistem akses remote.
- Penggunaan RADIUS diperluas untuk mencakup aplikasi dan perangkat jaringan.
- Popularitas RADIUS 'berasal dari fakta bahwa standar protokol itu yang dapat digunakan pada berbagai macam perangkat dan sistem.

- Pengaturan suatu RADIUS membutuhkan klien RADIUS, server RADIUS, dan protokol RADIUS.
- Klien RADIUS umumnya ada di perangkat di tempat usaha koneksi yang dibuat. bahwa perangkat pada gilirannya membuat panggilan ke server RADIUS.
- RADIUS menggunakan UDP untuk komunikasi

TACACS+

- TACACS is the Terminal Access Controller Access control System.
- TACACS adalah standar otentikasi remote. TACACS digunakan untuk dial-in dan akses jaringan.
- Para TACACS asli standar banyak digunakan di sistem UNIX.
- Protokol asli TACACS hampir tidak digunakan lagi. Ini telah digantikan oleh TACACS + dan RADIUS.

- TACACS + adalah ekstensi milik dari standar TACACS
  dikembangkan oleh Cisco.
- TACACS + yang digunakan oleh Cisco untuk otentikasi
  pengguna untuk perangkat jaringan seperti switch, router, dan jaringan akses server.
- Tidak seperti namanya, TACACS + sangat berbeda
  dari standar asli TACACS.
- Bahkan, bahkan mereka tidak kompatibel satu sama lain.

- TACACS dianggap upgrade terbaru dari RADIUS.

- TACACS + menggunakan TCP untuk komunikasi. TCP dianggap lebih dapat diandalkan dibandingkan UDP, UDP adalah apa yang RADIUS gunakan.

Diameter

- Diameter dianggap sebagai penerus protokol RADIUS.
- Dalam geometri, diameter lingkaran adalah dua kali panjang jari-jari lingkaran.
- Meskipun Diameter dianggap sebagai upgrade dari RADIUS, penting untuk dicatat bahwa RADIUS dan Diameter tidak langsung kompatibel.

- Diameter meliputi upgrade selama bertahun-protokol RADIUS.
- Diameter, seperti TACACS, menggunakan TCP untuk komunikasi, sebagai lawan dengan UDP.
- Diameter juga mendukung IPSec dan TLS. Ini mencakup kemampuan negosiasi dan error.
- Diameter juga mencakup lebih atribut-nilai pasangan.

Access Control

- akses kontrol sistem umumnya apa yang digunakan untuk melakukan otorisasi kebijakan anda.

Access Control Models

- *Mandatory Access Control (MAC)*
- *Discretionary Access Control (DAC)*
- *Role-Based Access Control (RBAC)*

Mandatory Access Control (MAC)

- Mandatory Access Control didasarkan pada model hirarkis.
- hirarki itu didasarkan pada tingkat keamanan.
- Semua pengguna ditugaskan keamanan atau izin tingkat.
- Semua obyek ditugaskan keamanan. Pengguna dapat mengakses sumber daya hanya yang sesuai dengan keamanan sama dengan atau lebih rendah dari mereka dalam hirarki tingkat.

Discretionary Access Control (DAC)

- Discretionary Access Control is based on Access Control Lists (ACLs).
- Daftar pengguna ACL mana yang memiliki akses ke sebuah obyek dan apa dapat mereka lakukan dengan objek.
- ACL akan mendaftar pengguna dan perizinan.
- Anda dapat memberikan hak akses khusus atau menolak perizinan.

Role-Based Access Control (RBAC)

- Access Control Sistem Berbasis Peran didasarkan pada peran pengguna dan tanggung jawab.
- Pengguna tidak diberikan akses ke sistem; peran itu.
- Dalam sistem RBAC, peran yang dikelola secara terpusat oleh administrator.
- Administrator menentukan peran apa yang ada dalam perusahaan mereka dan kemudian peta peran untuk fungsi pekerjaan dan tugas.