

Sistem Terdistribusi (ST)

Pertemuan 12 : Keamanan Sistem Terdistribusi

Alauddin Maulana Hirzan

Fakultas Teknologi Informasi dan Komunikasi
Universitas Semarang

Outline

Sistem Terdistribusi (ST)

Alauddin
Maulana
Hirzan

Keamanan Sistem Terdistribusi

Konsep CIA Triad

Jenis-Jenis Distributed Attack

Teknologi Keamanan Sistem Terdistribusi

Lastly

- 1 Keamanan Sistem Terdistribusi
- 2 Konsep CIA Triad
- 3 Jenis-Jenis Distributed Attack
- 4 Teknologi Keamanan Sistem Terdistribusi
- 5 Lastly

Keamanan Sistem Terdistribusi

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Mengapa Keamanan Penting?

Sistem terdistribusi biasanya terdiri dari:

- 1 Banyak node
- 2 Banyak pengguna
- 3 Banyak jalur komunikasi
- 4 Beroperasi melalui internet

Semakin banyak komponen yang terhubung, semakin besar pula attack surface (permukaan serangan).

Keamanan Sistem Terdistribusi

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Analogi Dunia Nyata

Bayangkan sebuah universitas memiliki:

- 1 Banyak gedung
- 2 Banyak pintu masuk
- 3 Banyak staf dan mahasiswa

Jika hanya satu pintu yang dijaga, keamanan relatif mudah. Namun jika terdapat 100 pintu dan ribuan pengguna, maka keamanan menjadi jauh lebih kompleks.

Konsep CIA Triad

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Confidentiality

Menjamin hanya pihak berwenang yang dapat mengakses data.

Contoh

Database mahasiswa:

- 1 NIM
- 2 Nilai
- 3 Data pribadi

Konsep CIA Triad

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Integrity

Menjamin data tidak berubah tanpa izin.

Contoh

Nilai mahasiswa:

A

Tidak boleh berubah menjadi:

E

akibat serangan.

Konsep CIA Triad

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Availability

Menjamin layanan selalu tersedia.

Contoh

Server e-learning harus tetap dapat diakses saat ujian berlangsung.

Ancaman utama:

- 1 DDoS
- 2 Kerusakan server
- 3 Kegagalan jaringan

Karakteristik Ancaman pada Sistem Terdistribusi

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Heterogeneity

Berbagai platform digunakan:

- 1 Linux
- 2 Windows
- 3 Android
- 4 IoT Device

Setiap platform memiliki kelemahan berbeda.

Karakteristik Ancaman pada Sistem Terdistribusi

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Open Network

Sebagian besar komunikasi terjadi melalui internet.

Risiko:

- Penyadapan
- Modifikasi paket
- Pemalsuan identitas

Karakteristik Ancaman pada Sistem Terdistribusi

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Scalability

Semakin besar sistem:

- Semakin banyak pengguna
- Semakin banyak layanan

Kompleksitas keamanan meningkat secara eksponensial.

Jenis-Jenis Distributed Attack

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Distributed Denial of Service (DDoS)

Serangan paling terkenal pada sistem terdistribusi.

Tahapan DDoS

- Penyerang menginfeksi perangkat.
- Membentuk botnet.
- Mengirim perintah serangan.
- Ribuan perangkat mengirim trafik bersamaan.

Dampak

- Website tidak dapat diakses.

Jenis-Jenis Distributed Attack

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Botnet Attack

Botnet adalah kumpulan perangkat yang dikendalikan secara terpusat.

Target:

- Komputer
- Router
- Kamera CCTV
- Perangkat IoT

Jenis-Jenis Distributed Attack

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Man-in-the-Middle (MITM)

Penyerang berada di antara dua pihak yang berkomunikasi.

Client <-----> Attacker <-----> Server

Penyerang dapat:

- 1 Membaca data
- 2 Mengubah data
- 3 Mencuri kredensial

Jenis-Jenis Distributed Attack

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Replay Attack

Penyerang merekam komunikasi yang sah lalu mengirim ulang paket tersebut.

Contoh

Transfer Rp100.000

Paket direkam dan dikirim ulang sehingga transaksi terjadi berkali-kali.

Jenis-Jenis Distributed Attack

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Sybil Attack

Satu node berpura-pura menjadi banyak identitas.

Umum ditemukan pada:

- 1 Blockchain
- 2 Peer-to-Peer Network
- 3 Dampak
- 4 Manipulasi voting
- 5 Manipulasi konsensus

Jenis-Jenis Distributed Attack

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Eclipse Attack

Penyerang mengisolasi node target dari jaringan.

Routing Attack

Penyerang memanipulasi rute jaringan.

Contoh:

- 1 BGP Hijacking
- 2 Route Poisoning

Serangan pada Arsitektur Modern

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Cloud Attack

Target:

- 1 Virtual Machine
- 2 Container
- 3 Cloud Storage

Contoh:

- 1 Data Exposure
- 2 Misconfigured Bucket
- 3 Credential Theft

Serangan pada Arsitektur Modern

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Microservices Attack

Microservices menghasilkan banyak API.

Ancaman:

- 1 API Abuse
- 2 Token Theft
- 3 Service Impersonation

IoT Attack

Karakteristik IoT:

- 1 Resource terbatas
- 2 Password lemah
- 3 Jarang diperbarui

Serangan pada Arsitektur Modern

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Edge Computing Attack

Target:

- 1 Edge Node
- 2 Gateway
- 3 Fog Node

Ancaman:

- 1 Physical Tampering
- 2 Malware Injection
- 3 Data Manipulation

Teknologi Keamanan Sistem Terdistribusi

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Authentication

- Metode: Password
 - Paling umum digunakan.
- Multi-Factor Authentication (MFA)
 - Kombinasi:
 - Password
 - OTP
 - Biometrik

Teknologi Keamanan Sistem Terdistribusi

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Authorization

Menentukan hak akses.

- RBAC -> Role Based Access Control
- ABAC -> Attribute Based Access Control
- DAC -> Discretionary Access Control
- MAC -> Mandatory Access Control

Teknologi Keamanan Sistem Terdistribusi

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Encryption

- Symmetric Encryption
 - Keuntungan:
 - Cepat
 - Kelemahan:
 - Distribusi kunci
- Asymmetric Encryption
 - Keuntungan:
 - Tidak perlu berbagi private key
 - Kelemahan:
 - Lebih lambat

Teknologi Keamanan Sistem Terdistribusi

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Digital Signature

Menjamin:

- 1 Keaslian
- 2 Integritas
- 3 Non-repudiation

Zero Trust Architecture

Prinsip:

Never Trust, Always Verify

Setiap akses harus diverifikasi meskipun berasal dari jaringan internal.

Mitigasi Distributed Attack

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

- **Load Balancer**
 - Mendistribusikan trafik ke banyak server.
- **Rate Limiting**
 - Membatasi jumlah request.
- **CDN**
 - Content Delivery Network menyerap sebagian besar trafik.
- **Anycast Routing**
 - Request diarahkan ke server terdekat.
- **Traffic Scrubbing**
 - Membersihkan trafik berbahaya sebelum mencapai server utama.

Security Monitoring

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Intrusion Detection System (IDS)

Mendeteksi aktivitas mencurigakan.

Contoh:

- Snort
- Suricata

Security Monitoring

Sistem
Terdistribusi
(ST)

Alauddin
Maulana
Hirzan

Keamanan
Sistem
Terdistribusi

Konsep CIA
Triad

Jenis-Jenis
Distributed
Attack

Teknologi
Keamanan
Sistem
Terdistribusi

Lastly

Intrusion Prevention System (IPS)

Tidak hanya mendeteksi tetapi juga memblokir serangan.

Security Information and Event Management (SIEM)

Mengumpulkan log dari:

- Server
- Firewall
- Router
- Cloud

Terima Kasih