

DRAFT

Description

CyberRAVE VPN Service Grid (The Grid) is a next-generation vertical network. The Grid interconnects trusted services for wireless (hands-free) user groups who demand high quality data security, compliance and information privacy.

Introduction

The old adage “content is king” is wrong. The real truth is that “contact” is, because the world is built on relationships being managed by complex systems that limit contact to resources.

CyberRAVE is compelled to provide Contact Services with Risk Management controls for Managed VPN Service Providers having wireless and hands-free user group customers that access business services over networked devices. CyberRAVE addresses fundamental risk issues at the intersection between public and private networks using a voice access and navigation framework with a cognitive (easy to say and remember) naming interface used for resource discovery. Naming systems establish the connective properties needed for secure interconnections between private network resources. They help associate data context with compliance processes. This solution is needed by the wireless industry so people will realize greater freedom roaming, data security and information privacy through policy driven compliance controls.

CyberRAVE has grasped an underlying naming scheme that targets user interest, and provides a speech interface to industry-specific business services. This naming framework offers the foundation for a voice driven, web-based interface that helps user groups define personal privacy rules for data, applications and virtual connections. A referencing architecture (naming schema) that uses voice recognition can interpret voice commands and authenticate users based on authorization privileges to data resources.

The public Internet increasingly uses a familiar, yet loosely defined “www.com” naming system that aides information seekers who need ready access to information communication technology services. CyberRAVE extends the state-of-the-art through cognitive domain naming schemes tied to private data resources using an access controlled authentication and authorization system.

Today’s search engines efficiently categorize information along horizontal and vertical market lines. Keyword (industry-specific) universal resource locators provide cognitive naming conventions needed for an intuitive voice activation and navigation system that connects user groups to discreet online business services.

Keyword domains are composed of common names. Names are like addresses. An address helps pinpoint an area of interest. Areas of interest can be related to user group policies. User group policies can be tied to user groups. User groups can be connected with credentials. Credentials can be linked to insurance underwriting. Underwriting can be associated to customer preferences, subscription services and law. Law is written according to public policy. Public policy incorporates social, economic, political, legal, technical and administrative risk variable controls. Risk variables help determine risk premiums, and risk premiums help user groups generate new value to data insurance coverage.

User group protections include strictly enforced policy controls, traffic reporting and systems auditing. CyberRAVE is bringing together important technologies, mechanisms and processes needed to help user groups locate and connect to virtual resources using a human-to-computer speech interface that navigates personal interests with available (directory) services and risk coverages.

Global Vision

The goal of The Grid initiative is to provide a hands-free resource discovery and private network interconnection service that allows wireless subscribers to effectively manage risk involved with digital rights for sensitive data

resources that reside on private networks using strict remote access and account verification controls that assure compliance with established user group policies. The Grid connects disparate resources through a common interface enabling access to industry specific gateway services.

CyberRAVE intends to establish a business culture that mitigates network data threats and vulnerabilities for horizontal markets, while simplifying the amount of effort needed for wider adoption of beneficial technologies. Efforts towards human computer interaction highlight the need for secure, hands-free remote access to bundled services having proven efficiency and usability benefits.

CyberRAVE's focus is to provide online user group communities a secure web-based lookup and interconnection service that couples wireless access, voice navigation, virtual private networking and data traffic management technologies with internationally recognized business process standards to increase profitability and reduce risk.

The Grid uses a community-driven approach to establish user group access rights and personal privacy preferences, data security levels and compliance standards. It is built with best-of-breed technologies that use recognized business processes to broadly define key performance indicators needed for optimized data management and administrative control over data assets.

CyberRAVE's web-based application interface monitors and enforces control points using client server accounting and auditing functions that protect data creation, storage, distribution and recovery. It involves a fabric of user group defined policies with cognitive resource discovery services built on top of a highly secure access, authorization and authentication platform.

The Grid is intended to help any size organization reduce costs, while creating new business efficiency using granular control over user group digital rights in wireless and hands-free environments.

Virtual Private Network (VPN)

VPNs provide underlying trust mechanisms including encryption, vulnerability scanning, filtering services, end-point security, network access control, threat detection and prevention, plus tunneling mechanisms for a host of data types and transmission protocols. As such, the definition provides that VPNs are truly an enabling business platform in use by a majority of business travelers and remote access user groups.

Technical and administrative provisioning obstacles that historically prevented wider adoption and interoperability between secure network connections are being addressed effectively using common off the shelf technologies from various vendors.

The perception of VPN in the global business community is that of necessity, where compliance with a number of internationally recognized laws now dictate their use. Gartner Research predicts VPNs will be the primary remote network access method for greater than 90 percent of casual employees by 2008, more than three-fourths of contractors and more than two-thirds of business telecommuting employees. Frost & Sullivan further asserts that VPNs provide comprehensive "Resource Gateway" capabilities where VPNs are broadly used for online banking and other security-sensitive Internet applications. Communication News says that VPNs will encompass the largest percentage (53%) of the network security market by 2009, and will be steadily fueled by wide spread adoption of voice over Internet technologies.

A well-constructed VPN environment offers user groups control mechanisms needed to guarantee service levels, tightly secure data and guarantee privacy according to generally accepted principals and compliance standards.

VPNs involve advanced logging capabilities needed to address forensic applications where a breach or policy violation may trigger the need for human intervention. They can be configured to comply with generally accepted accounting principals that use transparent processes. They offer high levels of investment return based on connection and delivery services that support business objectives for interest groups in all primary markets.

And they involve six key areas needed to effectively underwrite the risk of data security: Assessment, Access, Authorization, Authentication, Accounting and Auditing.

Semantic Grid

A semantic grid interprets user group data requests in terms of the relationship between naming conventions and its literal meaning in language. A naming platform that supplies contact services for vertical communities of interest must incorporate a reference system with common (keyword) names, specific industry taxonomies, a general ontology that unifies industry taxonomies, a modeling system that effectively translates names to appropriate user systems, and mapping services that allow users to successfully connect to resources found in a given network environment.

CyberRAVE reference schema uses cognitive, industry-specific, top-level keyword domains to establish its semantic resource discovery and topic navigation Web that interprets human speech using hands-free voice recognition technology. These well-formed names provide the specificity and relevancy needed to connect direct access to private data assets and secure business services using best-of-breed search and browser technologies.

CyberRAVE uses modeling languages that interpret industry-specific business rules through lookups within the domain, subdomains, and associated resource identifiers. Resources are defined within a reference directory that contain specific user account information. Access to resources defined within a user profile is granted according to policies established between customer(s) and service provider(s). Connection to resources is strictly enforced through CyberRAVE's traffic management utility that looks at data transmission contextually based on user group policies using voice-logging technology.

Enforcement and reporting of network traffic violations are monitored and controlled through a human computer interface that manages risk for known threats & vulnerabilities.

Data Insurance

The Grid uses risk management controls that protect user group data against loss associated with identity, integrity, survivability and recovery. CyberRAVE systems certification process has strictly enforced written policies that factor user group environmental variables. Policy statements with defined service levels differentiate risk management controls and computer assisted reporting & audit technology.

The underwriting criteria for The Grid coverage is determined by the degree of Risk/Cost/Benefit (to end user groups), Variable Risk Table Translations, Data Analytics, specific Insurance Underwriting Criteria and Amount of Asset Coverage.

Certification involves defining a user group risk rating used for determining insurance premiums. Data Insurance coverage aids business objectives to comply with laws & business rules, protect brands, and achieve optimized business performance. Different service levels address coverages with layered risk management that includes initial and ongoing Threat & Vulnerability Assessments, Risk Minimization, Environmental Monitoring, Measurements & Modeling (of key performance indicators), Mitigation and Remediation Services.

Service Levels

The Grid delivers service level products that offer vital guarantees with continuous data protection for network usage. Differentiated classes of service include Basic, Advanced and Premium products that add Quality of Service (QoS) value to policy instruments.