MINDLINK

Whitepaper:

MINDLINK X ISC

Data-centric end-to-end encrypted chat for classified mission collaboration

Company
MindLink

Website
mindlinksoft.com

Executive Summary

MindLink's secure chat messaging platform enables real-time information sharing for even exceptionally classified topics in National Security and Defence. MindLink delivers a next-generation zero-trust architecture through a unique data-centric end-to-end encryption approach, integrating assured cryptographic infrastructure from Information Security Corporation.

Background

The ability to share information in real-time is vital to the success of those working in National Security and Defence (NS&D), facilitating situational awareness and mission collaboration to achieve decision advantage against our enemies. Chat messaging is a proven paradigm in such contexts, but current tools are archaic or generic and fall short in delivering the assurance needed for such classified work.

The "need-to-know" nature of classified information directly conflicts with that of the "need-to-share" for operational mission work. Balancing these needs whilst enabling the agility and scale required across such challenging mission environments demands innovative technology approaches.

World events continue to drive the pressing need to collaborate better and faster at even the most classified areas of the mission. Meanwhile, a heightened and more sophisticated threat landscape necessitates step-changes in deployed security architectures e.g. zero-trust, but this is difficult to achieve without tools engineered to address the specific threat models and operational constraints of the NS&D sector.

Recent incidents have highlighted that threats do not only come from external national actors – rather, insider threat is also a prevalent and serious concern. Snowden et al. have shown that backend access with nefarious intent to infrastructural IT (e.g. collaboration systems) can lead to major cross-sectional compromise of an entire agency's mission.

End-to-end encryption

In light of advancing threats and pressing mission needs, we seek to deliver a mission-ready collaboration platform incorporating a zero-trust architecture to mitigate insider threat, whilst supporting and enabling the sharing of even the most classified information. Ensuring chat messages are encrypted end-to-end between participant clients nullifies any implicit trust previously afforded to backend servers or databases, and to those administering such systems with privileged access rights.

With end-to-end encryption (E2EE), scraping of sensitive information from the chat system databases – through nefarious or legitimate access – will only yield encrypted data, with encryption keys being held elsewhere. Similarly, tampering with chat system permissions (e.g. to self-authorize oneself as a member of a sensitive chat room), will only provide access to encrypted messages – encryption keys are distributed and secured out-of-band using independent verification and authorization mechanisms.

Whilst end-to-end encryption is a common feature in modern chat applications, e.g. WhatsApp etc, the typical key-sharing protocols used to generate, distribute, and manage encryption keys between chat participants (e.g. MLS, Signal etc.) are purposefully designed to support consumer-based privacy, trust, and behavioural models. Motivated to ensure the absolute privacy of the individuals involved, the use of such E2EE mechanisms in an NS&D mission environment would critically break the overarching governance necessary for classified regulated work.

Further, designed for small groups of manually authorized users using specific user-owned devices, these protocols are fundamentally incompatible with the operational nature of mission work at scale. An alternative approach to E2EE is required for NS&D mission scenarios, able both to deliver the agility demanded of modern operations, and to preserve the sovereignty and regulatory requirements for even exceptionally classified information.

About MindLink

MindLink are specialists in real-time information-sharing for highly secure, mission-critical operations in NS&D. Their state-of-the-art collaboration platform is designed for the highest levels of classified communication for government agencies and partner nations.

Developed to requirements provided by the FVEY intelligence community, MindLink natively integrates classified information-handling practices using data-centric and ABAC-enabled security principles. It is currently deployed at scale in multiple air-gapped environments to enhance mission collaboration through secure real-time chat messaging.

About ISC

Information Security Corporation (ISC) specializes in the design, development, and marketing of cryptographic software that complies with all leading standardization and interoperability efforts. Addressing the confidentiality, authentication, and credential management requirements of both the government and private sectors, ISC products employ state-of-the-art conventional and public key cryptographic technologies.

ISC offers a family of COTS solutions for: the protection of data-at-rest and data-in-transit, the creation and management of (RSA/ECC/ML-DSA/ML-KEM) private keys and certificates; the secure sharing of sensitive data among communities of interest; and the use of role-based credentials in brokered authentication. Most recently ISC has focused on the design and development of systems that help simplify credential lifecycle management. ISC also offers cryptographic development kits (CDKs) for use by other publishers of security-enabled applications.

MindLink BRAINCHAIN E2EE

MindLink's innovative "BRAINCHAIN" end-to-end encryption system delivers a secure zero-trust chat messaging capability appropriate for classified mission operations at up to and above TOP SECRET. MindLink have partnered with ISC to leverage the ISC "DAS" group-based encryption platform as a trusted external component to facilitate encryption key sharing between groups of authorized users.

This unique solution uses cutting-edge hybrid cryptography and object-level encryption techniques to deliver a scalable and dynamic secure information sharing capability. This approach aligns with latest data-centric security and zero-trust roadmaps from NATO (i.e. ACP-240 level 3 maturity) and US DoD (e.g. NIST SP 800-207).

With BRAINCHAIN, symmetric encryption keys for each chat message are distributed as cryptographically sealed data to the chat room's participants by the MindLink platform, whilst access to an encryption key's raw data is only possible by invoking the DAS service, an operation that is performed independently by each user's client on-demand. This approach mitigates clear-text attack surfaces from the backend chat tiers whilst multiplying the number of decoupled systems that must be compromised in unison to obtain sensitive data.

The BRAINCHAIN architecture is rooted in organizational PKI and trusted IDAM and encryption infrastructure, leveraging typical existing assured enterprise subsystems to retain governance and oversight of information shared within the encrypted subcomponents. By centralizing key sharing and using data-centric labelling and ABAC techniques, the system scales to many thousands of participants in linear time, enabling mission agility and longevity through the automation of users' "need-to-know" entitlements.

BRAINCHAIN is built around a “communities of interest” isolation architecture, designed to support sub-compartment working in above TOP SECRET scenarios. Using standard strong cryptography algorithms (e.g. AES 256) and delivered as a stateless web-browser application, the system has been accredited to the highest levels of classified working by US IC agencies.

Concluding

MindLink and ISC have delivered a next-generation secure information sharing capability for classified mission scenarios in National Security and Defence. The “BRAINCHAIN” solution uses an innovative key-sharing approach using the principles of data-centric security, separation-of-concerns, and assured organizational infrastructure, to mitigate traditional chat system insider-threat attack surfaces whilst supporting and enhancing mission effectiveness and regulatory constraints.

BRAINCHAIN encryption is integrated as an optional capability within the MindLink product suite, deployable on air-gapped networks alongside ISC DAS, and with integration points to existing IDAM and PKI infrastructure. Please contact sales@mindlinksoft.com and sales@infoseccorp.com for more details on MindLink BRAINCHAIN and ISC DAS.