USENIX Security Symposium 2025

Too Much of a Good Thing: (In-)Security of Mandatory Security Software for Financial Services in South Korea

Taisic Yun[1,2], Suhwan Jeong[2], Yonghwa Lee[1],
Seungjoo Kim[3], Hyoungshick Kim[4], Insu Yun[2], Yongdae Kim[2]

[1]Theori Inc., [2]KAIST, [3]Korea University, [4]Sungkyunkwan University

Can We Make Users Safer by Mandating Security Software?

Across the world, few governments have tried to secure users by installing SW on their devices.

China – Green Dam

China defends screening software

By Michael Bristow
BBC News, Beijing

China has defended the use of new screening software that has to be installed on all computers.

Every new computer in China will have the software installed

Foreign ministry spokesman Qin Gang said the software would filter out pornographic or violent material.

Critics have complained that it could also be used to stop Chinese internet users searching for politically sensitive information.

But Mr Qin, speaking at a regular press briefing, said China promoted the healthy development of the internet.

All computers sold in China - even those that are imported - will have to be pre-installed with the "Green Dam Youth Escort" software.

Kazahstan - Qaznet

Kazakhstan tries and fails to MITM all of its internet users with rogue certificate installation

Updated on Aug 3, 2021 by Caleb Chen

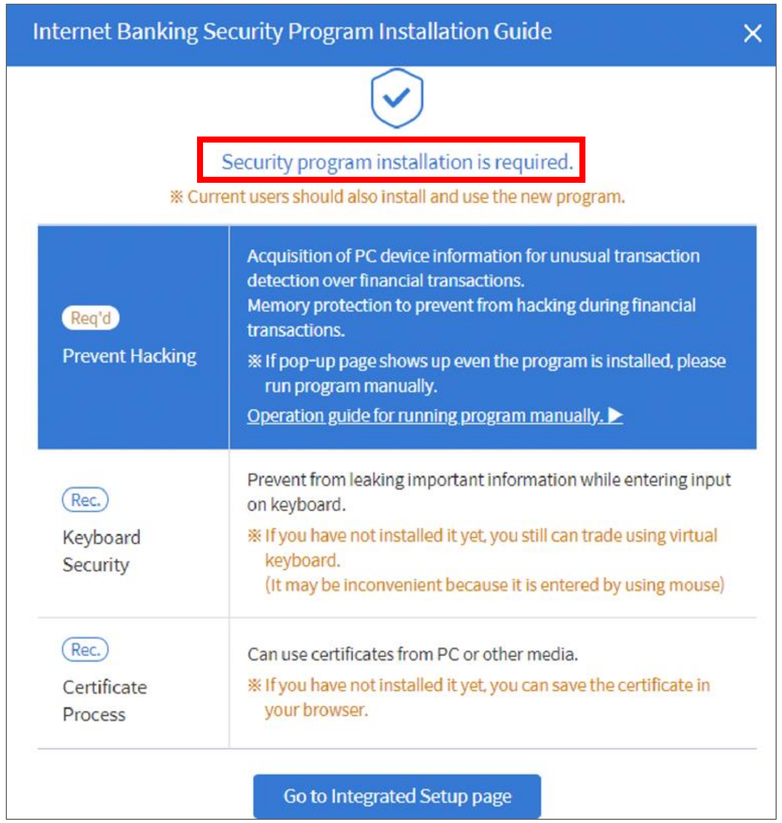
On July 17th, 2019, the government of Kazakhstan enacted a new cybersecurity measure that aims to spy on its citizens' internet traffic. Specifically, the Kazakh government ordered all of the internet service providers (ISPs) to force their customers to install a government-issued root certificate by Qaznet Trust Network on all of their internet accessing devices. If installed, this MITM cert allows the government to intercept, decrypt, analyze, then re-encrypt all browser encrypted HTTPS traffic in a country wide man-in-the-middle (MITM) attack. Since Wednesday, Kazakh internet users have been redirected to instructional pages asking them to install the new certificate. Forcing all of Kazakhstan's internet through one government issued certificate is a gargantuan privacy issue, but it is also a security issue. Any hacker that gets control of the Quaznet domain will be able to view the supposedly encrypted personal information from Kazakh internet users. Passwords, usernames, credit card information, all of it would be available unencrypted in such a scenario.

All of them were eventually withdrawn or blocked.

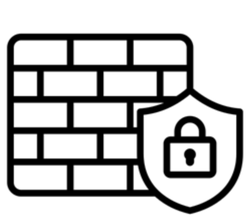
But what if one of them wasn't?

What Is Korea Security Application (KSA)?

Mandatory Security Software for Financial Services (and Public Services)

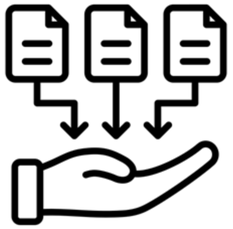


- Financial services (and public services) require system-level security features such as:



Firewall

Anti-keylogging



Anomaly detection

Certificate management

- **However, these cannot be provided through the browser — they require privileged access to the local system.**
- To enable them, users are required to install KSA before accessing financial or public services.

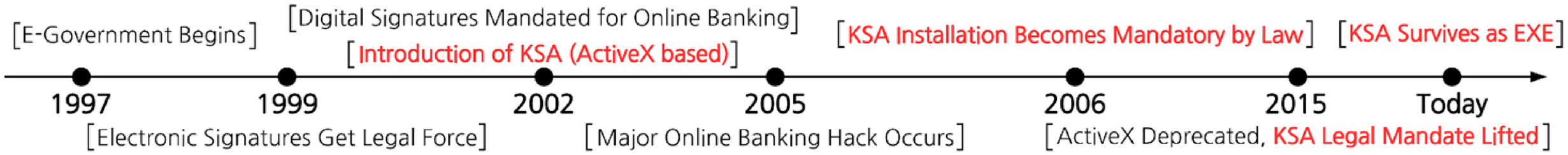
But… Why Go This Far?

KSA Was the Backbone of Korea's E-Government Expansion

- **Korea ranked #1 in e-Gov from 2010 to 2014.**
- **KSA enabled PKI-based authentication by allowing web access to local certificates.**
  - KSA (ActiveX based) was introduced in 2002 to support mandatory digital signatures for online banking — a critical part of Korea's early e-Government transition.
  - This infrastructure allowed Korea to safe and trusted digital public services.

UN E-Government Development Index

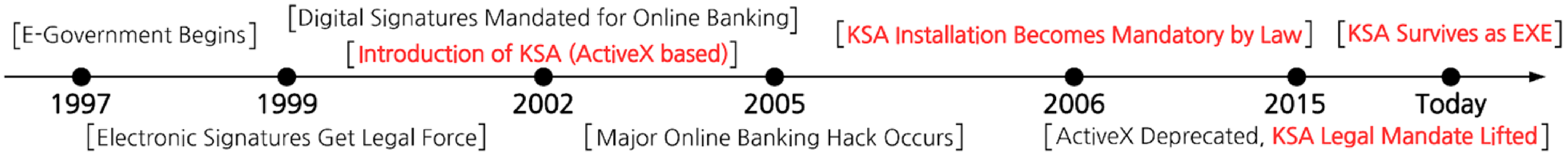
E-Government Development Index	2024	2022	2020	2018	2016	2014	2012	2010	2008	2005	2004	2003
Republic of Korea (Rank)	4	3	2	3	3	1	1	1	6	5	5	13
Republic of Korea (Value)	0.96789	0.95290	0.95600	0.90100	0.89149	0.94623	0.92832	0.87854	0.83170	0.87273	0.85745	0.74413



But… Why Go This Far?

From Legal Mandate to Persistent Requirement

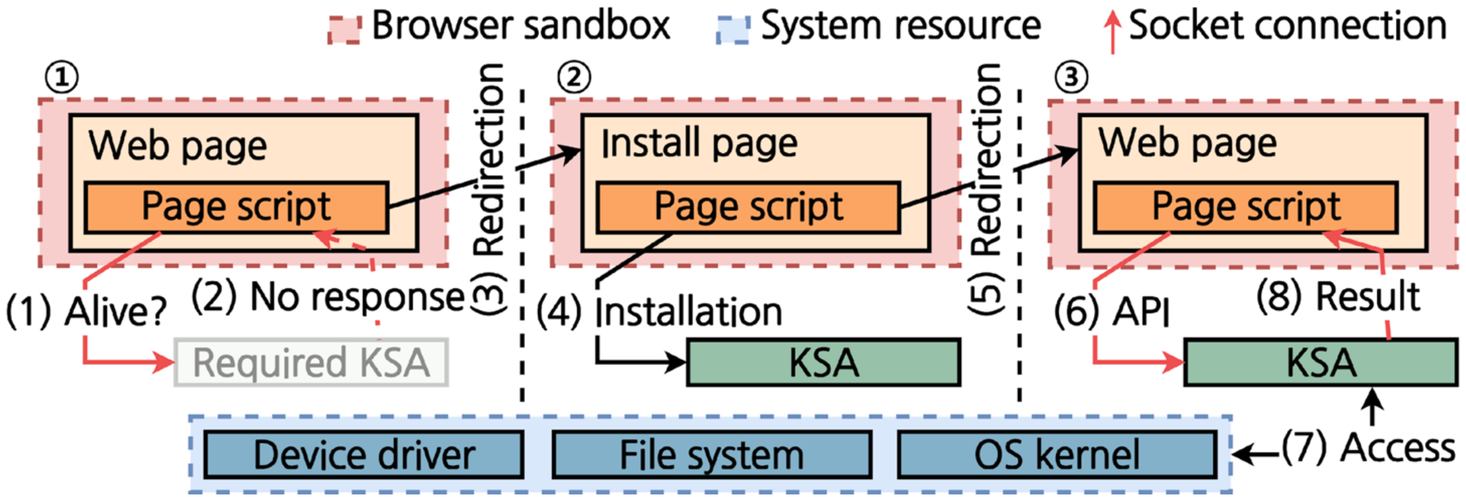
- Mandatory Installation by Law (2005 - 2006)
  - Law amended after a keylogging attack on online banking.
  - The new regulation explicitly required users to install various KSA for Financial services.
- **ActiveX Ends, Legal Mandate Lifted (2015)**
  - Microsoft officially phased out and discontinued ActiveX.
  - The Korean government repealed the legal requirement to install KSA.



So, Is KSA Gone Now?

No — It's Still Widely Used and Practically Mandatory.

- **Repackaged as a native executable (EXE)**
  - KSA runs as a local server, allowing web pages to access system resources beyond the sandbox.
- Still Required by Most Financial Services **– Users can't login without KSA installation.**



KSA was the backbone of Korea's E-Government expansion.

But is this what good security practice looks like?

Motivation

What If The Very Software We Trust to Secure Us... Opens The Door to Attackers?

- **Sweet Targets from  North Korea's Perspective**
  - 5 attacks targeting KSA in 2023
  - Supply chain attacks, compromising 61 institutions and over 10 million computers in 2023
- **By exploiting KSA, attackers can bypass browser-level protections and gain direct access to the system.**

NORTH KOREA-LINKED APT LAZARUS IS USING A MAGICLINE4NX ZERO-DAY FLAW IN SUPPLY CHAIN ATTACK

Pierluigi Paganini November 25, 2023

UK and South Korea agencies warn that North Korea-linked APT Lazarus is using a MagicLine4NX zero-day flaw in supply-chain attack

The National Cyber Security Centre (NCSC) and Korea's National Intelligence Service (NIS) released a joint warning that the North Korea-linked Lazarus hacking group is exploiting a zero-day vulnerability in the MagicLine4NX software to carry out supply-chain attacks.

Is KSA Secure?

The Risks of Korea’s Trusted Security Tool

- **What KSA Allows by Design**
  - Runs outside browser sandbox
  - Accepts requests from any website via localhost
  - Bypasses browser and web security standards
- **Why It’s Concerning**
  - Mandated in financial & public services
  - Used by tens of millions across Korea
  - One vulnerable product = Nationwide impact

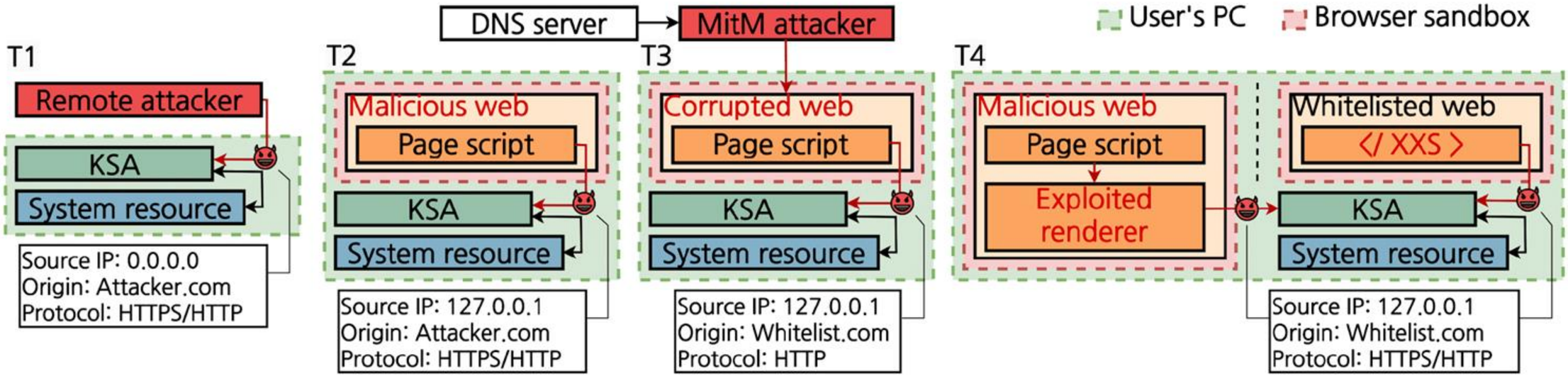
KSA’s widespread use and deep privileges call for serious security analysis.

Threat Models

Attackers Can Access KSA through Its Open Socket

We categorize threat models based on KSA's access control settings.

- **Threat Model 1 (T1) : Remote attacker**
  Binding: 0.0.0.0, Origin Check: Any, Protocol: Any
- **Threat Model 2 (T2) : Malicious web**
  Binding: 127.0.0.1, Origin Check: No, Protocol: Any
- **Threat Model 3 (T3) : Man-in-the-Middle**
  Binding: 127.0.0.1, Origin Check: Yes, Protocol: HTTP/TCP
- **Threat Model 4 (T4) : Origin spoofer**
  Binding: 127.0.0.1, Origin Check: Yes, Protocol: HTTPS/TLS



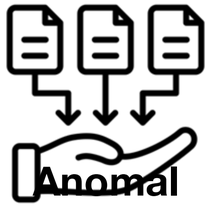
All KSA Products Are Vulnerable!

Mandatory KSA Used by Top-tier Banks

- We analyzed 7 mandatory KSA products used across 17 top-tier banks in South Korea.

Firewall

Anti-keylogging



Anomaly detection

Certificate management

- **Dataset & Identified Threat Models**

	Type				Access Control						Threat Model			
						Bind Address		Protocol Sec.						
Name	C	K	F	A	Localhost	Wildcard (+Filtering)	Wildcard	SSL	None	Origin Check	T1	T2	T3	T4
PRODUCT A	✓				✓			✓				✓		✓
PRODUCT B	✓				✓			✓		✓				✓
PRODUCT C	✓				✓			✓	✓	✓			✓	✓
PRODUCT D		✓			✓			✓		✓				✓
PRODUCT E		✓	✓	✓		✓		✓				✓		✓
PRODUCT F		✓	✓	✓		✓		✓				✓		✓
PRODUCT G				✓			✓	✓			✓	✓		✓

C - Certificate management, K - Anti-Keylogging, F - Firewall, A - Anomaly detection

Beyond Security: What KSA's Design Opens Up

Our Analysis Revealed Four Systemic Flaws Across KSA Implementations.

- **Inconsistencies in Threat Models between KSA and Web Browser**

Threat Modeling in Modern Browsers

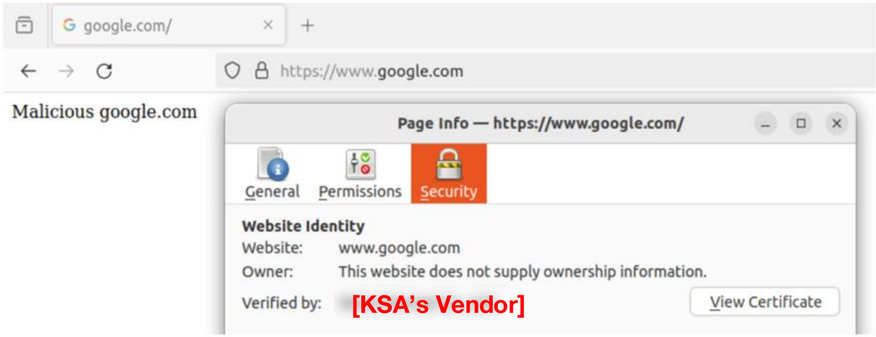
Type	Accessibility	Trust Level
Web Page	▲ High	▼ Low
Regular App	- Medium	- Medium
Admin Tool	▼ Low	▲ High

vs

Observed Trust Behavior in KSA

Type	Accessibility	Trust Level
Web Page	▲ High	▲ Equal to Admin
Regular App	- Medium	▼ Low
Admin Tool	▼ Low	▲ High

- **Disregard for the TLS Security Models**
  - KSA installs a custom root CA to enable TLS on 127.0.0.1 — bypassing browser trust.
  - Same root CA & key used for all users
    - One leak = Everyone exposed.
    - We extracted one vendor's private key in our analysis
  - Root CAs often remain after KSA uninstall



Beyond Security: What KSA's Design Opens Up

Our Analysis Revealed Four Systemic Flaws Across KSA Implementations.

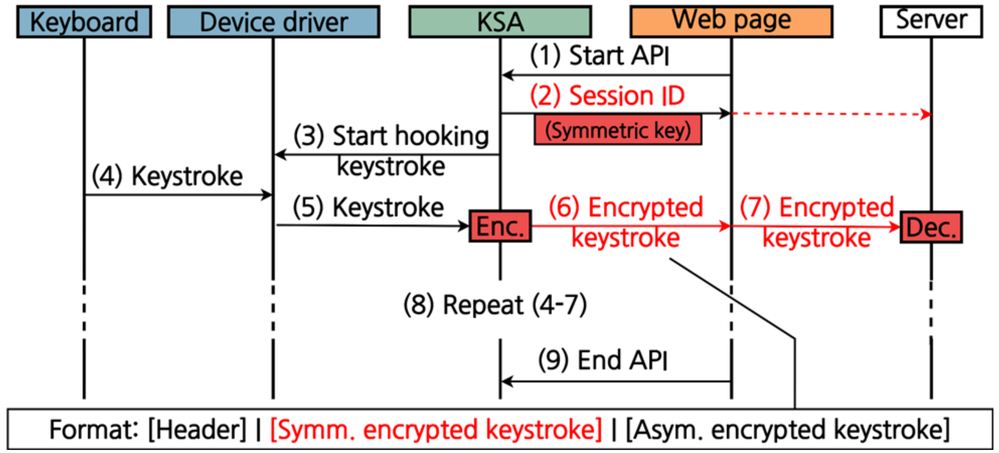
- **Violation of Browser Sandbox**
  - KSA is designed to bypass sandboxing — enabling web pages to run privileged actions.
  - Any structural flaw in KSA lets attackers exploit the system from the web — without browser exploits.
- **Enabling User Tracking**
  - KSA collects device and network identifiers for anomaly detection — but exposes them to any web page without user consent.
  - KSA Collects,

Network info: NAT and VPN IP, Mac Address
OS info: Version, Identification Number, Boot UUID
Hardware info: Various Hardware Serial Numbers
OS settings: Remote Access Permissions, Firewall

Case Studies: Exploiting KSA's Design Flaws

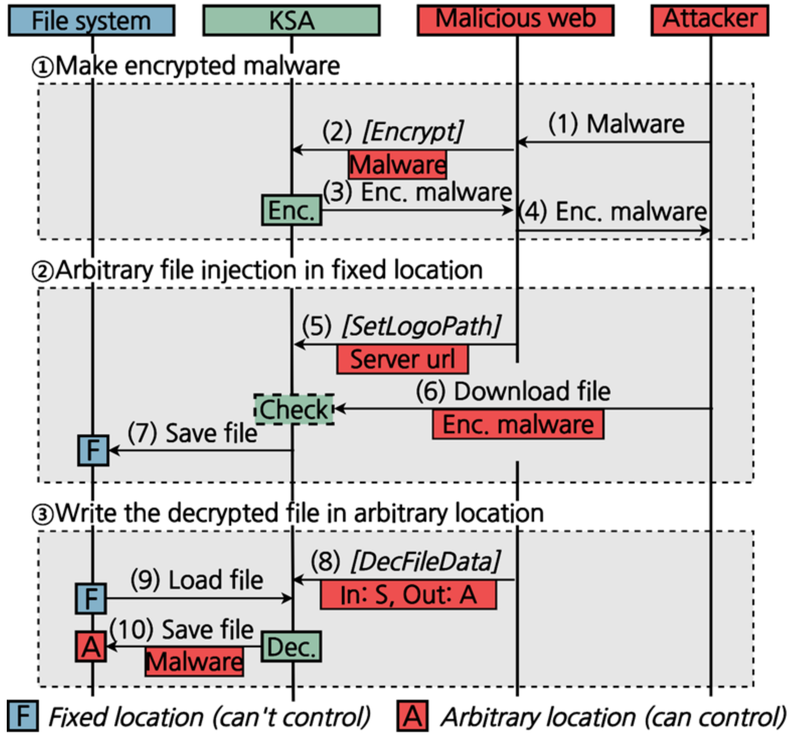
Based on The Four Systemic Flaws We Identified, We Discovered and Responsibly Disclosed 19 Vulnerabilities.

Keylogging



Demo Video

Remote Code Execution



Demo Video

KSA Remains, But No One Understands It

We Conducted a User Study to Understand KSA's Real-World Impact

- **KSA Is Still Everywhere:**
  - The legal mandate ended in 2015, but most financial services still require it today
  - For online banking, **97.35%** of users had KSA installed
  - Users had **9.1 KSA programs** installed on their PC (**max : 24**)
  - KSA's root CA certificates remained even after uninstalling KSA (**89.5%**)
- **Users Don't Understand KSA:**
  - Of all respondents, **59.25%** didn't understand what KSA does
  - Many users (**60.75%**) believed KSA is only active "on access" – but it always activate
  - A total of **20.75%** never attempted to uninstall KSA – software that lacks automatic updates.

Lessons Learned From The KSA Case

- Dangers of web security solutions controlling client devices
  - Security software should never bypass browser security boundaries to grant high-privilege access to the web.
- **Risks of solutions deviating from standards**
  - Security tools must align with standardized, peer-reviewed interfaces — or risk introducing unvetted attack surfaces.
- **Risks of mandating security solutions**
  - Mandates without structured maintenance can create lasting vulnerabilities.

Conclusion

So… Can We Make Users Safer by Mandating Security Software?

- KSA, mandated for online banking and public services in South Korea, was designed to enhance security.
  - But its flawed architecture introduced serious vulnerabilities.
- **Control ≠ Security. Design matters more than mandates.**

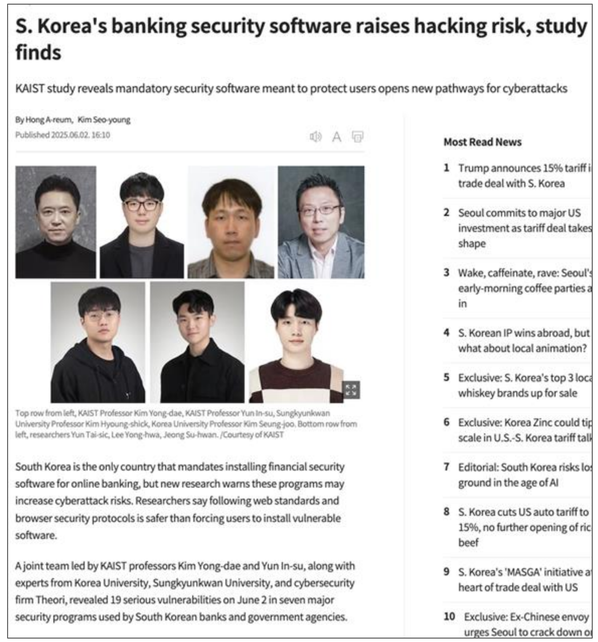
“Proprietary security software offers at best a modest improvement and certainly cannot provide the Holy Grail of a trustworthy user platform.
We have recommended that banks should minimize the use of external plugins.”

— Ross Anderson

What Has Changed After This Paper?

The Inertia of Mandated Insecurity

- **Public Attention — But Institutional Inertia:**
  - Our findings were widely reported in national media
  - Experts and the public voiced concern
  - But no technical or policy response followed



S. Korea's banking security software raises hacking risk, study finds

KAIST study reveals mandatory security software meant to protect users opens new pathways for cyberattacks

By Hong A-reum, Kim Seo-young
Published 2025.06.02, 16:10

Top row from left, KAIST Professor Kim Yong-dae, KAIST Professor Yun In-su, Sungkyunkwan University Professor Kim Hyoung-shick, Korea University Professor Kim Seung-joo. Bottom row from left, researchers Yun Tai-sic, Lee Yong-hwa, Jeong Su-hwan. /Courtesy of KAIST

South Korea is the only country that mandates installing financial security software for online banking, but new research warns these programs may increase cyberattack risks. Researchers say following web standards and browser security protocols is safer than forcing users to install vulnerable software.

A joint team led by KAIST professors Kim Yong-dae and Yun In-su, along with experts from Korea University, Sungkyunkwan University, and cybersecurity firm Theori, revealed 19 serious vulnerabilities on June 2 in seven major security programs used by South Korean banks and government agencies.

Most Read News

1 Trump announces 15% tariff i trade deal with S. Korea
2 Seoul commits to major US investment as tariff deal takes shape
3 Wake, caffeinate, rave: Seoul's early-morning coffee parties a in
4 S. Korean IP wins abroad, but what about local animation?
5 Exclusive: S. Korea's top 3 loca whiskey brands up for sale
6 Exclusive: Korea Zinc could tip scale in U.S.-S. Korea tariff tali
7 Editorial: South Korea risks lo ground in the age of AI
8 S. Korea cuts US auto tariff to 15%, no further opening of ric beef
9 S. Korea's 'MASGA' initiative a heart of trade deal with US
10 Exclusive: Ex-Chinese envoy urges Seoul to crack down o

- **A System Too Deeply Embedded:**
  - KSA is tied into critical infrastructure: banking, government services, and legacy systems
  - Vendors, banks, and regulators have little incentive — or mechanism — to act

What began as a workaround became the default — and now, changing it is harder than living with it.

Thank You!

theori

SYSSEC KAIST

保安工學研究室
SANE LAB
Security Assessment & Engineering
SECURITY BY DESIGN