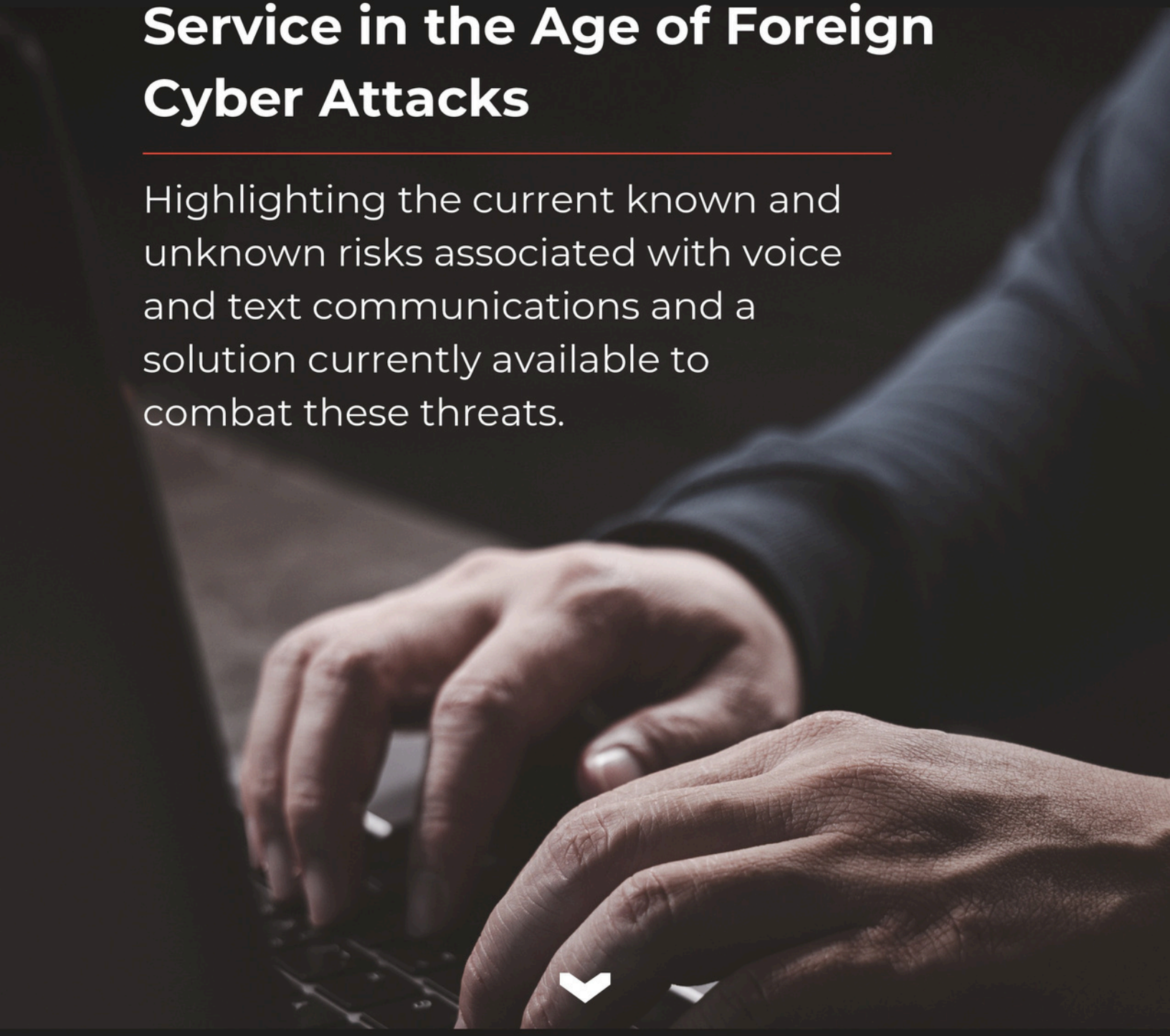
MOVIUS

PREMIER WIRELESS

Secure Communications as a Service in the Age of Foreign Cyber Attacks

Highlighting the current known and unknown risks associated with voice and text communications and a solution currently available to combat these threats.

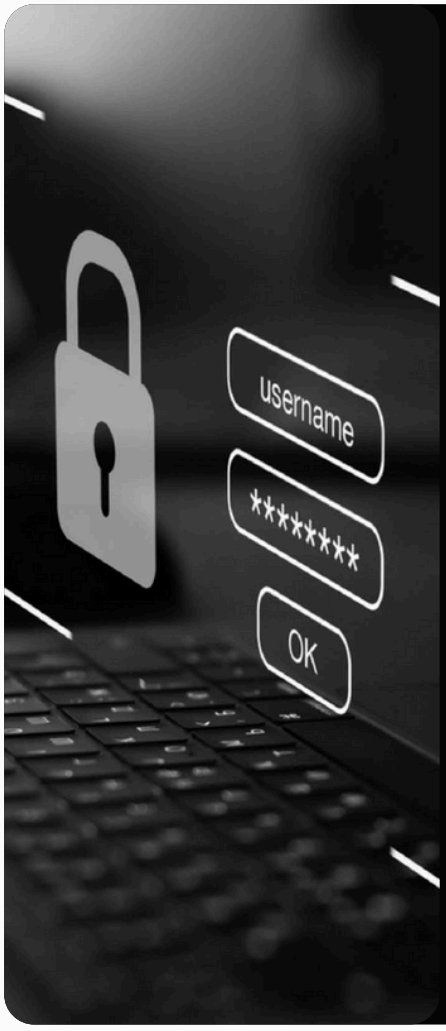


The Threat

Voice calls, messages, telemetries, geospatial data, and unstructured data transmitted through traditional carrier networks are inherently insecure.

These communications are often unencrypted or only weakly encrypted, making them susceptible to interception by malicious actors. Additionally, legacy protocols used in these systems were not designed with modern cybersecurity threats in mind, making them vulnerable to eavesdropping, spoofing, and man-in-the-middle attacks. While some wireless carriers have implemented security measures like end-to-end encryption for certain services, these are not universally applied, leaving many traditional communications exposed to potential breaches. Furthermore, the reliance on centralized infrastructure means that a single point of failure can compromise vast amounts of user data.

Current Vulnerabilities in phone calls, messages, telemetries, geospatial data, and unstructured data exist mainly (but not limited to) because of:



1. **Lack of Encryption:**
   - Many traditional phone calls and SMS messages rely on outdated protocols (e.g., SS7), making them vulnerable to interception.
   - Calls and messages transmitted without encryption can be intercepted by hackers, state actors, or malicious insiders.
2. **Metadata Exposure:**
   - Even encrypted communications often expose metadata (e.g., participants, time, duration) that can be exploited for surveillance.
3. **Man-in-the-Middle (MITM) Attacks:**
   - Calls and messages can be intercepted during transmission if secure key exchanges are compromised.
4. **Identity Spoofing and Phishing:**
   - Caller ID spoofing and fraudulent messages are used to deceive users into revealing sensitive information.
5. **Device and App Vulnerabilities:**
   - Malware or spyware on a device can record calls or read messages, bypassing network security.
6. **Unsecured Public Networks:**
   - Public Wi-Fi and open networks are common entry points for eavesdropping and data theft.
7. **Diameter Protocol Interception Attacks:**
   - This plays a critical role in the subscriber data, additional checks to validate the subscriber could lead to critical exposure to the subscriber data.

Continued evidence of this threat, including very recent exposure

Several high-profile hacks and incidents in recent years highlight the vulnerabilities of traditional carrier networks, including both voice callsand , text messages, telemetries, geospatial data, and unstructured data. These breaches underscore how attackers can exploit the weak security of telecom infrastructure, including signaling protocols and mobile device vulnerabilities.

As covered in a recent New York Times article, the Chinese government continues to grow more brazen in leveraging private telecommunications companies and 5G infrastructure for espionage purposes while the public nature of the conflict in Ukraine has highlighted key failures in current near-peer communications procedures. Evidence suggests that some of the roots of the Russian communication lapses lie in the inherent challenges of operating on foreign soil, where the enemy controls not only cellular networks but also wired communications that frequently serve as a reliable backup channel. From phone calls and group calls to text messages, communications are being compromised and intercepted, putting civilians and military missions at risk. And with a continuously expanding distributed and connected IOT ecosystem, the attack surface is broadening.

Additionally, the increased use of edge computing in 5G networks can introduce new vulnerabilities, such as the potential for malware to be injected into edge devices. And with the heightened activity of data injection attacks, attackers are increasingly introducing malicious data into the network through compromised edge end points.

An approach to addressing this growing threat

For secure voice and , messaging and data communications, several methods are considered much more resilient against common vulnerabilities like interception, eavesdropping, and man-in-the-middle (MITM) attacks. These methods generally rely on strong end-to-end encryption (E2EE), robust authentication, and the use of modern protocols that are designed with security in mind.

A summary of these mitigation strategies includes (but not limited to):

1. End-to-End Encryption (E2EE):
- Use encrypted communication platforms to ensure only intended recipients can access call or message content.

2. Secure Key Management:
- Implement robust encryption protocols for secure key exchanges.

3. Secure Apps and Hardware:
- Use privacy-focused devices and secure communication apps.
- Regularly update software and firmware to mitigate vulnerabilities.

4. Metadata Minimization:
- Use services that minimize or obfuscate metadata exposure.

5. Authentication Protocols:
- Implement multi-factor authentication (MFA) for messaging apps.
- Use digital signatures and blockchain-based identity verification to prevent spoofing.

6. Avoid Public Networks:
- Use private or secure connections for VoIP or app-based calls to protect against interception.

7. Education and Awareness:
- Train users to recognize phishing attempts, spoofed numbers, and the importance of secure communication tools.

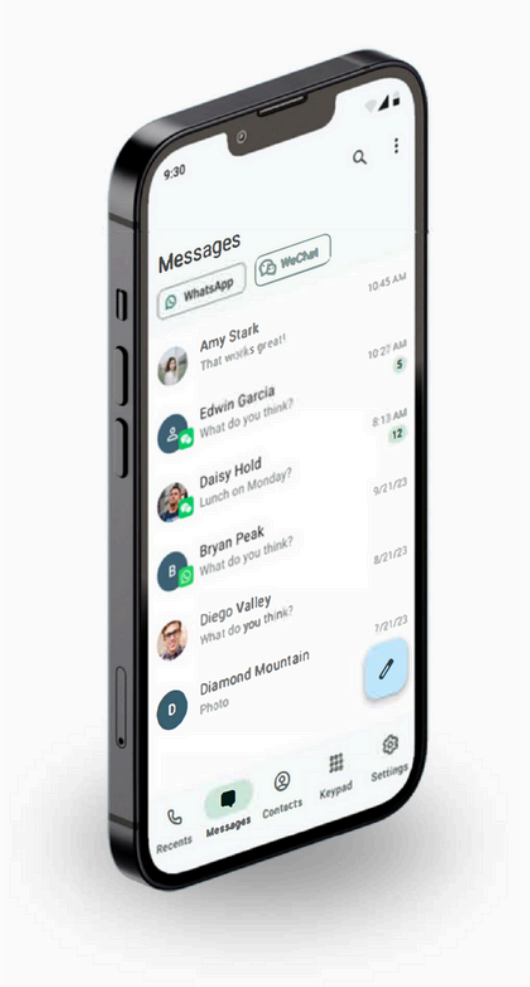
8. Regulatory and Organizational Policies:
- Advocate for stricter regulations to secure telecom infrastructure and encourage providers to upgrade legacy systems.
- Establish organizational policies for secure communication in sensitive environments.

By adopting a combination of encryption technologies, secure infrastructure, and user awareness, individuals and organizations can significantly reduce the risks associated with vulnerabilities in phone calls and messaging systems.

THE SOLUTION FOR TODAY AND THE FUTURE

T-Mobile MultiLine powered by Movius

Starting a decade ago, Movius Interactive Corporation's application, Multiline, was built exactly in anticipation of this core need to enable secure communications, anywhere, helping connect more people from more places securely.



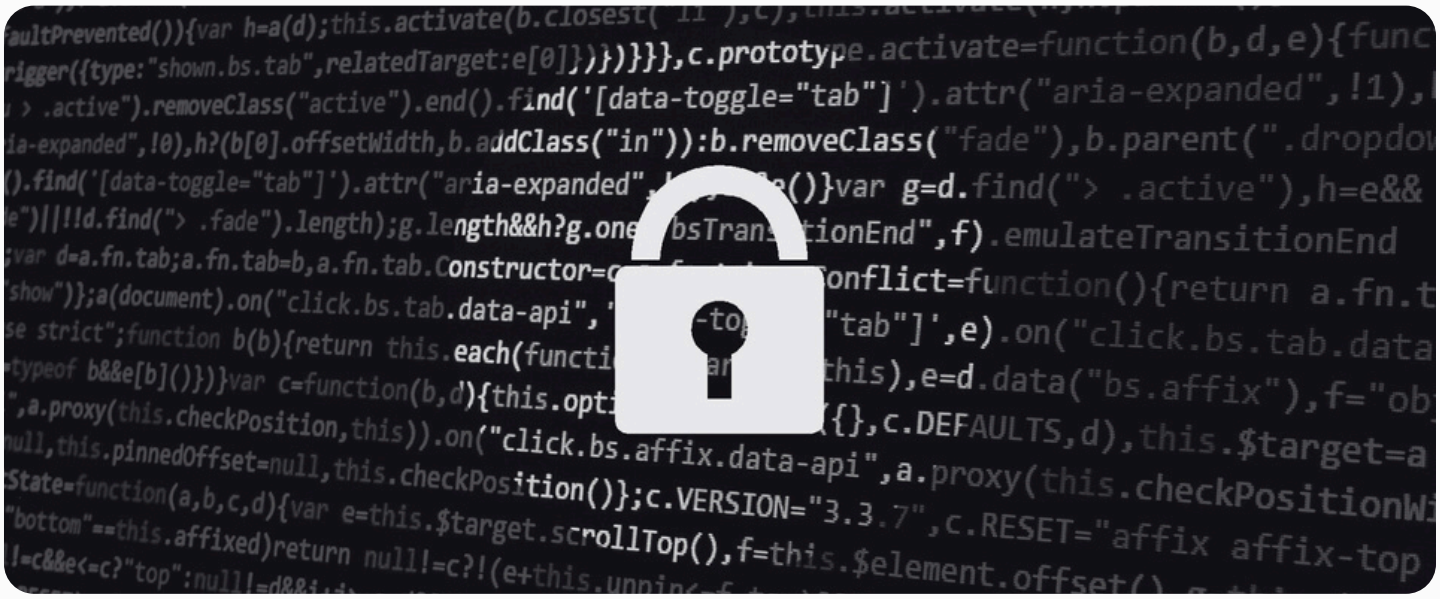
Movius Interactive Corporation (Movius) is a privately held "purpose driven, Secure Communications as a Service" (SCaaS™) company. MultiLine™ is the trusted solution for secure voice and text communications globally to secure their communications across various endpoints at the Edge. Leading regulated industries and enterprises around the world use Movius communications solutions. Movius is constantly pushing the frontier of communications innovation and is backed by strong intellectual property, consisting of more than 50 patents. Movius is also listed in the FedRAMP marketplace meeting all stringent NIST standards and National Security Agency (NSA) guidelines.

Since its creation, the main goals of the MultiLine solution were to support communities (each one of us) through a geographically dispersed, standards-based, and non-blockable communications service that allows users to communicate (voice, and messaging, telemetries, geospatial data, and unstructured data) across a secure, flat, non-hierarchical communications plane and can be utilized in a variety of mission critical operations, ranging from domestic support to civil authorities and major combat operations. These also include business-critical conversations (banker-client, healthcare provider-patient, teacher-student, and more) and simply normal human-to-human conversations.

The T-Mobile network+ MultiLine combines T-Mobile's secure 5G wireless network with the secure MultiLine communications solution. T-Mobile 5G network is generally considered secure, thanks to its implementation of modern G security standards and advanced technologies. While no network is entirely immune to threats, T-Mobile's adherence to advanced standards and proactive measures provides strong protection for its users. Continued vigilance, user education, and innovation remain critical to maintaining and improving security.

T-Mobile's 5G network security includes (but is not limited to):

- Advanced 5G Security Standards
- Network Slicing
- AI-Driven Threat Detection
- Zero Trust Architecture
- Edge Computing and Data Localization
- Mitigation of Legacy Vulnerabilities
- Commitment to Compliance and Standards



A Proven Partnership for Critical Mobile Security

Delivered through a strategic partnership between Premier Wireless and Movius, this, this solution combines cutting-edge technology, unmatched mobile network reliability, and expert enterprise deployment.

Premier Wireless plays an indispensable role in making this solution accessible and actionable across key sectors such as government, healthcare, financial services, healthcare and public safety. With over three decades of experience in the mobility and connectivity space, Premier Wireless is uniquely positioned to navigate the complexities of large-scale device deployments and enterprise-level mobile security integrations. Their expertise ensures that organizations can implement secure mobile communication systems without disruption to daily operations.

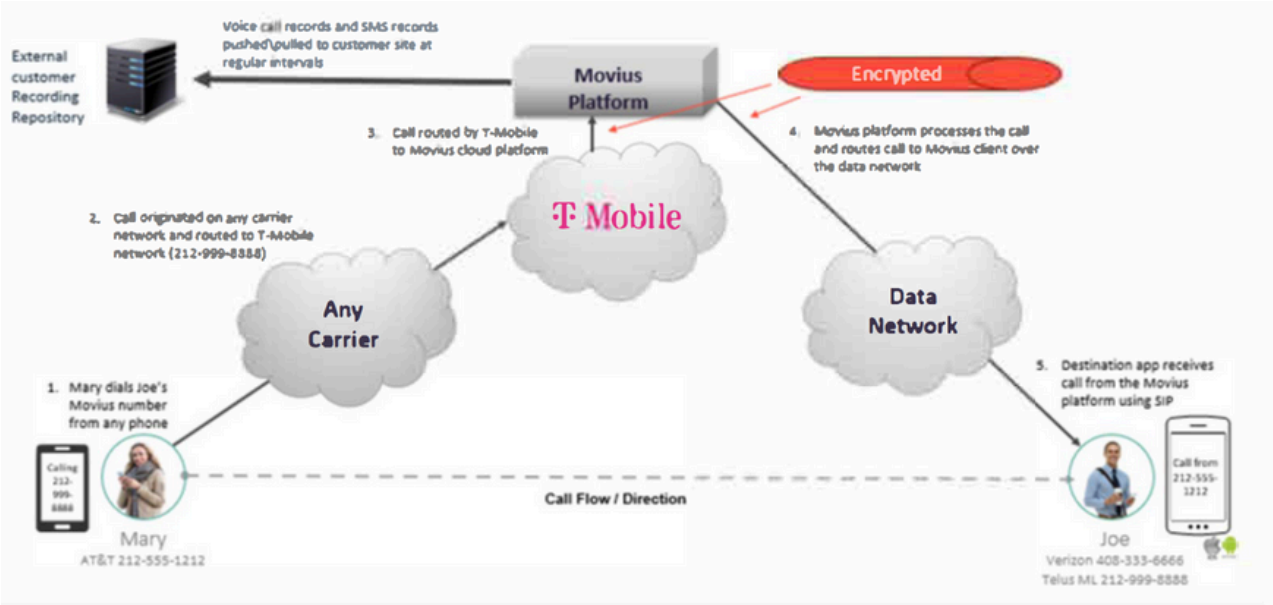
Premier Wireless doesn't just provide equipment; they offer a comprehensive end-to-end service that includes everything from customized deployment plans to ongoing support and training. Their team is dedicated to creating tailored security solutions that align with the unique needs of each organization, ensuring seamless rollout and minimal downtime.

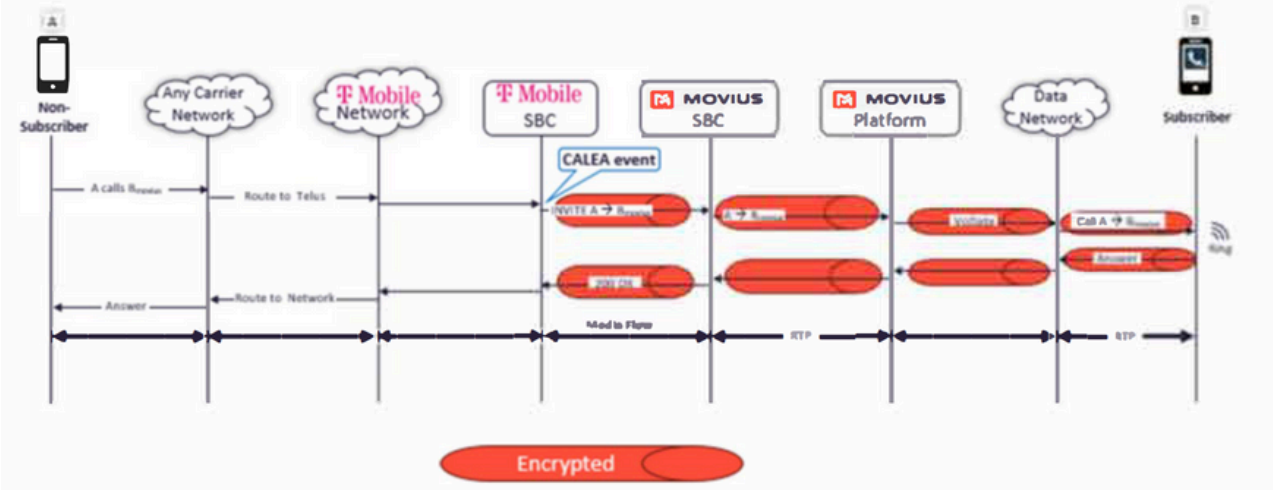
The document now dives deeper into the various call and text scenarios with the T-Mobile MultiLine solution

1

In this scenario an off-network non-MultiLine user calls a MultiLine user who is set for receiving the call in data mode: The flows indicate the legs that are fully secured. If the off-net user was another MultiLine user, the calls is completely secured.

INBOUND MESSAGE FLOW I VO DATA & MULTILINE MT ON VO DATA

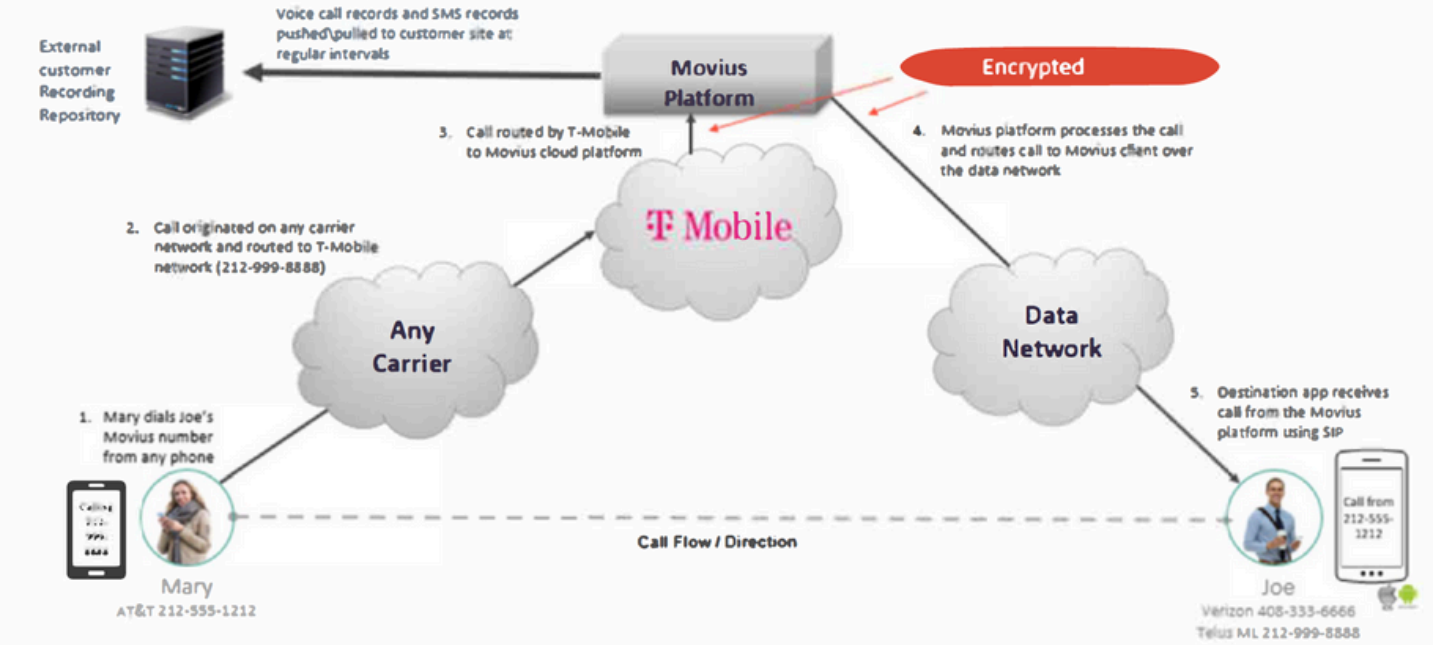


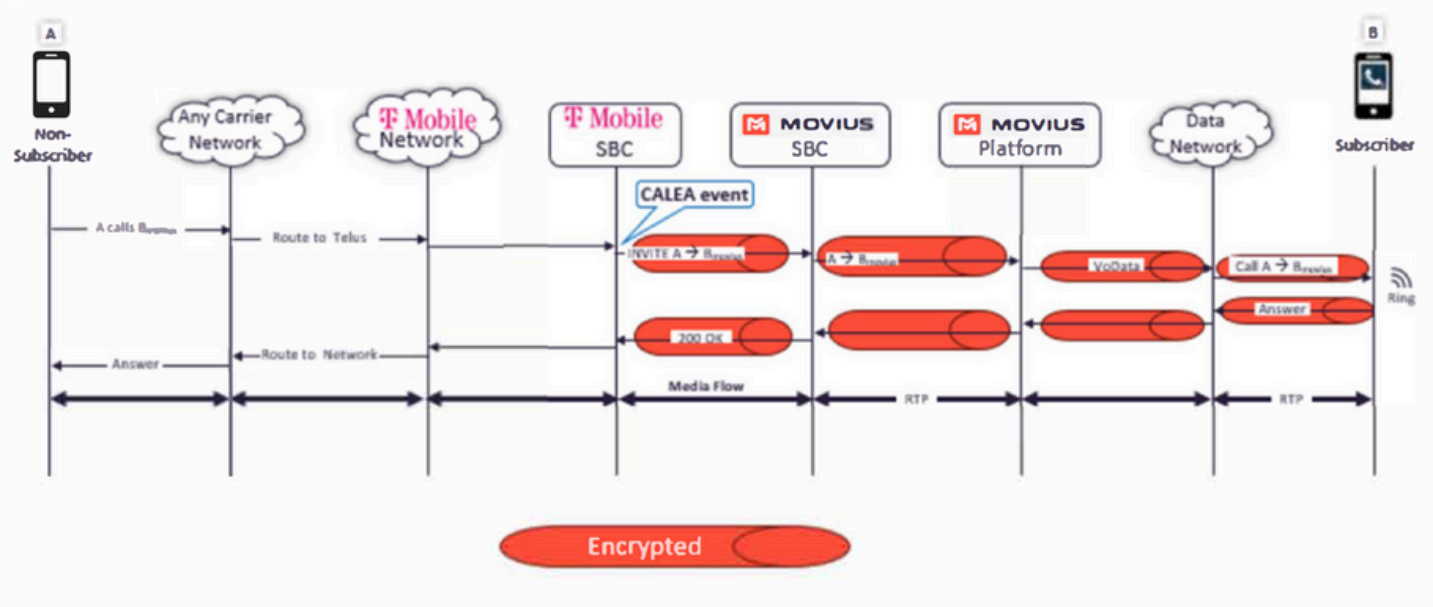


2

In this scenario, an off net (non-MultiLine user) calls a MultiLine user who is set for receiving the call in the Movius patented Minutes Mode: The flows indicate the legs that are fully secured. For an inbound minutes call, T-Mobile MultiLine encrypts data between the T-Mobile network and Movius Platform.

INBOUND MESSAGE FLOW I VO MINUTES &
MULTILINE MT ON VO MINUTES

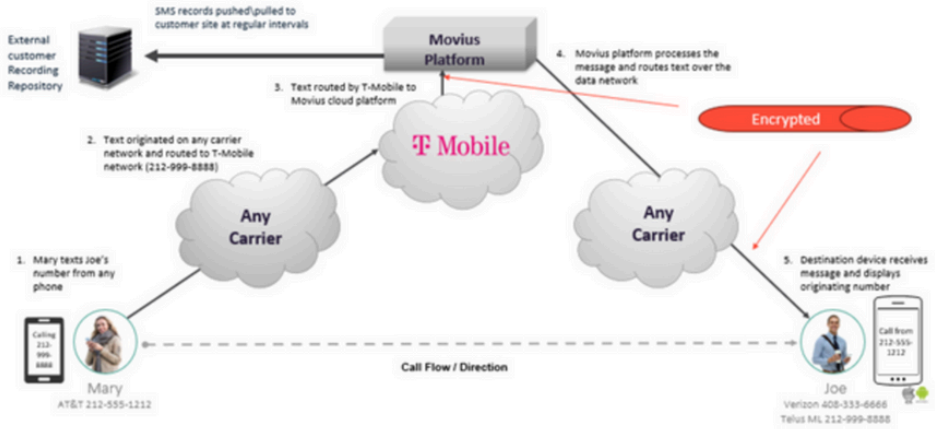




3

In this scenario an off-net (non-MultiLine user) texts a MultiLine user: The flows indicate the legs that are fully secured. Inbound Messages are encrypted from the T-Mobile network into Movius, and from the Movius Platform to the MultiLine client application.

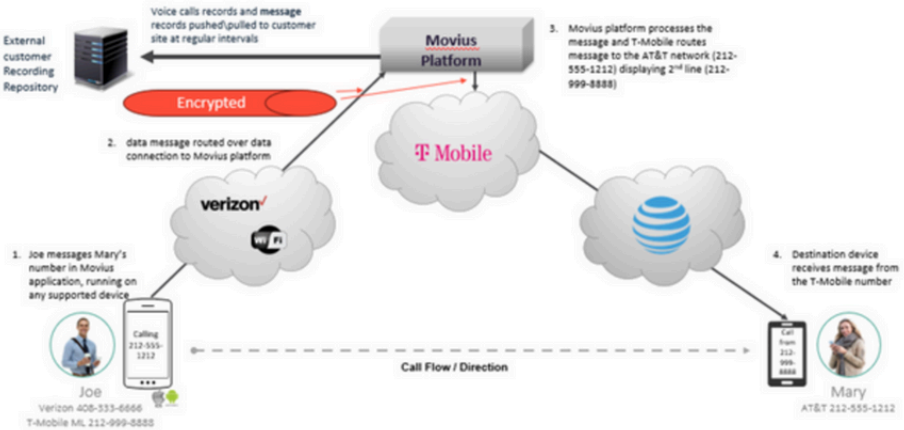
INBOUND MESSAGE FLOW



4

In this scenario MultiLine user texts an off-net (non-MultiLine) user: The flows indicate the legs that are fully secured. Outbound messages are encrypted from the client app to the Movius platform and then encrypted from the Movius Platform to the T-Mobile network.

OUTBOUND MESSAGE FLOW I VOiP



In scenarios 3 and 4 if the messages were exchanged between two MultiLine users, they would be fully secured end to end.

In Summary

1. Movius provides the most robust patented technology and security for always available secure communications when two users are not on the MultiLine application. In the addition to the encryption of data at rest and in motion, Movius also implements Secure by Design and Zero Trust principles.
2. Movius significantly enhances the security of communications while being always available for secure communications when two users are on the MultiLine applications.

Movius Differentiation:
- **REFERENCEABLE: Deployed at the most regulated enterprises at scale**
- **SECURE: Defense grade robustness and certifications**
- **FLEXIBLE: Simplifying enterprise communications and seamlessly integrated in workflows**
- **UNIQUE: 50 patents; not just another VoIP communications tool**
- **CERTIFIED: See below**

A Trusted Partnership—Movius & Premier Wireless Differentiation:
- **END-TO-END SERVICE: Including customized deployment, ongoing support, and training.**
- **SEAMLESS ROLLOUT: Minimal downtime; minor disruptions to daily operations**

By prioritizing innovative security architectures, adopting advanced encryption protocols, and fostering a proactive approach to emerging threats, T-Mobile, Movius and Premier Wireless remain steadfast in our commitment to ensuring the utmost privacy and protection for phone calls and text messages, now and into the future.

Movius welcomes the opportunity to further explore the partnership and recommends a joint planning workshop to review the technology in detail, use cases in action and commercial mode.

TO LEARN MORE, VISIT WWW.PREMIERWIRELESS.COM

PREMIER™ WIRELESS

(281) 667-0404
sales@pwbts.net

Appendix

Future Proofing the Secure Communications and Freedom of Secure Conversations

Blockchain technology can play a transformative role in securing phone calls by leveraging its decentralized, immutable, and cryptographically secure nature. Here are keyways blockchain can be applied to enhance the security of phone calls:

1. Decentralized Call Routing:
- Instead of relying on a centralized server to route calls, blockchain can enable a peer-to-peer (P2P) communication system. This reduces the risk of centralized attacks or surveillance.
- Benefits: No single point of failure; calls are routed securely through encrypted nodes in the blockchain network.

2. Identity Verification and Authentication:
- Blockchain can store and verify digital identities securely, ensuring that the calling parties are who they claim to be.
- Benefits: Prevents identity spoofing and man-in-the-middle attacks.

3. Secure Key Exchange for Encryption:
- How It Works: Blockchain can be used to facilitate secure key exchange for end-to-end encrypted calls.
- Benefits: Eliminates the need for third-party key distribution services, reducing vulnerabilities.

4. Immutable Call Records and Metadata:
- How It Works: Blockchain can record call metadata (time, duration, participants) in an immutable ledger. While the content of the call remains private, the metadata can be secured to prevent tampering or unauthorized access.
- Benefits: Provides transparency and auditability without compromising content privacy.

5. Smart Contracts for Automated Security Protocols:
- How It Works: Smart contracts can enforce security protocols automatically.
- Benefits: Enhances trust by automating security measures.

6. Fraud Prevention and Spam Blocking:
- How It Works: Blockchain can be used to verify caller identities and create a reputation system.
- Benefits: Reduces phishing and robocalls.

Appendix

7. Privacy-Preserving Protocols:
- How It Works: With blockchain-based privacy solutions (like zero-knowledge proofs), users can confirm their identity or credentials without revealing sensitive information.
- Benefits: Ensures privacy while maintaining a secure communication channel.

8. Tokenized Payment Systems:
- How It Works: Blockchain can enable tokenized payments for premium secure calling services.
- Benefits: Facilitates secure and decentralized monetization models.

Challenges and Considerations:

While blockchain offers promising security features, it is not a standalone solution and must be integrated thoughtfully:
- **Latency:** Blockchain systems can introduce delays due to the time needed for transactions to be verified and recorded.
- **Scalability:** High transaction volumes might challenge the scalability of blockchain networks.
- **Complexity:** Adoption requires technical infrastructure and user familiarity with blockchain concepts.
- **Energy Consumption:** Some blockchain systems, like Proof of Work (PoW), are resource intensive.

MultiLine: Architecture evolution

By integrating blockchain with secure communication protocols, phone calls can achieve higher levels of privacy, authentication, and resistance to attacks, making them safer for users worldwide.

Movius is working in partnership with the Department of Defense to develop a new class of secure communications.
- Built from the ground up with decentralized blockchain technology.
- Data transfers encrypted inside an outer encrypted tunnel. (Double Encrypted)
- Peer To Peer encrypted over any available data network (Network Agnostic)
- Self-Sovereign Identification capability available to the user
- End user key rotation by user on demand
- Not just a personal communications solution. Can relay any type of data (Coordinates, Supply Line Orders, etc.), via DOD devices, or any type of IOT device

Appendix

Movius Secure Communications as a Service is evolving with the following design tenets

- **Secure Communications Plane that augments the decentralized ecosystem**
  - MultiLine has a smart application logic on the distributed edge, controllable by an Intelligent Control Plane
    - Self-sufficient: Minimal and essential application logic for communications, control and capture
    - Thwart proof: Built with defense in depths and with the highest security standards
    - Mutable or Permanent: Application can persist or can be muted by ICP if risk of compromise
    - Situational aware: "Listens to" surroundings (see #5 on safer edge) and see (#3 on voice)
    - Non-Hierarchical: The architecture has a flat applications plane
    - Software Defined: Optimized for any edge hardware (Android, IOS, Linux) and network (Cellular, Wi-Fi, Satellite, Private, and more)
  -
- **Fungible or Non-fungible Identity**
  - Entity: Mobile device or any smart connected thing: persona/object map
    - Identity/Identifier: Token or an actual phone number or any ICP relatable identifier
    - Identity Attributes: Routable, non-thwartable, communicable, commercial grade and standard
    - Fungible: Dynamic identity assignment with intelligent network routing
    - Non-Fungible: Fixed persona/object for "always-available" communications
  -
- **Voice as a multi-faceted capability**
  - For mono-directional alerts
  - For bi-directional communication
  - For biometric authentication
  - For ambient condition detection
  - For deconstructed voice-gram messaging

- **Geographically dispersed, standards based and non-blocklable communications service**
  - Global in nature – works in any geography; local or "glocal"
  - Network agnostics – Cellular, Wi-Fi, Satellite, or even other defense specific networks
  - Cannot be blocked by Russia or China because of its "commercial" nature

Appendix

- **Natural Language Processing enabled safer distributed physical edge**
  - Ultra-optimized edge Voice processing with capabilities like:
    - Speech recognition
    - Self-learning models
    - Energy efficient
    - Light-weight ruggedized APIs to work with edge hardware
  - Model engines coexisting with the ICP
  - A tamper-proof and immutable network which makes sure all transactions are secure and untampered
  - Distributed security leveraging consensus mechanisms, such as proof-of-work or proof-of-stake, to ensure that all nodes on the network agree on the validity of transactions and communications
  - Multi-language support to cater to diverse user bases and enable global communication

Movius and Premier Wireless are on a joint mission to deliver the freedom of secure communication without compromise. In today's landscape, where threats are constant and communication is critical, recent events have only intensified the urgency to deploy defense-grade secure solutions. Together, we're empowering industries with technology that ensures safety, reliability, and uninterrupted connectivity.