工業技術研究院
Industrial Technology
Research Institute

A Whitelisting Approach to Zero-Trust Cyber Defense

Tzi-cker Chiueh 關志克

Information and Communications

Research Laboratories 資通所

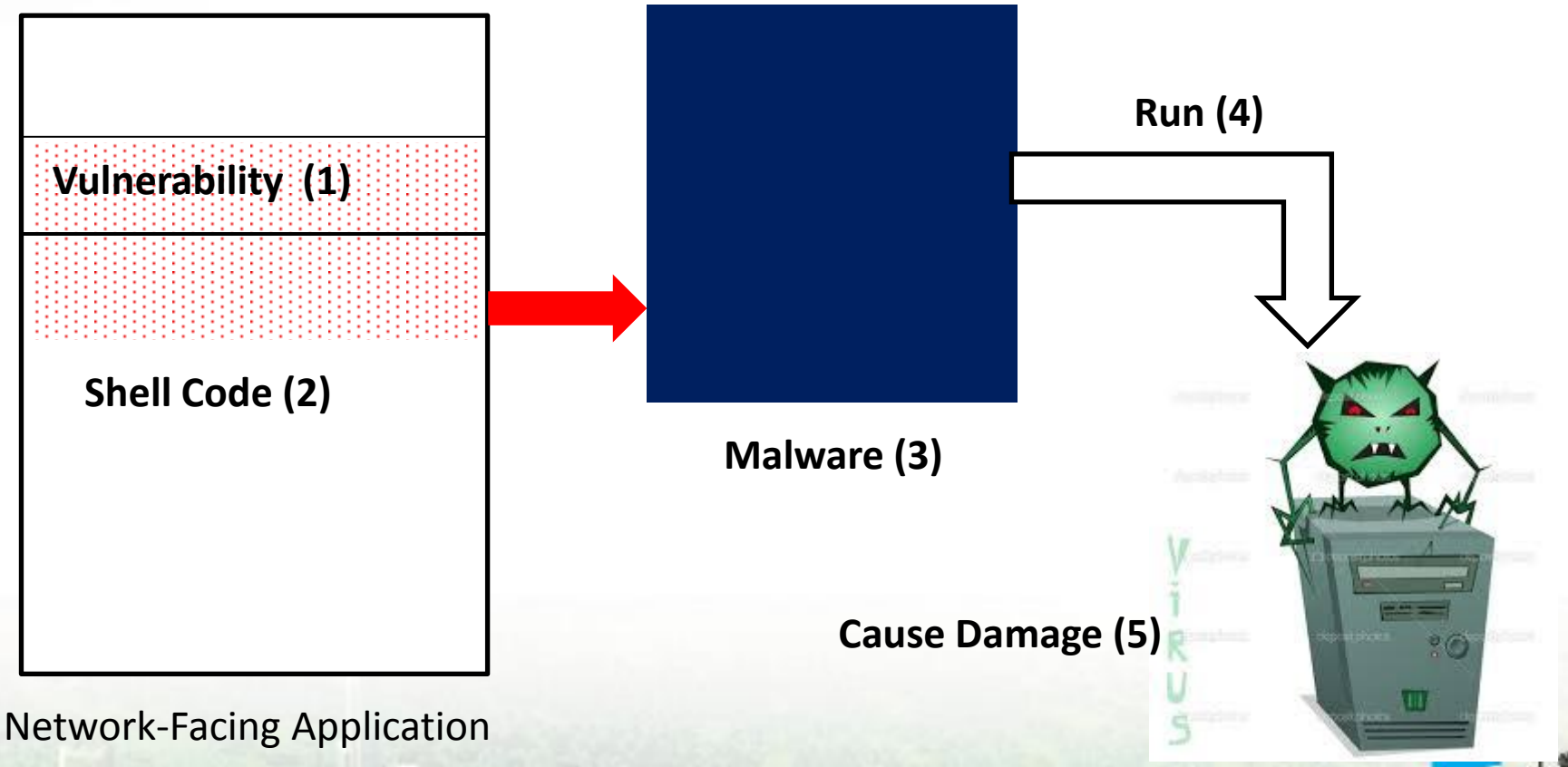
Lessons from Recent Incidents

- **TSMC security breach**
  1. Software installation USB carries malware (WannaCry)
  2. Connected new computer to internal network without AV scan
  3. Malware propagated around the network without barriers
- 總統府被駭
  1. Staff computer was compromised when connected to Internet
  2. Compromised computer brought into intranet to access email server
- 中油網路系統遭到駭客攻擊
  1. AD server compromised and job scheduling policy tampered
  2. All hosts under compromised AD server run distributed malware
- Ransomware attacks against 台塑化 、力成、盟立, Garmin, etc.

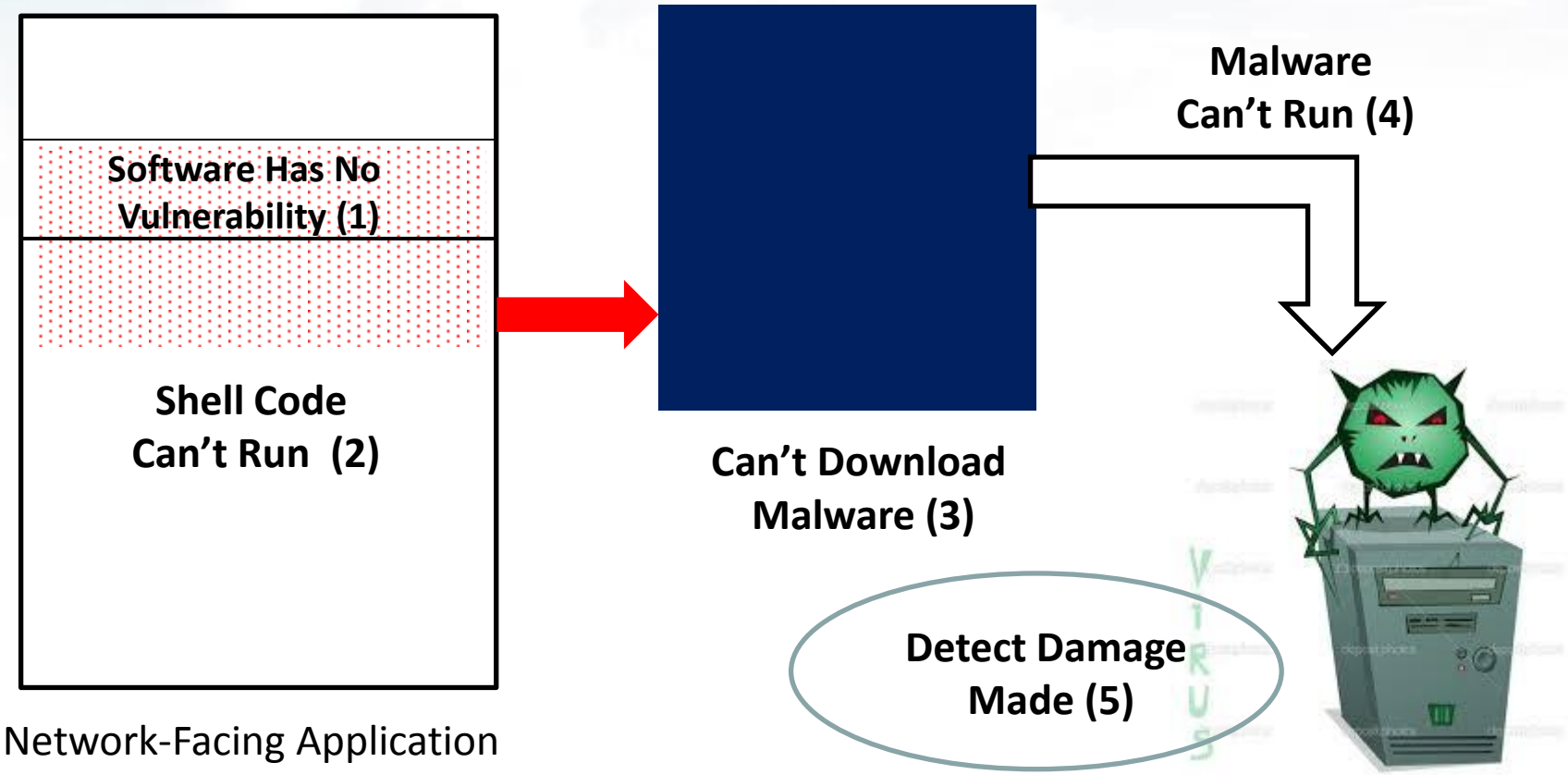
- Lessons: (1) Vulnerability exploitation (2) BYOD (3) Lateral propagation

How to Exploit a Vulnerability

Attacker's objective: get a program into the victim's computer
Example: Drive-by download, in which an email containing a link, which points to a page whose content exploits a vulnerability of a browser



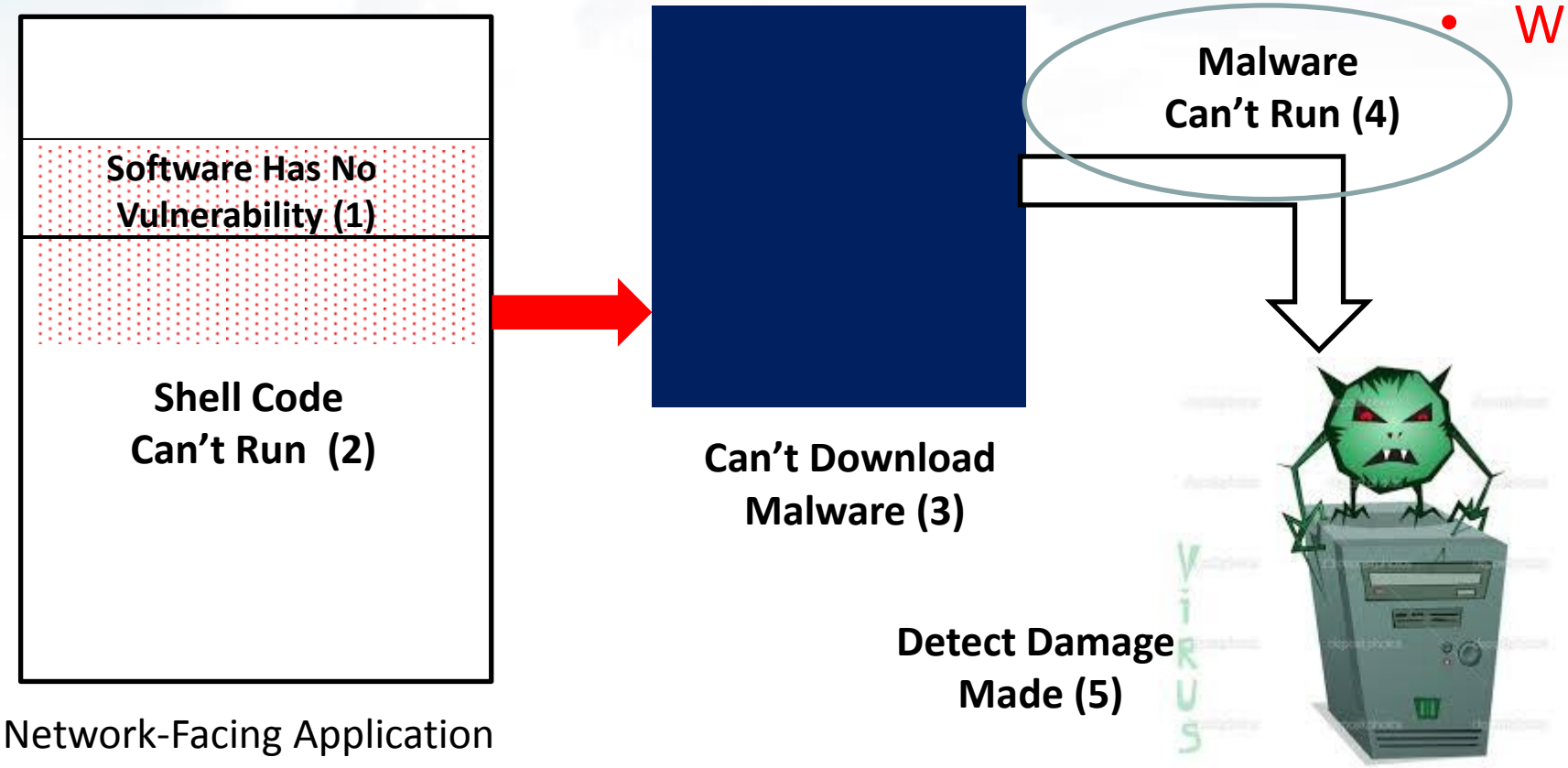
How to Stop a Vulnerability-Exploiting Attack



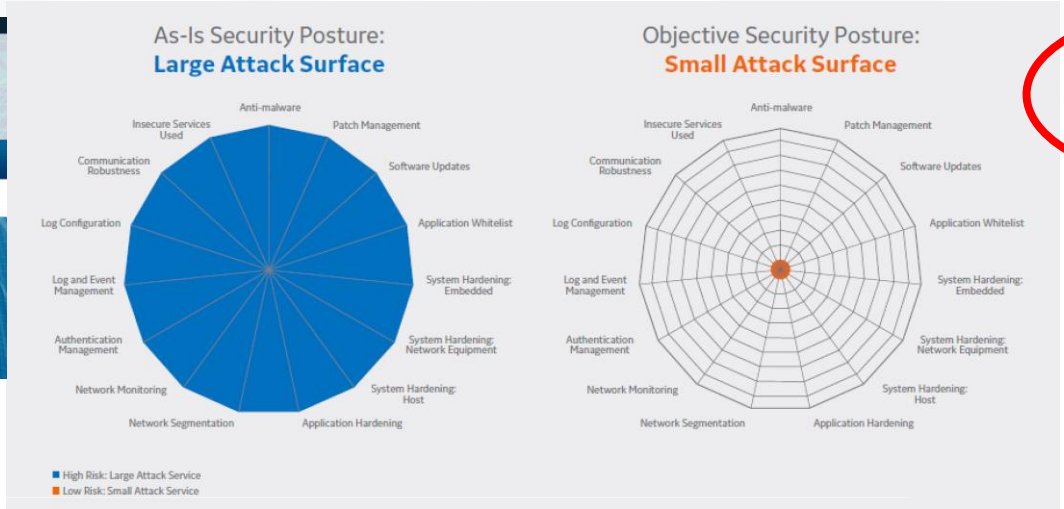
Many AI-based or anomaly detection-based cyber security solutions are here ➔ Security Information and Event Management (SIEM)

How to Stop a Vulnerability-Exploiting Attack

- Blacklist
- Whitelist



NCCIC's Seven Strategies for Defending Industrial Control Systems



7
NUMBER OF STRATEGIES
recommend by ICS-CERT to mitigate top cyber threats.

243
AVERAGE NUMBER OF DAYS
before detection that a system is compromised.

10/12
THE NUMBER OF SOFTWARE PATCHES TESTED MONTHLY
in the BHGE Validation Lab that require modifications to ensure no negative effect on operations.

26%
OF INCIDENTS
investigated by ICS-CERT were spear phishing, making it the leading threat for 2016.

74%
OF EXPLOITS
are targeted at applications, with more than 40% of those being Microsoft & Adobe.

98%
NUMBER OF INCIDENTS
ICS-CERT responded to in FY2014 and FY2015 that would have been prevented using the Seven Strategies.

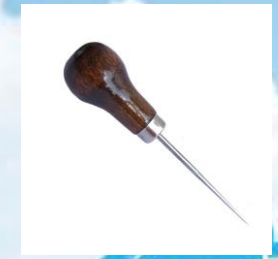
SecurityST addresses ALL 7 STRATEGIES

Percentages represent the number of ICS-CERT reported incidents in 2014 and 2015 that would have been prevented using that specific strategy.

- **38%** APPLICATION WHITELISTING
- **29%** PROPER CONFIGURATION/ PATCH MANAGEMENT
- **17%** REDUCE YOUR ATTACK SURFACE
- **9%** BUILD A DEFENDABLE ENVIRONMENT
- **4%** MANAGE AUTHENTICATION
- **2%** MONITOR AND RESPOND
- **1%** SECURE REMOTE ACCESS

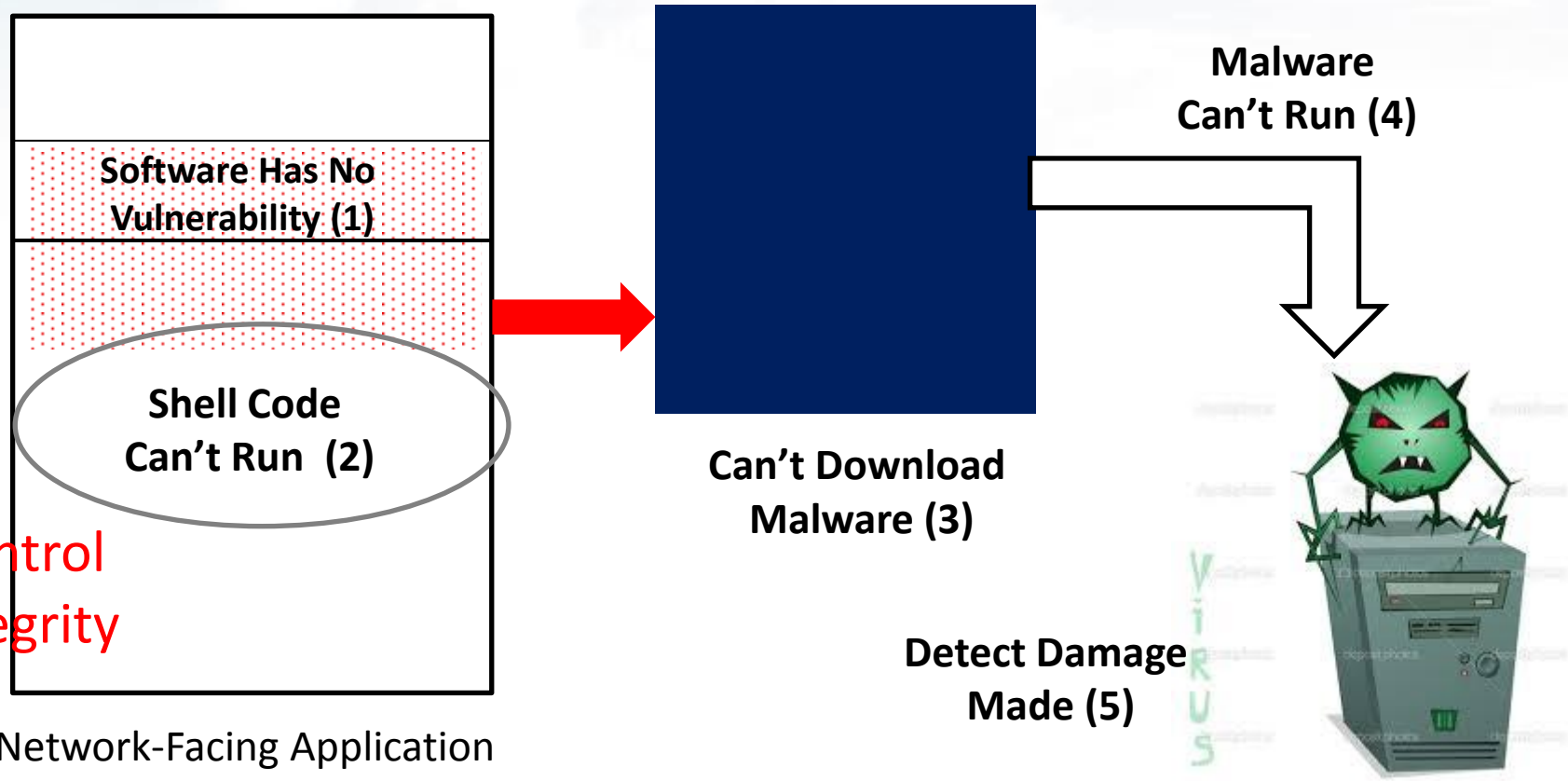
工業技術研究院
Industrial Technology Research Institute

Windows-based AWL



- AWL check for binary code, shared library and kernel module, as well as scripts written in interpretive languages, e.g., Power shell, command shell, python, Java, etc.
- System administration flexibility: physically enabled scoped turn-off of AWL check to enable interactive system maintenance & false positive resolution
- Main Technical Challenges:
  - Automated creation of the initial application whitelist, e.g., a Windows 2020 server
  - Automated and accurate AWL update upon application Installation or update (AIU)
    - Manually re-scan a given Windows machine
    - Manually initiate an AIU transaction against a set of machines
    - A Windows Update server initiates an AIU transaction against a set of client machines
    - An AD server initiates an AIU transaction against a set of AD client machines
    - When an application whitelisted on a Windows machine self-updates itself, e.g., Chrome

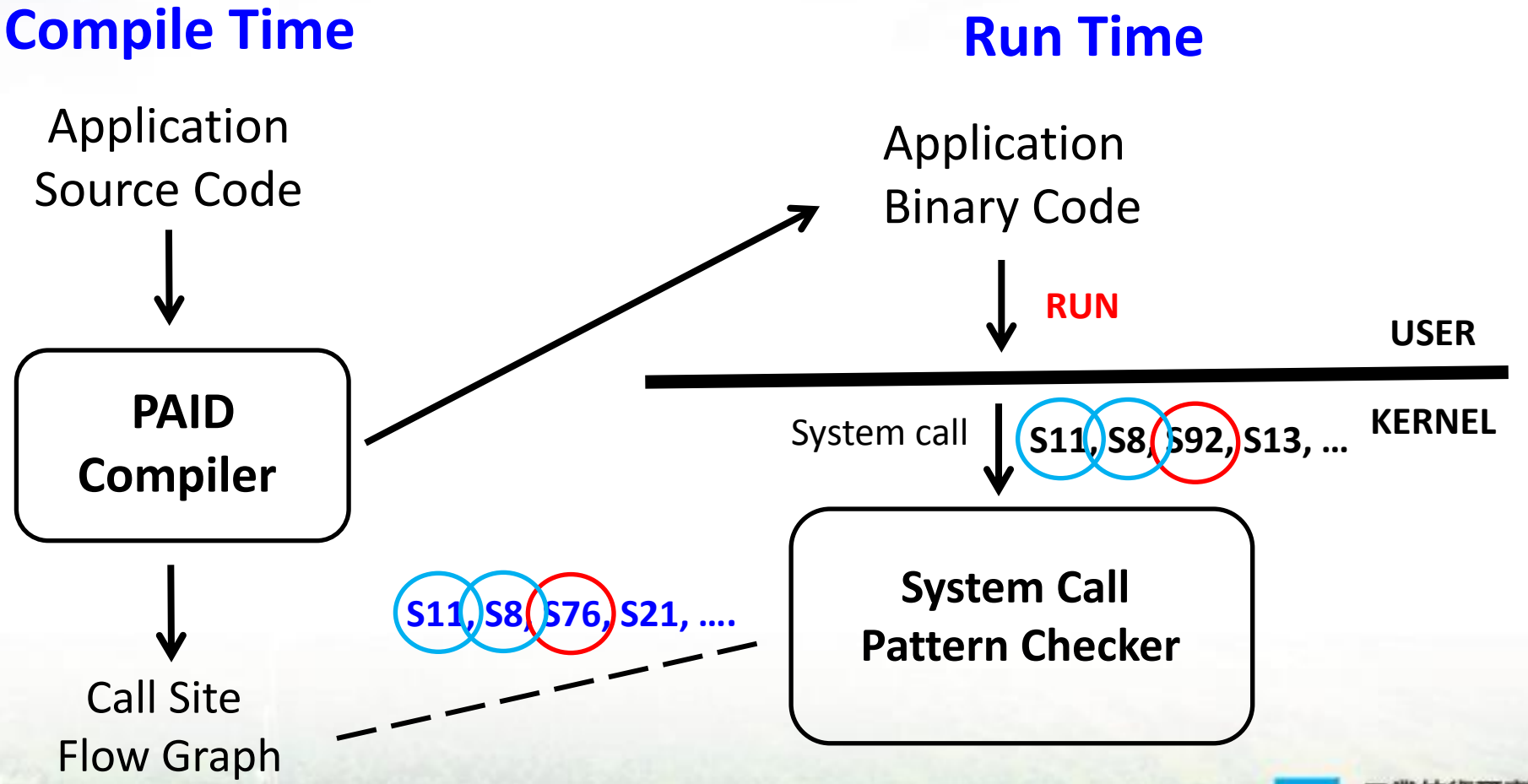
What If Allowed Programs Have Vulnerabilities?



PAID, Control Flow Integrity

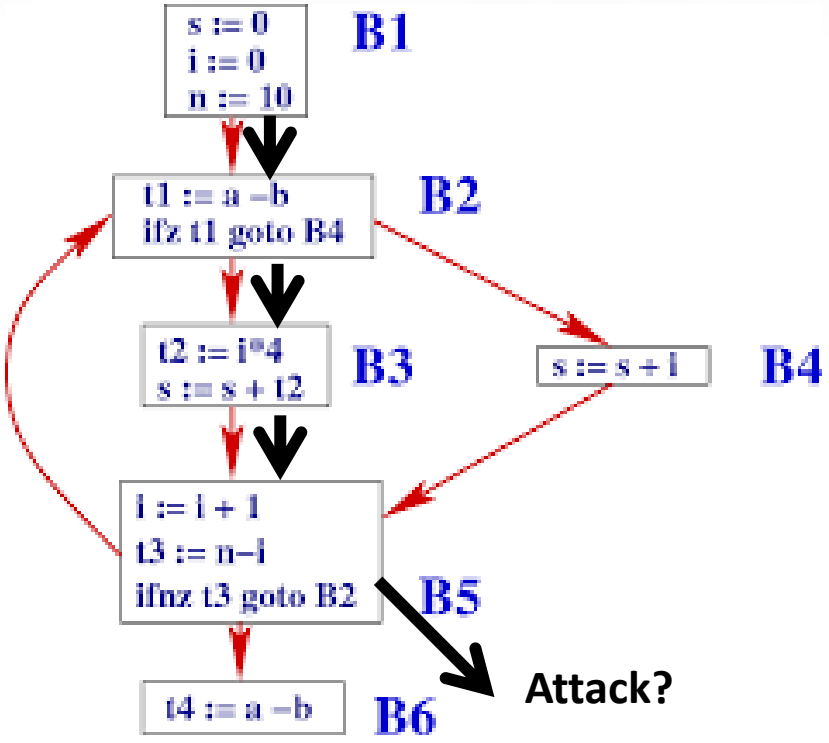
Program Semantics-Aware Intrusion Detection

Objective: A program is only allowed to make system calls at run time in a way specified by its code: which calls, where and in what order



Control Flow Integrity Assurance

- **Objective**: A program's execution follows its control flow graph
- Why?
  - Code injection attack is getting harder
  - Code reuse attack is on the rise
    - Return to libc
    - Return-oriented programming (ROP)
- Enforcement of control flow integrity
  - **Compile time**: compute the control flow graph and targets of indirect jumps/calls
  - **Run time**: check the actual targets of indirect jumps/calls are the same as those computed at compile time
- Used in Android kernel/framework



Multi-Tier Whitelisting as Unified Host Defense

- **Key idea**: Extract the allowed run-time behaviors from programs installed on a fixed-functionality device, and check the run-time execution of these programs against the allowed behaviors to detect any deviations/attacks
  - Characterize the good rather than profile the bad
  - **Fixed-functionality devices** include IoT device/gateway, ATM, SWIFT server, PLC controlle, machining tool, WiFi router, smart lamp post, smart meter, smart speaker, home gateway, drone, autonomous driving vehicle, etc.
- Multiple tiers of whitelist check on a program's run-time behavior

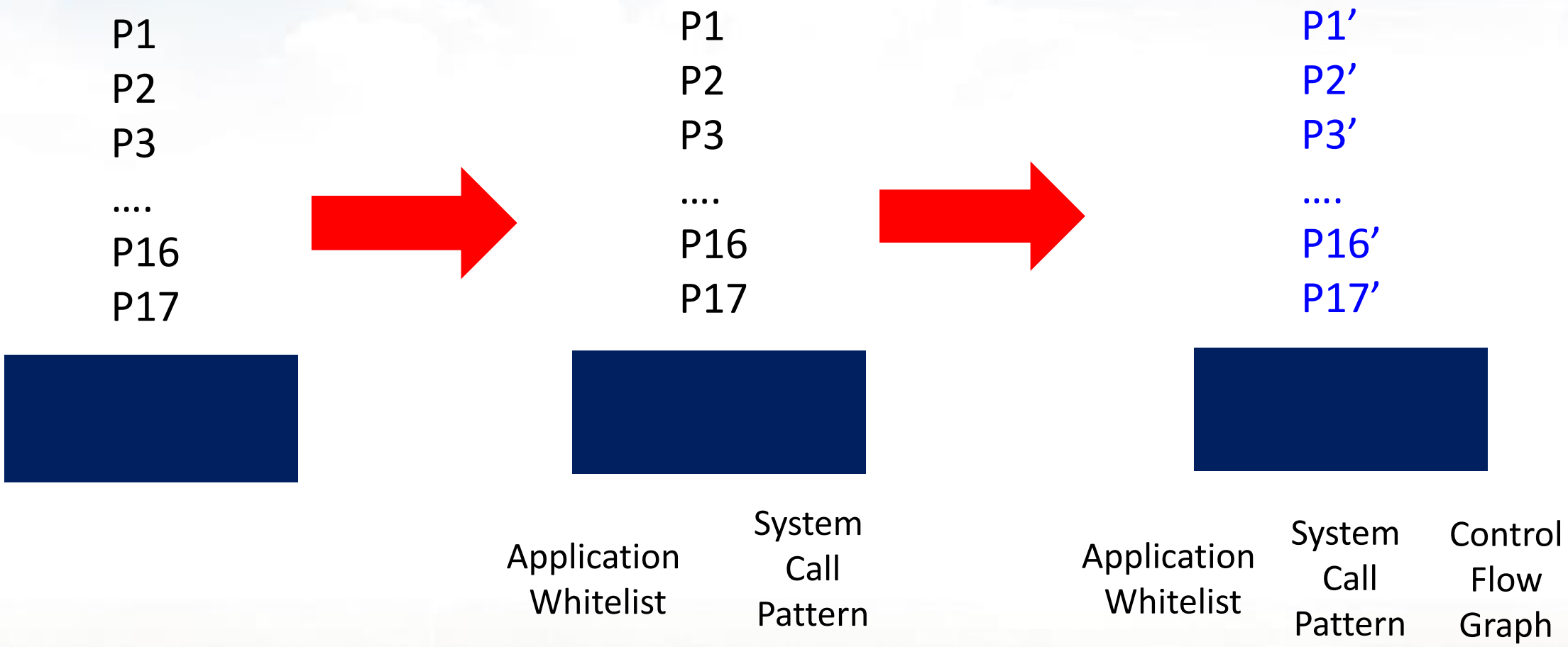
  Tier 1: A program's binary code as a whole

  Tier 2: The set of system resources accessed by a program

  Tier 3: The system calls that a program makes

  Tier 4: The control transfer flow during a program's execution

How to Whitelist a Fixed-Functionality Device?



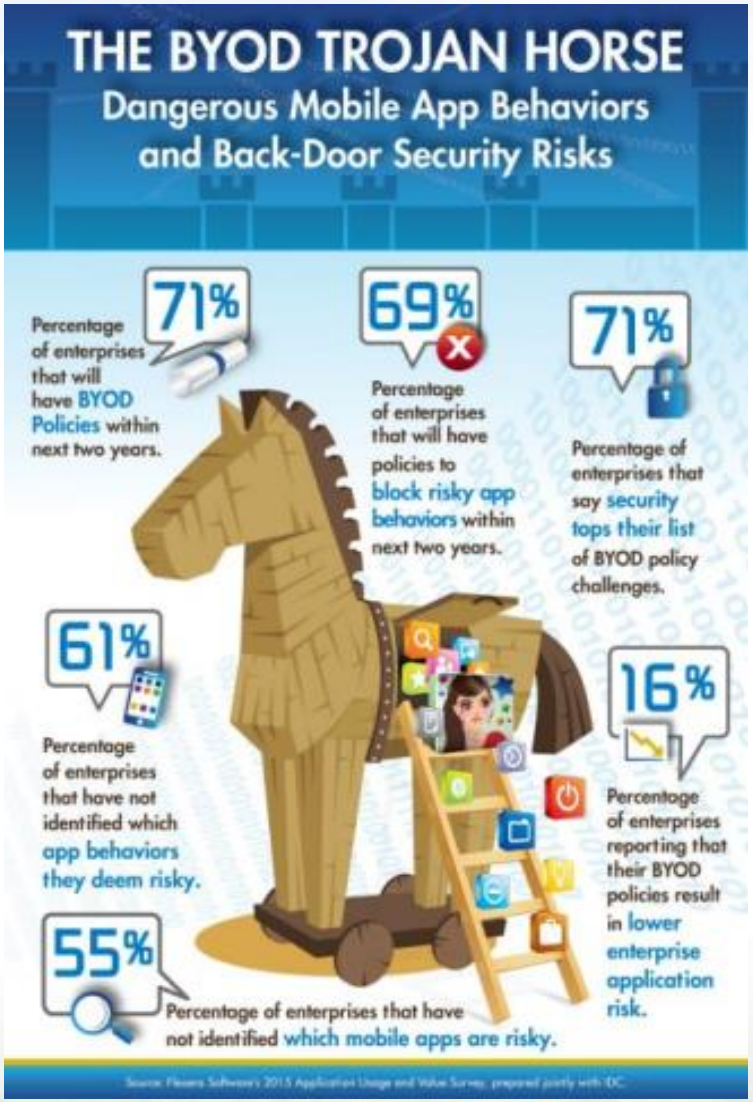
Beyond Individual Hosts

Applying Whitelisting to Enterprise Security

- **Level 1:** Which programs are allowed to run on a server
- **Level 2:** Which system resources on a server are accessible to each allowed program on that server
- **Level 3:** Which client computers and other servers are allowed to interact with programs running on a server
- **Level 4:** Which programs on allowed clients/servers are permitted to interact with programs running on a server

Bring Your Own Device (BYOD)

- Devices brought into an enterprise by official employees and unofficial contractors
  - Laptop, smartphone, USB flash drive
- Malware on these devices could bypass peripheral defense to compromise the enterprise network
- Defense strategy: Enforce the invariant that on BYOD devices, only pre-defined programs, e.g. virtual smartphone client, could interact with services on the enterprise network



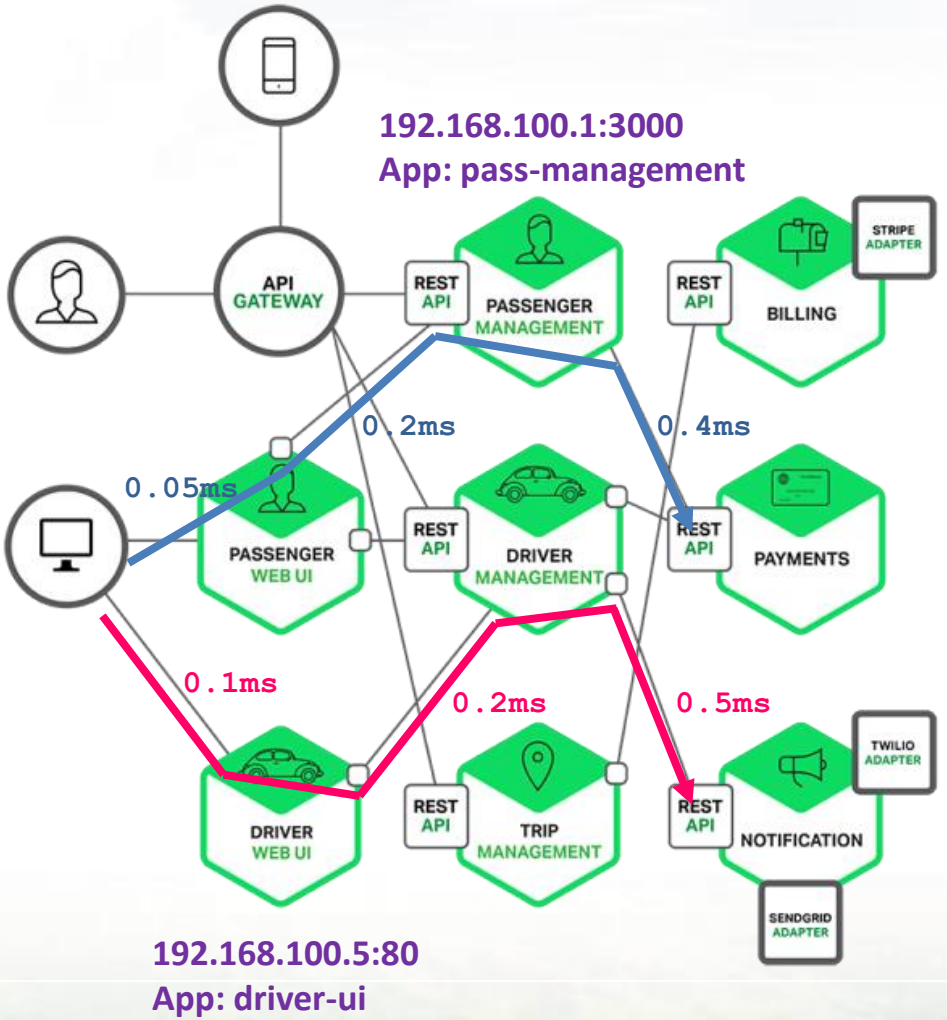
APP Streaming/VMI

- Use model: every enterprise employee is given a virtual smartphone in the cloud to do office work
  - An enterprise employee's or contractor's smartphone/laptop is able to interact with the enterprise's IT services through exactly one program: the AP/VMI client.

- Vision: One APP for all (Android) APPs
  - APPs run in the cloud, experience all sensors in a user's smartphone, and stream their outputs to the smartphone's audio/video devices.
  - No enterprise data could be downloaded to employee smartphones.
  - Enterprise smartphones/laptops now could be managed: data leakage prevention for LINE.

App-Level Firewalling: Micro-Segmentation

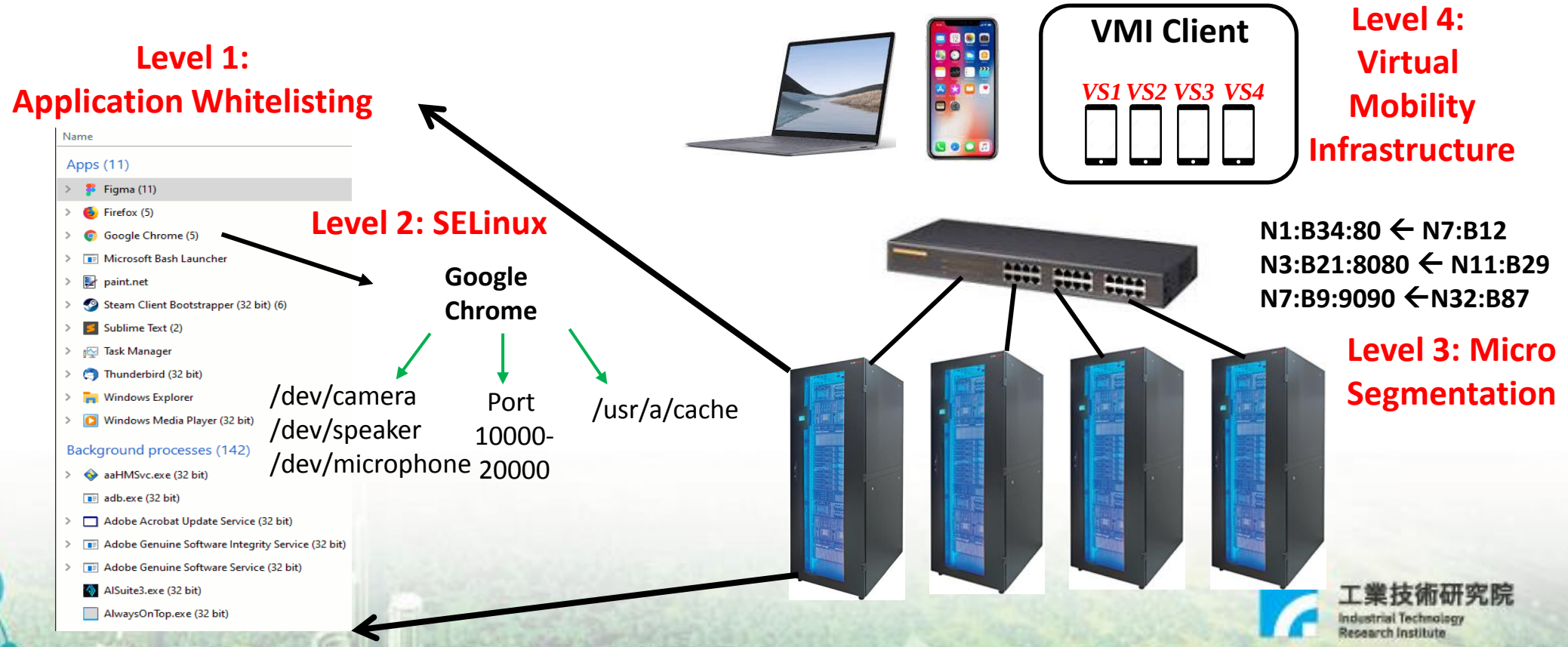
- Objective: Limit the scope of lateral propagation of a malware attack when it compromises an enterprise net node
  - Flat ➔ VLAN ➔ Application-aware network segment
- Communications Whitelisting: Restrict the allowed communications among virtual machines or containers according to application-level communications patterns
  - 192.168.1.10:7891 --- 192.168.2.3:80
  - Chrome: xxxx --- Apache:80
- Challenge: How to distinguish between attacks and firewall rule violations due to exceptions or dynamic environments?



工業技術研究院
Industrial Technology Research Institute

Whitelisting as Unified Cyber Defense Strategy

- Carefully design (green field) or characterize (legacy) allowed system behaviors
  - Which software programs
  - What resources they could access
  - Which programs could communicate with which



Summary

- Whitelisting is a generalization of secure boot to every aspect of a computer system's run-time behavior
  - BIOS
  - OS
  - Application's static image
  - Application's dynamic behavior
  - Communicating parties over the network
  - Programs used by communicating parties
- **Unified zero-trust design principle**: Only those that are explicitly allowed could proceed at run time
  - Pro: Zero false negative and no need to worry about new attacks
  - Con: How to ensure zero false positive in the presence of incomplete security policy rules and system changes

Thank You!

Questions and Comments?

tcc@itri.org.tw