자동차공학회 추계학술대회
사이버보안 세션

OS Hardening

2022.11.17

한국자동차공학회
The Korean Society of Automotive Engineers

FESCARO

목차

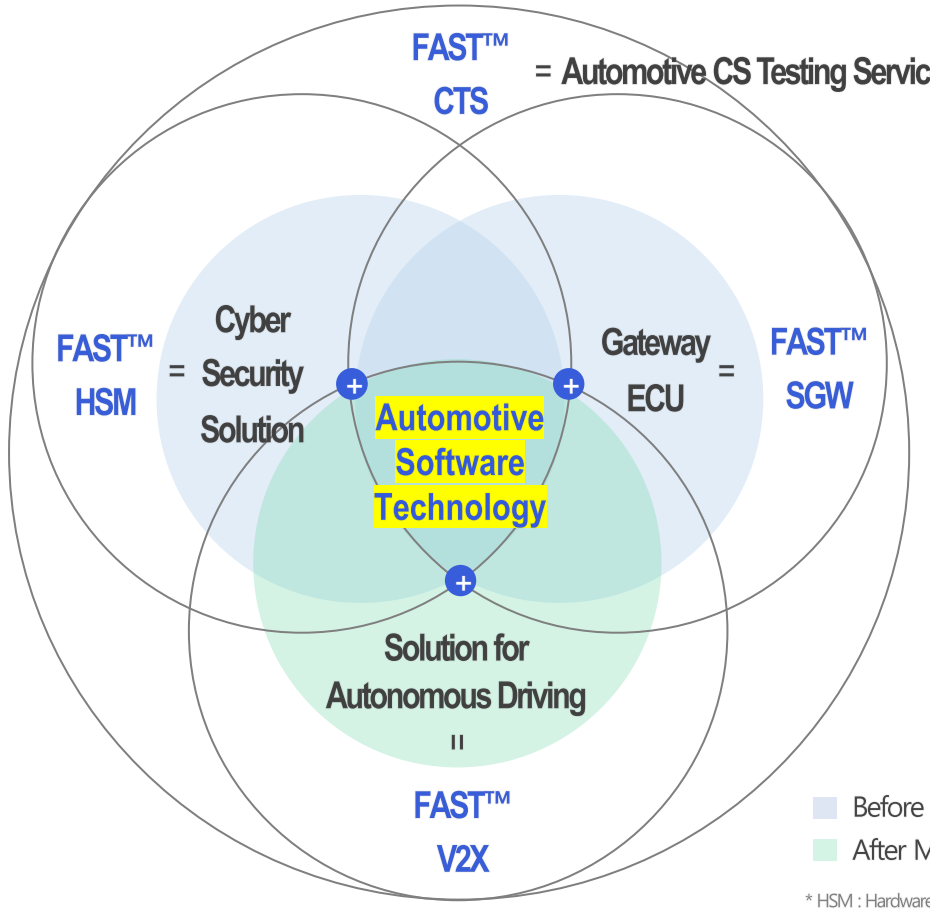
01 회사 소개

Who's FESCARO?

- Fescaro is Automotive total **software solution company**
- Conducted various SW solutions with **global OEMs and top tiers**
- Fully experienced with **Analysis, Design, Development, Maintenance and security solutions**
- Strong **talent management and education programs**
- **Fast decision** making and flexible **workload management** during development

Company	**FESCARO**	
Location	(Republic of Korea) Kyounggi-do Suwon-si	
Founder	Seok-Min Hong	CEO & co-founder
	Hyun-Jung Lee	CTO & co-founder
Employees	52 employees **(Engineers : Over 80%)**	
Customer	SSANGYONG MOTOR, HYUNDAI, KIA, STELLANTIS, RENAULT NISSAN MITSUBISHI, BYD, LUCID, Continental, HYUNDAI AutoEver, HYUNDAI MOBIS, Mando, HL Klemove, KANAVI AUTOMOTIVE, BorgWarner, SL Corporation, kyungshin, CHEMTRONICS, ESTRA, LG Electronics, SK telecom	

FESCARO Product Portfolio FAST™



* HSM : Hardware Security Module
* SGW : Security GateWay
* CTS : Cybersecurity Testing Service
* V2X : Vehicle to Everything

FESCARO Follows Automotive SW Mega Trend

Cyber Security Solution & Engineering

- 7 vehicles and over 150 ECUs are applying Fescaro cybersecurity solutions
- FESCARO has expertise in various ECU specifications and development

Classification	HSM (Standard type)	Virtual HSM (SW type)	Library (Library type)

Required Security level	• High
	  • Reprogrammable
	  • Related to Safety
	  • Has external interfaces
		• Medium
		  • Reprogrammable
		  • Related to Safety
			• Low
			  • Reprogrammable
			  • Not directly related to Safety

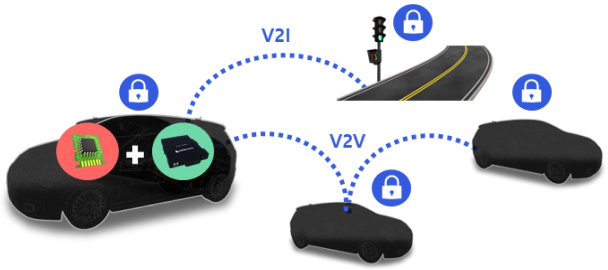
Semiconductor type (HSM)	• Standard with HSM • Sperate Security Core • Sperate Secure Storage	• Non-standard w/o HSM • Partial HW security module (Accelerator)	• Non-standard w/o HSM
Application implementation method	• Use the HW interfaces in the Semiconductor HSM	• Use the HW interfaces in the Semiconductor Host core • Use Fescaro SW Cryptographic module	• Use the HW interfaces in the Semiconductor Host core • Use Fescaro SW Cryptographic module
Available Secure Applications	• Secure Access • Secure Flash • Secure Boot • Runtime tuning protection • Secure Storage • Secure Debug • Memory protection	• Secure Access • Secure Flash • Secure Boot • Runtime tuning protection • Secure Storage • Secure Debug • Memory protection	• Secure Access • Secure Flash

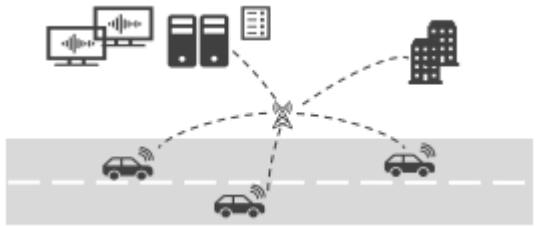
Secure Gateway

- High performance SGW is about to mass production for global OEM cybersecurity solutions
- Basic features and SW update management system is integrated
- One Chipset solution (MCU+AP)
- Well-known AutoSAR is implemented

V2X + IT Infra

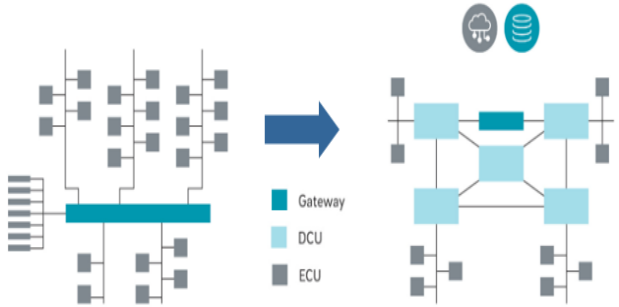
- OBU embedded SW V2X solution and Back-end server certificate management system
- Government project for misbehavior detection is implemented

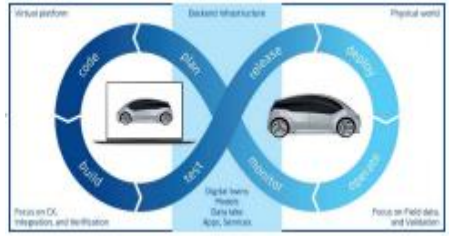




SDV

- Transformation to SDV technology with Fescaro SW solutions
- Developing future oriented SDV ECUs from distributed concept to centralized concept
- FESCARO DevOps platform will support for SDV





02 OS Hardening

2-1. OS Hardening 이란?

- 사전적 의미는 **"경화"** 이며, 보안관련 의미는 **"굳건하게 한다"** 라는 뜻으로 사용한다.
- 공격자가 사용 가능한 **"공격 방법(취약성의 표면)을 줄이는 것"** 이다.
- 한 번만 하면 되는 것이 아니라 **"기본적이고 착실한 대책을 거듭하는 것"** 이다.
- **"다층 방어 시스템 적용"**으로 위협에 대한 방어를 강화할 수 있다.
- 한국인터넷진흥원(KISA) **"주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드"** 표준을 사용한다.
  - <https://www.kisa.or.kr/2060204/form?postSeq=12&lang_type=KO&page=1>

2-2. OS Hardening 현황 – 멀티 미디어 시장

- Nagra : NASC (Nagra Advanced Security Concept)라는 이름으로 2012년부터 요구
- Cisco : LHCR (Linux Hardening Compliance Report)라는 이름으로 2013년부터 요구
- Conax : 2014년부터 SES(Security Environment Statement)과정에서 점검
- Irdeto : Linux Hardening Guide 로 2015년 부터 요구
- Verimatrix : Security Compliance and Robustness Rules에서 2013년부터 요구
- Viaccess : Cyber Security Requirement에 2017년에 추가되어 요구
- Playready : 2014년부터 Robustness Requirements 에 비슷한 요구사항 추가
- Netflix : 2013년부터 Netflix Security Verified (NSV) Security Specification에서 의해 요구
- MovieLabs : 2014년부터 Enhanced Content Protection에서 Hardware TEE로 요구
- Sony Pictures for 4K : 2014년부터 4K(UHD) Set top box제품에 요구

2-3. OS Hardening 적용 순서

- **불필요한 프로그램/서비스 비활성화 또는 제거**
  - 서비스 관리
    - 단일 기능 시스템은 다목적 시스템보다 안전하다. (공격 접점 최소화)
    - Windows OS의 경우 90개 이상의 서비스를 기본으로 제공한다.
    - 불필요한 서비스 (finger, cron, NFS, DHCP, FTP 등) 비활성화

- **취약점이 개선된 패치의 신속한 적용**
  - 작동 프로그램 및 OS는 수시로 최신 버전으로 업데이트 한다.
  - CVE(Common Vulnerabilities and Exposures) 웹사이트 등을 통한 사용 프로그램의 주기적인 취약점 확인 및 수정 패치 적용

- **불필요한 사용자 이름 또는 로그인 제거**
  - 계정 관리
    - UID/GID 점검 및 불필요한 계정 삭제, root 계정 접속 제한 및 관리자 그룹 최소화, 패스워드 관리 정책 수립 등

- **파일 및 디렉토리 관리**

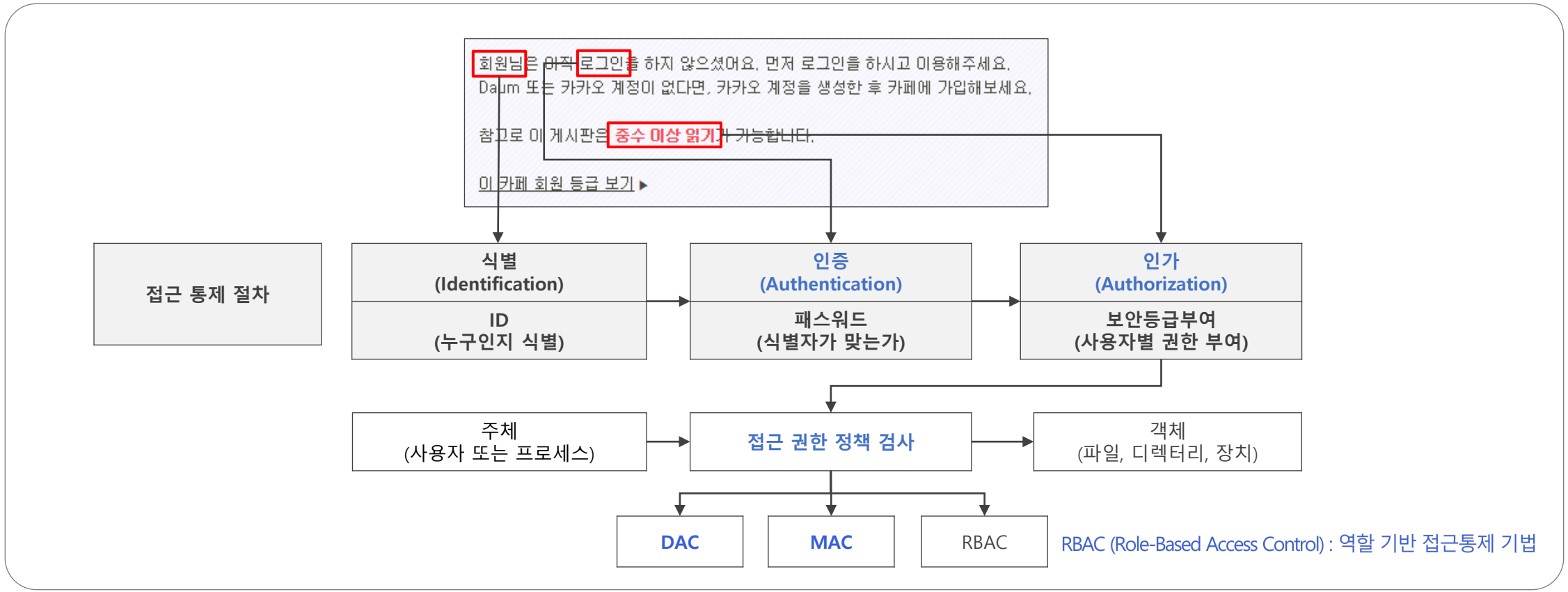
- **네트워크 관리**
  - 불필요한 IP forward, ping 응답, proxy 서버 비활성화 등

- **로그 관리**
  - 로그의 정기적 검토 및 보고 관리 정책 수립, 시스템 로그 생성 및 권한 점검, 로그 원격전송 기능 비활성화 등

- **보안 기능 관리**

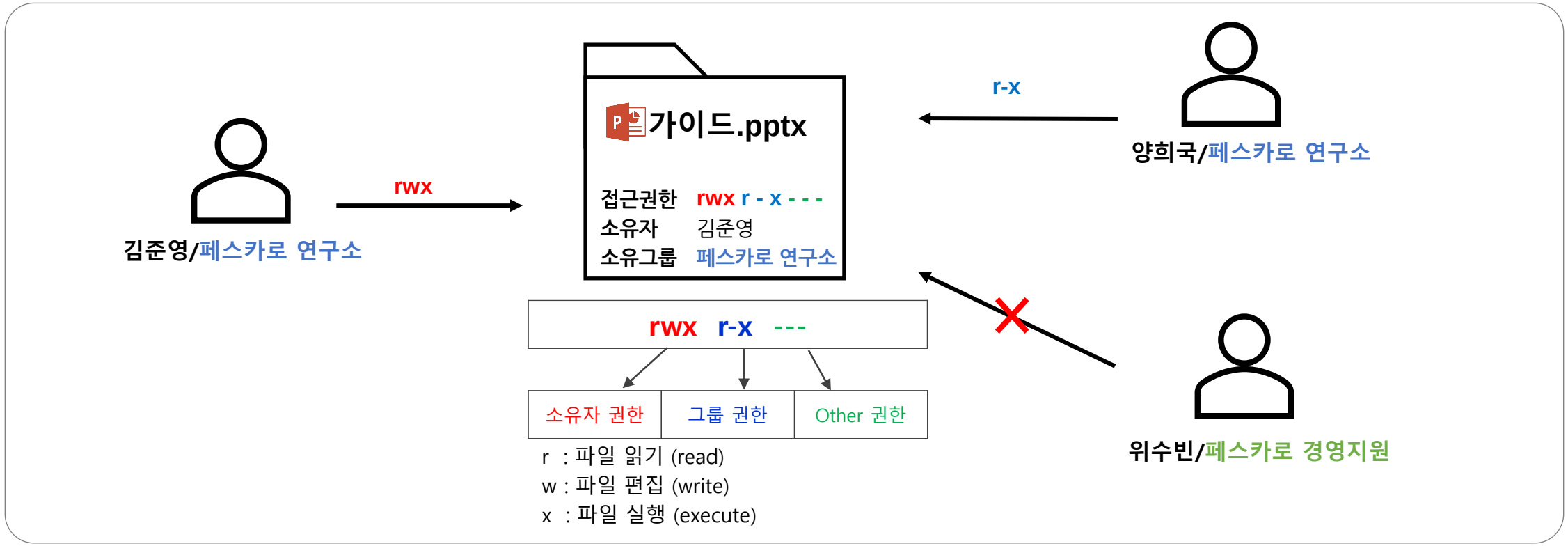
2-4. 접근 통제 (Access Control) 개념

- 파일 및 디렉토리, 네트워크 소켓같은 **"시스템자원(객체)을 적절한 권한을 가진 사용자나 그룹(주체)이 접근하고 사용할 수 있게 통제"**하는 것을 의미
  - **"인증(Authentication)"**은 **"사용자(주체) 가 누구인지 판별"**하는 것, 로그인 또는 회원가입을 통해 사용자가 누구인지를 판별하는 과정.
  - **"인가(Authorization)"**는 어떤 사용자가 어떤 **행위를 수행할 "권한(Permission)을 가지고 있는지를 판별"**하는 것, 다음 카페 같은 곳의 회원 등급에 따라 접근할 수 있는 게시판(객체) 같은 접근 대상을 말한다.



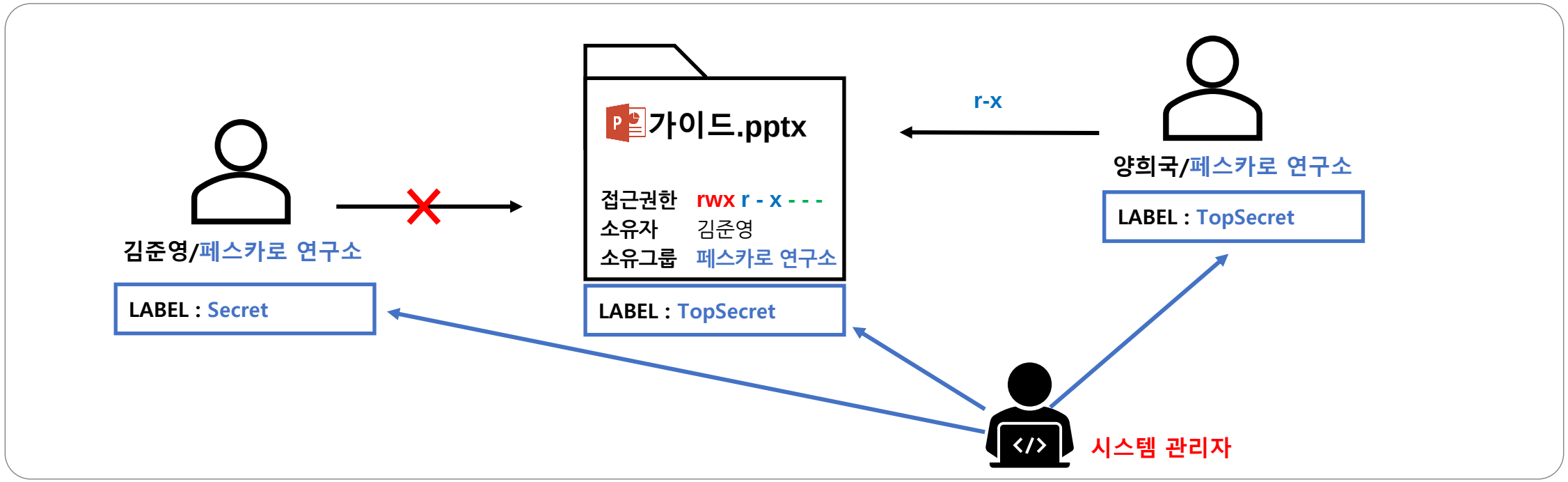
2-5. DAC 개념

- DAC (Discretionary Access Control) 임의 접근 제어
  - 객체에 대한 접근을 **"사용자나 그룹의 신분을 기준으로 제한"**하는 방식
  - **"임의적(Discretionary)"**이란 **"객체 소유자의 판단에 의해 권한을 줄 수 있다는 것을 의미"** 함
  - **구현이 용이**하고 **사용이 간단**하다.
  - 강제적 접근 제어**(MAC)에 비해 상대적으로 "보안성이 취약",** 시스템 차원의 일관성 있는 접근 제어가 어렵다
  - 접근 제어를 신분에 의존하다 보니 다른 주체의 신분을 도용한 경우 중대한 결함이 발생할 수 있다. **root 슈퍼 계정이 탈취되면 DAC의 접근 권한 설정이 무용지물**



2-6. MAC 개념

- MAC (Mandatory Access Control) 강제 접근 제어
  - **미리 정해진 정책과 보안 등급에 의거하여** 주체(Subject)에게 허용된 접근 권한과 객체(Object)에 부여된 허용 등급을 비교하여 **접근을 제어하는 방법**
  - 다음 카페의 **회원**(주체)마다 부여된 **등급에 따라 게시판**(객체)에 접근할 수 있는 권한 등급을 직접 비교하여 **접근 허용 여부를 결정하는 방법**
  - 파일의 소유자가 아닌 **"시스템 관리자"** 가 접근 권한 수준을 제어
  - MAC 권한 체크 순서는 **DAC 체크 후 MAC 체크하는 방식**으로, **DAC 설정 오류의 2차 피해를 방지할 수 있음(다층방어)**
  - 자원의 소유자라고 할 지라도 정책에 어긋나면 객체에 접근할 수 없으므로 **강력한 보안을 제공**합니다.
  - **구현 및 권한 설정이 복잡**하고 어려우며, 시스템 관리자가 접근 통제 모델에 대해 잘 이해하고 있어야한다.
  - Linux에서는 **LSM(Linux Security Modules) 기반의 SMACK, SELinux,** AppArmor, TOMOYO 등과 같은 다양한 **MAC 모듈 방식을 지원** 함

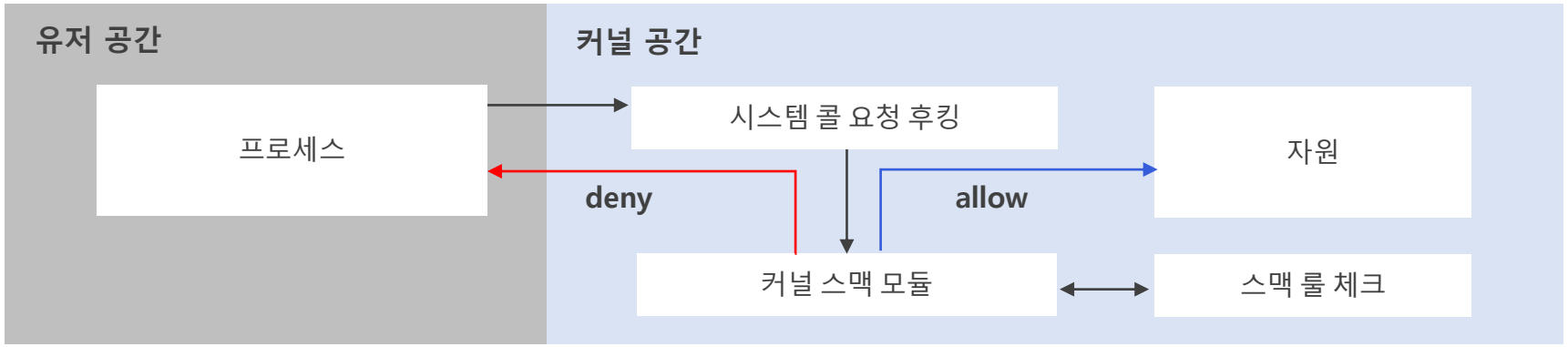


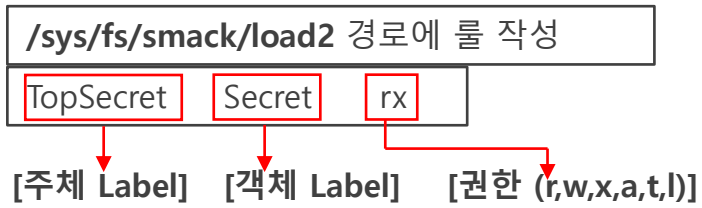
2-7. DAC vs MAC의 차이점

항목	MAC	DAC
정의	**주체와 객체의 등급을 비교**하여 접근 권한 부여	접근하려는 **주체의 신분**에 따라 접근 권한 부여
권한부여	**시스템 관리자**	**소유자**
접근결정	라벨	신분
정책	고정적	유연함
장점	중앙집중적	구현 용이
단점	구현 및 운영이 어려움	아이디 도용에 취약

2-8. MAC - SMACK

- SMACK (Simplified Mandatory Access Control Kernel)
  - **주체와 객체 각각 Label을 정의하고 Label간**의 세분화된 **권한을 지정**하여 강제적 접근 통제(MAC) 보안 기능을 제공하는 리눅스 보안 모듈
  - Linux kernel 2.6.25 부터 SMACK 사용 가능 함 (TIP : systemd 를 사용하는 경우 최소 2.18 이상 - SMACK 프로세스 라벨 설정 - 권장 2.29이상)
  - **정책을 컴파일 하지 않아 간단**하게 사용할 수 있음



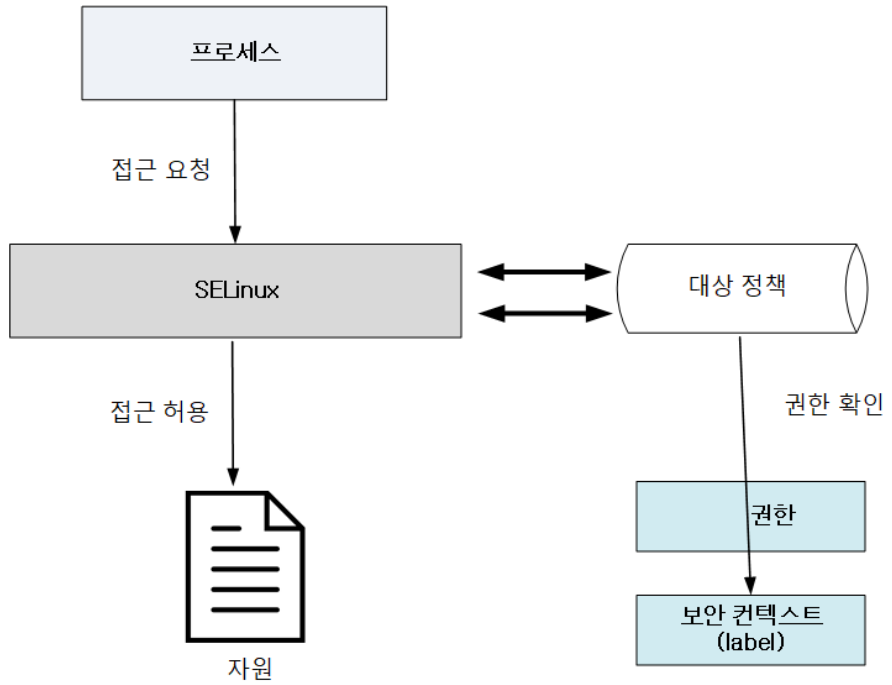


주체에서 객체로 접근할 때의 권한을 의미
- 즉, TopSecret 라벨을 가진 주체는 Secret 라벨을 가진 객체의 read 와 execute 권한이 있음을 의미

권한	설명
Read(r)	읽기 권한
Write(w)	쓰기 권한
Execute(x)	실행 권한
Append(a)	추가 액세스 권한 부여
Transmute(t)	프로세스가 파일 생성시 상위 폴더의 Label로 상속
Lock(l)	다른 프로세스가 액세스할 수 없도록 파일 잠금

2-9. MAC - SELinux

- SELinux (Security Enhanced Linux)
  - 모든 **주체와 객체에** 접근 권한을 확인하기 위한 **보안 컨텍스트(Security Context)**, 또는 보안 레이블(Security Label) **정보를 부여하여 접근 권한**을 관리
  - SELinux 는 미국 국가안보국(NSA - National Security Agency)이 개발한 Flask 라는 보안 커널을 리눅스에 이식한 커널 레벨의 보안 모듈
  - SELinux는 RHEL(Red Hat Enterprise Linux) 버전 4 이상과 Android kitkat 4.4 이상 부터 SELinux 사용 가능 함
  - Android **정책 파일** (system/sepolicy) 은 file_contexts 파일의 콘텐츠를 연결하여 file_contexts.bin 으로 **빌드하여 사용**된다.



<보안 컨텍스트>

요소	설명
SELinux user	SELinux 사용자
Role	타입과 연결되어 사용자의 접근을 허용 결정
Type	프로세스의 도메인이나 파일의 타입을 지정하고 이를 기반으로 접근 통제를 수행
Level	강제 접근 통제보다 더 강력한 보안이 필요할 때 사용

system_u : object_r : **httpd_exec_t** : s0 /usr/sbin/httpd

LABEL	PID	TTY	TIME	CMD
unconfined_u : system_r : **httpd_t** : s0	30374	?	00:00:00	httpd

system_u : object_r : **httpd_sys_content_t** : s0 /var/www/html/

<대상 정책>

allow **httpd_t httpd_sys_content_t** : file { ioctl read getattr lock open };

감사합니다.