KEAMANAN JARINGAN NIR-KAWAT (*WIRELESS SECURITY*)

Jazi Eko Istiyanto
Pengajar Program Magister Ilmu Komputer
Universitas Gadjah Mada
e-mail: jazi1elins@yahoo.com

I. PENDAHULUAN

Dengan meluasnya penggunaan PC, Internet, dan telepon seluler maka kita dapat mengharapkan munculnya *ubiquitous computing* di mana komputer/dan komputasi ada di mana-mana: di setiap tempat, di setiap peralatan, pada setiap orang.

Permasalahan yang muncul di antaranya adalah interoperabilitas antar system, antar muka system dengan instrument, system operasi yang real-time, bandwidth jaringan, *coverage area*, keamanan data, dsb.

Keamanan data menjadi permasalahan penting ketika orang bisa mengendalikan peralatan rumah tangganya secara remote menggunakan teknologi seluler, apalagi bila nanti dicapai interoperabilitas antara Web Internet dengan WAP telepon seluler, sehingga orang dapat mencek status pintu rumahnya (terkunci, terbuka, tertutup tidak terkunci) dan kemudian mengaktifkan actuator pintu (membuka kunci, menutup, mengunci, mengaktifkan alarm) melalui telepon seluler, warung internet, ataupun dari PC yang terhubung ke Internet di kantornya.

II. SEJARAH ANCAMAN KEAMANAN SISTEM

Sejarah mencatat para hacker muda seperti Kevin Mitnick (1981-mencuri manual Pac Bell-ketika itu ia berumur 17 tahun), dan Robert T. Morris (1988-menginjeksikan *Morris worm* dengan teknik *buffer overflow* ke dalam jaringan). Tahun 1985 ada serangan *sniffer* terhadap *Sun workstation*, kemudian 1986 dikenal virus *cuckoo's egg*, diikuti dengan *Morris worm* pada 1988. Tahun 1991 Phil Zimmerman menulis sendiri *Pretty Good Privacy* sebagai proteksi atas serangan keamanan terhadap *e-mail*. 1993 Mosaic mengalami point-click attack. 1994 muncul Linux. 1995 Kevin Mitnick menyerang SDSL/SATAN/SSL. 1998 mencatat *smurf attack*, dan tahun 2000 mencatat fenomena *carding*, yang tidak hanya di negara maju tetapi bahkan di kota-kota pendidikan di Indonesia.

Fenomena yang relatif baru adalah:

- ✓ Maret 1999, virus Melissa (menyerang Word 97/2000, kerugian $300 juta, 150.000 sistem dalam 4 hari).
- ✓ Oktober 2000, Microsoft 2 kali kebobolan.
- ✓ Oktober 2000, situs Israel kebobolan.
- ✓ Agustus 2000, situs Kementrian Penerangan Korea dibobol hacker.
- ✓ Februari 2000, denial of service menyerang eBay, Yahoo, Amazon.
- ✓ Mei 2000, I LOVE YOU (menyerang Outlook, kerugian $10 milyar, 500.000 sistem dalam 24 jam)
- ✓ 22.000 serangan terhadap sistem Pentagon pada tahun 2000
- ✓ Februari 2001, virus Anna Kournikova
- ✓ Akhir Juli 2001, virus Code Red

Kejadian-kejadian ini memberikan gambaran betapa keamanan data merupakan hal yang krusial. Sementara itu posisi *information security officer* masih dipandang marginal. Masalah keamanan data tidak semata-mata teknologi tetapi yang lebih penting adalah *policy*. Dari hasil survey diketahui bahwa gangguan keamanan system komputer disebabkan oleh *bugs* dan *error* pada system (65%), pemakaian tidak sah oleh orang dalam (19%), bencana alam (13%), dan orang luar (3%).

III. KEAMANAN JARINGAN NIR_KAWAT

Dua buah aspek komunikasi nir-kawat yang tidak menyediakan tingkat proteksi yang sama dengan jaringan tetap:

1. *Radio path* = ancaman muncul karena intersepsi data pada antarmuka udara yang menyebabkan hilangnya konfidensialitas data pengguna, informasi *signalling*, dan informasi identitas pengguna.
2. *Akses ke layanan bergerak* = ancaman muncul karena akses illegal yang dilakukan dengan teknik *masquerading* atau *impersonating.* Dulu ada teknik *tumbling* yakni eksploitasi ketiadaan *real-time authentication* pada saat *roaming*. Ini dimungkinkan karena dipakai metoda autentikasi negatif, yakni *default*nya semua permintaan *roaming* diterima. Akibatnya banyak ditemui *bad account*. Dengan membaca *SIM card* dan system elektronik pesawat telepon genggam, orang dapat pula membuat *cloning* (dua atau lebih pesawat menggunakan *SIM card* dengan data yang sama)

IV. LAYANAN KEAMANAN NIR-KAWAT

Untuk melindungi provider jaringan dan pelanggan dari serangan-serangan tersebut, harus disediakan fitur keamanan seperti konfidensialitas/autentikasi identitas pelanggan, konfidensilaitas data pengguna, dan konfidensialitas informasi signaling.

Sistem komunikasi nir-kawat yang banyak dijumpai (misalnya GSM-*Global System for Mobile Communciations*) menyediakan tiga layanan keamanan dasar: Konfidensialitas identitas pengguna, autentikasi identitas pengguna, dan konfidensialitas data pengguna.

V. ARSITEKTUR JARINGAN GSM

Suatu jaringan GSM tersusun atas beberapa fungsionalitas, yang fungsinya maupun antarmukanya telah dispesifikasikan. Jaringan GSM dapat dibagi menjadi 3 bagian besar. *Mobile Station* (MS) dibawa oleh pelanggan. *Base Station Subsystem* (BS) mengendalikan jalur radio dengan MS. *Network Subsystem*, yang mempunyai bagian utama disebut *Mobile Services Switching Center* (MSC), melaksanakan pensaklaran panggilan antar pengguna bergerak dengan pengguna jaringan tetap. MSC juga menangani operasi pengelolaan mobilitas. Selain itu ada *Operations and Maintenance Center*, yang menjamin operasi yang benar dan setup jaringan. MS dan BSS berkomunikasi melalui antarmuka, yang dikenal sebagai antarmuka udara atau jalur radio. BSS berkomunikasi dengan MSC melalui antarmuka A. Beberapa istilah berikut akan dibahas :

SIM = *Subscriber Indentity Module*
ME = *Mobile Equipment*
BTS = *Base Transceiver Station*
BSC = *Base Station Controller*
HLR = *Home Location Register*
VLR = *Visitor Location Register*
MSC = *Mobile Service Switching center*
EIR = *Equipment Identity Register*
AuC = *Authentication Centre*

VI. STASIUN BERGERAK (MS)

MS tersusun atas peralatan bergerak (terminal) dan suatu *smart card* yang disebut *Subscriber Identity Module* (SIM). SIM menyediakan mobilitas personal, sehingga pengguna dapat mengakses layanan yang ia langgan tidak tergantung terminalnya. Dengan menyisipkan kartu SIM kedalam terminal lain, pengguna dapat menerima panggilan dari terminal tersebut, membuat panggilan dari terminal tersebut, dan menerima layanan lainnya.

Peralatan bergerak secara unik diidentifikasi dengan *International Mobile Equipment Identity* (IMEI). Kartu SIM berisi *International Mobile Subscriber Identity* (IMSI) yang dipakai untuk

mengidentifikasi pelanggan sistem, sebuah kunci rahasia untuk autentikasi, dan informasi lainnya. IMEI dan IMSI adalah independen, sehingga memungkinkan mobilitas personal. Kartu SIM dapat diproteksi terhadap pemakaian yang tidak sah dengan sebuah *password* atau PIN (*Personal Identification Number*).

VII. SUBSISTEM BASE STATION

Subsistem base station tersusun atas dua bagian, *Base Transceiver Station* (BTS) dan *Base Station Controller* (BSC). Keduanya berkomunikasi menggunakan antar muka standar Abis, yang memungkinkan operasi antara komponen-komponen yang dibuat oleh pabrik yang berbeda (interoperabilitas).

BTS mempunyai *tranceiver* radio yang mendefinisikan suatu sel dan menangani protokol jalur radio dengan stasiun bergerak. Di daerah urban yang luas, akan banyak terdapat BTS karena itu BTS harus memenuhi persyaratan: tahan banting (*ruggedness*), reliabilitas, portabilitas, dan biaya minimum.

BSC mengelola sumberdaya radio untuk satu atau lebih BTS. Ia menangani setiap saluran radio, *frequency hopping*, dan *handover*. BSC merupakan koneksi antara stasiun bergerak dengan MSC.

VIII. SUBSISTEM JARINGAN

Komponen utama subsistem jaringan adalah MSC. Ia berperanan seperti halnya *switching node* pada PSTN atau ISDN, dan selain itu menyediakan semua fungsionalitas yang diperlukan untuk menangani pelanggan bergerak, seperti halnya registrasi, autentikasi, *location updating*, *handover*, dan *call routing* ke pelanggan yang *roaming*. Layanan-layanan ini disediakan berkaitan dengan berbagai entitas fungsional, yang bersama-sama membentuk subsistem jaringan. MSC menyediakan koneksi ke jaringan tetap (PSTN atau ISDN). Pensinyalan antara entitas fungsional pada subsistem jaringan menggunakan *Signalling System Number* 7 (SS7), yang dipakai untuk *trunk signaling* pada ISDN dan secara meluas dipakai pada jaringan publik.

HLR dan VLR bersama dengan MSC, menyediakan kompatibilitas *call-routing* dan *roaming* dari GSM. HLR berisi semua informasi administratif dari setiap pelanggan yang tercatat pada jaringan GSM yang berkaitan, bersama-sama dengan lokasi saat itu dari unit bergerak. Lokasi unit bergerak biasanya dalam bentuk alamat pensinyalan dari VLR yang berkaitan dengan stasiun bergerak. Secara logika ada sebuah HLR untuk tiap jaringan GSM, sekalipun dapat diimplementasikan sebagai basis data terdistribusi.

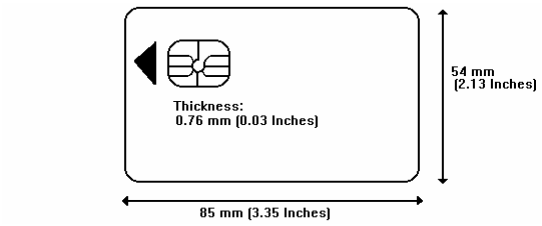
VLR berisi informasi administratif terpilih dari HLR, yang diperlukan untuk pengendalian panggilan dan penyediaan layanan-layanan, untuk tiap unit bergerak yang saat ini berlokasi di daerah yang secara geografis dikendalikan oleh VLR. Sekalipun tiap entitas fungsional dapat diimplementasikan sebagai suatu unit independen, semua manufakturer piranti *switching* hingga saat ini masih mengimplementasikan VLR bersama dengan MSC, sehingga area geografis yang dikendalikan oleh MSC sama dengan area yang dikendalikan VLR, sehingga menyederhanakan persyaratan pensinyalan. Harap dicatat bahwa MSC tidak berisi informasi tentang stasiun bergerak tertentu. Informasi ini disimpan pada register lokasi**.**

IX. *SUBSCRIBER IDENTITY MODULE* (SIM)

SIM enyediakan identitas ke ME. SIM tidak lain adalah sebuah *smart card* yang memiliki CPU dan memori. Parameter pelanggan disimpan di SIM. SIM mempunyai EEPROM dan ROM. ROM berisi algoritma A3 dan A8. EEPROM berisi IMSI dan Ki. PIN memproteksi SIM terhadap penggunaan yang tidak sah. PUK (**Personal Unblocking Key**) memproteksi terhadap pemasukan PIN yang salah berikutnya.

Tabel 1. Memori pada SIM card

Memori	Ukuran Umum	Ukuran Maksimum
ROM	4-6 Kbyte	16 Kbyte
RAM	126-160 Byte	256 Byte
EEPROM	2-3 KByte	8 KByte



Gb.1. Smart Card
(Standar ISO 7810 mendefinisikan ukuran, bahan, flamabilitas, toksisitas)

X. HOME LOCATION REGISTER (HLR)

HLR menyimpan identitas dan data pengguna dari semua pelanggan di area tersebut. Ini meliputi IMSI, Ki, ijin layanan suplementer, dan beberapa data temporer. Data temporer adalah address dari VLR di mana pengguna tercatat, informasi *call forwarding*, dan parameter transien untuk autentikasi dan enkripsi.

XI. VISITOR LOCATION REGISTER (VLR)

VLR berisi data yang relevan dari semua stasiun bergerak yang sedang tercatat pada suatu area layanan. Data permanen ada di HLR. Data temporer agak berbeda, misalnya data dapat berisi TMSI. Bahkan sekalipun stasiun bergerak berada pada areanya sendiri, ia akan tercatat di VLR dan tentu saja HLR.

XII. AUTHENTICATION CENTER (AUC)

Semua algoritma autentikasi dan parameter-parameternya disimpan di AuC. AuC menyediakan untuk HLR atau VLR parameter-parameter yang diperlukan untuk mengautentikasi identitas pengguna. AuC mengetahui algoritma yang mana dan paremeter yang harus dipakai untuk pengguna tertentu. *SIM card* yang diberikan kepada pengguna berisi algoritma dan parameter yang sama dengan yang ada pada AuC

XIII. KONFIDENSIALITAS IDENTITAS PENGGUNA

Sebelum penggguna membuat panggilan atau mulai *standby* untuk menerima panggilan, identitasnya harus diketahui oleh jaringan.

IMSI (*International Mobile Subscriber Identity*) secara unik mengidentifikasikan pelanggan. Biasanya yang dikirim adalah identitas temporer TMSI (*Temporary Mobile Subscriber Identity*), bukan IMSI. Ini dilakukan untuk mencegah *intruder*:

1. memperoleh informasi mengenai sumberdaya yang sedang digunakan pengguna
2. mencegah pelacakan lokasi pengguna
3. mempersulit pencocokan data pengguna dengan data yang dikirimkan.

IMSI hanya dikirimkan bila diperlukan, misalnya ketika pengguna mengggunakan *SIM card* nya untuk saat pertama kali atau ada kehilangan data di VLR.

Ketika SIM card digunakan pertama kali, MS(*Mobile Station*) membaca *TMSI default* yang disimpan pada *card*. Kemudian MS mengirim TMSI *default* ini ke VLR. Karena VLR tidak tahu adanya TMSI ini, ia akan meminta IMSI dari MS. MS mengirim IMSI ke VLR. Kemudian VLR memberikan TMSI baru bagi pengguna tersebut.

VLR mengirim TMSI baru ke MS dalam bentuk terenkripsi. Algoritma enkripsinya adalah A5. Kunci enkripsi adalah Kc. MS mendekripsikan pesan dan memperoleh TMSI. Selanjutnya MS hanya menggunakan TMSI untuk mengidentifikasi dirinya. TMSI hanya berukuran 5 digit, dan unik dalam area lokasi MS bergerak.

LAI (*Location Area Identification*) dan TMSI secara unik mengidentifikasikan penggguna. VLR menyimpan LAI dan TMSI untuk tiap pengguna pada areanya. Sebuah TMSI baru akan dialokasikan untuk tiap prosedur *update* lokasi.

Jika system tidak gagal beroperasi (i.e. beroperasi dengan baik), IMSI tidak dipakai lagi. VLR baru selalu memperoleh IMSI dari VLR lama dengan menggunakan TMSI lama dan LAI yang dikirim oleh MS.

XIV. AUTENTIKASI IDENTITAS PENGGUNA

Autentikasi adalah verifikasi identitas orang yang mengklaim punya hak.

Alasan dilakukannya autentikasi identitas pelanggan adalah untuk memproteksi jaringan terhadap penggunaan tak sah, dan oleh karena itu menjamin billing yang benar dan mencegah serangan topeng (*masquerading attack*).

Metodanya adalah protocol tantangan/tanggapan (*challenge/response*) menggunakan bilangan-bilangan yang tak terduga. SIM berisi kunci autentikasi spesifik pelanggan yang bersifat rahasia Ki yang berukuran 128 bit. Suatu algoritma autentikasi yang dinamakan A3 dipakai di dalam *SIM card* maupun pada jaringan. A3 adalah suatu MAC; ia tidak dipublikasikan. MAC (*Message Authentication Code*) adalah serupa dengan enkripsi, hanya saja tidak selalu *reversible*.

XV. PROSEDUR UMUM AUTENTIKASI PENGGUNA

Verifikasi dilaksanakan oleh VLR di mana MS pada saat itu tercatat. Jaringan mengetahui TMSI dan tentu saja IMSI. Jaringan mengambil Ki dari IMSI. Jaringan menghasilkan suatu bilangan acak RAND. Jaringan mengirimkan RAND ke MS sebagai suatu *challenge*. SIM berisi Ki. SIM menghitung SRES menggunakan Ki dan RAND. MS mengirim SRES ke jaringan. Bila SRES dari MS = SRES yang dihitung SIM, maka identitas autentik. Ki dan RAND masing-masing adalah 128 bit, dan SRES adalah 32-bit.

XVI. MENGAPA BUKAN PKC?

Pemanfaatan PKC (*Public Key Cryptography*) akan memungkinkan verifikasi local terhadap tanggapan tanpa memerlukan diberikannya informasi rahasia ke VLR. Autentikasi menggunakan PKC kini hampir distandardisasikan. Tetapi, PKC tidak digunakan baik pada GSM maupun pada system DECT (*Digital European Cordless Telephone*). Alasannya adalah kendala waktu pada proses autentikasi dan banyaknya data yang harus ditangani. PKC lebih lambat dan memerlukan lebih banyak data. Antarmuka udara tidak mendukung transmisi data sebanyak yang diperlukan PKC.

XVII. MANAGEMEN KUNCI

Parameter kunci terdiri dari: Ki (128-bit), RAND (128-bit), SRES (32-bit), dan Kc (64-bit). Verifikasi dilakukan oleh VLR di mana MS saat itu tercatat. Komputasi dilakukan oleh HLR/AuC dari pelanggan.

Ketiga unsur RAND, SRES, dan Kc dinamakan triplet autentikasi. VLR memperoleh 5 buah triplet dari HLR/AuC dan menyimpannya. Tiap triplet hanya dipakai sekali saja, dan dibuang sesudah digunakan. Ketika pengguna bergerak ke VLR yang lain, VLR baru meminta IMSI dari VLR lama dengan mengirimkan IMSI lama dan LAI. VLR lama mentransfer IMSI dan semua triplet yang tidak digunakan ke VLR baru. Ini mempercepat prosedur autentikasi.

Kunci autentikasi Ki dan IMSI dialokasikan pada saat subskripsi. Ki disimpan di pusat autentikasi (AuC). Algoritma autentikasi A3 dan kunci cipher Kc diimplementasikan di AuC. Manajemen kunci merupakan permasalahan utama dengan banyaknya pelanggan GSM.

XVIII. KONFIDENSIALITAS DATA PENGGUNA

Digunakan algoritma enkripsi yang dinamakan A5. Algoritma ini tidak dipublikasikan dan dapat diimplementasikan menggunakan kira-kira 1500 gerbang. Algoritma A5 disimpan pada silicon khusus di dalam ME dan BS. Aktivasi dikendalikan oleh BS dengan perintah *Start Cipher*. Plaintext dipecah menjadi blok-blok, masing-masing berukuran 114 bit. Kunci Kc dijabarkan pada SIM selama proses autentikasi menggunakan algoritma khusus jaringan A8.

A8 adalah suatu algoritma pembangkit kunci yang didefinisikan oleh penyedia layanan jaringan. Bilangan tantangan RAND (128-bti) dan kunci autentikasi Ki (128 bit) digunakan untuk membangkitkan Kc (64 bit).

XIX. PEMBANGKITAN KUNCI

Metoda membangkitkan dan menyimpan berjuta-juta kunci autentikasi dan penanganan permintaan adalah sangat penting untuk keamanan dan operasi jaringan.

Fungsionalitas AuC tidak dispesifikasikan pada GSM, tetapi diserahkan sepenuhnya pada penyedia layanan, sekalipun dispesifikasikan bahwa A3 dan A8 akan diimplementasikan di AuC.

Pada dasarnya ada dua pendekatan dalam membangkitkan kunci autentikasi pengguna

1. **Bilangan Acak**
   Dipilih Ki secara acak dari semua kemungkinan nilai bilangan 128-bit (jadi ada 2^{128} pilihan. Tetapi tidak ada kaitan natural antara Ki dan informasi tentang pengguna (IMSI). Karena itu AuC harus menyimpan Ki dan informasi tentang pengguna dalam sebuah *data bank*. Kunci harus disimpan dalam bentuk terenkripsi untuk melindungi dari pembacaan oleh pihak yang tidak berhak. Mungkin pula diperlukan suatu *backup* pada lokasi yang secara fisik berbeda.
2. **Metoda Algoritmik**
   Dipilih Ki berdasarkan informasi data pengguna yang diinputkan ke suatu algoritma enkripsi yang dikendalikan oleh kunci master MK. Algoritma enkripsi ini bisa saja DES (*Data Encryption Standard* – data dipandang tersusun atas blok 64-bit, dan kunci adalah 56-bit). Ki = DES(MK1, UD) || DES(MK2, UD), di mana UD = user data, MK1, MK2 dua buah kunci master. Kunci master harus selalu di*update* untuk keamanan. Variasi yang mungkin adalah menambahkan suatu random string (salt) ke user data, e.g. pada Linux, file **/etc/passwd** berisi *password* yang dienkripsi dengan DES plus salt sehingga dua orang yang *password*nya sama, enkripsinya akan berbeda, yang mempersulit *password cracking* berdasarkan **/etc/passwd**.

XX. KESIMPULAN

Dari pembahasan di atas, nampaknya pendekatan keamanan yang diambil berpusat pada kehandalan algoritma-algoritma A3, A5, dan A8. Sekalipun referensi untuk teknologi nir-kawat masih cukup jarang, paling tidak di Indonesia (dimana Anda bisa memperoleh *ETSI Technical Specification GSM 03.20*, misalnya) dibandingkan dengan referensi tentang TCP/IP, namun dengan pengalaman para *hacker* membobol enkripsi, kita tinggal menunggu munculnya insiden-insiden *security* di dunia nir-kawat khususnya system digital (GSM, DECT, DCS1800, PCS1900, dsb – system analog lebih mudah dibobol). Insiden belum banyak karena *M-commerce* belum meluas.

Tentu saja makalah ini tidak bermaksud menakut-nakuti, tetapi bermaksud melakukan edukasi kepada masyarakat agar terbentuk *awareness*. Di dunia perguruan tinggi *wireless computing/technology/networking* sudah saatnya dikembangkan di berbagai bidang (ilmu komputer, teknik elektro, fisika), sementara itu *information security* seharusnya menjadi kuliah wajib untuk semua jurusan (tentu saja disesuaikan dengan sudut pandang program studi masing-masing).

XXI. RUJUKAN

1. **www.seas.upenn.edu/~magda**
2. **www.cs.berkely.edu/~randy**
3. **ece.wpi.edu/courses/ee535**
4. **www.cerias.purdue.edu**
5. **www.ece.orst.edu/ece575**

BIODATA PEMAKALAH

Nama **:** Jazi Eko Istiyanto
Tempat/Tgl Lahir **:** Sleman, 18 Oktober 1961
Alamat Kantor **:** FMIPA UGM Sekip Utara, Yogyakarta 55281
E-mail : jazi1elins@yahoo.com

Pendidikan **:**

1. 1991-1995 Ph.D. **Electronic Systems Engineering**, University of Essex, UK
   (bidang *Electronic Design Automation*)
   Thesis: **The Application of Architectural Synthesis to the Reconfiguration of FPGA-Based Special-Purpose Hardware**
   Supervisor : Dr. Sean Monaghan
2. 1987-1988 M.Sc. **Computer Science**, University of Essex, UK
   (bidang *Computer Systems Architecture*)
   Disertasi: **The Design of A High Speed Hardware Sorter**
   Supervisor: Prof. Simon Lavington
3. 1986-1987 Postgraduate Diploma in
   Computer Programming and Microprocessor Applications,
   University of Essex, UK
4. 1980-1986 Sarjana **Fisika** FMIPA UGM
   (bidang: *Komputasi Fisika Reaktor*)
   Skripsi : **Gangguan Lokal Terhadap Medan Netron**
   Pembimbing : Prof. Dr. Ir. Prayoto, M.Sc.

Pengalaman Mengajar:

1. **S1 Ilmu Komputer UGM :** Pengantar Teknologi Informasi, Komputer Paralel
2. **Magister Ilmu Komputer UGM :** Keamanan Jaringan, Interoperabilitas

3. **Magister Teknik Elektro UGM :** Asas Perancangan Sistem Elektronik
4. **Magister Manajemen UGM :** Business Data Communciations
5. **Magister Sains Managemen UGM :** Metoda Kuantitatif Untuk Manajemen

Pengalaman Penelitian:

1. **1987 : C Programmer dalam project Artificial Intelligence, Open University, Milton Keynes, UK**
2. **1996-1998 : Peneliti Utama Riset Unggulan Terpadu IV (bidang Elektronika dan Informatika) – Sistem Sintesis Arsitektur Untuk Merekonfigurasi FPGA (Dewan Riset Nasional/BPPT)**
3. **2000 : Chief Programmer, Sistem Monitoring dan Evaluasi Bandara Angkasa Pura I (via PT. Asana Wirasta Setia)**
4. **2000 : IT Specialist, Riset Unggulan Kemitraan – Pengembangan Policy Decision Tools Untuk Perusahaan Penerbangan dalam Menghadapi Deregulasi Angkutan Udara (Pusat Studi Pariwisata UGM, PT. Merpati Nusantara, IPTN, dan Dewan Riset Nasional /KMNRT).**