

Security Solutions



Security is an imperative for today's complex, distributed systems. A distributed application infrastructure must be flexible to support a variety of secure operating systems (OSs), secure transports and higher-level assurance features. It also must support varying levels of security required for different applications on the network. RTI offers a rich set of security features, including domain separation, access control, deep packet inspection, data range checking and filtering, as well as secure OS and secure transport support.

Highlights:

Works within existing infrastructure: communicates through firewalls and NAT with or without VPN

Delivers a reliable solution based on open standards and proven techniques, such as OpenSSL TLS/DTLS for encryption and STUN protocol for NAT traversal

Provides transport level authentication and data encryption over WAN or LAN

Enables the five essential attributes of information assurance: confidentiality, integrity, availability, authentication and non-repudiation

RTI Security and Information Assurance Leadership

A sampling of U.S. Department of Defense security projects that have used RTI solutions:

- USAF Airborne Network Trusted Code (Assurance) Involving the Anti-Access Environment
- USN Integrity and Authentication of Real-Time Data in Navy Combat Systems
- OSD Improving Software and Data Security in SCADA Systems
- USAF Technologies for Cost-Effective Mixed-Criticality Flight Control Systems
- OSD Developing Cyber Situation Awareness for Enterprise Health
- USAF Proactive Determination of Network Node Vulnerabilities
- USN Real-Time, Secure and Fault Tolerant Discovery for Publish-Subscribe Middleware in a WAN Environment
- USN Secure Community of Interest (COI) Communications
- USN DDS Performance, Portability and Security

RTI Connex provides a comprehensive solution to ensure the security of your distributed system. In addition to offering the broadest set of security features of any DDS-based communication infrastructure solution, we are at the forefront of new standards-based security additions via the Object Management Group (OMG).

Domain Separation, Access Control and Secure Bridging

Underlying RTI Connex, Data Distribution Service (DDS) separates applications so those in different domains cannot communicate with each other unless the domains are explicitly bridged. Domain separation is enforced using the following:

- **Access control:** Each application is configurable with a set of network interfaces to use and a set of IP addresses for communication.
- **OS-based enforcement:** A secure OS enforces the access-control policy by restricting access to related system resources.
- **Secure transport:** Encryption prevents unauthorized parties from snooping the communication.

RTI gives system architects the flexibility to send data peer-to-peer within a domain to avoid broker-related vulnerabilities, thus improving performance and scalability at the same time. System flexibility also enables the deployment of services such as data routing and persistence where they are needed. In particular, the standards-based routing capabilities of Connex Integrator can selectively forward data between different domains and supports:

- Configurable one-way data routes
- Data filtering and transformation
- Remote monitoring and administration

Deep Packet Inspection

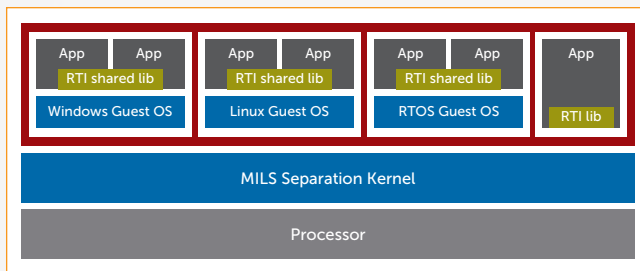
The content-aware DDS infrastructure and strongly typed messages enable efficient deep packet inspection. RTI can interrogate each message from the header down to individual fields. This enables a new class of high-performance software-based Cross Domain Solutions (CDS).

Data Filtering

Each DDS subscription can be associated with a set of content-based rules so that applications do not receive data that is out of range or irrelevant. These data filters are expressed in an OMG-standard SQL-based syntax and are evaluated for each data sample. Filters are dynamically changeable so that each application can adjust its valid region of interest based on operational scenarios. Furthermore, a re-locatable service can monitor the network for offending data values and issue appropriate security alerts.

Secure Operating Systems

OS security is essential to prevent both local and remote security violations. RTI Connexx supports a comprehensive set of OSs including the latest secure OS. These provide OS-level policy enforcement to restrict access to particular networks and domains.



RTI was also the first DDS vendor to provide a Multiple Independent Levels of Safety/Security (MILS) architecture solution. MILS OSs that implement the Common Criteria Separation Kernel Protection Profile (SKPP) provide time and space partitioning that limit the ability of a rogue application to impact the behavior of valid applications.

Secure Transports

RTI allows each application to be configured with a set of transports appropriate for its requirements. The example in Figure 1 shows a distributed system that includes three different domains. The first domain is not using a secure transport, while the second and third are configured using Transport Layer Security (TLS, the successor to SSL) and Datagram Transport Layer Security (DTLS) protocols.

TLS encrypts TCP network connections using symmetric cryptography for privacy and a keyed message-authentication code for message reliability. DTLS is a TLS variant for UDP datagrams. Both DTLS and TLS provide certificate-based authentication and encryption, protecting the exchanged data from unauthorized applications.

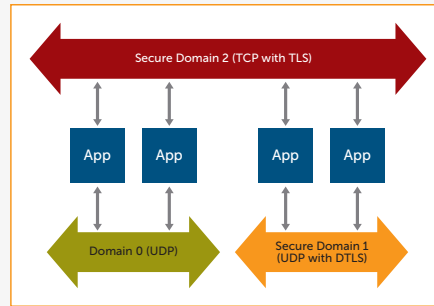
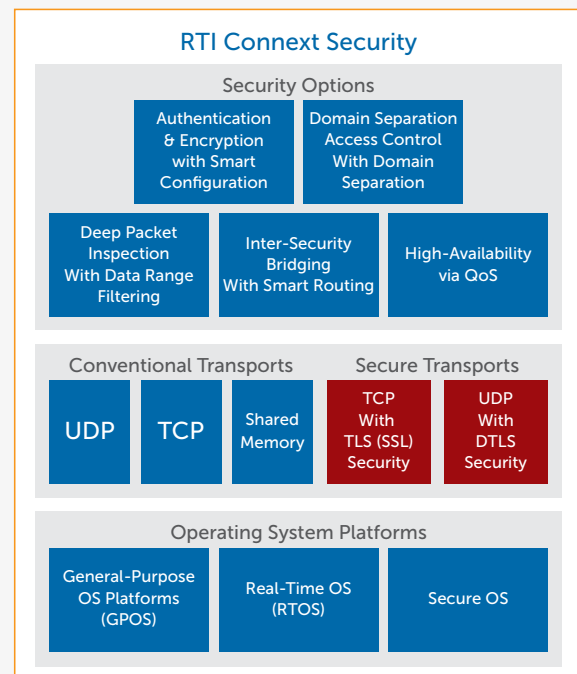


Figure 1: a multi-domain DDS network with mixed security protocols.

Improved Paradigm for Secure Distributed Infrastructure

Shared messaging infrastructure, such as a message broker, can be a security liability: The infrastructure must be trusted to the highest level of any message flow that passes through it, and an attack on a broker is an attack on all applications that rely on it. However, in some cases—such as when shuttling data between security domains—such infrastructure is necessary.

Because a secure transport protects only a single network link, a message broker requires access to cryptographic keys to decrypt and subsequently re-encrypt the messages that it processes, leaving messages temporarily in the clear. In contrast, when RTI Connexx is used in a peer-to-peer configuration, links connect producers and consumers end-to-end, eliminating this weakness.



About RTI

RTI is the world leader in delivering fast, scalable, communications software that addresses the challenges of building and integrating real-time operational systems. RTI Connexx solutions meet the needs of enterprise-wide integration — from the operational edge to the enterprise data center. The RTI standards-based software infrastructure improves the efficiency of operational systems while facilitating better decisions, actions and outcomes for the business enterprise.

For over ten years, RTI has delivered industry-leading products and solutions for customers in markets ranging from Aerospace & Defense, Process Automation, Financial Services, Energy, Automotive, Health Sciences and Transportation Management.

Founded in 1991, RTI is privately held and headquartered in Sunnyvale, California.



Your systems. Working as one.

CORPORATE HEADQUARTERS
232 E. Java Drive
Sunnyvale, CA 94089
Tel: +1 (408) 990-7400
Fax: +1 (408) 990-7402
info@rti.com
www.rti.com