



DIGITAL  
TALENT  
SCHOLARSHIP



# VOCATIONAL SCHOOL GRADUATE ACADEMY

## Mobile Programmer

### Pertemuan #13- : Mobile Security



KOMINFO



## #JADIJAGOANDIGITAL

Badan Penelitian dan Pengembangan Sumber Daya Manusia

# PROFIL PENGAJAR



Jabatan Akademik / Kepala LAB Prodi Teknik Komputer

Latarbelakang Pendidikan Pengajar

- S1– STMIK Budi Darma (Skripsi : Aps Mobile Kompresi SMS)
- S2– Universitas Putra Indonesia YPTK Padang (Tesis : Aps Mobile Security SMS)

Riwayat Pekerjaan

- Dosen Tetap Politeknik Negeri Medan
- Trainer Pemrograman Java dan Mobile, Networking, Cyber Security, OS Server
- Konsultan Bidang Aplikasi, Networking, Cyber Security dan Server
- CEO PT. Nusa Tirta Teknologi

Sertifikat Kompetensi :

- Program : Senior Programmer (BNSP)
- Networking : Mikrotik, CISCO
- Server : Windows Server, Redhat
- Project : Comptia Project +

Contact Pengajar

Ponsel :-

Email : azanuddin@polmed.ac.id

# Deskripsi Singkat

## Deskripsi Singkat mengenai Topik

Topik berisi Penjelasan dasar dasar Mobile Communications Security, Wireless Vulnerabilities, Tipe Attack pada Mobile Environment, Teknik Perlindungan (Protection Technique) pada Mobile Systems

## Tujuan Pelatihan

Setelah mengikuti pelatihan ini, peserta dapat meningkatkan kompetensi teknis dalam membuat security pada mobil sesuai dengan kebutuhan.

## Materi Yang akan disampaikan:

1. Dasar-dasar mobile security
2. Wireless vulnerabilities
3. Type Attack pada mobile environment

**Tugas : *Mempersiapkan peralatan dan bahan/materi, Mengumpulkan informasi dan menuliskan hal-hal yang berkaitan dengan security pada mobile.***

## Outcome/Capaian Pelatihan

***Mengumpulkan informasi mengenai mobile security dan Menuliskan tentang security yang ada pada mobile serta type-type attack pada mobile environment.***

# Mobile Communication Security

Mobile Security adalah Keamanan yang di miliki oleh sebuah handphone dalam melindungi sebuah data yang di miliki, masing - masing handphone miliki struktur mobile yang berbeda - beda namun hampir semuanya sama mementingkan aspek keamanan.

# Risiko Keamanan Perangkat Mobile

1. Risiko Fisik
2. Risiko data storage
3. Risiko strong Password
4. Risiko Internet Browsing
5. Risiko Privasi Lokasi
6. Risiko Sistem Operasi

# Mobile Security Secure Design Principles

Prinsip-prinsip keamanan dalam mendesain aplikasi mobile:

1. Identifikasi dan Proteksi Data Sensitif pada Perangkat Mobile
2. Pastikan Data Sensitif Terlindungi Saat Transit
3. Jalankan Aplikasi dengan Hak Akses Minimum
4. Ikuti Praktik Secure Coding

# Mobile Security Testing

Metodologi umum dalam melakukan pengujian aplikasi mobile:

1. Memahami proses bisnis aplikasi (Understanding application business process)
2. Menguraikan aplikasi (Decomposing application)
3. Mengembangkan skenario serangan (Developing attack scenarios)
4. Menentukan prioritas risiko (Prioritizing risks)
5. Melakukan pengujian (Conducting tests)
6. Menganalisis hasil pengujian (Analyzing test results)
7. Merekomendasikan perbaikan

# Mobile Security Assessment

Mobile security assessment dapat dilakukan dengan melakukan pengujian pada aplikasi yang sedang dijalankan atau pada aplikasi yang sedang tidak dijalankan.

Metodologi pengujian aplikasi mobile :

1. Analisis Dinamik (Dynamic Analysis)
2. Analisis Statis (Static Analysis)



# Pengujian statis dapat dilakukan

1. Ekstrak aplikasi dari perangkat atau dapatkan paket aplikasi dari pengembang
2. Melakukan source code review.
3. Melakukan reverse engineering
4. Melakukan dissassembling

# Security Wirelles Network

- ❑ Sistem keamanan pada wireless LAN ;
  1. WEP (Wired Equivalent Privacy).
  2. WPA (Wi-Fi Protected Access).

# Ancaman Jaringan Wirelles

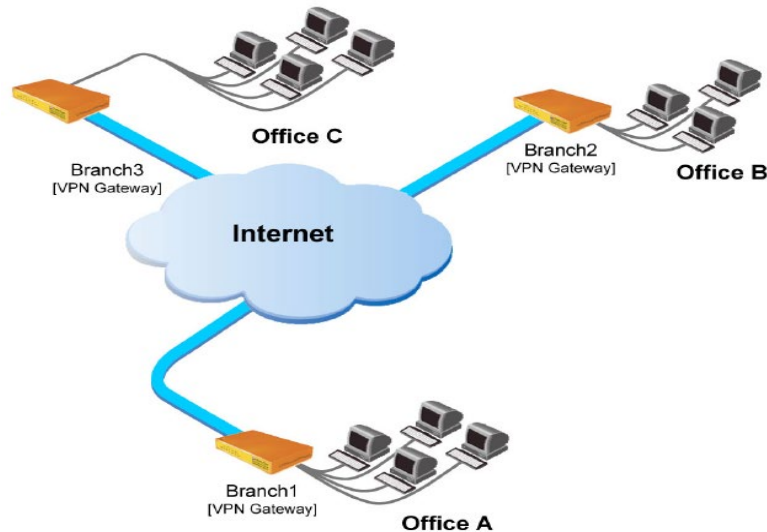
Jenis-jenis ancaman jaringan wariless:

1. Sniffing to Eavesdrop.
2. Denial of Service Attack.
3. Man in the Middle Attack.
4. Rogue/Unauthorized Access Point.
5. Konfigurasi access point yang tidak benar.

# Virtual Private Network

- ❑ VPN: suatu metode pengamanan dengan membentuk koneksi logical antar beberapa node dalam jaringan yang bersifat public.
- ❑ Teknologi VPN menyediakan tiga fungsi utama:
  1. Confidentially (Kerahasiaan) .
  2. Data Integrity (Keutuhan Data / Keaslian Data) .
  3. Origin Authentication (Autentikasi Sumber).

# Virtual Private Network



Gambar 1. Jaringan WAN Sumber :  
(<http://www.checkpoint.com/smb/help/utm1/8.0/1195.htm>)

# Virtual Private Network

## ❑ Site-to-Site VPN

Ada 2 jenis site-to-site VPN:

1. Internet VPN.
2. Extranet VPN.

# Virtual Private Network

Jenis VPN secara garis besar ada 2:

1. Remote-Access VPN.
2. Site-to-Site VPN.

# Virtual Private Network

## ❑ Keamanan VPN

Fitur-fitur penting yang ada dalam VPN :

1. Enkripsi
2. Tunneling
3. IPSec



# Mobile IP

IP mobile ( Mobile IP ) adalah protokol komunikasi standar terbuka yang didefinisikan oleh IETF (Internet Engineering Task Force) yang memungkinkan pengguna perangkat mobile untuk menjaga IP yang sama ( Internet Protocol ) alamat saat roaming antara jaringan IP.

# Mobile IP

## ❑ Komponen IP mobile:

1. Mobile Node
2. Home Agen
3. Agen Asing
4. Perawatan Alamat
5. Koresponden Node

# Mobile IP

## Menjelaskan dasar-dasar mobile security

### 2. Menjelaskan Wireless Vulnerabilities

- 2.1. WLAN Vulnerabilities dijelaskan sesuai dengan standar yang ada.
- 2.2. Cellular System Vulnerabilities dijelaskan sesuai dengan standar yang ada.
- 2.3. Application based Vulnerabilities dijelaskan sesuai dengan standar yang ada.
- 2.4. Content-Based Vulnerabilities dijelaskan sesuai standar yang ada.
- 2.5 Mixed Application Vulnerabilities dijelaskan sesuai standar yang ada.

(Kerentanan Jaringan Wireless)

# WLAN Vulnerabilities

# WLAN Vulnerabilities

Jaringan wireless (tanpa kabel) menjadi semakin ramai dipergunakan di rumah / perkantoran / tempat makan / dikarenakan kemudahan dalam segi penggunaannya.

Dhingra, M. et al, Wireless Network Security Threats and Their Solutions: a short study, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-1,2, 2012

# WLAN Vulnerabilities

The 802.11 WLAN beroperasi pada dua mode:

- Infrastructure mode
- Ad-hoc mode

Dhingra, M. et al, Wireless Network Security Threats and Their Solutions: a short study, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-1,2, 2012

# WLAN Vulnerabilities

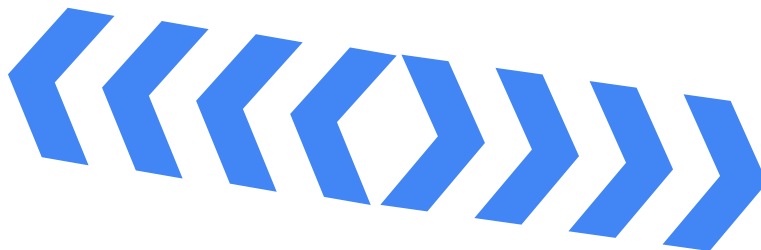
## Infrastructure mode

- Setiap pengguna langsung terkoneksi dengan perangkat Access Point (AP)
- Tidak ada hubungan langsung (direct connection) antar pengguna
- AP juga menjalankan peran sebagai perangkat HUB untuk menjembatani koneksi antar pengguna

Dhingra, M. et al, Wireless Network Security Threats and Their Solutions: a short study, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-1,2, 2012

# WLAN Vulnerabilities

## Infrastructure Mode





# WLAN Vulnerabilities

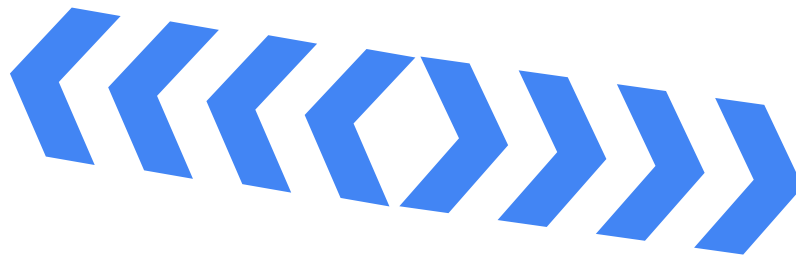
## Ad-hoc mode

- Setiap pengguna terhubung langsung dengan pengguna lainnya (direct connection)
- Tidak ada Access Point untuk manajemen koneksi jaringan
- Jaringan biasanya bersifat sementara (temporary network) dikarenakan tidak adanya perangkat yang mengatur koneksi jaringan

Dhingra, M. et al, Wireless Network Security Threats and Their Solutions: a short study, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-1,2, 2012

# WLAN Vulnerabilities

## Adhoc Mode



# WLAN Vulnerabilities

WLAN memiliki kelebihan terhadap penggunaanya dalam hal :

- portable (dapat dibawa kemana saja),
- fleksible (dapat digunakan kapanpun),
- dan biaya pemasangan yang rendah (tanpa memerlukan kabel).

Dhingra, M. et al, Wireless Network Security Threats and Their Solutions: a short study, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-1,2, 2012

# WLAN Vulnerabilities

WLAN memiliki kekurangan berupa :

- Jarak yang terbatas (berdasarkan radius),
- Perantara medium berupa gelombang (bisa mengakses jaringan tanpa ketahuan secara fisik)

Dhingra, M. et al, Wireless Network Security Threats and Their Solutions: a short study, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-1,2, 2012

Larsson, J. and Waller, Ida. Security in wireless networks: Vulnerabilities and countermeasures, Department of Software Engineering and Computer Science Blekinge Institute of Technology, Springer, 2003

# WLAN Vulnerabilities

- Konsentrasi keamanan pada WLAN mirip dengan lingkungan jaringan LAN
- Kemiripannya adalah sebagai berikut :
  - Confidentiality (Kerahasiaan),
  - Integrity (keutuhan),
  - Availability (ketersediaan),
  - Authentication (keaslian)
  - Accountability (akuntabilitas)

Dhingra, M. et al, Wireless Network Security Threats and Their Solutions: a short study, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-1,2, 2012

Larsson, J. and Waller, Ida. Security in wireless networks: Vulnerabilities and countermeasures, Department of Software Engineering and Computer Science Blekinge Institute of Technology, Springer, 2003

# WLAN Vulnerabilities

## Confidentiality (kerahasiaan)

Kerahasiaan dalam hal ini adalah informasi yang kita miliki pada sistem/database kita, adalah hal yang rahasia dan pengguna atau orang yang tidak berkepentingan tidak dapat melihat/mengaksesnya. Atau dengan kata lain, hanya pihak yang berhak dan berwenang saja yang dapat mengakses informasi tersebut.

# WLAN Vulnerabilities

## Integrity (keutuhan)

Integrity maksudnya adalah keutuhan suatu data yang dikirimkan dari pengguna ke perangkat/pengguna. Keutuhan dapat dilihat dari ketahanan data yang dikirimkan akan terkirim seutuhnya (file dapat dibaca) atau rusak (file corrupt)

# WLAN Vulnerabilities

## Availability (ketersediaan)

Maksud dari availability adalah memastikan sumber daya yang ada siap diakses kapanpun oleh user/application/sistem yang membutuhkannya.



# WLAN Vulnerabilities

## Authentication (keaslian)

Authentication maksudnya adalah data tidak dirubah dari aslinya oleh orang yang tidak berhak, sehingga konsistensi, akurasi, dan validitas data tersebut masih terjaga. Dengan bahasa lain, integrity mencoba memastikan data yang disimpan benar adanya, tidak ada pengguna yang tidak berkepentingan atau software berbahaya yang mengubahnya.

# WLAN Vulnerabilities

## Accountability (akuntabilitas)

Menjamin pengirim data akan mendapatkan laporan keberhasilan data yang dikirimkan (delivered) dan penerima mendapatkan informasi pengirim.

# WLAN Vulnerabilities

Secara umum terdapat dua perhatian pada jaringan WLAN :

- Akses

Memastikan pengguna resmi dapat mengakses jaringan dan tidak bisa mengakses system utama

- Privacy

Memastikan privacy pengguna resmi terlindungi dari penyadapan komunikasi di dalam jaringan oleh pihak luar

Dhingra, M. et al, Wireless Network Security Threats and Their Solutions: a short study, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-1,2, 2012

Larsson, J. and Waller, Ida. Security in wireless networks: Vulnerabilities and countermeasures, Department of Software Engineering and Computer Science Blekinge Institute of Technology, Springer, 2003

# WLAN Vulnerabilities

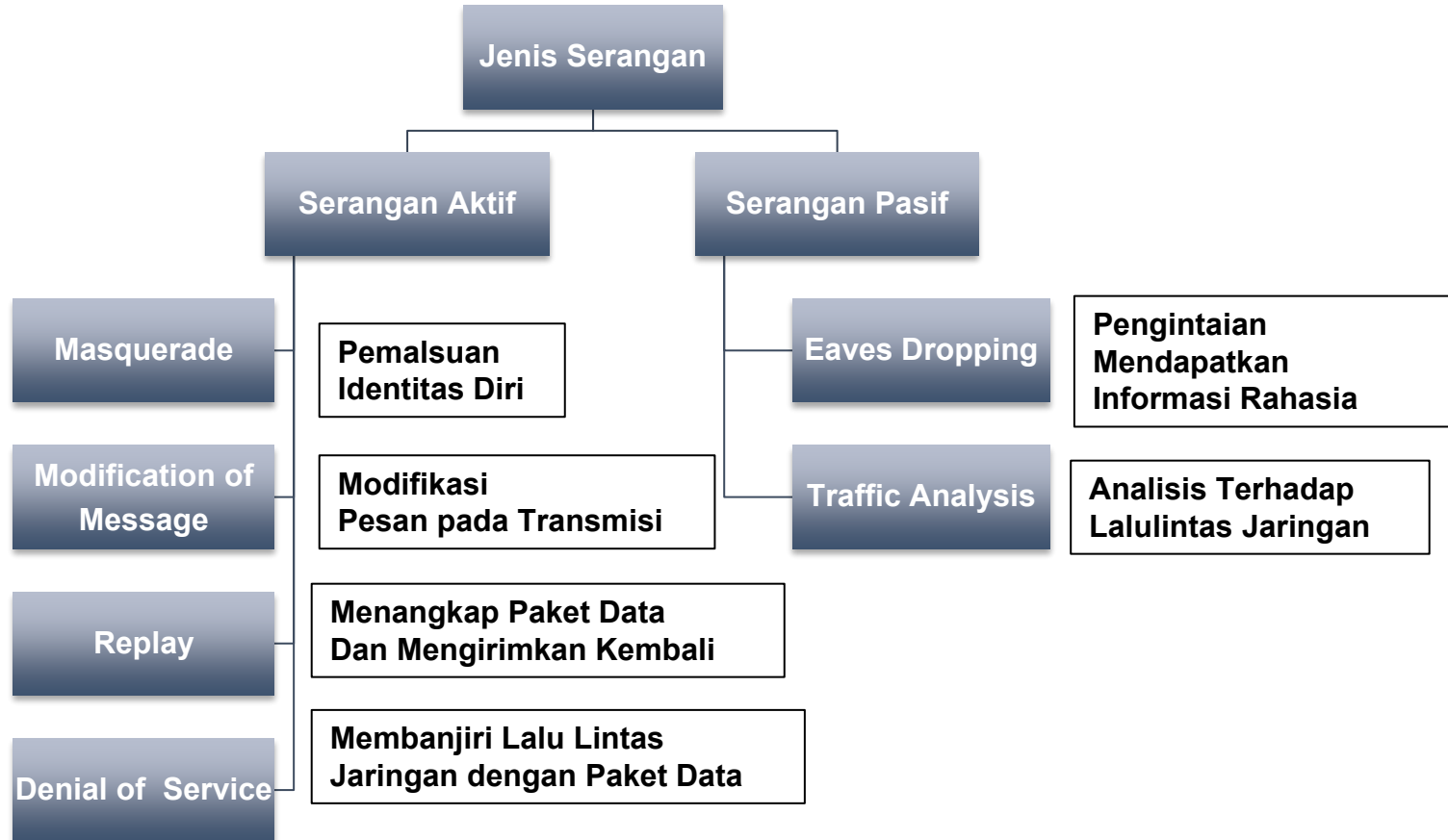
Bahaya dari Pengguna yang ilegal (Unauthorized users) yaitu :

- Dapat memperoleh akses ke sistem utama langsung,
- Kecenderungan ingin merusak sistem,
- Menggunakan jaringan bandwidth yang dikhususkan pada pengguna resmi,
- Menurunkan kinerja jaringan bila melakukan serangan aktif,
- Meluncurkan serangan yang mencegah pengguna resmi (authorized users) untuk mengakses jaringan,
- atau penyalahgunaan informasi sistem untuk menyerang sistem jaringan lainnya.

Dhingra, M. et al, Wireless Network Security Threats and Their Solutions: a short study, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-1,2, 2012

Larsson, J. and Waller, Ida. Security in wireless networks: Vulnerabilities and countermeasures, Department of Software Engineering and Computer Science Blekinge Institute of Technology, Springer, 2003

# WLAN Vulnerabilities



# WLAN Vulnerabilities

## Contoh Serangan Aktif

- Session Hijacking Attack (Masquerade)
- Man in the middle Attack (Message Modification)
- Replay Attack (Replay)
- Denial of service attack (DDoS)

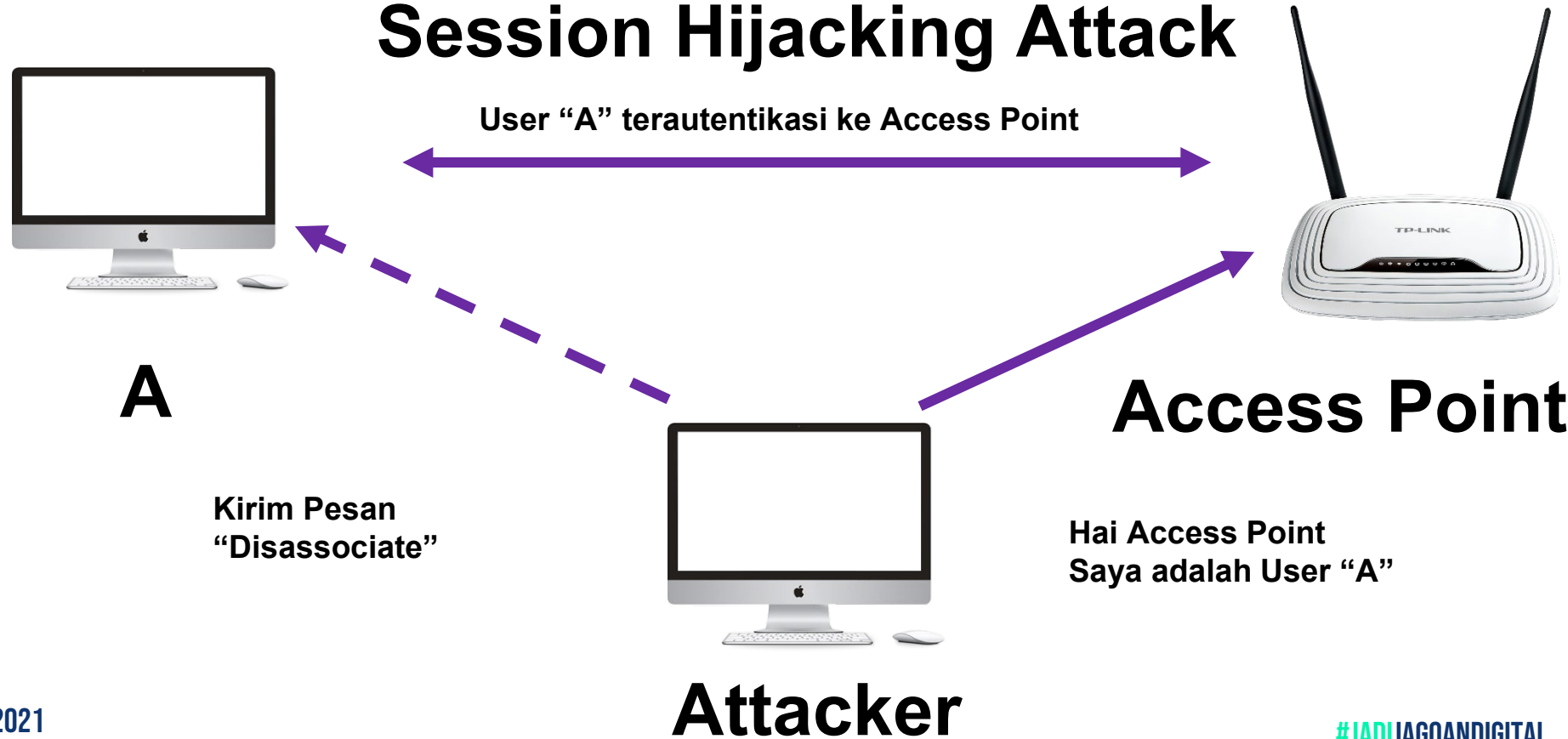
# WLAN Vulnerabilities

## Session Hijacking Attack

- Serangan ini dilakukan untuk mencuri session dari seorang wireless user yang sudah terotentikasi dengan access point.
- Penyerang akan mengirimkan pesan disassociate kepada wireless user dengan membuatnya seolah-olah berasal dari access point. Wireless user akan mengira bahwa koneksi dengan access point telah terputus, namun access point tetap beranggapan bahwa wireless user masih terkoneksi dengannya.
- Kemudian penyerang akan menggunakan MAC Address dan IP Address untuk melakukan koneksi dengan access point seolah-olah sebagai wireless user tersebut.

# WLAN Vulnerabilities

## Session Hijacking Attack





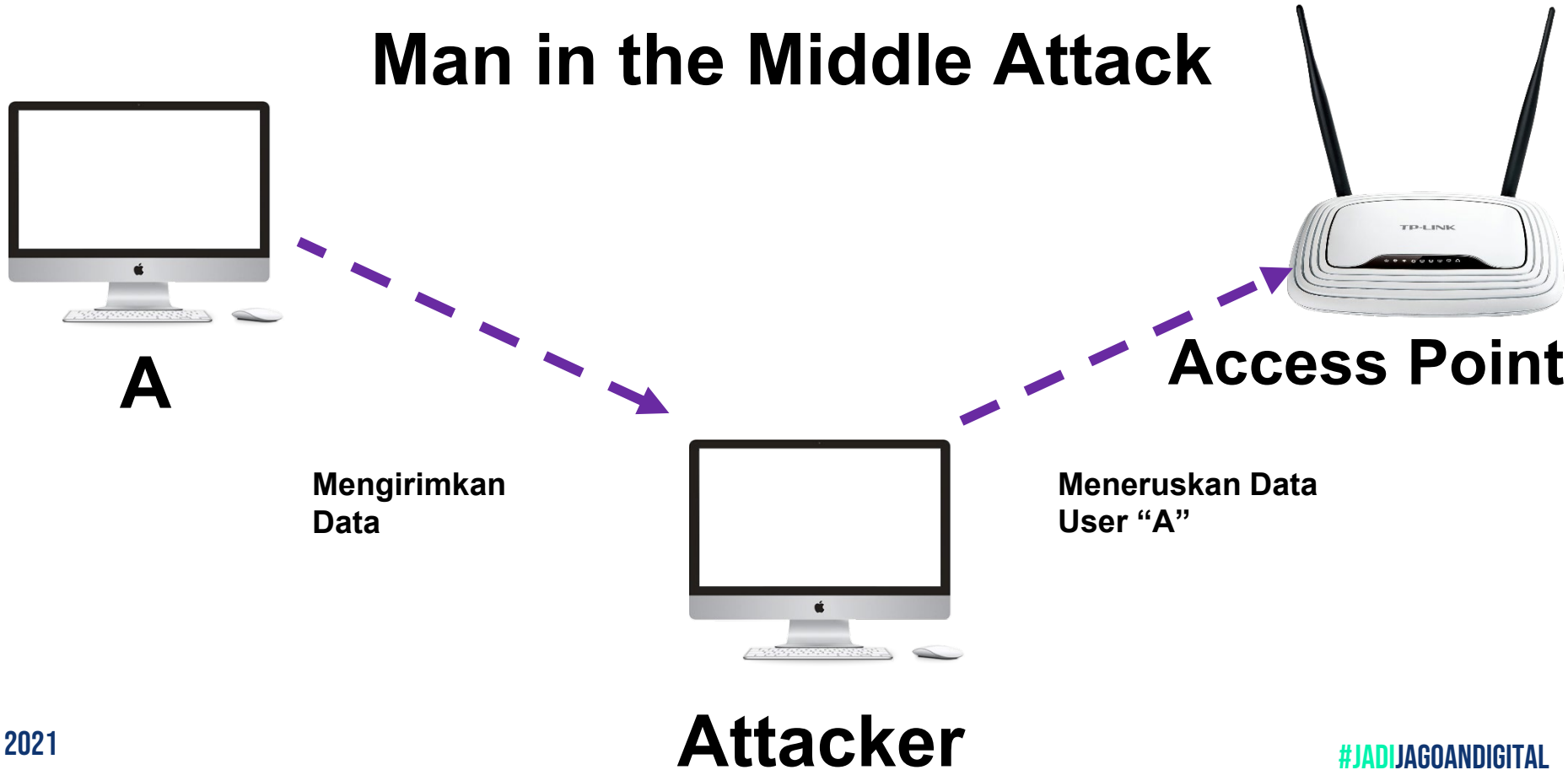
# WLAN Vulnerabilities

## Man in the Middle Attack

- Serangan ini dapat dilakukan apabila otentikasi dilakukan dalam proses satu arah (One Way Authentication).
- Dalam WLAN otentikasi satu arah ini biasanya berupa access point melakukan otentikasi terhadap wireless user, namun tidak sebaliknya. Hal ini berarti bahwa access point selalu dianggap sebagai pihak yang dapat dipercaya (Trusted Entity).
- Penyerang bertindak seolah-olah sebagai access point dihadapan wireless user dan bertindak seolah-olah sebagai wireless user dihadapan access point.
- Kedua pihak tidak menyadari kehadiran penyerang ini karena lalu lintas jaringan tidak ada gangguan, namun penyerang akan mengetahui informasi username dan password selama dalam jaringan

# WLAN Vulnerabilities

## Man in the Middle Attack



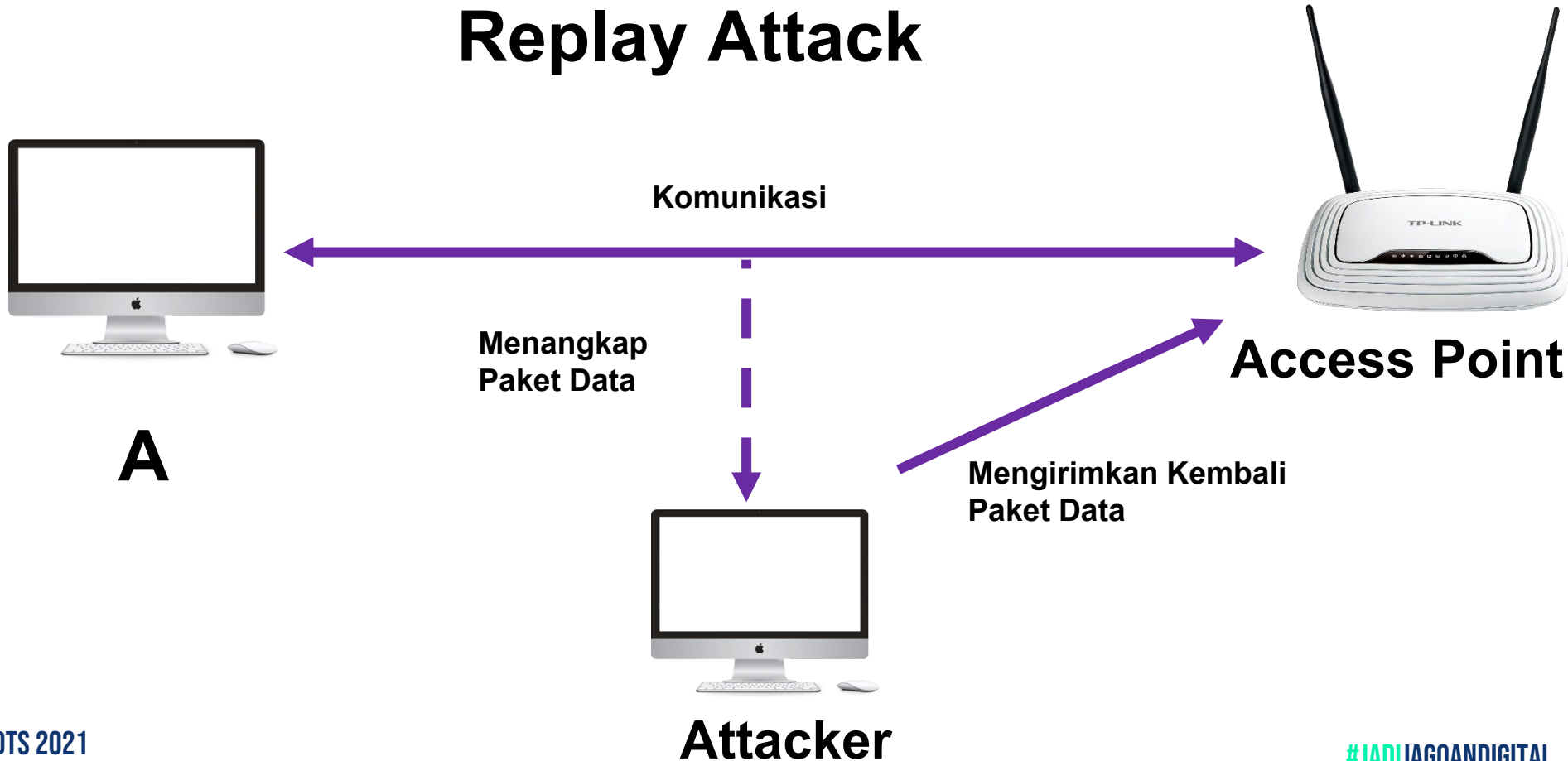
# WLAN Vulnerabilities

## Replay Attack

- Serangan ini termasuk dalam kategori interception dan monitoring attack, yaitu dengan menangkap lalu lintas jaringan.
- Serangan ini dilakukan oleh penyerang untuk menyadap sebuah pesan dari wireless user yang sah dan kemudian mengirimkan kembali kepada access point seolah-olah pesan tersebut memang dikirimkan kembali oleh wireless user.
- Memiliki kemiripan dengan session hijacking attack, namun letak perbedaanya adalah attacker tidak memberikan pesan “Disassociate” kepada user

# WLAN Vulnerabilities

## Replay Attack



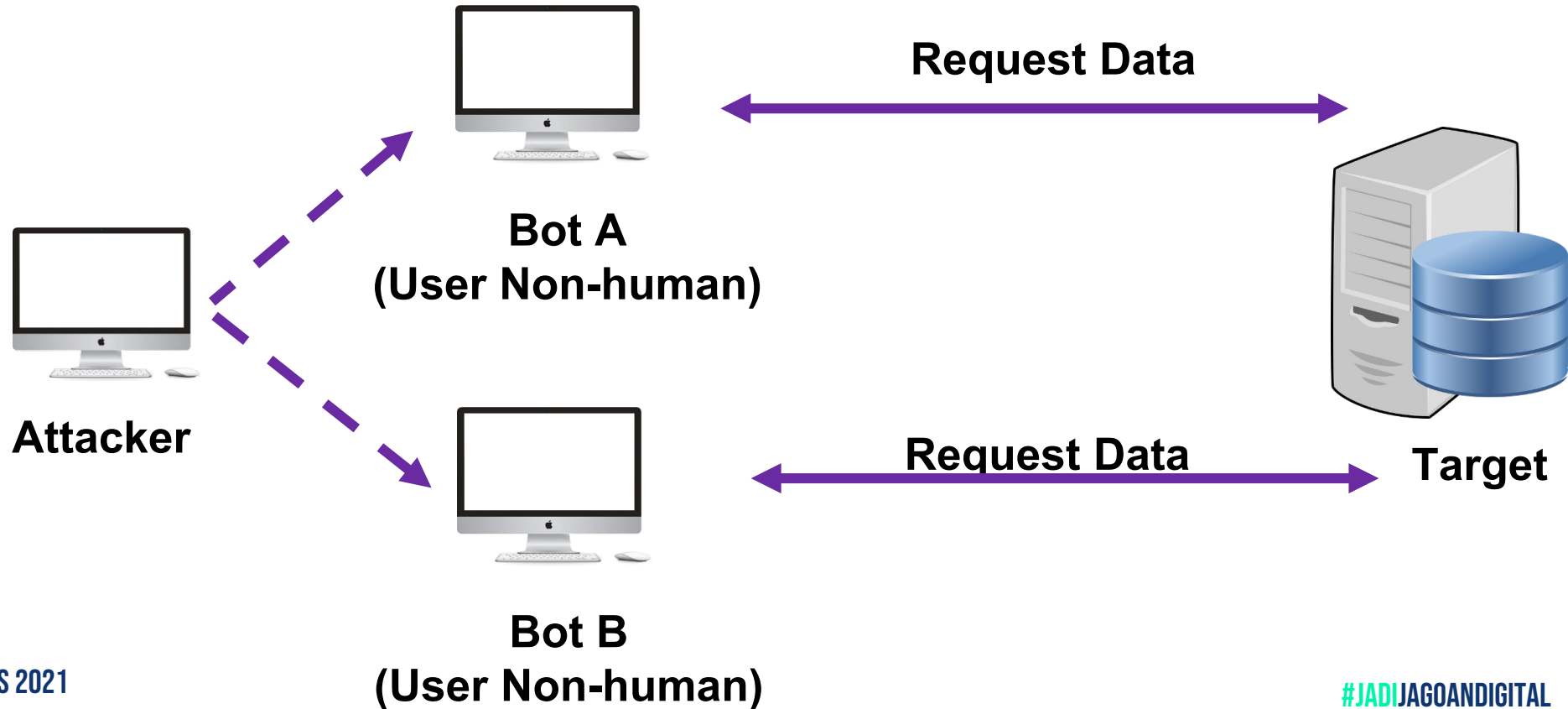
# WLAN Vulnerabilities

## Denial of service attack (DDoS)

- Jenis serangan Jamming ini biasanya dilakukan untuk melumpuhkan ketersediaan jaringan sehingga wireless user tidak dapat mengakses jaringan
- Mengirimkan paket data yang membanjiri lalu lintas jaringan (flooding), ada dua flooding yang digunakan, yaitu :
  - Request flooding merupakan teknik yang digunakan dengan membanjiri jaringan menggunakan banyak request.
  - Traffic flooding merupakan teknik yang digunakan dengan membanjiri lalu lintas jaringan dengan banyak data.

# WLAN Vulnerabilities

## Denial of service attack (DDoS)



- (Kerentanan Jaringan Seluler)

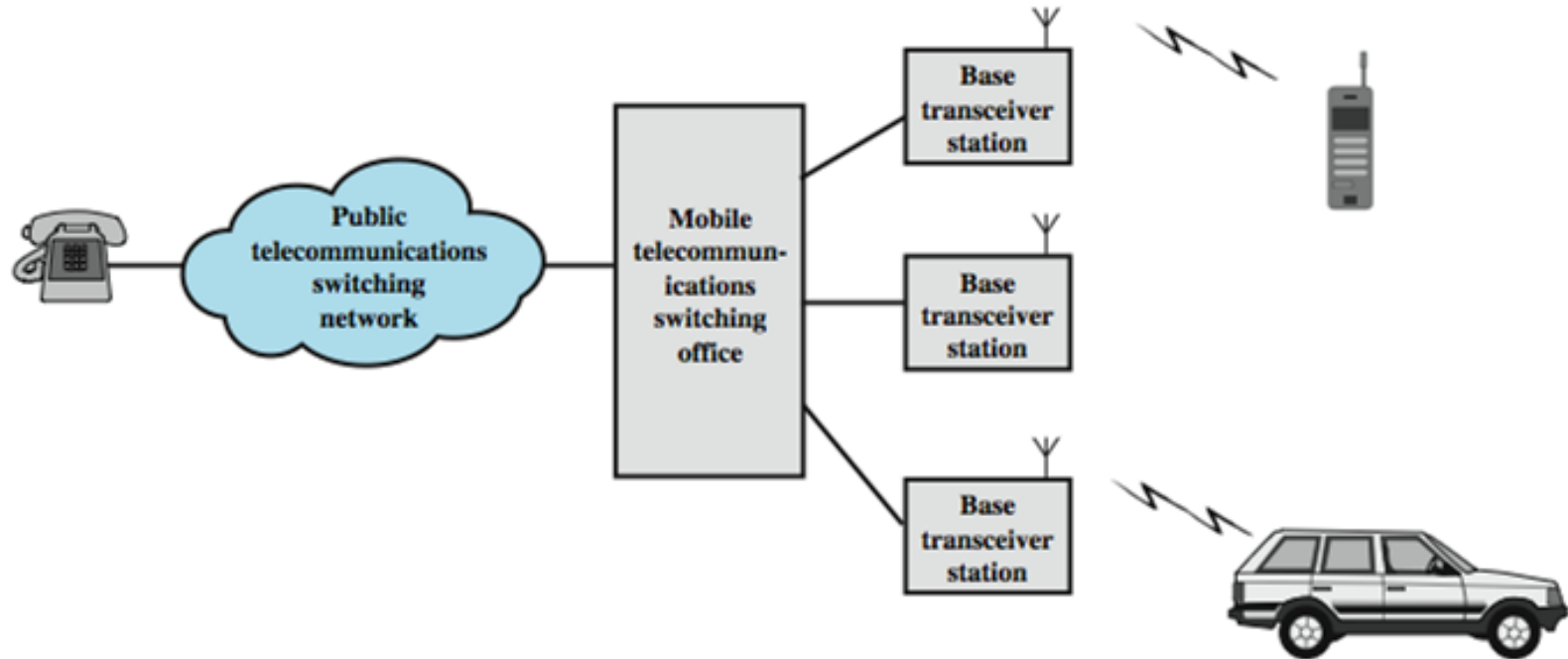
## Cellular Vulnerabilities

# Cellular Vulnerabilities

- Jaringan seluler merupakan jaringan nirkabel yang bertujuan untuk meningkatkan kapasitas penggunaan device mobile
- Sistem yang digunakan pada jaringan seluler adalah sistem yang menggunakan daya rendah, sehingga lebih cost effective dalam penggunaannya.
- Setiap device yang berperan dalam jaringan seluler akan memiliki antena masing masing menggunakan daya yang relative rendah, dan antara device yang saling berhubungan, contohnya antara device pengguna dengan BTS akan menggunakan frekuensi yang berbeda, agar mengurangi terjadi interferensi ataupun crosstalk.



# Cellular Vulnerabilities



# Cellular Vulnerabilities

## Perkembangan Jaringan Seluler

Technology	1G	2G	2.5G	4G
Design began	1970	1980	1985	2000
Implementation	1984	1991	1999	2012
Services	Analog voice	Digital voice	Higher capacity packetized data	Completely IP based
Data rate	1.9. kbps	14.4 kbps	384 kbps	200 Mbps
Multiplexing	FDMA	TDMA, CDMA	TDMA, CDMA	OFDMA, SC-FDMA
Core network	PSTN	PSTN	PSTN, packet network	IP backbone

# Cellular Vulnerabilities

- FDMA (Frequency Division Multiple Access)

Sistem multiple access yang menempatkan seorang pelanggan pada sebuah kanal berbentuk pita frekuensi (frequency band) komunikasi. Jika satu pita frekuensi dianggap sebagai satu jalan, maka FDMA merupakan teknik “satu pelanggan, satu jalan”.

- TDMA (Time-division Multiple Access)

TDMA memberikan satu pita frekuensi untuk dipakai beberapa pelanggan. Jadi kanal-kanal komunikasi dirupakan dalam bentuk slot-slot waktu. Slot waktu adalah berapa lama seorang pelanggan mendapat giliran untuk memakai pita frekuensi.

# Cellular Vulnerabilities

- CDMA (Code-division Multiple Access)

Kanal yang satu dengan lainnya tidak dibedakan dari frekuensi/FDMA atau waktu/TDMA yang secara awam lebih mudah dipahami, melainkan dengan perbedaan kode. Jadi pada CDMA, seluruh pelanggan menggunakan frekuensi yang sama pada waktu yang sama

Dhingra, M. et al, Wireless Network Security Threats and Their Solutions: a short study, International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-1,2, 2012

# Cellular Vulnerabilities



GLOBAL SYSTEM FOR  
MOBILE COMMUNICATIONS

- GSM merupakan standar seluler yang paling banyak digunakan dunia
- Handsets and SIMs
- International Mobile Equipment Identifier (IMEI)
- International Mobile Subscriber Identity (IMSI)

# Cellular Vulnerabilities

## Kelebihan GSM

- Jaringan lebih luas karena telah ada banyak provider GSM diseluruh Indonesia
- Bebas dari Roaming (1 nomor telepon tidak berubah walaupun sering berpindah provinsi)
- Teorinya, timeslot dedicated yang disediakan ini menjamin penggunaanya bisa mendapatkan kualitas layanan komunikasi yang lebih konstan, tidak naik turun.
- Handset & penyedia layanan yang tersedia untuk dipilih lebih beragam.

# Cellular Vulnerabilities

## Kekurangan GSM

- Sistem keamanan yang kurang baik sehingga mudah disadap
- ketika jaringan GSM sudah penuh, maka pemilik ponsel biasanya akan mengalami kesulitan untuk melakukan panggilan atau bahkan menerima panggilan. Hal ini disebabkan oleh tidak adanya timeslot kosong yang bisa digunakan.

# Cellular Vulnerabilities

## Penyalahgunaan di Indonesia

- Pemalsuan identitas pengisian informasi pengguna baru
- Pengoperasian penguat sinyal seluler (repeater) tanpa izin
- Penyalahgunaan internet gratis dengan SSH
- Penyalahgunaan trafik roaming internasional menjadi nasional melalui SIMBox



# Cellular Vulnerabilities

Pemalsuan identitas pengisian informasi pengguna baru

- Penyebab pemalsuan karena satu penduduk Indonesia memiliki lebih dari satu SIM Card
- Sistem pakai-buang SIM card
- Untuk Aktivasi SIM Card memerlukan registrasi NIK atau KK
- Terdapat penduduk Indonesia yang didaftarkan melalui NIK atau KK punya Outlet

# Cellular Vulnerabilities

## Penguat sinyal seluler (repeater) tanpa ijin

- Penyebabnya terdapat kantor atau rumah yang memiliki sinyal jelek pada salah satu operator
- Padahal di Indonesia terdapat 3 operator besar yang BTS nya sdh tersebar dimana saja
- Niatan yang baik dari masyarakat, namun kurang paham akan peraturan dari UU No. 36 tentang Telekomunikasi, PP No. 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi, dan Peraturan Menteri Kominfo No. 29/PER/M.KOMINFO/8/2008 tentang Sertifikasi Alat dan Perangkat Telekomunikasi.
- Akhirnya repeater yang dipasang masyarakat mengganggu sinyal dari BTS operator lain, contoh memperkuat sinyal penerimaan Telkomsel, namun karena pemasangan yang tanpa ijin, akhirnya melemahkan sinyal XL Axiata

# Cellular Vulnerabilities

## Penyalahgunaan internet gratis dengan SSH

- Penyebabnya masyarakat sangat membutuhkan internet, namun harga yang sulit terjangkau bagi masyarakat menengah ke bawah atau pelajar
- Terdapat sharing knowledge yang beredar bebas di internet tentang Config penggunaan SSH dan akun SSH
- Metodenya secara umum berupa inject pada service provider
- Terdapat Aplikasi Freeware Inject di internet

# Cellular Vulnerabilities

## Penyalahgunaan trafik roaming melalui SIMBox

- Harga Roaming Internasional yang cukup mahal di Indonesia
- Maraknya voice call dari luar negeri ke Indonesia
- Terdapat oknum yang memanfaatkan celah tersebut melalui perangkat SIMBox
- Pada umumnya, penelepon dari luar negeri ke Indonesia tidak akan dikenakan tarif roaming Internasional. Melainkan, akan dikenakan tarif lokal dimanapun asal negara penelepon internasional.

# Cellular Vulnerabilities

## Pemalsuan User (Pengguna)

- Penyusup mengirimkan sinyal pengguna kepada perangkat jaringan agar meyakinkan perangkat tersebut bahwa penyusup merupakan pengguna yang asli. Umumnya perangkat yang dimodifikasi adalah mobile station.

## Pemalsuan Jaringan (Sinyal Operator)

- Penyusup mengirimkan sinyal kepada pengguna agar meyakinkan pengguna tersebut bahwa penyusup merupakan jaringan yang asli. Umumnya perangkat yang dimodifikasi adalah Base Transceiver Station

# Cellular Vulnerabilities

## Man-in-the-middle

- Penyusup menempatkan dirinya antara pengguna dan perangkat jaringan, sehingga memiliki kemampuan untuk eavesdrop, modifikasi, menghapus, re-order, replay dan spoof sinyal. Perangkat yang dimodifikasi ialah Mobile Station dan Base Transceiver Station

## Eavesdropping (Memata-matai)

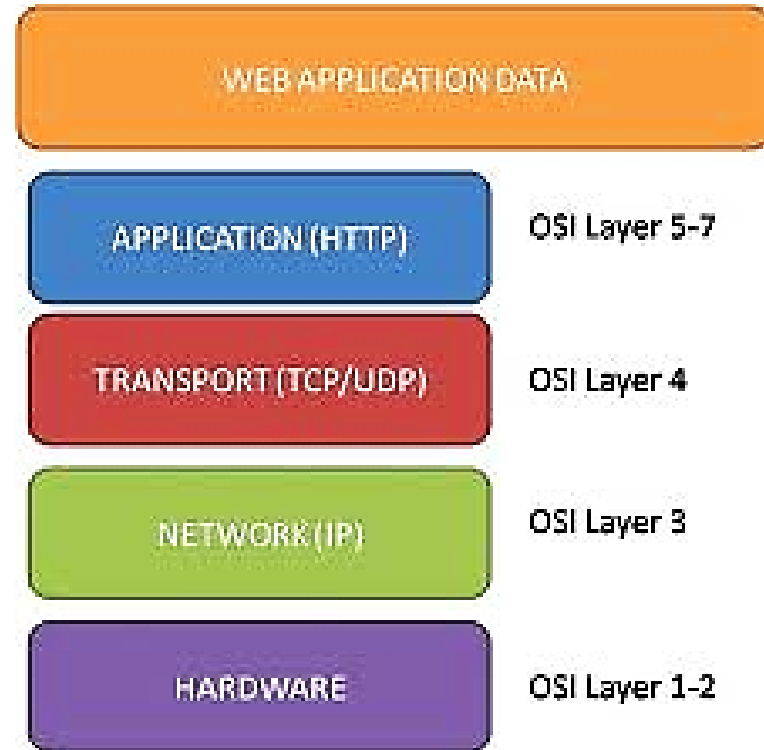
- Penyerang melakukan penyusupan melalui jalur sinyal dan jalur data yang terhubung dengan pengguna. Umumnya perangkat yang dimodifikasi adalah mobile station.

(Kerentanan Aplikasi)

# APPlication Vulnerabilities

# Application Vulnerabilities

- Keamanan aplikasi termasuk didalamnya pengukuran melalui life-cycle aplikasi untuk mencegah serangan pada sistemnya
- Layer utama adalah layer 7
- Keamanan aplikasi juga bagian dari Software (or System) Development Life-Cycle (SDLC)
- Pihak yang sangat memperhatikan keamanan pada aplikasi adalah pengembang aplikasi dan manajer dari pengembang aplikasi





# Application Vulnerabilities

## Resiko Pada Keamanan Aplikasi Desktop

- Akses Ilegal terhadap data pelanggan atau data perusahaan
- Pencurian data sensitive seperti data kartu kredit
- Terjadinya cracking aplikasi

# Application Vulnerabilities

## Resiko Pada Keamanan Aplikasi Jaringan

- Pengalihan link ke web berbahaya
- Deface Web
- Phishing dan malware distribution
- Denial of service;

# Tim Penyusun

- Alif Akbar Fitrawan, S.Pd, M. Kom (Politeknik Negeri Banyuwangi);
- Anwar, S.Si, MCs. (Politeknik Negeri Lhokseumawe);
- Eddo Fajar Nugroho (BPPTIK Cikarang);
- Eddy Tungadi, S.T., M.T. (Politeknik Negeri Ujung Pandang);
- Fitri Wibowo (Politeknik Negeri Pontianak);
- Ghifari Munawar (Politeknik Negeri Bandung);
- Hetty Meileni, S.Kom., M.T. (Politeknik Negeri Sriwijaya) ;
- I Wayan Candra Winetra, S.Kom., M.Kom (Politeknik Negeri Bali) ;
- Irkham Huda (Vokasi UGM) ;
- Josseano Amakora Koli Parera, S.Kom., M.T. (Politeknik Negeri Ambon) ;
- I Komang Sugiartha, S.Kom., MMSI (Universitas Gunadarma) ;
- Lucia Sri Istiyowati, M.Kom (Institut Perbanas) ;
- Maksy Sendiang, ST, MIT (Politeknik Negeri Manado) ;
- Medi Noviana (Universitas Gunadarma) ;
- Muhammad Nashrullah (Politeknik Negeri Batam) ;
- Nat. I Made Wiryana, S.Si., S.Kom., M.Sc. (Universitas Gunadarma) ;
- Rika Idmayanti, ST, M.Kom (Politeknik Negeri Padang) ;
- Rizky Yuniar Hakkun (Politeknik Elektronik Negeri Surabaya) ;
- Robinson A.Wadu, ST., MT (Politeknik Negeri Kupang) ;
- Roslina. M.IT (Politeknik Negeri Medan) ;
- Sukamto, SKom., MT. (Politeknik Negeri Semarang) ;
- Syamsi Dwi Cahya, M.Kom. (Politeknik Negeri Jakarta) ;
- Syamsul Arifin, S.Kom, M.Cs (Politeknik Negeri Jember) ;
- Usmanudin (Universitas Gunadarma) ;
- Wandy Alifha Saputra (Politeknik Negeri Banjarmasin) ;

# #JADIJAGOANDIGITAL TERIMA KASIH



digitalent.kominfo



DTS\_kominfo



digitalent.kominfo



digital talent scholarship