A Knowledge Grid

Coordinated Public & Private Network

Abstract. The CyberRAVE™ (CR) proposed 'interpersonal interactions' architecture (boundaryless design) illustrates an 'open' approach to future IP network development among public and private Communities-of-Interest (COI). While the design protects existing technology investment, it establishes a new ROI metric for network security and business intelligence. It defines an integrated solution for technical and social issues, while establishing methodology for 'change management', motivational factors for implementation, and a plan for user adoption. The design addresses chief concerns associated with data security, user privacy, and decision support. The design establishes a developer platform involving Common-Off-The-Shelf (COTS) technologies, and an illustration for scalability among all primary vertical markets. The design describes a strategy for unifying public and private interests with standards-based metadata ontologies and semantic metadata packet encapsulation. Furthermore, CR offers an outlook for reduced implementation costs that facilitate broad-based deployment by groups of all size.

Motivation. Private industry is reluctant to report security breaches, or share information that may illuminate any network vulnerability. They are resistant to regulation that can impose new costs and restrictions over their current infrastructure or business processes. Public interests are under increasing pressure to establish Critical Infrastructure Protection (CIP) best-practices, methods, and technologies that safeguard national resources, while identifying and communicating threats and opportunities relative to specific sectors within the economy. Return on network security investment, and privacy concerns remain principal conditions preventing cooperation between these two interests.
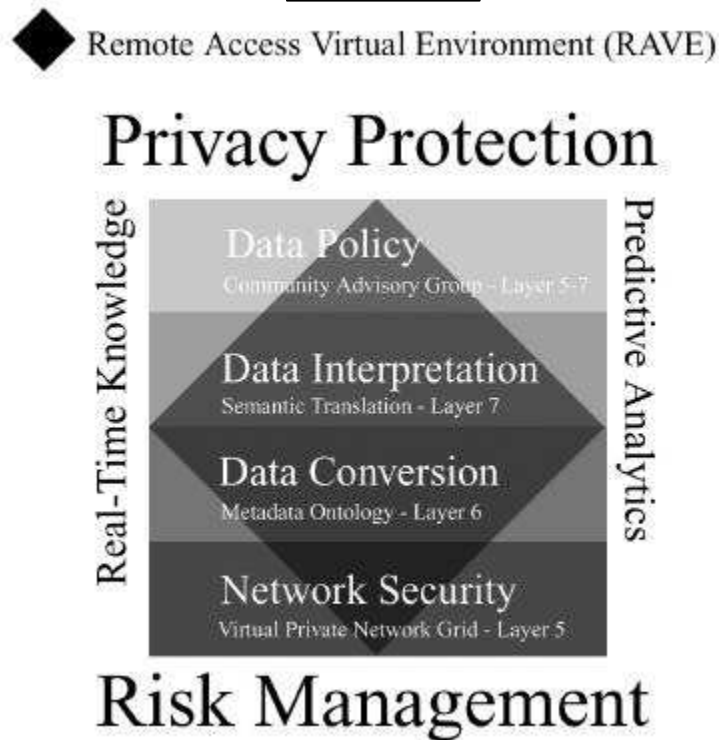
RAVE Description. A RAVE uses open-source data "wrapper" technology to disguise, encrypt, and cloak user data. Aggregated data flows are indexed within a cognitive meta data directory. The directory provides a contextual resource for knowledge discovery, and supports tools that enable specific business, analytic, and risk management goals. A RAVE converts structured data into a product that serves the interest of an individual, group, enterprise, or community. Structured RAVE data can be commoditized by assigning relevancy values, and used for decision support. Real-time decision support facilitates:

- ➢ Increased business efficiencies

- ➢ Support for regulatory compliance

- ➢ Protected privacy rights

- ➢ Maximized data services risk management benefits

- ➢ Protection of sensitive information and intellectual property

- ➢ Coordinated public and private information sharing and analysis

- ➢ Quantifiable efficiencies associated with business process, customer behavior, competitor behavior, and community (market) environment

- ➢ Minimizes the complexity of selecting, standardizing, and measuring data usefulness

- ➢ Establishes a defense-in-depth high level of network security

- ➢ Business Intelligence metric for Security ROI

- ➢ Aggregated price structure

- ➢ Pay-as-you-go shared usage model

Advisory Groups. Each RAVE is governed by a Vertical Community Advisory Group (VCAG). VCAG Directors are democratically elected to represent the interests of a vertical market segment (e.g. banking, healthcare, insurance etc). VCAG Directors are luminaries from within industry, institutions, governments, ISACs and related associations. VCAG Directors fully understand market conditions, and can fairly represent the interests of their respective community. VCAG data management policies support defined community objectives, and help determine 'fair use' laws for RAVE data brokering services; including collection, contextualization, and visualization of 'semantically rich' data.

Knowledge Grid. Information that exists in email, calendars, task assignments, reports, manuals, process guides, blogs, news feeds, digital libraries and archives etc can help fuel knowledge discovery. A 'knowledge grid' provides a communications infrastructure supported by user communities, investigative and diagnostic tools (see figure 1).

Figure 1

Remote Access Virtual Environment (RAVE)

Privacy Protection

Real-Time Knowledge

Predictive Analytics

Data Policy
Community Advisory Group - Layer 5-7

Data Interpretation
Semantic Translation - Layer 7

Data Conversion
Metadata Ontology - Layer 6

Network Security
Virtual Private Network Grid - Layer 5

Risk Management

Data Management. A RAVE establishes a transparent customer-driven platform for applied research tools, intelligent agents, and data analytics, while enabling predictive modeling with clear, natural language descriptions of potential threats and opportunities. RAVE open-source packet inspection and referencing methods establish a real-time registry of relevant network resources. RAVE advanced data brokering services include support for Authentication, Authorization, and Accounting (AAA) control. Proposed RAVE open source technologies will enable data security, predictive modeling, intelligent agents, and resource discovery for Users and Groups within a secure online community Virtual Private Network (VPN) grid. The RAVE platform works in conjunction with existing technology investments, and supports 'open standards' for transparent operation and developer participation.

Open Network Solution. CR proposes the use of semantic metadata as an aid to defining threats and opportunities associated with COI data security, business intelligence, and User privacy (see figure 2).

Figure 2
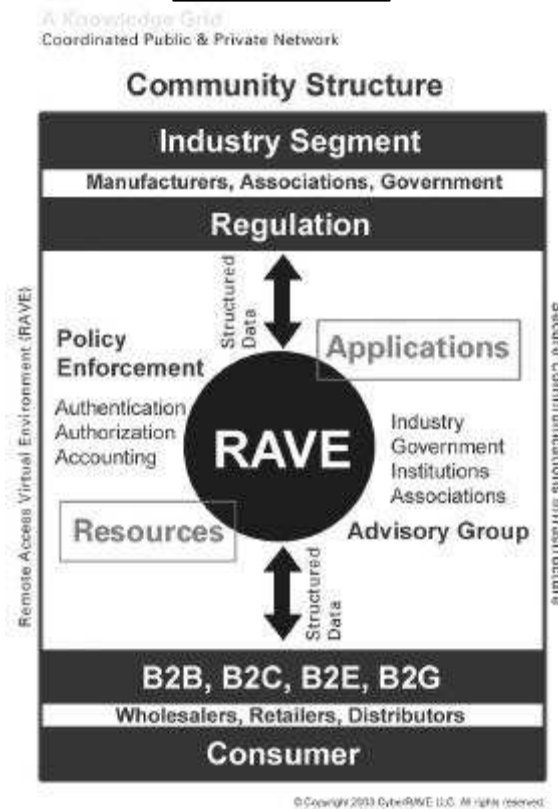
The CR proposed open network solution considers the convergence of these principal areas of interest in conjunction with Open Systems Interconnection (OSI) data packet description and translation functions. The CR solution involves VCAG policy definition and controls that establish the basis for industry-specific online democracies.

Prior to the distribution of outgoing RAVE data, information is structured using semantic markup language (e.g. XML, SAML). A VCAG defined semantic mediation process interprets the encapsulated data taxonomy including syntactic and semantic ontological profiles before indexing User and Group data flows (e.g. subject, verb, context, and administrative policy). The foundation for RAVE encapsulation can be found within the OSI structure at the layer 5 (security) level, and describes the User and Group in terms of their respective security policies. Well-formed data is interpreted within a semantic mediation process that attaches a VCAG profile at the layer 6 (syntax) level. And, a profile interpretation is given for the definition of 'actionable intelligence' at the layer 7 (semantics) level based upon User and Group, and VCAG policy description. OSI/TCP translation will transfer the described contents to level 4, within the 'reserved space' partition.

Business Solutions. Intelligence is assimilated via aggregated network data traffic flows from RAVE Users and Groups. CR establishes business intelligence, supply chain efficiencies, threats and opportunities assessment, and regulatory compliance by monitoring the flow of network information in a controlled VPN grid environment. CR increases data privacy with an open-source 'packet wrapper' technology that examines, contextualizes, and indexes the contents of User and Group data packets based upon acknowledged policies.

Technology Integration. To facilitate User and Group integration into the RAVE, CR proposes VCAG Director participation among 'Force Multiplier' customers, in conjunction with broad-based reseller arrangements. Force Multipliers should posses significant market influence, internal resources, and the desire to meet the ever-increasing demands associated with business intelligence, network security, and regulatory compliance. CR 'Charter Member' Directors serve as the basis for the initial community VCAG, and will help define policy development and enforcement best practices.

CR Value Add. CR portal development will support semantic keyword domain names, sub-domains, and file name extensions. CR registered and maintained library of well-formed, semantically structured generic Top Level Domains (gTLDs) are industry-specific, and aimed towards private and secure communications (see http://vpn.cyberrave.com). CR domains form a semantic foundation that establishes contextual relevancy for RAVE metadata with properly formed namespace. Stateful inspection of contextual data flows are logged into the RAVE meta directory, creating a reference structure (catalogue) where analytical tools can reference, and interpret data.

cyberRAVE
Decision Power

33 Westbury Dr.

Bella Vista, Arkansas 72714

Joseph A. Sprute

479-876-6255 Work

479-876-6218 Fax