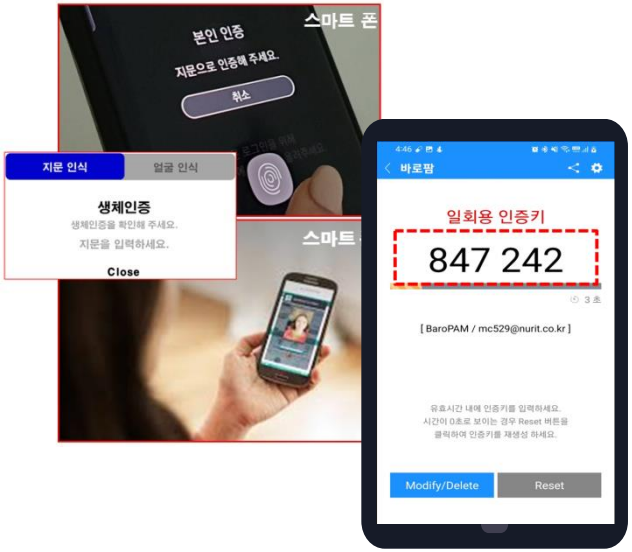
nurit

정보자산의 보안강화를 위하여 다계층 인증을 위한

개방형 OS와 BaroPAM 솔루션 연동

2025. 5.



Content

nurit

Ⅰ. 배경 및 변화

1. 시작 전에

"**기본 보안부터 철저히 해야**"

현재의 보안체계로는 정보자산을 충분히 지킬 수 없다는 거, 보안 전문가라면 다 알고 있습니다.

주요 인프라 공격의 85%가 "**패치, 2차 인증(추가 인증), 최소 권한 원칙**" 등 기본적인 수준의 보안을 지키지 않아서 발생한 것으로 나타납니다.

랜섬웨어를 포함한 **침해 사고의 80~90%가 원격 접속과 관련된 문제**입니다.

보안 솔루션 중 도입해야 할 1순위가 **우회 및 원격접속을 차단할 수 있는 2차 인증 솔루션**입니다.

기본 보안 정책만 지켜도 대부분의 공격은 막을 수 있습니다.

또한, "**망분리**"는 새로울 것도, 특별할 것도 없는 보안 전략이자 개념입니다.

"**망분리**" 했다고 해커들의 침투를 100% 막을 수 없다는 걸 인정해야만 하는 때가 도래했습니다. 이 시대에는 피해를 줄이는 게 보안의 가장 큰 임무였습니다.

이게 어디까지 갔냐면, "**사이버 공격자들이 이미 네트워크에 들어와 있는 걸 상정하고 보안 전략을 마련해야 한다**"가 보안의 명제가 되었습니다.

외부의 해커 또는 내부 사용자가 불법적으로 정보자산에 접근하는 상황을 제한하고, 보안의 위험을 분산함으로써 피해를 최소화해야 합니다.

최근 들어, 중앙 집중식 관리 서버의 운영체제(OS) 및 관리자 계정이 해킹되어, 관리 서버를 장악하고 정보를 유출하여 도용 및 악용하거나, 악성코드 삽입, 정보를 삭제한 후 관리 서버를 무력화시켜 서비스를 불능 상태로 만드는 "**단일 지점 공격**"의 침해사고가 발생하여 기업에 많은 피해를 주고 있습니다.

2. 보안 모델의 변화

AS-IS(경계보안 모델)

-전통적인 네트워크 경계 기반 보안모델로 충분하지 않음
-공격자가 경계를 침해한 후 내부에서 이동하는 것에 대한 한계성 내포

TO-BE(제로 트러스트 모델)

-사용자의 위치, 네트워크 등에 관계없이 모든 요청을 신뢰하지 않음
-내 · 외부 구별 없이 신뢰하지 않음 (검증요구)
-최소 권한과 지속적 검증

내부 침투시 위협 내부 전파 가능

내부 침투시에도 위협 내부 전파 불가능

"아무 것도 신뢰하지 않는다" = "아무도 믿지 마라" = "계속 검증하라"

nurit

2. 보안 모델의 변화(계속)

보안 모델의 변화로 기존 보안 솔루션으로는 이젠 막을 수 없습니다. 보안 솔루션의 변화가 필요한 시점입니다.

▶경계보안에서 제로 트러스트 보안으로 보안모델의 변화.

▶공격 표면으로 보안 취약점을 약용한 공격.

▶보안 위험의 최소화하기 위한 위험 분산 필요.

▶중앙집중식에서 벗어나 탈중앙화 필요.

▶단일지점 공격으로 보안 솔루션의 무력화 차단 필요.

3. 침해 사고가 발생한 기업의 특징

주요 인프라 공격의 85%가 패치, 2차 인증(추가 인증), 최소 권한 원칙 등 기본적인 수준의 보안을 지키지 않아서 발생한 것으로 나타납니다. 기본 보안 정책만 지켜도 대부분의 공격은 막을 수 있습니다.

▶OS 최신패치 및 업데이트 하지 않음.

▶2차 인증(추가 인증)을 사용하지 않음.

▶기본 포트를 그대로 사용함.
예) SSH/SFTP:22, VPN: 4433, RDP: 3389, SMB: 139, 445 등

▶불필요한 서비스를 비활성화 하지 않음.

▶정기적인 보안 감사를 하지 않음.

▶직원들의 보안에 대한 인식 결여(보안 교육 미비).

사이버 보안은 현대 기업의 IT 환경에서 복잡하고 중요한 문제입니다.

최근 해커들은 중앙 집중식 시스템에 침투(단일 지점 공격)하여 시스템을 장악, 정보를 유출하여 도용 및 악용하거나, 악성코드 삽입, 정보를 삭제한 후 시스템을 무력화시켜 서비스를 불능 상태로 만듭니다.

이젠 중앙 집중식에서 벗어나 탈중앙화 방식으로 보안의 위험은 분산 시키는 것이 기본 입니다.

4. 2차 인증이란?

2차 인증은 정보자산의 보안 강화를 위하여 로그인-ID 및 비밀번호(지식기반 인증) 이외에 별도의 추가인증(소유기반/속성기반/행위기반/장소기반 인증)절차를 의미하며, 2 Factor 인증과 2 Channel 인증으로 구분합니다.

2 Factor 인증

2 Factor 인증의 개념도

"지식기반 인증"인 로그인-ID/비밀번호 인증에 다른 요소 즉 소유기반 인증 및 생체인증 요소를 추가한 인증 기법으로 서비스 채널과 인증 채널이 하나로 결합된 형태.

- -다양하고 광범위한 적용, 관리가 단순하고 운영비용 절감.
- -통신망을 사용하지 않기 때문에 보안지역이나 통신장애에 영향을 받지 않아 서비스 보장.
- -모듈인증 방식은 사용자 정보 동기화가 필요 없으며, 통신 및 인증서버 미사용으로 서비스 보장.
- -인증폭주 시 부하분산으로 인증속도 보장.

2 Channel 인증

2 Channel 인증의 개념

2 Factor 인증을 포함한다고 보는 것이 일반적이며, 인증과 서비스를 수행하는 통신망을 서비스 채널과 인증채널로 물리적으로 분리한 형태.

- -구현복잡, 제한적 적용, 관리가 복잡하고 운영비용 증가
- -통신망을 사용하기 때문에 보안지역이나 통신장애에 영향을 받아서 서비스 중단.
- -인증서버 방식으로 사용자 정보 동기화가 필요하며, 인증서버 장애 시 서비스 중단 및 인증 폭주 시 인증속도 저하.
- -우회기술 및 피로공격으로 사이버 범죄에 악용 (삼성전자, MS, 우버, 레딧 등)

※ 다중 인증(MFA)은 최소 두 가지 이상의 본인인증 요소를 이용하여 본인 여부를 인증하는 것으로 2차 인증은 다중 인증의 일종.

5. 2차 인증 적용 순서

주요 인프라 공격의 85%가 패치, 2차 인증(추가 인증), 최소 권한 원칙 등 기본적인 수준의 보안을 지키지 않아서 발생한 것으로 나타납니다. 기본 보안 정책만 지켜도 대부분의 공격은 막을 수 있습니다.

1. 운영체제(OS)

최우선적으로 Windows, Windows server, Linux, Unix, MacOS 등의 다양한 운영체제(OS)와 VPN이다.

해커들은 2차 인증이 적용되어 있지 않은 OS의 원격접속에 주로 사용되는 RDP나 SSH 등을 이용하여 서버에 침투하여 서버를 장악한 후 불능 상태로 만든다.

또한, VPN은 사용자와 전체 네트워크로 접근 권한을 부여하기 때문에 내부 시스템에 보안 경계를 설정하기 어려워 해커들의 집중 공략 대상이다.

2. 관리자 계정이나 관리 콘솔

다양한 애플리케이션, WAS, 가상화, 클라우드 등의 관리자 계정이나 관리 콘솔에 대한 2차 인증 설정이다.

계정 정보를 유출하여 도용 및 악용하거나, 관리콘솔에 악성코드 삽입 또는 계정정보 또는 VM을 삭제한 후 시스템을 무력화시켜 서비스를 불능 상태로 만든다. 이는 기업에 커다란 피해를 준다.

3. 일반 사용자 계정

회사 내에서 업무를 위해 사용하는 애플리케이션(ERP, 포탈, 그룹웨어, 웹메일), 가상화, 클라우드 등의 일반 사용자 계정에 대한 2차 인증 설정이다.

특히, 외부에서 접속할 수 있는 시스템에 2차 인증을 설정해 보안을 강화할 수 있도록 해야 한다.

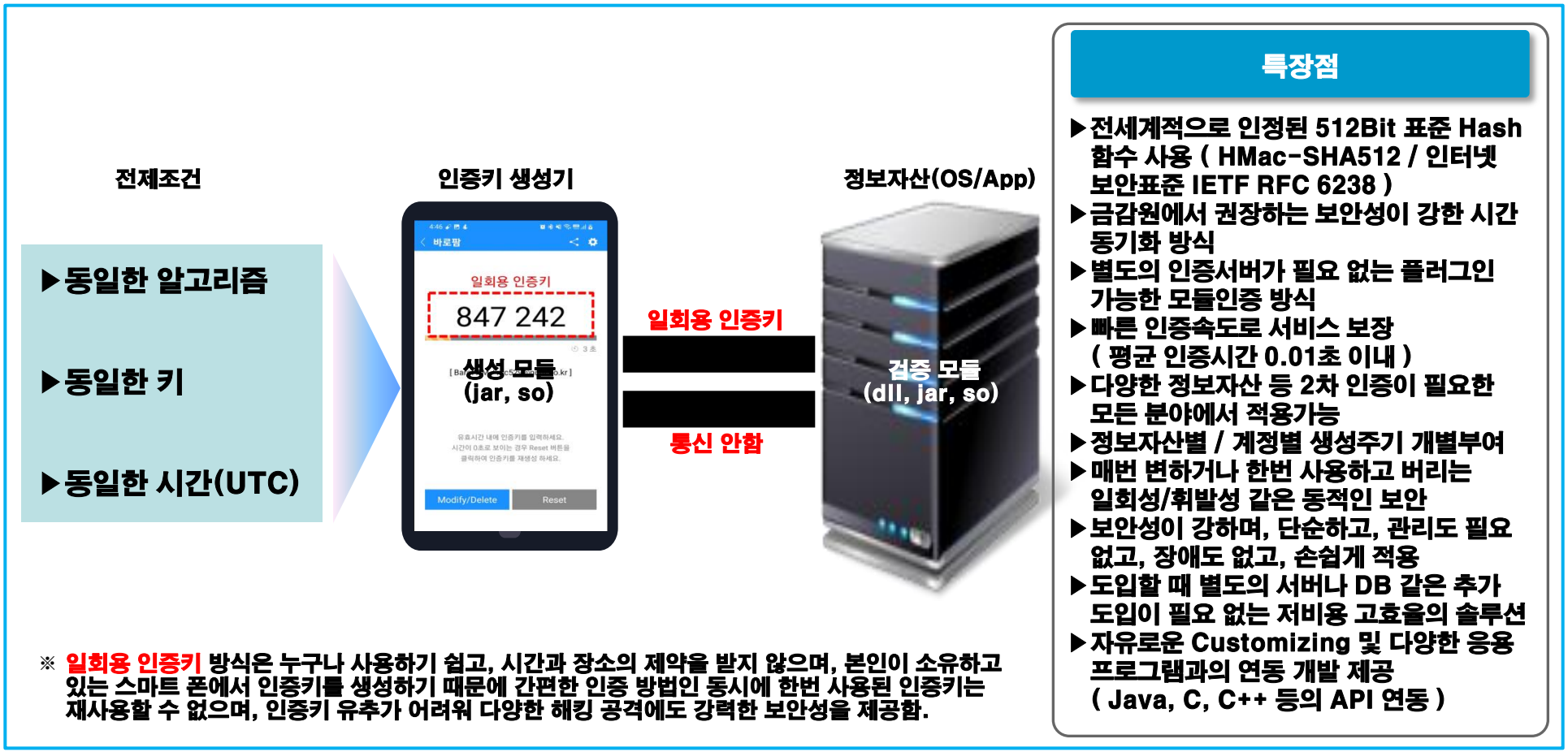
1. 기본 전제

보안성이 강하며, 단순하고, 관리도 필요 없고, 장애도 없고, 누구나 손쉽게 곧바로 적용하여 사용할 수 있고, 솔루션을 도입할 때 별도의 서버나 DB 같은 추가 도입이 필요 없는 저비용 고효율의 솔루션은 없을까?

왜, 이런게 필요하지?

2. 일회용 인증키란?

일회용 인증키(OTA, One-Time Authentication)는 **제로트러스트 보안 모델**로 별도의 인증서버가 필요 없는 모듈 인증 방식으로 단방향 암호 기반의 해시 알고리즘에 따라 매 생성주기마다 변경되는 추정 할 수 없는 인증 키를 생성하여 이용하는 보안 시스템으로 아이디어 자체는 100년도 넘은, 그리고 그만큼 검증된 기술입니다.



특장점

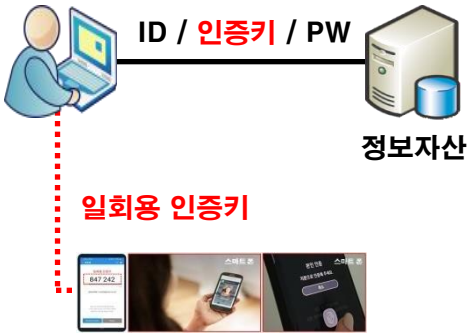
- ▶전세계적으로 인정된 512Bit 표준 Hash 함수 사용 (HMac-SHA512 / 인터넷 보안표준 IETF RFC 6238)
- ▶금감원에서 권장하는 보안성이 강한 시간 동기화 방식
- ▶별도의 인증서버가 필요 없는 플러그인 가능한 모듈인증 방식
- ▶빠른 인증속도로 서비스 보장 (평균 인증시간 0.01초 이내)
- ▶다양한 정보자산 등 2차 인증이 필요한 모든 분야에서 적용가능
- ▶정보자산별 / 계정별 생성주기 개별부여
- ▶매번 변하거나 한번 사용하고 버리는 일회성/휘발성 같은 동적인 보안
- ▶보안성이 강하며, 단순하고, 관리도 필요 없고, 장애도 없고, 손쉽게 적용
- ▶도입할 때 별도의 서버나 DB 같은 추가 도입이 필요 없는 저비용 고효율의 솔루션
- ▶자유로운 Customizing 및 다양한 응용 프로그램과의 연동 개발 제공 (Java, C, C++ 등의 API 연동)

※ **일회용 인증키** 방식은 누구나 사용하기 쉽고, 시간과 장소의 제약을 받지 않으며, 본인이 소유하고 있는 스마트 폰에서 인증키를 생성하기 때문에 간편한 인증 방법인 동시에 한번 사용된 인증키는 재사용할 수 없으며, 인증키 유추가 어려워 다양한 해킹 공격에도 강력한 보안성을 제공함.

3. BaroPAM 이란?

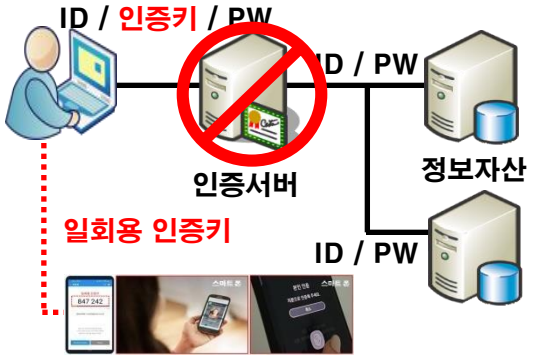
BaroPAM 솔루션은 제로 트러스트 보안 모델로 정보자산의 보안 강화를 위하여 2차 인증(추가 인증)이 필요한 다양한 운영체제와 애플리케이션에 누구나 손쉽게 곧바로 적용할 수 있는 플러그인 가능한 인증 모듈(PAM, Pluggable Authentication Module) 방식을 기반으로 하는 보안에 최적화된 다계층 인증 체계를 지원하는 솔루션입니다.

정보자산 접근 보안강화



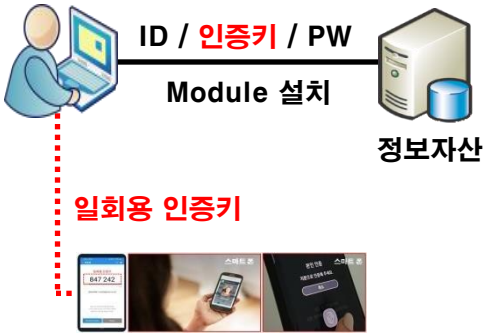
- 외부의 해커 또는 내부 사용자가 불법적으로 정보자산에 접근하는 상황을 제한하여 정보자산의 보안 강화
- 2-Factor 인증으로 기존의 "지식기반 인증"인 ID / PW 인증에 다른 요소인 소유기반/속성기반 인증요소를 추가한 인증기법

서비스의 용이성



- 2차 인증을 별도 인증키 토큰/카드 필요 없이 BaroPAM 앱을 이용하여 인증이 용이함
- 별도 인증서버나 Windows/서버 접근 제어를 관리하는 서버가 필요 없는 구조로 관리/운영비용 절감

손쉬운 적용



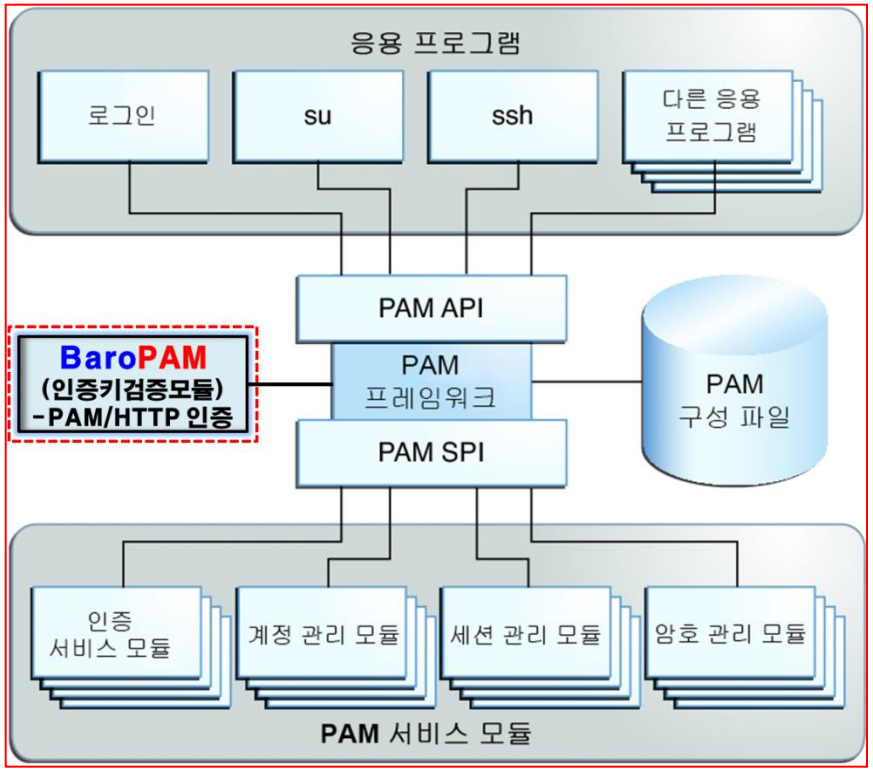
- 각 Windows 또는 서버에 모듈을 설치하는 구조로 간단히 적용 가능
- Windows 또는 서버를 재기동하지 않기 때문에 운영 중에도 적용 가능
- 기존 네트워크 장비의 설정변경 불필요

nurit

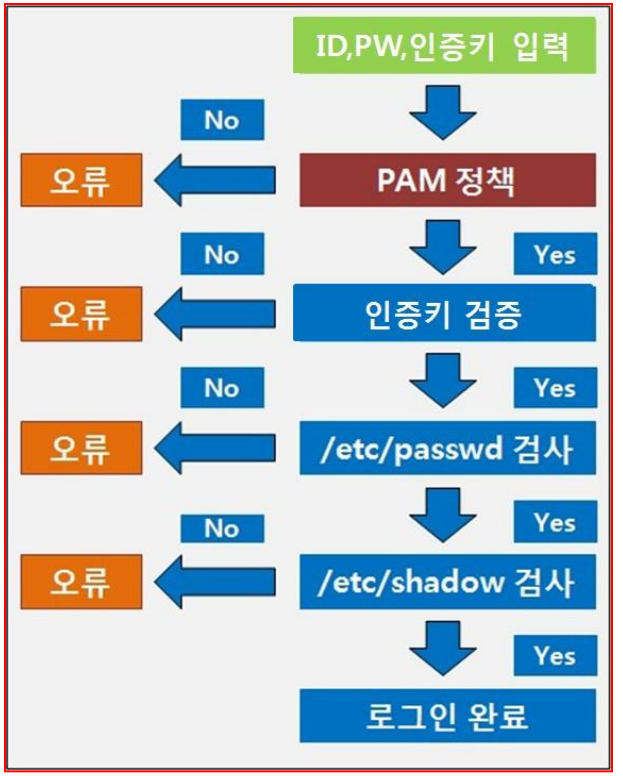
4. 아키텍처와 인증절차

BaroPAM 솔루션은 기본적으로 운영체제의 PAM(Pluggable Authentication Modules)과 정보자산의 다중인증 솔루션이 결합하여 기존의 "지식기반 인증"인 ID/Password 인증에 일회용 인증키와 같은 소유기반의 인증 요소를 사용해 보안이 한층 강화된 모듈인증 방식으로 아키텍처와 인증절차는 다음과 같습니다.

BaroPAM 아키텍처



BaroPAM 인증절차



nurit

5. 솔루션 특장점

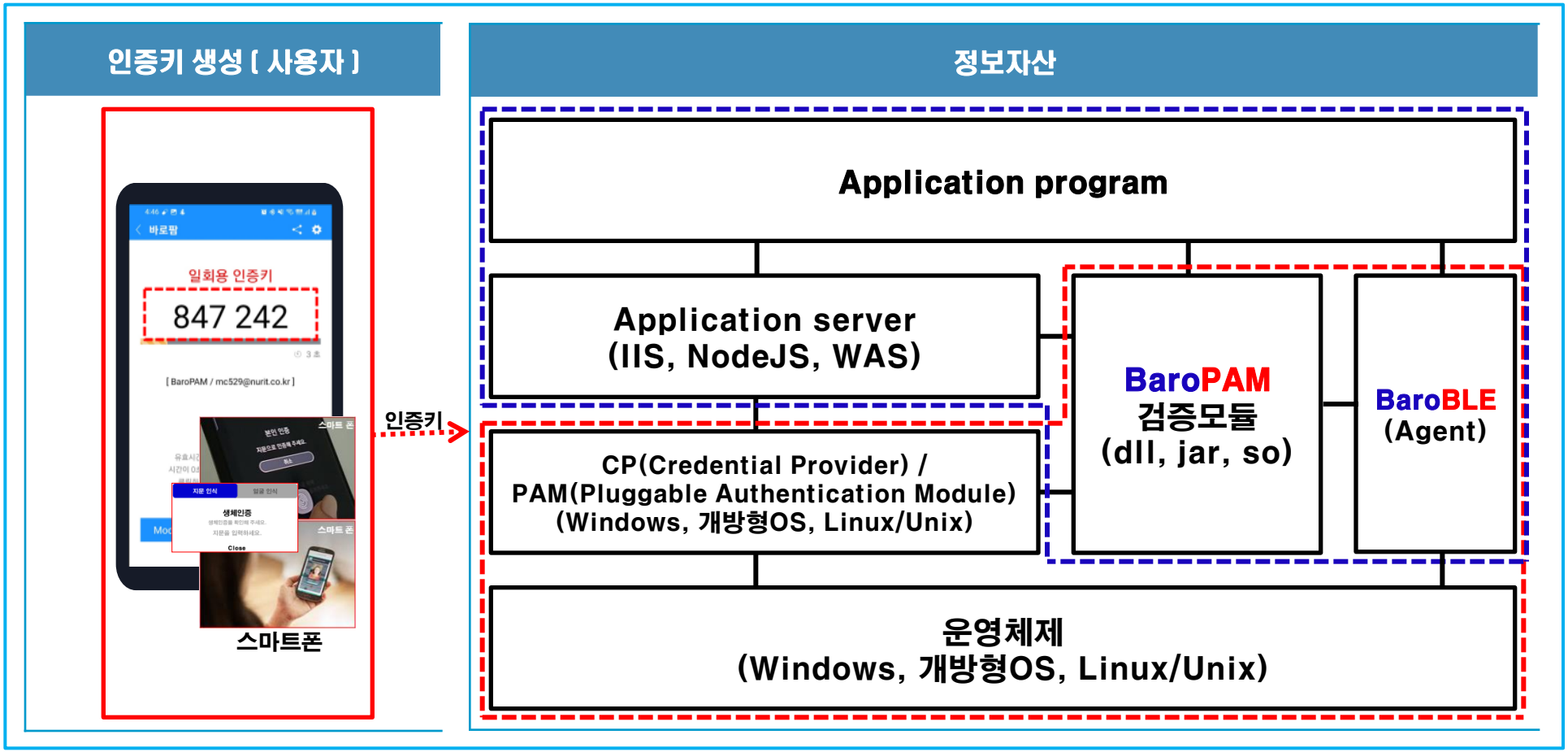
BaroPAM 솔루션은 별도의 인증서버가 필요 없는 모듈인증 방식으로 중앙 집중식에서 벗어나 탈중앙화 방식의 다계층 인증 체계를 지원하며, 보안성이 강하고, 단순하고, 관리도 필요 없고, 장애도 없고, 누구나 손쉽게 곧바로 적용하여 사용할 수 있고, 솔루션을 도입할 때 별도의 서버나 DB 같은 추가 도입이 필요 없는 저비용 고효율의 솔루션입니다.

- ▶별도의 인증서버가 필요 없는 모듈인증 방식의 다계층 인증 지원
- ▶빠른 인증속도로 서비스 보장 (평균 인증시간 0.01초 이내)
- ▶BaroPAM 앱 소스 난독화 및 화면 캡쳐 방지 기능 제공
- ▶BaroPAM 앱 실행 시 생체인증(지문인식,얼굴인식) 기능 제공
- ▶전세계적으로 인정된 512Bit 표준 Hash 함수 사용 (HMac-SHA512 / 인터넷 보안표준 IETF RFC 6238)
- ▶금감원에서 권장하는 Time-Sync, 동적 Secret key 방식 지원
- ▶환경 설정 정보를 파일 이외에 MariaDB와 연동 기능 제공
- ▶인증의 제한 횟수 및 제한 시간(예: 30초에 3회) 설정 기능 제공
- ▶중간자(man-in-the-middle) 공격을 예방하는 기능 제공
- ▶빈번하게 발생하는 통신 장애 또는 보안 지역에서도 인증 가능
- ▶매번 변하거나 한번 사용하고 버리는 일회성/휘발성 같은 동적인 보안 지원
- ▶인증절차 시 인증정보가 위변조 되더라도 우회인증 불가능
- ▶인증 우회(우회기술, 피로공격 등) 불가능
- ▶간단(느슨)한 구성에서 시작해 더 복잡(견고)한 보안 시스템으로 진화 가능
- ▶iOS는 자체적으로 본인인증 할 수 있는 기능 제공
- ▶자동 로그인 기능을 악용한 계정 정보 탈취해도 로그인 불가능
- ▶스마트 폰 이용 불가 시 응급 일회용 인증키 제공
- ▶다양한 정보자산 등 2차 인증이 필요한 모든 분야에서 적용가능 (정보자산의 RADIUS 인증 중 PAM/SQL/HTTP 인증도 지원)
- ▶2차 인증에서 허용 / 제외할 수 있는 계정에 대한 ACL 기능 제공
- ▶자유로운 Customizing 및 다양한 응용 프로그램과의 연동 개발 제공 (Java, C, C++ 등의 API 연동)

※ HMac (Hash-based Message Authentication Code) : 해쉬 기반 메시지 인증 코드
HMac는 Key를 조합하여 Hash 함수를 구하는 방식으로, 송신자와 수신자만이 공유하고 있는 Key와 메시지를 혼합하여 Hash 값을 만드는 방식이다. 또한 채널을 통해 보낸 메시지가 훼손되었는지 여부를 확인하는데 사용할 수 있으며, Mac 특성상 역산이 불가능하므로, 수신된 메시지 와 Hash 값을 다시 계산하여, 계산된 HMac과 전송된 HMac이 일치하는지를 확인하는 방식이다.

6. 솔루션 구성

BaroPAM 솔루션은 사용자가 일회용 인증키를 생성하는 장치, 일회용 인증키를 적용하는 정보자산, 일회용 인증키를 검증하는 모듈, BaroPAM 앱과 데스크탑의 블루투스/애플리케이션간 통신하는 BaroBLE로 구성되어 있습니다.



nurit

7. 보안 강화

악성코드를 탐지 및 제거하는 백신 솔루션/사용자에 대한 철저한 통제와 감독하는 서버접근통제 솔루션과 정보자산의 다계층 인증 체계를 통한 계정도용, 권한상승, 불법적인 우회/원격 접속, 중간자 공격 등을 차단하는 BaroPAM 솔루션이 결합하여 정보자산의 보안을 강화하는 시너지 효과를 낼 수 있습니다.

정보자산 보안 =

- Windows NT Server
- Mac OS
- Linux / Unix Server
- Application
- Database
- Network, IoT Device
- 저장장치

악성코드 탐지/제거 (백신)

V3

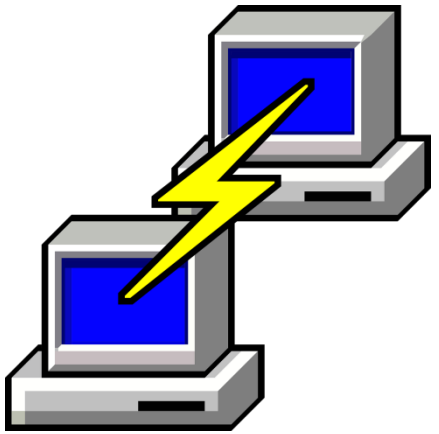
관리 서버 보안 취약

서버접근통제솔루션

- ▶접근 권한 통제
- ▶시스템 명령어 통제
- ▶실시간 세션 통제
- ▶작업 로그 기록/ 감사

+

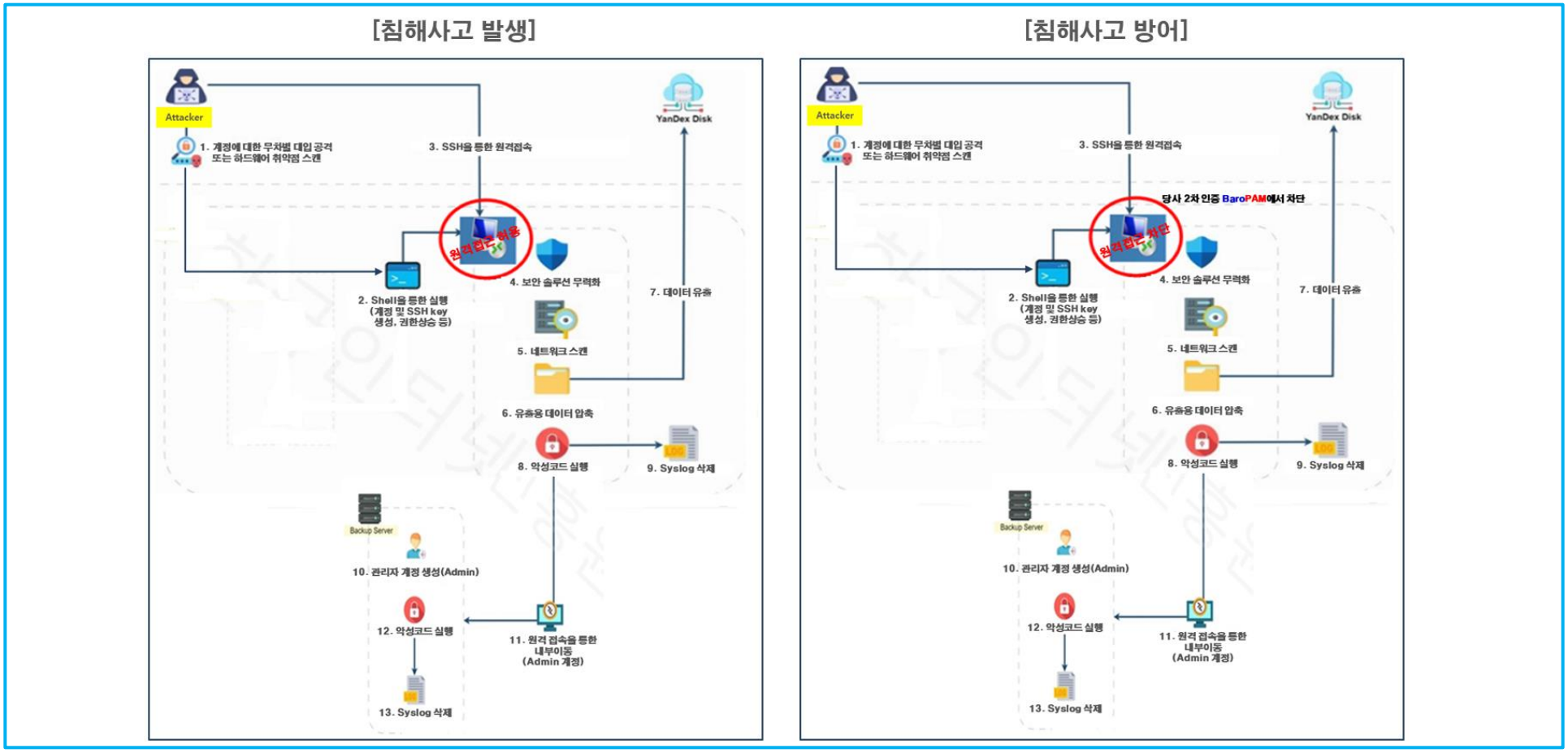
우회/원격 접속차단 (BaroPAM)



Desktop to Application
Desktop to Desktop
Desktop to Server
Desktop to Database
Server to Server

8. 해킹 차단 사례

해커들이 계정에 대한 무차별 대입 공격 또는 네트워크, 서버 등 하드웨어 취약점을 스캔/악용하여 쉘을 통한 계정 및 SSH key 생성, 권한 상승 등을 활용하여 원격 접속을 시도하였는데, 2차 인증(추가 인증) 솔루션인 바로팜(BaroPAM) 솔루션으로 인하여 원격 접속을 차단한 사례.



nurit

9. 솔루션 도입의 필요성

"정보자산의 로그인-ID/비밀번호가 유출이 되어도 대안이 있느냐?"

1. 보안 강화를 위하여 사용자 식별・인증을 위한 OTP 등을 활용한 2단계 인증 체계 적용

2차 인증 적용(예: ID/PW + OTP), 일정 횟수(예: 5회) 이상 인증 실패 시 접속 차단 및 인증수단을 특정하지는 않고 있으나, 지식기반.소유기반.특정기반 인증 수단 중 서로 다른 방식에 속하는 인증수단 2개를 조합해서 사용해야 함.

2. 중앙 집중식에서 벗어나 탈중앙화 방식의 다계층 인증 체계 적용

중앙 집중화 방식은 해커들의 "**단일 지점 공격**"의 표적이 되어 집중 공격을 받아 서비스가 중단되는데 비해서 탈중앙화된 **다계층 인증 체계**는 "**단일 지점 공격**"을 없애고, 사용자 식별.인증을 정보자산의 각 레이어별 분산하여 시스템의 보안을 강화시켜, 해커들의 공격으로 부터 서비스가 중단되거나 시스템에 접속하는 상황을 최소시켜 신뢰를 증가시킴.

3. 악의적인 목적으로 만들어진 프로그램인 악성코드에 의한 불법적인 우회/원격접속을 차단

악의적인 목적으로 만들어진 프로그램인 악성코드 프로그램에 의하여 정보자산의 접속정보(Desktop to Application, Desktop to Desktop, Desktop to Server, Desktop to Database, Server to Server 등)를 불법 취득한 뒤 불법적으로 정보자산에 우회/원격으로 접속하는 것을 차단 해야 함.

4. 분실.도용.해킹으로 인한 사용자 비밀번호 초기화에 적용

사용자 본인 스스로 로그인-ID, 특정항목, **일회용 인증키**를 입력하여 맞으면 새로운 비밀번호를 등록하여 사용하게 함.

"정보자산의 보안 강화를 위하여 **비밀번호 대체** 또는 **2차 인증(추가 인증)**은 선택이 아닌 반드시 적용해야 할 솔루션!"

10. 도입 시 검토사항

1. 제로 트러스트(Zero Trust) 개념이 적용되어 있는지?

2. 별도의 인증서버 방식인지, 모듈인증 방식인지?

3. 통합인증인지 분산인증인지?

4. 다양한 운영체제/애플리케이션 환경에 손쉽게 적용할 수 있는지?

5. 인증키 생성 및 검증 시 사용되는 키는 정적인지, 동적인지?

6. 제한된 시간 내에 횟수 제한을 할 수 있는지?

7. 간단(느슨)한 구성에서 시작해 더 복잡(견고)한 보안 시스템으로 진화할 수 있는지?

8. 중앙 집중식에서 벗어나 탈중앙화 방식의 다계층 인증 체계(Multi-Layer authentication system)를 지원하는지?

9. 보안 관점에서 위험을 얼마나 분산 시킬 것인지?

10. 인증 폭주 시 인증 속도는 얼마나 저하되는지?

11. 통신망을 사용하는지?

12. 보안시스템의 우회 및 원격접속을 차단할 수 있는지?

13. 보안지역이나 통신장애에 영향을 받는지?

14. 인증절차 시 데이터를 위변조하여 우회 인증절차에 대한 문제가 없는지?

[국가 사이버안전센터 인증 솔루션 보안 취약점]
15. 로그인 계정이나 개인정보의 도난, 스파이 행위, 통신 방해, 데이터 변경 등에 사용되는 중간자 공격(Man-in-the-middle attack)을 방어할 수 있는지?

16. 모바일 문자 메시지로 인증코드를 전송 했을 때 발생하는 심스와핑(SIM-swapping) 공격을 방어할 수 있는지?

17. 리버스 프록시(Reverse Proxy)와 같은 기술을 적용하여 인증을 우회할 수 있는 구조인지?

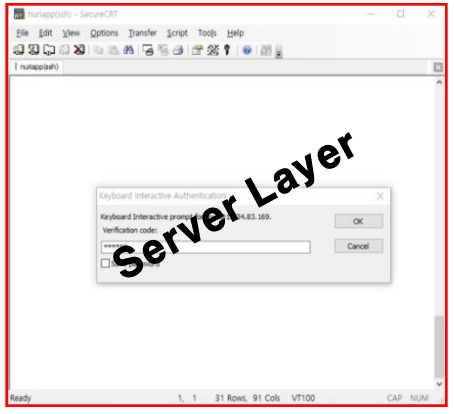
18. 푸시 알림을 계속 보내 상대방을 지치게 만들어 우발적으로 로그인 승인 버튼을 누르게 만드는 공격인 "MFA 피로 공격(fatigue attacks)"을 방어할 수 있는지?

Ⅲ. 인증 정책

1. 다계층 인증체계(Multi-layer authentication system)

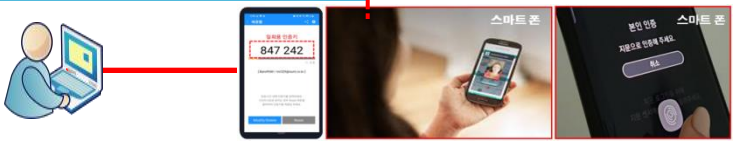
BaroPAM 솔루션의 모든 정보자산에 대한 인증 정책은 다양한 사이버 공격에 대비하여 통합해 보호하는 방법이 아니라 각각의 컴포넌트 하나하나를 "단일 지점 공격"에서 시스템을 보호하는 방안으로 중앙 집중식에서 벗어나 탈중앙화 방식의 다계층 인증 체계를 지원하여 보다 안전하게 정보자산을 보호할 수 있습니다.

Desktop/PC	Application	Server / Network 장비	Database / Storage
로그인-ID, 비밀번호 이외의 추가 인증(2차 인증) (일회용 인증키)	비밀번호 대체 또는 추가 인증(2차 인증) (일회용 인증키)	로그인-ID, 비밀번호 이외의 추가 인증(2차 인증) (일회용 인증키)	로그인-ID, 비밀번호 이외의 추가 인증(2차 인증) (일회용 인증키)




```
$ sqlplus baropam/baropam

Verification code: 613045

SQL*Plus: Release 11.2.0.1.0 Production on
금 11월 30 09:38:50 2018

Copyright (c) 1982, 2009, Oracle.  All
rights reserved.

SQL> exec twofactor.authenticate(691199);

PL/SQL procedure successfully completed

SQL> exec enable_role('APPOBJACCESS');
PL/SQL procedure successfully completed.
```

Storage Layer



※다계층 인증 체계는 제로 트러스트 모델의 핵심 요소 중 하나이며, 각 레이어별로 인증을 강화하여 네트워크 보안을 혁신하는 안전한 해결책.

nurit

Ⅳ. 보안 전략

1. 개방형 OS의 데스크탑 환경

BaroPAM의 보안 전략은 3단계로 구성되며, 1단계는 전형적인 기본 보안(지식기반 인증: ID/Password), 2단계는 스마트 폰의 생체인식 기능을 BaroPAM 앱에 적용하여 인증하는 생체인식 보안(속성기반 인증: 생체정보), 3단계는 BaroPAM 앱에서 생성한 일회용 인증키(소유기반 인증)를 적용하여 보안 강화에 최적화되게 구성되어야 합니다.

1단계: 지식기반 인증

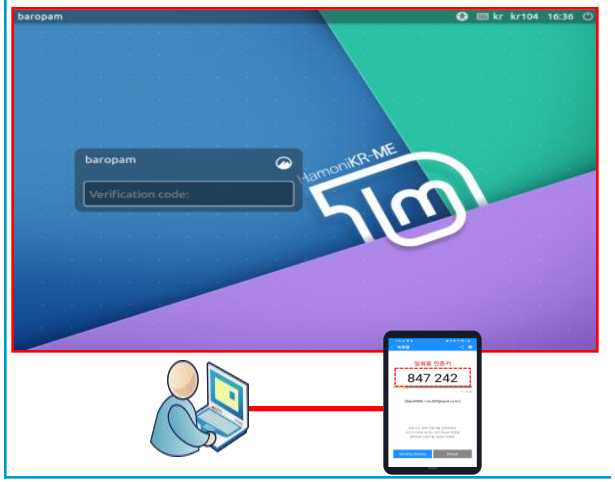
기존의 전형적인 기본보안
(ID / Password)

2단계: 속성기반 인증

생체인식 보안
(생체정보)

3단계: 소유기반 인증

BaroPAM 앱을 이용하여
2세대 인증키를 부여 받아 입력
(일회용 인증키)



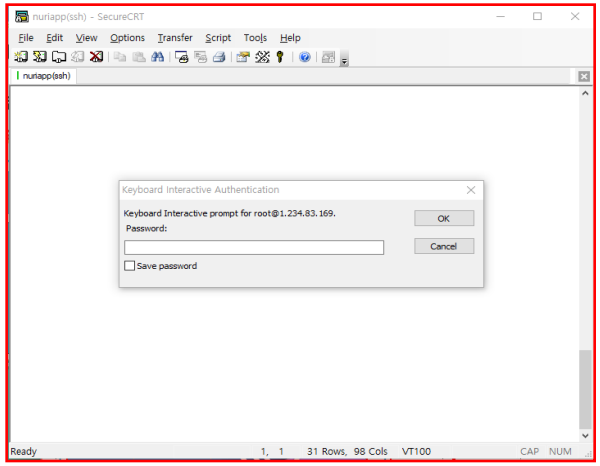
nurit

2. 개방형 OS의 서버 환경

BaroPAM의 보안 전략은 3단계로 구성되며, 1단계는 전형적인 기본 보안(지식기반 인증: ID/Password), 2단계는 스마트 폰의 생체인식 기능을 BaroPAM 앱에 적용하여 인증하는 생체인식 보안(속성기반 인증: 생체정보), 3단계는 BaroPAM 앱에서 생성한 일회용 인증키(소유기반 인증)를 적용하여 보안 강화에 최적화되게 구성되어야 합니다.

1단계: 지식기반 인증

기존의 전형적인 기본보안
(ID / Password)

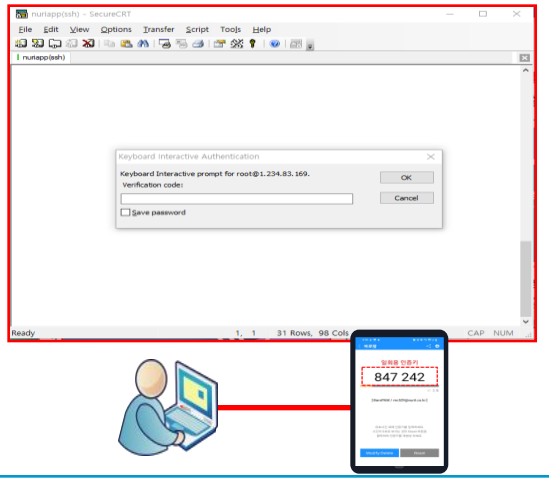


2단계: 속성기반 인증

생체인식 보안
(생체정보)

3단계: 소유기반 인증

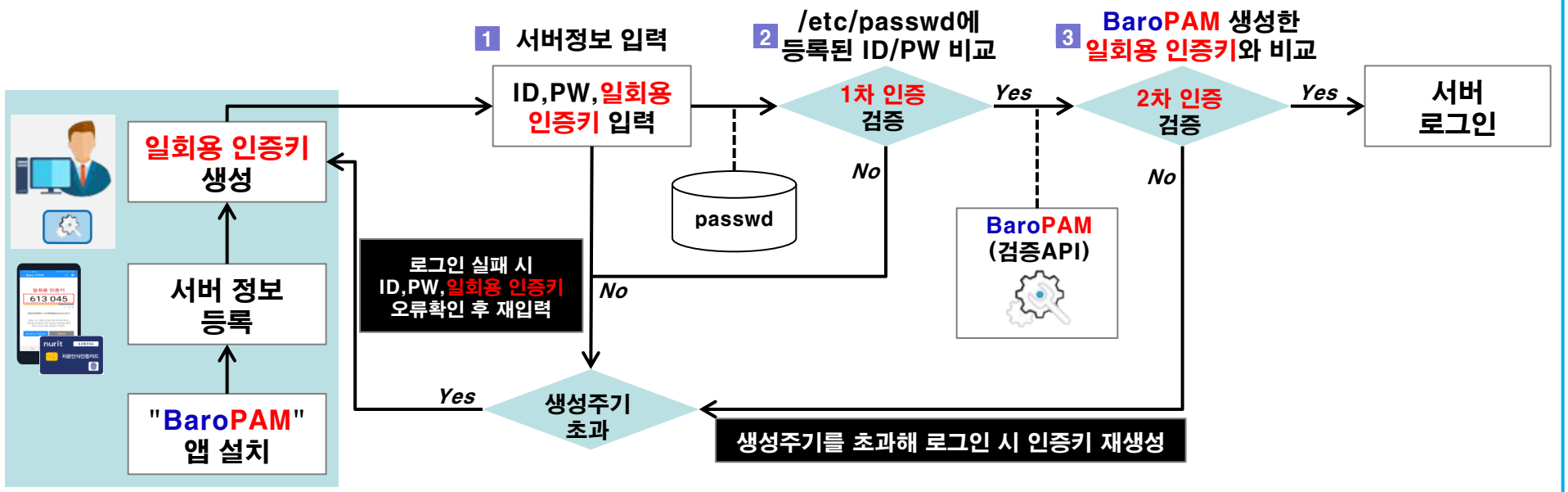
BaroPAM 앱을 이용하여
2세대 인증키를 부여 받아 입력
(일회용 인증키)



nurit

Ⅴ. 적용 프로세스

1. 2차 인증 적용 프로세스



No	구분	내용	설명
1	2차 인증 앱 (BaroPAM)	BaroPAM 앱 다운로드 및 설치	-안드로이드폰: 구글 플레이스토어 접속 및 "바로팜" 앱 다운로드 -아이폰: 애플 앱스토어 접속 및 "BaroPAMs" 앱 다운로드
2		BaroPAM 앱 실행	
3		"인증 코드" 버튼 선택	-실행된 앱 하단 왼쪽 버튼 선택
4		서버 정보 등록	-시스템명: 서버 명칭(임의 등록 가능) -Secure key: 서버에 부여된 Secure key(벤더발급) -생성주기: 3~60초 사이 입력
5		저장 후 목록 조회 시 나오는 항목 클릭, 일회용 인증키 생성	
6		서버에 접속해 ID, PW, 일회용 인증키를 입력해 로그인	-Secure key, 생성주기, 일회용 인증키를 이용해 2차 인증 검증

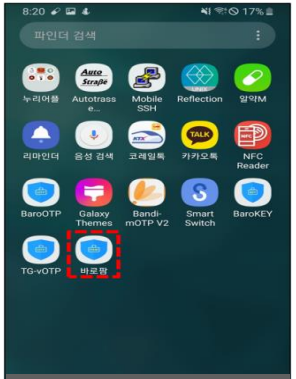
Ⅴ. 적용 프로세스

2. 2차 인증 데모 적용화면

1. 앱 다운로드 및 설치

폰 > 플레이스토어 > BaroPAM 검색

2. 앱 실행



바로팜 아이콘 클릭

3. 왼쪽 버튼 클릭

"인증 코드" 버튼 클릭

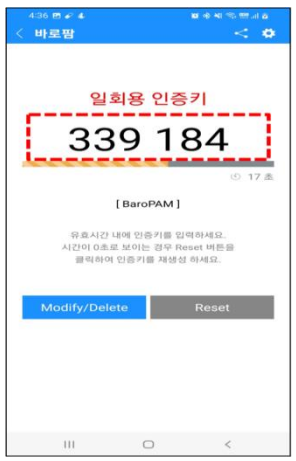
4. 서버 정보 등록

"Save" 버튼 클릭 (Secure key, 생성주기는 BaroPAM 환경설정과 일치)

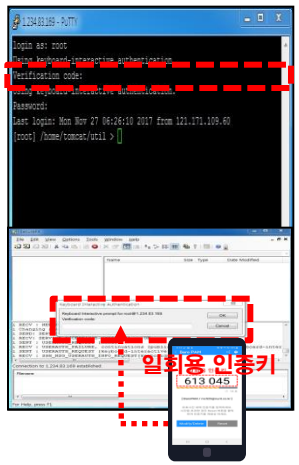
5. 서버 정보 조회

일회용 인증키를 생성할 항목 선택

6. 일회용 인증키 생성



7. 로그인(2차 인증)

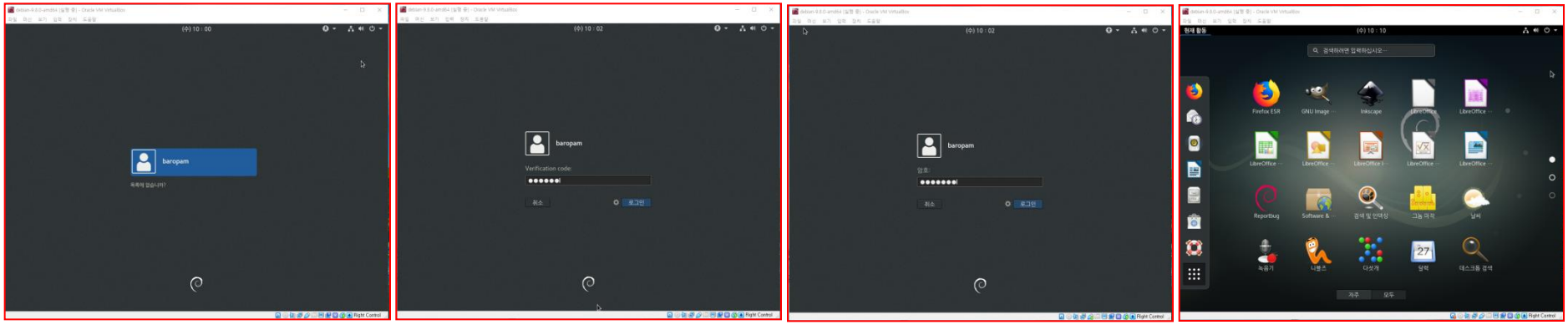


Ⅵ. 적용 결과

1. Debian

1. Desktop 로그인

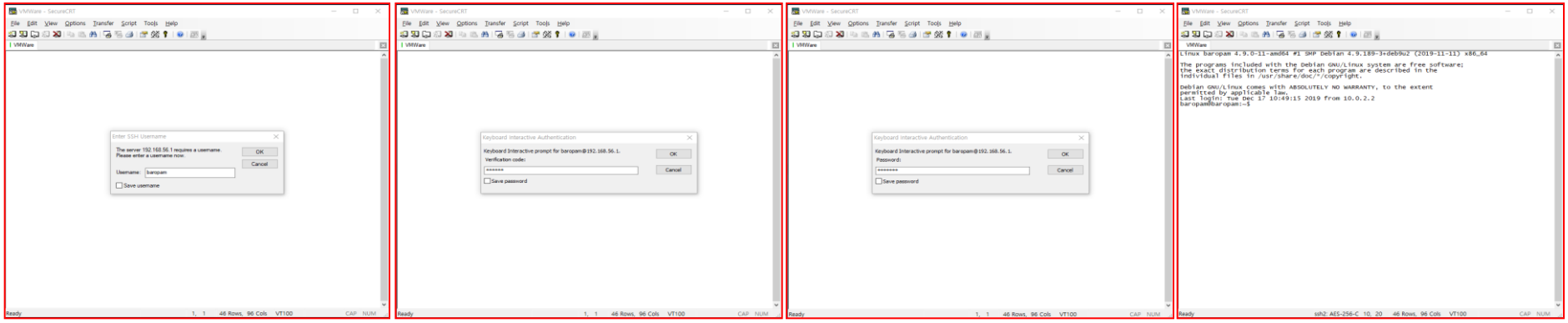
1) 로그인 화면(로그인-ID 선택) 2) Verification code 입력 3) 비밀번호 입력 4) 메인 화면



/etc/pam.d/gdm-password ➔ auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no auth=pam

2. SSH 접속(SecureCRT)

1) 로그인-ID 입력 2) Verification code 입력 3) 비밀번호 입력 4) 메인 화면



/etc/pam.d/sshd ➔ auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no auth=pam

2. 하모니카OS/구름OS

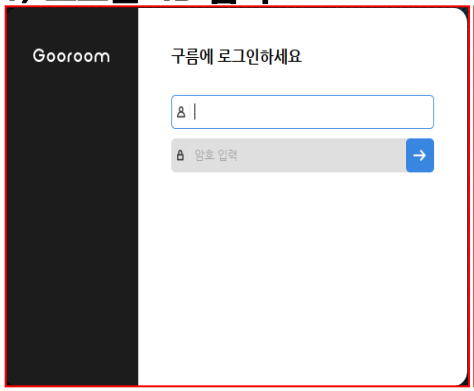
1. 하모니카OS

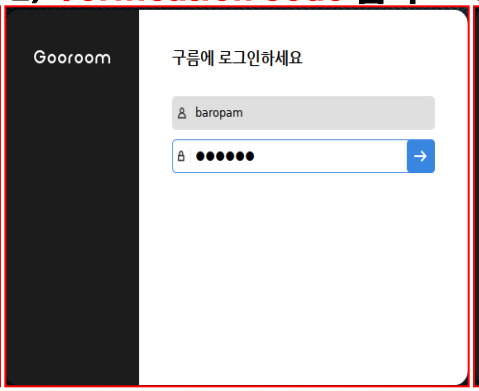
1) 로그인 화면(로그인-ID 선택) 2) Verification code 입력 3) 비밀번호 입력 4) 메인 화면

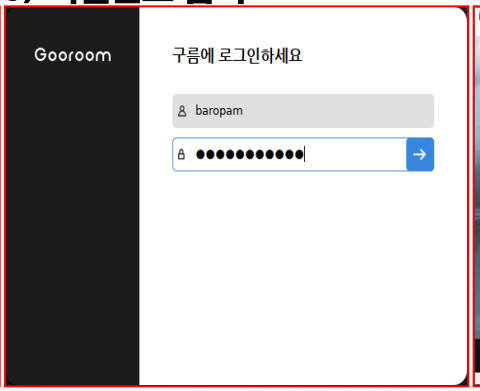
/etc/pam.d/lightdm → auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no auth=pam

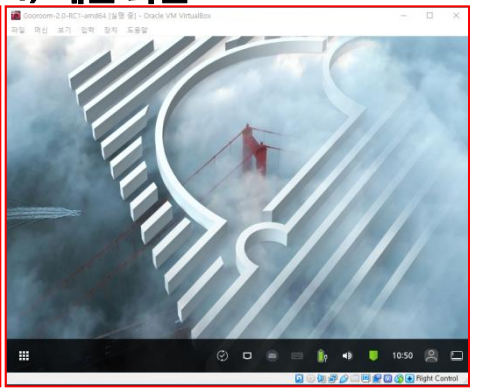
2. 구름OS

1) 로그인-ID 입력 2) Verification code 입력 3) 비밀번호 입력 4) 메인 화면









/etc/pam.d/gdm-password → auth required /usr/baropam/pam_baro_auth.so nullok secret=/usr/baropam/.baro_auth encrypt=no auth=pam

nurit

3. 맺는 말

망분리로 인한 보안이 강화된다는 것은 어불성설이며, 지금은 정보보안에 대한 인식의 대전환이 필요한 시대.

아직도 보안에 취약한 이런 방식이 사용되고 있다는 현실
▶2차 인증 중 해커들의 가장 좋아하는 적용 방식: Gateway(+Proxy) 방식
▶2차 인증 중 가장 취약한 인증 방식: SMS, 이메일 등 문자기반의 인증
▶2차 인증 중 해커들이 가장 애용하는 우회 기술과 피로공격에 취약한 인증 방식: 2 채널 인증
▶피싱 공격에 잘 속는 링크 방식: QR 코드 방식

정보자산의 보안 강화를 위해서는 가장 중요한 기본 사항
▶보안 관점에서 위험을 얼마나 분산 시킬 것인지?
▶인증 절차 시 데이터 위변조를 어떻게 방어할 것인지?
▶계정 정보 도용 및 악용은 어떻게 차단할 것인지?
▶브라우저 자동 로그인은 어떻게 방어할 것인지?
▶단일 지점 공격을 어떻게 방어할 것인지?
▶우회/원격접속을 어떻게 차단할 것인지?
▶중간자 공격을 어떻게 방어할 것인지?
▶다중 인증(MFA)의 우회기술을 어떻게 차단할 것인지?
▶다중 인증(MFA)의 피로공격을 어떻게 방어할 것인지?

무엇보다도 인증키는 본인이 소유하고 있는 인증키 생성매체를 사용해서 본인이 직접 인증키를 생성하여 본인이 접근하고자 하는 정보자산에 직접 입력 및 검증해야 그나마 정보보안 사고를 예방할 수 있는 최선책.

결론은 "2차 인증을 도입했다"는 것이 아니라 기술 및 보안성 등 "어떤 2차 인증을 도입했느냐"가 관건.
"아무 것도 신뢰하지 않는다" = "아무도 믿지 마라" = "계속 검증하라"

1. 회사 소개

일반현황

상호:	주식회사 누리아이티
설립일:	2018년 1월 19일
주사업분야:	정보자산의 보안강화를 위한 다계층 인증S/W
사업장:	서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)
주요 품목:	BaroPAM, BaroCRYPT, BaroCollector, BaroFDS, BaroIDS
자문교수:	문영상 숭실대학교정보과학대학원 소프트웨어공학과 겸임교수

「BaroPAM 솔루션의 전략은 정보자산에 대한 보안을 강화하기 위하여 탈중앙화 방식의 다계층 인증을 지원하는 방향으로!」

연혁

2025.02 Linux용 BaroPAM에 환경설정 정보를 MariaDB와 연동하는 모듈 출시
2025.02 도어락용 BaroPAM 출시

2024.09 파트너 체제에서 총판 체제로 전환
2024.06 Cloudera Data Platform과 Hi-ware 접근제어 솔루션에 BaroPAM 연동
2024.05 피앤피 시큐리티 서버접근제어 솔루션에 BaroPAM 연동
2024.04 오픈소스 협업 툴인 Mattermost 에 BaroPAM 연동

2023.08 Cisco VPN, Foti-gate VPN, OpenVPN OpenVPN에 BaroPAM 연동
2023.04 BaroPAM 앱에 생체인식(지문.얼굴인식) 기능 추가

2022.12 Palo Alto Networks Firewall(비전테크 공급)에 BaroPAM 연동
2022.11 KOICA 클라우드 컴퓨팅 기반환경 구축 및 무선 네 트워크 고도화 용역 사업에 2차 인증으로 BaroPAM 선정
2022.11 시큐어레터의 Anyclick AUS에 Wifi 접속 시 2차 인증으로 BaroPAM 적용
2022.08 Beyondtrust Password safe(아이리스인포테크 공급)에 2차 인증으로 BaroPAM 연동
2022.06 2022년 정보보호 선도기술 개발 지원사업에 BaroCARD(지문인식OTP카드) 참여
2022.05 TTA에서 하모니카 OS와 BaroPAM 제품의 SW상호운영성 시험진행

2021.10 FreeRADIUS에 BaroPAM 연동
2021.08 Windows용 BaroPAM에 화면 보호기의 잠금 방지 및 해제 기능 추가
2021.07 BaroPAM v1.0 조달 등록
2021.07 2021 보안솔루션(SECaaS)공급 Pool 등록 솔루션에 BaroPAM 선정
2021.04 세윤씨엔에스에서 Microsoft365, Power Apps, ERP 등 Microsoft 제품과 BaroPAM 연동
2021.04 TS Solution의 NVR 솔루션에 BaroPAM 임베디드 공급

2021.03 Sophos SSLVPN(엘리시스 공급)에 BaroPAM 연동
2020.09 중소기업벤처기업부 'K-비대면 바우처 플랫폼', 네트워크, 보안 솔루션 분야에 BaroPAM 참여
2020.09 2020년 엘지유플러스 정부업무망 모바일화 레퍼런스 실증 사업에 2차 인증 SW(BaroPAM) 납품
2019.10 "범정부 데이터 플랫폼 2단계 구축" 사업(309개 공공기관)에 BaroPAM 공급
2019.05 개방형OS인 하모니카OS, 구름OS용 BaroPAM 출시
2019.04 유도전류를 이용한 무충전 방식의 지문인식 출입카드 출시
2019.04 BaroPAM GS인증 누리아이티 -> 주식회사 누리아이티로 양도양수
2019.03 BaroPAM 저작권 등록

2018.12 웹용 일회용 인증키 생성기 오픈(www.baropam.com)
2018.07 BaroPAM 인증카드 및 지문인식 인증카드 출시
2018.06 Windows용 BaroPAM 출시
2018.04 금융결제용 OTP토큰/카드 Firmware 개발
2018.01 주식회사 누리아이티 설립(마곡나루)

2017.09 BaroPAM 어플 서비스 개시
2017.07 BaroIDS(이상접속 탐지 및 차단) 제품 출시
2017.07 바로팜 V1.0(BaroPAM V1.0) GS인증 1등급 인증
2017.05 BaroCRYPT(암복호화) 제품 출시
2016.11 Linux/Unix용 BaroPAM(정보자산 2차 인증) 제품 출시
2016.05 BaroKEY(일회용 인증키) 제품 출시
2016.01 BaroFDS(이상금융거래 탐지시스템) 제품 출시
2015.10 BaroCollector(실시간 로그 수집기) 제품 출시
2014.04 특허출원(OTP카드를 이용한 본인인증 결제시스템 및 그 방법)
2009.11 누리아이티로 상호 변경
2006.03 케이피엘 인포텍 설립(대방동 경원빌딩)

nurit

2. 소프트웨어 품질인증 (GS 인증서 / 시험성적서 / 특허증 / 저작권 등록증)

2017년 7월
GS인증 1등급

2017년 7월
TTA 시험성적서

2014년 6월
특허번호
제 10-1413971호

2022년 6월
SW상호운용성시험

2019년 3월
저작권 등록증

3. BaroSolution 제품군

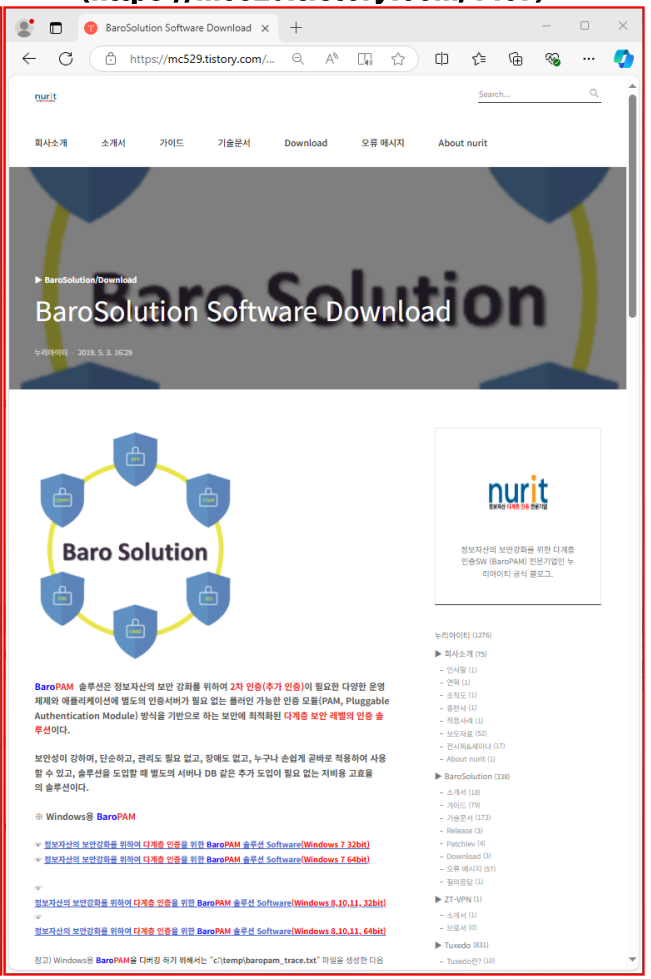
구 분	설 명	비고
BaroPAM	제로 트러스트(Zero trust) 보안 모델로 정보자산의 보안 강화를 위하여 2차 인증(추가 인증)이 필요한 다양한 운영체제와 애플리케이션에 누구나 손쉽게 곧바로 적용할 수 있는 플러그인 가능한 인증 모듈(PAM, Pluggable Authentication Module) 방식을 기반으로 하는 보안에 최적화된 생체인식이 적용된 3단계 인증 솔루션.	
BaroCRYPT	Feistel 암호를 사용하여 크기가 작고 구현이 쉬운 블록 암호화 알고리즘인 XXTEA (Extended Extended Tiny Encryption Algorithm)를 기반으로 하는 가볍고 가장 빠른 암호화 알고리즘을 적용한 솔루션.	
BaroCollector	다양한 Source에서 발생된 많은 양의 로그 데이터(Big Data)를 중앙의 데이터 저장소로 효율적으로 수집해 주는 분산처리, 신뢰성, 가용성을 갖춘 실시간 로그 수집기.	
BaroFDS	이상금융거래탐지 및 대응업무에 대한 모 금융기관의 2년간의 Know-how을 바탕으로 개발된 금융권 유일의 검증된 FDS 솔루션으로서 복잡한 금융권 환경에서 쉽고 빠르게 적용하여, 구축 즉시 효과를 발휘할 수 있음.	
BaroIDS	정보자산(서버, 네트워크장비, 보안장비, 저장장치, 데이터베이스, 애플리케이션, 기타)의 이상접속 탐지 및 차단에 대한 현장의 Know-how을 바탕으로 FDS(Fraud Detection System)를 적용하여 개발된 솔루션.	

4. BaroSolution Download

BaroSolution 소개서 Download (https://mc529.tistory.com/1401)

BaroSolution 가이드 Download (https://mc529.tistory.com/1406)

BaroSolution Software Download (https://mc529.tistory.com/1407)



nurit

기억할 필요가 없는 비밀번호!
BaroPAM이 함께 합니다.

감사합니다!

www.nurit.co.kr

서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)
주식회사 누리아이티 대표전화 : 02-2665-0119