Strategic ST Evaluation/Confirmation

Kai Naruki

Information Security Certification Office,
IT Security Center, Information-Technology Promotion Agency, Japan

Agenda

- Security issues in Japanese e-Government
- CC based Solution
- Future of ST evaluation/confirmation
- IPA effort to promote ST evaluation/confirmation

Security issues in Japanese e-Government

Japanese e-Government

- e-Government : improvement of administrative service and clerical work based on intensive use of IT
  - Supply of Electronic Administrative Information
    - Administrative information can be easily accessed 24 hours a day by visiting homepages on the Internet.
  - Electronic Processing of Applications, Reports and Other Procedures
    - All administrative procedures including applications and reports can be processed 24 hours a day at home or in the office.
  - Electronic Payment of Fees and Taxes
    - Fees, taxes and other charges related to applications, reports and other procedures can be paid through the Internet.
  - e-Procurement
    - Bids can be submitted and opened through the Internet.
  - Paperless Offices
    - Utilizing LANs of Cabinet offices and ministries, electronic information will be exchanged electrically instead of paper documentation.

e-Government in Japan

IPA

- Progress of e-Government
  - In 2001, Japanese Government planned to make it possible that administrative procedures from citizens to government or government to citizens could be done through the Internet.
  - In 2003, 96% of the procedures could be done through the Internet
  - e-Gov portal site (http://www.e-gov.go.jp) provides one stop service for the administrative procedures
- e-Government security
  - e-Government handle important information assets. So it must maintain the highest information security
  - But e-Government security was breached many times (e.g. leakage of information, service discontinuity caused by a reported DOS attack)

e-Government in Japan

e-Government Infrastructure

KWAN
(Internal Network of Ministries)

LGWAN
(Local Government WAN)

GPKI
(CA for Digital Certificate)

Juki Net
(Network for resident registration)

e-Gov

Government Web portal site

Digital Certificate

Juki Card

Citizen/Company

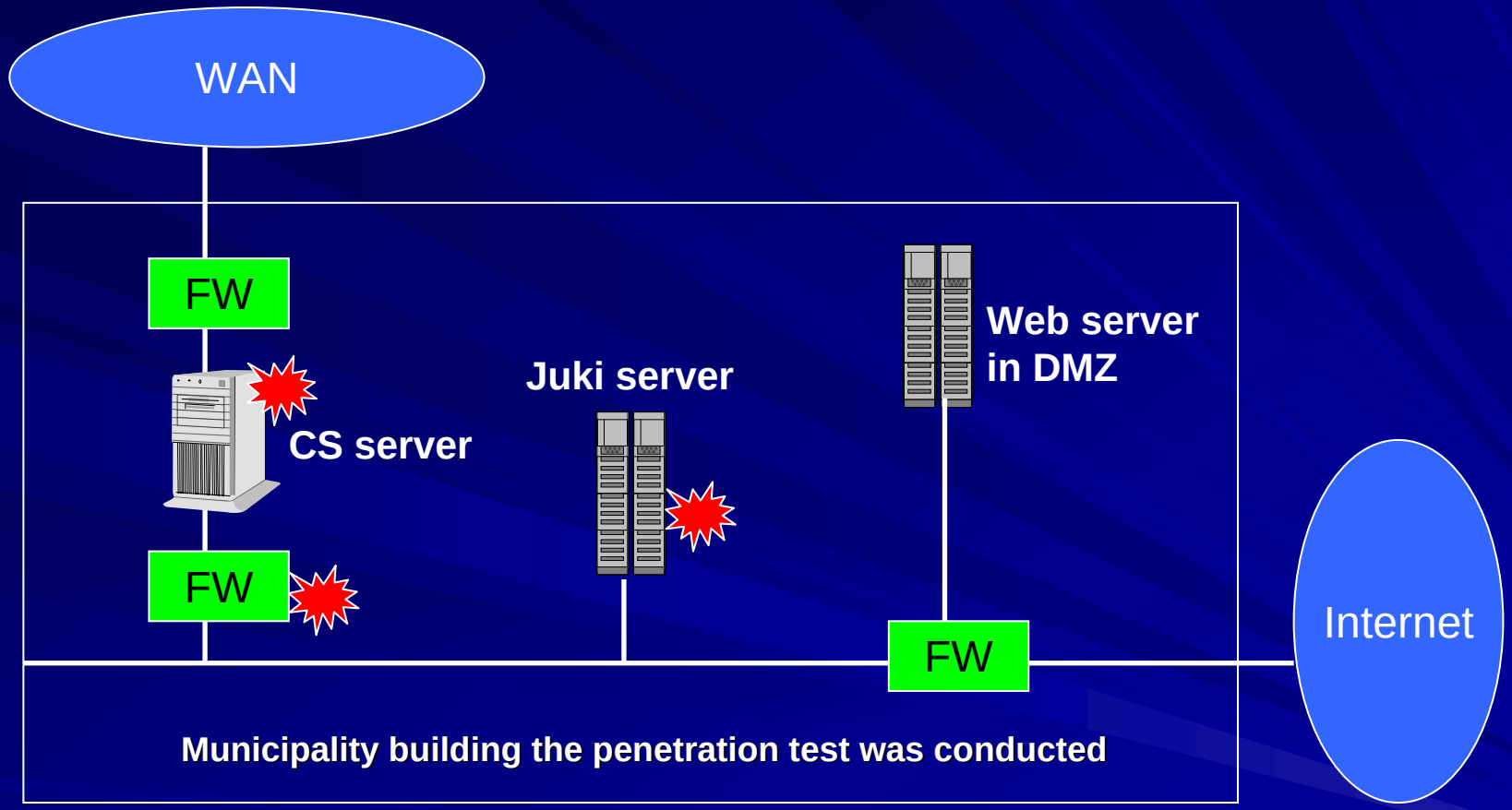
Internet

Juki Net links all municipalities and prefectures so that the central and local governments can share resident information (Name, Address, Sex, and Date of Birth) based on 11-digit identification number

Juki Net

- Juki Net：A national network of databases that contain the names and personal details of nearly every person residing in Japan
- The operation started on 5th Aug 2003. Before this date several vulnerabilities were found by security experts during the penetration test at Nagano prefecture.
- 32 municipalities reported accidentally releasing personal information 10 days after the operation began.
- Some of the municipalities refused to link their databases to the Juki Net because of security concerns.
- The number of Juki Cards that were issued at the request of residents to access the Juki Net was 0.25 million and fell far short of the government's initial projection of 3 million because of security concerns.

Vulnerabilities found at Nagano prefecture

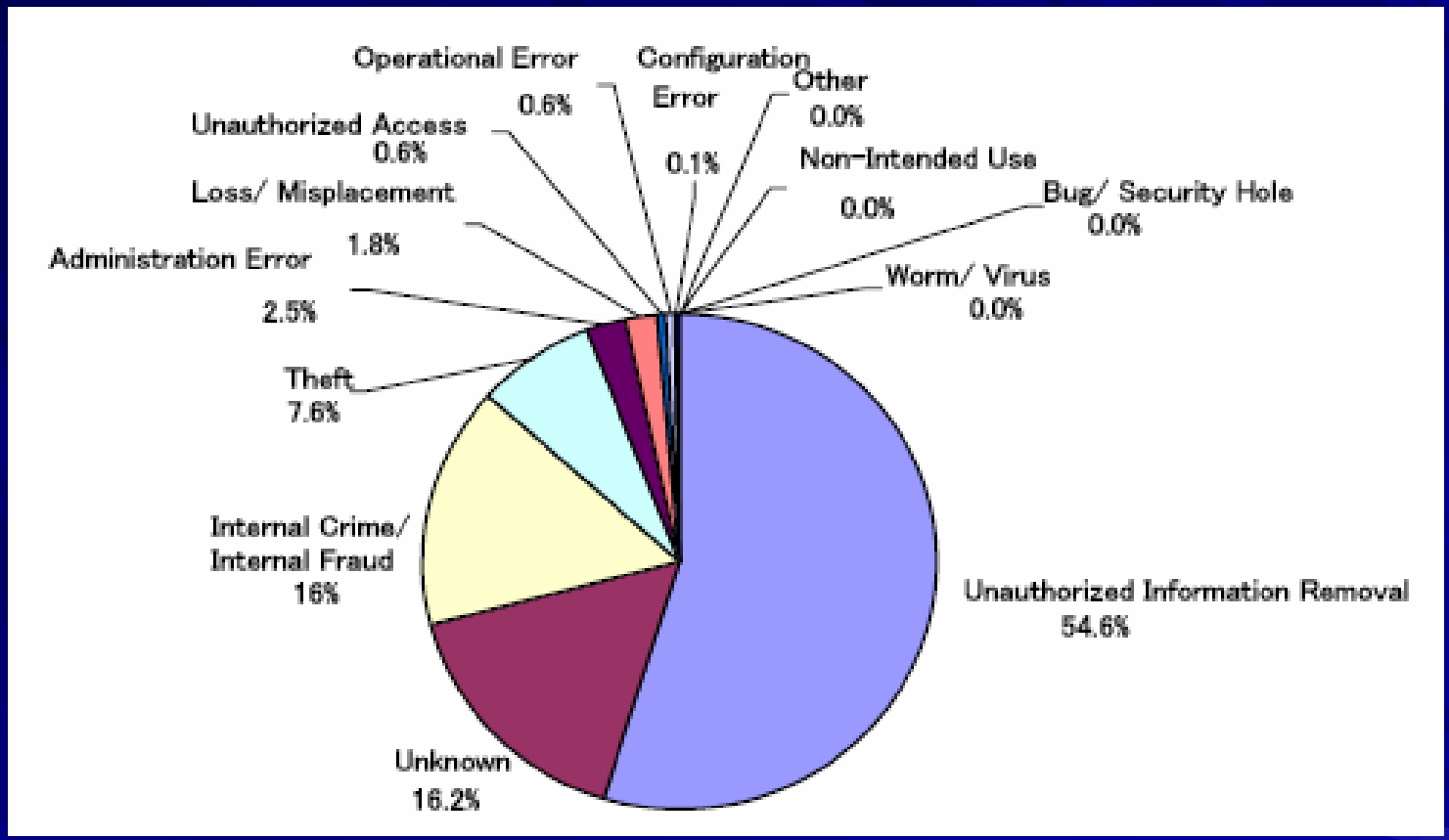


- ✓Inadequate password setting
- ✓Exploit vulnerabilities in OS
- ✓Insufficient access control
- ✓Vulnerable application
- ✓Password stored in plain text file
- ✓Configuration errors

Personal Information Disclosure Incidents

- The number and scale of Personal Information Disclosure Incidents have increased to historic levels in Japan.
  - 366 incidents in 2004 (57 in 2003)
- JNSA (Japan Network Security Association) published the report that summarize the results of an independent evaluation of a survey and accompanying analysis related to Personal Information Disclosure Incidents in Japan
  - Average Projected Compensation for Damages per Incident in 2004 was about $13 million
- Like Juki Net, one of the most important information assets of e-Government is Personal Information.

Personal Information Disclosure Incidents in 2004



Ratio of Victims by Disclosure Cause

2004 Information Security Incident Survey Report
http://www.jnsa.org/houkoku2004/incident_survey_en.pdf

What is the cause of these incidents?

Example of the incidents

- Internet service provider company
  - The number of victims was 6.6 million
  - A database password was shared among hundreds of contractors
  - Audit log was retained for only one week
  - Company sent vouchers worth $5 to all its customers
  - The company didn’t anticipate attacks from contractors
- Retail company
  - The number of victims was 0.5 million
  - Personal information in magnetic tape was not protected adequately
  - The company overlooked the threat to asset in removable media
- Esthetics company
  - The number of victims was 50 thousand
  - Personal information in Web server was stolen
  - Cause of the incident was configuration errors in web server
  - Forced browsing attack

Possible cause of the incidents

- Overlooked threats to assets
  - Does not consider obvious threat agents
  - Attack methods were overlooked
- Weak counter measure
  - Threat was identified but the counter measure was not appropriate
  - Does not verify that threats were removed or diminished to an acceptable level
- Configuration error in COTs product
  - Counter measures were implemented with COTs product but configuration errors allowed sensitive information to be viewed by unauthorized persons
  - Latest patch not applied or obsolete version was used
- Vulnerabilities in web applications
  - Web applications had lots of vulnerabilities
  - IPA received 292 reports related to vulnerabilities in web application in 2005

Most causes were obvious. They could easily have been prevented

CC based Solution

Information Security Standards for e-Government

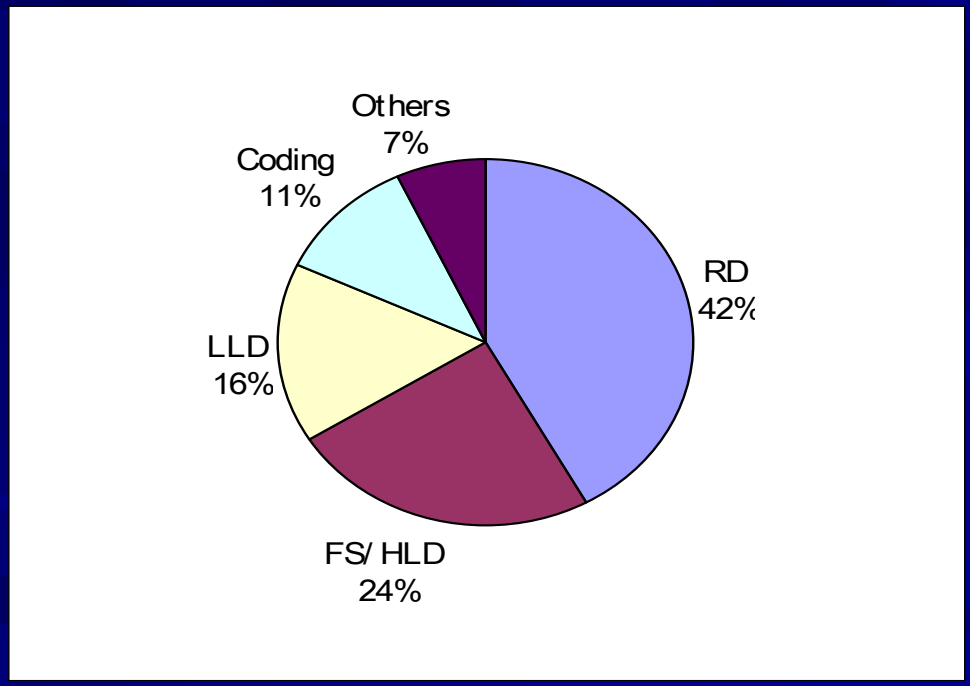
- Japan issued standards for improving e-government security (Standards for Information Security Measures for the Central Government Computer Systems, Dec 2005)
- Require ST evaluation and confirmation for e-government information systems and software developments (Mandatory requirement)
- Also require to consider CC certification during IT products procurement (Enhanced requirement)
- Secure Japan 2006 (Japanese national strategy on information security)
  - Upgrade the level of the standards to the world's highest level by fiscal 2008
  - Enable all the government agencies to implement measures at the level meeting the required standards by fiscal 2009

What is ST evaluation/confirmation?

- ST evaluation/confirmation is subset of EAL1
  - Before May 2006, Only ASE evaluation
    - 29 products and systems have already been certified
  - After May 2006, ASE, ADV_FSP.1 and ADV_RCR.1 evaluation
    - No products or systems have been certified.
    - About 10 systems will apply for ST evaluation/confirmation in 2006
- Low assurance ST in CC V3 is not permitted
  - SPD (Security Problem Definition) is an important part of the evaluation

Why ST evaluation/confirmation?

- Where are defects most common?
  - Survey conducted among 309 developers in Japan

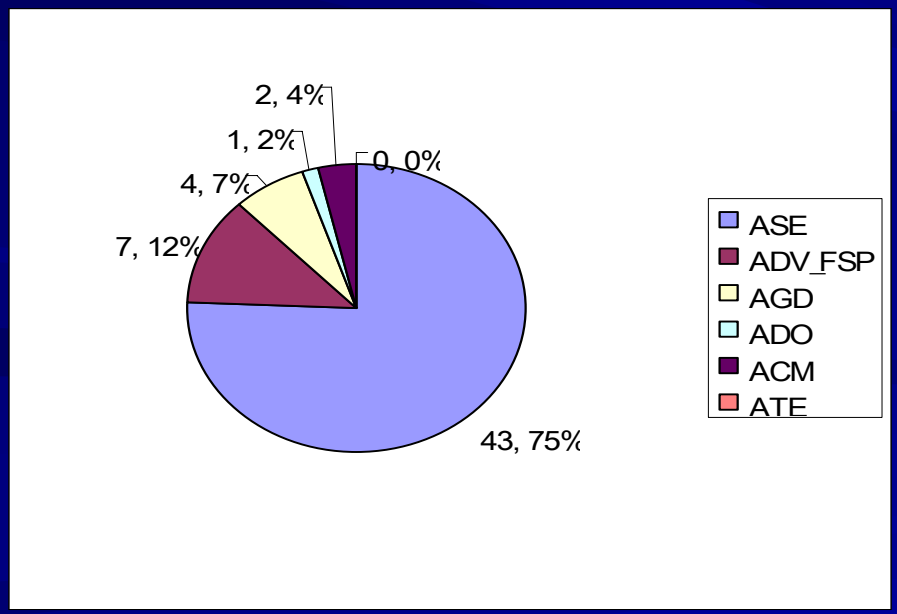


Critical defects are witnessed in Requirement Definition and the Specification phases

http://hotwired.goo.ne.jp/original/maegawa/041130/textonly.html

Why ST evaluation/confirmation?

- What are the best assurance components which contribute to enhance security?
  - Examine number of OR and CR issued during the system evaluation (EAL1) in Japan
  - Most of OR/CRs were made during ASE and ADV_FSP
  - All critical OR/CRs also originated from ASE and ADV_FSP
    - Failed to highlight all attack methods
    - Did not consider threats to assets in backup media



Most of defects were discovered in ASE and ADV_FSP component evaluation

Why ST evaluation/confirmation?

- Studies have shown that:
  - Finding errors early in a system development costs less to fix than finding errors later in a project.
  - The factors of 1 time unit for a specification error, 10 time units for a design error, 100 time units for a coding error, to 1000 time units for an integration testing error.
  - These numbers have not been formally validated, but the basic principle that errors found later are harder to fix seems to be sound.

Removing any defects as soon as possible after introduction is the most cost-effective manner

Why not evaluate any other components?

- Issues on e-Government system evaluation
  - Lack of CC experience
    - Most system developers have little knowledge about CC
    - Might take much longer for evidence documentation development than previously expected
  - Tight system development schedule

✓Most of defects are introduced in Requirement Definition (ST) and Specification (ADV_FSP) phases
✓Removing any defects as soon as possible after introduction is the most cost-effective manner

ST evaluation/confirmation is the most feasible and cost-effective approach

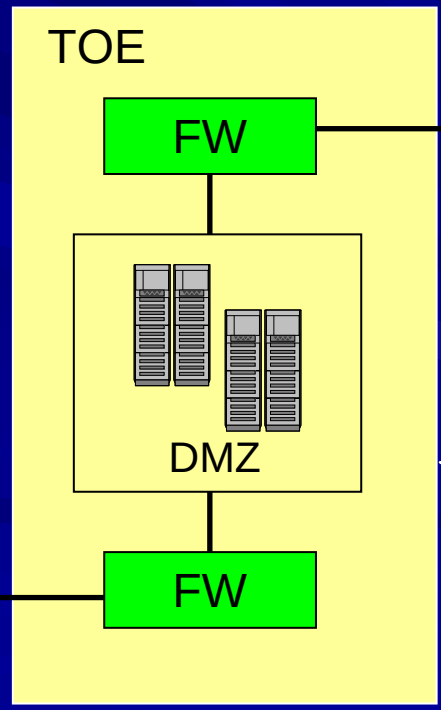
Future of ST evaluation/confirmation

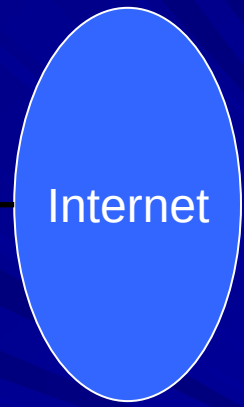
Incremental Approach

- Security of e-government system should be considered as a whole
- An incremental approach to improve e-government security is needed
  - First phase
    - Developers need CC experience and knowledge
    - TOE scope could be adjusted based on an agreement between developers and procurers.

ST
✓Identify threats
✓Justify security objective

FSP
✓TSF fully implemented?
✓Examine configuration
•Firewall rule set
•OS access control

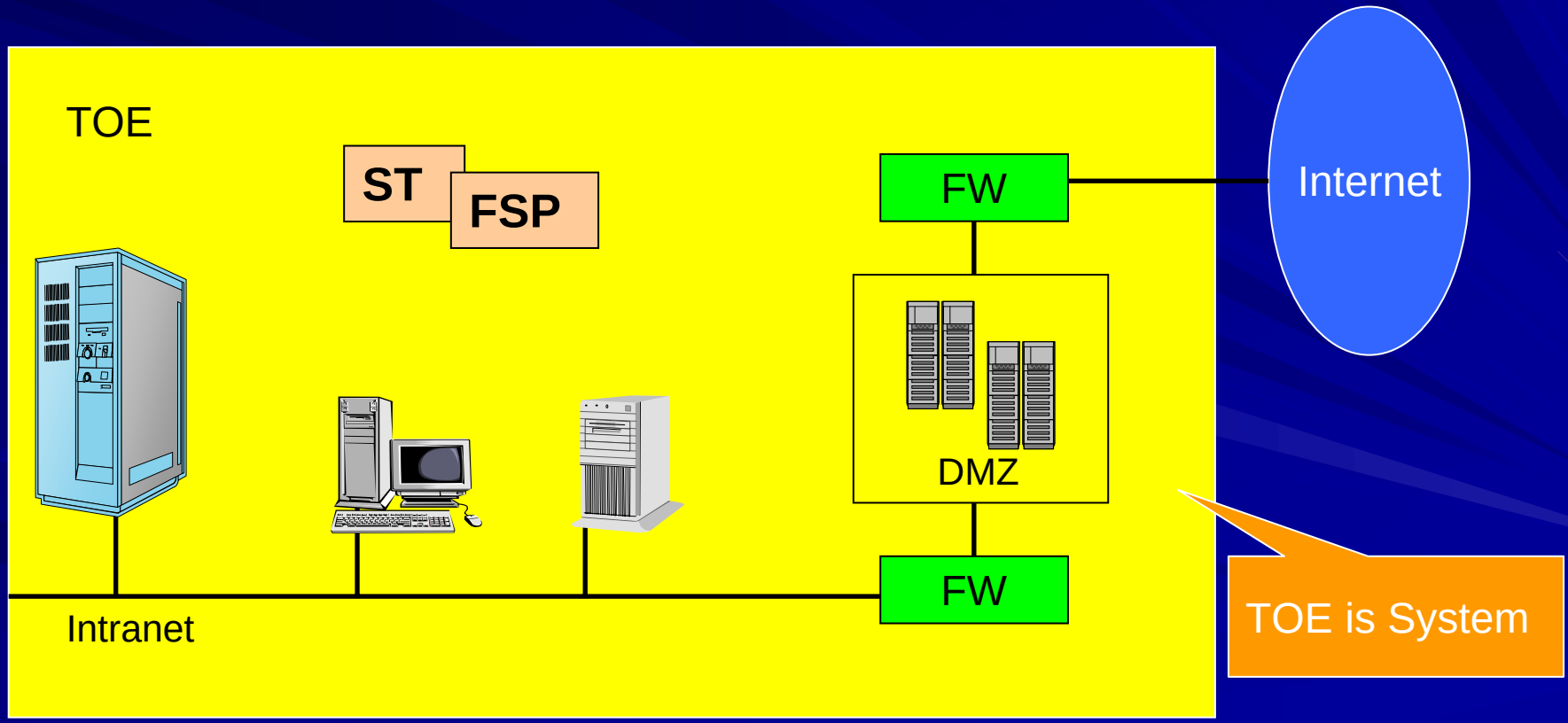




TOE is the most vulnerable area

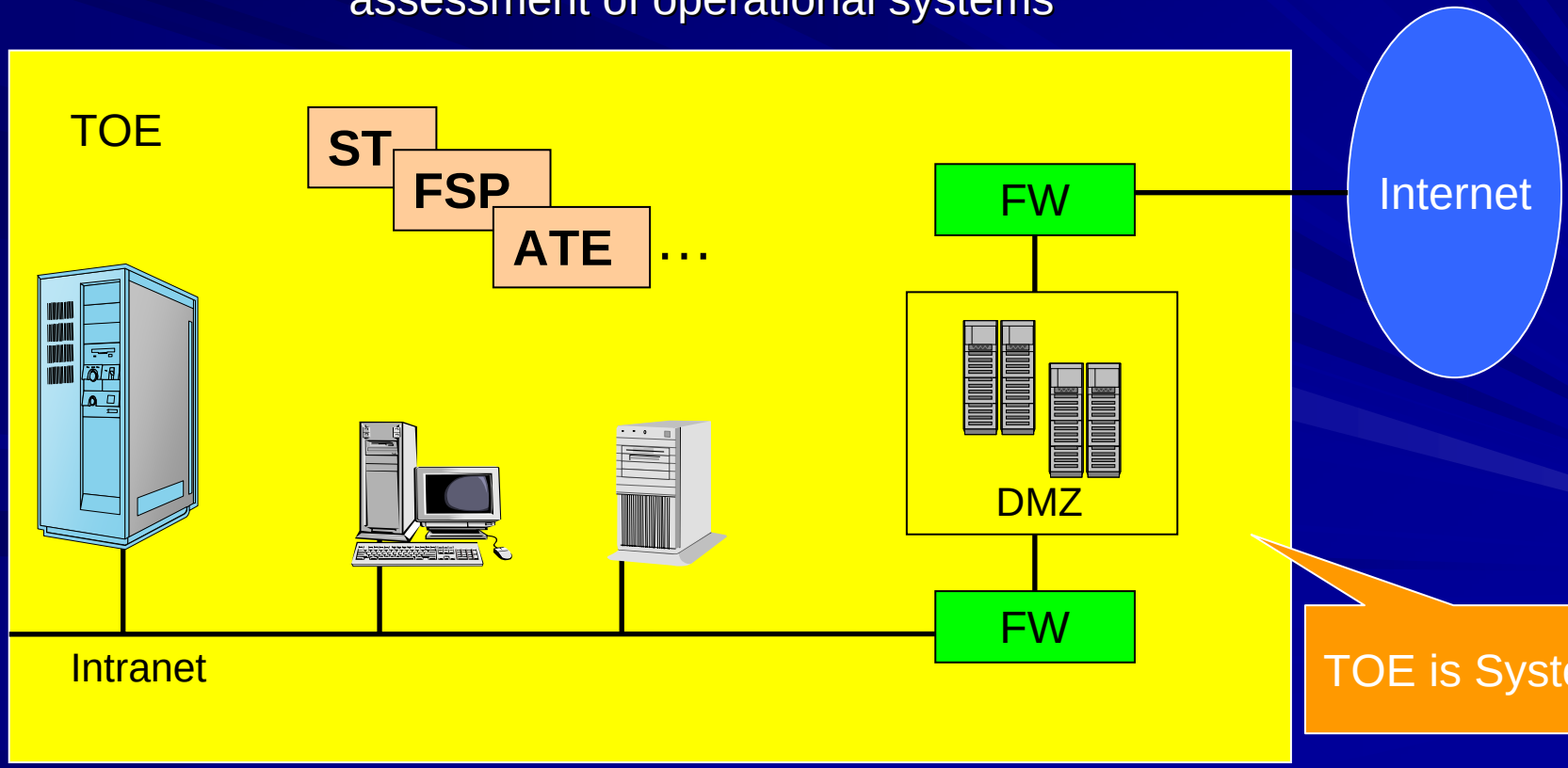
Incremental Approach

– Second phase
- Developers already know CC and understand the merits of CC
- Developers have experience of developing evaluation evidence
- TOE scope can expand based on past experiences



Incremental Approach

- Third phase
  - Increase assurance components
  - Shift from ST evaluation/confirmation to;
    - EAL1 evaluation
    - ISO/IEC/TR 19791 (2006-05)
      - Information technology - Security techniques - Security assessment of operational systems



IPA effort to promote ST evaluation/confirmation

IPA effort to promote ST evaluation/confirmation

- Developer Review
  - Improve quality of evaluation evidence
    - Evaluation schedule are often delayed because of insufficient evidence
    - It takes more time to modify them based on ORs from evaluators
    - IPA recommends developers check their evaluation evidences based on CEM by themselves before evaluation to reduce the time and cost of evaluation
    - IPA offers education courses to developers for the Developer review
- IPA education courses
  - Help to enhance CC knowledge for developers
  - Support evaluation evidence development
    - CEM work unit basis
- Guidance documentation
  - System ST sample for ST development
  - ASE ETR sample for Developer review
  - CC V3 transition guidance (Planned)