Lightweight Monitoring of Program Authenticity and Integrity for IoT Devices in Operation

NEC Corporation

Detect program tampering by verifying the authenticity and integrity of its execution codes and control flows

Application Area: IoT, ICT vendor, Manufacturer, Infrastructure, Distribution, Building / Smart City

Technology Features

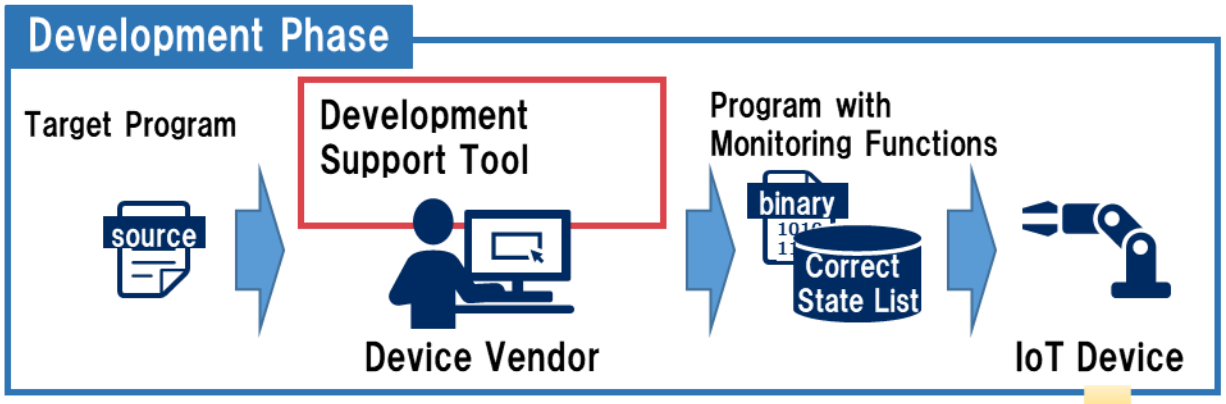
- **Monitor program integrity for IoT devices with limited performance and memory capacity**
  Detect tampering in execution codes and control flows of the programs on memory for IoT devices in operation immediately, by incorporating this mechanism into those target programs.
- **Generate "correct state list" automatically that minimize the impact on device operation**
  Analyze the target program structure of IoT device, and automatically determine the timings and ranges of verifying the authenticity and integrity which are suitable for each program, and generate "correct state list" that is the criteria for verification.

Effects

- **Enable to monitor IoT devices continuously, having difficulty to apply security measures**
  Enhance the security of entire IoT system by monitoring continuously the authenticity and integrity of IoT devices, located at the distant end and operating without stopping for a long time.
- **Facilitate applying this security measure for ones without advanced IT or security skills**
  Make it easy to apply this security measure by providing support tools including "correct state list" generator for the target program of IoT device, and reduce the maintenance costs accompanied with updates of the target program.

Use case

- **Monitor the authenticity and integrity of programs for IoT devices used in the fields of manufacturing (factory) , merchandising, mobility, building, etc.**

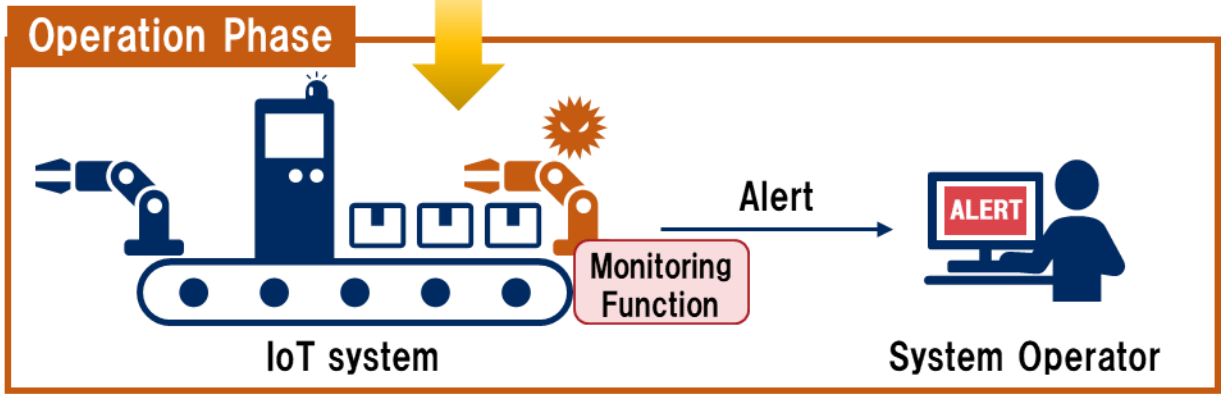


For device vendors

Support introducing the monitoring function into IoT devices by development tool

For device users / system operators

Quickly detect unauthorized modifications on the target programs



Lightweight Monitoring of Program Authenticity and Integrity for IoT Devices in Operation

NEC Corporation

Technology Description

■ Security Problems in IoT Devices and Overview of R&D

- Cyber attack risk in IoT devices is increasing, and its impacts are spreading to the entire system
- IoT devices have difficulty to apply security measures due to hardware resource constraints

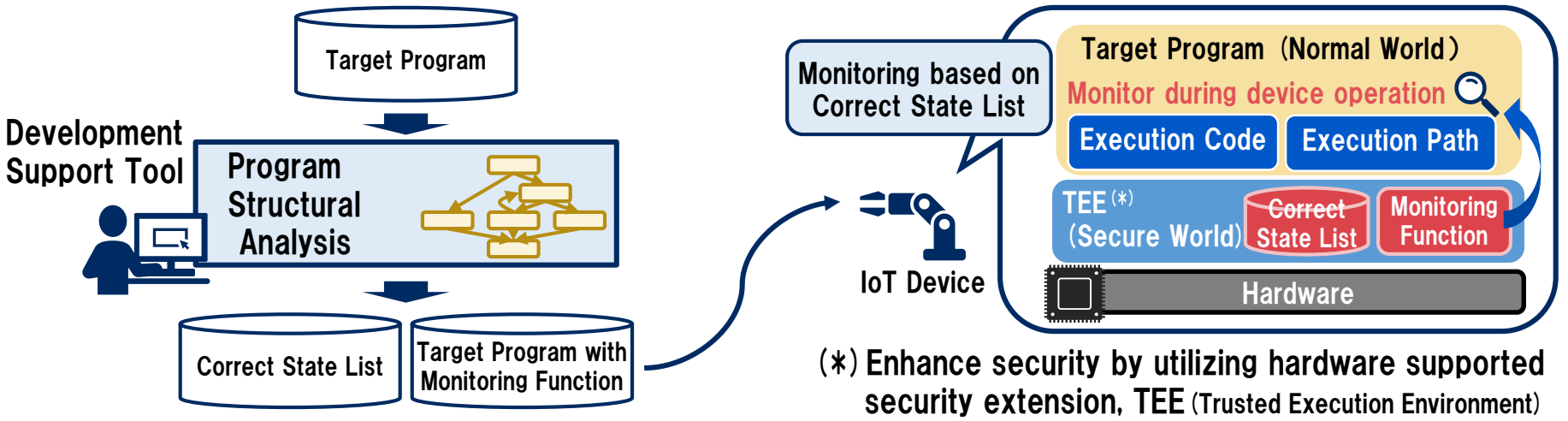
Focusing on program tampering, this R&D realizes the lightweight real-time monitoring technology on program authenticity and integrity for IoT devices.

Development Phase

Correct State List Generation
Analyze the target program, automatically determine the timings and ranges of verifying the authenticity and integrity, and generate "correct state list"

Operation Phase

Low-load Monitoring Function
Monitor the authenticity and integrity of the target program by verifying its execution codes and paths (control flows) on memory, "part by part"

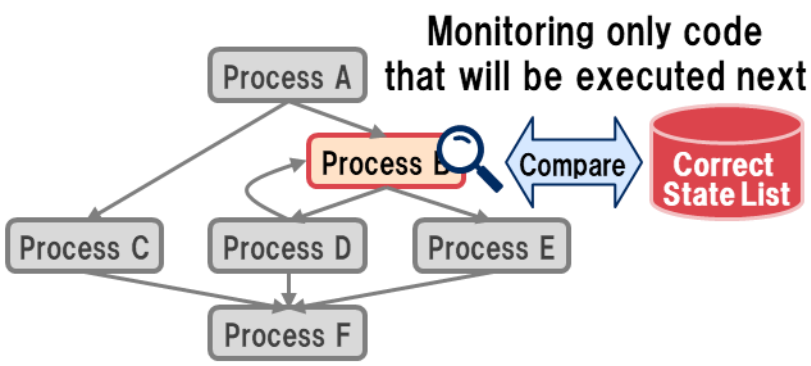


(*) Enhance security by utilizing hardware supported security extension, TEE (Trusted Execution Environment)

■ Monitoring Target

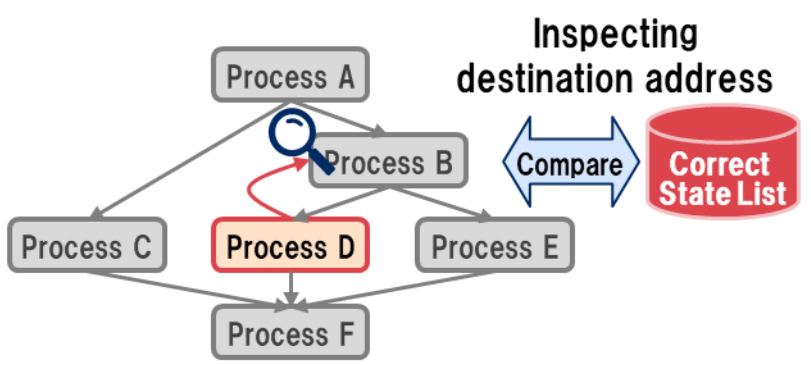
✓ Execution Code

- Monitor attacks that tamper with execution code in memory and incorporate malicious code
- Reduce the verification time by monitoring only the limited range based on execution path



✓ Execution Path (Control Flow)

- Monitor attacks that tamper with execution sequence and execute malicious code
- Reduce overhead by verifying only whether the destination is probable one or not



Contact

NEC Corporation
Email: nec-sip2-ac2@secl.jp.nec.com