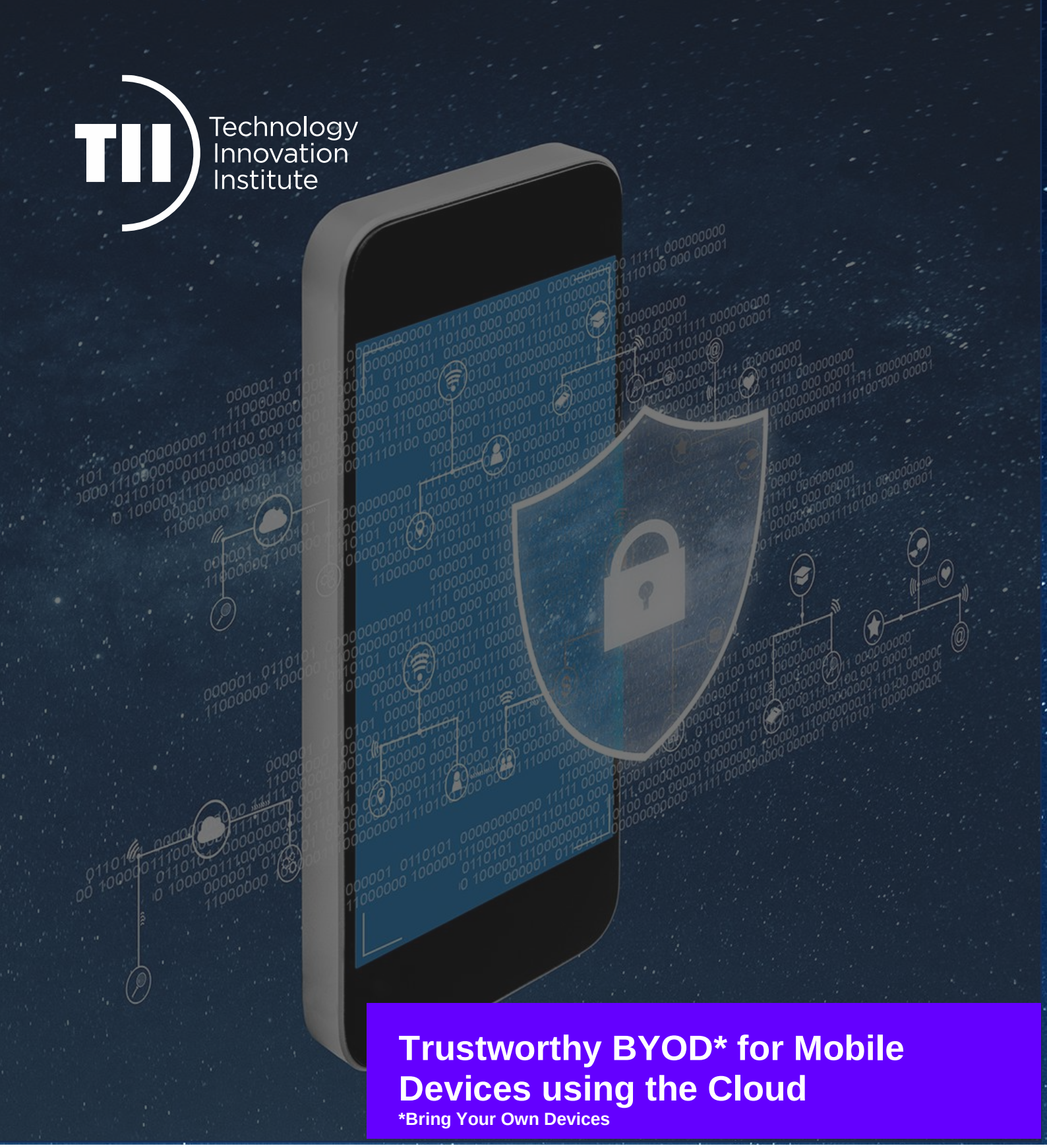
Technology Innovation Institute



Trustworthy BYOD* for Mobile Devices using the Cloud

*Bring Your Own Devices

tii.ae

Abstract

Existing approaches to mobile security leave many gaps, gaps that new, Virtual Mobile Interfaces (VMIs) could close. VMIs are analogous to Virtual Desktop Interfaces (VDIs)—instances of computer operating systems running in the cloud. Cloud-based Virtual Mobile Interfaces promise enterprises and governments the highest level of security while simultaneously reducing the need for employees to carry multiple mobile phones.

Furthermore, VMIs reduce the risk of data leakage, mitigate the impact of lost or stolen phones, and provide additional protections for data and apps running on the phone. The approach employs a novel Zero Trust approach that spans multiple subsystems running on both phone and cloud.

This new architecture promises a wider security perimeter and simpler management than existing mobile security tools. It also provides better security than current mobile virtualization tools.

Introduction

Government and enterprise mobile phones continue to be hacked, despite advancements in mobile security tools and technology. In 2023, Apple warned customers in more than 150 countries to beware of sophisticated attacks on their mobile devices, while Google warned billions of Android users to update critical vulnerabilities. Advanced hacking tools like Pegasus spyware[1] developed by companies like NSO group can covertly monitor calls, capture text messages, collect passwords, and track a users' locations.

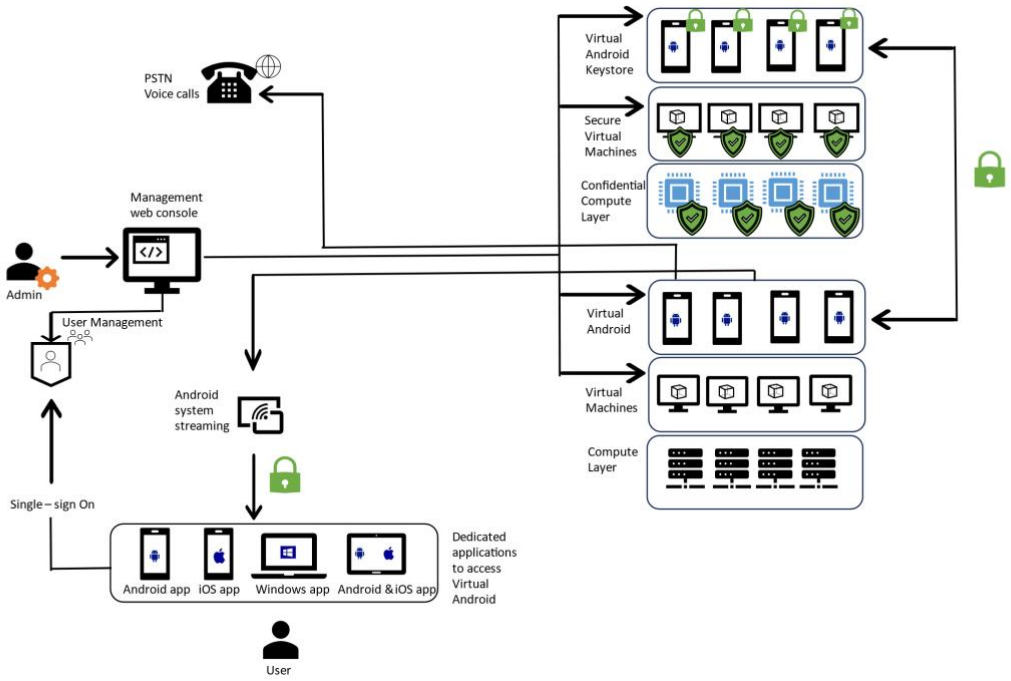
These concerns have driven the market for mobile threat defense tools, estimated at US $2.25 billion in 2022 with 22.95% annual growth.[2] Today's mobile security utilities commonly detect viruses, manage mobile devices, and protect mobile endpoints. Niche solutions supply a smaller market with costly hardened mobile devices that provide better protection but offer lower functionality and a poorer user experience.

Virtual Mobile Infrastructure (VMI) offers another layer of protection for sensitive apps and data outside conventional approaches. The approach is akin to the Virtual Desktop Infrastructure (VDI) widely used to protect conventional desktop workloads by connecting to hardened operating systems running in the cloud. Early VMIs include Canonical's Anbox Cloud and the Cophone virtual smartphone. Such implementations, however, focus on improving performance of compute-intensive apps like games, rather than increasing security.

The Technology Innovation Institute's Secure Software Research Center (SSRC) has pioneered a new VMI architecture optimized for trustworthy BYOD ("bring your own device") mobile phones, an architecture that plugs many vulnerabilities and gaps that existing tools leave open. SSRC reimagines security from the ground up, using Zero Trust principles. Its VMI lets users interact seamlessly with critical apps and process sensitive data in the cloud, all in a virtualized interface isolated from other apps and data running physically on the phone. This separation provides the highest levels of security while obviating any need for carrying multiple phones.

[1] "Mobile Phone Tracking." In Wikipedia, August 13, 2024. https://en.wikipedia.org/w/index.php?title=Mobile_phone_tracking&oldid=1240067467

[2] [1] "Mobile Threat Defense Market Size & Share Report, 2030." Accessed: Apr. 04, 2024. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/mobile-threat-defense-market-report



What SSRC has done

Research on ultra-secure mobile phone design inspired SSRC's remote mobile environment for corporations and organizations. Key innovations included custom hardware design, a secure software stack, and a secure remote update process that mitigates vulnerabilities in the software supply chain. Such expensive specialty devices have so far earned only limited adoption beyond the narrow market for highly critical applications.

A second line of research produced secure sleeves—add-on hardware that can be attached to an existing phone to isolate input and output, insulate data, and increase intrusion resistance. This allowed users to run less secure apps in a more secure environment to extend their functionality. Again, however, the solution requires dedicated hardware and software, with the concomitant expensive maintenance.

Early users of dedicated, high-security mobile devices complained that their app ecosystems were too limited. The customers asked for more functionality—like access to popular productivity apps—without opening security boundaries. TII's SSRC realized that the future of mobile computing and communication lay in leveraging SSRC's research on security-enhanced hardware and software supply chains, turning this experience into a more scalable, more cost-effective cloud virtualization approach.

Background
Evolution of the concept

Ultra Secure

- Limited applications
- Primarily Internal Trusted applications
- "Paranoid" security levels
- Government Entities
- Users generally carry 3 phones
- Limited reach (too specialized)

Secure Sleeve

- Companion to Ultra Secure device
- Less trusted apps run on the sleeve
- Extends the functionality of Ultra Secure
- Requires Hardware and Software
- Expensive to maintain consumer electronics

Mobile Device Virtualization

- 2 phones in 1 hardware
- Allows to extend Ultra Secure use case
- Currently Difficult to achieve
- Very active focus for SSRC long term
- Still requires manufacturing HW
- Limited deployment scope

Meanwhile, other SSRC research also explored enhancing mobile security via device virtualization. Here, hypervisors manage one or more virtualized OSs running in isolated instances on the physical hardware. This is currently difficult to do, however, and requires specially designed and manufactured hardware, which has limited adoption and deployment.

Our early analysis determined that a more scalable approach would be to run virtualized Android instances in the cloud (rather than on the handset) and stream the interface to an app on standard Android and iPhone devices. The SSRC calls its VMI implementation “Android in the Cloud” (AiC). This new approach allows organizations to move away from physical device management approaches—the specialty solutions that require employees to carry multiple phones, each dedicated to one or a handful of specific functions.


TII
Technology
Innovation
Institute

Essential drivers for the new “Android in the Cloud” approach include:

Hardware: Remove hardware dependencies, especially requirements for designing, building & maintaining custom hardware.

Security: Move user data and applications *away* from the device. Retrieving data from a lost device is vastly more difficult that reclaiming it from a secure cloud.

Simplicity::Users no longer need to carry (and keep track of) multiple devices. Administrators no longer have to manage and replace complex inventories of specialized devices.

This new AiC VMI architecture allows remote connections from almost any Android or iPhone device to virtual cloud-based Android instances. These instances are mirrored to physical devices to look and feel like native apps. UI and touch interactions on the physical device are streamed to the virtual Android side. This approach also simplifies the administrative services for monitoring and controlling cloud resources and end users.

In the next phase of development, this new architecture was ramped up to include 10,000 simultaneous virtual Android instances, ensuring scalability and manageability. SSRC is also working on optimizations that improve performance and end-user experience during interactions with virtual Android sessions. More fundamentally, SSRC is also building its pillars of resilience and trust through a hardened, secured, robust, and security-vetted solution.

At the core of our proof of concept is WebRTC, the foundational open-source framework that revolutionized real-time communications. WebRTC optimizes performance and enhances user experience on mobile devices. It supports adaptive bitrate streaming and peer-to-peer connectivity to mitigate network latency, ensure smooth multimedia experiences, and reduce battery drain. This low-latency foundation minimizes delays and enhances responsiveness and user integration.

Organizations that adopt public or private cloud services require strong defense and security systems. A core driver of Android in the Cloud architecture was removing sensitive data from the physical device. Further investigation revealed, however, that the entire infrastructure—everything running on the device and on the cloud—must be secured, resilient, and protected against attacks from whatever sources. Threats include assaults on the public cloud, on applications running on the physical device, on applications running on the virtual Android instance itself, on the cloud hosting environment, or on administrators' access privileges.

The development focus has moved to ensuring security and resilience via a novel user-data protection mechanism and a virtual Android secure-boot solution. These build on protections afforded by standard security systems surrounding authentication, access control, Zero Trust server component policies, and integrity mechanisms—all continually validated by third-party penetration testing.

Builders of secure solutions must regularly find the appropriate trade-offs between security, usability, and performance. Although it will never be possible to guard against all threats or all types of threats, the SSRC approach shows how a new architecture can strike a better balance—epitomized by BYOD's consolidation of multiple devices into one, eliminating a common source of complexity and frustration that reduces productivity and saps motivation.

Current enterprise mobile security landscape

Here is a high-level view of existing enterprise security approaches and some of their current limitations when compared to a VMI Zero Trust approach:

- **Mobile Antivirus detects and removes mobile malware using code signatures and behavioral analysis.** Reactive. Relies on experience with known threats and struggles against zero-day attacks. They are also limited by mobile OS restrictions, especially on iOS, which hinders deep scanning. This can allow malware to hide. Despite false positives and performance impacts, the most significant security threat arises from user behavior, such as clicking suspicious links or downloading from untrusted sources, which can bypass antivirus measures entirely.

- **Mobile Device Management (MDM):** Centralizes management and updates for enterprise mobile devices. There is limited control over personal devices, particularly BYO devices, risking diversion or loss of corporate data touched by individual apps. MDM solutions may not safeguard against phishing attacks and jailbroken/rooted devices, leaving vulnerabilities like zero-day attacks.

- **Mobile Endpoint Protection (MEP):** Improves security and data management when interacting with enterprise apps. MEP solutions impose performance penalties, false positives, and limited visibility, compromising overall security efficacy. Mobile OS restrictions may hinder MEP's ability to scan deeply for malware hidden within apps.

- **Mobile Threat Defense (MTD):** Enhances protections against known mobile attack tactics and techniques. MTD background operation can drain the battery and slow down devices. It may also incur high licensing fees and increase costs of managing and maintaining the system. Not all MTD solutions work with every device, OS, or app. They can also introduce privacy concerns.

- **Hardened Phones:** Depends on specialized mobile devices hardened across the chip, operating system, and application supply chain. Hardened phones increase security measures at the expense of features, app selection, and ease of use. They come with a steeper learning curve, higher cost, limited availability, and potential compatibility issues.

- **Virtualized Mobile Infrastructure (VMI):** Enhances the mobile experience for less capable hardware using virtualized OSs running in the cloud. Early implementations focused on performance rather than security.

- **SSRC Android in the Cloud (AiC):** Zero Trust approach to VMI enhances the resilience and security of data, apps, mobile hardware, and cloud infrastructure.

Closing the hardware vulnerability gap

Existing tools (other than expensive hardened phones and SSRC's AiC) provide minimal protection against numerous hardware vulnerabilities. The AiC environment ensures a secure separation of vulnerable apps and data from the physical device, shielding information assets against adverse impacts from the virtualized environment. SSRC's VMI safeguards the AiC environment against disruptions originating on the device or hardware side. This isolation, separating the AiC instance from the physical device, enhances overall security, ensuring that issues in one do impair the other.

Here are some common hardware vulnerabilities, and how AiC combats them:

- **Baseband Vulnerabilities**: Can be exploited for unauthorized access control. AiC uses a virtual instance to reduce the risk of exploitation, since the baseband functionality is not present in a cloud environment.

- **Wireless Communication Protocols:** Wi-Fi and Bluetooth attacks exploit implementation weaknesses. AiC uses secure connections and protocols whenever it accesses a virtual mobile instance, reducing the risk of wireless data diversion.

- **USB-Based Vulnerabilities:** Improperly managed USB connections can open mobile devices up to malware. AiC cloud virtual mobile instances are accessed remotely and isolated from any direct USB connection, reducing the attack surface exposed to these assaults.

- **SIM Card Vulnerabilities:** Security flaws in physical SIM cards can be exploited to gain unauthorized access to the device or its network. Cloud virtual mobile instances are isolated from these vulnerabilities.

- **Memory Vulnerabilities:** Buffer overflows, data leakage, and other memory-related vulnerabilities can compromise a device's security. In AiC, the virtual cloud mobile instance is again isolated from the host on which the AiC is running. Cloud providers implement security measures at the hypervisor level to prevent unauthorized access, secure memory allocation, and protect against potential memory-related attacks.

- **Processor Vulnerabilities:** Flaws in microprocessor design can leave sensitive data wide open. A cloud-based virtual mobile instance benefits from cloud-provider efforts like secure boot and firmware integrity, firewall/network security rules, antivirus protection, intrusion detection and prevention systems (IPDS), encryption and secure communication protocols such as TLS and VPN, and security monitoring and logging

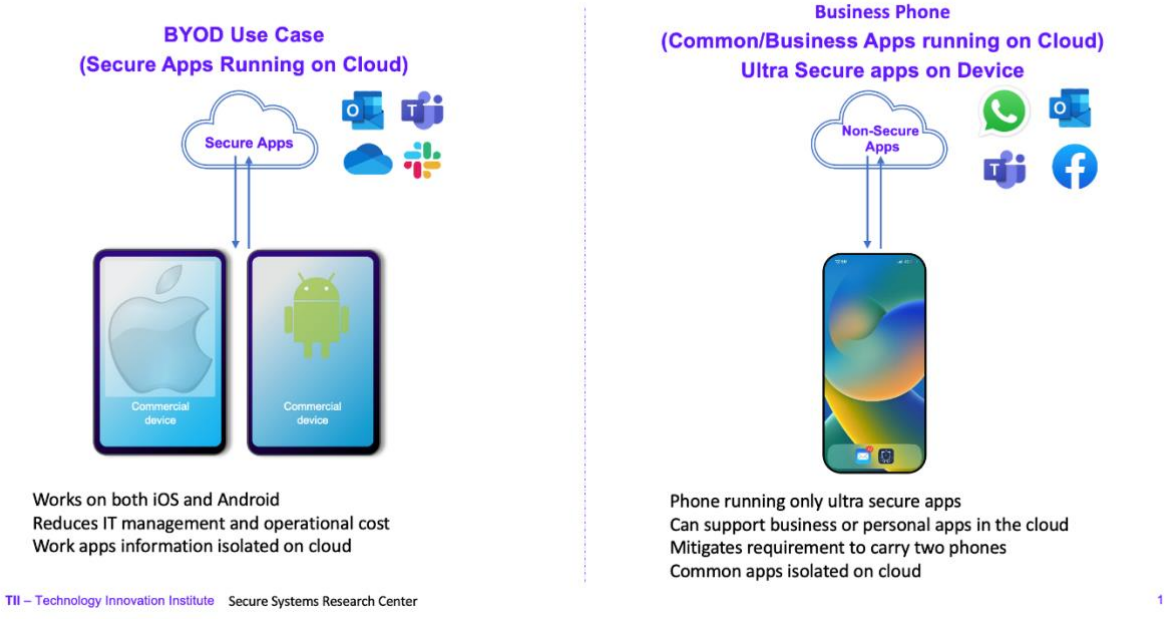
- **Device Loss or Theft:** Losing a phone exposes data and could allow attackers to bypass security measures like PINs or passwords. AiC revokes keys and certificates after a user reports an incident. This is crucial for maintaining the security of the cryptographic system and preventing unauthorized access.

Deep dive into the essential elements of the AiC solution, benefits, and roadmap

SSRC is developing a core architecture to support two complementary approaches for enhancing mobile security:

1. Secure applications running in virtual Android instances on personal mobile devices. AiC protects against vulnerabilities on physical devices—and the applications and software that run on them—for the BYOD use cases mentioned above. The same AiC infrastructure could also be extended to Virtual Desktop Infrastructure (VDI) use cases, supporting secure mobile access from workstations. The BYOD use case aligns better with mainstream adoption from operational, financial, and security perspectives. In this use case, SSRC's work has covered reducing both possible attack opportunities and attack surfaces in the system. It also reduces the impact when an attack does occur.

2. Personal applications running in a virtual Android instance on enterprise or custom secure mobile hardware. AiC protects hardened devices from vulnerabilities of consumer apps running in a virtual OS. This protection allows employees to access less secure mainstream application environments and run existing mobile apps safely isolated in the cloud.




TII
Technology
Innovation
Institute

Security hardening and protection mechanisms must be tailored to these different scenarios. Since there are far more consumer-grade than high-security devices on the market, much of the work has focused on protecting secure VMI in the host environment and insulating them and existing devices.
The hosting environment and administration functions must also be protected in both scenarios. A certain level of trust in the hosting environment will always be a consideration. Additional security hardening developed by SSRC reduces risks posed by an unfriendly hosting provider or administrator—a danger only occasionally acknowledged by many public cloud services. SSRC is working to make the AiC server platform-agnostic—equally ready to run on Azure, Google Cloud Platform, or on-premises. There are also efforts to support use cases whose remote functionality is available only at certain times or in certain locations. It may also be necessary for some applications or data to be available one-time-only. Or remote functionality may be made available only with additional authorization.

Essential components of the AiC architecture include the following:

Client: GALA (Generic Android Look-Alike), an app installable on iOS, Android, Windows, and Linux that can connect to the remote virtual Android instance.

Cloud backend: Virtual machines and isolated container systems to run individual Android Open Source Project (AOSP) instances.

Automated updates: Tools for maintaining a hardened version of the most recent AOSP for running Android virtual instances.

UI: Mirroring technology and protocols for interacting with remote Android view on the physical device.

Media: A secure bridge connecting user inputs from the physical device—including camera, audio, and Bluetooth peripherals—to the virtual Android side. This supports camera and audio use cases, such as Microsoft Teams calls.

Network: Connectivity mechanisms to allow multiple GALA applications to access their own virtual Android instance from anywhere in the world.

User management: A user-enrollment wizard for registering users and setting up physical devices.

Backend databases: Secured database infrastructure for protecting data on the backend.

Administration: Virtual Android and user-management functions with recovery features.

Scalability: Automation tools for creating and removing virtual instances.

Incident management: Tools for diagnostics and reports.

Mobile calling: A proof-of-concept, allowing cellular calling from the virtual Android instance.

Security features:
The following security features can be configured for various use cases:

- Novel end-to-end security for end-users' data.
- Android Secure boot option together with hardened AOSP.
- Hardened virtual machine environment to run isolated Android VD instances.
- Attestation mechanisms within cloud services to ensure trust.
- Session-specific certificates and authentications.

Here is a deeper analysis of some of the security features that SSRC has added to AiC, based on our third-party security reviews conducted throughout the project:

Isolation: Virtualization is a core mechanism allowing cloud services to efficiently use underlying resources. Virtualization also lends itself to isolation. Isolating server components and groups of virtual Android instances on dedicated virtual machines creates an additional barrier or layer between running code and applications. This makes it more difficult for malicious code or an attack to permeate the full system.

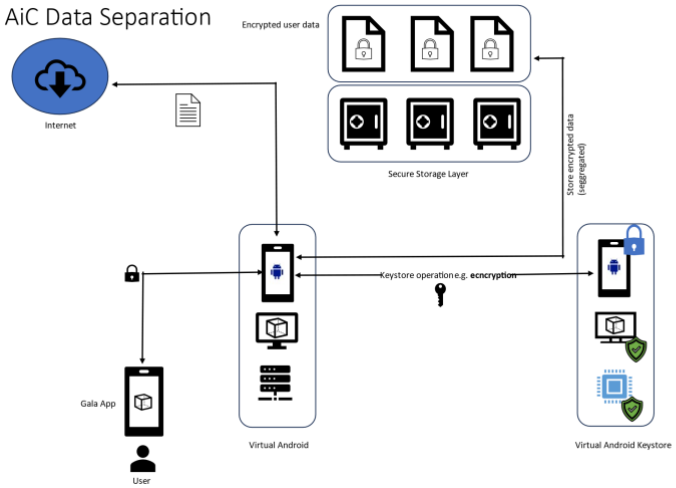
E2E: A novel end-to-end user data security implementation protects end user's data. This involves moving the user data related to the virtual Android *away* from the virtual Android instance itself, locating the information on another confidential node and adding an additional security layer.

Secure boot: An Android Secure boot option and a hardened AOSP protect the instance from boot-image compromise. This standard security mechanism locks the software to the hardware in commercial physical devices. AiC extends this concept to virtual instances.

Hardened OS: A hardened VM environment running isolated Android instances creates stricter isolation boundaries between the virtual machines in the cloud and the virtual Android instances. This limits the reach of any threats that do materialize.

Trust: Attestation mechanisms within cloud services ensure trust for the cloud backend components to keep rogue code from running.

User Testing: The AiC User Testing program has focused on optimizing deployment processes, improving user experiences with a focus on security, and enhancing the overall adoption of AiC. SSRC and its partners maintain an active testing program to ensure optimal usability without sacrificing security or innovative function.



Caption: Overview of AiC data separation architecture.

Closing the UX-security gap

Today, the highest level of security is available only by carrying a personal phone and an expensive, secondary phone with limited UI for complete isolation. Traditional ultra-secure phones generally have fixed operating systems with only a few, limited, security-hardened apps. Users, however, want *more* functionality, such as access to standard office suites and other productivity apps, without opening security hazards to other, less-sensitive apps.

Some of the critical aspects for improving the experience for users, administrators, and security teams include the following:

Efficient deployment: The User Testing program has successfully deployed virtual Android devices, even to larger user groups. This showcases the program's scalability and accessibility.

Enhanced user experience: Integrating the Native GALA application has significantly improved the user experience by seamlessly integrating with the host operating system. This positive integration contributes to a more user-friendly environment.

Data separation for maintenance: Separating user data has proven beneficial for maintenance tasks like recovery and upgrades. This feature contributes to the overall stability and reliability of virtual Android devices.

Compatibility with standard business applications: The User Testing program has proven its compatibility with standard business applications like Outlook, Slack, and OneDrive, making these essential tools easy to use on virtual Android devices.

Cloud security considerations

With the rising number of attacks on cloud infrastructure, it's also important to characterize how this security work can help protect against vulnerabilities in the cloud. In particular, our current approach helps reduce threats emanating from holes in administering roles and right, and in the cloud host processes. Part of the solution: Restricting virtual machine host and manager access to individual virtual machines and, thus, to individual Android-in-the-Cloud instances.

In addition to security features outlined above (novel E2E data security and isolation, hardened virtual machine environments, and attestation mechanisms) SSRC continues its efforts to fundamentally rethink a number of AiC business logic and infrastructure host processes, distributing them across client-server communication protocols to reduce the potential impacts of host vulnerabilities.

Ongoing work

The User Testing program has enjoyed several successes, particularly in deployment efficiency, user experience with business applications, and maintenance support. Significant questions remain, however—challenges related to security complexity, user adoption, network transitions, and entertainment app compatibility. These all require attention and further refinement to optimize AiC experience.

Complex security scheme: The User Testing program has successfully improved security through a complex security scheme and key management. However, some security measures can also degrade the user experience. Striking a balance between security and user convenience is a key consideration for improvement.

User adoption: User Testing revealed that users may revert to their legacy physical devices unless there are compelling reasons to use the virtual Android devices. Understanding and addressing user motivations is crucial to ensuring sustained adoption.

Latency: Ensuring a smooth user experience under different conditions can also pose a problem. During handovers between networks, addressing and minimizing transition disruptions should be a focus for improvement. It is just as important to understand, and minimize, the factors that increase lag times.

Entertainment App Compatibility: Some entertainment apps, particularly games, reportedly do not work correctly on cloud-hosted Android devices. Investigating and addressing these compatibility issues will provide better user experiences.
Mass deployment of this framework will also require ongoing work to future-proof the infrastructure, providing foundations from which to address unforeseen vulnerabilities in the post-commercialization phase. It will be necessary to keep up with Android releases, stay on top of vulnerabilities, and leverage improvements in AI and ML techniques to support these activities in the future. The Technology Innovation Institute is actively seeking commercial partners who are willing to undertake this more active side of product development and commercialization.

Complexity and Implementation Challenges:

The AiC architecture was developed to facilitate integration with existing IT infrastructure, compatibility with various devices and operating systems, and reduce network latency.

Our customer integration and pilot work are ongoing to uncover and optimize the following key integration points:

Network: AiC relies on a solid network connection between end users and servers for data transmission. Integrating AiC with existing network infrastructure requires optimizing network configurations and possibly upgrading network resources.

Resources: Integrating with existing IT infrastructure requires allocating resources for hardware, software licenses, training, etc.

Security: Integrating AiC with existing security policies and measures is crucial to protect sensitive data and mitigate cyber threats.

Change management: Implementing AiC within existing IT infrastructure often involves significant organizational change. Effective change management practices, including training programs and communications strategies, are essential to facilitate a smooth transition and minimize disruption.

Responsiveness: The AiC solution must meet performance expectations—in responsiveness, reliability, and scalability, among other areas. Ensuring optimal performance while integrating with existing IT infrastructure can be challenging, especially in heterogeneous environments.

UX: Maintaining a consistent and satisfactory user experience is essential for a successful AiC integration. This involves addressing factors such as network latency, application performance, and user accessibility within existing IT infrastructure.


TII
Technology
Innovation
Institute

Cloud virtualization comparison

VDI—virtual desktop infrastructure—was introduced by VMWare in 2006 and has since been essential in many enterprise and government IT strategies.[3] VMI—virtual machine infrastructure—is a relatively new concept. Canonical Anbox[4] and Cophone[5] were early innovators in this area. These implementations focus on improving performance of applications on less capable phones, such as supporting demanding GPU use cases for running graphics-intensive games.

In contrast, AiC approaches VMI with a strong focus on improving the end-to-end security of applications using a novel end-to-end user data security approach to safeguard personal data, incorporating Android Secure Boot and a hardened AOSP, along with a fortified virtual machine environment for isolated Android VD instances. Additionally, it employs attestation mechanisms within cloud services to establish trust.

The solution considers security-conscious scenarios for organizations that intend to allow users to run secure business applications on their personal phones. It also allows for greater control and flexibility on the administration and system-management side, through supporting tools and mechanisms for self-managing and controlling the entire system and its user base.

Other VMI solutions support use cases that demand little end-user knowledge or offer plug-and-play remote Android for individual users without organizational management support or tools. AiC has been optimized towards secure environments, where user management, scalability, usability, and data separation are critical for the organization's user base. SSRC’s Android in the Cloud positions itself for secure environments, where user management, scalability, usability, and data separation for the organization's user base are vital.

Conclusion

The VDI market reached $USD 19.5 billion in 2022 and is expected to grow 18.3% through 2028, owing to its ability to secure desktop workflows for enterprises and governments.[6]

The market is led by vendors like AWS, Citrix, Microsoft, Nutanix, Parallels, and VMware.

The market for virtual mobile infrastructure, such as AiC, is in its early days and virtually nonexistent, but it represents a tremendous opportunity for security, cloud, and mobile device management vendors to enhance their core offerings.

The Technology Innovation Institute comprises various groups, including the SSRC, and has a broad mandate to pioneer foundation technologies that promise to build a more sustainable and trustworthy future.

AiC is a foundational innovation that could form the basis for more secure, resilient, and reliable mobile computing services for enterprises, governments, and consumers.

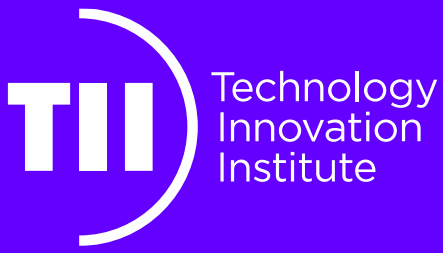
The SSRC has been making significant progress in demonstrating the architecture and solution.

It has also launched a comprehensive User Testing program, run both internally and with multiple partners.

AiC has achieved a technology readiness level (TRL) 4, suggesting it is ready for the next step of fine-tuning, product development, and wide-scale deployment by an industry partner.

The technology stack is currently ready for licensing for enterprise vendors with the internal engineering talent and business acumen to help bring this innovation to the mobile security mark.

[6] "Virtual Desktop Infrastructure (VDI) Market Outlook by 2030 with Demand | LinkedIn." Accessed: Apr. 04, 2024. [Online]. Available: https://www.linkedin.com/pulse/virtual-desktop-infrastructure-vdi-market-outlook/



tii.ae