

Building Your First Truly Secure Enterprise Network

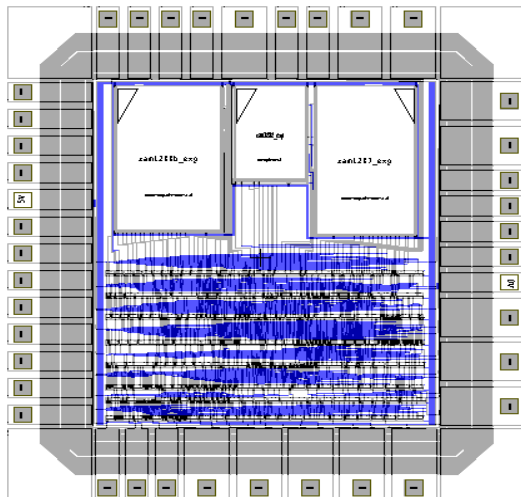
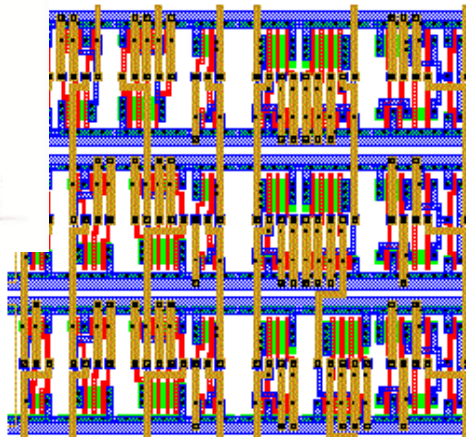
Presented at
CONNECTIVITY 1999
ENTERPRISE NETWORKING SOLUTIONS FOR INDONESIA
October 12, 1999 - Regent Hotel, Jakarta

Budi Rahardjo

PPAU Mikroelektronika ITB
br@paume.itb.ac.id

PIKSI ITB
budi@piksi.itb.ac.id

About the author: affiliation



Topics

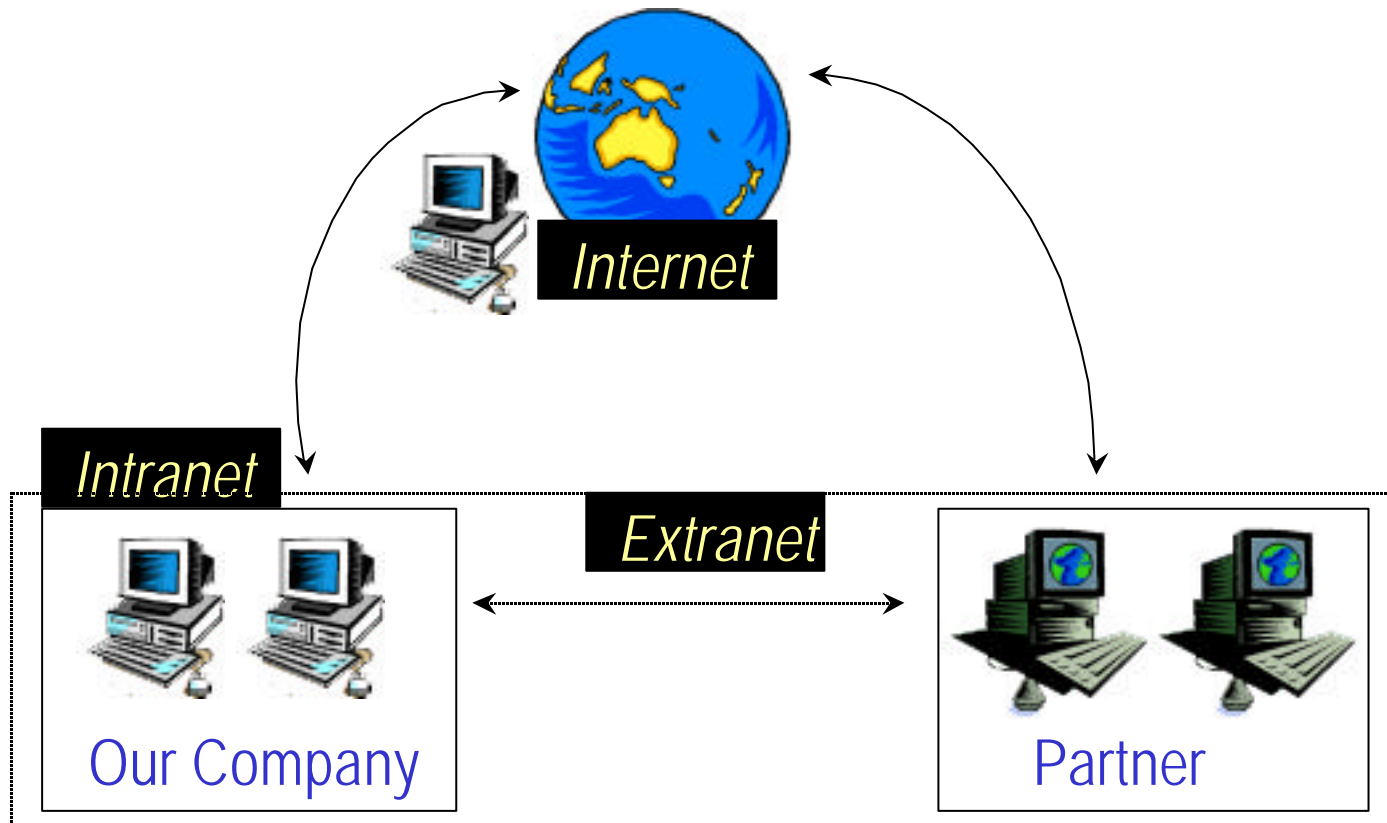
- About enterprise network
- Security issues, risk analysis
- Building secure network
 - non-technical
 - technical

Enterprise Network



- Network is being used in enterprises to increase productivity
- Link internal units with LAN, provide Intranet services
- Remote office, workers, partners connect via private line, Internet, or Virtual Private Line (VPN)

{Intra,Inter,Extra}net



Security Issues

- Security within company?
- 100% secure is impossible. What's the definition of **TRULY SECURE**?

*A computer is secure if you can depend on it and its software to behave as you expect.
(Garfinkel & Spafford)*

- Security vs {convenience, services}

Statistics: Likely source of attack

1999 CSI/FBI Computer Crime and Security Survey

Disgruntled employees	86%
Independent hackers	74%
US Competitors	53%
Foreign corp.	30%
Foreign gov.	21%

<http://www.gosci.com>

Risk Analysis

- Identify assets
 - what are you trying to protect?
hardware, software, data, people, documentation, supplies
- Identify threats
 - what are you trying to protect the assets from?
unauthorized access to resources & information,
unintended/unauthorized disclosure of information
denial of service

Risk Analysis (2)

- how likely the threats are?
Need statistics to show this.

Measures

- Implement measures in cost effective manner
 - security policy
- Review process to improve
 - security holes found regularly, people come and go
 - service improvement, new services

Building secure network: Security Policy

- what data should be protected
- how to protect data
- logging and audit
- review of information
- response to violation, events management

Appropriate Use Policy (AUP)

- Also called Acceptable Use Policy
- Describes what the user shall and shall not do
- Legal aspects



Security Aspects

- Privacy / Confidentiality
 - Corporate setting: whatever you do belongs to the company
 - That's an Orwellian approach: Big brother
 - Attack: sniff
- Integrity
 - info should not be tampered, modified
 - Attack: spoofing, modification, trojan horse, virus

Security aspects (2)

- Non-repudiation
 - cannot deny
- Availability
 - info / service must be available when you need it
 - Attack: Denial of Service (DoS) attack

Security aspects (3)

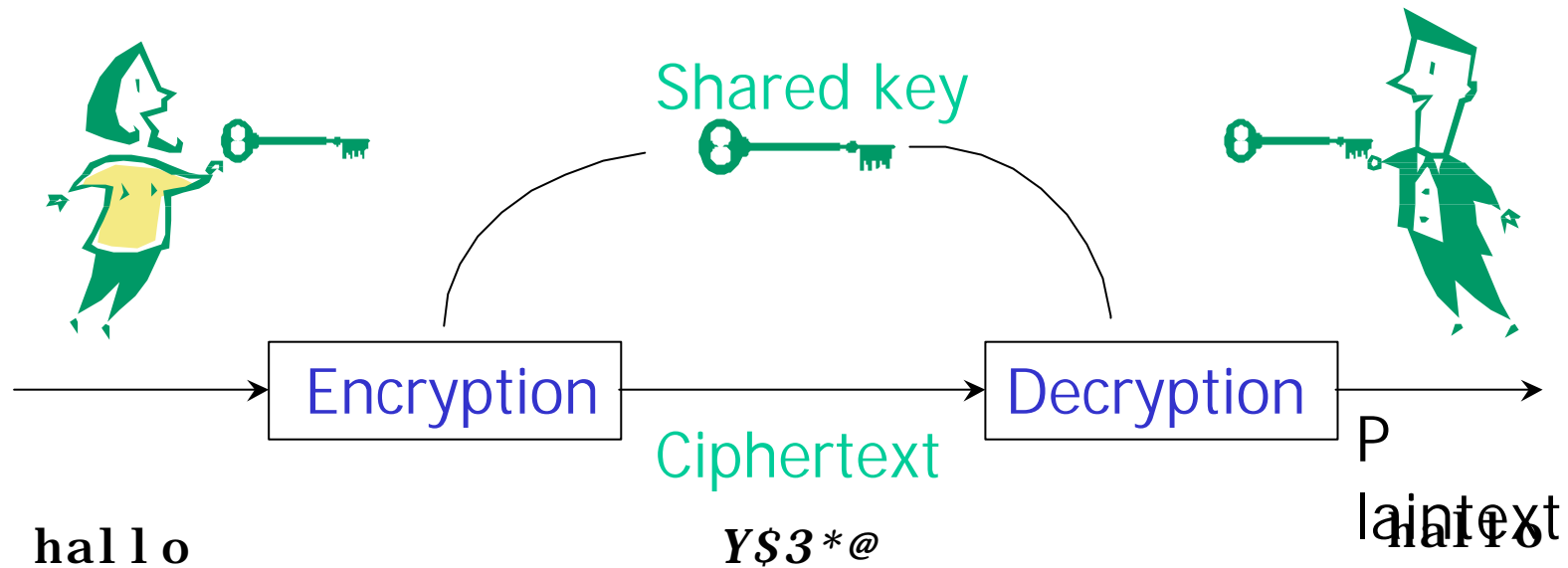
- Authentication
 - to make sure that you are talking to the right person
 - Attack: stolen password
- Access control
 - to make sure that only authorized persons have access to services

Improving Security

- Cryptography technology
 - encryption, decryption
 - secure email: PGP, GPG, S/MIME
 - secure access: SSH
 - digital signature, certificates
 - crypto devices: smartcard, cryptoprocessor
- Public Key Infrastructure
 - Certificate Authority (CA)

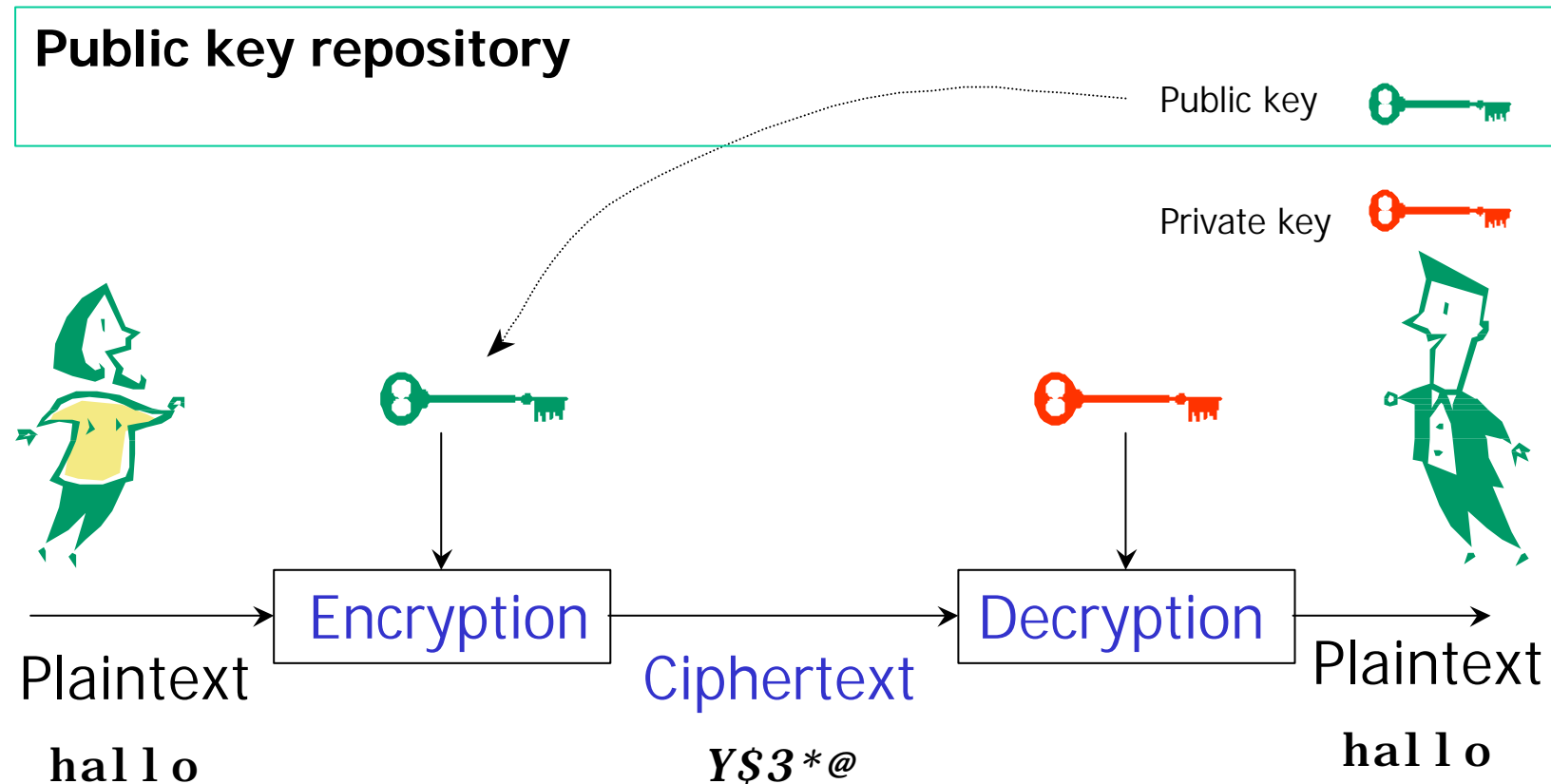


Private (secret, symmetric) key



One key to encrypt and decrypt
Key distribution problem

Public (asymmetric) key



Approach of building secure network

- Best-of-breed tools
 - mix and match tools
 - best in individual area
 - integration problem, duplicate / overlap functions, different level of assurance
 - less expensive(?)
 - need good Human Resources



Building secure network (2)

- One tool/package/vendor
 - integrated
 - may not the best in a specific purpose
 - more expensive(?)

Various Security Tools

- Firewall
- Filtering routers
- Virus detection & protection
- Network scanning tools
- Intruder Detection System/Services
- Certificate Authority (CA)
- Directory Services

Examples of recent security issues

- SSL is not safe anymore?
https uses SSL
- RSA 512 has been broken
Netscape, IE use 40-bit encryption
- NSAKEY in your Windows
NSA backdoor (escrow) in your system?

ID-CERT



- Indonesia Computer Emergency / Incident Response Team
- Mailing list
id-cert@paume.itb.ac.id
New domain: cert.or.id
- Web
<http://www.paume.itb.ac.id/rahard/id-cert>
- Contact: budi@cert.or.id

Reading Materials

- RFC 2196 Site Security Handbook
- Handbook Keamanan Sistem Informasi Berbasis Internet
<<http://www.paume.itb.ac.id/rahard/id-cert/handbook.pdf>>
- Security Portal: news
<<http://www.securityportal.com>>
- Rootshell: exploits
<<http://www.rootshell.com>>
- Tools: audit, protection
<<http://www.opensec.net>>

Reading materials (2)

- SANS: System Administration, Networking and Security
<<http://www.sans.org>>