



# **Network-based Anti-spam Mail System Protection Profile**

**Lee, June Ho**  
**Junior Researcher**  
**Korea Information Security Agency**  
**[juneho@kisa.or.kr](mailto:juneho@kisa.or.kr)**

# Contents

I

Background

II

PP Introduction

III

Security environment

IV

Security objectives

V

IT security requirements

VI

Future work

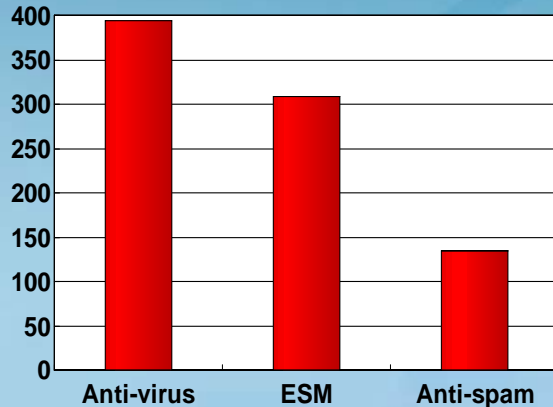


# Background

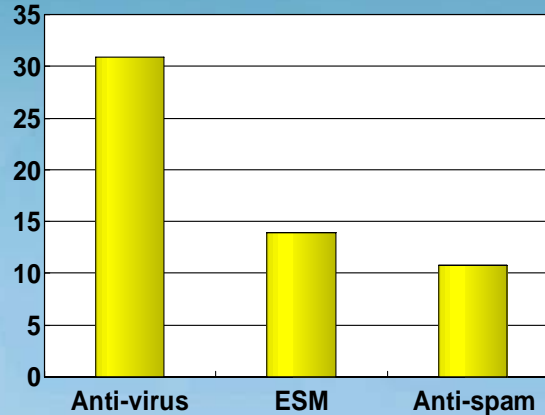


## Selection of PP development target

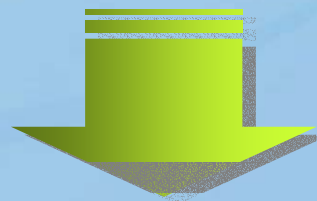
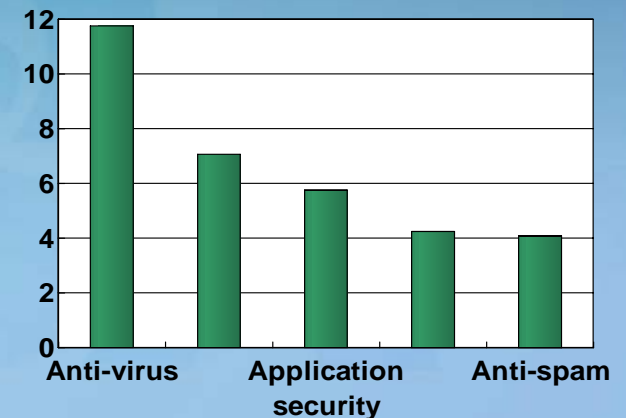
The research on the government and public institutional demand for security product



The analysis of domestic IT field in 2005



The analysis of foreign IT field in 2005



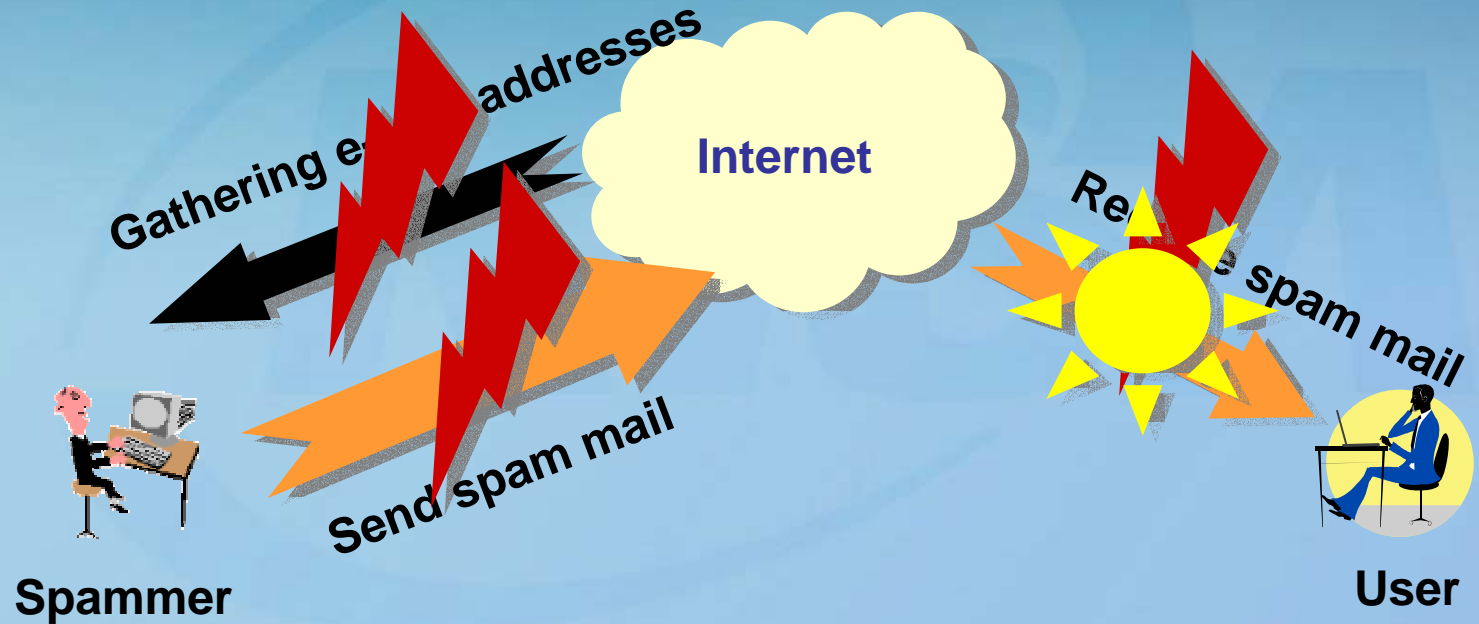
Anti-virus, **Anti-spam**, ESM, Wireless LAN

## → Schedule

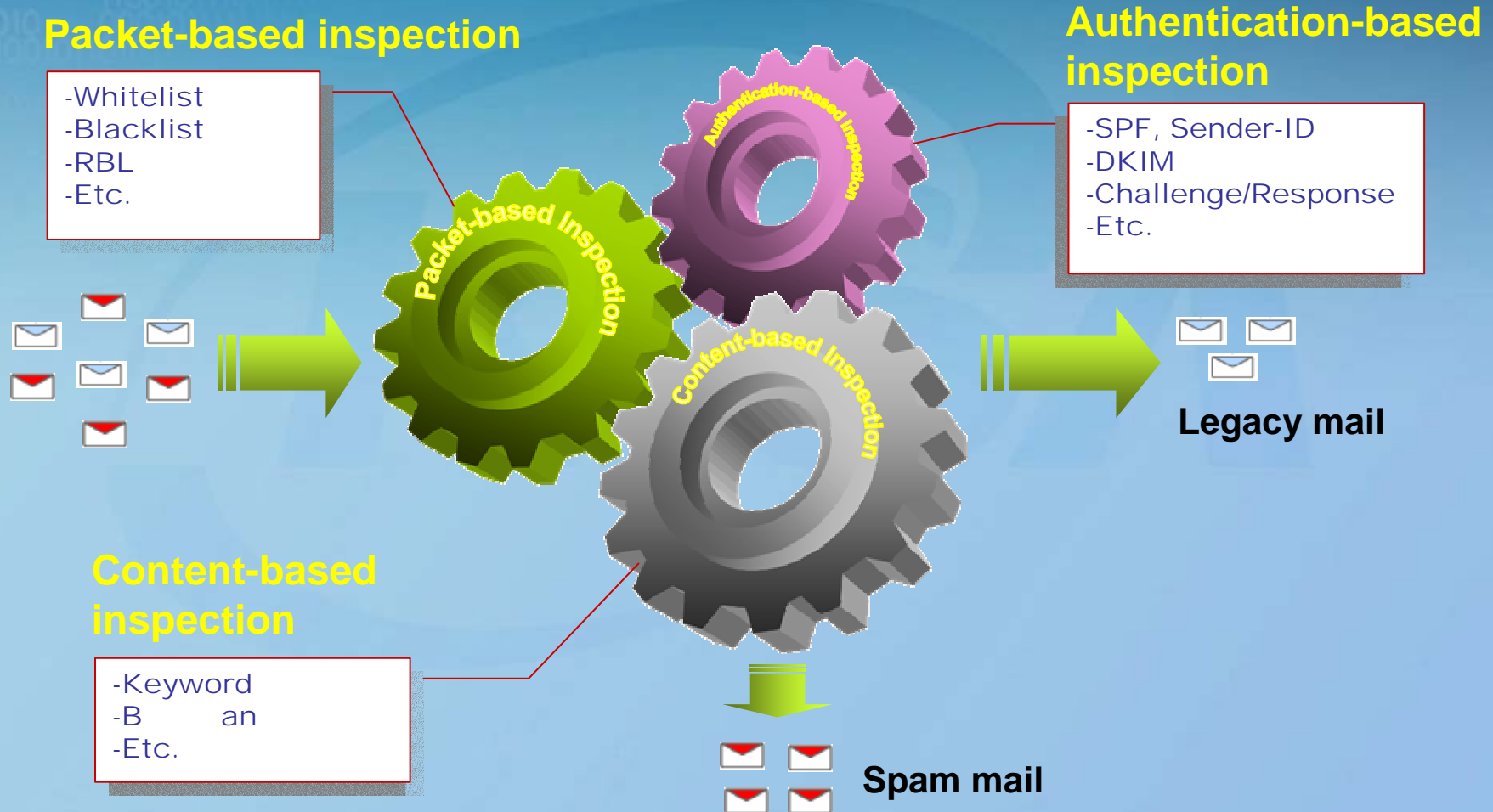
2006

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Explanatory meeting												
Frist meeting												
Third meedting												
Public review												
Evaluation/ Certification												

## → Anti-spam mail techniques

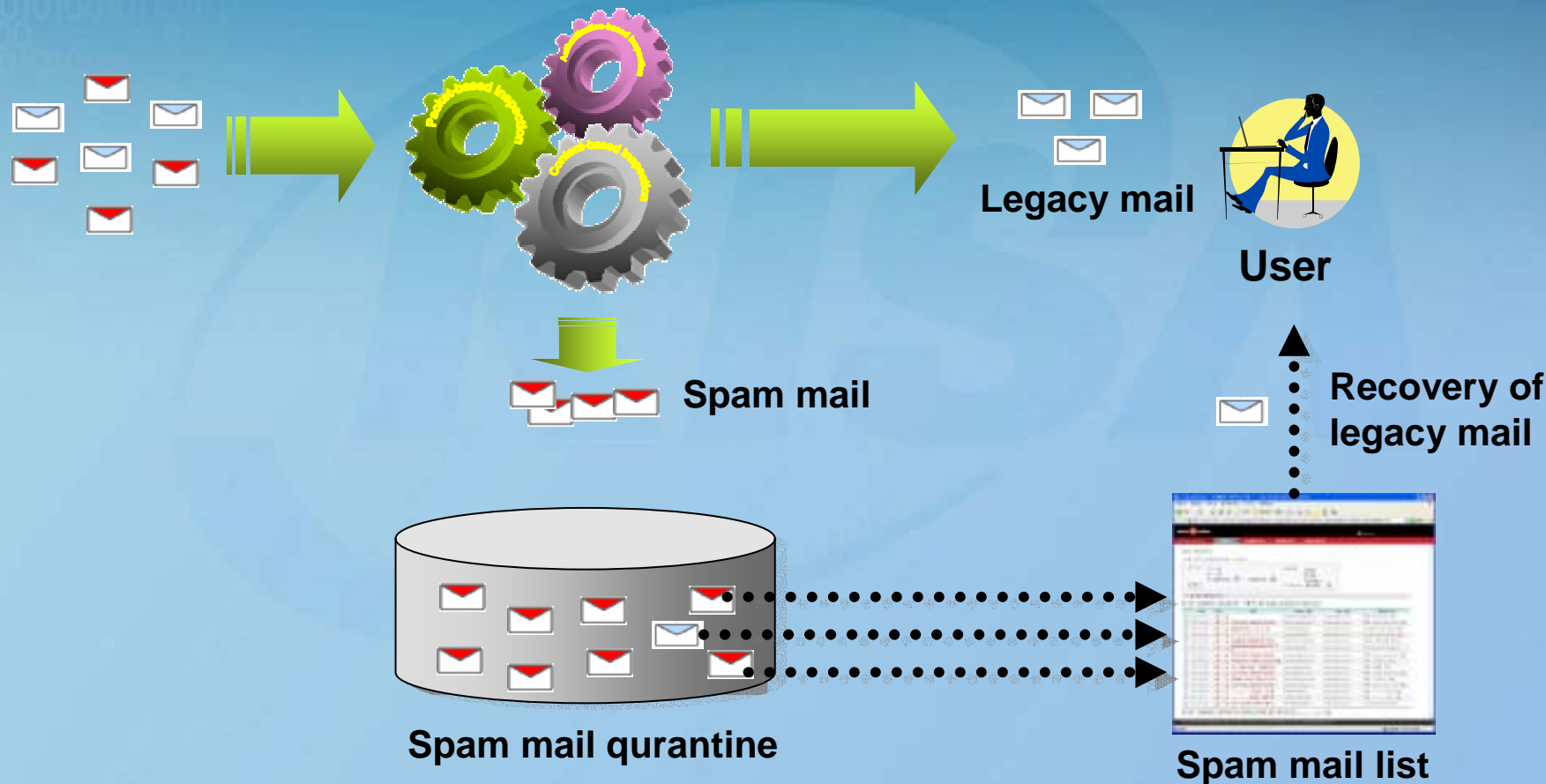


## → Anti-spam mail techniques





## → Anti-spam mail techniques







## PP Introduction

## → PP identification

<b>Title</b>	<b>Network-based Anti-spam Mail System V0.2</b>
<b>Assurance Level</b>	<b>EAL4</b>
<b>SOF</b>	<b>SOF-basic</b>
<b>CC version</b>	<b>2.3</b>

## → New terms and definition

*Mail Server*

*Spam Mail*

*Spam Mail Quarantine*

*Anti-spam Mail System*

*Spam Mail Signature*

*Spam Mail Signature Update Server*

*Whitelist*

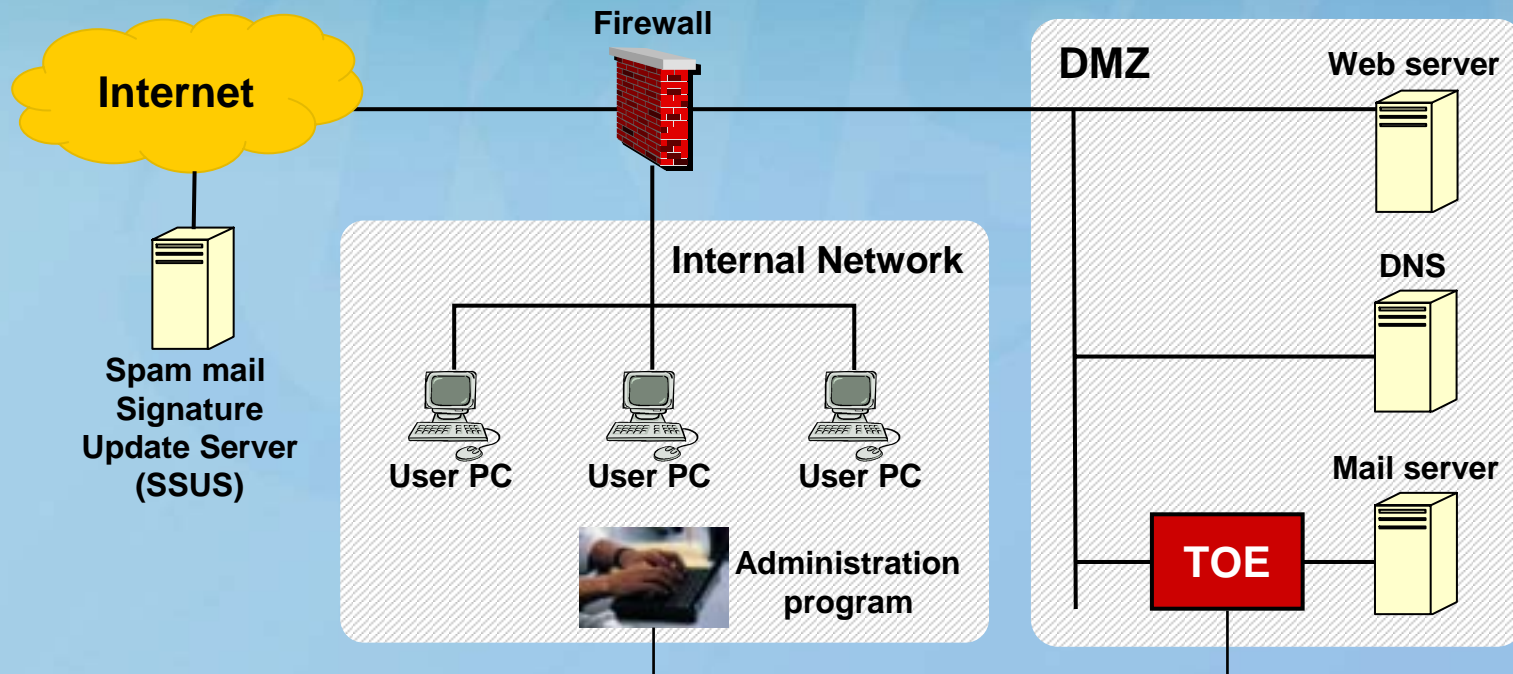
*Blacklist*



## Security environment

## → TOE operational environment

- Implemented as OS-independent application or as a hardware-unified product
- Located in front of mail server physically or logically



# III. Security environment (2/4)



## Assumption

A.PhysicalSecurity

A.CheckRuleUpdate

A.TrustedAdmin

A.HardeningOS

A.Non-bypassibility

A.Firewall

## Threat

T.Failure

T.AuditFailure

T.SpamMail

T.BruteForceAttack

T.Bypass

T.Masquerade

T.TamperStoredData

T.TamperTransmittedData

TE.PoorManage

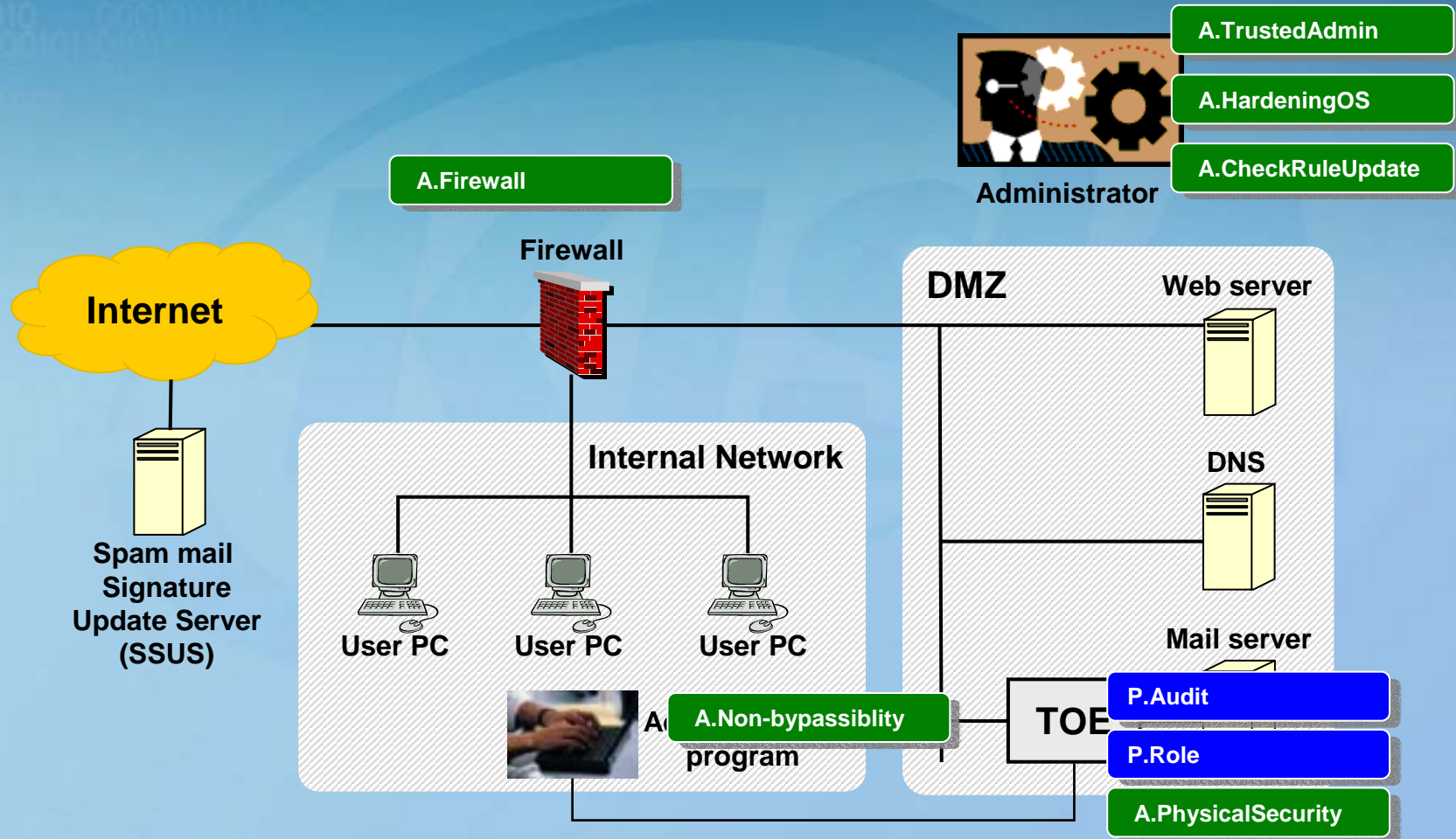
TE.Delivery&Installation

## OSP

P.Audit

P.Role

## → Assumption & OSP



## → Threat

Failure

AuditFailure

SpamMail

BruteForceAttack

Bypass

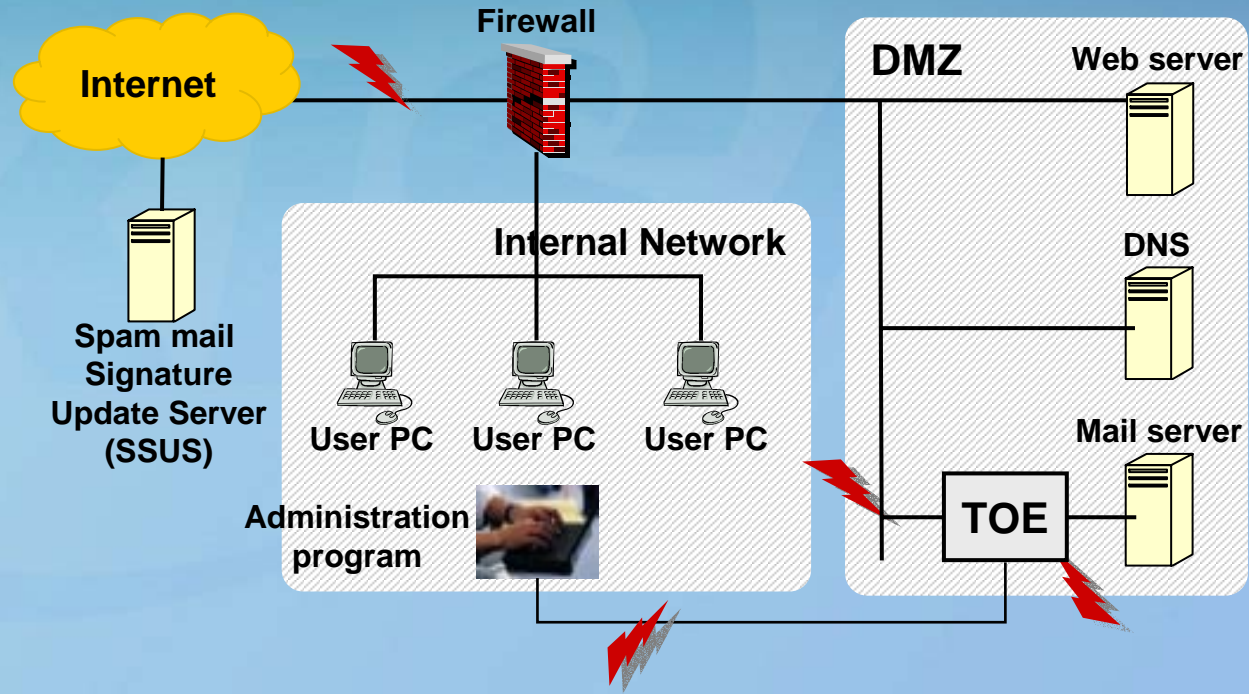
Masquerade

TemperStoredData

TemperTransmittedData

PoorManage

Delivery&Installation







## Security objectives



## Assumption & OSP

## Security objectives

<b>A.PhysicalSecurity</b>	<b>OE.PhysicalSecurity</b>
<b>A.CheckRuleUpdate</b>	<b>OE.CheckRuleUpdate</b>
<b>A.TrustedAdmin</b>	<b>OE.TrustedAdmin</b>
<b>A.HardeningOS</b>	<b>OE.HardeningOS</b>
<b>A.Non-bypassibility</b>	<b>OE.Non-bypassibility</b>
<b>A.Firewall</b>	<b>OE.Firewall</b>
<b>P.Audit</b>	<b>O.Audit, OE.AuditBackup, OE.Timestamp</b>
<b>P.Role</b>	<b>O.Manage, O.Role</b>



## Threat

## Security objectives

<b>T.Failure</b>	<b>O.TSFRecovery</b>
<b>T.AuditFailure</b>	<b>O.Audit</b>
<b>T.SpamMail</b>	<b>O.SpamMail</b>
<b>T.BruteForceAttack</b>	<b>O.I&amp;A, OE.TOEAcess</b>
<b>T.Bypass</b>	<b>O.SpamMail</b>
<b>T.Masquerade</b>	<b>O.I&amp;A, OE.TOEAcess</b>
<b>T.TamperStoredData</b>	<b>O.Manage, O.ProtectStoredData</b>
<b>T.TamperTransmittedData</b>	<b>O.ProtectTransmittedData</b>
<b>TE.PoorManage</b>	<b>OE.SecureManage</b>
<b>TE.Delivery&amp;Installation</b>	<b>OE.SecureManage</b>

# IV. Security objectives (3/3)

## Security objectives for the TOE

**O.Audit**

**O.Manage**

**O.SpamMail**

**O.I&A**

**O.Role**

**O.TSFRecovery**

**O.ProtectStoredData**

**O.ProtectTransmittedData**

## Security objectives for the environment

**OE.AuditBackup**

**OE.PhysicalSecurity**

**OE.CheckRuleUpdate**

**OE.TOEAcess**

**OE.TrustedAdmin**

**OE.SecureManage**

**OE.HardeningOS**

**OE.Non-bypassibility**

**OE.Firewall**

**OE.Timestamp**



## IT security requirements

## TOE security functional requirements

FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2
FAU_SAR.3	FAU_STG.1	FAU_STG.3	FAU_STG.4
FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.1
FIA_UID.1	FMT_MOF.1	FMT_MTD.1	FMT_SMF.1
FMT_SMR.1	FPT_FLS.1	FPT_RCV.1	FPT_RVM.1
FPT_TST.1	FTA_SSL.1	FTA_SSL.3	FTP_ITC.1

3 2

## Explicitly stated IT security requirements

FAS_ART.1(Extended)	FAS_DTN.1(Extended)	FAS_RCV.1(Extended)	FAS_RES.1(Extended)
FAS_SAR.1(Extended)	FAS_SAR.2(Extended)	FAS_STG.1(Extended)	FAS_STG.2(Extended)

## Security functional requirement for the IT environment

<b>FAU_STG.1</b>	<b>FIA_UAU.2</b>	<b>FIA_UID.2</b>	<b>FPT_AMT.1</b>
<b>FPT_SEP.1</b>	<b>FPT_STM.1</b>		

6



## → Security audit

### FAU\_GEN.1 Audit data generation

FAU\_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions;
- b) All auditable events for the minimum level of audit; and
- c) [ Spam mail detection, spam mail response, spam mail recovery, other audit event { determined by ST author } ]



## Security Management (1/4)

### • FMT\_MOF.1 Management of functions in TSF

FMT\_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [

- a) Spam mail detection, alert, response, recovery
- b) Security audit
- c) Identification and authentication
- d) Security management
- e) Other list of functions { determined by the ST author }

] to [ the authorized administrator ].



## Security Management (2/4)

### • FMT\_MTD.1(1) Management of TSF data

FMT\_MTD.1.1 The TSF shall restrict the ability to [selection: *change\_default, query, modify, delete, clear*, [assignment: *other operations*]] the [

- a) *Whitelist*
- b) *Blacklist*
- c) *Signature*
- d) *Other TSF data { determined by the ST author }*

] to [ *the authorized administrator* ].



## Security Management (3/4)

### • FMT\_MTD.1(2) Management of TSF data

FMT\_MTD.1.1 The TSF shall restrict the ability to [selection: *change\_default, query, modify, delete, clear*, [assignment: *other operations*]] the [

- a) *Whitelist*
- b) *Blacklist*
- c) *Other TSF data { determined by the ST author }*

] to [ *the authorized users* ].



## Security Management (4/4)

### • FMT\_SMR.1 Security roles

FMT\_SMR.1.1 The TSF shall maintain the roles [

- a) The authorized administrator { determined by the ST author }
- b) The authorized user { determined by the ST author }

].



## Protection of the TSF (1/2)

- FPT\_FLS.1 Failure with preservation of secure state

FPT\_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [assignment: *list of types of failures in the TSF*].

- FPT\_RCV.1 Manual recovery

FPT\_RCV.1.1 After [assignment: *list of failures/service discontinuities*] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.



## Protection of the TSF (2/2)

### • FPT\_TST.1 TSF testing

FPT\_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, periodically during normal operation, at the request of the authorized user, at the conditions*[assignment: *conditions under which self test should occur*]] to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*].

FPT\_TST.1.2 The TSF shall provide authorised users with the capability to Verify the integrity of [selection: [assignment: *parts of TSF*], *TSF data*].

FPT\_TST.1.3 The TSF shall provide authorised users with the capability to Verify the integrity of stored TSF executable code.





## Trusted path/channels (1/2)

### FTP\_ITC.1 Inter-TSF trusted channel (1/2)

FTP\_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP\_ITC.1.2 The TSF shall permit [selection: the TSF, the remote trusted IT product] to initiate communication via the trusted channel.



## Trusted path/channels (2/2)

### FTP\_ITC.1 Inter-TSF trusted channel (2/2)

FTP\_ITC.1.3 The TSF shall initiate communication via the trusted channel for [

- a) Security management between TOE and remote management program
- b) Signature management between TOE and remote SSUS
- c) Other security management { determined by the ST author }

].

## → Anti-spam mail (1/5)

### ● FAS\_ART.1(Extended) Spam mail alert

FAS\_ART.1.1 The TSF shall report list of information of spam mail which was detected by contents-based inspection, and provide the following items:

- a) Detection date
- b) E-mail subject
- c) Information of sender
- d) Other information { determined by the ST author }

## → Anti-spam mail (2/5)

### • FAS\_DTN.1(Extended) Spam mail detection

FAS\_DTN.1.1 The TSF shall detect spam mail using the following functions:

- a) packet-based inspection : a function which inspects e-mails using sender's IP/e-mail address
- b) contents-based inspection : a function which inspects e-mail's subject or contents using signature
- c) authentication-based inspection : a function which inspects sender using authentication mechanism

## → Anti-spam mail (3/5)

### • FAS\_RCV.1(Extended) Spam mail recovery

FAS\_RCV.1.1 When an user selects an e-mail from the list of spam mail which was transferred by FAS\_ART.1.1 and requests for recovery of the e-mail, the TSF shall ensure that the e-mail is recovered from the spam mail quarantine

### • FAS\_RES.1(Extended) Spam mail response

FAS\_RES.1.1 The TSF shall take the following actions upon detection of a spam mail :

- a) Quarantine spam mail
- b) Other response action { determined by the ST author }

## → Anti-spam mail (4/5)

### • FAS\_SAR.1(Extended) Spam mail quarantine review

FAS\_SAR.1.1 The TSF shall provide an authorized administrator with the capability to read spam mails stored in spam mail quarantine.

FAS\_SAR.1.2 The TSF shall provide spam mail information in a manner suitable for the authorized administrator to interpret the information.

### • FAS\_SAR.2(Extended) Selectable spam mail quarantine review

FAS\_SAR.2.1 The TSF shall provide the ability to perform [selection: *searches, sorting, ordering*] of spam mails stored in spam mail quarantine based on [assignment: *criteria with logical relations*].

## → Anti-spam mail (5/5)

- FAS\_STG.1(Extended) Protected spam mail quarantine

FAS\_STG.1.1 The TSF shall protect the spam mail stored in spam mail quarantine from unauthorised deletion.

- FAS\_STG.2(Extended) Action in case of possible spam mail quarantine data loss

FAS\_STG.2.1 The TSF shall take [selection: *“overwrite the oldest stored spam mail”*, [assignment: *other actions to be taken in case of possible spam mail quarantine failure*]] if the spam mails stored in spam mail quarantine exceeds [assignment: *pre-defined limit*].












## Future work

# VI. Future work

2006

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
<b>Explanatory meeting</b>												
<b>Frist meeting</b>												
												
<b>Third meedting</b>												
<b>Public review</b>												
<b>Evaluation/ Certification</b>												
<b>Explanatory meeting</b>												

*Thank you*