

Multi-Level Network Gateway and Remote Administration Infrastructure

RedPhone Security

2019 Palace Avenue
Saint Paul, MN, 55105

Mr. Mark Brown

Phone: (651) 204-3372

Email: mark@redphonesecurity.com

Website: www.redphonesecurity.com



Command: SPAWAR

Topic: N06-089

PROBLEM STATEMENT

Internet Protocol-based networking has become a national infrastructure component, on par with superhighways, telephone service, pipelines and electric grids. Normal functioning of both civilian and military enterprises depend on this infrastructure. However, networks are different from all other infrastructure in one way: they enable remote management. Networking's unique strength also presents a unique vulnerability: remote cyber attack.

The threat of remote cyber attack against interconnected network infrastructures and the systems they serve remains largely unsolved despite decades of research and development. For the elite few systems that address the threat of cyber attack well, usability and obsolescence has typically rendered these systems useless. Interoperability challenges, high costs and obsolescence risks affect network infrastructure to a greater degree than more established infrastructures because the rate of technology change is greater in this area. In the short history of computer and network security most of the highly assured solutions became unusable due to obsolescence and usability issues.¹

Fifteen years later, today's next-generation military systems designs are clamoring for "high assurance" and "multi-level secure" features – the same goals that motivated each of the projects listed above. Now, from the Department of Defense's Joint Vision 2020, to the NSA's Global Information Grid (GIG), the \$1 trillion Joint Strike Fighter, the Army's Future Combat System, the Joint Tactical Radio System, and DARPA's Next Generation Internet, the use of high assurance networking is required.

¹ See, for example, insider-practitioner Richard E. Smith, "Trends in Security Product Evaluations," *Information Systems Security*, 2007, v16, no 4, pp 203-216. See also sociologist Donald MacKenzie *Mechanizing Proof: Computing, Risk, and Trust*, 2004, p. 190-191. See also Garrel Pottinger, "Proof Requirements in the Orange Book: Origins, Implementation, and Implications." 1994, commissioned by contract N000173-93-P-G934, available at: <http://chacs.nrl.navy.mil/publications/other/pottinger94.pdf>

Not only must the next generation multi-level secure solution be secure, but it must also be ubiquitous, reliable, maintain a low size-weight-and-power profile, up-to-date, and since there will be so many such systems they must be remotely administratable. Not only must they share information across three or more classification levels, they must also allow information sharing between foreign nations, ad-hoc coalitions, humanitarian groups, civilian legal systems, the intelligence community, universities, law enforcement, coast guards, international banks, prime contractors, supply chain companies, and many more. And unlike previous generations of computer users, the next generation of users will interpret mantras such as "Need to share" and "The right information at the right time to the right people," through a lens of expectations formed by using Twitter, iPhone, and Facebook. High assurance systems that must be installed into a secure operating center with help from a forklift need not apply.

RedPhone Security's Distributed Secure Router (DSR) technology has been designed to provide a secure, remotely administered gateway to the GIG, packaged in a variety of easy-to-install and easy-to-own network card form factors. All form factors provide high assurance publish and subscribe, infinite scalability, with configurable pipelines and integrated cross-domain capability with Type I cryptographic capability. All DSR network cards provide a secure, remotely administered network infrastructure. Thus enabling the possibility for almost-real time C2ISR data feeds; such as, SAR images, FLIR, video, Blue and Red force tracks, force dispositions, ordnance loads, GMTI, etc., keeping the warfighter informed from the command center to the "last mile".

WHO CAN BENEFIT?

With SBIR funding support from SPAWAR, the technology is aimed at insertion within PEO JTRS due to its highly assured remote management and multi-level capabilities. Simple operations like changing the channel or encryption keys on a JTRS radio can be securely accomplished remotely, en masse, and by a high user even if part of the effect of changing the channel must be accomplished on the "low side" of the radio unit.



The cross-domain challenges inherent in the Navy Maritime Domain Awareness (MDA) effort, including its requirement to interact with a very large number of domains spanning numerous countries and diverse agencies provide another opportunity for RedPhone Security's high assurance network card. MDA requires a Services Oriented Architecture, including a dynamically updated catalog of web services provided by an ad-hoc network of participants. The DSR connects joint forces within the same country (or public key infrastructure) that agree to Bell-LaPadula rules with zero configuration, and can be easily configured to reflect the specific information sharing laws, treaties, agreements and policies that arise from a global effort such as MDA. In addition to SOA catalog and

search capabilities, the DSR includes a strong XML feature set, and easily integrates with third party products and web services, within Bell-LaPadula constraints, without reducing its high assurance posture.



Organizations that require a common operating picture (COP) created as an overlay of informational “pins on a map” while at the same time multiple classification levels separate groups of users will benefit immediately from using the DSR. The DSR is uniquely capable of achieving a secure “command down” operation, for example, one that affects the published COP. “Command down” will be a part of the certification package for the DSR, and falls within the formally verified information flow policy of the DSR. For example, a high user may command that one of the pins on the map change to a predefined state or color, and immediately that effect can be securely seen on the COP and, in near real time, published to all subscribers.

BASELINE TECHNOLOGY

In terms of baseline, Unified Cross Domain Management Office has recently been established to identify a baseline list and sunset list. Currently, no deployable, true Multi Level solutions exist on their lists. The closest match would be cross-domain guards such as Radiant Mercury, AF ISSE, CDWSG, DSCDS. Their functionality can be summarized at a requirements level by the recent NSA I81 tool/file format called Bray/DFCF. Current solutions are expensive to own, configure and patch. For example, current prices range from \$20K for a single entry-level guard and up, but annual maintenance costs are high since even something as simple as updating a version of software must follow a specified process and must be done by someone with similar security clearance. DISA DECCs are being deployed at a cost between \$75-85K for setup plus \$65-80K per year, per “flow”/ “file type” / “requirement” (used synonymously). The DECC is hailed as a price breakthrough accomplished by economies of scale. The problem is that only 6-8 DECCs in the world are planned, so they will likely remain centralized.

Next generation guards (per NSA I81 vision stated 6/25/2009) will be “distributed” across the enterprise although they will provide enterprise-standard (and enterprise-accredited and certified) functionality to users. Distributing the guards has a tendency to multiply the amount of configuration and patching required in the enterprise. Guards are currently limited in the number of simultaneous network (classification level) connections they can use due to security/certification limitations which tends to increase the number of guards required throughout the enterprise.

Guards do not currently provide NSA Type I cryptography, nor high enough assurance to acceptably cross three or more domains. Current enabling technologies for guards (Trusted Solaris, SE Linux, and BAE STOP operating systems) are suited to server-class

machines but not low size/weight/power devices (such as those in use by deployed troops); but NSA typically requires hardware-based devices for Type I cryptography certifications. In addition, Guards employed for Services Oriented Architectures (SOAs) typically require XML firewalls to sandwich them on the network, and several other types of servers (DNS, UDDI, central/enterprise administration) are often employed together with a guard in order to create a functional and accreditable “stovepiped system”. Instead, a new, multi-level solution is sought, as seen below.

Attribute	Description
Internet & World Wide Web Like	Adapting Internet & World Wide Web constructs & standards with enhancements for mobility, surety, and military unique features (e.g., precedence, preemption).
Secure & available information transport	Encryption initially for core transport backbone; goal is edge to edge; hardened against denial of service.
Information/Data Protection & Surety (built-in trust)	Producer/Publisher marks the info/data for classification and handling; and provides provisions for assuring authenticity, integrity, and non-repudiation.
Post in parallel	Producer/Publisher make info/data visible and accessible without delay so that users get info/data when and how needed (e.g., raw, analyzed, archived).
Smart pull (vice smart push)	Users can find and pull directly, subscribe or use value added services (e.g., discovery). User Defined Operational Picture v Common Operational Picture.
Information/Data centric	Info/Data separate from applications and services. Minimize need for special or proprietary software.
Shared Applications & Services	Users can pull multiple applications to access same data or choose same apps when they need to collaborate. Applications on "desktop" or as a service.
Trusted & Tailored Access	Access to the information transport, info/data, applications & services linked to user's role, identity & technical capability.
Quality of service	Tailored for information form: voice, still imagery, video/moving imagery, data, and collaboration.

Against the point solutions provided by today’s UCDMO-approved cross-domain solutions, the National Security Agency has provided a forward-looking GIG Architectural Vision document. Version 1.0 (June 2007) identifies the nine desirable attributes for the future GIG² (listed above). These “attributes” of the NSA’s desired solutions are described in further detail in the referenced document. We expect the RedPhone Security Distributed Secure Router (DSR) will provide a solution to all nine of these attributes, packaged as a high assurance and general solution.

TECHNOLOGY DESCRIPTION

RedPhone Security’s standard DSR can be plugged into new and existing Windows or Linux desktop and server systems as a two-port gigabit Ethernet network card. One port is multi-level, cryptographically labeled, “black” (confidentiality and integrity assured

² Page 31. See <http://www.defenselink.mil/cio-nii/docs/GIGArchVision.pdf>

via Suite B algorithms) channel; this port may be connected to any existing network including LAN, WAN, ad-hoc network or MANET. This "first port" expects to automatically form cryptographic tunnels within the logical scope of a single public key infrastructure (PKI). The second port uses SSL/TLS and may be connected to any single level network, and configured as either a local area network, or to enhance global sharing, to SIPRnet, NIPRnet, or the Internet.³ The second port provides extensive discretionary access controls, which must be configured to allow access. For example, the second port allows for the possibility of sharing among domains outside of the logical scope of a single PKI.

Installation of the two-port network card on Windows or Linux variants requires the installation of an operating-system-specific device driver, the DSR catalog and logging database, and also the installation of the DSR administration tool graphical user interface. Upon completion of the installation, the network card will have generated cryptographic keys (benign fill using a certified RNG), requested and received a PKI certificate for itself, and auto-discovered all other DSR instances on the first "multi-level" network port. It will have completed replicating all dominated catalog entries into its database.

Following installation, administrators may begin to extend the DSR catalog with a list of local resources (data or nouns) and operations (services or verbs). The DSR formal model and security proofs explicitly provide for the catalog to be extended by any DSR instance at any time, and replicated throughout connected DSR instances that dominate, where the dominates relation is applied at a very granular, per-catalog-entry level. Typically the extension of the DSR catalog is performed using a web browser running on the host system, the SSL protocol, the network card, and the DSR administrative web application and database. However, browsers connected via either Ethernet ports may also be authorized, via discretionary access control, to perform remote administration of the DSR catalog located at any remote DSR instance.

The DSR catalog provides a unified view of all network services, regardless of technical protocol specifics. For example, the DSR catalog may be populated to include Web Services Definition Language (WSDL) service descriptions, and at the same time it may include catalog entries for RSS or ATOM feeds, Common Object Request Broker Architecture (CORBA) or Remote Method Invocation (RMI) calls, specific web pages including Representational State Transfer (REST) conforming resources, filesystems, email servers, and so on. In this way, the DSR provides a generalized networking capability; however, all access is configured and controlled using the Type Enforcement abstraction at the application level of the Open System Interconnection (OSI) reference

³ DSR form factors with more ports, or with different physical layers are expected additions to the DSR family of products. Additional ports may be desirable to increase performance, add wireless or optical networking or fabrics, etc. Some ports may be configured to run "red" (unencrypted) for high volume, single-level traffic.

model. Whether the data was obtained from a filesystem, ORB, or web server becomes transparent, and the location from which the data was actually sourced is obscured. At the same time, an unprecedented level of metadata is included with every information transfer performed by the DSR, and that metadata is stored within the DSR audit database and can be automatically analyzed by either the DSR or a third party tool.

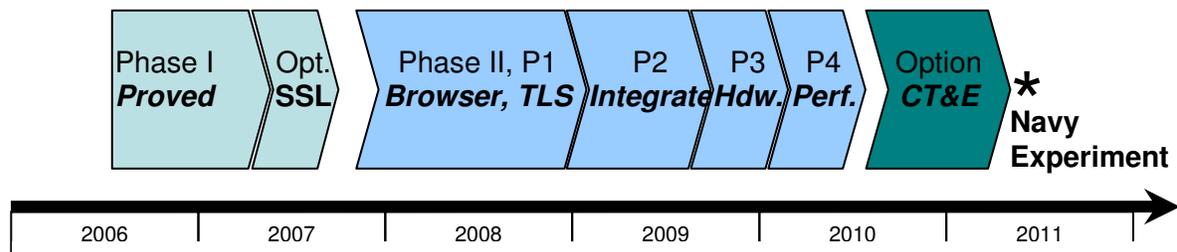
Features, Advantages, and Benefits of RedPhone Security DSR

Feature	Advantage	Benefit to Customer
Type I Cryptographic Binding & Metadata	Cryptographically strong, Type I labels are always authenticable, traceable, and bound to stored and transmitted information flows. All reads and updates are recorded and can be automatically analyzed to create releasability decisions. Metadata may include: status, confidence level, pedigree, revocation, alternatives, caveats, legal concerns/requirements, technical information relating to cryptography and quality of service	By accurately storing the lowest allowable classification level and the complete information pedigree, decisions to share information in new ways and with new partners can be rapidly configured. By allowing for metadata markup, data sharing can be more valuable and better understood.
Publish-and-Subscribe Architecture	PubSub allows users to define a narrow ongoing topic of interest, to which s/he subscribes. This can be more efficient and timely than search, pull or poll-based approaches.	Users receive immediate updates for only information topics for which they are prepared to act on.
High Assurance Pipeline	All authorized accesses can be augmented with "smart" filters, cross-checks, pattern matching, verification, format-to-format conversion, etc.	Users can configure "Smart Push" and "Smart Pull" operations as defined by Hayes-Roth. Information flows can be monitored and protected against malicious activity and malware. Covert channels can be controlled.
Networked Read-down / Browse-down	Innovative formal security policy has been proven to enforce mandatory access controls while allowing a network interpretation of "read-down".	Cross-domain browsing is supported. Storing large quantities of information at low, and referencing a small subset of that information is supported. This obviates the need to push large quantities of data up when only a small subset is required at the high domain.
Command-down	Innovated formal security policy allows high to send a highly specific one-bit signal to low that results in a predefined action taking place automatically at low.	Allows high to communicate a relatively unique, specifically defined command or decision to low without requiring a traditional downgrader.
Remote Administration	Any network card is technically capable of administering the security policy of any other network card, provided the total information flow policy allows it. Any network card can also securely deliver cross-domain updates to any connected system.	Both the underlying network infrastructure and any relying computer applications can be remotely patched, configured, monitored, etc., either at-level or across domains.
Formally Verified Design	The system delivers an extremely high level of assurance of confidentiality protections and data integrity and data quality to its users and their organizations.	The system mitigates threats of subversion and threats to confidentiality and data integrity at an extremely high level. In addition to design-level verification, the system's actual correct operation can be field-tested and remotely monitored.

Feature	Advantage	Benefit to Customer
Standard, Common-Off-the-Shelf integration	The system's network cards can be securely added to common-off-the-shelf computer systems such as Microsoft Windows® and Linux-based operating systems. The system can be configured using a web browser or web services.	Low cost of ownership due to: system transparency for primary users, ease of use and remote access for administrators, COTS hardware installation methods, configurable environmental requirements to allow for varying degrees of physical security to protect the network cards.

CURRENT STATE OF DEVELOPMENT

The RedPhone Security DSR is currently a TRL3 prototype implementation, with a mechanically verified Formal Top Level Specification and derivative Design artifacts that will support a high assurance evaluation. The prototype has demonstrated ease of integration with numerous standards and COTS products including unmodified web browsers and COTS web server technologies. We plan to demonstrate a TRL3 prototype in San Diego, CA in late 2009, and a TRL5 hardware prototype again in Q1 2010. Following the completion of the TRL5 prototype we will produce several standalone demonstration boards and develop (modify) Windows and/or Linux driver software.



A first release of the product and administrative tool is scheduled for 3Q 2010. The first release must be subjected to certification testing and evaluation by an authorized center, and will result in a TRL-6 SABI release, estimated for 2011.

RedPhone Security intends to sell certified DSR network cards either directly to the government or as common, off-the-shelf parts to system integrators, relationships are sought with government and systems integrators to deploy the DSR as a common networking infrastructure component within programs; such as, JTRS, MDA and CANES.

REFERENCES

- Technical Point of Contact, Navy SPAWAR PEO C4I:
(619) 524-7587
- Constance Heitmeyer, Head, Software Engineering Section, NRL CHACS:
(202) 767-3596
- Richard O'Brien, DSR Vulnerability Analysis Technical Lead:
(612) 387-5644

ABOUT THE COMPANY

RedPhone Security is a small business located in Saint Paul, Minnesota, founded for the purpose of securing practical Internet communications. It has patents pending in the areas of federated identity and authorization, and has worked with IETF Chair (former PKIX and TLS working group chair, and former Security Area Director) and standards author Russ Housley to develop an experimental Internet standard for SSL/TLS authorizations. RedPhone Security principals have had the privilege of working with leading scientists from Adventium Labs (formerly with Honeywell/Security Computing during the development of the SAT and LOCK platforms) and the Naval Research Labs Center for High Assurance Computing. In support of the legal merit and contractual fairness of its secure recordkeeping, RedPhone Security has earned letters of support for its technology from several leaders of the American Bar Association's Uniform Commercial Code Committee. A primary strength of RedPhone Security lies in its ability to absorb the "lessons learned" from earlier attempts to secure computers, and to apply them to current and anticipated technology capabilities.

RedPhone Security envisions transitioning the cross-domain DSR network cards either directly to the government or as common, off-the-shelf parts to system integrators.