

KEAMANAN WIRELESS WEB MENGGUNAKAN WIRELESS TRANSPORT LAYER SECURITY PROTOKOL (WTLS)



**OLEH :
WINARTO
23202155
(Kelas Dikmenjur)**

**DEPARTEMEN TEKNIK ELEKTRO
BIDANG KHUSUS TEKNOLOGI INFORMASI
PROGRAM PASCASARJANA
INSTITUT TEKNOLOGI BANDUNG
2004**

DAFTAR ISI

Daftar isi	2
A. Model keamanan dalam wireless web	3
Kriptografi kunci publik dan kunci privat	4
B Model Pengamanan Dengan WTLS	6
1. Cara Kerja WTLS	7
a. Kelas-Kelas WTLS	8
b. Celah dari WAP	8
2. Tujuh lapis dari pengamanan titik ke titik	9
a. Embedded Security Technology	10
b. Mobile Operator Network Security	10
c. Secure Mobile operator Gateways	11
d. Authentication	11
e. Data Center and Network Security	11
f. Secure Application Interfaces	15
3. Problem dalam model pengamanan titik ke titik	15
a. Sniffing dan Spoofing	15
b. Session Management and URL Rewriting	16
c. Man-in-the-Middle Attack	16
d. Tidak ada solusi yang tidak lengkap	16
4. Teknologi PKI dan Model Keamanan dari ujung ke ujung	17
a. Penerapan PKI	18
b. Keterbatasan Teknologi PKI	20
C. Kesimpulan	20

KEAMANAN WIRELESS WEB MENGGUNAKAN WIRELESS TRANSPORT LAYER SECURITY PROTOKOL (WTLS)

A. Model keamanan dalam wireless web

Terdapat dua model pengamanan untuk wireless yaitu dari titik ke titik dan dari ujung ke ujung. Dalam aplikasi Web banyak lengan dalam perjalanan data yang diperlukan untuk komunikasi peralatan bergerak (mobile device) dalam mengadakan transaksi. Pengamanan dari titik ke titik berarti komunikasi diamankan pada masing-masing lengan dan berpindah dengan teknologi keamanan yang sesuai untuk setiap bagian komunikasi.

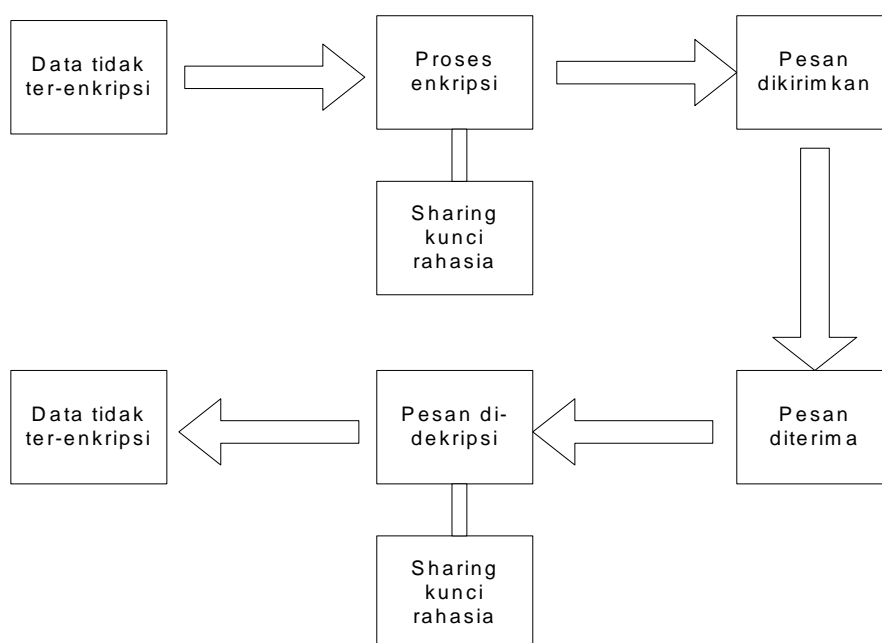
Dengan menyatukan potongan-potongan kerja teknik pengamanan dapat menutup seluruh perjalanan dari peralatan bergerak sampai dengan aplikasi dan sebaliknya. Sayangnya pada setiap titik dimana satu tipe sistem keamanan mulai dihentikan dan tipe yang lain dimulai hal ini secara teoritis memungkinkan mendapat serangan.

Pengamanan dari ujung ke ujung berarti bahwa hanya ada satu teknologi pengamanan yang bekerja pada seluruh jalur dari ujung peralatan sampai dengan sampai dengan aplikasi dari berbagai jaringan yang dipergunakan berkomunikasi.. dalam keamanan seperti ini pengamanan titik ke titik tetap dipergunakan hanya sebagai cadangan untuk bertahan. Dengan keamanan dari ujung ke ujung aplikasi wireless akan lebih aman sebagai aplikasi berbasis Web. Sayangnya hal ini tidak akan menyelesaikan tanpa adanya pembatasan dalam aplikasi wireless, peralatan dan browser yang dipergunakan. Sebagaimana teknologi *Secure Sockets Layer* (SSL) dan *Public Key Infrastructure* (PKI) dalam Web pengamanan dari ujung ke ujung berarti informasi dienkripsi sebelum meninggalkan peralatan bergerak dan tetap terenkripsi sebelum mencapai server dalam suatu jaringan yang aman.. Tidak seperti dalam web disana terdapat berbagai teknologi PKI yang berbeda, masing-masing hanya mendukung peralatan bergerak, browser dan aplikasi tertentu.

Kriptografi kunci publik dan kunci prifat

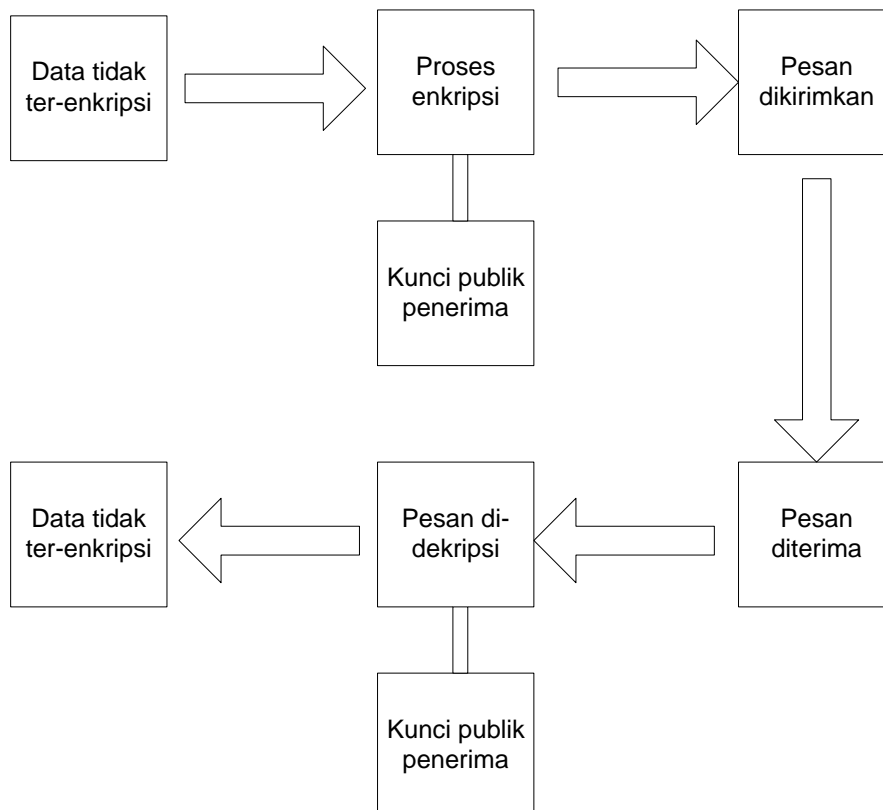
Solusi menggunakan pengamanan dengan titik ke titik dan dari ujung ke ujung keduanya memerlukan suatu bentuk kriptografi. Kriptografi adalah ilmu yang mengambil informasi biasa dan merubahnya menjadi sesuatu yang hanya dapat dimengerti oleh penerima pesan yang dimaksud. Intermediate data atau cipher text kelihatannya acak dan tidak dapat dikembalikan seperti semula oleh seseorang tanpa mengetahui bagaimana mengkonversi kembali menjadi menjadi informasi yang dapat dimengerti. Metoda mengenkripsi dan mengembalikannya data menggunakan algoritma matematika yang dinamakan *cryptosystems*. Banyak algoritma yang mengenkrip dan men-dekrip data dengan sistematis dalam informasi data yang dikenal dengan nama *kunci*. Sebuah data yang dienkripsi hanya dapat dibuka kembali oleh orang aorang yang tahu algorima enkripsinya dan kunci enkripsi. Hal ini mempersulit orang orang yang tidak berhak mengambil informasi dalam perjalanannya. Di Internet kunci hanya dibuat dan diedarkan dalam bentuk sertifikat digital.

Terdapat dua macam dasar kriptografi yang menggunakan kunci. Yang pertama adalah kriptografi dengan kunci prifat, yang menggunakan algoritma simetris untuk mengendripsi dan mendekripsi data menggunakan kunci yang sama. Ini kadang kadang dinamakan kriptografi kunci rahasia (*secret key cryptography*) sebab saling berbagi rahasia atau kunci yang digunakan dikedua ujung komunikasi.



Metoda pertukaran kunci publik dan kunci prifat sangat kritis dalam kriptografi sehingga pertukaran kunci harus benar-benar aman dalam sistem kriptografi. Metoda untuk pertukaran kunci dalam sistem kriptografi ditemukan oleh Rivest Shamir Adelman (RSA), Diffie-Hellman, and Elliptic Curve Diffie-Hellman systems.

Tipe kriptografi yang kedua adalah kriptografi kunci publik (*public key cryptography*) menggunakan algoritma *asymmetric*, hal ini berarti informasi dienkripsi menggunakan salah satu kunci (kunci publik), kemudian didekripsi menggunakan kunci yang lain (kunci prifat). Dalam dkriptografi menggunakan kunci publik kenyataannya menggunakan dua kunci di masing masing ujung. Kunci prifat hanya diketahui oleh penerima informasi dan kunci publik diketahui oleh pengirim sebagaimana orang orang yang lain. Informasi dienkripsi menggunakan kunci publik tetapi hanya dapat dibuka oleh penerima menggunakan kunci prifat. Selamanya hanya penerima pesan yang dapat membuka pesan tersebut, kriptografi kunci publik dapat juga digunakan untuk memeriksa identitas dari penerima. Hal ini berkenaan dengan digital authentication.

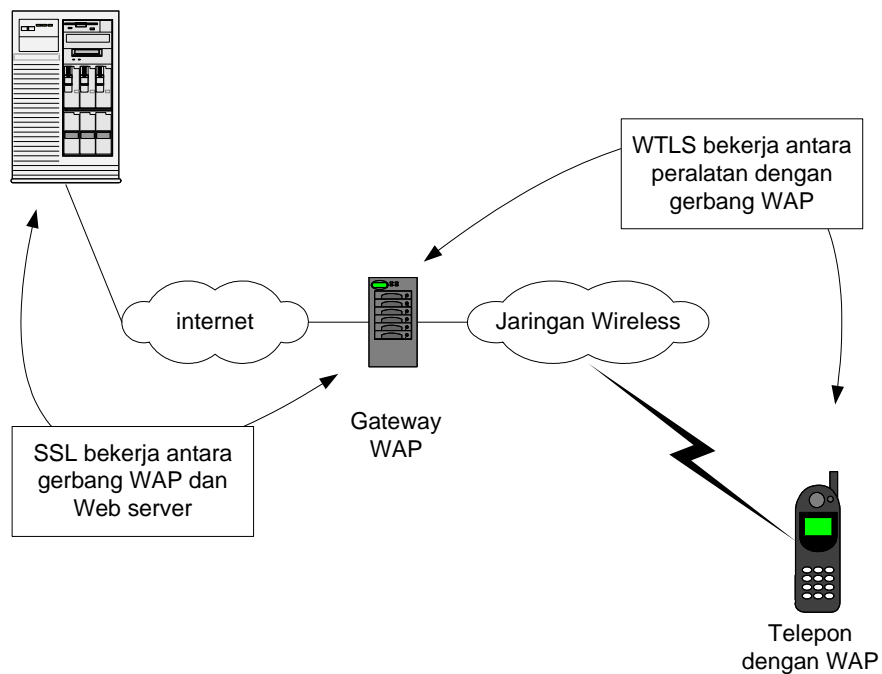


Untuk enkripsi dengan kunci privat dan kunci publik, derajat keamanan tergantung kepada algoritma dan panjang dari kunci. Metoda enkripsi menggunakan kunci untuk mengenkripsi data mengacu pada *cipher*. Blok cipher memecah informasi kedalam beberapa blok yang mempunyai panjang tetap (normalnya 64 bit) dan selanjutnya mengenkripsi masing masing blok menjadi kunci rahasia bersama (shared secret key). Blok cipher menggunakan kunci yang sama untuk semua enkripsi. Urutan cipher mengenkripsi sebagian kecil data menggunakan sederetan kunci yang dihasilkan oleh kunci bersama (shared key) yang terpisah atau pembangkit kunci untuk setiap blok dari informasi yang dienkripsi.

SSL menggunakan beberapa enkripsi cipher yang telah didefinisikan dengan baik yang terdiri RC5, *Data Encryption Standard* (DES), 3DES dan *International Data Encryption Algorithm* (IDEA). DES merupakan salah satu contoh cipher yang mengenkripsi 64-bit blocks data dengan 56-bit shared secret key yang pada awalnya dikembangkan oleh IBM dan selanjutnya diadopsi sebagai standard oleh pemerintah Amerika.

B. Model Pengamanan Dengan WTLS

Yang terpenting dari pengamanan dari titik ke titik adalah bagaimana informasi diamankan pada setiap lengan pada saat pejalanannya dari user sampai Web server dengan menggunakan teknologi pengamanan untuk masing masing bagian dari komunikasi. Yang terpenting teknologi dalam pengamanan model dari titik ke titik adalah *Wireless Transport Layer Security* (WTLS). WTLS adalah sebanding dengan *Secure Sockets Layer* (SSL) untuk *Wireless Application Protocol* (WAP), dan disana menyediakan enkripsi antara browser wireless dengan gateway WAP. Kebanyakan strd WTLS (WTLS Class 1) adalah didesain untuk bekerja bersama SSL sehingga WTLS dapat bekerja pada sisi jaringan wireless dengan gateway WAP dan SSL bekerja disisi internet. WTLS dan SSL bersama sama memastikan bahwa informasi dalam keadaan terenkripsi dari titik ke semua titik pada jalan dari browser wireless ke Web server.



1. CARA KERJA WTLS

WTLS adalah bagian dari spesifikasi desain WAP untuk memastikan privasi, kebenaran dan integritas dalam komunikasi. Lalulintas komunikasi diudara mungkin juga terenkripsi tergantung pada jaringan wireless dan teknologi yang menghubungkannya, sebagaimana WTLS, akan tetapi hal ini tidak menyediakan enkripsi yang benar-benar dari ujung ke ujung.

Tiga komponen utama dalam WTLS adalah: (1) protokol *Handshaking* yang menyediakan pertukaran kunci; (2) struktur perekaman untuk informasi terenkripsi dan (3) *Wireless Identity Module* (WIM). Protokol handshaking digunakan ketika clien dan server menginisialisasi sesi. Selama proses handshaking cliend mendukung metoda cryptographic dan pertukaran kunci dan server memilih metoda yang telah ditentukan. Setelah autentifikasi masing masing, client dan server memilih versi protocol dan chipper. WTLS membawa bentuk strd SSL dan mendukung RC5, DES, 3DES, dan IDEA chipper, akan tetapi DES dan 3DES yang banyak digunakan. WTLS juga menyediakan pertukaran kunci yang berbasis tanpa nama kedalam server public key. Ketika autentifikasi tanpa nama clien mengekrip kunci rahasia menggunakan server public key dan mengirimkan *Client Key Exchange message* . Struktur perekaman dalam WTLS menyediakan mekanisme untuk privasi data dan pengecekan integritas data.

a. Kelas Kelas WTLS

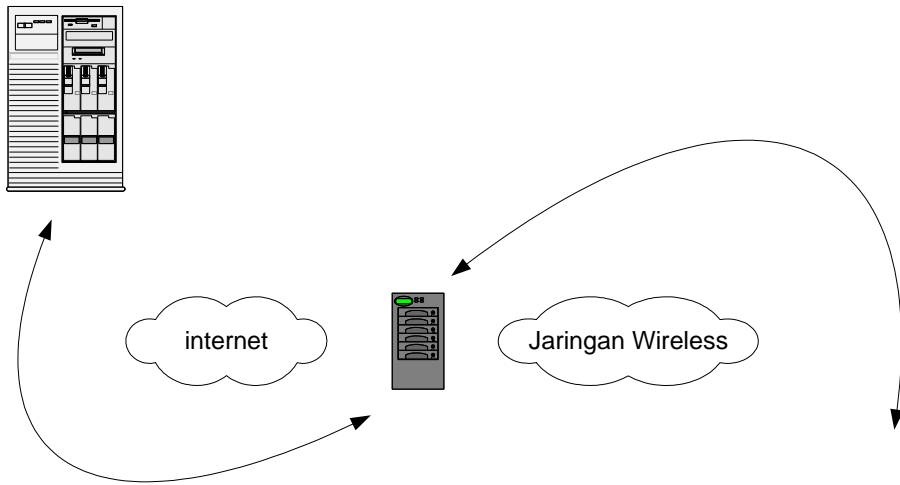
WTLS terdiri dari tiga kelas, yaitu:

- WTLS kelas I, yang hanya menyediakan enkripsi antara wireless browser dengan wireless web.
- WTLS kelas II, Sepenuhnya sama dengan SSL didalam internet sebab dia memberikan enkripsi seperti SSL langsung antara browser wireless dengan web server.
- WTLS kelas III, menyediakan framework untuk PKI security.

b. Celah dari WAP

Peralatan bergerak yang menggunakan WAP tidak berhubungan secara langsung dengan web server atau aplikasinya kemungkinan ya atau tidak mendukung protokol HTTP atau SSL. Kenyataannya gateway WAP sebagaimana proxy server untuk peralatan bergerak. Sebuah gateway menterjemahkan komunikasi dari satu bentuk ke bentuk ke yang lain. Dalam kasus ini gateway WAP menterjemahkan komunikasi dari protokol WAP ke protokol HTTP melalui internet. Ketika gateway meneruskan permintaan ke webserver untuk kepentingan peralatan bergerak dia menggunakan protokol WAP untuk berkomunikasi dengan peralatan dan HTTP untuk berkomunikasi dengan WEB server. Seperti Web browser gateway WAP mendukung SSL yang merupakan metode standard untuk meng-enkripsi komunikasi HTTP. SSL umumnya digunakan antara Web browser dan web server. Komunikasi antara peralatan bergerak dan gerbang WAP diamankan dengan WTLS dan komunikasi antara gateway WAP dan Web server diamankan dengan SSL. Gerbang WAP men-decrypt komunikasi dengan WTLS dan kemudian meng-encrypt kembali dengan SSL. Hal ini berarti disisi gateway WAP informasi tidak ter-enkripsi pada titik ini. Hal ini secara teoritis memungkinkan kesalahan dalam wab gateway dan membuka komunikasi HTTP yang tidak terenkripsi daripada menggunakan SSL.

Celah dalam WAP seperti dalam gambar berikut ini yang merupakan titik ideal untuk man in the middle attack.



4. Secure Mobile operator Gateways
5. Authentication
6. Data Center and Network Security
7. Secure Application Interfaces

a. Embedded Security Technology

Lapisan pertama yang dijaga dalam system computer adalah selalu diujung terminal. Akses phisik pada peralatan harus selalu dikontrol. Jika peralatan ini adalah sebuah pesawat telephone, kerap kali mempunyai kode pengunci atau password yang mencegah dari pemakaian tanpa memasukkan kode. PDA sebagaimana peralatan Palm OS mempunyai pasword dan pengunci untuk mencegah pemakaian yang tidak berhak jika pelatan tersebut hilang atau tercuri. Komputer notebook mempunyai kemampuan yang sama dalam BIOS atau tersedia dalam operating system. Ini akan efektif apabila kemampuan ini Webmaster wireless harus bebas mengatur kebijaksanaan keamanan dan menentukan strd konfigurasi untuk peralatan yang dipergunakan dalam jaringan dan server. Tidak seperti desktop workstation, kita berharap bahwa peralatan bergerak tidak dapat dielakkan dari hilang atau tercuri. Pedoman mencakup apa dan bagaimana untuk berkomunikasi dan mengamankan informasi yang rahasia ketika semua yang lainnya keliru. Kebijaksanaan pengamanan pada barisan terkhir untuk bertahan adalah pemakai harus harus mengatakan apa yang akan disimpan dalam peralatan bergerak sebagaimana PDA. Pemakai harus dianjurkan untuk memperlakukan peralatan komunikasi wirelessnya sama dengan yangdiharapkannya sebagai percakapan yang pribadi dengan sesama pekerja didalam area umum.

b. Mobile Operator Network Security

Keamanan WTLS diperluas sepanjang melekat dengan *keamanan hubungan udara (air-connect security)* melalui berbagai operator jaringan bergerak sampai dengan tepi internet pada WAP gateway. Sepintas lalu setelah meninggalkan WAP Gateway sudah tidak diamankan oleh teknologi WTLS atau keamanan internal jaringan operator. Sama dengan ketika pemakai memasuki area dimana dia tidak mendapatkan pelayanan yang sama atau mungkin menggunakan teknologi *keamanan hubungan udara (air-connect security)* yang lebih rendah sebagaimana dalam sistem analog AMPS. Teknologi keamanan yang diterapkan pada antarmuka udara seperti

pada CDMA adalah didesain guna mengamankan jaringan dan dan pelanggan dari kesalahan penggunaan seperti tercurinomor telephone atau penggunaan jaringan oleh orang orang yang tidak berhak. Keamanan dari interface udara itu sendiri dan jaringan operator bergerak meningkatkan keamanan dari pelayanan data wireless seperti WAP briwsing, tetapi juga didesain utuk mengamankan komunikasi data

c. Secure Mobile operator Gateways

Celah dalam WAP dan potensi untuk *Man-in-the Middle Attack* berarti bahwa keamanan dari operator bergerak WAP gateway adalah kritis. Didalam WAP gateway informasi dienkripsi melalui WTLS class 1 dilaksanakan deenkripsi kemudian dienkripsi kembali menggunakan SSL. Informasi mudah diserang pada titik ini. Sebagai webmaster kita tidak dapat mengatur operator WAP gateway dan tidak ada jalan untuk mengetahui mesin-mesin yang digunakan untuk membuat kompromi. Untuk suatu organisasi memungkinkan untuk membeli jaringan pelayanan sehingga memungkinkan meminta deskripsi dari keamanan jaringan yang biasanya disediakan oleh penyedia layanan internet. Hanya ada satu cara supaya tidak tergantung pada hal ini adalah dengan menerapkan keamanan dari ujung ke ujung SSL atau PKI.

d. Authentication

Membuka aplikasi adan informasi pada web berarti harus menyediakan lebih dari sari baris pengamanan terhadap akses oleh yang tidak berhak dan kejahatan hacker. Strategi yang sederhana adalah mendukung satu str authentication seperti pada *Remote Authentication Dial-In Use Service (Radius) atau Lightweight Directory Acces Protocol (LDAP)* yang berbasis pada user-ID/ password. Teknologi seperti pada Secure ID dapat mudah ditambahkan pada aplikasi wireless akan tetapi tidak mudah untuk pemakai hal ini berkaitan dengan terbatasnya kecepatan memasukkan informasi kedalam telephone bergerak atau dalam wireless PDA.

e. Data Center and Network Security

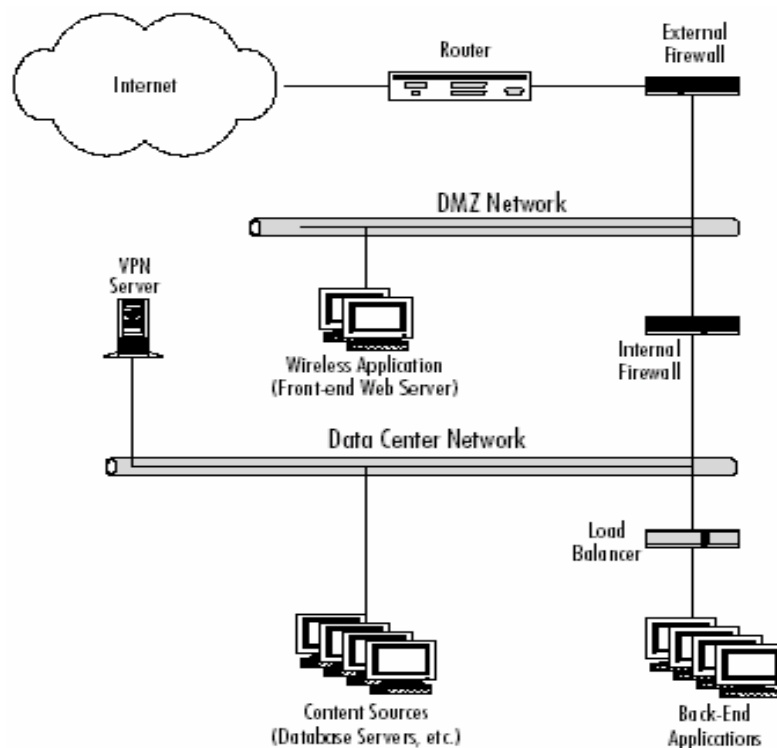
Jika kita menggunakan sebuah WASP kita harus memastikan bahwa fasilitas pusat data WASP adalah aman. Hal ini berarti pengaman phisik, kebijaksanaan keamanan, prosedur dan metoda operasi dan tols untuk mendeteksi adanya upaya

penyusunan. Jelasnya WASP harus tersedia arsitektur keamanan dan dalam prakteknya meliputi:

1. Secure Data Center Design
2. Customer Network Isolation
3. Secure Router Configurations
4. VPNs and Private Pipes
5. Secure Methodology
6. Security Management
7. Security Auditing

Secure Data Center Design

Sebuah data center yang aman terdiri atas arsitektur jaringan fisik yang memisahkan server dan pemakai informasi dari akses melalui internet. Hal ini umumnya menggunakan dua firewall yang mana server yang diakses dari internet dipisahkan dari mesin yang lain dan akses ke mesin dibatasi dengan firewall yang kedua hanya untuk alamat jaringan dan aplikasi tertentu.



Customer Network Isolation

Mengisolasi pemakai jaringan berarti bahwa firewall dikonfigurasi untuk memisahkan masing-masing data dan customer server. Hal ini mengurangi penerimaan informasi yang tidak aman jika ada yang tidak terenkripsi dari berbagai alasan dari penyedia jasa layanan jaringan.

Secure Router Configurations

Sebagaimana penyedia jasa layanan lainnya, harus mempunyai router jaringan WISP dan konfigurasi alat yang aman. Hal ini berarti bahwa peralatan dikonfigurasi dengan benar sesuai dengan prosedur yang telah ditetapkan. Jalan yang terbaik untuk memastikan bahwa konfigurasi router jaringan WISP aman adalah melalui audit yang terpisah.

Virtual Private Network (VPN)

Agar jaringan-jaringan pribadi yang terdistribusi dapat saling berkomunikasi secara aman melalui jaringan umum seperti internet, dibutuhkan pengamanan data terhadap pencurian.

Sebuah sistem VPN mengatasi masalah ini dengan menciptakan suatu Jaringan Pribadi Virtual (Virtual Private Network) sehingga remote user (pengguna jarak jauh) yang menjadi anggota jaringan pribadi virtual tersebut dapat berkomunikasi secara bebas dan aman melalui jaringan umum.

Sebuah VPN, biasanya menggunakan internet sebagai tulang punggung transportasi data untuk membuat jalur yang aman dengan partner bisnis, mengembangkan komunikasi dengan kantor cabang regional dan di daerah terisolasi. VPN dapat menurunkan biaya komunikasi dan meningkatkan mobilitas tenaga kerja karena akses internet biasanya lokal dan jauh lebih murah dibandingkan dengan sebuah server khusus untuk remote akses (dedicated remote access server).

Ketersediaan sebuah teknologi *Virtual Private Network* atau koneksi jaringan pribadi menjadi pertimbangan yang penting. Sebuah VPN kenyataannya menyerupai

penghantar melalui internet. Informasi yang melalui penghantar ini dalam keadaan terenkripsi, tetapi enkripsi ini adalah transparan untuk aplikasi pada ujung koneksi yang lain. VPN memberikan informasi melalui internet dengan tanpa resiko adalah suatu kompromi. Metoda yang lain memberikan koneksi jaringan pribadi antara pusat data WASP dengan pemakai jaringan, akan tetapi pendekatan ini lebih memerlukan biaya dibandingkan dengan VPN, akan tetapi secara teori lebih amanselama disana membypass internet secara total.

Secure Methodology

Penerapan metodologi keamanan dan remote administration protocol seperti SSH sangat baik untuk memastikan disana tidak terdapat bagian yang terbuka untuk keamanan informasi atau system pada setiap titik, selama system baru diterapkan. Metodologi keamanan meliputi prosedur administrasi dan tools sehingga hanya orang-orang yang berhak yang menjalankan tugas-tugas administrasi. Metodologi yang aman melindungi kecelakaan terbukanya atau aktifitas penyusupan dalam jaringan WASP.

Security Management

Desain dan penerapan sebuah sistem yang aman tidak hanya berarti bahwa akan selalu aman. Kerusakan keamanan dalam aplikasi perangkat lunak dan komputer atau sistem operasi router jaringan harus diawasi dan diperbaiki setiap waktu. Pengawasan dan memperbaiki keamanan secara tambal sulam akan memperbaiki dari kemudahan terkena serangan.

Security Auditing

Kita dapat menegosiasikan audit yang terpisah sebagai bagian yang terpisah dari WASP. Sebuah WASP tidak akan memberikan kita akses langsung kedalam jaringannya, Firewall atau router, oleh karena itu harus dicantumkan dalam perjanjian kontrak untuk suatu audit yang terpisah.

f. Secure Application Interfaces

Aplikasi wireless dan server pada umumnya berhubungan dengan sumber data dan aplikasi seperti database dan aplikasi sejenisnya. Pada umumnya *Three-tier Architecture* (Web browser, Web Server plus middleware dan aplikasi pendukung) sebuah web server adalah terbuat di internet sedikit aplikasi pendukung disimpan di daerah yang aman dari jaringan. Komunikasi dengan sistem pendukung mungkin diimplementasikan dengan menggunakan protokol yang aman dan jika memungkinkan menggunakan jaringan pribadi. Jika menggunakan ASP maka VPN atau jaringan pribadi harus dikonfigurasi, tetapi hal ini tidak menyediakan keamanan dari webserver sampai peralatan bergerak akan tetapi hanya sampai penyedia layanan jaringan.

Cara yang terbaik untuk menangani keamanan komunikasi antar aplikasi adalah dengan jalan server berkomunikasi dengan menggunakan protokol yang aman seperti SSL.

3. PROBLEM DALAM PENGAMANAN MODEL TITIK KE TITIK

Secara teori permasalahan keamanan dalam arsitektur dari titik ke titik tidak akan pernah terpecahkan. Solusinya adalah pengamanan dari ujung ke ujung. Jadi dalam pengamanan di ujung ke ujung harus disediakan layer tambahan untuk pengamanan seperti penghantar untuk komunikasi yang aman melalui sebuah PKI. Keunggulan dari pengamanan point to point adalah mempunyai fleksibilitas yang lengkap yang mengacu pada peralatan dan lokasi dari user seperti ketika dia dalam bepergian, dan diasumsikan bahwa perangkat lunak *mobile application* dipergunakan secara global.

a. Sniffing dan Spoofing

Sniffing adalah proses pengumpulan informasi kasar dari suatu jaringan dan menyaringnya sesuai dengan informasi yang diperlukan pemakai, mesin atau aplikasi. Spoofing mengarah kepada meniru suatu *node* dalam jaringan bertujuan mengalihkan pemakai untuk meniru suatu aplikasi dan menipunya untuk mengetahui password atau nomor credit card. Sebagai hukum dari komunikasi yang tidak dienkripsi dapat

diamati dan dapat dipalsukan tanpa terdeteksi. Pengamanan dengan PKI membatasi kemungkinan untuk ini.

b. Session Management and URL Rewriting

Didalam *web cookies* digunakan untuk perawatan antara web browser dan web server. Didalam wireless web tidak semua browser mendukung cookies. Ketidakterdapatannya PKI mengurangi metode keamanan dari keberadaan perawatan seperti didalam penulisan URL, harus selalu dipergunakan. Didalam penulisan URL server dapat menentukan permintaan dari pemakai yang spesifik. Metode ini membuka resiko keamanan, sehingga URL dapat disadap dan dipergunakan oleh hacker untuk membypass authentication sebelum mengakses aplikasi.

c. Man-in-the Middle Attack

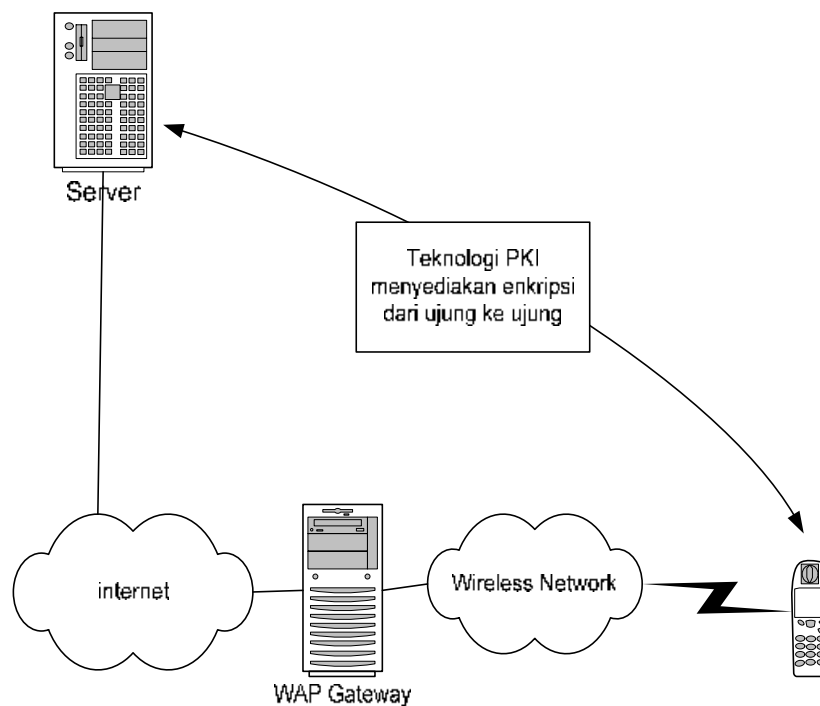
Man-in-the Middle adalah seseorang yang menangkap komunikasi yang melalui sebuah titik yang tidak ter-enkripsi (seperti sebuah WAP gateway), dan selanjutnya menggantikan komunikasi yang sebenarnya dengan sebuah komunikasi yang salah yang dibuat kelihatannya lis. Ketika penerima dari pesan yang salah dia percaya bahwa dia berhubungan dengan orang yang seharusnya berhubungan

d. Tidak Ada Solusi Yang Lengkap

Selama model keamanan point to point memungkinkan, hal ini merupakan cacat dasar dan membutuhkan pendekatan yang terbatas. Ketika data tidak dienkripsi akan mudah diserang dan dari titik standpoint security ini akan lebih jelas kesalahan untuk diasumsikan bahwa kecelakaan dalam pengiriman data melalui internet, hal ini jelas sebab pendekatan konfigurasi gateway WAP atau WSP data center adalah aman. WTLS mungkin aman, tetapi sebuah pertanyaan yang tidak relevan jika penyediaan keamanan dihentikan pada gateway WAP. Masing-masing sambungan antara rangkaian kerja keamanan wireless adalah memungkinkan untuk itu. Salah satu kunci keamanan yang terbaik adalah bersikap bahwa banyak bagian yang memungkinkan mudah terkena serangan adalah tidak mudah diterima jika disana diabaikan.

4. Teknologi PKI dan model pengamanan dari ujung ke ujung

Pengamanan menggunakan *Public Key Infrastructure* (PKI) menjanjikan pengamanan yang lengkap dari ujung ke ujung jika diperlukan komunikasi yang tetap aman. Hal ini disebabkan karena tidak ada titik antara peralatan bergerak dengan Web Server atau mobile application yang tidak terenkripsi. Hal ini memperjelas bahwa pengamanan PKI memberikan pengamanan dari ujung ke ujung dengan menyebarkan sertifikat digital ke pemakai sebagaimana dalam browser wireles. PKI dapat pula diterapkan untuk menyediakan pengamanan yang kuat dalam atau antar perusahaan selama PKI menyediakan pengamanan sebagaimana mengamankan transaksi bisnis melalui internet.



Model pengamanan dari ujung ke ujung

Meskipun PKI pada umumnya digunakan dalam jaringan perusahaan dan pada internet, sertifikat berbasis teknologi enkripsi dan PKI tidak diterapkan secara luas dalam wireless Web. Beberapa alasannya adalah tidak dominannya standar untuk teknologi sertifikat wireless digital dan PKI

- Perbedaan teknologi pengamanan dengan PKI dan persaingan antar vendor.
- Perbedaan dalam wireless browser

- Terbatasnya bandwidth, kapasitas pelatan dan kemampuan memproses
- Tidak adanya standard global untuk browser dan peralatan

Sebelumnya pemakaian pengamanan PKI pada WEB berkonsentrasi pada industri dan difokuskan hanya pada aplikasi yang berhubungan dengan data yang sensitif dibandingkan dengan penggunaan manapun. Dalam wireless Web tidak ada perbedaan dan web master perlu menentukan jika disana kembali ke ongkos investasi dan biaya tambahan dalam mengimplementasikan sebuah PKI.

a. Penerapan PKI

Peralatan yang mendukung teknologi keamanan PKI belum dipakai secara luas. Setiap penerapan PKI hanya untuk organisasi tertentu atau aplikasi yang memerlukan pengamanan. Sebagai alasan bahwa PKI adalah bukan produk yang tersendiri. Untuk menerapkan PKI kita harus memilih teknologi Wireless dan vendornya. Teknologi dan vendor harus dipilih berdasarkan aplikasi dan pada browser wireless serta peralatan yang akan diterapkan.

Integrasi PKI disisi server

Kebanyakan vendor wireless PKI menyediakan Software Development Kit (SDK) yang memberikan teknologi untuk digabungkan dengan aplikasi wireless dan beberapa aplikasi berbasis wireless serta WAP selalu mendukung salah satu dari PKI yang baik.

Peralatan Disisi Client

Teknologi PKI harus mendukung aplikasi client seperti wireless browser dan aplikasi server. Penerapan PKI untuk wireless Web berarti distrkan pada wireless browser tertentu dan pada peralatan yang didukungnya mendukung browser yang dipilih. Beberapa tersedia wireless browser yang mendukung teknologi PKI, akantetapi untuk dirinya sendiri bukan merupakan pemecahan yang lengkap sebab server harus mendukung teknologi yang sama seperti pada browser dan PKI harus diterapkan

apabila diminta untuk digunakan. Sudah menjadi hukumnya bahwa peralatan yang sudah ada tidak dapat diupgrade untuk teknologi keamanan PKI yang lebih baru yang diterapkan pada peralatan yang lebih baru.

Pemilihan Sertifikat otoritas.

Penerapan PKI untuk Web maupun Wireless Web tergantung pada Penerapan sertifikat otoritas (CA). Ketika klien dibuatkan sertifikat, algoritma yang digunakan oleh pembuat root sertifikat dan tangan digital dari sertifikat klien. Root sertifikat merupakan dasar untuk kepercayaan antara server dan klien dan saling berbagi sertifikat dengan sesama root. Setiap organisasi yang menggunakan PKI harus menentukan apakah CA dipergunakan.

Certificate management Framework

Vendor teknologi PKI menyediakan tools untuk membuat, mengatur dan menyebarkan sertifikat. Pengaturan sertifikat adalah proses pemilihan atau mendapatkan sertifikat kewenangan untuk membuat dan mengamankan penyebaran sertifikat dan menjaganya dari suatu sebab misalkan rusak atau hilang, dan mengatur masa berlakunya serta memperbaharainya. Jika sertifikat sudah kadaluwarsa harus segera dikirimkan guna mengganti sertifikat yang disebarkan dalam peralatan bergerak.

Certificate Deployment

Penyebaran PKI melibatkan integrasi disisi server, peralatan bergerak atau pemilihan browser, pembuatan sertifikat dan penyebaran sertifikat disisi client . Dengan PKI memerlukan pemakai, IT administrator, atau keduanya untuk menginstall dan memperbaharui sertifikat sisi klien. Proses penyebaran sertifikat dapat merupakan problem untuk peralatan yang bergerak sebab pada umumnya berada ditangan pemakai yang tersebar . Penyebaran sertifikat harus aman, karena sertifikat yang tertangkap pihak lain dapat digunakan untuk melakukan penyusupan.

b. Keterbatasan Teknologi PKI dalam praktek

Yang menjadi keterbatasan dalam menerapkan PKI adalah keterbatasan standard yang tidak memungkinkan teknologi ini diterapkan disisi server dan dan mengakomodasikan semua peralatan yang sudah dimiliki oleh pemakai untuk membebaskan pemakai memilih perangkatnya. Dalam prakteknya disamping keterbatasan standard juga terdapat keterbatasan geografis cakupannya. Sebagai contoh PKI hanya dapat diterapkan pada browser c-HTML pada platform PDA wireless di Amerika Utara tidak dapat digunakan di Eropa karena menggunakan keamanan WAP standard. Sedangkan di Jepang tidak menggunakan WAP. Guna menghindarkan penggantian standard wireless telepon mendekatannya adalah menerapkan PKI dan menghubungkan PDA khususnya ketikadiinginkan mengurangi kebutuhan akan komputer notebook guna mengurangi biaya adalah alasan mengapa menggunakan PDA dan akses wireless.

C. Kesimpulan

Teknologi wireless aplikasi yang diadopsi disesuaikan dengan pertukaran informasi dan transaksi keuangan yang harus dipastikan aman. Wireless menjanjikan perluasan data perusahaan, aplikasi dan Web untuk peralatan yang bergerak (mobile device), tanpa keamanan yang menjanjikan merupakan penghalang, tetapi keamanan untuk wireless Web tidaklah sederhana. Berbeda dengan Internet wireless Web pekerjaannya terpisah-pisah dan berbeda serta tidak adanya standar yang saling cocok. Terdapat dua pendekatan dalam pengamanan Wireless Web yaitu : dari titik ke titik dan dari ujung ke ujung. Pengamanan dari titik ke titik memberikan pilihan yang luas untuk peralatan bergerak dan browser, dan merupakan jalan untuk mencapai solusi yang benar-benar global. Pengamanan dari ujung ke ujung sinonim dengan teknologi keamanan PKI merupakan pendekatan yang benar-benar nyata, disana banyak kendala dalam mensukseskan penerapannya, tidak sedikit dari yang mempergunakan PKI mendapat keterbatasan alat ketika akan diterapkan. Dasar teknologi keamanan (enkripsi kunci privat atau rahasia dan kunci publik) adalah mengidentifikasi wireless WEB dan konvensinya, tetapi ada beberapa permasalahan keamanan didalamnya. Kebanyakan permasalahan dapat diatasi dengan mengubah derajat jaminan dengan mengacu kepada meminimalkan resiko dengan pemecahan analisa, perencanaan dan manajemen yang hati-hati, dan dengan menyeimbangkan

kebutuhan keamanan dengan dengan keinginan fleksibilitas browser dan dukungan jaringan untuk peralatan bergerak. Untuk masa yang akan datang banyak keterbatasan keterbatasan dalam peralatan bergerak yang terpecahkan.

Untuk isi Web dan aplikasi seperti e-mail cocok untuk keamanan yang terbatas melalui internet, keamanan titik ke titik dan WTLS kelas I merupakan pemecahan yang cukup memadai. Untuk aplikasi keuangan dan informasi perusahaan yang sensitif, menekankan pada SSL pada Web server dan aplikasinya merupakan kebutuhan . Implementasi WTLS yang baru yang meningkatkan keamanan dalam kasus ini adalah dengan PKI yang memberikan keamanan yang tinggi untuk aplikasi . cara yang terbaik untuk pengamanan ini adalah menggunakan PDA dibandingkan menggunakan telephon bergerak. Akan tetapi telah tersebar isu untuk apabila komunikasi generasi ke 3 (3G) yang akan datang akan menggantikan infrastrukur yang ada sekarang ini akan menyediakan keamanan yang lebih tinggi karena akan mendukung SSL dari ujung ke ujung.

Sumber pustaka : Webmaster's Guide to the Wireless internet

<http://www.syngress.com>