IPA Information-technology Promotion Agency, Japan

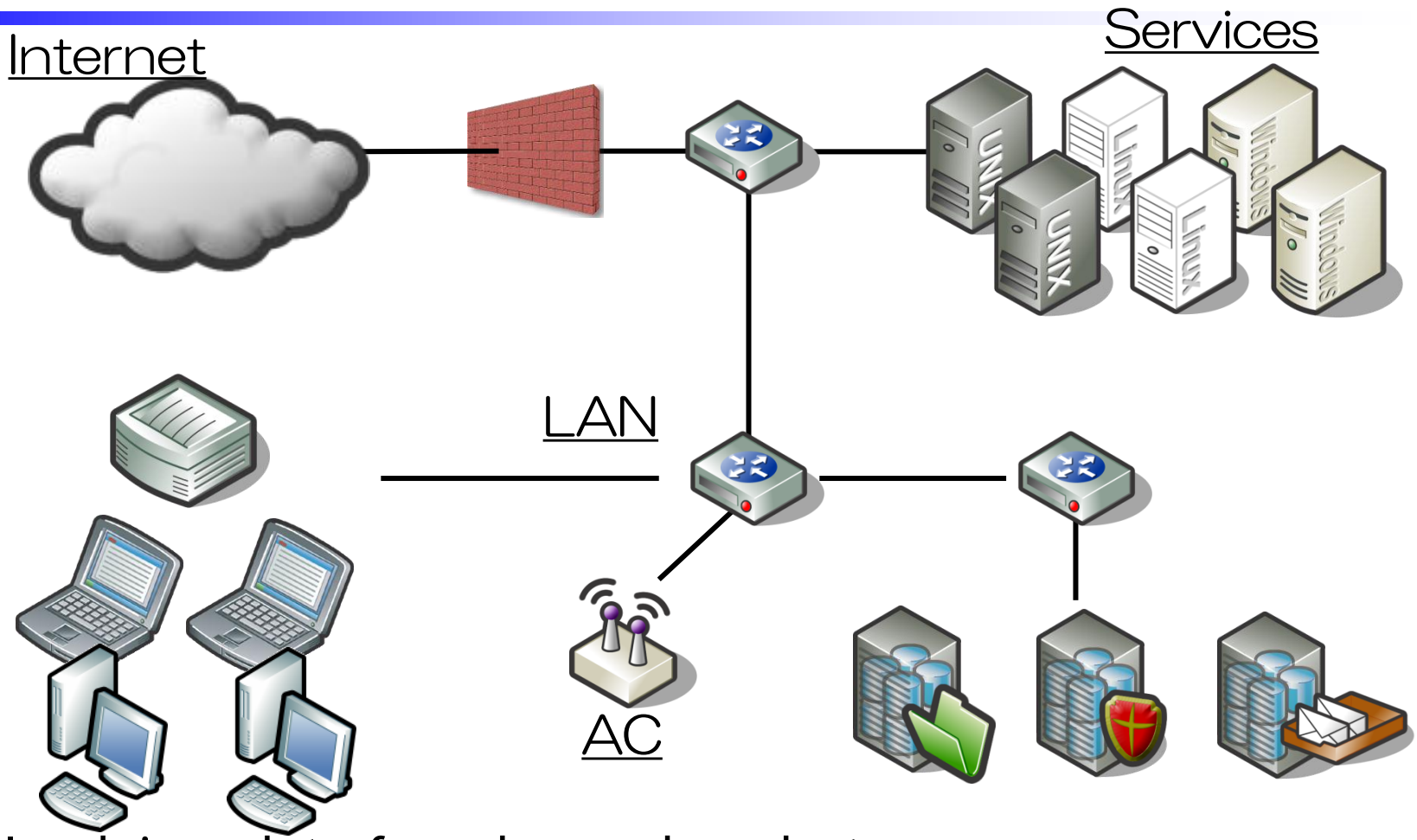
Vulnerability-centric assurance activities for MFP PP
as a candidate for cPP

Fumiaki Manabe
JISEC / IPA, Japan
September 11, 2013

Agenda

- The security surrounding the MFP
- PP development for Government Procurement (as a cPP candidate)
- Vulnerability-centric Evaluation
- Vulnerability-centric Assurance Activities
- The development of the vulnerability report of the MFP
- Summary

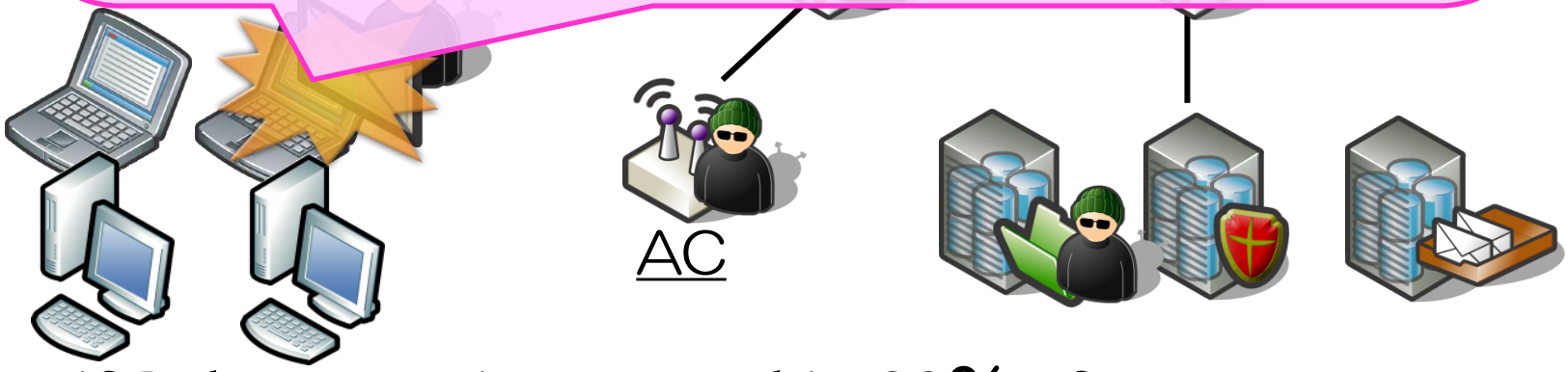
IT Systems



- Involving a lot of vendors and products
- Operational management and robustness of each products are critical

Only one problem but …

Once a malware could intrude the Windows PC, various attacks may happen.
In some cases, it may happen that
Administrator's Password related information (Password Hash)
which is temporarily stored in the client PC managed by Active Directory Domain is disclosed. And then...?!

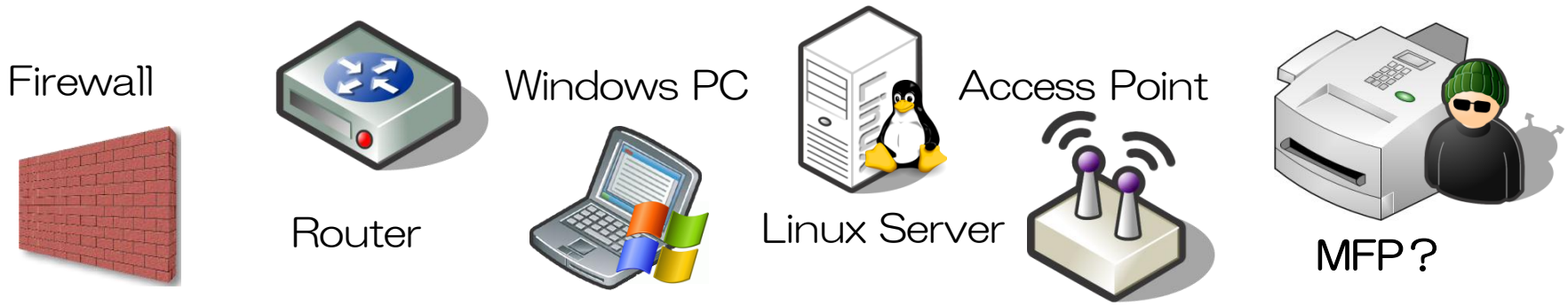


Even if Robustness is assumed in 99% of a system, the remaining 1% problems may impact the whole system.

MFP as a target of attack

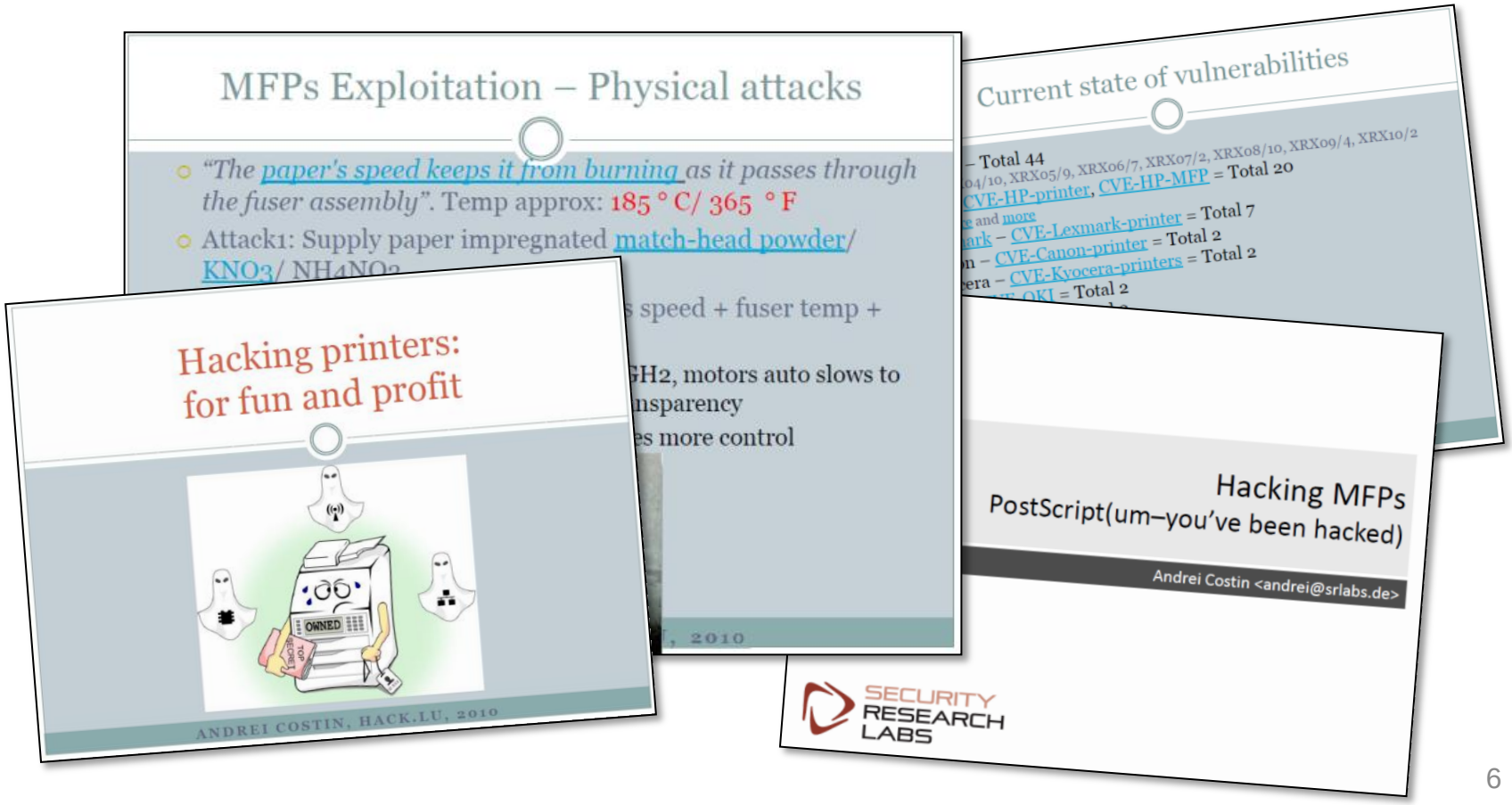
- We would have to consider the risk that IT products, which had been used without considering security so far, would be the target of attack.

Next target?



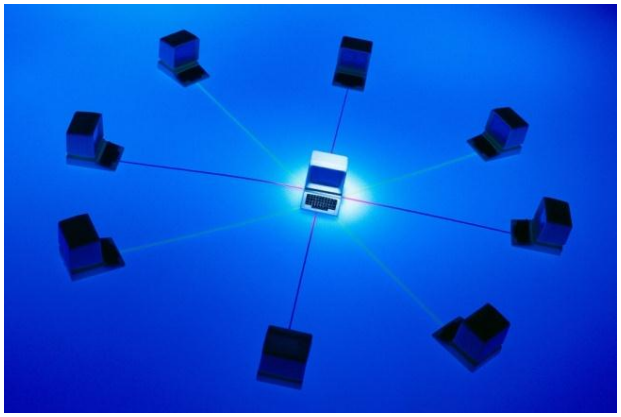
MFP: in the world-wide spotlight

- Vulnerabilities of the MFP are reported in the several International Conferences for IT Security



MFP: why・・・

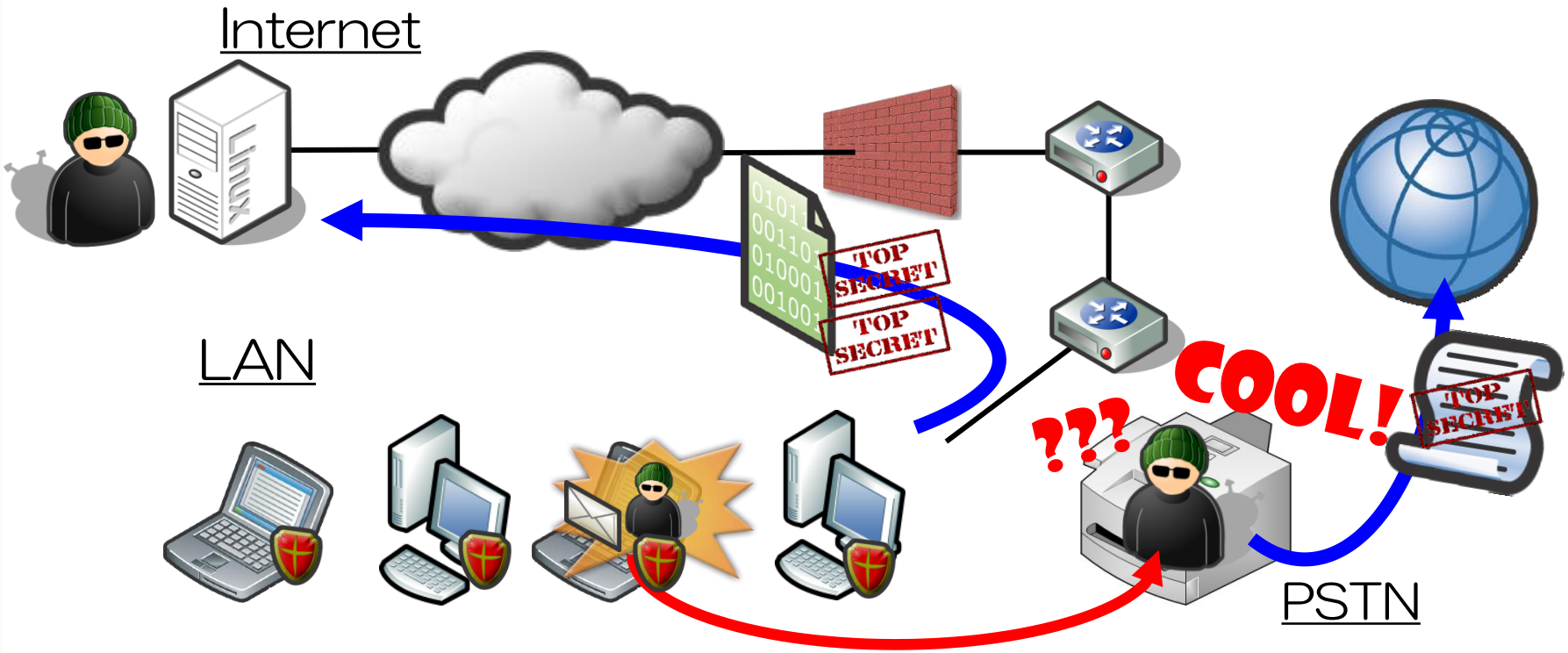
- A lot of services are working in the MFP, like web service for the administration function.
  - WEB Server
  - Printing Service (Printing/FAX)
  - FTP Server
  - Windows file share(SMB)
  - Mail server
  - Remote maintenance (toner management etc.)
  - Vendor original services　etc.



⇒ Sophisticated network device rather than PC

Moving the platform to a common architecture

Attacking scenario with MFP



For the embedded devices…
Security Function of itself + Secure operation are significant

➡ Procurement of Secure products

Security policies for procurement of Japanese government

- Security policy for Japanese government

  (Cyber Security Strategy 2013: Information Security Policy Council)

  - The risk regarding the information leakage from MFPs in the office is mentioned
  - The development of the security requirement for the MFPs and the security assessment are required as a measures towards the risk

CC certified products are expected to be utilized as the requirements for government procurement

Development of MFP PP

- IPA and NIAP lead the development of new MFP PP with TC in the CCUF for government procurement based on the governmental security policy
- In the future, this MFP PP is expected to be used worldwide as a cPP

(Road map)

2013.09 SFR draft

2013.12 First draft(SFR,SAR)

2014.03 Ver.1.0 release

- With the evaluation compliant with MFP PP, the assurance for non-existence of the exploitable vulnerabilities is required

Vulnerability-centric evaluation (VCE)

- CC based evaluation method published from CESG, known as an evaluation method for the smartcard
- Focused on the effective vulnerability analysis and testing

Apply this idea
to the MFP evaluation

satisfying the requirement regarding vulnerability and testing with minimum assurance components

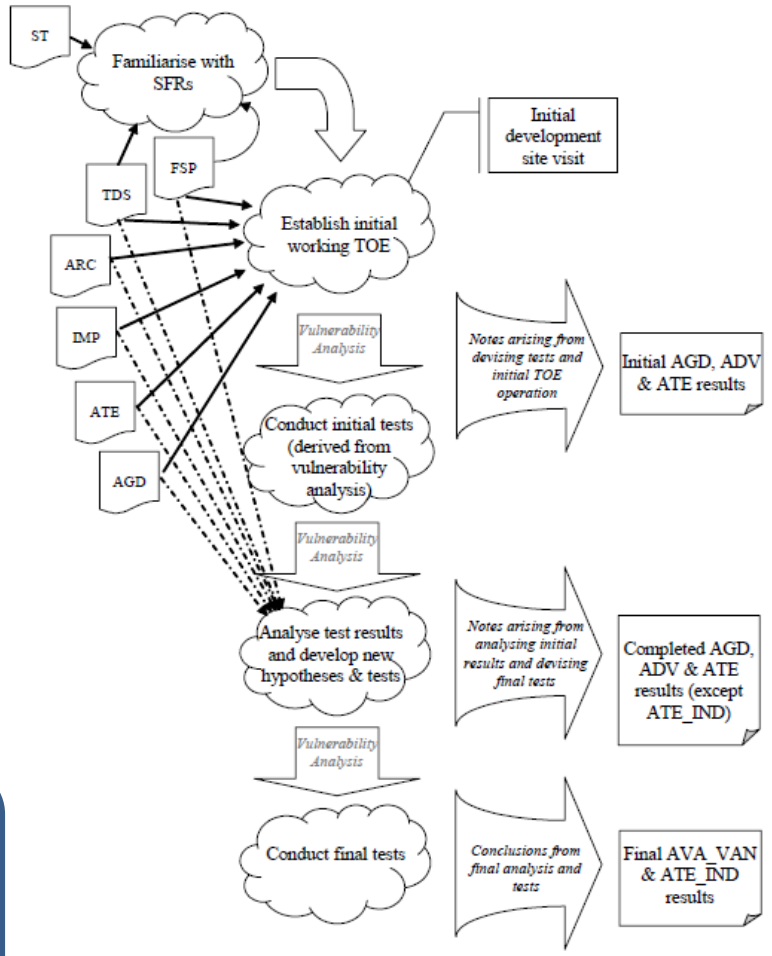


Image of the VCE process (from CESG)

Vulnerability-centric assurance activity

The flow image of VCE process in MFP Evaluation.

Comprehensive identification of potential vulnerabilities for MFP

Investigation of the testing method for vulnerabilities

Guideline about the MFPs vulnerabilities
(provide with PP)

Evaluation process (ASE, AGD, ADV etc.) to make clear the testing scope and method regarding the TOE

Planning the test scenario and conducting the penetration test

Vulnerability-centric assurance activities
(define for each SFRs)

Maximize the benefit with minimum SAR
(Benefit : assurance for the vulnerability)

Development of the vulnerability research report of the MFP(1)

- Conducting the vulnerability research in order to provide the exhaustive information of vulnerabilities and testing methods for the MFP evaluation
  - Based on the vulnerability database, experiences of evaluation/validation, other sources…
  - Published the research report on the web site (latest version: ver.2 March,2013)
  - Consists of 2 parts

    Part1: The comprehensive list of vulnerabilities

    Part2: Details of the typical vulnerabilities

Development of the vulnerability research report of the MFP(2)

Part1: The comprehensive list of vulnerabilities

- Based on the threats and attack scenario assumed in the operational environment of the MFP, identify the vulnerabilities comprehensively
- Classify the list according to the assets
- Totally, over 200 vulnerabilities are listed

▪ 6.12 Shared files on the MFP

	T. Threats to these secondary assets	M. Examples of attack methods or incidents that realize these threats	V. Vulnerabilities that may cause the examples of attack methods or incidents	Those who should take measures	
				Users	Developers
1. Confidentiality	- Files containing confidential information are leaked to a third party from shared folders in the main MFP.	- An attacker changes the requested argument to locate the path names of the configuration management files that contain the passwords for the MFP.	- Vulnerability of the undisclosed shared folders and the names of the folders that can be read because of insufficient examinations of the requests to the shared folders in the MFP.		✓
		- An attacker tricks the SQL injection to the request argument, and takes out the confidential files, regardless of any restrictions.			
		- Confidential files are leaked to a third party, because such confidential files are in the public folder in the shared folder of the MFP.	- Confidential documents are placed in the public folder by mistake (Vulnerability of the security policy leakage or insufficient security policy among administrators).	✓	

▪
▪
▪

Development of the vulnerability research report of the MFP(3)

Part2: Details of the typical vulnerabilities

- Pick up the typical vulnerabilities of the MFP, explain the detailed information of them including attack scenario, countermeasures, testing methods etc.
- Conduct the verification experiments

(examples of picked up vulnerabilities)

- Information leakage from HDD and SSD (attacking to the controller etc.)
- Vulnerability of the MFP's SDK (Java VM etc.)
- Vulnerability of the printer driver protocols (PJL,PS etc.)
- Vulnerability of the network protocols implemented in the MFP (SSL,SNMP etc.)
- Infection by a malware
- Hijacking a web session of MFP's admin function

Summary

The effective and substantial vulnerability analysis with “The vulnerability-centric assurance activities” and “The vulnerability report”

Realizing the governmental requirements with CC-certified MFP compliant with MFP PP

(The vulnerability report of the MFP (English version) will be available on the IPA’s Web-site!)

Thank you

- Fumiaki MANABE

- Japan IT Security Evaluation and Certification Scheme (JISEC)
- Information-technology Promotion Agency (IPA)
- 2-28-8, Hon-komagome, Bunkyo-ku,
- Tokyo, 113-6591, Japan

- Phone:+81(0)3-5978-7538
- Fax: +81(0)3-5978-7548

- jisec@ipa.go.jp
- http://www.ipa.go.jp/security/jisec/jisec_e/