nurit

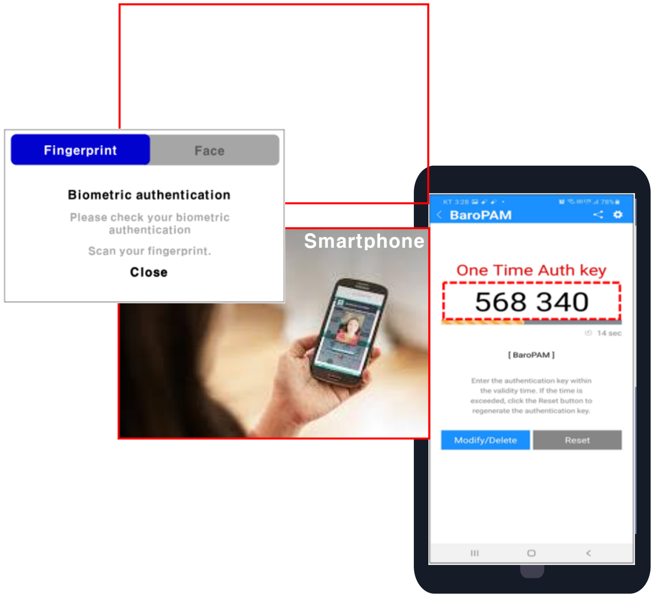
Introduction to the BaroPAM solution

for multi-layer authentication that strengthens the security of information assets

Jun, 2025

PAM

1등급 GOOD Software



Biometric authentication

Please check your biometric authentication

Scan your fingerprint.

Close

[BaroPAM]

Enter the authentication key within the validity time. If the time is exceeded, click the Reset button to regenerate the authentication key.

••• Content •••

Ⅰ. Background and changes

Ⅱ. BaroPAM

Ⅲ. Etc

Ⅰ. Background and changes

1. Before starting

"**Basic security must be thoroughly implemented first.**"

Any security expert knows that current security systems are not sufficient to protect information assets.

It appears that 85% of critical infrastructure attacks are caused by failure to adhere to basic levels of security, such as "**patching, 2nd authentication (additional authentication), and the principle of least privilege.**"

80~90% of breaches involving Ransomware are related to remote access.

The first security solution to be introduced is a **2nd authentication** solution that can **block account theft, privilege escalation, and bypass/remote access.**

Most attacks can be prevented by simply following basic security policies.

Additionally, "**Network Segmentation**" is a security strategy and concept that is neither new nor special.

The time has come when we must admit that "**Network Segmentation**" cannot 100% prevent hacker infiltration. In this era, reducing damage was the biggest task of security.

As far as this has gone, "**a security strategy must be prepared assuming that cyber attackers are already in the network**" has become a security proposition.

Damage must be minimized by limiting situations where external hackers or internal users illegally access information assets and distributing security risks.

Recently, the operating system (OS) and administrator account of the centralized management server have been hacked, taking control of the management server and leaking information, stealing and abusing it, inserting malicious code, deleting information, and disabling the management server to disable services. "**Single-point attacks**" are causing a lot of damage to companies.

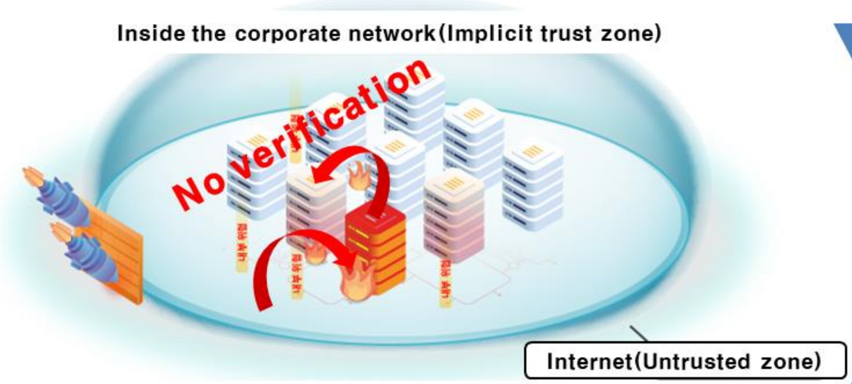
2. Changes in security model

AS-IS(Perimeter security model)

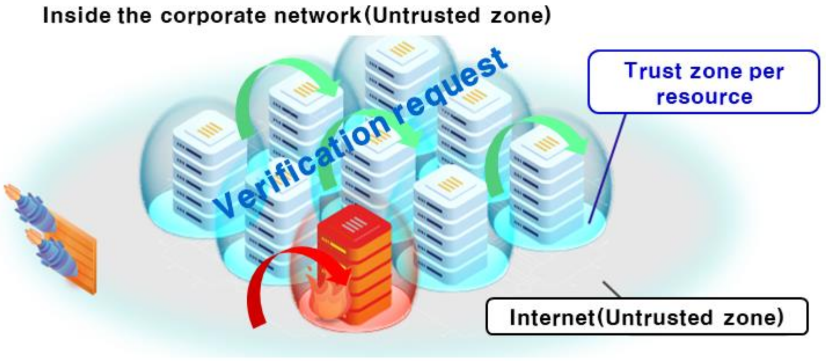
- ▶Traditional network perimeter-based security models are not sufficient.
- ▶Connotations of limitations to the attacker's ability to move within the boundary after violating it.

TO-BE(Zero trust model)

- ▶Enhanced Authentication
- ▶Micro Segmentation
- ▶Software defined boundary



Threats can spread when infiltrated internally



Threats cannot be spread even when infiltrated internally

"Never Trust, Always Verify"

2. Changes in security model(Continue)

As security models change, existing security solutions can no longer block them, and it is time for a change in security solutions.

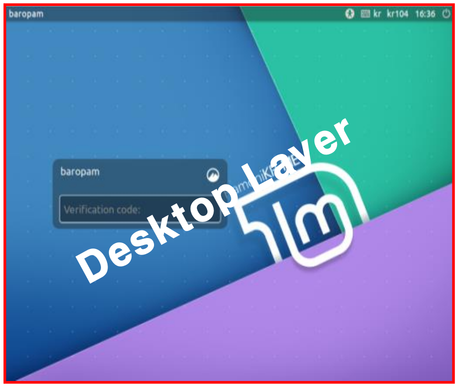
- ▶Change in security model from perimeter security to zero trust security.
- ▶Attacks that exploit security vulnerabilities as attack surfaces.
- ▶Need to distribute risks to minimize security risks.
- ▶Need to decentralize from centralization.
- ▶Need to block single-point attacks from neutralizing security solutions.

3. Multi-layer authentication system

An authentication system that protects the system from "single point attacks" by decentralizing components (layers) to disperse security risks like a tight mesh network, moving away from centralization to prepare for various cyber attacks.

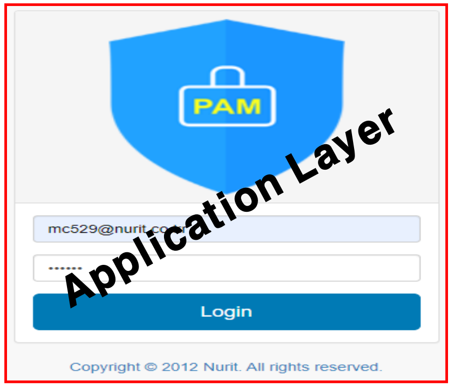
Desktop/PC

Using the BaroPAM app Entered after receiving 2nd generation authentication key (OTA key)



Application

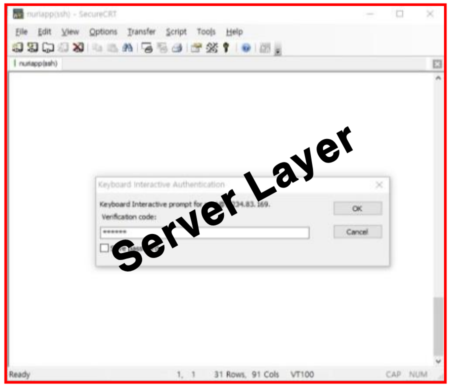
Using the BaroPAM app Entered after receiving 2nd generation authentication key (OTA key)



Copyright © 2012 Nurit. All rights reserved.

Server / Network

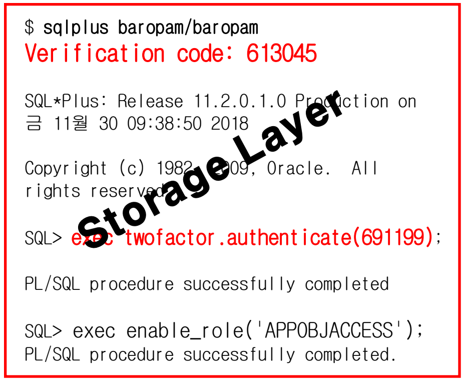
Using the BaroPAM app Entered after receiving 2nd generation authentication key (OTA key)


nuriapp(ssh) - SecureCRT
File Edit View Options Transfer Script Tools Help
nuriapp(ssh)
Keyboard Interactive Authentication
OK
Cancel
Server Layer
Ready 1, 1 31 Rows, 91 Cols VT100 CAP NUM

Keyboard Interactive prompt for ...234.83.169.
Verification code: ******

Database / Storage

Using the BaroPAM app Entered after receiving 2nd generation authentication key (OTA key)



```
$ 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.
```

※ **Multi-layer authentication** is one of the core elements of the zero trust model and is the most secure solution to innovate network security by strengthening authentication at each layer. **MFA** is one element of a **multi-layer authentication system**.

4. The need for multi-layer authentication system

It plays a key role in protecting an organization's sensitive assets, ensuring regulatory compliance, and ultimately providing more secure and reliable services to users.

Enhanced security and prevention of unauthorized access

Dramatically strengthens security to block access by hackers and unauthorized users.

▶Overcoming the vulnerability of single authentication

▶Protection against password leaks/theft

▶Defense in Depth strategy

Responding to evolving cyber threats

Today, cyberattacks are an essential line of defense against increasingly sophisticated and intelligent threats.

▶Defense against various attack methods

▶Protection of various information assets

Improve regulatory compliance and trust

Beyond simple security technologies, it increases the trustworthiness of the organization and meets legal and regulatory requirements.

▶Meet legal and regulatory requirements

▶Improve customer and user trust

Ensuring business continuity and reducing costs

Reduce the risk of accidents, secure business continuity, and contribute to long-term cost reduction.

▶Reduce accident response costs

▶Increase operational efficiency

※ A multi-layer authentication system is one of the core elements of the zero trust model, revolutionizing network security by strengthening authentication at each layer.

5. Characteristics of companies where infringement incidents occurred

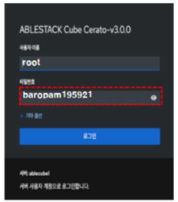
85% of major infrastructure attacks occur due to failure to maintain basic levels of security such as patching, 2nd authentication (additional authentication), and the principle of least privilege.

- ▶OS is not updated with the latest patches.
- ▶Do not use 2nd authentication.
- ▶The default port is used as is.
  Ex) SSH/SFTP:22, VPN: 4433, RDP: 3389,
  SMB: 139, 445 etc.
- ▶Do not disable unnecessary services.
- ▶No regular security audits.
- ▶Lack of security awareness among employees (lack of security training).

2nd authentication application order

1. Operating system(OS)

2. Administrator account or Admin console


ABLESTACK Cube Cerato-v3.0.0

사용자 이름: root

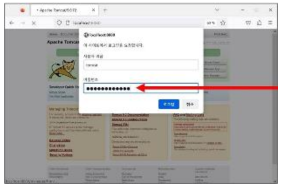
비밀번호: baropam195921

› 기타 옵션

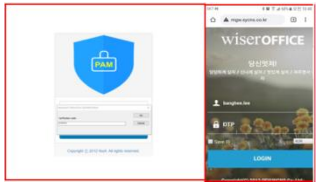
로그인

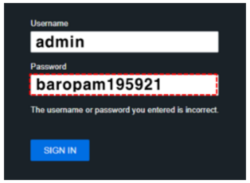
서버: ablecube1

서버 사용자 계정으로 로그인합니다.



3. Normal user account




Username: admin

Password: baropam195921

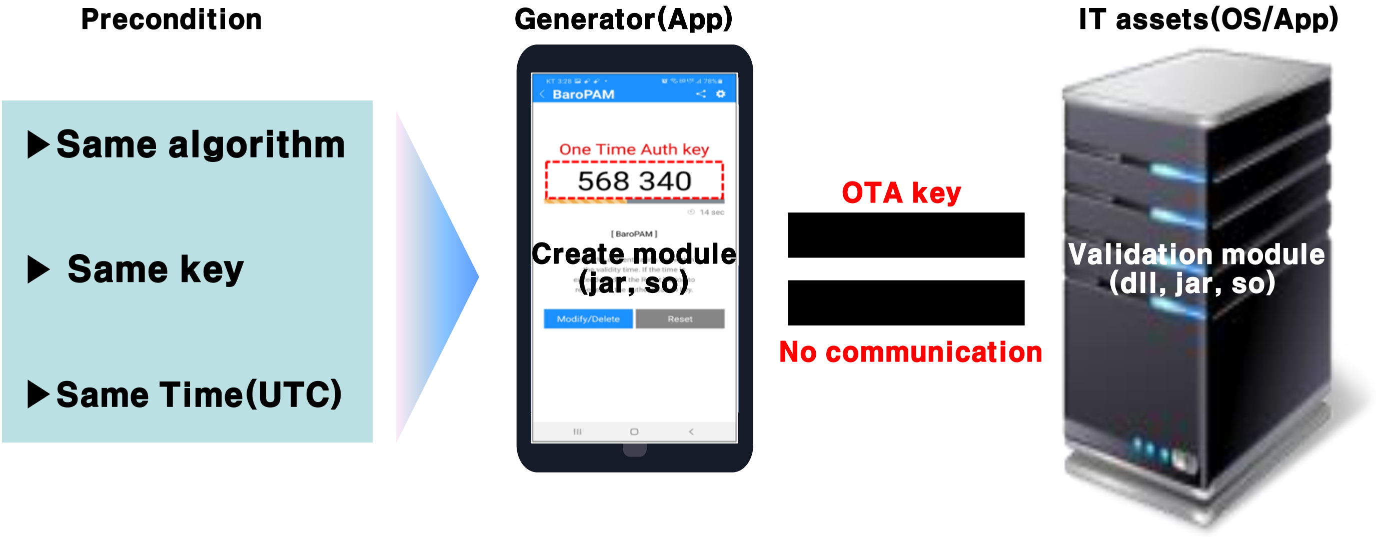
The username or password you entered is incorrect.

SIGN IN

One Time Auth key
818 126
Smartphone
Smartphone
본인 인증

1. What is a OTA key?

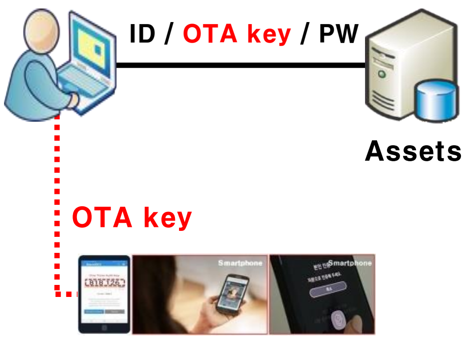
With the modular authentication method, the authentication key once used cannot be reused, and it is difficult to infer the authentication key, providing strong security against various hacking attacks.



2. What is BaroPAM?

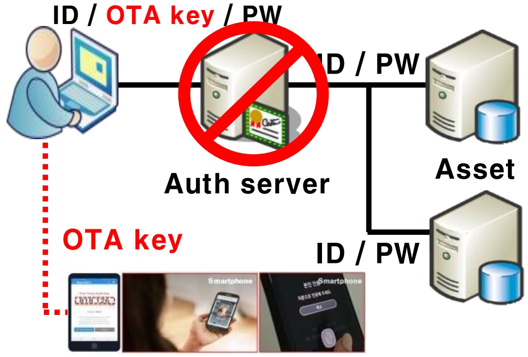
A solution that supports security-optimized multi-layer authentication based on the Pluggable Authentication Module (PAM) method for various operating systems and applications.

Reinforcing information asset access security



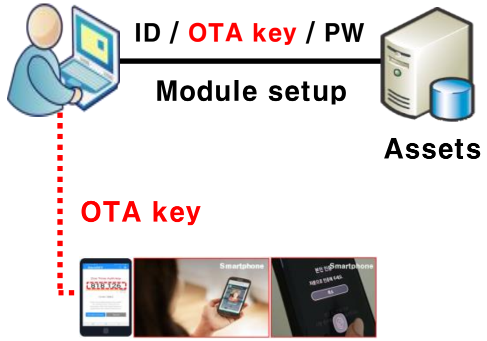
- Reinforcing the security of information assets by limiting the illegal access of information assets by external hackers or internal users
- 2-Factor authentication is an authentication method that adds another element, ownership-based/attribute-based authentication, to ID / PW authentication, which is the existing "knowledge-based authentication"

Ease of service



- Easy authentication using the BaroPAM app without the need for a separate authentication key token/card for secondary authentication
- Reducing management/operation costs with a structure that does not require a separate authentication server or a server that manages Windows/server access control

Easy to apply



- Simple application with a structure that installs modules in each Windows or server
- Applicable during operation as it does not restart Windows or the server
- No need to change settings of existing network equipment

3. Solution Benefits

A low-cost, high-efficiency solution that has strong security, is simple, requires no management, has no problems, can be easily applied and used by anyone, and does not require additional introduction such as a separate server or DB when introducing the solution.

▶Supports multi-layer authentication using a module authentication method that does not require a separate authentication server
▶Guaranteed service with fast authentication speed (average authentication time within 0.01 seconds)

▶BaroPAM provides app source obfuscation and screen capture prevention functions
▶Biometric authentication (fingerprint recognition, face recognition) function is provided when running the BaroPAM app

▶Using the globally accepted 512-bit standard Hash function (HMac-SHA512 / Internet security standard IETF RFC 6238)
▶Provides the ability to link environment setting information with a database (MariaDB) in addition to files.

▶Provides a function to set the number of times and time limit for authentication (eg, 3 times in 30 seconds)
▶Provides the ability to prevent man-in-the-middle attacks

▶Authentication is possible even in frequently occurring communication failures or secure areas
▶Dynamic security support such as one-time/volatile that changes every time or is used once and then discarded

▶Even if authentication information is forged or altered during the authentication process, bypass authentication is not possible
▶Authentication bypass (bypass technology, fatigue attack, etc.) is not possible

▶You can start with a simple (loose) configuration and evolve to a more complex (strong) security system
▶iOS provides a function that allows you to authenticate yourself

▶Even if your account information is stolen by abusing the automatic login function, you will not be able to log in
▶Emergency one-time authentication key provided when smartphone is not available.

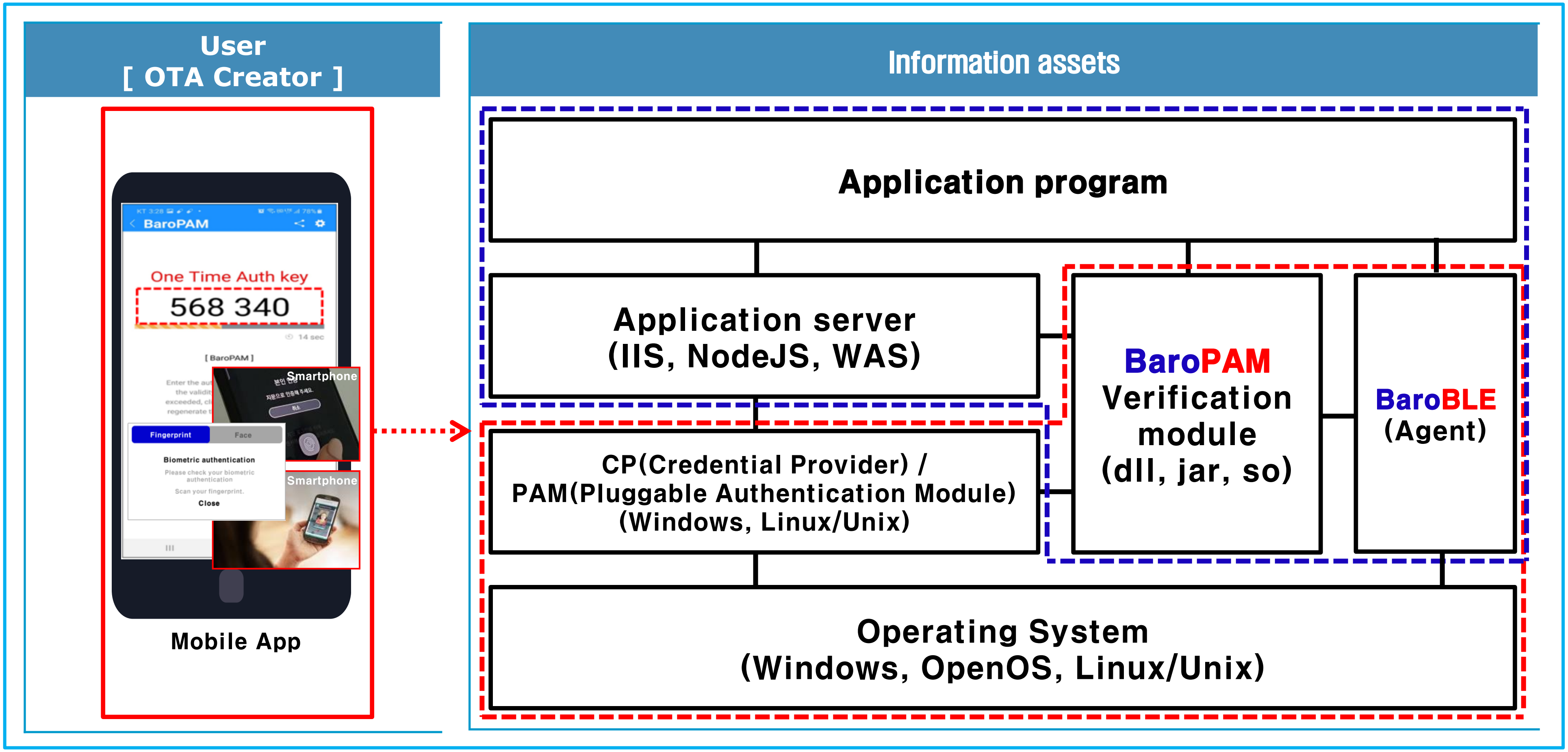
▶It can be used in all fields requiring 2nd authentication, such as information assets (Among RADIUS authentication of information assets, PAM/SQL/HTTP authentication is also supported)
▶Provides ACL function for accounts that can be allowed/denied from 2nd authentication

▶Provides free customization and interworking development with various applications
(API interworking of Java, C, C++, etc.)

Ⅱ. BaroPAM

4. Solution configuration

It consists of a device that generates a one-time authentication key for the user, an information asset that applies the one-time authentication key, a module that verifies the one-time authentication key, and BaroBLE that communicates between the BaroPAM app and the Bluetooth/application on the desktop.



User
[OTA Creator]

Mobile App

Information assets

Application program

Application server
(IIS, NodeJS, WAS)

CP(Credential Provider) /
PAM(Pluggable Authentication Module)
(Windows, Linux/Unix)

BaroPAM
Verification
module
(dll, jar, so)

BaroBLE
(Agent)

Operating System
(Windows, OpenOS, Linux/Unix)

5. Support environment

Supports various development and operating environments.

No	Division		Description	Etc
1	OS	Windows series	Windows 8.1 or later Windows server 2012 R2 or later	
		Linux series	Open Linux support such as Radhat, CentOS, AlmaLinux, RockyLinux, NAVIX, Oracle linux, Debian, Fedora, Mint, Ubuntu, openSUSE, KaliLinux, and Open OS (HamoniKR OS, Gooroom OS), etc	
		Unix series	AIX, HP-UX, Solaris, FreeBSD, MacOS, etc	
2	Language		C, C++, C#, Java, ASP, PHP, PowerBuilder, Delphi, etc	
3	Application	ARM system	Shard object provided (Authentication, Encryption/Decryption)	
		IIS	dll provided (Authentication, Encryption/Decryption)	
		NodeJS	jar provided (Authentication)	
		WAS	jar provided (Authentication, Encryption/Decryption)	
4	Database	Encryption and decryption	Oracle, Tibero, MySQL, MariaDB, PostgreSQL, etc.	
		Authentication	Database that supports Radius authentication such as Oracle, MySQL, MariaDB, PostgreSQL, etc.	
5	Network equipment		Devices that support Open Linux and RADIUS authentication, OpenVPN supports PAM/RADIUS authentication	
6	Storage device		Devices that support commercial OS.	

6. Differentiation from competing technologies (products)

It is strong in security as it is difficult to leak or infer because it uses dynamic Secret values.

▶ Supports dynamic Secret values

▶ Ability to prevent man-in-the-middle attacks

▶ iOS has the ability to authenticate itself

▶ Decentralized rather than centralized

▶ Module authentication method rather than a separate authentication server method

▶ Supports multi-layer authentication systems

▶ Supports various operating systems and applications

▶ Support for dynamic security such as one-time/volatile

▶ No additional equipment (server, DB) required

▶ No problem in using and applying anywhere overseas

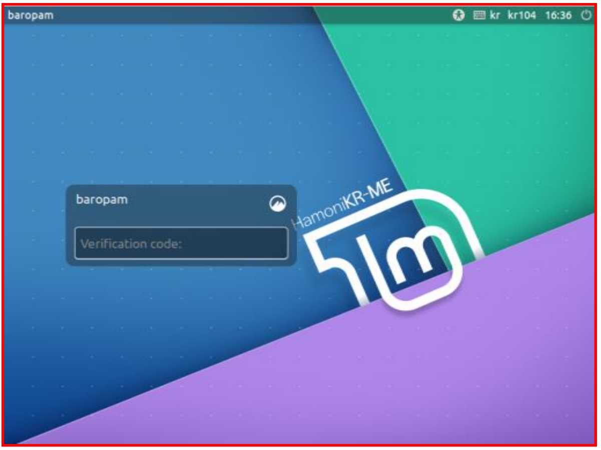
▶ Easy to apply and no hassle

7. Application plan

New application methods such as additional authentication, password replacement, and new password are required.

1 alternative(additional certification)

Apply OTA key as additional authentication (2nd authentication) other than login-ID and password(ID/PW/OTA)


baropam

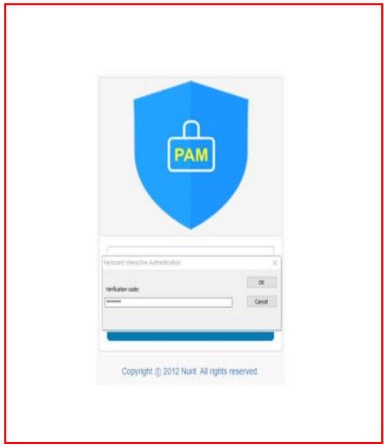
kr kr104 16:36

baropam

Verification code:

2 alternative(password replacement)

Remove the password and replace it with a OTA key (ID/OTA)



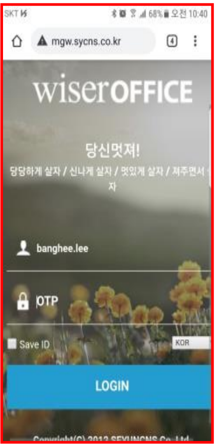
Keyboard Interactive Authentication

Verification code: ******

OK

Cancel

Copyright © 2012 Nurit. All rights reserved.


mgw.sycns.co.kr

wiserOFFICE

당신멋져!

당당하게 살자 / 신나게 살자 / 멋있게 살자 / 져주면서 자

banghee.lee

OTP

□ Save ID

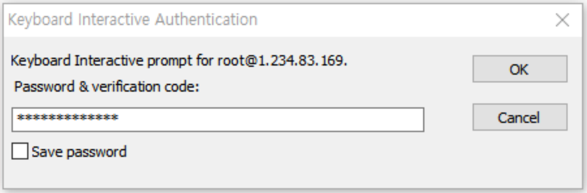
KOR

LOGIN

Copyright(C) 2012 SEYUNCNS Co.,Ltd.

3 alternative(new password)

By combining the password and the OTA key, a new OTA is generated and applied for each OTA key generation cycle (ID/PW+OTA)


Keyboard Interactive Authentication

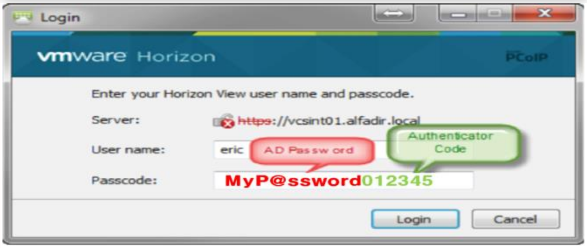
Keyboard Interactive prompt for root@1.234.83.169.

Password & verification code: **************

OK

Cancel

□ Save password


Login

vmware Horizon

PCoIP

Enter your Horizon View user name and passcode.

Server: https://vcsint01.alfadir.local

User name: eric

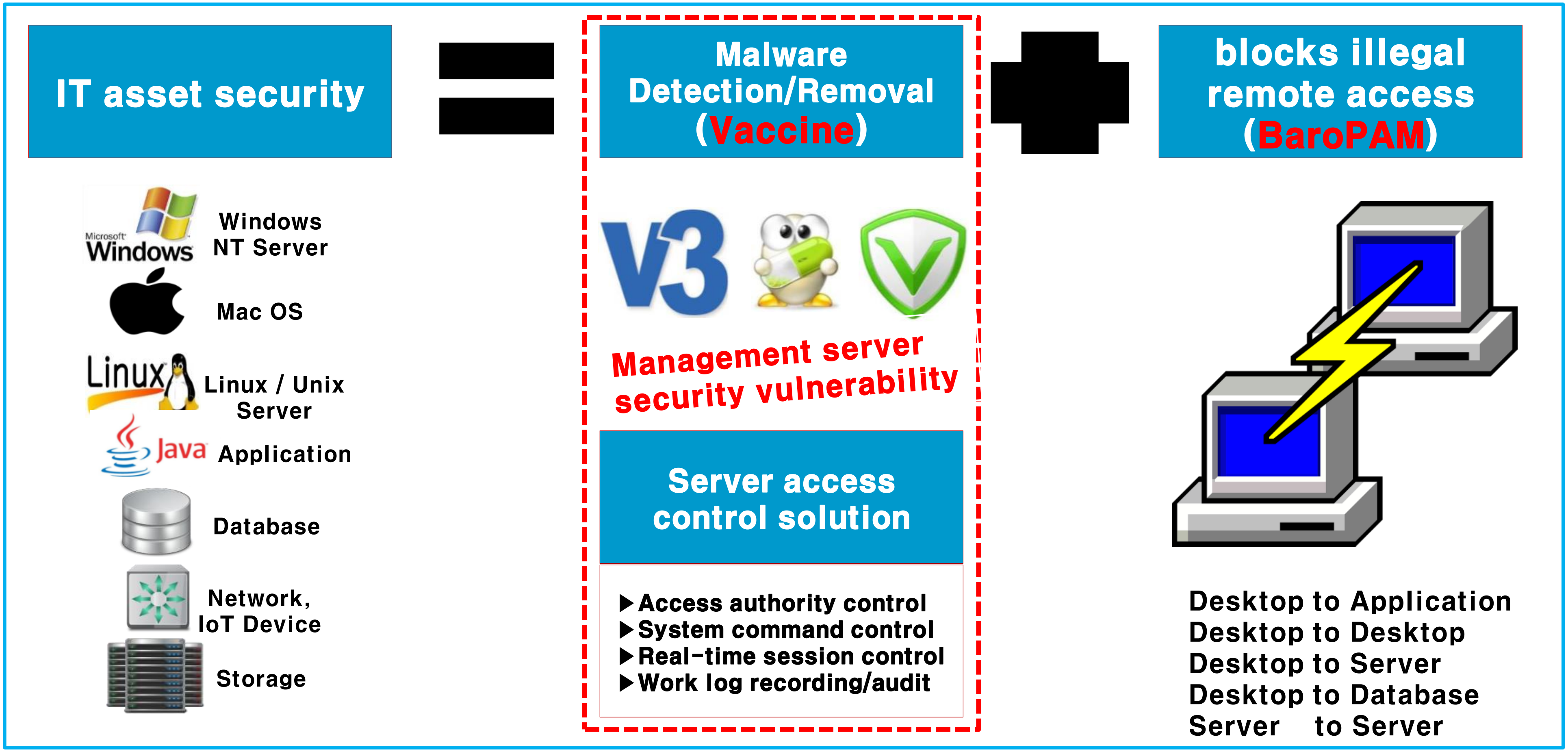
Passcode: MyP@ssword012345

Login

Cancel

8. Enhanced security

The combination of the vaccine solution/server access control solution and the BaroPAM solution creates a synergy effect that strengthens the security of information assets.



IT asset security

Malware Detection/Removal (Vaccine)

blocks illegal remote access (BaroPAM)

Windows NT Server

Mac OS

Linux / Unix Server

Application

Database

Network, IoT Device

Storage

Management server security vulnerability

Server access control solution

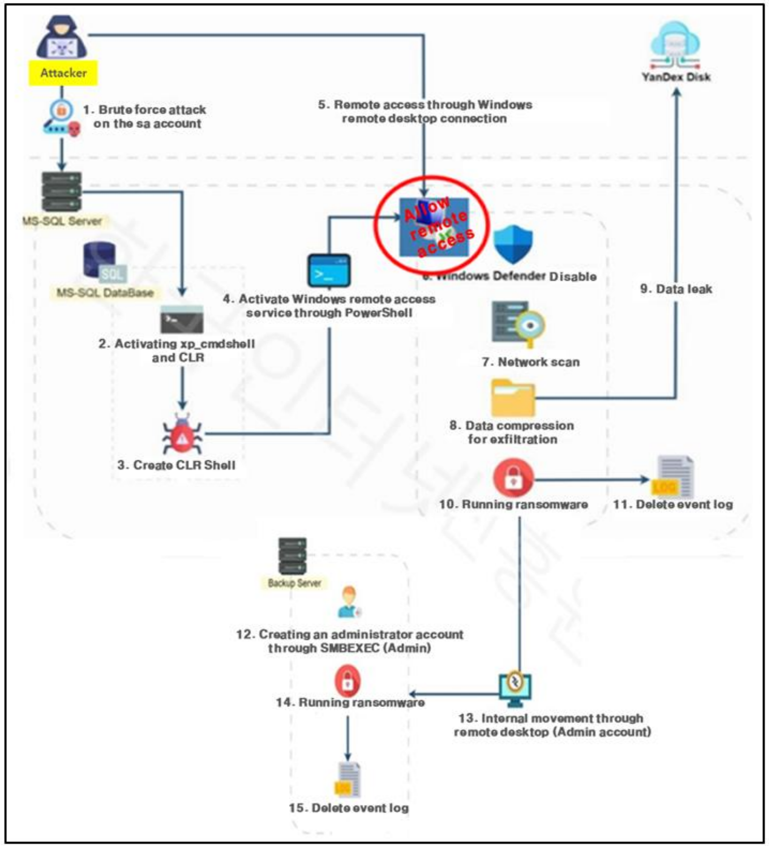
- ▶Access authority control
- ▶System command control
- ▶Real-time session control
- ▶Work log recording/audit

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

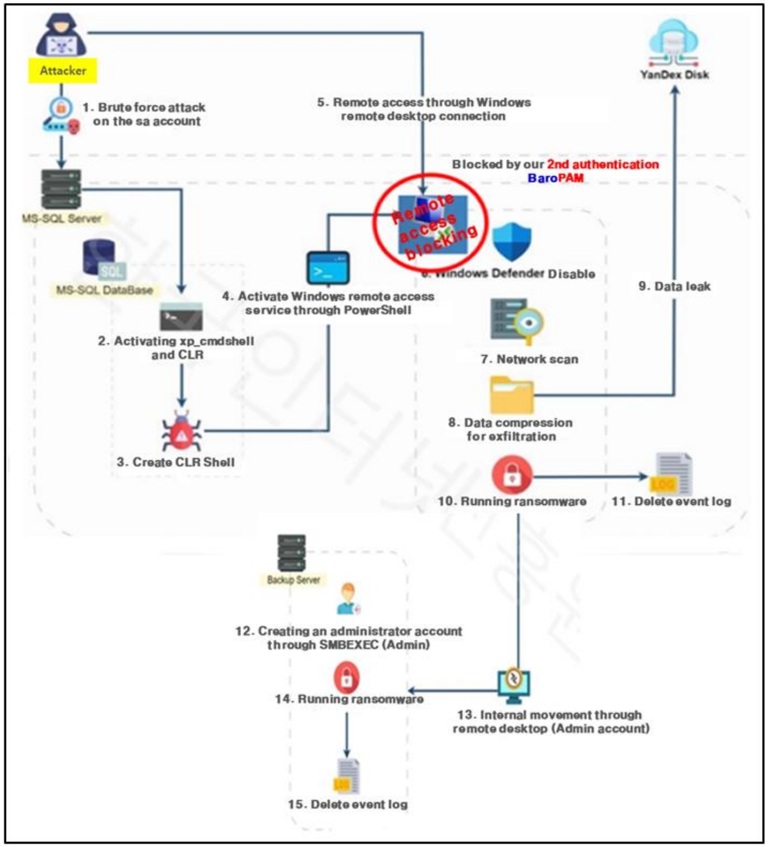
9. Hacking blocking case(Windows environment)

Hackers attempt to remotely connect via a remote desktop (RDP) connection after activating remote access services and elevating privileges via PowerShell through SQL injection attacks by brute-force attacks on accounts or scanning/exploiting hardware vulnerabilities such as networks and servers.

[Infringement incident occurred]


Attacker
1. Brute force attack on the sa account
5. Remote access through Windows remote desktop connection
YanDex Disk
MS-SQL Server
Allow remote access
6. Windows Defender Disable
MS-SQL DataBase
SQL
4. Activate Windows remote access service through PowerShell
9. Data leak
2. Activating xp_cmdshell and CLR
7. Network scan
8. Data compression for exfiltration
3. Create CLR Shell
10. Running ransomware
LOG
11. Delete event log
Backup Server
12. Creating an administrator account through SMBEXEC (Admin)
14. Running ransomware
13. Internal movement through remote desktop (Admin account)
15. Delete event log

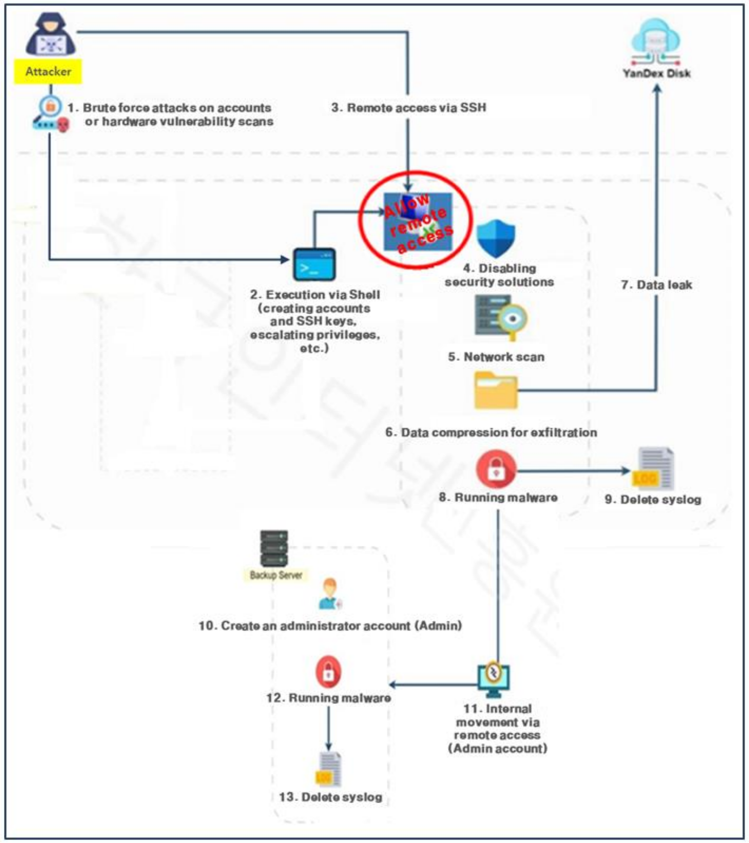
[Defense against infringement incidents]


Attacker
1. Brute force attack on the sa account
5. Remote access through Windows remote desktop connection
YanDex Disk
Blocked by our 2nd authentication
BaroPAM
MS-SQL Server
Remote access blocking
6. Windows Defender Disable
MS-SQL DataBase
SQL
4. Activate Windows remote access service through PowerShell
9. Data leak
2. Activating xp_cmdshell and CLR
7. Network scan
8. Data compression for exfiltration
3. Create CLR Shell
10. Running ransomware
LOG
11. Delete event log
Backup Server
12. Creating an administrator account through SMBEXEC (Admin)
14. Running ransomware
13. Internal movement through remote desktop (Admin account)
15. Delete event log

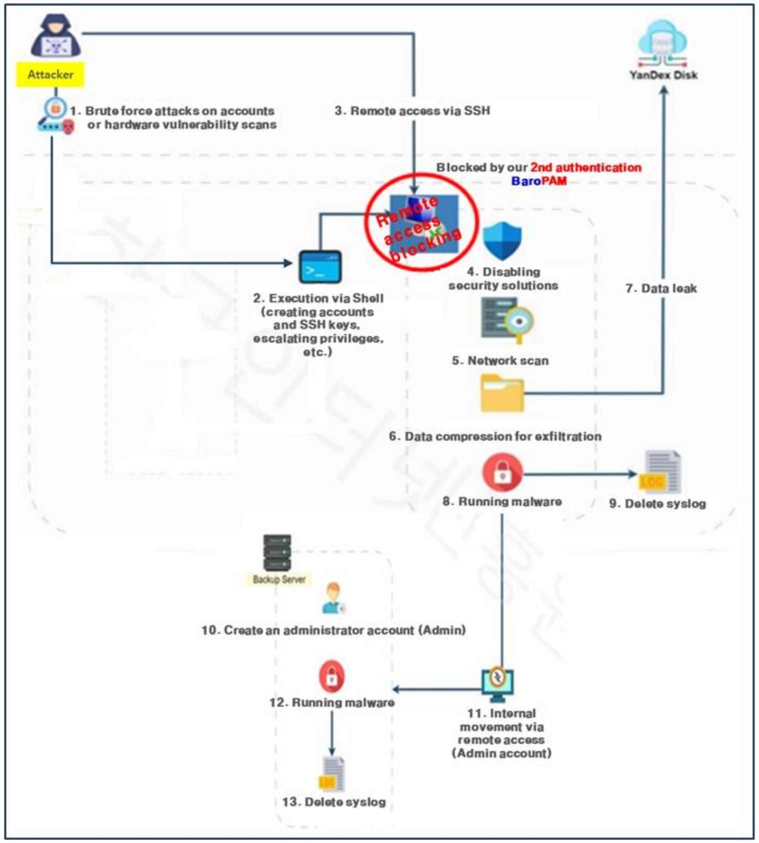
9. Hacking blocking case(Linux/Unix environment)

Hackers attempt to create accounts and SSH keys, elevate privileges, and bypass/remotely access accounts by brute-force attacking accounts or scanning/exploiting hardware vulnerabilities such as networks and servers to achieve remote code execution (RCE).

[Infringement incident occurred]


Attacker
YanDex Disk
1. Brute force attacks on accounts or hardware vulnerability scans
3. Remote access via SSH
Allow remote access
2. Execution via Shell (creating accounts and SSH keys, escalating privileges, etc.)
4. Disabling security solutions
7. Data leak
5. Network scan
6. Data compression for exfiltration
8. Running malware
9. Delete syslog
LOG
Backup Server
10. Create an administrator account (Admin)
12. Running malware
11. Internal movement via remote access (Admin account)
13. Delete syslog

[Defense against infringement incidents]


Attacker
YanDex Disk
1. Brute force attacks on accounts or hardware vulnerability scans
3. Remote access via SSH
Blocked by our 2nd authentication BaroPAM
Remote access blocking
2. Execution via Shell (creating accounts and SSH keys, escalating privileges, etc.)
4. Disabling security solutions
7. Data leak
5. Network scan
6. Data compression for exfiltration
8. Running malware
9. Delete syslog
LOG
Backup Server
10. Create an administrator account (Admin)
12. Running malware
11. Internal movement via remote access (Admin account)
13. Delete syslog

10. Concluding remarks

We need to acknowledge that "network separation" does not 100% prevent hackers from penetrating the network, and we need to prepare a security strategy assuming that hackers are already inside the network.

The reality is that this method, which is vulnerable to security, is still being used

- ▶Hackers' favorite application method among 2nd authentication: Gateway (+Proxy) method
- ▶The weakest authentication method among 2nd authentication: Text-based auth such as SMS and e-mail
- ▶Among the 2nd authentication, hackers use bypass technology and authentication method vulnerable to fatigue attacks: 2-channel authentication
- ▶Link method that is prone to phishing attacks: QR code method

The most important fundamentals for strengthening the security of information assets

- ▶How much risk do you want to distributed from a security perspective?
- ▶How to protect against data forgery and falsification during the authentication process?
- ▶How do we prevent account information theft and abuse?
- ▶How to block privilege escalation?
- ▶How to protect against browser automatic login?
- ▶How to defend against single point attacks?
- ▶How to block bypass/remote access?
- ▶How to defend against man-in-the-middle attacks?
- ▶How to protect against multi-factor authentication (MFA) bypass technology/fatigue attacks?

Above all, the best way to prevent information security incidents is to generate the authentication key yourself using the authentication key generation medium you own and enter it yourself.

The conclusion is not that "they introduced 2nd authentication", but rather "what kind of 2nd authentication was introduced" such as technology and security.

Ⅲ. Etc

1. About Us

General Information

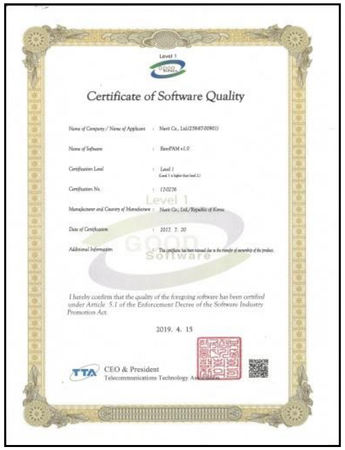
Company: Nuri IT Co., Ltd.
Establishment: January 19, 2018
Main business: 3-step authentication security s/w to strengthen the security of information assets
Address: #913, 15 Magokjungang 2-ro, Gangseo-gu, Seoul (Magok-dong, Magok Techno Tower 2)
Main items: BaroPAM, BaroCRYPT, BaroCollector, BaroFDS, BaroIDS
Advisory Professor: Youngsang Moon, Adjunct Professor, Department of Software Engineering,
Graduate School of Information Science, Soongsil University

「The strategy of the BaroPAM solution is to support decentralized multi-layer authentication to strengthen the security of information assets!」

History

2024.04 Integrating BaroPAM with Mattermost, OpenVPN, Palo Alto Networks Firewall, Beyondtrust Password safe, FreeRADIUS, Sophos SSLVPN
2023.04 Addition of biometric recognition (fingerprint, face recognition) function to BaroPAM app
2022.11 BaroPAM selected as secondary certification for KOICA cloud computing infrastructure construction and wireless network advancement service project
2022.11 BaroPAM is applied as secondary authentication when connecting to SecureLetter's Anyclick AUS via Wifi.
2022.06 Participating in BaroCARD (fingerprint recognition OTP card) in the 2022 information security leading technology development support project
2022.05 TTA conducts SW interoperability testing of Hamonikr OS and BaroPAM products
2021.07 BaroPAM v1.0 procurement
2021.07 BaroPAM selected as the 2021 security solution (SECaaS) supply pool registration solution
2021.04 BaroPAM integration with Microsoft products such as Microsoft365, Power Apps, ERP, etc.
2020.09 Participation in BaroPAM in the field of 'K-non-face-to-face voucher platform', network and security solutions of the Ministry of SMEs and Startups
2020.09 In 2020, secondary authentication SW (BaroPAM) was supplied to the LG U+ government business network mobilization reference demonstration project.
2019.10 Supplied BaroPAM to the "Second stage establishment of government-wide data platform" project (309 public institutions)
2019.04 BaroPAM GS certification transferred from Nuri IT to Nuri IT Co., Ltd.
2019.03 BaroPAM copyright registration
2018.06 BaroPAM released for Windows
2018.01 Establishment of Nuri IT Co., Ltd
2017.09 BaroPAM app service launched
2017.07 BaroIDS (abnormal access detection and blocking) product launched
2017.07 BaroPAM V1.0 GS certification level 1 certification
2017.05 BaroCRYPT (encryption/decryption) product launched
2016.11 BaroPAM (Secondary Authentication of Information Assets) product launched
2014.04 Patent application (identity authentication payment system and method using OTP card)
2009.11 Company name changed to Nuri IT
2007.12 Wily Add-on module development
2006.03 Establishment of KPL Infotech

2. Software Quality Assurance(GS Certificate / Test Report /Patents)



Level 1

Certificate of Software Quality

Name of Company / Name of Applicant : Nurit Co., Ltd.(25887-00901)

Name of Software : BaroPAM v1.0

Certification Level : Level 1
(Level 1 is higher than level 2.)

Certification No. : 17-0276

Manufacturer and Country of Manufacture : Nurit Co., Ltd./Republic of Korea

Date of Certification : 2017. 7. 20

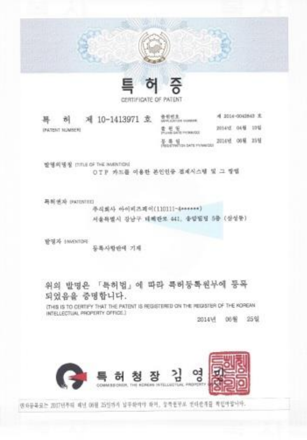
Additional Information : This certificate has been reissued due to the transfer of ownership of the product.

I hereby confirm that the quality of the foregoing software has been certified under Article 5.1 of the Enforcement Decree of the Software Industry Promotion Act.

2019. 4. 15

TTA CEO & President
Telecommunications Technology Association

July 2017
GS Certificate
Grade 1



특 허 증
CERTIFICATE OF PATENT

특 허 제 10-1413971 호
(PATENT NUMBER)

출원번호 (APPLICATION NUMBER) 제 2014-0042843 호
출원일 (FILING DATE YY/MM/DD) 2014년 04월 10일
등록일 (REGISTRATION DATE YY/MM/DD) 2014년 06월 25일

발명의명칭 (TITLE OF THE INVENTION)
OTP 카드를 이용한 본인인증 결제시스템 및 그 방법

특허권자 (PATENTEE)
주식회사 아이비즈페이(110111-4******)
서울특별시 강남구 테헤란로 441, 송암빌딩 5층 (삼성동)

발명자 (INVENTOR)
등록사항란에 기재

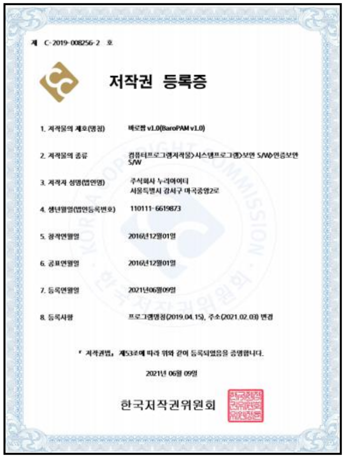
위의 발명은 「특허법」에 따라 특허등록원부에 등록되었음을 증명합니다.
(THIS IS TO CERTIFY THAT THE PATENT IS REGISTERED ON THE REGISTER OF THE KOREAN INTELLECTUAL PROPERTY OFFICE.)

2014년 06월 25일

특 허 청 장 김 영 민
COMMISSIONER, THE KOREAN INTELLECTUAL PROPERTY OFFICE

연차등록료는 2017년부터 매년 06월 25일까지 납부하여야 하며, 등록원부로 권리관계를 확인바랍니다.

June 2014
Patent Number:
No. 10-1413971



제 C-2019-008256-2 호

저작권 등록증

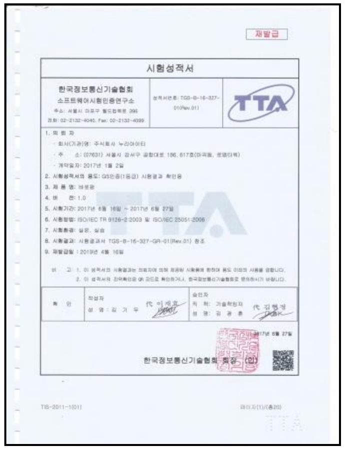
1. 저작물의 제호(명칭) 바로팜 v1.0(BaroPAM v1.0)
2. 저작물의 종류 컴퓨터프로그램저작물>시스템프로그램>보안 S/W>인증보안 S/W
3. 저작자 성명(법인명) 주식회사 누리아이티
서울특별시 강서구 마곡중앙2로
4. 생년월일(법인등록번호) 110111-6619873
5. 창작연월일 2016년12월01일
6. 공표연월일 2016년12월01일
7. 등록연월일 2021년06월09일
8. 등록사항 프로그램명칭(2019.04.15), 주소(2021.02.03) 변경

「저작권법」 제53조에 따라 위와 같이 등록되었음을 증명합니다.

2021년 06월 09일

한국저작권위원회

March 2019
Copyright
Registration
certificate



재발급

시험성적서

한국정보통신기술협회
소프트웨어시험인증연구소
주소: 서울시 마포구 월드컵북로 396
전화: 02-2132-4040, Fax: 02-2132-4099

성적서번호: TGS-B-16-327-01(Rev.01)

TTA

1. 의 뢰 자
- 회사(기관)명: 주식회사 누리아이티
- 주 소: (07631) 서울시 강서구 공항대로 186, 617호(마곡동, 로뎀타워)
- 계약일자: 2017년 1월 2일
2. 시험성적서의 용도: GS인증(1등급) 시험결과 확인용
3. 제 품 명: 바로팜
4. 버 전: 1.0
5. 시험기간: 2017년 6월 16일 ~ 2017년 6월 27일
6. 시험방법: ISO/IEC TR 9126-2:2003 및 ISO/IEC 25051:2006
7. 시험환경: 실온, 실습
8. 시험결과: 시험결과서 TGS-B-16-327-GR-01(Rev.01) 참조
9. 재발급일 : 2019년 4월 16일

비 고 1. 이 성적서의 시험결과는 의뢰자에 의해 제공된 시험품에 한하며 용도 이외의 사용을 금합니다.
2. 이 성적서의 진위확인은 QR 코드로 확인하거나, 한국정보통신기술협회로 문의하시기 바랍니다.

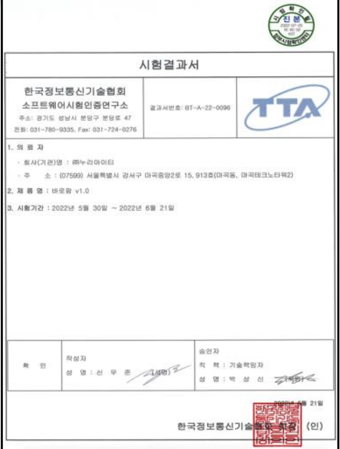
확 인	작성자 성 명 : 김 기 우 代 이재효	승인자 직 책: 기술책임자 성 명: 김 광 훈 代 김형정

2017년 6월 27일

한국정보통신기술협회 회장 (인)

TIS-2011-1(01) 페이지(1)/(총20)

July 2017
TTA Test Report



시험확인필
진본
2022-07-25
KST

시험결과서

한국정보통신기술협회
소프트웨어시험인증연구소
주소: 경기도 성남시 분당구 분당로 47
전화: 031-780-9335, Fax: 031-724-0276

결과서번호: BT-A-22-0096

TTA

1. 의 뢰 자
· 회사(기관)명 : ㈜누리아이티
· 주 소 : (07590) 서울특별시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)
2. 제 품 명 : 바로팜 v1.0
3. 시험기간 : 2022년 5월 30일 ~ 2022년 6월 21일

확 인	작성자 성 명 : 신 우 준 (서명)	승인자 직 책 : 기술책임자 성 명 : 박 상 신 (서명)

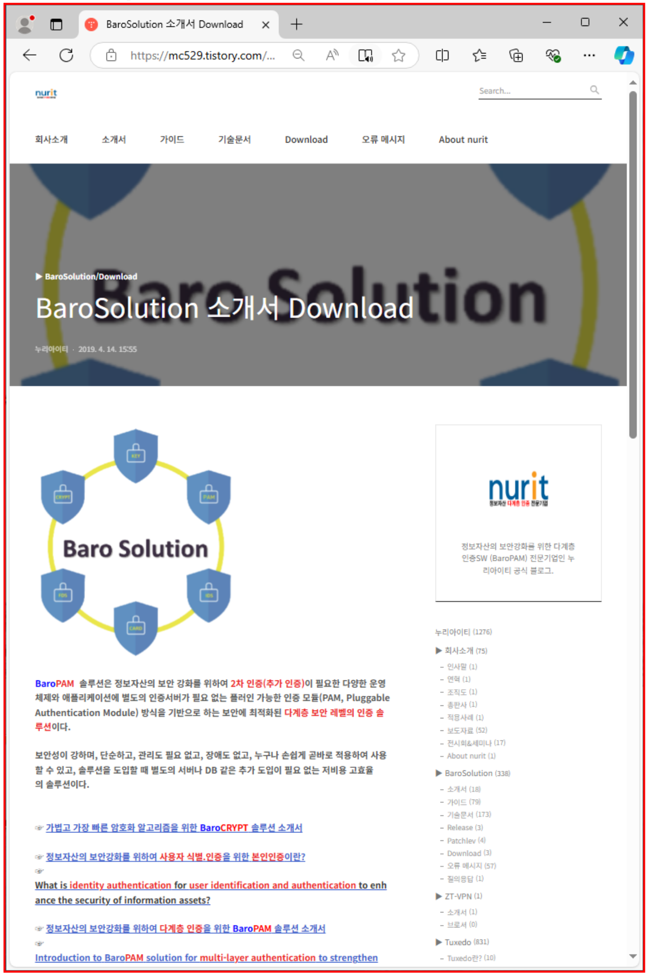
2022년 6월 21일

한국정보통신기술협회 회장 (인)

June 2022
Interoperability
test

3. BaroSolution Download

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



▶ BaroSolution/Download

BaroSolution 소개서 Download

누리아이티 · 2019. 4. 14. 15:55

BaroPAM 솔루션은 정보자산의 보안 강화를 위하여 2차 인증(추가 인증)이 필요한 다양한 운영 체제와 애플리케이션에 별도의 인증서버가 필요 없는 플러인 가능한 인증 모듈(PAM, Pluggable Authentication Module) 방식을 기반으로 하는 보안에 최적화된 다계층 보안 레벨의 인증 솔루션이다.

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 솔루션이다.

☞ 가볍고 가장 빠른 암호화 알고리즘을 위한 BaroCRYPT 솔루션 소개서

☞ 정보자산의 보안강화를 위하여 사용자 식별.인증을 위한 본인인증이란?
☞
What is identity authentication for user identification and authentication to enhance the security of information assets?

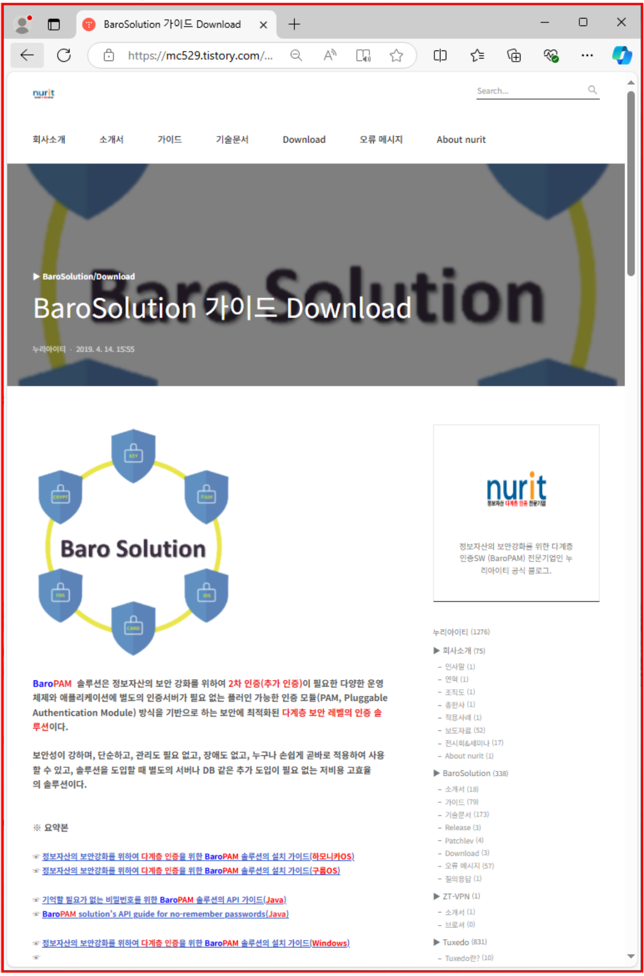
☞ 정보자산의 보안강화를 위하여 다계층 인증을 위한 BaroPAM 솔루션 소개서
☞
Introduction to BaroPAM solution for multi-layer authentication to strengthen

nurit
정보자산 다계층 인증 전문기업

정보자산의 보안강화를 위한 다계층 인증SW (BaroPAM) 전문기업인 누리아이티 공식 블로그.

누리아이티 (1276)
- ▶ 회사소개 (75)
  - 인사말 (1)
  - 연혁 (1)
  - 조직도 (1)
  - 총판사 (1)
  - 적용사례 (1)
  - 보도자료 (52)
  - 전시회&세미나 (17)
  - About nurit (1)
- ▶ BaroSolution (338)
  - 소개서 (18)
  - 가이드 (79)
  - 기술문서 (173)
  - Release (3)
  - Patchlev (4)
  - Download (3)
  - 오류 메시지 (57)
  - 질의응답 (1)
- ▶ ZT-VPN (1)
  - 소개서 (1)
  - 브로셔 (0)
- ▶ Tuxedo (831)
  - Tuxedo란? (10)

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



▶ BaroSolution/Download

BaroSolution 가이드 Download

누리아이티 · 2019. 4. 14. 15:55

BaroPAM 솔루션은 정보자산의 보안 강화를 위하여 2차 인증(추가 인증)이 필요한 다양한 운영 체제와 애플리케이션에 별도의 인증서버가 필요 없는 플러인 가능한 인증 모듈(PAM, Pluggable Authentication Module) 방식을 기반으로 하는 보안에 최적화된 다계층 보안 레벨의 인증 솔루션이다.

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 솔루션이다.

※ 요약본

☞ 정보자산의 보안강화를 위하여 다계층 인증을 위한 BaroPAM 솔루션의 설치 가이드(하모니카OS)
☞ 정보자산의 보안강화를 위하여 다계층 인증을 위한 BaroPAM 솔루션의 설치 가이드(구름OS)

☞ 기억할 필요가 없는 비밀번호를 위한 BaroPAM 솔루션의 API 가이드(Java)
☞ BaroPAM solution's API guide for no-remember passwords(Java)

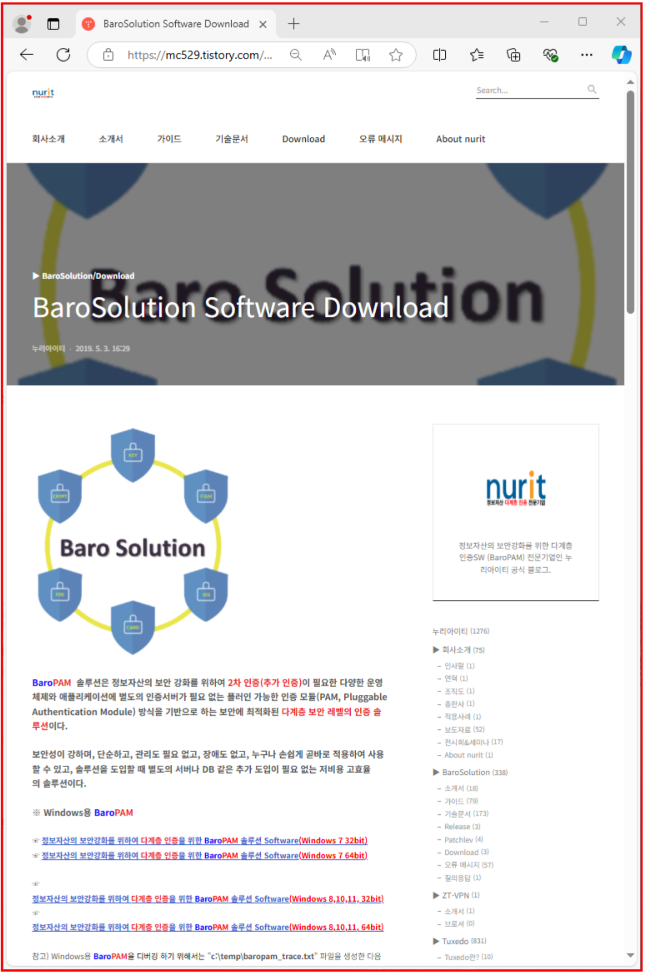
☞ 정보자산의 보안강화를 위하여 다계층 인증을 위한 BaroPAM 솔루션의 설치 가이드(Windows)
☞

nurit
정보자산 다계층 인증 전문기업

정보자산의 보안강화를 위한 다계층 인증SW (BaroPAM) 전문기업인 누리아이티 공식 블로그.

누리아이티 (1276)
- ▶ 회사소개 (75)
  - 인사말 (1)
  - 연혁 (1)
  - 조직도 (1)
  - 총판사 (1)
  - 적용사례 (1)
  - 보도자료 (52)
  - 전시회&세미나 (17)
  - About nurit (1)
- ▶ BaroSolution (338)
  - 소개서 (18)
  - 가이드 (79)
  - 기술문서 (173)
  - Release (3)
  - Patchlev (4)
  - Download (3)
  - 오류 메시지 (57)
  - 질의응답 (1)
- ▶ ZT-VPN (1)
  - 소개서 (1)
  - 브로셔 (0)
- ▶ Tuxedo (831)
  - Tuxedo란? (10)

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



▶ BaroSolution/Download

BaroSolution Software Download

누리아이티 · 2019. 5. 3. 16:29

BaroPAM 솔루션은 정보자산의 보안 강화를 위하여 2차 인증(추가 인증)이 필요한 다양한 운영 체제와 애플리케이션에 별도의 인증서버가 필요 없는 플러인 가능한 인증 모듈(PAM, Pluggable Authentication Module) 방식을 기반으로 하는 보안에 최적화된 다계층 보안 레벨의 인증 솔루션이다.

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 솔루션이다.

※ Windows용 BaroPAM

☞ 정보자산의 보안강화를 위하여 다계층 인증을 위한 BaroPAM 솔루션 Software(Windows 7 32bit)
☞ 정보자산의 보안강화를 위하여 다계층 인증을 위한 BaroPAM 솔루션 Software(Windows 7 64bit)

☞
정보자산의 보안강화를 위하여 다계층 인증을 위한 BaroPAM 솔루션 Software(Windows 8,10,11, 32bit)
☞
정보자산의 보안강화를 위하여 다계층 인증을 위한 BaroPAM 솔루션 Software(Windows 8,10,11, 64bit)

참고) Windows용 BaroPAM을 디버깅 하기 위해서는 "c:\temp\baropam_trace.txt" 파일을 생성한 다음

nurit
정보자산 다계층 인증 전문기업

정보자산의 보안강화를 위한 다계층 인증SW (BaroPAM) 전문기업인 누리아이티 공식 블로그.

누리아이티 (1276)
- ▶ 회사소개 (75)
  - 인사말 (1)
  - 연혁 (1)
  - 조직도 (1)
  - 총판사 (1)
  - 적용사례 (1)
  - 보도자료 (52)
  - 전시회&세미나 (17)
  - About nurit (1)
- ▶ BaroSolution (338)
  - 소개서 (18)
  - 가이드 (79)
  - 기술문서 (173)
  - Release (3)
  - Patchlev (4)
  - Download (3)
  - 오류 메시지 (57)
  - 질의응답 (1)
- ▶ ZT-VPN (1)
  - 소개서 (1)
  - 브로셔 (0)
- ▶ Tuxedo (831)
  - Tuxedo란? (10)

A password you don't need to remember!
BaroPAM will be with you.

Thank You!

www.nurit.co.kr
mc529@nurit.co.kr