NDP

NET-CENTRIC DESIGN PROFESSIONALS

Data Confidentiality and Integrity for Real-Time Pub/Sub Systems
NDP Research – Tech Note

July 2010

Data Confidentiality and Integrity for Real-Time Pub/Sub Systems

Tech Note Number	NDP-TN-100
Problem	Existing pub/sub systems lack required real-time, scalable cybersecurity and information assurance guarantees for use on mission critical systems (C4ISR, Weapons Systems, Safety-of-Life Systems, and Financial Systems). Solutions are needed to protect data in real-time from unauthorized disclosure, interception, and tampering in pub/sub networks where not all participants are known *a priori*.
Description	NDP adds robust data confidentiality and data integrity guarantees to pub/sub networks, protecting data from interception and tampering. The approach preserves real-time performance by minimizing per-message encryption overhead and key-exchange/re-key operations. Addition and removal of subscribers is accomplished without rekeying in nearly all cases. Subscription revocation capabilities enable publisher to maintain strict control of data dissemination. Authentication features enhance data provenance capabilities within the pub/sub network.
Core Technology	The key advances are achieved by enhancing a derivative of Shamir's *(k,n)-threshold secret sharing scheme* for data encryption, and novel integration of public-key infrastructure (PKI) into the pub/sub network. Predictive re-keying and other advanced key-management significantly reduces overhead and data interruptions.
Benefit	NDP's technology will enable open-architecture information systems to securely utilize pub/sub networking for real-time services and data distribution. Next-Gen C4ISR, Tactical, Mission, and Financial systems will more easily meet Cybersecurity and Information Assurance requirements.
Market	Primary markets include numerous defense, civil, and commercial customers. In defense, all departments operate multiple C4ISR and Weapons Systems in which real-time pub/sub networks play a critical role. Academic and scientific communities using pub/sub networks for data collection or sharing are other potential customers. Commercial markets include: Financial companies for market and transaction data systems; Energy companies for energy grid monitoring and control system; and many other industries that utilize pub/sub networks. This primary market is a subset of the SOA market, which was estimated at $3.5 billion in 2009 and forecast to reach $8.2 billion by 2016.
Technology Readiness Level	2. Technology concept and/or application formulated.

NDP, LLC | 2575 Pearl Street, Suite 220 | Boulder CO 80302 | Phone: (303) 339-0853 | Fax: (303) 325-5136
Learn more at ndpgroup.com

NDP

NET-CENTRIC DESIGN PROFESSIONALS

Data Confidentiality and Integrity for Real-Time Pub/Sub Systems
NDP Research – Tech Note

July 2010

Keywords publish/subscribe (pub/sub), cybersecurity, net-centric, information assurance (IA), service oriented architecture (SOA), open architecture, real-time, encryption, public-key infrastructure (PKI), data pedigree, data provenance.

About NDP NDP designs and deploys complex computer systems and networks. We also assure that these systems and networks can operate securely in cyberspace. By integrating sound net-centric designs into our customer systems, we enable them to gain a competitive advantage that translates to mission effectiveness. We primarily support DoD, Intel and Federal customers and are currently expanding our offerings to the commercial and academic markets. We are a customer-centric, technology-centric and people-centric company.

NDP, LLC | 2575 Pearl Street, Suite 220 | Boulder CO 80302 | Phone: (303) 339-0853 | Fax: (303) 325-5136
Learn more at ndpgroup.com