Internet of Thing

Catatan Kuliah #10

Alauddin Maulana Hirzan, M. Kom
0607069401

Keamanan dan Privasi *Internet of Things* #1

Keamanan dan Privasi *Internet of Things* #1

Dunia *Internet of Things* #1

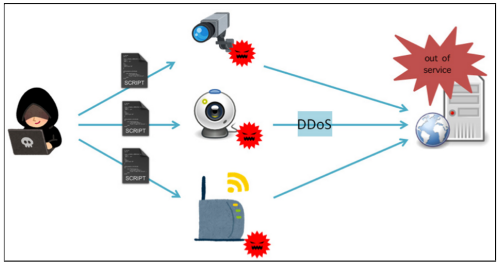
Semua perangkat *Internet of Things* yang memanfaatkan koneksi internet akan dapat terhubung satu sama lain. Artinya, selain perangkat komoditas tradisional dan PC, semua jenis peralatan elektronik yang ada dapat diakses secara online.

Sehingga sangat berbahaya sekali jika ada orang-orang pihak luar yang mencoba mengakses perangkat-perangkat tersebut.

Dalam skenario dimana perangkat yang terhubung lebih masif, keamanan menjadi persyaratan yang sangat penting untuk dipenuhi.

Keamanan dan Privasi *Internet of Things* #1

Dunia *Internet of Things* #2



Info

Setiap hari setidaknya ada lebih dari 100 kejadian pencurian data yang disebabkan oleh *hacker* maupun *malware*

Keamanan dan Privasi *Internet of Things* #1

Dunia *Internet of Things* #3

Sistem IoT rentan terhadap sejumlah kerentanan keamanan, serangan tertentu, eksploitasi kelemahan dan inefisiensi protokol keamanan.

Selain itu, vektor serangan tertentu dapat dengan mudah dieksploitasi di IoT karena dua alasan utama.

- Pertama, sebagian besar perangkat IoT terhubung langsung ke Internet agar dapat dijangkau secara langsung, Sehingga mudah terlihat pada orang asing.
- Kedua, banyak perangkat IoT yang sumber dayanya terbatas, karena dilengkapi dengan jumlah memori, komputasi, dan sumber daya energi yang terbatas.

Keamanan dan Privasi *Internet of Things* #1

Serangan Keamanan *Internet of Things*

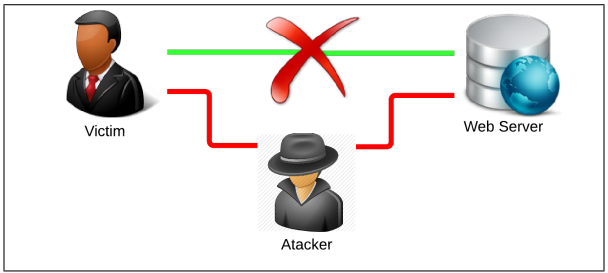
Perangkat *Internet of Things* juga memiliki kelemahan seperti komputer biasa sehingga serangan-serangan seperti berikut ini mampu melemahkan atau menghentikan sistem.

- **Man in The Middle**
- **Botnet**
- **IP Spoofing**
- **DOS (Denial of Service)**
- **Distributed Denial of Service**
- **Worm**

Keamanan dan Privasi *Internet of Things* #1

Serangan Keamanan *Internet of Things - Man in The Middle* #1

Serangan *Man-in-The-Middle* adalah sebuah serangan yang di mana pihak luar berada di tengah-tengah perangkat pengguna dan perangkat tujuan. Sehingga pihak luar tersebut dapat mencegat, memantau bahkan mengontrol komunikasi yang ada.



Keamanan dan Privasi *Internet of Things* #1

Serangan Keamanan *Internet of Things - Man in The Middle* #2

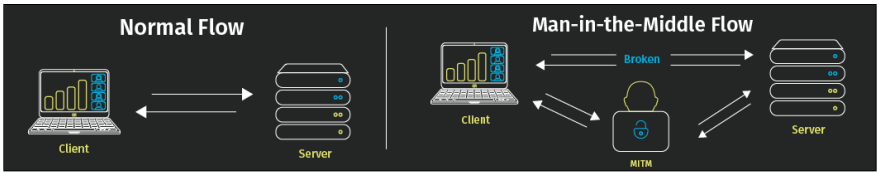
Ciri khas dari Serangan man-in-the-middle:

- Jenis pembajakan sesi pengguna
- Melibatkan penyerang yang memasukkan diri mereka sebagai relai atau proxy dalam percakapan atau transfer data yang berkelanjutan dan asli
- Memanfaatkan sifat percakapan dan transfer data real-time agar tidak terdeteksi
- Mengizinkan penyerang untuk mencegat data rahasia
- Mengizinkan penyerang memasukkan data dan tautan berbahaya dengan cara yang tidak dapat dibedakan dari data yang asli

Keamanan dan Privasi *Internet of Things* #1

Serangan Keamanan *Internet of Things - Man in The Middle* #3

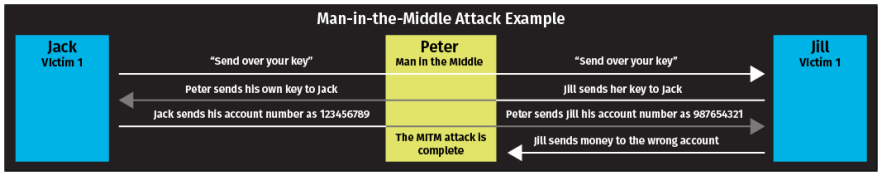
Skenario yang bisa terjadi dalam MITM berdasarkan **veracode.com**:



- Penyerang menganalisis lalu lintas jaringan untuk komunikasi yang tidak aman.
- Saat pengguna masuk ke sebuah situs, penyerang membaca dan mengarahkan ke situs palsu
- Situs palsu mengumpulkan data dari pengguna, dan digunakan di situs asli

Keamanan dan Privasi *Internet of Things* #1

Serangan Keamanan *Internet of Things - Man in The Middle* #4

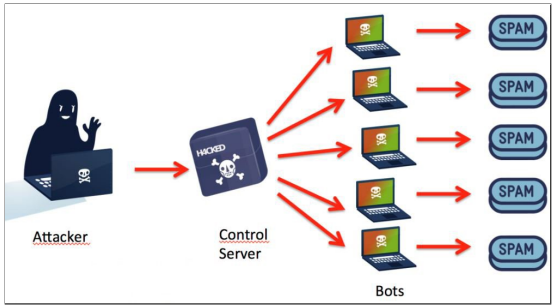


- Penyerang membuat lobrolan palsu yang meniru layanan bank asli
- Menggunakan data yang dicegat dalam skenario pertama, penyerang berpura-pura menjadi bank dan memulai obrolan dengan target.
- Penyerang kemudian memulai obrolan di situs bank asli, berpura-pura menjadi target untuk mendapatkan akses ke akun target.

Keamanan dan Privasi *Internet of Things* #1

Serangan Keamanan *Internet of Things* - *Botnet* #1

Botnet adalah kumpulan bot. Istilah ini juga mengacu pada malware yang dijalankan pada perangkat yang terhubung untuk mengubahnya menjadi bot. Sinonim: jaringan zombie



Keamanan dan Privasi *Internet of Things* #1

Serangan Keamanan *Internet of Things - Botnet* #2

- Tahap 1 - Mempersiapkan dan Mengekspos kelemahan
- Tahap 2 - Menginfeksi pengguna melalui malware
- Tahap 3 - Mengontrol perangkat yang ditargetkan

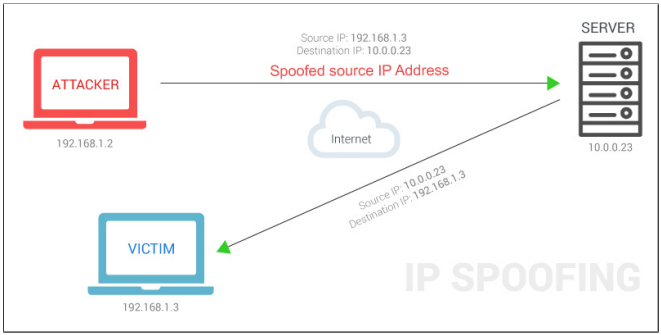
Info

Botnet adalah awal mula dari serangan DDOS. Semua perangkat IoT dengan kekuatan komputas dapat diambil alih dan dijadikan alat DDOS

Keamanan dan Privasi *Internet of Things* #1

Serangan Keamanan *Internet of Things - IP Spoofing*

Metode ini menggunakan alamat sumber palsu untuk memasukkan paket ke Internet dan merupakan salah satu cara untuk menyamarkannya sebagai pengguna lain.



Keamanan dan Privasi *Internet of Things* #1

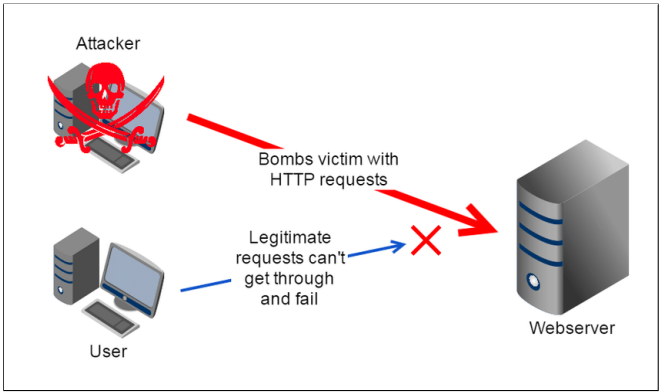
Serangan Keamanan *Internet of Things - Denial of Service* #1

Denial-of-Service adalah serangan kritis yang dapat membunuh jaringan korban atau infrastruktur TI dengan memblokir pengguna yang berwenang dari mengaksesnya.

- **Bandwidth Flooding** : Melalui pengiriman kaskade paket, penyerang teroris dapat memblokir paket yang valid untuk mengakses server.
- **Vulnerability Attacks** : Ketika beberapa pesan yang dibuat dengan baik dikirim ke sistem operasi yang tidak aman atau ke perangkat di server target, layanan gagal atau memburuk jika host runtuh.
- **Connection Flooding** : Dengan membuat sejumlah besar koneksi TCP di server yang ditargetkan, penyerang menjadi macet

Keamanan dan Privasi *Internet of Things* #1

Serangan Keamanan *Internet of Things - Denial of Service* #2



Keamanan dan Privasi *Internet of Things* #1

Serangan Keamanan *Internet of Things - Denial of Service* #3

Bandwdith Flooding merupakan Penyerang mengirim begitu banyak paket sehingga tautan akses target menjadi tersumbat, mencegah paket yang sah mencapai server.

Teknik ini membuat jaringan menjadi penuh dengan paket-paket sampah dan membuat *bandwidth* menjadi habis dan tidak mungkin dilalui oleh paket asli.

Info
Teknik ini sangat umum untuk digunakan melumpuhkan jaringan IoT yang banyak mengirimkan pesan-pesan monitoring perangkat

Keamanan dan Privasi *Internet of Things* #1

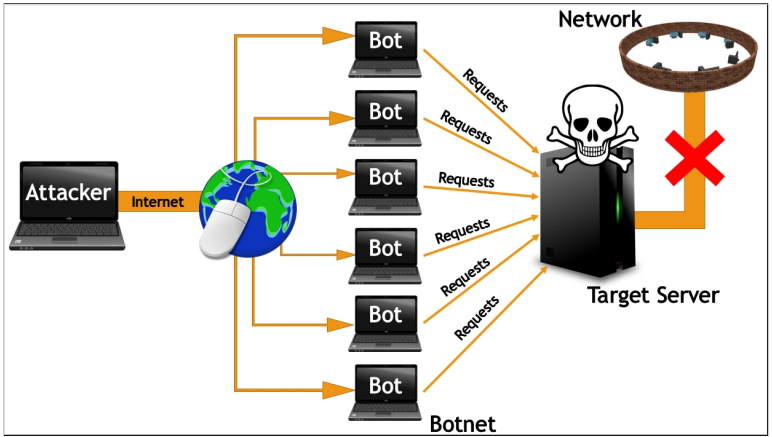
Serangan Keamanan *Internet of Things - Distributed Denial of Service* #1

Serangan DDOS adalah versi yang rumit dan jauh lebih sulit untuk dideteksi dan dilindungi daripada serangan DOS biasa. Penyerang menggunakan beberapa sistem yang dikompromikan untuk menargetkan satu sistem serangan dos yang ditargetkan. Dalam penyerangan ini. Serangan dari DDOS bahkan mengangkat botnet.

Info
DDOS menggunakan beberapa komputer yang di-remote untuk melakukan sekaligus. Sehingga menjadi sangat berbahaya jika menerimanya

Keamanan dan Privasi *Internet of Things* #1

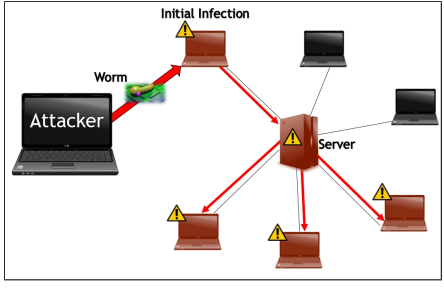
Serangan Keamanan *Internet of Things - Distributed Denial of Service* #2



Keamanan dan Privasi *Internet of Things* #1

Serangan Keamanan *Internet of Things - Worm*

Jika pengguna menjalankan program jaringan yang rentan, penyerang malware dapat mengirim malware ke aplikasi tersebut pada koneksi Internet yang sama. Aplikasi akan menerima dan mengeksekusi malware dari internet untuk membangun worm.



Keamanan dan Privasi *Internet of Things* #1

What To Do?

Untuk melindungi perangkat IoT yang terpasang, ada beberapa hal yang dapat dilakukan seperti:

- Pengamanan Fisik : Cara ini dilakukan untuk mencegah perangkat-perangkat dari gangguan eksternal termasuk pencurian maupun hal-hal lainnya
- Pengamanan Digital : Cara ini dilakukan untuk mencegah pencurian maupun kerusakan data yang disebabkan oleh serangan internet

Keamanan dan Privasi *Internet of Things* #1

Pengamanan Fisik #1

Pengaman secara fisik mampu mencegah perangkat dari hal-hal yang tidak diinginkan seperti pencurian perangkat, perusakan perangkat, kemasukkan debu, korsleting karena hujan dan lain-lain.

Sehingga sangat penting untuk membuatkan *case* atau wadah yang dapat digunakan untuk menutup perangkat.

Info
Sebagian perangkat IoT tidak memiliki box secara default, sehingga pengguna harus membeli atau membuat sendiri box yang sesuai dengan kebutuhan mereka.

Keamanan dan Privasi *Internet of Things* #1

Pengamanan Fisik #2

Bagaimana cara menentukan wadah yang tepat? Perhatikan aspek berikut:

- Lokasi pemasangan alat
- Ekspos dari udara lembab, air asin, atau bahan kimia korosif
- Ekspos dari debu, benda kotor lainnya
- Digunakan untuk pribadi, industri, atau penelitian
- Perlu pendingin
- Adanya antena
- Transparansi wadah diperlukan
- *Form Factor* perangkat

Keamanan dan Privasi *Internet of Things* #1

Pengamanan Fisik #3

Keamanan dan Privasi *Internet of Things* #1

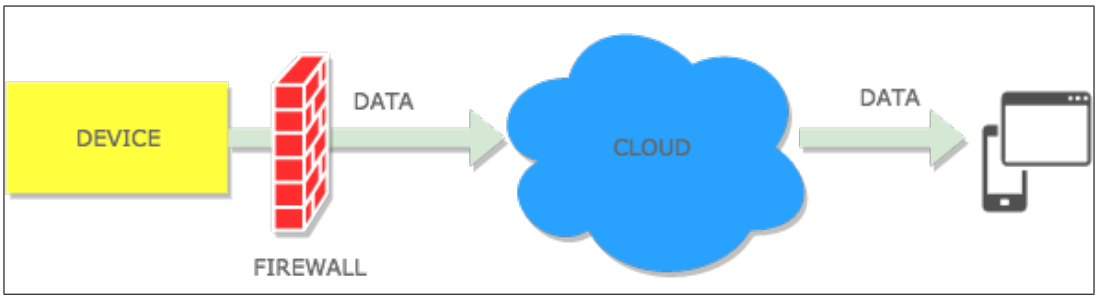
Pengamanan Digital #1

Cara ini digunakan untuk melindungi perangkat-perangkat yang terhubung ke Internet. Sebaiknya memasang perangkat lunak seperti:

- *Firewall*
- *Intrusion Detection System*
- *VPN*

Keamanan dan Privasi *Internet of Things* #1

Pengamanan Digital #2




THANK YOU