Korea Hackers Reunion (https://h4ru.org) - HARU
사단법인 화이트해커 연합

A Risk of Security Solutions

“믿는도끼의 위협 : 기능 중심 보안솔루션의 위험성 "

passket@gmail.com

PASCON 2018

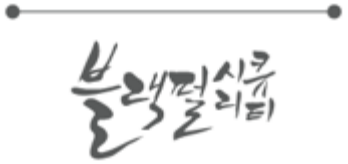
Who is it ?

Always Thinking about how to help people using hacking tech.

- **Shim, Junbo (aka passket)**
  1. HARU, CEO (since 2016)
  2. BlackPERL Security, CTO (since 2011)
  3. Advisory of KOREA Gov.
- **What's going on ?**
  1. Home Trading System Hacking
  2. SCADA / ICS System Hacking
  3. Proving Failure of ICS System over Internet
  4. Running CODEGATE Hacking Competition
  5. Many times winning of Hacking Competitions
  6. Many times giving talks for Hacking Conference.

HARU HACKERS REUNION

Introduction

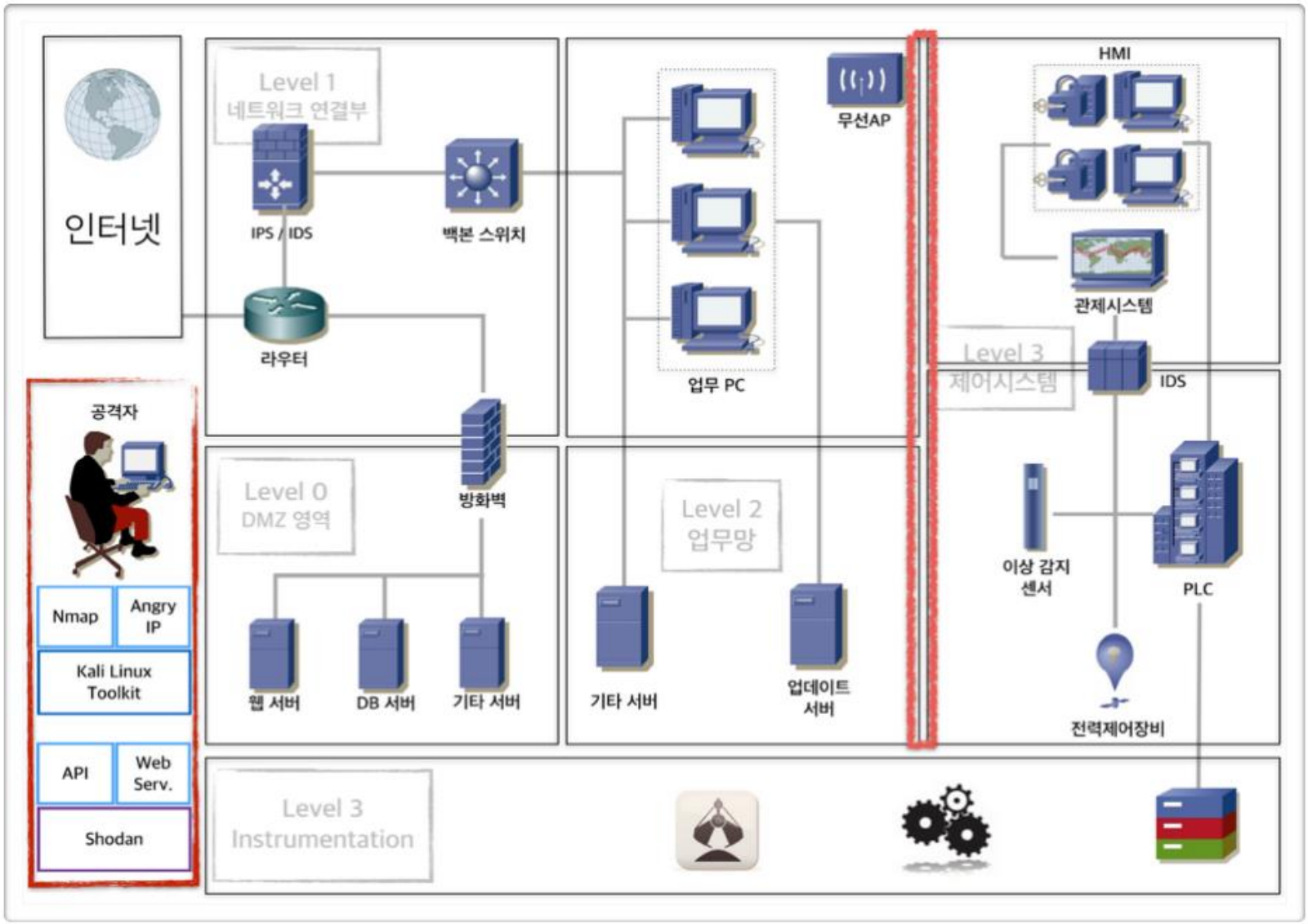


- **ALL Thing you should remember,**
- **ALL Matters has patched in this talk at this time.**

Introduction

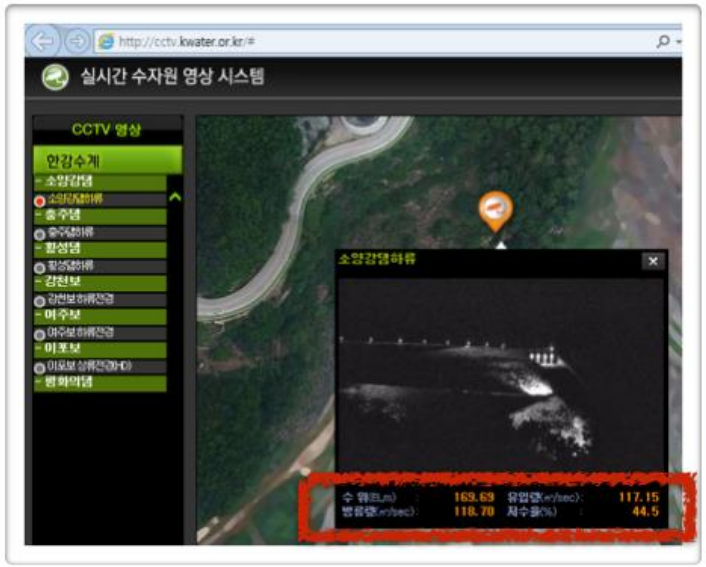
- **Gov. says .....**

Introduction



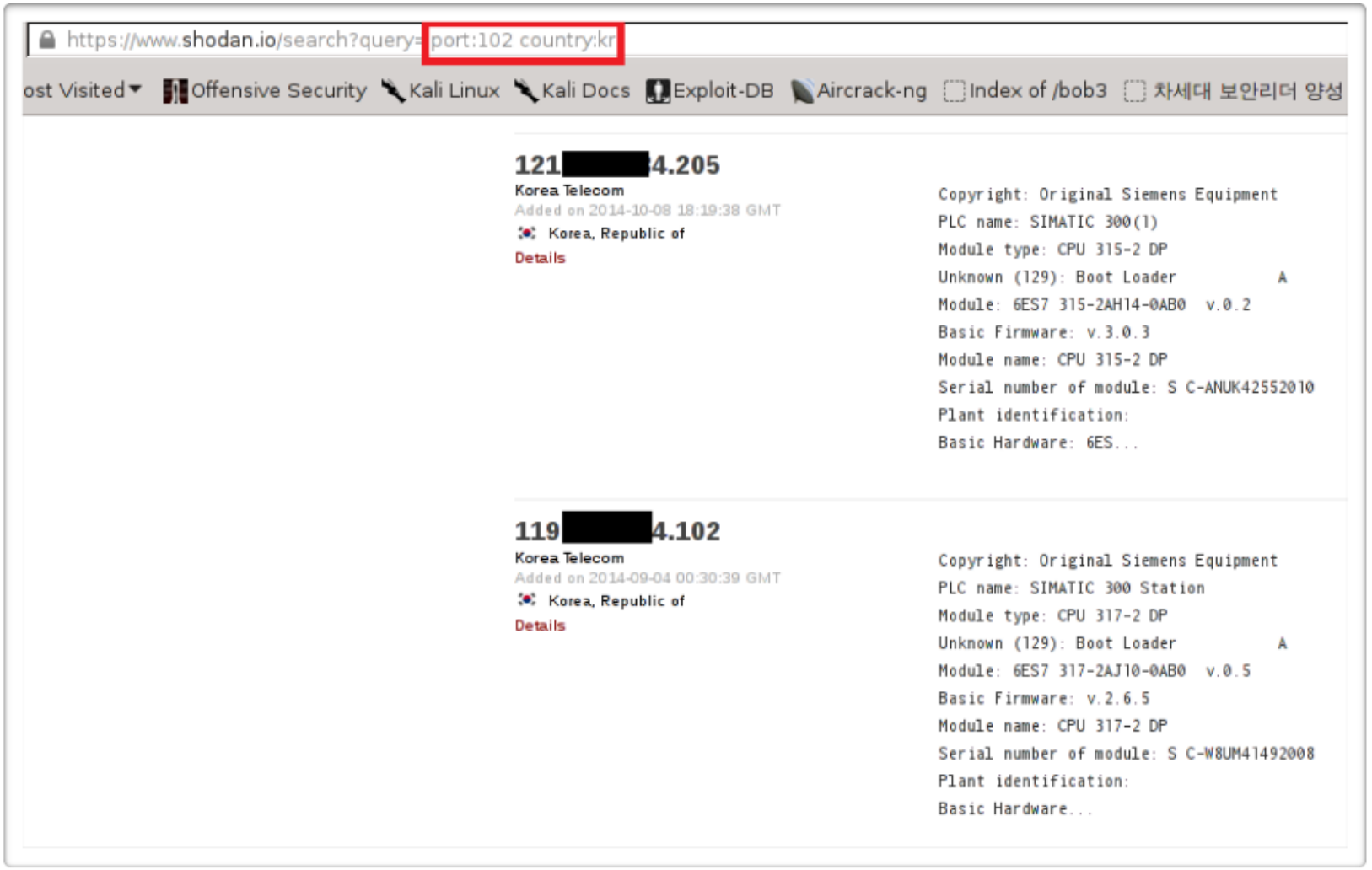
Introduction

➢ **But we have ….**



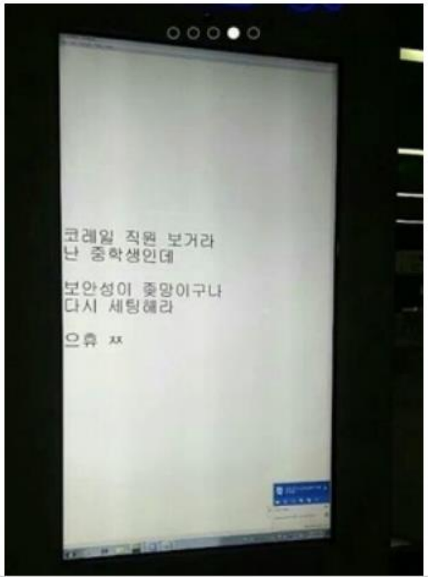
Introduction

➢ **But we have ....**



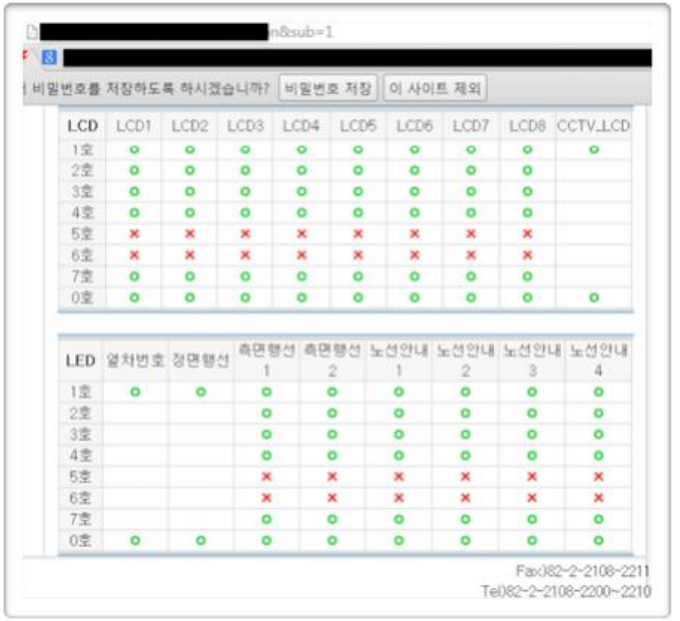
Introduction

➢ **But we have ....**



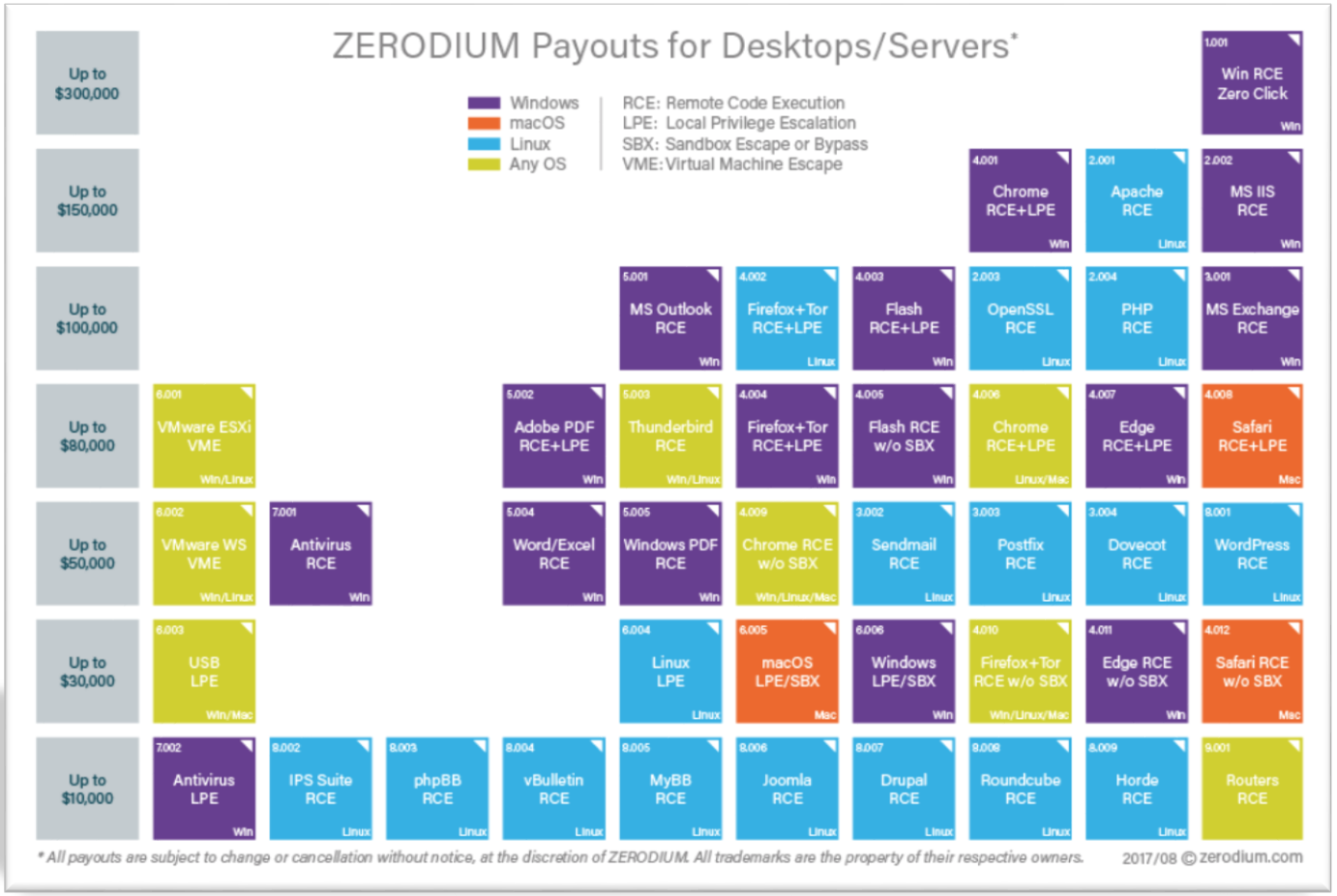
Introduction

➢ **But we have ….**



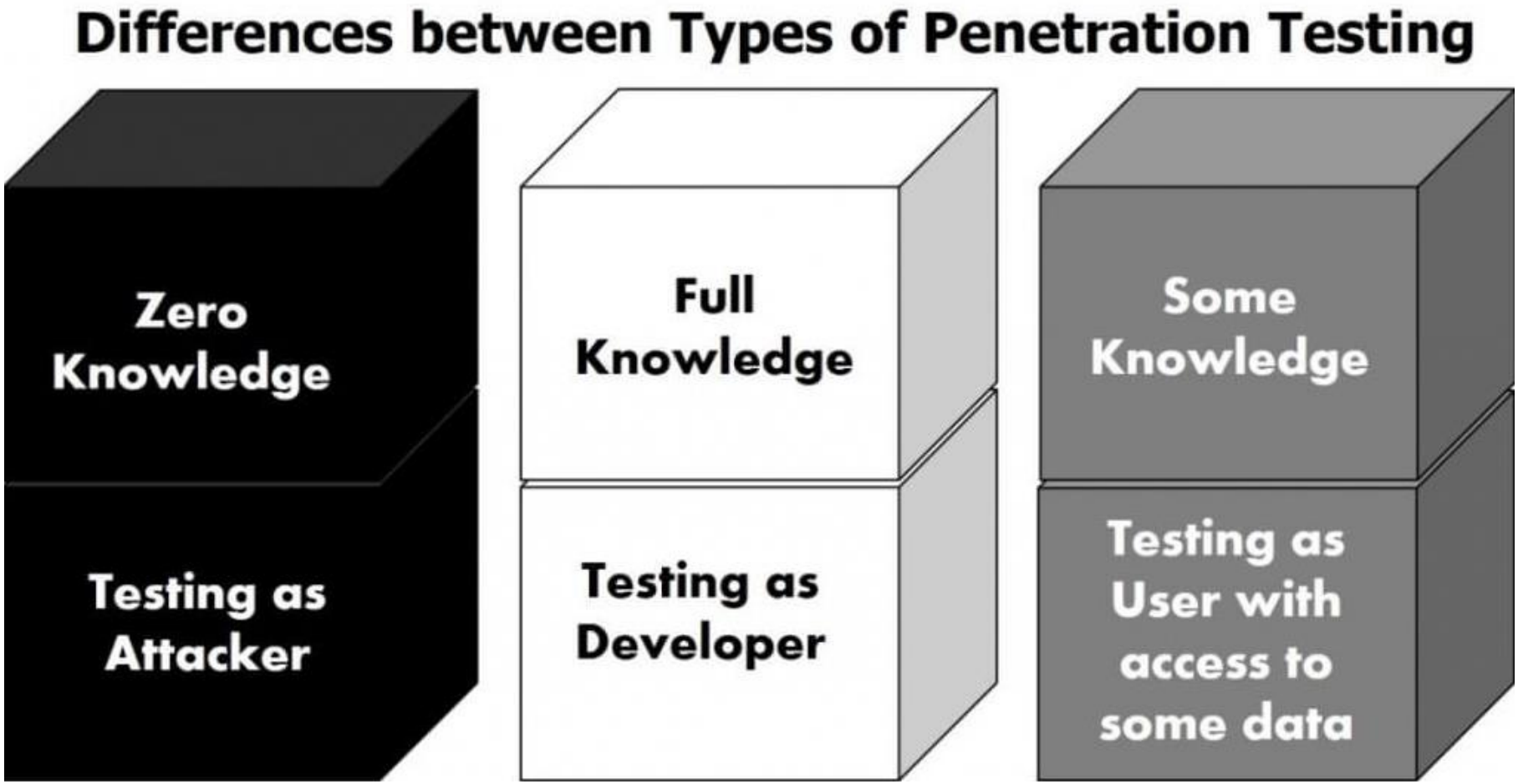
Introduction

➢ **But we have ….**



Introduction

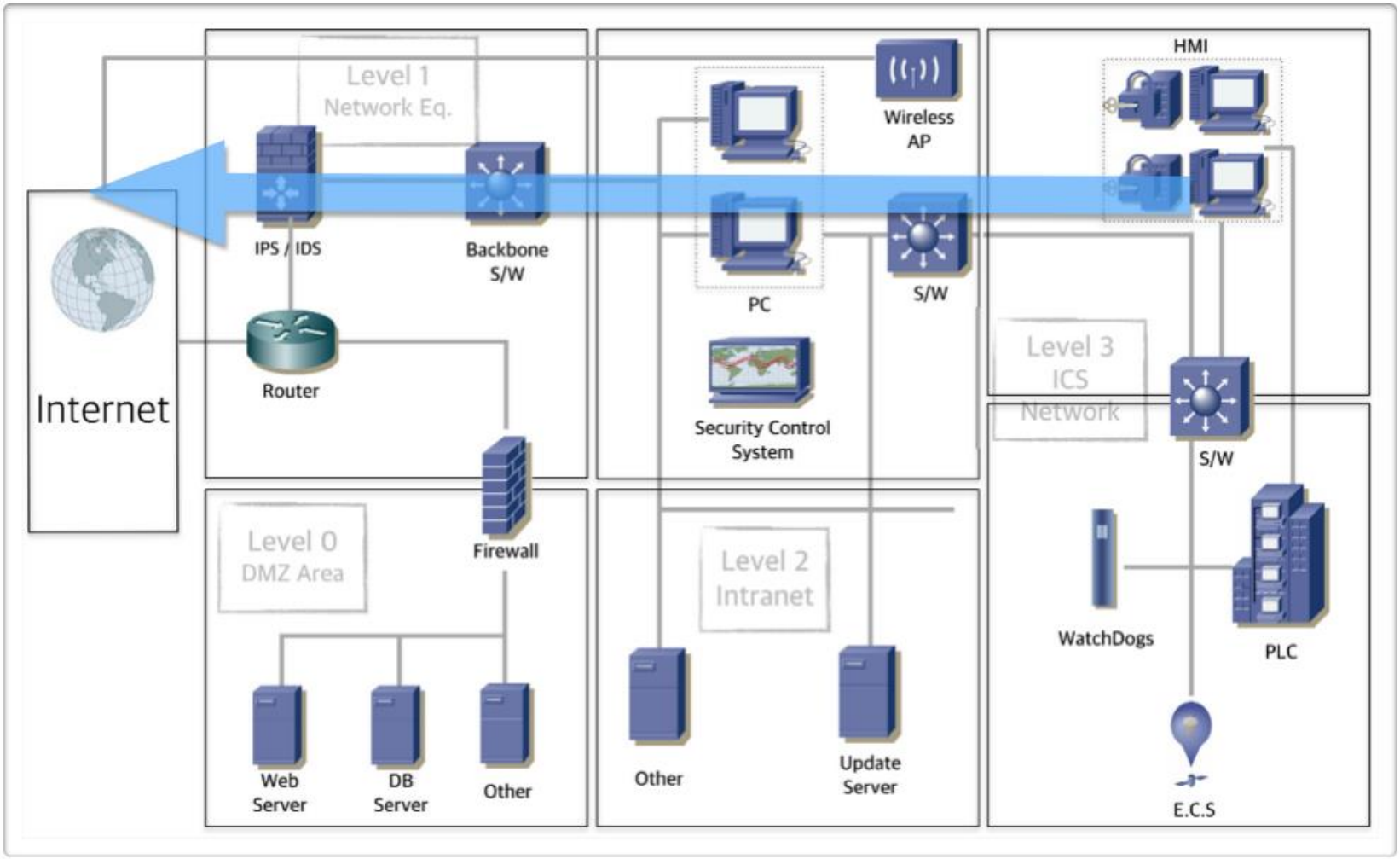
➢ **All Matters relate with**



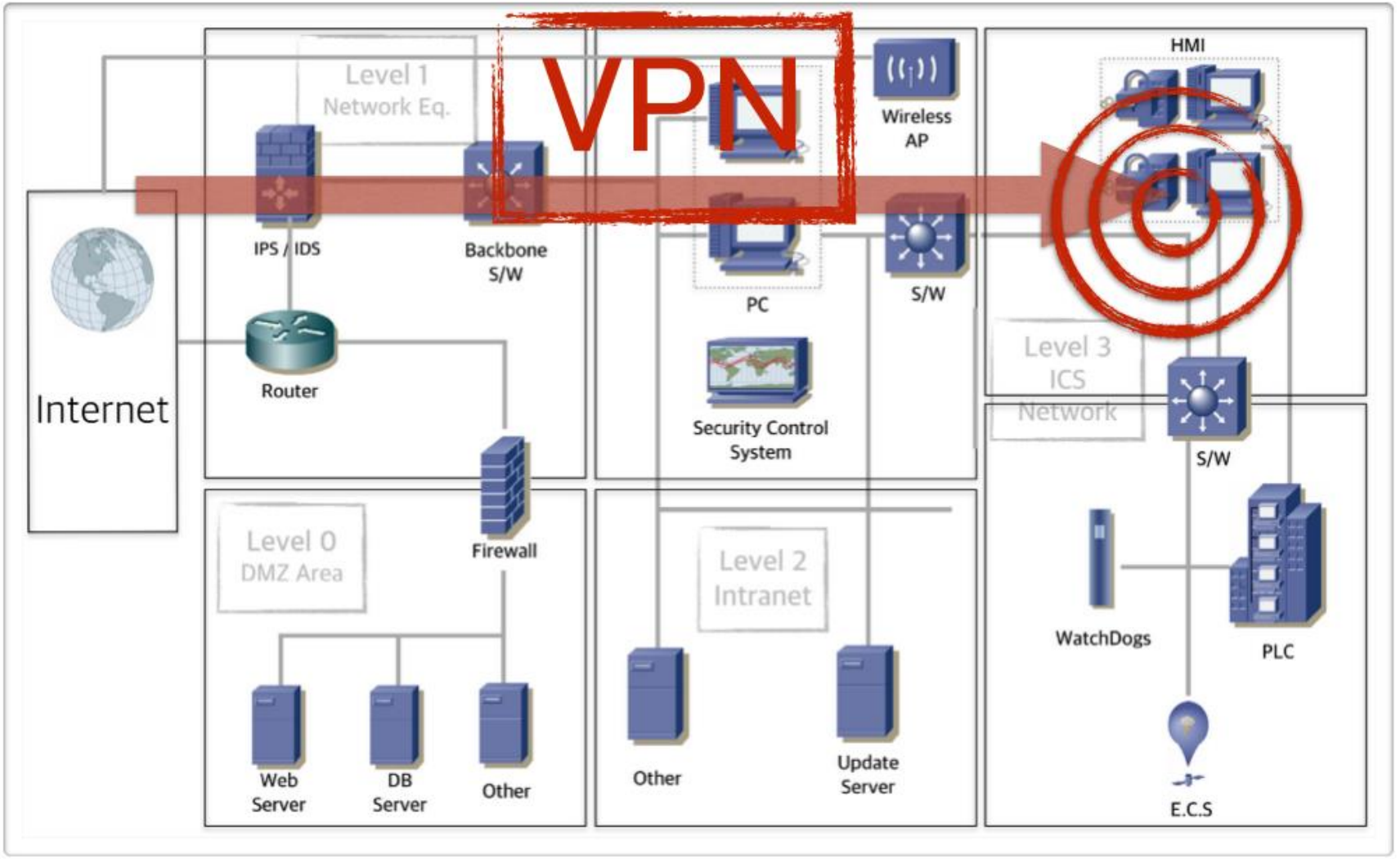
Chap. 1 DIRECT HIT

- **ALL Thing you should remember,**
- **ALL Matters has patched in this talk at this time.**

Direct Hit



Direct Hit



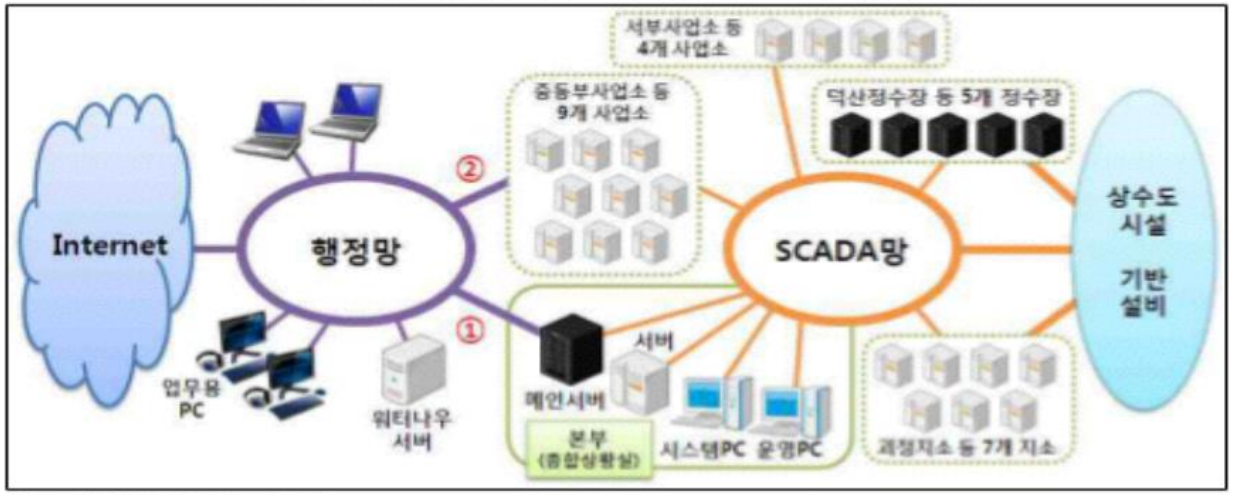
② 전산 및 제어 · 계측시스템

감사결과 요지

- 첫째, 원전 감시제어시스템(SCADA시스템)에 인터넷이 연결된 개인PC 등을 무단 연결하여 사용하거나 외부 저장매체 사용을 통제하지 않는 등 보안의식 부족으로 사이버테러에 취약한 실정이었고,
- 둘째, 원전을 감시하고 운전상태를 통보하기 위한 장비를 이중화하지 않거나 데이터 관리가 부실하여 원전 감시정보를 효율적으로 제공하지 못하고 있었으며,
- 셋째, 주제어실의 원자로를 정지시키는 기능을 갖춘 설비를 부적정하게 구성하고 개선조치를 적기에 시행하지 않는 등 원전 전산 및 제어 · 계측시스템의 구성과 운영 등에 문제가 있었다.
- 이에 대해 SCADA시스템에 대한 사이버보안을 강화하는 방안을 마련하도록 통보하였고, 원전 실시간 감시시스템과 원격정지제어반 설비를 보완하도록 통보하였다.

1.2-②-(1)	원전 중앙감시제어시스템 보안관리 부적정

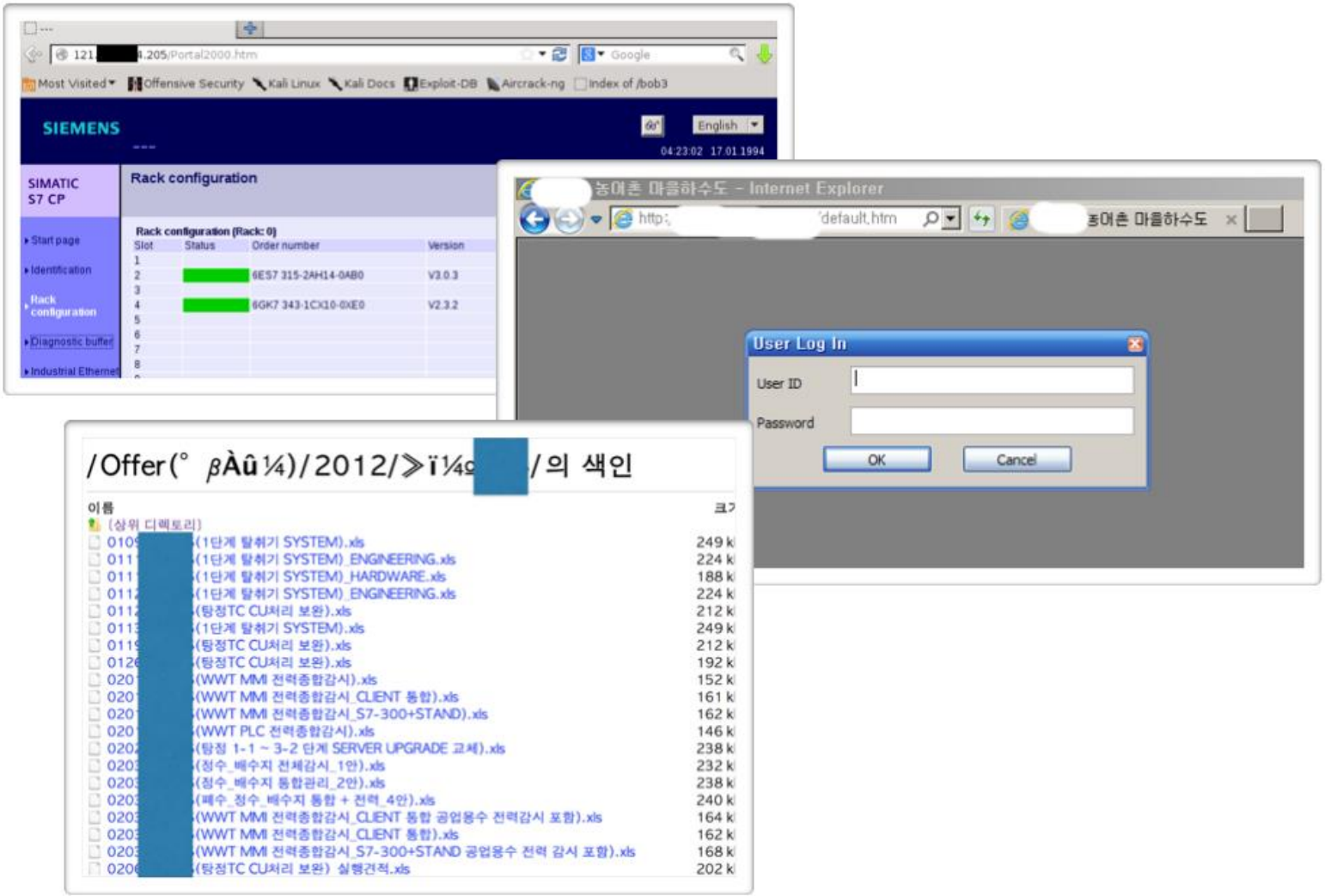
[그림 23] 부산광역시 상수도사업본부 SCADA시스템 구성도



자료: 부산광역시 자료 재구성

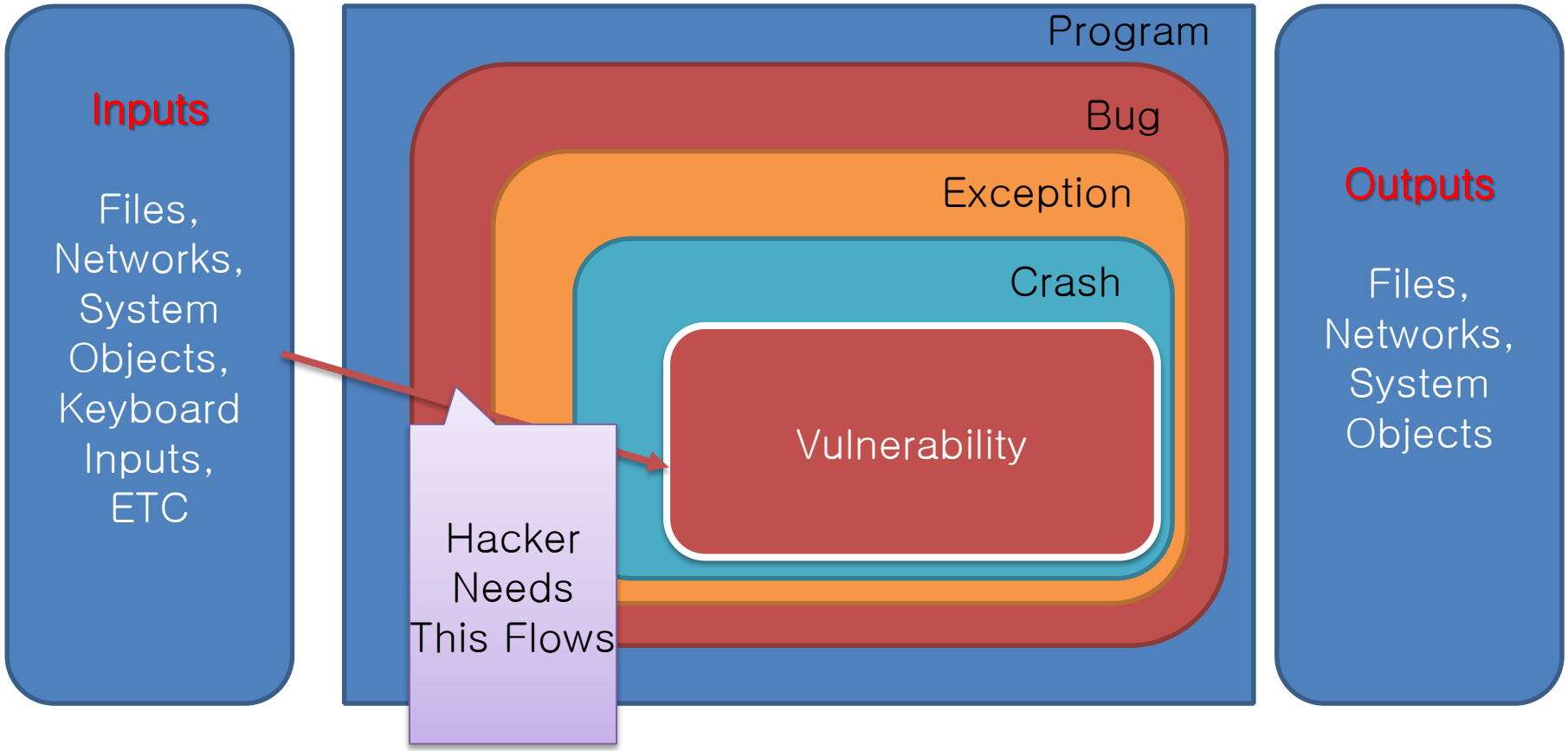
또한 2000년 부산광역시 도시정보포털시스템과의 자료 연계를 위하여 사업소 SCADA시스템을 행정망·인터넷과 임의로 연결하였고 2006년 9월과 2008년 5월에 SCADA시스템의 네트워크를 재구축할 때에도 연결을 분리하지 않아 [그림 23]의 ②와 같이 중동부사업소 등 9개 사업소의 SCADA시스템이 행정망·인터넷과 연결되어 있었고 별도의 보안대책도 수립하지 않아[323] 외부 정보통신망에서 SCADA시스템 침입이 가능하였다.[324]

Direct Hit



Direct Hit

➢ **Untrusted INPUT**



Chap. 2 INDIRECT HIT

- **ALL Thing you should remember,**
- **ALL Matters has patched in this talk at this time.**

INDirect Hit

➢ **Affected on WAF**

APACHE STRUTS VULNERABILITY CVE-2018-11776

By Larry Cashdollar August 23, 2018 11:30 AM
0 Comments

On Wednesday, August 22nd, the Apache team patched another vulnerability in the Apache Struts2 framework. Apache Struts is an open-source web application framework for developing Java web applications. The vulnerability exists when these conditions are met:

1. The alwaysSelectFullNamespace flag setting is set to true in the Struts configuration.
2. The Struts configuration file contains an <action ...> tag that does not specify either the optional namespace attribute or a wildcard namespace.

The impacted versions are Struts 2.3 - Struts 2.3.34 and Struts 2.5 - Struts 2.5.16 of the Apache Struts framework. If you are currently running an affected version, malicious users could execute code on the system remotely by injecting a custom namespace parameter via HTTP request. The user supplied value of that parameter is not sufficiently validated by the Struts framework. Successful exploitation does not require the user to be authenticated. Apache has classified the vulnerability as a "possible remote code execution"; however, the vulnerability is easy to exploit and allows code to be executed using the user context of the account running the Tomcat server. Multiple working exploits have been publicly disclosed.

For more detailed information on the vulnerability, please refer to Apache's advisory:
https://cwiki.apache.org/confluence/display/WW/S2-057

Exploits are publicly available and successful exploitation of this vulnerability has been observed in the wild.

INDirect Hit

- **Affected on AV**

Analysis and Exploitation of an ESET Vulnerability

Do we understand the risk vs. benefit trade-offs of security software?
Tavis Ormandy, June 2015

Introduction

Many antivirus products include emulation capabilities that are intended to allow unpackers to run for a few cycles before signatures are applied. ESET NOD32 uses a minifilter or kext to intercept all disk I/O, which is analyzed and then emulated if executable code is detected.

Attackers can cause I/O via Web Browsers, Email, IM, file sharing, network storage, USB, or hundreds of other vectors. Whenever a message, file, image or other data is received, it's likely some untrusted data passes through the disk. Because it's so easy for attackers to trigger emulation of untrusted code, it's critically important that the emulator is robust and isolated.

Unfortunately, analysis of ESET emulation reveals that is not the case and it can be trivially compromised. This report discusses the development of a remote root exploit for an ESET vulnerability and demonstrates how attackers could compromise ESET users. This is not a theoretical risk, recent evidence suggests a growing interest in anti-virus products from advanced attackers.

FAQ

- **Which platforms are affected?**
  ESET signatures are executable code, they're unpacked at runtime from the DAT and NUP files and then loaded as modules. As the DAT files are shared across all platforms and versions, all platforms are affected.
- **Which versions and products are affected?**
  All currently supported versions and editions of ESET share the vulnerable code.

  This includes, but is not limited to, these products:
  - ESET Smart Security for Windows
  - ESET NOD32 Antivirus for Windows
  - ESET Cyber Security Pro for OS X
  - ESET NOD32 For Linux Desktop
  - ESET Endpoint Security for Windows and OS X
  - ESET NOD32 Business Edition
- **Is the default configuration affected?**
  Yes.
- **Am I still vulnerable if I disable "Real Time" scanning?**
  If you also disable the scheduled scan, you would only be affected if you manually scan a file from a context menu or GUI.

  Note that if you disable "Real Time" scanning, ESET will constantly warn that you're not getting "maximum protection".
- **Is an exploit available for analysis?**
  Yes, a working remote root exploit is included with this report.
- **Is there an update available?**
  Yes, ESET released an update to their scan engine on 22-Jun-2015.

INDirect Hit

- **Affected on Security Protocol**

➢ **Affected on Security Protocol**

Vendor libssh CVE-2018-10933 advisories

Arch Linux

Arch Linux suggests that users upgrade to libssh version 0.8.4-1 using the command:

```
pacman -Syu "libssh>=0.8.4-1"
```

Cisco

Cisco has stated in a security advisory that they are currently investigating what devices may be affected by this vulnerability.

> "Cisco is investigating its product line to determine which products may be affected by this vulnerability. As the investigation progresses, Cisco will update this advisory with information about affected products."

Debian

Debian has announced that they released updated packages for libssh that resolve the vulnerability.

➢ **Affected on Security Protocol**

Vendor libssh CVE-2018-10933 advisories

Arch Linux

Arch Linux suggests that users upgrade to libssh version 0.8.4-1 using the command:

```
pacman -Syu "libssh>=0.8.4-1"
```

Cisco

Cisco has stated in a security advisory that they are currently investigating what devices may be affected by this vulnerability.

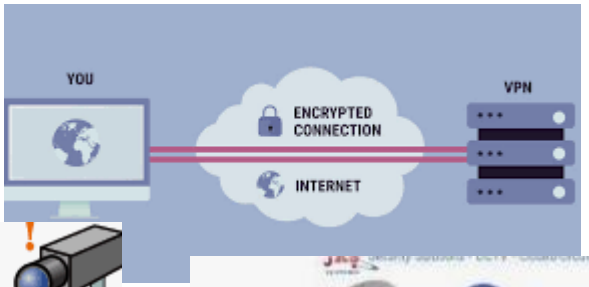
> "Cisco is investigating its product line to determine which products may be affected by this vulnerability. As the investigation progresses, Cisco will update this advisory with information about affected products."

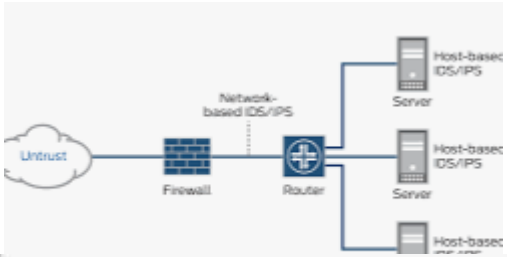
Debian

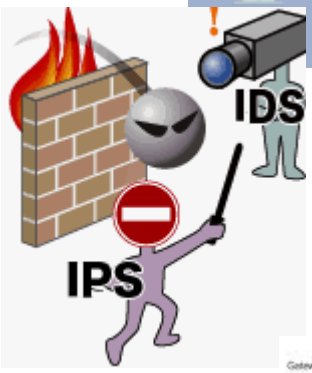
Debian has announced that they released updated packages for libssh that resolve the vulnerability.

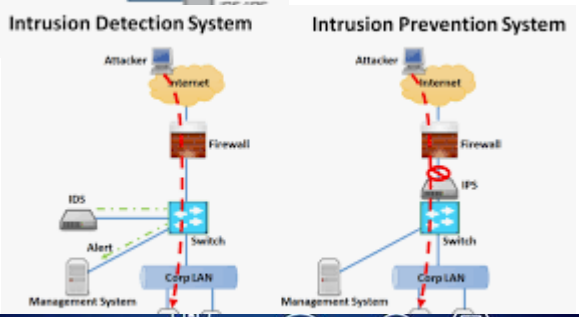
INDirect Hit

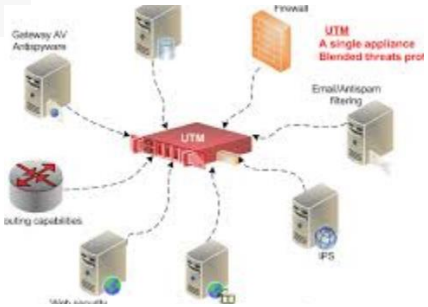
➢ **Affected on any security solutions**

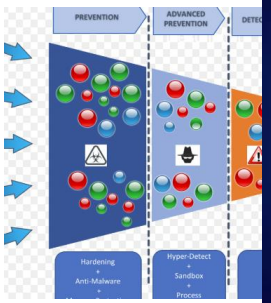












Chap. 3 What we can do ?

- **ALL Thing you should remember,**
- **ALL Matters has patched in this talk at this time.**

What we can do ?

- **APT is just word.**

  Attacking is basically side-effect problem.

What we can do ?

Proactive Security

Thank you