FISSURE for TAK & Mobile

Christopher Poore
Assured Information Security, Inc.
153 Brooks Road
Rome, NY 13441
315-336-3306 x1569
poorec@ainfosec.com

1. EXECUTIVE SUMMARY

FISSURE is an open source, modular framework for RF, EW, and cyber experimentation that brings actionable spectrum capability to phones, laptops, and small edge nodes, then scales to fleets. The aim: task nodes from where operators already work, see results in the shared picture, and keep evidence tied to time, place, and configuration for audit and analysis.

Current mobile practice is fragmented and hard to adapt. Tools that sense, classify, and act on signals often sit outside the collaboration tools units already use. Links are intermittent and bandwidth is limited, so operators need compact messages, store-and-forward, and confirmations that survive real conditions. FISSURE provides an upgrade by pairing commercial off-the-shelf (COTS) hardware with a plugin architecture and policy-aware messaging.

Mobile integration follows two paths. In the Team Awareness Kit (TAK) path, FISSURE posts detections, classifications, and status to a TAK server for visibility in WebTAK today, with tasking tools for Android Team Awareness Kit (ATAK), Windows Team Awareness Kit (WinTAK), and Windows Team Awareness Kit-Civilian (WinTAK-Civ) in development. In the native app path, a lightweight phone app speaks the same compact FISSURE messages to the central hub or directly to a node. Both replicate key Dashboard actions on mobile and keep formats compatible so units can mix TAK clients and native apps.

Connectivity sets the ceiling for mobile use. On constrained links, operators see abbreviated alerts and can trigger small preset actions; on IP links, they can pull artifacts, run richer tasking, and confirm outcomes with more detail. In all cases, tasks carry source, destination, and hub identifiers, and the central hub routes status and evidence to TAK or a mobile app for a consistent picture.

FISSURE remains open, extensible, and affordable. New radios, classifiers, and effects appear as plugins that light up corresponding mobile tools and presets. Units can begin with viewing only, add simple tasking, and grow to fuller mobile control as tools mature.

2. PROBLEM STATEMENT

Mobile control of RF operations remains fragmented. Even with TAK in wide use, sensing, classification, and effects often run in separate consoles and only fragments return to the shared picture. Operators lose time switching tools and reconciling entries, which slows tasking and erodes trust during live missions.

Field links are intermittent and low throughput. Tasks, alerts, and evidence must cross austere networks and sync later. On low throughput, mobile operators are limited to short presets and abbreviated alerts. On higher throughput they can pull artifacts and run richer playbooks. Many tools do not degrade gracefully, either failing on low-throughput links or overwhelming them.

Teams also struggle with provenance and parity. It is hard to see who initiated an action, which node executed it, and whether success criteria were met. Android mobile devices, Windows vehicle kits, and WebTAK in operations centers often behave inconsistently, which increases training overhead and drives fragile one-off integrations. Effects also require clear authorities, audit trails, and guardrails, plus predictable fallbacks when links drop.

Licensing and procurement add friction. Closed toolchains tied to specific radios complicate university use, partner sharing, and mixed coalitions. An open approach reduces acquisition hurdles and makes adaptation easier without removing the need for accreditation and disciplined change control.

FISSURE mitigates many of these issues. It uses compact, mobile-friendly messages and source, destination, and hub identifiers to tie tasks to results. A central hub routes status and evidence to TAK or to a lightweight phone app that speaks the same messages. The open-source posture and plugin model lower cost and enable extension. FISSURE does not replace rules of engagement or guarantee confirmation in hostile environments, but it reports partial indicators and timeouts consistently and keeps a reliable record of who requested what and what the node attempted.

3. CURRENT STATE OF PRACTICE

Teams commonly use TAK for the shared operational picture while RF and cyber tasks run elsewhere. One camp includes open-source tools such as GNU Radio, Scapy, and Wireshark. They are powerful in the lab and flexible for research, yet they rarely ship with turnkey TAK integration, role controls, or mission policies. Moving them into the hands of operators takes expert time and a layer of custom glue that is difficult to sustain.

Another camp centers on vendor applications that pair tightly with a small set of radios or sensors. These tools often perform well on a single device and a single platform, but cross-platform reuse is limited and TAK-native markers, forms, or overlays are uncommon. Adding a different radio, a side-channel sensor, or a cyber workflow such as packet crafting and replay usually means jumping to a separate interface or buying into a new vendor-specific bundle.

Large closed systems promise end-to-end dashboards with multi-sensor fusion and sometimes basic cyber effects, but their cost, export restrictions, and slow update cycles make them hard to field with partners, students, or mixed coalitions. Integration points exist, yet they are often proprietary and do not expose enough detail for smaller teams to extend the system.

At the opposite end are ad hoc scripts and one-off bridges that push a few events into TAK or listen for simple commands. These bridges are useful for demonstrations and narrow tasks, but they rarely include role control, audit, conflict prevention, or robust behavior on low throughput links. They also lack a shared library and plugin structure, so each team rebuilds device support and workflows without a common catalog.

Across these approaches the split remains clear. Operators collaborate in TAK while the RF and cyber work happens in different user interfaces tied to specific radios, sensors, and operating systems. Valuable data from platform interfaces such as health, positioning, or ancillary sensors is present on the network, but it is not consistently tapped to enrich RF context. Discoverability is weak too. Mobile clients have no reliable way to enumerate which actions, plugins, or effects are actually available at a given node.

Against this backdrop FISSURE offers a different pattern. The central hub can present a discoverable catalog that mobile apps can query for available actions and plugins, then launch them with consistent parameters and receive results in a common format. That capability is developed in parallel with the TAK path and keeps compatibility with existing sensors and radios so teams can grow from what they already have.

These realities cut across classrooms, simulation ranges, field work, joint events, and operational use. Educators need a path from lab tools to field behaviors without expensive systems. Exercise directors want realistic message flows and evidence handling that survive constrained links. Field teams need mobile tasking that fits short interactions and mixed devices. During operations the same patterns must scale to multiple nodes with clear authorities and confirmations. FISSURE aligns with these use cases by preserving the same tasking, messaging, and evidence patterns across environments.

4. SOLUTION: FISSURE FRAMEWORK

FISSURE provides one framework with two operator views. The Dashboard (running on a computer) is the full console for building playlists, tuning parameters, reviewing data, and development, while mobile apps and TAK clients provide limited remote control that fits field use. From a phone or laptop an operator can start and stop tasks, switch modes, and launch defined actions. Each action can present either a minimal set of fields or a full parameter view depending on configuration, and operators can view abbreviated status and alerts with mapping capabilities.

The central hub coordinates everything. It brokers messages between clients and nodes, records tasks and results, and exposes a catalog that mobile clients can query for available actions and plugins before tasking. The hub can host a TAK server locally or sit on the same network as an existing one. That lets multiple Dashboard instances and mobile apps connect to the same nodes and see a consistent picture.

Clients authenticate using appropriate certificates. Mobile apps authenticate to the central hub with client certificates issued for FISSURE. TAK clients authenticate to the TAK server with TAK certificates and roles, while the central hub integrates with that server on the network. Connections use standard IP transports on the same network or a simple routed path. Clients select a target node by ID, and the hub includes its own hub identifier in each task so the node knows where the request originated. Clients receive limited acknowledgments and basic status today with improvements planned. Other mission applications besides mobile and TAK can integrate the same way: authenticate, discover available actions, select a node, submit a parameterized task, and retrieve status and artifacts.

Message detail is constrained by the throughput between the central hub and the sensor node. For TAK, FISSURE data is wrapped in Cursor on Target (CoT) so markers and status appear in the client, while mobile apps use the native FISSURE message format. On constrained links only minimal receipts and alerts are practical. On IP links clients can receive more detailed outcomes and retrieve artifacts. The operator workflow stays the same as connectivity and tooling improve.

5. DEPLOYMENT SCENARIOS

The scenarios below show common ways teams use FISSURE in practice. Each one highlights who is operating, which nodes are involved, and what level of results to expect given the link capacity.

Handset to Node in the Field: A mobile user launches a targeted capture, quick classification, or a mode change from a phone or laptop. Alerts and labels return to a map with abbreviated status on constrained links, while richer outcomes and artifacts are available on IP links. Evidence can be deferred for later retrieval when needed.

Vehicle Kits and Patrols: A vehicle workstation coordinates nearby nodes for on-the-move sensing and effects. One node can maintain wideband or area watch while another executes a defined action. When link capacity allows, operators review results and pull artifacts.

Operations Center Coordination: An operations center monitors markers and status in WebTAK and tasks nodes as needed. Operators can extend dwell, adjust frequency, or retask mobile nodes, keeping a single picture for mixed teams and partner units.

Perimeter and Infrastructure Defense: Fixed or semi-fixed nodes watch facilities and campuses for rogue access points, unusual beacon behavior, or protocol misuse. When a signal of interest appears, mobile users receive a geofenced alert and can trigger a focused capture or dispatch a mobile node for additional coverage.

Education and Simulation: In classrooms and training ranges, instructors use the same mobile patterns to teach field-realistic workflows. Synthetic signals and scripted responses let students practice tasking, see updates on a map, and download evidence bundles tied to time and location.

Joint and Industry Events: FISSURE integrates with existing TAK servers so mixed teams share one operational picture. Teams use TAK or a lightweight mobile app to task participating nodes, and RF detections, classifications, and sensor context publish back to TAK as CoT. With a continuous backhaul, artifacts transfer in real-time for evaluation and after-action review.

6. KEY BENEFITS

FISSURE delivers mobile-ready advantages that streamline RF operations while staying interoperable with TAK and open to extension:

Single Operator Workflow: Task nodes from phones, vehicle kits, and operations centers using the same patterns.

Central Hub Coordination: Broker messages between clients and nodes, record tasks and results, and support multiple apps on one network.

TAK Interoperability: Publish detections, classifications, and status to existing TAK servers as CoT so teams share one picture.

Mobile-Ready Control: Start and stop tasks, switch modes, and launch defined actions with minimal or full parameter views.

Discoverable Actions: Query the hub for available plugins, radios, sensors, and actions before tasking.

Link-Aware Behavior: Send minimal receipts on constrained links and richer outcomes and artifacts on IP links.

Evidence Handling: Tie markers and artifacts to time, location, and configuration for review and compliance.

Open and Extensible: Add radios, classifiers, and effects through the plugin architecture without rewrites.

Low Cost to Field: Rely on COTS hardware and open software to reduce procurement friction and enable partner adoption.

Authentication and Roles: Use certificates for client authentication and TAK roles where applicable to separate authorities.

Scale Path: Begin with a single node and grow to small fleets without changing how operators work.

Developer Velocity: Keep the Dashboard as the full console for building playlists and reviewing data while mobile mirrors the essentials.

7. RELEVANT EXPERIENCE

Assured Information Security (AIS) has exercised FISSURE in classrooms, laboratories, field demonstrations, and joint technology events, pairing RF workflows with the collaboration tools operators already use. The focus is turning research workflows into field-relevant patterns that fit real networks and mixed teams.

FISSURE has flown on small drone platforms as part of combined solutions, and alerts from FISSURE nodes have been plotted in WebTAK along with live sensor node positions. Separate efforts outside the FISSURE team are building mobile and TAK applications for handsets and phones equipped with SDRs; those projects run in parallel and may inform future development.

AIS conducts safe prototyping and evaluation at facilities such as ORION in Rome, New York. Work at ORION includes experimenting with networking and TAK solutions and exercising large populations of Internet of Things (IoT) and Internet of Military Things (IoMT) devices. The environment supports testing and integration and serves as a source of shared knowledge.

Best practices and lessons learned from these efforts guide ongoing FISSURE development. The same openness that defines the framework extends to mobile applications and plugins so partners can adopt, inspect, and adapt while maintaining interoperable, auditable workflows.

8. CONCLUSION

FISSURE brings mobile control to RF operations while preserving existing workflows. The framework pairs a full Dashboard on a computer with focused control from phones, vehicle kits, and operations centers. A central hub coordinates clients and nodes, records tasks and results, and publishes to TAK using CoT so detections, classifications, and status appear in the shared picture. Detail scales with the link: constrained paths carry receipts and alerts, IP links return richer outcomes and artifacts.

The approach is practical across classrooms, field work, joint events, and live operations. Teams can start with WebTAK viewing that exists today, add basic mobile tasking as tools mature, and grow to broader control over time. Evidence handling ties results to time, location, and configuration; certificate-based authentication and TAK roles preserve policy and access control; and a discoverable catalog keeps mobile clients aligned with each node’s capabilities. FISSURE’s open, plugin-driven design lowers cost and speeds adaptation, allowing new radios, sensors, and effects without rewriting the workflow. Other mission applications can integrate the same way as TAK and mobile clients. The result is an upgrade path for RF situational awareness and effects that fits real networks and mixed teams, scales from a single node to small fleets, and remains interoperable and auditable as capabilities grow.