# ISU KEAMANAN FEMTOCELL

**Agung Ridwan SN**[1]
1Mahasiswa Magister Program Studi Teknik Telekomunikasi, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung
agung.ridwan@students.itb.ac.id

**Abstrak**

*Femtocell hadir dengan menawarkan layanan konektivitas jaringan mobile yang lebih baik yakni dengan menempatkannya di area yang lemah sinyal dan mengantarkan layanan jaringan mobile melalui jaringan berbasis IP ke operator service provider. Dengan membangun jaringan Femtocell maka mampu menurunkan biaya infrastruktur, berdaya rendah, plug and play, meningkatkan availabilitas dan mobilitas baik bagi pengguna maupun bagi operator jaringan. Peningkatan cakupan jaringan Femtocell akan memecah domain akses bagi operator sehingga perlu diperhatikan pula isuisu keamanan yang akan muncul dan bagaimana mengatasinya sesuai dengan standar keamanan yang berlaku. Beberapa Femtocell Access Point (FAP) yang ada di pasaran tidak memenuhi standar ini sehingga keamanannya dapat ditembus. Tulisan ini akan mensarikan informasi mengenai isu-isu keamanan jaringan Femtocell mulai dari sisi pengguna hingga ke sisi operator.*

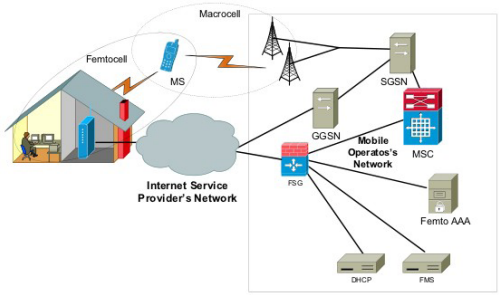
**Keywords**: *femtocell, jaringan seluler, hacking*

## Pendahuluan

Femtocell adalah sebuah *Base Transceiver Station* (BTS) mini yang ditempatkan pada wilayah bersinyal rendah sehingga dapat meningkatkan availabilitas, konektivitas, mobilitas, serta performansi layanan jaringan dengan kebutuhan daya yang rendah. Femtocell terhubung ke jaringan Service Provider melalui koneksi layanan broadband Internet, misalnya ADSL (*Assymmetric Digital Subscriber Line*). Instalasi perangkat Femtocell yang mudah dan murah, sehingga pemilik Femtocell dapat membangun sendiri jaringan Femtocell di wilayahnya dan dapat pula disewakan untuk pengguna lain yang ingin berlangganan ke jaringan Femtocell di wilayah itu. Bagi operator kehadiran Femtocell dapat menurunkan biaya pembangunan infrastruktur serta memberikan layanan yang lebih prima kepada pelanggan pada daerah yang tidak terjangkau. Pemasangan perang-kat Femtocell tidak hanya pada tempat-tempat ruangan tertutup dari suatu gedung, tetapi juga dapat diterapkan pada daerah terpencil dan wilayah sekitar terjadinya bencana sehingga dapat meningkatkan mobilitas jaringan seluler dengan mudah dan cepat. Namun bagaimana jika segala kemudahan tersebut dapat menimbul-kan potensi keamanan tersendiri dan memberikan masalah baru baik bagi pelanggan, non-pelanggan, dan operator jaringan.

Seperti misalnya kasus yang pernah terjadi pada Vodafone[1]. Serangan Femtocell pada jaringan Vodafone dilakukan pada awal tahun 2010 oleh sekelompok grup yang menamakan dirinya sebagai The Hacker Choice (THC). THC menemukan celah keamanan dan dapat melakukan eksploitasi terhadap perangkat tersebut. Vodafone kemudian mengaku telah mengatasi masalah tersebut. Namun yang terjadi serangan berikutnya pada bulan Juli 2011 oleh kelompok yang sama[2] dimana hacker meretas port serial pada FAP dan dapat mengambil alih secara penuh terhadap *access point*

tersebut. Sejak adanya serangan itu Vodafone kembali menambal celah keamanannya[3].




*Gambar 1: Topologi Jaringan Femtocell[4]*

Kehadiran Femtocell secara komersial dibuat sejak tahun 2007. Beberapa vendor telah memproduksi sejumlah perangkat Femtocell Access Point (FAP) dan dijual ke pasaran. Sejumlah negara yang telah menggunakan perangkat Femtocell diantaranya Jepang, Amerika, Cina, dan sebagainya. Berikut adalah tabel informasi beberapa negara yang menggunakan Femtocell beserta operator jaringannya.

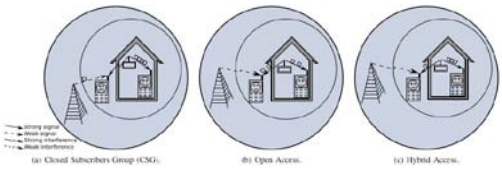
Tabel 1. Beberapa negara yang telah menggunakan Femtocell[5]

| Operator | Country |
|---|---|
| Sprint | US |
| StarHub | Singapore |
| Verizon Wireless | US |
| Vodafone | UK, Spain, Qatar, Greece, New Zealand |
| AT&T | US |
| SFR | France |
| NTT DoCoMo | Japan |
| China Unicom | China |
| Optimus | Portugal |
| SingTel | Singapore |
| SoftBank | Japan |
| KDDI | Japan |
| Movistar | Spain |
| T-Mobile | UK |
| MoldTelecom | Molodova |

## Pembatasan Akses Pengguna Femtocell

Saat setiap pengguna dapat menggunakan akses jaringan selulernya melalui Femtocell, maka akan muncul isu keamanan yang baru. Artinya siapa pun dalam berpotensi menimbulkan masalah keamanan baik itu sengaja maupun tidak sengaja (dikuasai oleh orang lain). Untuk itu 3GPP (3rd Generation Partnership Project) membuat model akses kontrol jaringan Femtocell yang berguna untukmembatasi siapa saja yang berhak terhubung ke FAP[6]. Metoda akses jaringan Femtocell ini dibagi menjadi tiga, yaitu Open Access, Closed Subscriber Group (CSG), dan Hybrid[7]. Masing-masing model akses kontrol ini memiliki kelebihan dan kekurangan masingmasing serta pengaruhnya terhadap keamanan jaringan.

Open Access memiliki keamanan yang paling rentan diantara yang lain dan berpeluang menurunkan performansi karena tidak ada batasan siapa saja pengguna yang diperbolehkan mengakses FAP. Penyerang dapat melakukan berbagai serangan terhadap target dengan mudah pada jenis ini. Pada CSG, yang bukan pelanggan tidak dapat mengakses jaringan meskipun sinyal FAP lebih kuat dari sinyal Macrocell. Kondisi ini berpeluang terjadinya interferensi dan jamming sehingga akan sulit terhubung ke FAP. Hybrid dapat menawarkan solusi yang lebih baik terhadap masalah performansi yang akan dihadapi pelanggan dan memberikan perizinan akses yang bertingkat-tingkat kepada onpelanggan.



*Gambar 2: Metode Akses Femtocell [7]*

## Femtocell Access Point

Sebagian besar FAP yang banyak beredar di pasaran memiliki celah keamanan. Hal ini disebabkan karena perangkat tersebut tidak mengikuti standar 3GPP2 dan GSMA[8] yang telah berlaku sehingga dapat diretas (hacking) dan dapat berakibat buruk bagi pelanggan Femtocell[9]. Saat serangan

terhadap FAP telah dilakukan dan perangkat tersebut telah dikuasai, maka data-data sensitif yang bersifat pribadi seperti akun bank, password, dan lainnya dapat diperoleh.

Beberapa jenis serangan yang dapat terjadi pada perangkat Femtocell diantaranya serangan pensinyalan, Femtocell *Botnets*, penyadapan secara global, injeksi trafik dengan kamuflase (otentikasi), merubah trafik (integritas), pengambilan informasi IMSI (kerahasiaan). Jika dirangkum secara keseluruhan masalah dari Femtocell ini terbagi menjadi tiga, yaitu keamanan *end-user* yang meliputi aspek integritas, kerahasiaan, otentikasi, dan availabilitas; keamanan pada sisi infrastruktur terhadap perangkat FAP yang nakal; dan keamanan pada saat melakukan implementasi pembangunan jaringan Femtocell[10]. Berdasarkan lokasi target penyerangan dibagi menjadi serangan pada udara (pasif/aktif), serangan pada femtocell, dan serangan pada core network[11].

FAP juga dapat di-*spoof* sehingga penyerang dapat membuat FAP palsu dan melakukan penetrasi penyerangan terhadap korban. Ada teknik atau metoda pertahanan yang dapat dilakukan untuk menanggulanginya, yaitu dengan menggunakan Improved Proxy Signature[12].

**Link Backhaul Femtocell**

Sejak link Backhaul Femtocell menggunakan jaringan publik Internet maka perlu diperhatikan keamanannya. Femtocell Access Point (FAP) terhubung ke Femtocell Security Gateway (FSG) pada sisi operator melalui protocol IPsec. IPsec akan menyediakan koneksi link yang aman dari FAP ke FSG dengan memperhatikan tiga hal: kerahasiaan data, integritas data, dan sistem otentikasi atau yang biasa dikenal dengan singkatan CIA (Confidentiality, Integrity, dan Authencity).

Encapsulating Security Payload (ESP) termasuk dalam bagian dari protokol IPsec yang berfungsi untuk menjamin kerahasiaan data dengan melakukan enkapsulasi terhadap paket data. Kemudian untuk menjamin integritas suatu data digunakan HMAC-SHA1. HMAC-SHA1 (Hash-based Message Authentication Code) menjamin integritas suatu data dengan membandingkan nilai checksum dari pengirim ke tujuan menggunakan algoritma fungsi hash SHA1SUM sebanyak 160 bit[13]. Jika sama maka data tersebut tidak mengalami perubahan selama dalam perjalanan. Kemudian untuk menjamin agar host tujuan yang benarlah yang akan menerima informasi dari sumber, maka digunakan sistem otentikasi IKEv2 (Internet Key Exchange). Dua host ini akan saling berkomunikasi melalui *secure key agreement* melalui media *tunnel*[14][15].

Proses aliran data yang terjadi antara FAP dengan FSG berdasarkan aliran komunikasi standarisasi 3GPP, yaitu FAP pertama-tama melakukan otentikasi dan otorisasi. Jika sukses maka FAP meminta alamat IP lokal untuk dirinya. Melalui DNS untuk mendapat-kan alamat gateway. Lalu membangun IPsec tunnel dengan cara inisiasi asosiasi melalui IKEv2 dan meminta IP remote pada payload IKEv2 yang terkonfigurasi. Setelah itu IPsec tunnel berhasil dibangun dan komunikasi antar-IP terhubung melalui media tunnel.

Protokol IPSec dinilai kurang baik digunakan untuk jenis paket data *voice*, karena memiliki *overhead* yang cukup signifikan terhadap ukuran paket data *voice* yang relatif lebih kecil. Sehingga alternatif protokol lain yang dapat digunakan, yaitu TLS dan DTLS di bawah mekanisme NAT (Network Address Translation)[4].

Peningkatan keamanan terhadap mobilitas pengguna yang berkaitan terhadap teknologi jaringan Femtocell meliputi layanan registrasi, verifikasi identitas, dan noda multihoming dapat diwujudkan dengan Location Locking Methods dan Host Identity Protocol (HIP). Teknik verifikasi lokasi yang ada saat ini memiliki kelemahan dan sebaiknya dihindari[16]. HIP dapat meningkatkan dukungan mobilitas dengan memisahkan identitas/lokasi dan noda multi-homing tanpa melihat IP sebagai identitas[17].

**Kesimpulan**

Keamanan jaringan Femtocell perlu diperhatikan mulai dari sisi user hingga ke network operator. Tidak ada sistem yang sempurna, masing-masing memiliki potensi celah keamanan sehingga perlu menjadi perhatian dan kewaspadaan bagi pengguna, pemilik FAP, dan network operator. Secara umum dapat dikatakan bahwa apa-apa yang ada pada jaringan 2G/3G/4G/ WiMax dan jaringan berbasis IP juga merupakan isu keamanan yang berpeluang muncul pada jaringan Femtocell. GSMA dan 3GPP telah membentuk aturan dan mekanisme teknik berupa standar yang seharusnya direalisasikan oleh vendor. Kebanyakan vendor gagal memenuhi hal itu sehingga menimbulkan masalah pada perangkat Femtocell.

**Daftar Pustaka**

[1] Anonymous. The Hacker's Choice, http://wiki.thc.org/vodafone [2] Steve Gold. *Cracking cellular networks via femtocells*. 2011.

[3] R. Rajavelsamy, Jicheol Lee and Sungho Choi. *Towards security architecture for Home (evolved) NodeB: challenges, requirements and solutions*. Security ommunications Networks. 2011.

[4] Tomas Vanek, Matej Rohlika. *Alternative Protocols for Femtocell Backbone Security*. IFIP WMNC 2011.

[5] Anonymous. *Regulatory Aspects of Femtocells Second Edition*. 2011. Femto Forum.

[6] Assen Golaup, Mona Mustapha, and Leo Boonchin Patanapongpibul. *Femtocell Access Control Strategy in UMTS and LTE*. IEEE Commnunications Magazine, September 2009.

[7] Guillaume de la Roche, et al. *Access Control Mechanisms for Femtocell*. IEEE Communications Magazine, JULY 2009.

[8] Robindhra Mangtani. *Security Issues in Femtocell Deployment*. (GSMA). 23 July 2008.

[9] Ravishankar Borgaonkar, Kevin Redon, Jean-Pierre Seifert. *Security Analysis of a Femtocell Device*. SIN'11. 2011.

[10] Ravishankar Borgaonkar, Nico Golde, et al. *Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunication*. ttp://www.isti.tu-berlin.de. Akses: 4 Maret 2012.

[11] Igor Bilogrevic, Jean-Pierre the baux, et al. *Security Issues in Next Generation Mobile Networks: LTE and Femtocell*. Femtocell Workshop. 2010.

[12] Chan-Kyu Han, Hyoung-Kee Choi. *Building Femtocell More Secure with Improved Proxy Signature*. GLOBECOM. 2009.

[13] Anonymous. IPsec. http://en. wikipedia.org/wiki/IPsec. Diakses: 2 Mei 2012.

[14] Tomas Vanek, Matej Rohlik. *Perspective Security Procedures for Femtocell Backbone*. ICUMT. 2011.

[15] Jing Chen and Marcus Wong. *Security Implications and Considerations for Femtocells*. Journal of Cyber Security and Mobility, 21–35. 2012.

[16] Ravishankar Borgaonkar, Kevin Redon, et al. *Experimental Analysis of the Femtocell Location Verification Techniques*. 2010.

[17] Suneth Namal, et al. *Securing the Backhaul for Mobile and*