

Request for Information Response

Red Lambda, Inc.

Date: June 15, 2008

To: The Joint Committee of the Higher Education and Entertainment Communities,
Technology Task Force
ATTN: Bruce Block, Mark Luker

RFI: *Technologies for Addressing Issues Associated with
Unauthorized filesharing on the University and College Campus*

Issued: May 20, 2008

1	Executive Summary	2
2	Technology Overview	4
	2.1 Features of the Technology	4
	2.1.1 Network architecture	6
	2.1.2 Scalability	7
	2.1.3 Protocol identification	7
	2.1.4 Granularity of protocols	8
	2.1.5 Product Configuration and Installation	13
	2.1.6 Content identification	14
	2.1.7 Examination of network packets or file content	14
	2.1.8 Distribution systems	17
	2.1.9 Resilience of the technology to countermeasures	18
	2.1.10 Testing and installed base	18
	2.1.11 Competitive approaches	19
	2.1.12 Third-party components	19
	2.1.13 Comparison with Hypothetical Scenario	20
	2.2 Performance w/respect to the Requirements Described in the 2007 Workshop Report	21
	2.2.1 Identifying Infringing Traffic at the Campus Border	21
	2.2.2 Responding to Infringing Traffic at the Campus Border	23
	2.2.3 Identifying Infringing Traffic Local to the Campus Network	23
	2.2.4 Responding to Infringing Traffic Local to the Campus Network	23
	2.2.5 Supporting the Campus Judicial System	24
	2.2.6 Avoiding Disruption of All Non-infringing Traffic	24
	2.2.7 Considerations for Purchase and Operations	24
	2.3 Intellectual Property	25
	2.4 Corporate Characteristics and Resources	25
	2.5 Pilot Testing	26
	2.6 Commercial Terms	26
	2.7 Additional Information	26
3	Confidentiality	27
4	Conflicts of Interest	28
5	Readership and Dissemination	29
6	Miscellaneous	30
	6.1 No Obligations	30
	6.2 Neutrality	30

1 Executive Summary

On May 20, 2008, the Joint Committee of the Higher Education and Entertainment Communities Technology Task Force issued a Request for Information for technological controls as they pertain to illegal file-sharing on campus networks. In response, Red Lambda has issued this RFI response to clearly describe how its *Integrity* solution addresses these needs in one easy and cost-effective deployment. Red Lambda is pleased to note that **Integrity delivers all of the elements of the Task Force's hypothetical solution today**. Please see section 2.1.13 for more information.

We believe six key considerations distinguish Red Lambda from our competitors:

Experience

Red Lambda was founded in 2005 by a group of network engineers from the University of Florida who developed software specifically designed to eliminate illegal file-sharing on campus. In 2002, the founders began using a technology they developed called *role-based traffic management* to control network traffic based on identity instead of IP addresses.

Red Lambda's *Integrity* was constantly vetted protecting the campus wired and wireless networks, handling tens of thousands of mobile users, and **eliminating all DMCA complaints and pre-litigation notices for over 5 years**. At the University of Florida, *Integrity* evolved to meet the specific needs of universities: educational content delivery, judicial system and help desk integration, network architecture independence with high scalability, and fine grained policy control over traffic.

Met with acclaimed success, *Integrity*'s creators received the State of Florida's Davis Award for its outstanding reduction of network operations costs while automating and improving service to users. With a widespread impact on university user behavior, Red Lambda founders testified before the US Congress to highlight the virtual elimination of unapproved file-sharing at the University of Florida.

Red Lambda has helped universities across the United States monitor and eliminate inappropriate network file-sharing. In short, there is no vendor that can deliver Red Lambda's unique combination of experience, documented success, and sensitivity to campus policy issues.

Customer Support

Red Lambda's customer support provides an array of services the company developed throughout years of supporting university networks while meeting strategic university needs. Red Lambda's support services are flexible, global in scope, and available 24 hours a day. The range of services enables Red Lambda to support customers with varying levels of expertise. Support services, including pre-sale and post-sale consulting, installation, training, policy advisory and on-going support are made available to our customer base.

Red Lambda never outsources our technical support and each support engineer is an experienced network and systems engineer with prior university network experience.

Extensive Protocol Support

Red Lambda's *Integrity* is the only product available that uses a combination of deep packet inspection/behavioral analysis system that detects every known P2P protocol, even when encrypted, or hidden with evasion techniques. Unlike other products that claim encryption detection, *Integrity* can still determine what protocol is in use when it is encrypted, ensuring accurate, granular policy enforcement instead of clumsy encryption penalties.

Role-based Traffic Management

Red Lambda's *Integrity* is truly unique, enabling customers to define their file-sharing enforcement policies based on the identity of the infringer. This capability allows customers to simply map user groups to enforcement policies, without concern for where they are in the network, what device they are using, or what IP address they may have. *Integrity*'s identity-based policy system guarantees that authorized users will always have appropriate access regardless of how they access the network, preventing perceived outages and downtime.

Unrivaled Integration & Automation

Red Lambda's *Integrity* is designed to do far more than simply detect and stop file-sharing, rather, *Integrity* was

designed to enable customers to automate the complete problem life cycle associated with file-sharing management on campuses. Whether it is delivering educational content, creating judicial cases, managing help desk tickets, or communicating with students, Integrity enables customers to implement the policies of their choice automatically, drastically reducing operational costs. With Integrity, it is unnecessary for customers to purchase multiple products to solve the entire problem.

Commitment to Transparency & Standards

From an open standards perspective, product development at Red Lambda is driven by a commitment to the development and implementation of current and emerging industry standards that permit true interoperability among disparate systems. Red Lambda is an active member of the Internet Engineering Task Force, participating in the creation of standards for Operational Security, Network Endpoint Assessment, and Mobile Ad-Hoc Networks.

Red Lambda also believes strongly in the transparency of its products, giving customers full access to their data, detection mechanisms, and the underlying mechanics of Integrity's operation. Customers have the ability to customize Integrity as much or as little as they like, ensuring a smooth integration and maximum effectiveness from the simplest to the most extreme environments.

2 Technology Overview

Red Lambda's *Integrity* is a role-based traffic management solution. Building on five years of proven success, Integrity's value is simple: for the first time it's possible to control network traffic directly based on user identity.

Red Lambda delivers highly survivable, distributed security solutions for network defense and management. Our solutions combine patent-pending end-user intelligence gathering, pattern recognition, and cGRID peer-grid systems with network security automation to provide *role-based network security* for the first time to customers.

Believing that security policies are written for people and not IP addresses, Red Lambda's products allow customers to secure their networks and ensure compliance without concern for where their users are located, what IP address they have, or what device is used to access the network. By constantly mapping identity and behavior, assessing risk, and dynamically applying security controls based on a user's role and usage, Red Lambda's solutions provide the most comprehensive adaptive network security available.

2.1 Features of the Technology

This section of the response to the RFI should provide sufficient information about the vendor's technology so that the reader can acquire an adequate understanding of the tool, its method of operation, and its capabilities and effectiveness.

All technology submittals that are considered by the vendor to be applicable to the problem addressed by this RFI will be considered. However, the Joint Committee of the Higher Education and Entertainment Communities believes that most proposals will range over the following classes of tools. Some submissions may include features of several of these classes of tools. In those cases where the vendor possesses multiple tools, each should be separately discussed in its particular area of class of tool.

Audit Tools - *This class of tool covers applications that could be used by systems administrators to configure and maintain computer assets owned by the university or college. Such tools may allow auditing of installed applications against a standard "build" for the machine or may allow profiling of file archives on university-owned storage devices, for instance on public ftp servers, etc.*

Bandwidth Shaping - *This class of tools has the capability to adjust and/or alert other devices to adjust the amount of bandwidth and/or priority allocated in a network to a particular file type or application at any point in time. The technology may address uploading, downloading, or both, and may take origin or destination IP addresses into account.*

Data/filesharing Blocking - *This class of tool takes an active role in blocking and preventing access to file-sharing and/or streaming applications on a network or machine basis. The technology may block access based on external information such as DMCA notices.*

Matching, Screening and Filtering - *This class of tool can match transmitted data with, for example, data in a predetermined database and provide administrative reporting and/or selective filtering. This includes technologies that can provide activity reporting without blocking.*

User Management and Communication - *This class of tool can match the inappropriate action with the infringer and then communicate with the user. This includes technology to configure graduated levels of response and actions.*

Network Performance - *This class of tool is directed at overall network operation, performance and traffic analysis. Such tools may simply provide information such as traffic data/session, source address, application type, destination address, ports, etc.*

Integrity is a full-featured solution which spans a number of the classes listed above. For clarity, we have described Integrity's features by class:

Bandwidth Shaping - Integrity features a hybrid deep packet inspection/behavioral analysis system for advanced layer-7 analysis, and is capable of alerting simpler layer-4 bandwidth shaping tools, such as packet shapers and routers, to adjust bandwidth to infringers. In addition, if Integrity is configured to collect user

telemetry, Integrity can dynamically adjust shaping rules to ensure that the user, and not just the IP address of the original infringer, is restricted. This capability includes the ability to enforce policies on mobile users as well.

Data/files sharing Blocking – Integrity uses a hybrid deep packet inspection/behavioral analysis system to monitor network traffic for infringing application use. Based on detection, Integrity can then combine its user telemetry information (if configured) to dynamically enforce policy. A number of response mechanisms are available and may be combined as desired, including:

- Port deactivation
- Access Point deassociation
- VLAN steering
- DHCP steering
- Bandwidth shaping (triggering existing packet shapers or routers)
- Dynamic firewall rules and packet filters
- Account restriction (AD, NDS, LDAP, SQL)
- Communication with the end user via email, IM, RSS and more
- Content delivery via HTTP redirect and wildcard DNS entries
- Ticket management and database actions
- Monitoring only with **no** enforcement

In addition, Integrity may be configured to check email, and can engage policy automatically based on the receipt of DMCA complaints for a completely automated solution.

Rich policy control is one of the hallmarks of Integrity, allowing the creation of any policy which can be defined by business rules using the information collected. This includes elaborate escalating policies with white-list/black-list user exceptions, location exceptions, and more. Customers have used Integrity to automate complicated content and test delivery to students, dynamically place students in “time out” and other creative policies. We strongly encourage potential customers to contact Red Lambda regarding their policy goals. Our motto is, “If you can dream it, we can automate it”.

User Management and Communication – Integrity is a *role-based traffic management* solution. As such, Integrity is designed to collect as much or as little user telemetry as desired by the customer, and to make that available for policy decisions and reporting. Integrity can restrict an infringer's traffic based on their identity and their role in the network, instead of basing decisions merely on their IP address. This capability enables customers to make more intelligent policy decisions that fit real-world, mobile computing environments.

Integrity's patent-pending user intelligence gathering system is capable of tracking where a user is located, when they are there, what resources they are using and what they are doing on the network at all times. Additionally, customers may configure Integrity to retain historical records of as much or as little of this information as required.

Integrity features a case-based incident handling system which pre-correlates all available historical data for each user, including identity, IP addresses, times, locations, bandwidth usage, protocol usage, hardware identification and more. This feature virtually eliminates the manpower overhead associated with tracing DMCA violations and presents all information in a single intuitive interface. Customers also have the power of a rich reporting engine built into Integrity for administrative reporting, compliance, and visualization.

Finally, because Integrity can be configured to collect user telemetry, it is also capable of communicating with end users and administrators as defined by policy. This includes sending notifications by email, IM, and RSS as well as delivering custom educational content via HTTP redirection and wildcard DNS entries.

2.1.1 Network Architecture

The vendor should provide descriptions of how its technology could be installed in typical networks including architecture diagrams.

Integrity is installed by simply connecting the machine running the Integrity software to a span port configured to monitor the desired networks. The hardware required for Integrity is typical 1U server hardware, running Windows XP/2003/Vista, Linux, Solaris 9/10 or OS X. Integrity is *not* typically installed on end user machines. Two simple architectural diagrams have been included to demonstrate how Integrity would be installed in a network to monitor the campus border and how it would be installed to monitor the internal campus network. Customers are free to install as many instances of Integrity as they wish at no additional cost, eliminating the costs (aside from hardware) for the ability to monitor the internal network.

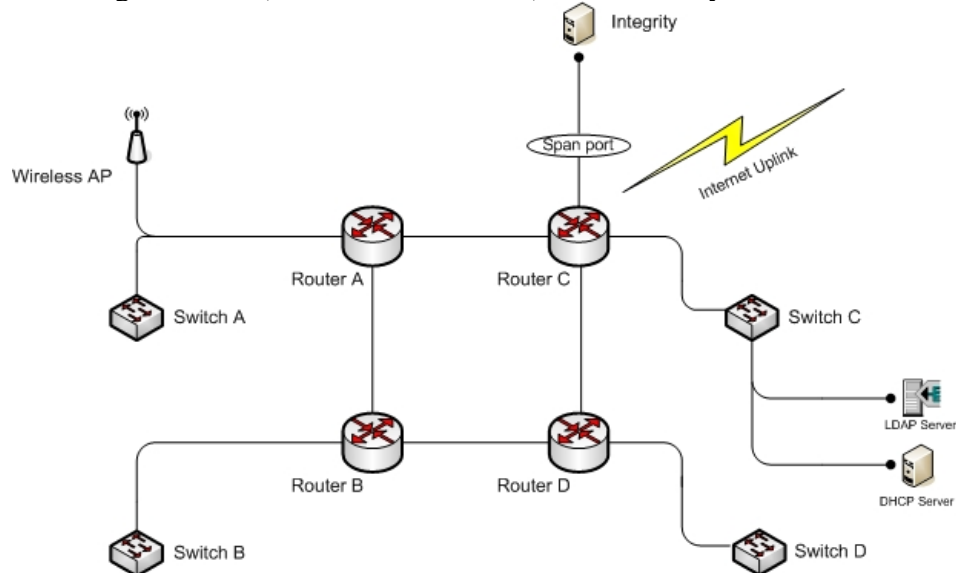


Figure 1. Integrity installed for border monitoring

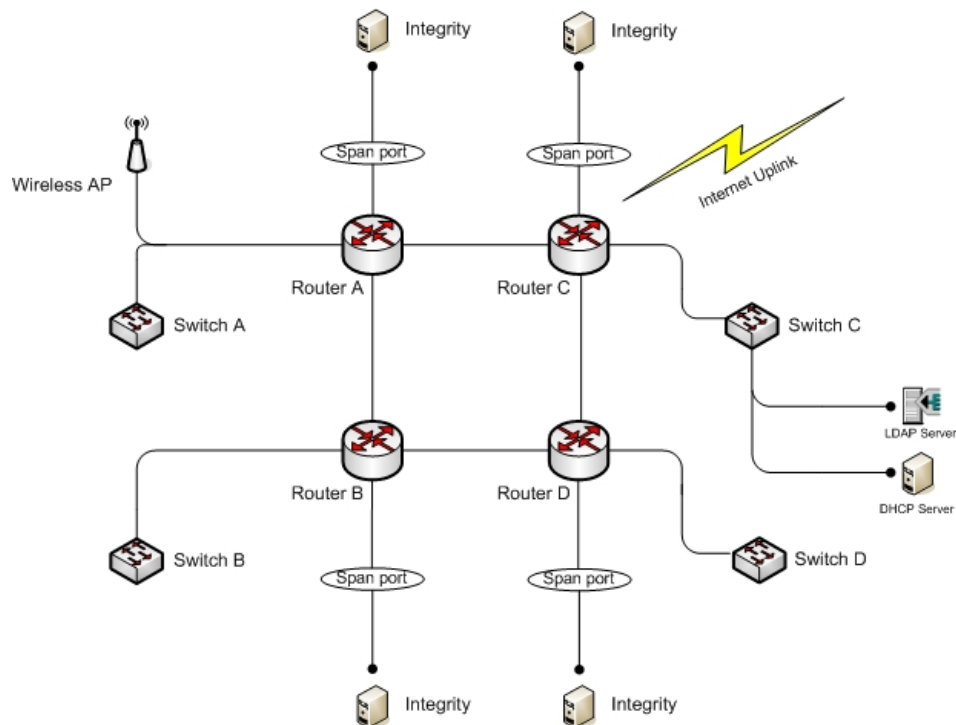


Figure 2. Integrity installed for border and internal monitoring

2.1.2 Scalability

Due to the high capacity of many university networks, particular reference should be made to the scalability of the tool. Each vendor should discuss the throughput of its technology (using aggregate bandwidth handled as the standard of measure), and the potential effects of its technology on network latency.

Currently, Integrity's monitoring system is conservatively certified for analysis using commodity server hardware at line rates up to 1Gbps with 128-byte packets. Under typical operating conditions in a production network, where the average packet size is significantly larger, Integrity is capable of line rate inspection in excess of 3Gbps. Integrity also supports jumbo frames, header compression, and other advanced technologies typically found in large enterprise networks.

As Integrity monitors traffic passively via span ports in the network, the technology cannot impose latency or cause network traffic to be dropped under high load conditions.

In addition, Integrity is based on Red Lambda's cGRID peer-grid platform, which means that all systems running Integrity in a campus environment will automatically work together to distribute the load under high load conditions. The more locations that are monitored, the more capable and resilient Integrity becomes.

2.1.3 Protocol Identification

The vendors should discuss whether and how network protocols are identified (e.g. by port number, by layer 7 analysis, etc.) and the methods that the vendor uses to update its software to detect new and mutated protocols. The vendor should address how the technology is able to adapt to changes in protocols as they evolve.

Integrity's monitoring system is a hybrid deep packet inspection (DPI) / behavioral analysis engine, capable of performing full OSI layer 2-7 inspection of IPv4 packets and featuring defragmentation, flow reassembly, and application decoding of common protocols and side-channels. Network protocols are identified by a combination of layer 7 analysis methods, including pattern matches and behavioral rules that involve information from both protocol headers (such as IP addresses, ports, etc.) and data fields.

Similar to common anti-virus software, updating Integrity's monitoring is as simple as updating the signature database. Customers can choose to update these signatures automatically or manually and may add, remove, and edit signatures as they see fit. Rigorous in-house testing procedures are applied daily to ensure the quality and accuracy of Integrity's signatures against live applications and not just static packet captures.

Deep packet inspection means that Integrity is capable of inspecting any bit inside of a packet. Signatures may include both pattern matching rules and behavioral rules, and use a standard XML-based rule grammar for customers who wish to create their own rules or modify the ones provided. Red Lambda does not believe in hiding the mechanics of its monitoring system, therefore, all signatures and signature grammars are well-documented and based on open standards. Each signature is different and each inspects multiple elements from packets or flows to detect infringements. Furthermore, each protocol can be detected using multiple signatures for various elements of detectable behavior, such as uploading, downloading, searching, and initialization.

As protocols evolve and change, Integrity is uniquely poised to respond to the increased monitoring demands. By combining behavioral analysis with deep packet inspection, Integrity detects the activity of protocols, even with the use of encryption or side-channels. Red Lambda has the highest level of demonstrated success in the industry of detecting encrypted and tunnelled protocols, and unlike other vendor's products, Integrity does not merely flag all encrypted traffic as suspicious. Finally, Red Lambda has additional pattern recognition technologies, including those developed under the charter of NSF research, that will be included in Integrity as they mature, future proofing the solution for years to come.

2.1.4 Granularity of Protocols

Each vendor should discuss its technology (where applicable) in terms of addressing those filesharing applications that employ multiple protocols (e.g. control, searching, file transfer, etc). Descriptions should be provided as to: which protocols does the vendor's technology detect; whether the technology can address each of these protocols independently; and whether different rate limits can be set for "search" vs. "file download."

Integrity includes a vast signature database which detects the operation of all known P2P protocols in addition to other file transfer and communication protocols commonly used as side channels. For each protocol, multiple detection vectors are provided which separately monitor uploading, downloading, searching, and initialization, depending on the level of encryption and steganography employed by the protocol. Customers may define policy based upon any of this information.

A current list of P2P protocols and clients detected is included, though it should be noted that this list evolves constantly.

Network	Number of Detection Vectors	PC Clients	Mac Clients	Linux Clients	Various
Skype	5				Skype
TOR	3				Various
FastTrack	4	Grokster	iSwipe	Apollon	
		iMesh Light	mldonkey	mldonkey	
		Jubster MP3 Finder	Poisoned		
		Kazaa	XFactor		
		Kazaa Lite Resurrection			
		Kazaa Lite Tools K++			
		KazaaGhost			
		K-Lite			
		Mammoth			
		mldonkey			
		Morpheus			
		Shareaza			
		TrustyFiles			
		XoloX			
ed2k	13	amule	amule	amule	
		eAnt	eDonkey	eAnt	
		eDonkey	Hydranode	eDonkey	
		eMule	iSwipe	Hydranode	
		eMule eF-mod	mldonkey	Lmule	
		eMule LSD	MLmac	mldonkey	
		eMule MorphXT			
		eMule Pawcio			
		eMule pHoenix			
		eMule Plus			
		Epicea			
		FileScope			
		HebMule			
		Hydranode			
		Jubster MP3 Finder			
		Lphant Plus			
		mldonkey			
		Morpheus			

		Neo Mule			
		RevConnect ++			
		Shareaza			
		Shareaza Plus			
		XoloX			
Kademlia	6	amule	mldonkey	mldonkey	
		eMule	Various eMule mod clients	Various eMule mod clients	
		eMule eF-mod			
		eMule LSD			
		eMule MorphXT			
		eMule Pawcio			
		eMule pHoenix			
		eMule Plus			
		HebMule			
		mldonkey			
		Neo Mule			
		RevConnect ++			
		SababaDC			
Overnet	4	eDonkey	eDonkey	eDonkey	
		Epicea	mldonkey	mldonkey	
		mldonkey			
		Overnet			
		Trusty Files			
Gnutella	5	AlienIdol	Acquisition	Apollon	CocoGnut
		Bearshare	Cabos	Gnewtellium	FrostWire
		BearShare Lite	Gtk-Gnutella	Gtk-Gnutella	giFT
		Cabos	iSwipe	LimeWire	Symella
		Deepnet Explorer	LimeWire	mldonkey	
		DM2	MacTella	Mutella	
		FileScope	mldonkey	Phex	
		FreeWire	Mutella	Qtella	
		Gluz	Phex	XNap	
		Gnucleus	Poisoned		
		i2PHEX	Qtella		
		iMesh	XFactor		
		Jubster MP3 Finder	XNap		
		KCeasy			
		Kiwi Alpha			
		Limewire			
		mldonkey			
		MoodAmp			
		Morpheus			
		MyNapster			
		NeoNapster			
		Nova P2P			
		P2PStorm Client			
		Phex			
		Shareaza			
		Shareaza Plus			

		Swapper			
		TrustyFiles			
		XNap			
		XoloX			
		Zultrax			
WinMX	5	WinMX			
		WinZO			
MP2P	2	Blubster			
		Piolet			
Ares	8	Ares			
		Warez			
BitTorrent	4	µTorrent (micro torrent)	Acquisition	Anatomic P2P	
		Anatomic P2P	Anatomic P2P	Azureus	
		Arctic Torrent	Azureus	BitTornado	
		Azureus	Bits on Wheels	BitTorrent	
		BitBuddy	BitTornado	BT Queue	
		BitComet	BitTorrent	BT++	
		BitLord	Blizzard Downloader	BtManager	
		BitPump	BT Queue	CTorrent	
		BitSpirit	BT++	Flash! Torrent	
		BitTornado	BtManager	freeloader	
		BitTorrent	Hydranode	Gnome BitTorrent	
		BitTorrentExperimental	iSwipe	Hydranode	
		Blizzard Downloader	Localhost	KTorrent	
		Blog Torrent	mldonkey	mldonkey	
		BT Queue	MLNet	MLNet	
		BT++	Opera 9 browser	Opera 9 browser	
		BtManager	rtorrent	Qbittorrent	
		Burst!	Rufus	QTorrent	
		Flash! Torrent	Tomato Torrent	rtorrent	
		G3 Torrent	TorrentFlux	Rufus	
		Hydranode	Transmission	TorrentFlux	
		Localhost		Transmission	
		Lphant Plus		Yet ABC	
		mldonkey			
		MLNet			
		MooPolice			
		Nova Torrent			
		Opera 9 browser			
		Rufus			
		Shareaza			
		Shareaza Plus			
		Torrent Searcher			
		TorrentFlux			
		TorrentSpy Rufus			
		TorrentStorm			
		TorrentTopia			
		TrustyFiles			
		Turbo Torrent			

		TurboBT			
		XBT Client			
		Yet ABC			
		ZipTorrent 1.3.6			
SoulSeek	4	Nicotine	Nicotine	Museek	
		SoulSeek	SolarSeek	Nicotine	
			SoulSeek	pysoulseek	
			soulseeX	PySoulSeek	
DirectConnect	6	BCDC++	ShakesPeer	Aquila	PtokaX
		CZDC	ShastaHub	Asami	
		DC++	Valknut	BCDC++	
		DirectConnect		CCCP	
		fulDC		Chiyo	
		McDC++		DB Hub	
		Py-DCHub		DCH++	
		Revconnect		DConnect Daemon	
		SababaDC		DC-QT	
		ShastaHub		DCTC	
		StrongDC++		Dolda Connect	
		Valknut		GtkDC	
		Verlihub		Idec	
		xHub		Linux DC++	
		YnHub		microdc	
				microdc	
				Py-DCHub	
				QuickDC	
				RCCP	
				ShastaHub	
				Valknut	
				Verlihub	
				xHub	
Gnutella2	5	5 Scope	Adagio	Adagio	Pocket G2
		Adagio	Caribou	Caribou	
		Caribou	MLDonkey	MLDonkey	
		FileScope			
		Gnucleus			
		iMesh			
		Kiwi			
		MLDonkey			
		Morpheus			
		Shareaza			
		TrustyFiles			
Filetopia	2	Filetopia			Torrentopia
NeoNet	6	Morpheus			
NNTP	4	mIRC			
		News Rover			
		NewsBin			
IRC	4	Xnews			
Our Tunes	4				Our Tunes

My Tunes	4				My Tunes
iTunes	4	iTunes	iTunes		
Hamachi	5	Hamachi			
WASTE	6				WASTE
SSH 1.x,2.x	2				Various
SOCKS 4, 4a, 5	18				Various
HTTP Proxy	4				Various
PHP Proxy	1				Various
Telnet	2				Various
ICMPv4	274				Various
DNS	31				Various
Windows filesharing (SMB)	14				Various
FTP	6				Various
SFTP	6				Various
XMPP	8				Various
AIM	8				Various

2.1.5 Product Configuration and Installation

The vendor should describe how much downtime is required for installation and maintenance and what elements of the network are involved. The degree of network integration and integration with other products should be presented. The vendor should discuss if the technology requires initial setup by individual users or requires installation of any components on individual user PCs. Specify if there are other setup or maintenance actions at the user level.

Configuration and installation of Integrity is straightforward, and requires no setup or maintenance at the user level or with user machines. Integrity is designed to passively monitor the network via span ports, therefore, no downtime is associated with the installation of Integrity. Customers are free to activate as many or as few of Integrity's features as they choose, and are not locked in to pre-determined configurations. By default, Integrity is setup to monitor and log infringements with no special configuration required. Common use cases follow, along with their integration requirements (these are not the only possible configurations).

- **Monitoring Only**
 - A span port or ports configured to monitor the desired networks

 - **User Telemetry Only - Three integration options, which may be combined**
 - **Option 1 (provides user location, device, IP address & identity):**
 - ◆ Access to Radius logs for 802.1x
 - **Option 2 (provides user location, device, IP address & identity):**
 - ◆ SNMP READ access to switches, access points, and other network devices hosting monitored users
 - ◆ DHCP server(s) log access
 - and either**
 - ◆ Access to Active Directory, NDS, or LDAP sign-on logs
 - or**
 - ◆ Access to network hardware registration database, such as NetReg or customer's system
 - **Option 3 (provides user location, device, IP address):**
 - ◆ SNMP READ access to switches, access points and other network devices hosting monitored users
 - ◆ DHCP server(s) log access

 - **Monitoring with User Telemetry & Enforcement Response (Layer 2, VLAN Steering)**
 - A span port or ports configured to monitor the desired networks
- and**
- **User Telemetry Information - three integration options, which may be combined**
 - ◆ **Option 1 (provides user location, device, IP address & identity):**
 - Access to Radius database for 802.1x

 - ◆ **Option 2 (provides user location, device, IP address & identity):**
 - SNMP READ/WRITE access to switches, access points and other network devices hosting monitored users
 - DHCP server(s) log access
 - and either**
 - Access to Active Directory, NDS, or LDAP sign-on logs
 - or**
 - Access to network hardware registration database, such as NetReg or customer's system

 - ◆ **Option 3 (provides user location, device, IP address):**
 - SNMP READ/WRITE access to switches, access points, and other network devices hosting monitored users
 - DHCP server(s) log access

2.1.6 Content Identification

If the technology operates at the individual file level and is intended to selectively identify communications that represent potential infringements of copyright law, explain in detail how the technology will identify such content. The vendor should specify what categories of content can be identified (i.e. compressed audio files, video, images, etc). The vendor should list any external content databases that are required, and whether or not they are proprietary. The vendor should indicate what information, if any, is captured and reported for further analysis and actions.

Integrity does not attempt to perform content identification of any kind, strictly using application-layer information for protocol identification. Integrity also does not record or log user identity information such as email addresses, IM accounts, or website logins from application-layer information.

2.1.7 Examination of Network Packets or File Content

Each vendor should indicate any aspects of the use of its technology that requires the examination or “opening” of network packets or files of information in order to carry out the technology’s work. The vendor should indicate which fields of the Internet packets and which components of corresponding files are used by the technology and in what way. The vendor should include not only the degree of content inspection that is required in order to make the technology work, but also the degree of inspection and logging that the technology is capable of performing (even if “turned off” by the user or system administrator).

Integrity's monitoring system is a hybrid deep packet inspection (DPI) / behavioral analysis engine, capable of performing full OSI layer 2-7 inspection of IPv4 packets, and featuring defragmentation, flow reassembly, and application decoding of common protocols and side-channels. Signatures define what is detected and are provided by Red Lambda for all known P2P protocols as well as other types of file transfer and communication protocols. These signatures are open and transparent to customers. Red Lambda does not provide any Integrity signatures which inspect the file content or personal information being transmitted. If customers desire network traffic to be analyzed, the Integrity deep packet inspection engine **must** be activated. The deep packet inspection engine is not required for Integrity's other functions, such as user telemetry gathering.

Customers have full control over which signatures are used and may also add, edit, or delete signatures as desired. Updates to Red Lambda-provided signatures are provided to customers as part of their support agreement and are included free for the first year along with all updates to the software. In addition, customers may determine which signatures to apply to which users or user groups and the policy of their application (e.g. at certain times of day, from certain locations, using certain hardware, etc.).

Deep packet inspection means that Integrity is capable of inspecting any bit inside of a packet. Signatures may include both pattern matching rules and behavioral rules and use a standard XML-based rule grammar, which is documented for customers who wish to create their own rules or modify the ones provided. Each signature is different and each inspects multiple elements from packets or flows to detect infringements. Furthermore, each protocol is detected using multiple signatures for various elements of detectable behavior, such as uploading, downloading, searching, and initialization. A complete list of all signatures is available upon request. Currently, besides each OSI layer's *data field* information, the standard header information which **can** be inspected is as follows.

Layer 3 – Network Layer

Protocol: IP

Header Field	Description
Version	The version number of the IP protocol in use.
Internet Header Length (IHL)	Describes the length of the header in 32-bit words
Type of Service (TOS)	RFC 791-defined Type of Service bits
Total Length	Defines the entire datagram size in bytes
Identification	Identification field primarily used for fragments of an original IP datagram
Flags	Used to control or identify fragments

Fragment Offset	Indicates the offset of a particular fragment relative to the beginning of the original unfragmented IP datagram
Time to Live (TTL)	Usually indicates the number of hops remaining before being dropped
Protocol	Defines the protocol used in the data portion of the IP datagram; RFC 790
Header Checksum	Used for error checking of the header
Source Address	The IP address sending the IP datagram
Destination Address	The IP address receiving the IP datagram
Options	Rarely used optional header fields

Protocol: ARP

Header Field	Description
Hardware Type (HTYPE)	The data link layer protocol in use
Protocol Type (PTYPE)	The network layer protocol in use
Hardware Length (HLEN)	Length in bytes of a hardware address
Protocol Length (PLEN)	Length in bytes of a logical address
Operation	Indicates the operation being performed, 1 for request, 2 for reply
Sender Hardware Address	Hardware address of the sender
Sender Protocol Address	Protocol address of the sender
Target Hardware Address	Hardware address of the intended receiver
Target Protocol Address	Protocol address of the intended receiver

Protocol: ICMP

Header Field	Description
Type	ICMP type as defined by RFC 792
Code	Further specification of the ICMP type
Checksum	Error checking data calculated from the ICMP header+data
ID	ID value
Sequence	Sequence number

Layer 4 – Transport Layer

Protocol: TCP

Header Field	Description
Source Port	Identifies the sending port
Destination Port	Identifies the destination port
Sequence Number	Used in conjunction with the SYN flag to determine sequence number
Acknowledgment Number	Used in conjunction with the ACK flag to determine next byte expected
Data Offset	Specifies the size of the TCP header in 32-bit words
Reserved	For future use; should be 0
Flags	Control bits, contains 8 bit flags
Window	The number of bytes past the sequence number that the receiver is willing to receive
Checksum	Used for error-checking the header and data
Urgent Pointer	Used in conjunction with the URG flag to indicate offset of the last urgent data byte
Options	Variable bits used to indicate other TCP options

Protocol: UDP

Header Field	Description
Source Port	Identifies the sending port
Destination Port	Identifies the destination port
Length	Specifies the length in bytes of the entire datagram
Checksum	Used for error-checking the header and data

Protocol: SCTP

Header Field	Description
Source Port	Identifies the sending port
Destination Port	Identifies the destination port
Verification Tag	A random value created to distinguish stale packets from a previous connection
Checksum	Used for error-checking the header and data
Chunks	RFC 2960 Chunks

Protocol: DCCP

Header Field	Description
Source Port	Identifies the source port
Destination Port	Identifies the destination port
Data Offset	The offset from the start of the DCCP header to the start of the data in 32-bit words
CCVal	Used by the HC-Sender CCID
Checksum Coverage (CsCov)	Determines the parts of the packet covered by the Checksum field
Checksum	Used in conjunction with the CsCov to determine checksum
Reserved	Reserved bits
Type	The type of the packet
Extended Sequence Numbers	Bit field indicating the use of an extended header
Sequence Number	Identifies the packet uniquely in the sequence of all packets
<i>Additional RFC 4340 fields</i>	Dependent upon type

Layer 7 – Application Layer

Protocol Decoders

Decoder Type	Description
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
FTP/SFTP	File Transfer Protocol/Secure File Transfer Protocol
HTTP	Hyper Text Transport Protocol
POP3	Post Office Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
Telnet	
TLS/SSL	Secure Socket Layer
IMAP	Internet Message Access Protocol
SOAP	Simple Object Access Protocol (deprecated name as of v1.2)
RPC	Remote Procedure Call
XML-RPC	XML-encoded RPC, transported over HTTP

2.1.8 Distribution Systems

Each vendor's response should specifically list all filesharing protocols or networks for which the technology is effective. In addition, the vendor should list other distribution systems, such as FTP, IRC, Usenet, for which the technology is applicable.

Integrity is capable of monitoring many other distribution, side-channel, and hiding protocols other than P2P protocols. Customers may also create their own signatures to detect anything they desire. The current list of additional protocols is as follows, though it should be noted that this list evolves constantly:

Protocol	Number of Detection Vectors	Windows Client	Mac Client	Linux Client	Other
Skype	5				Skype
TOR	3				Various
NNTP	4	mIRC			Various
		News Rover			
		NewsBin			
IRC	4	Xnews			Various
Our Tunes	4				Our Tunes
My Tunes	4				My Tunes
iTunes	4	iTunes	iTunes		
Hamachi	5	Hamachi			
WASTE	6				WASTE
SSH 1.x,2.x	2				Various
SOCKS 4, 4a, 5	18				Various
Proxies					
HTTP Proxy	4				Various
PHP Proxy	1				Various
Telnet	2				Various
ICMPv4	274				Various
DNS	31				Various
Windows filesharing (SMB)	14				Various
FTP	6				Various
SFTP	6				Various
XMPP	8				Various
AIM	8				Various

2.1.9 Resilience of the Technology to Countermeasures

Each response should indicate the technology's ability to resist:

- i. Countermeasures by filesharing software, for example, file compression, data encryption, etc.
- ii. Circumvention efforts by users (i.e. port tunneling, proxy servers, fragmented packets, etc).
- iii. Denial-of-service or other attacks against components of the technology.

Integrity has been designed from the ground up to resist countermeasures and has been vetted for over five years in production university environments where students, faculty, and staff have actively tried to circumvent the system. Integrity's highly survivable architecture evades the countermeasures:

- **Countermeasures by filesharing software:** Integrity's detection engine was designed from the beginning with the assumption that P2P protocols would all be encrypted one day. Because of that assumption, Integrity combines behavioral analysis with traditional pattern matching for detection in the face of data encryption, file compression, and steganography. Since 2005, Integrity has been the only product able to make and demonstrate this claim.
- **Circumvention efforts by users:** Originally developed and implemented at a major research university trying to solve the same problem, Integrity was designed with the assumption that users would actively try to circumvent the system using side channels, fragmentation, and proxies. Because of that assumption, Integrity combines behavioral analysis with traditional pattern matching to assure detection in the face of side channel hiding, fragmentation, and proxies.
- **Denial-of-service attacks:** While any network device can be affected by denial-of-service attacks, Integrity is capable of outsurviving many of the network components that it relies on while operating. Because Integrity is based on Red Lambda's patent-pending cGRID peer-grid architecture, Integrity dynamically load balances and fails over during high load situations. Participating Integrity systems automatically self-organize, virtually eliminating provisioning overhead during emergencies. Finally, customers are free to run as many instances of Integrity as they see fit at no additional cost, allowing them to automatically scale their security architecture as need requires.

2.1.10 Testing and Installed Base

Each vendor should provide descriptions of the extent of testing of its technology, particularly the testing procedures employed prior to releasing an updated version (e.g. an updated detector) and specific examples (where available) of how technology applies in real-life situations. The vendor should describe the features, maturity, status, availability, and installed base of its technology for each version that is currently supported.

- **Features:** Please see section 2.1 for a detailed treatment of the current features of Integrity.
- **Maturity Status:** The current release version of Integrity is v1.2.3. This release is considered to be a fully stable, mature product release. The next planned release of Integrity is v1.3, scheduled for release Q3 2008. All non-critical or security related software updates receive a minimum of 90-days continuous, automated integration testing before release, in addition to rigorous hands-on testing on a mock production network using typical hardware found in universities. Signature updates are made available as required to customers on a daily basis and are vetted both by automated consistency testing using live applications as well as static packet captures.
- **Availability:** Integrity has been in broad commercial availability since May 2007.
- **Installed Base of Technology:** Integrity is currently in production at three major US research universities and in pilot testing at an additional five locations in higher education and K-12 environments.

2.1.11 Competitive Approaches

Each vendor should provide clear descriptions of how its technology compares to other known competitive approaches and the benefits of its technology over competitive approaches.

Integrity Compared to Competitive Approaches

- **Compared to Content Inspection Technologies**
 - Unlike content inspection technologies, Integrity's protocol detection abilities do not diminish in the face of encryption and steganography.
 - Integrity is able to analyze network traffic at significantly higher line rates
 - Integrity has higher protocol identification rates, and significantly lower false positives
- **Compared to Products Blocking Connections with TCP Resets**
 - Integrity's responses are not limited to blocking TCP connections
 - Integrity's layer 2, 3, 4 and 7 responses are dramatically more difficult to bypass, and impossible in some configurations; superior mitigation
 - Integrity's responses are capable of selectively blocking based on the telemetry of the user, including identity, group membership, location, time, hardware used, etc.; superior resolution and flexibility
- **Compared to All Competitive Products**
 - Integrity is the only product which delivers all the requirements of the Task Force's hypothetical scenario today (see section 2.1.13)
 - Integrity is the only product with broadly documented, conclusive results in the public domain (US Congressional Testimony, 2004, 2005)
 - Integrity is the only product which can be expanded to monitor the internal network with no additional software or licensing costs to the customer
 - Integrity is the only product which can make enforcement decisions based on the identity of the user
 - Integrity is the only product which can dynamically enforce policy as users roam from machine to machine and location to location without requiring reinfringements, or local installation of software on user machines
 - Integrity is the only product which enables broad automation of the policy processes associated with filesharing, including those involving judicial case management, ticket management, content delivery, notification, ERP integration and directory integration

Red Lambda's Competitive Technology Edge

- First to offer comprehensive *role-based traffic management* for combating P2P filesharing, side-channels, botnets, and other inappropriate network use
- First to develop a vendor-agnostic network user intelligence gathering system
- First to develop a service-oriented P2P computing architecture (cGRID)
- First to create an unsupervised anomaly detection system that performs life-long learning while evolving its own memory

2.1.12 Third-party Components

Each response should describe any third-party components required by the technology that are not provided by the vendor, but necessary for implementation (i.e. content databases, etc).

Integrity has no specific dependency on third-party components, however, the ability to use identity for policy is dependent on either the implementation of 802.1x, OR Active Directory, NDS, or LDAP sign-on OR a database or file-based user hardware registration system such as NetReg. In the event that there is no way to associate user identity with hardware usage, policy will be limited only to the available information configured to be collected by the customer, including IP addresses, location, date and time, protocol, etc.

2.1.13 Comparison with Hypothetical Scenario

Technology and its capabilities to respond to the hypothetical scenario should be discussed.

All participants thought that one example solution held promise for widespread adoption—a technology that allows all traffic to flow through the network but automatically notifies the campus judicial system and/or the user when it identifies a potentially infringing transmission. This proposed system was looked upon favorably by many of the higher education representatives because it has the potential for increased privacy protections and allows a graduated response at the institution's discretion after the fact, similar to the operation of external DMCA notices. Depending on configuration, it could have the advantage of detecting on-campus as well as off-campus violations, however, and so would have correspondingly greater effect. The more automated the system could be, the better, according to campus network representatives. The possibility of generating large numbers of infringement claims makes automation a most important quality. However, the privacy of the content would need to be protected. From a performance and design perspective, the group found an out-of-band, tap-like technology to be far preferable to an inline device. The participants felt that such a solution could be important to most campuses.

In comparison with the hypothetical scenario, Integrity delivers **all** functions specified:

- *Allows all traffic to flow through the network but automatically notifies the campus judicial system and/or the user:* This requirement demands three important elements, **all** of which Integrity provides. First, the ability to passively inspect traffic without blocking it. Second, the ability to collect user telemetry so that the system knows *who* was sending the traffic. Third, the ability to notify judicial affairs, potentially via a judicial database update, email, etc., and the ability to notify the user, potentially via email, IM, or other mechanism.
- *Allows a graduated response at the institution's discretion after the fact, similar to the operation of external DMCA notices:* This requires the system to perform various actions in either an automated or manual fashion following detection, potentially after a certain number of repeat infringements are detected, or based on other factors (such as enrollment status, judicial history, etc.). Integrity is designed to be used in exactly this fashion and can be configured to periodically check databases for updates in case status which may require additional action. In addition, Integrity can be configured with a blend of automated and manually-triggered graduated responses, including escalating policies and ones requiring information from external databases for decision making.
- *Depending on configuration, it could have the advantage of detecting on-campus as well as off-campus violations:* Integrity is designed to be installed in a distributed environment and customers are able to install as many instances of Integrity as required for their environments at no additional licensing or maintenance cost. With Integrity, monitoring the internal network is as simple as setting up more monitoring points and allowing the Integrity systems to self-organize into one cohesive system. Additional policy configuration and identity integration are unnecessary. Please see section 2.1.1 for a treatment of architectural details.
- *The more automated the system could be, the better, according to campus network representatives. The possibility of generating large numbers of infringement claims makes automation a most important quality. However, the privacy of the content would need to be protected:* This requirement demands two elements, **both** of which Integrity provides. First, the ability to automate the detection, notification, escalation, and adjudicatory processes. Second, the ability to protect the privacy of the content being transferred. Rich policy control and process automation are hallmarks of Integrity. In fact, the original creators of the software were award the State of Florida's Davis Award for outstanding cost recovery for using Integrity to automate the entire lifecycle of the filesharing problem at the University of Florida. As to respecting the privacy of the content, Integrity does not inspect content in any way; please see section 2.1.6 for a detailed treatment of this material.
- *From a performance and design perspective, the group found an out-of-band, tap-like technology to be far preferable to an inline device:* Integrity operates as a passive, out-of-band system.
- *The participants felt that such a solution could be important to most campuses:* Red Lambda is pleased to note that **Integrity delivers all the requirements of this hypothetical solution today in full** and looks forward to working with customers who are interested in implementing a similar solution.

2.2 Performance w/respect to the Requirements Described in the 2007 Workshop Report

Provided in this section is a brief summary of the requirements that were documented at the April 2007 Workshop. Each vendor should refer to the report itself (<http://www.educause.edu/ir/library/pdf/CSD5170.pdf>) for a more detailed presentation. The vendor should provide a description on how their technology responds to the requirements presented in each of the areas in the Workshop Report.

2.2.1 Identifying Infringing Traffic at the Campus Border

The level of false positives (i.e., transmissions that are identified as infringing but are not) should be controllable by each individual campus. The settings that determine how many, or how few, false positives are generated should be selectable, rather than hard-wired into the solution. The solution should be time synchronized with the campus network to support accurate identification of the current assignment of IP addresses. The system should have a method for dealing with false positives (such as some sort of adjudicatory process that could be initiated by the student in response to an infringement notification). Further, it must be able to guarantee that critical traffic (e.g., network control signals) will always pass through the system unhindered.

The solution must be network friendly to the existing campus network architecture and “fail open.” That is, it must have no effect on network traffic in the case of system failure. The solution must be transparent to unrecognized traffic and induce no additional latency and jitter. The solution should operate in a way that leaves decisions to notify users and the Network Operations Center (NOC) of flagged infringements up to the individual campus. It should have the capability and flexibility to identify and/or block at either the application level or at the individual media file content level.

The solution must be able to evolve technologically as new protocols, signatures, modalities, and other changes occur in the filesharing technologies. Updates and upgrades should be supplied automatically by the vendor and must be easy to install and operate. The solution should work not only at the current speed, but also have the ability to be upgraded through a range of speeds (E.g. 1-10-100 Gigabits/sec) in tandem with the campus network.

Logging should be capable of being turned on or off, as well as be able to set the retention and deletion dates of logs, determine what is captured in the logs, and how those logs are used. The ability to move logs to other devices should also be a capability, and such logs should be protected.

2.2.1.1 Handling False Positives

Integrity has a resistance to false positives by design. By using multifactor deep packet inspection and behavioral signatures in conjunction with multiple signatures for each protocol, false positives for each protocol have been minimized or eliminated (depending on protocol). To give an indication of the success of this approach to ferriting out false positives, Integrity only had four false positives in five years of production operation at the University of Florida where it was originally developed.

Additionally, customers are able to individually select the type and method of detection for every protocol AND for every user, giving direct control over the potential level of false positives far exceeding the granularity of competitive products.

Finally, Integrity's rich policy system can be configured to avail students of an automated adjudicatory process when they are in dispute of an alleged violation of campus policy. By automating the entire lifecycle of the filesharing problem, and not just detection and response, Integrity is able to provide a much more consistent and predictable end user experience.

2.2.1.2 Network Friendliness

Integrity was designed with the goal of having a zero-residue network footprint. Many features were incorporated into Integrity explicitly to make it more friendly to large enterprise networks, including:

- NTP or STP integration for automatic time synchronization across the enterprise.
- Explicit white and blacklisting guarantees that critical traffic can never be misclassified or impacted.
- Passive monitoring design is transparent to network traffic and guarantees zero impact to network operation in the event of an Integrity system failure. Furthermore, it eliminates any possibility of jitter or latency introduction.
- Support for advanced networking features such as hierarchical, multilevel NAT backtrace, jumbo frames, and header compression.
- Fully customizable policy engine allows each campus to define their notification and enforcement policies in any way desired, including specifying no-response, monitoring-only policies.
- Integrity automatically load balances across multiple systems, providing automatic redundancy and improved performance.
- Integrity was designed to be scalable in excess of 10 million monitored endpoints, working in a federated environment; there is no practical limit to the number of systems which can run Integrity due to its underlying peer-grid architecture, offering enormous scalability with no additional investment.

2.2.1.3 Technical Evolution

As protocols evolve and change, Integrity is uniquely poised to respond to the increased monitoring demands. By combining behavioral analysis with deep packet inspection, Integrity detects the activity of protocols even with the use of encryption or side-channels. Red Lambda has the highest level of demonstrated success in the industry of detecting encrypted and tunnelled protocols, and unlike other vendor's products, Integrity does not merely flag all encrypted traffic as suspicious. Finally, Red Lambda has additional pattern recognition technologies including those developed under the charter of NSF research. These technologies will be included in Integrity as they mature, future proofing the solution for years to come.

Regarding future scalability, Red Lambda has steadily scaled inspection rates to meet customer needs, and currently conservatively certifies Integrity's monitoring engine at 1Gbps with 128-byte packets using commodity server hardware. It is expected that the broad availability of multi-core processors and 10Gb ethernet cards will result in a commodity hardware certification of Integrity for inspection at 10Gbps by Q1 2009.

Finally, all updates to software and signatures are made automatically by default with Integrity and customers have full control over the update process should they choose to manually control it. Integrity includes the first year's software and signature updates for free and all recurring service contracts also include software and signature updates.

For additional information regarding Integrity's ability to adapt to the changing filesharing protocol landscape, please see section 2.1.9.

2.2.1.4 Log Flexibility

With Integrity, customers have full control over the content, retention and deletion schedules for all logged information as well as full control over how that information is used. Customers may select to retain as much or as little information as they choose, including the requirement of Integrity to discard records immediately following the identification of infringement.

All data collected by Integrity is stored in an industry standard SQL-accessible database, completely accessible to customers and protected by database best practices. Customers may also choose to use their own existing database infrastructure should they so desire. Furthermore, like all Red Lambda products, customers have full access to database schema information as well as detailed documentation about how to use their data in custom systems.

2.2.1.5 Identifying Infringing Traffic

Please see sections 2.1.3, 2.1.4, 2.1.6, 2.1.7 & 2.1.8 for a detailed treatment of this issue

2.2.2 Responding to Infringing Traffic at the Campus Border

The technology should be selectively configurable to perform a range of responses, and the response policy at the campus level should be capable of being modified according to such considerations as source, destination, etc. The solution should be capable of integration with existing judicial systems so that the campus could elect to have an automated response to those users committing infringement violations. A flexible white list of addresses that will never be blocked should accompany a solution that blocks at the border.

Please see section 2.1 & 2.2.5 for a detailed treatment of this issue

2.2.3 Identifying Infringing Traffic Local to the Campus Network

Technology solutions should be capable of identifying infringing traffic within subnets at the lowest possible level. Technology implemented on the internal network must meet all the network-friendly requirements discussed in the border case in 2.2.2.

Please see sections 2.1.1 – 2.1.8 for a detailed treatment of this issue

2.2.4 Responding to Infringing Traffic Local to the Campus Network

Technology implemented must support the usual topologies of internal campus network architecture. The technology cannot require routing all traffic through single points of failure. The overall solution must not interfere with the legal access to and transport of, non-infringing or authorized content within the campus network. The technology should provide the ability to select different levels of responses to flagged infringements. A technology designed to identify infringing traffic local to the net should support multiple CIDR blocks, or IP address blocks.

Please see section 2.1 & 2.2.5 for a detailed treatment of this issue

2.2.5 Supporting the Campus Judicial System

Technology should provide appropriate, integrated, automated support for the campus judicial system and an interface for reporting flagged infringements. Communication between the identifying technology and the network operators (judicial system) should be secure. The technology should be flexible enough to provide campuses with a broad range of metadata and allow each campus to select what information is required. Communication of evidence to and from campus systems should be tamper-proof.

Integrity was designed to integrate with judicial systems from the ground up and features the ability to automate case management in conjunction with these judicial systems, either commercial or custom. Integrity supports multiple open standards for communication with external systems, including: RSS, SMTP, POP3, IMAP, HTML, Jabber, AIM, SNMP, SOAP, and SQL. Customers are free to completely customize the judicial response process, including notification, escalation, enforcement, and metadata retention policies for their environment. Customers may also use their own databases for some or all of the data either stored or collected by Integrity at their discretion.

Integrity organizes infringement information based on a user's identity in a case-based incident handling system. This system, which automatically correlates all known information about a user in one simple interface, is designed to eliminate the information overload associated with traditional security tools. From within this interface, customers may view all historical information, and control the status of cases in addition to creating extensive detail reports in support of judicial process.

Regarding secure communications, all internal Integrity communications are encrypted using TLSv1.1 which prevents message tampering through digital signatures. The security of external communications is limited only by the protocol employed though secure versions have been implemented and are favored where available.

2.2.6 Avoiding Disruption of All Non-infringing Traffic

Technology should not affect the transmission of any and all non-infringing traffic. It should have the ability to support access to and distribution of content that has been flagged as potentially infringing, but could be permissible under fair use.

Since Integrity is based on passive monitoring and active response, it is not capable of affecting the transmission of non-infringing traffic, except by false-positive. Customers may configure the enforcement policy after detection to be as strict or as relaxed as they choose; they are not forced to restrict protocols just because their use could potentially be infringing. This flexibility enables customers to set the response that is most appropriate for their environment, and Integrity's broad library of responses ensures the most appropriate method is always available.

Additionally, because Integrity is not an inline device, it does not represent a choke point or single point of failure for the transmission of network traffic.

2.2.7 Considerations for Purchase and Operations

The technology should possess the characteristics of predictability, transparency, auditability, and scalability. Pricing must be predictable and include cost to purchase (or license), install, operate, maintain and upgrade.

Please refer to the following sections for treatment of these issues:

Predictability – 2.1

Scalability – 2.1.2

Transparency – 2.1

Auditability – 2.2.1.4 & 2.2.5

Pricing – 2.2.11

2.2.8 Intellectual Property

This section of the vendor's response to the RFI should provide information concerning intellectual property associated with the technology. The information should provide insight as to whether any patents have been applied for, when and in what territories, and what (if any) claims have been granted. Where a patent has been granted, the vendor should provide the patent number and attach an abstract of the patent.

The vendor should remember that submissions to this RFI are governed by Section 7. The vendor should not have the expectation that information held to be confidential will necessarily remain within the Joint Committee. (Confidential information should not be included in the response.)

Integrity is based on intellectual property licensed from the University of Florida and developed internally at Red Lambda. This intellectual property has multiple patents pending and covers holistic network management, service-oriented computing in peer environments, unsupervised pattern recognition, and process automation technologies. Additional information regarding the underlying intellectual property is available to interested parties under a nondisclosure agreement.

2.2.9 Corporate Characteristics and Resources

This section of the vendor's response to the RFI should provide information about the vendor's corporate capabilities. Include information about the vendor in terms of general and specific corporate characteristics: size, personnel, facilities, year of organization, corporate history, clients, revenues, capitalization, investors, etc. Information about corporate products or technologies other than that directly applicable to this RFI should not be included.

Red Lambda, Inc. delivers highly survivable, distributed security solutions for network defense and management. Our solutions combine patent-pending end-user intelligence gathering, pattern recognition, and cGRID peer-grid systems with network security automation to provide *role-based network security* for the first time to customers. Believing that security policies are written for people and not IP addresses, Red Lambda's products allow customers to secure their networks and ensure compliance without concern for where their users are located, what IP address they have, or what device is used to access the network. By constantly mapping identity and behavior, assessing risk, and dynamically applying security controls based on a user's role and usage, Red Lambda's solutions provide the most comprehensive adaptive network security available.

Red Lambda, Inc. is a venture-backed portfolio company of V2R Group, Inc. with corporate offices in Orlando, Florida. Founded in 2005, Red Lambda was formed with award-winning technology originally developed at the University of Florida (UF) in 2002 for combating malicious and inappropriate use of the network. This technology creates a peer-grid which defends the network, characterized as a 'white-net' or 'white hat botnet'.

Red Lambda's first product, Integrity, has been recognized as a 'First in World' achievement for merging user telemetry with network traffic management. Integrity benefits from over five years of production use at UF and other universities as a role-based traffic management system. Integrity has received nationwide recognition from the US Congress as well as the Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA) for its efficiency in stemming P2P file-sharing. Integrity delivers unprecedented visibility, award-winning cost recovery, flexibility of control, and near zero-effort scalability to millions of endpoints. Red Lambda's mission is to make network security intuitive and accessible by eliminating the constraints of scale and identity via ground-breaking technology.

2.2.10 Pilot Testing

It is possible that certain colleges or universities may elect to test some of the technologies. The selection of those technologies will be done by the individual campuses based in part upon the results of the knowledge base created as a result of this RFI. Many factors will enter into the decision as to which technologies will be tested. One significant factor will be the level of interest and potential involvement of the vendor in the actual testing. Therefore, the vendor should present the vendor's concept for testing its technology in a real-life situation on campus. The vendor should also provide its concept for an evaluation license and any conditions that are associated with it.

The vendor's schedule for implementing its particular technology should be provided, allowing a period of sufficient duration to test and evaluate the results of that implementation.

The vendor should also provide information regarding the costs that might be incurred by a campus during pilot testing as well as information on whether or not they might consider conducting testing on a pro bono basis.

Red Lambda offers a pilot testing program to interested customers, including professional services for planning and installation. Typical pilot testing licenses involve a 30-90 day evaluation period with documented objectives and success criteria for purchase. Professional services provided during the pilot testing phase are typically waived in the event that prospective customers purchase Integrity.

2.2.11 Commercial Terms

*This section of the vendor's response to the RFI should discuss, in general, information about the commercial terms for its product (e.g. requirements for an annual license, requirements for annual maintenance, ability for one-time purchase). In those cases where the vendor has published prices for the subject technology, the vendor should provide those prices. If standard licenses exist, they should be provided as well. **In no instance should the vendor provide cost information that would not be considered public information.***

Integrity has simple per-seat pricing, ranging from \$1-\$10/per seat MSRP, depending on volume, with a 1,000 seat minimum. This license permits customers to operate Integrity in as many locations as needed, with no additional charges per monitoring location or per server. Red Lambda also offers educational discounts and reference account partnerships to interested parties. Initial purchases includes 1 year of Silver level support as well as all software and signature updates free of charge. Red Lambda offers professional services covering installation, training, and policy advisory at an additional charge, depending on the scope of the project. Recurring costs are limited to a customer's support contract and depend on volume and level of support. All software and signature updates are included as part of the customer's support contract.

Other licensing options, including one-time purchase and unlimited site licenses are available upon request. Interested customers should contact Red Lambda sales for specific information and consultation.

2.2.12 Additional Information

This section of the vendor's response should present other information or raise issues that the vendor considers important in terms of documenting its product.

3 Confidentiality

*This RFI solicits detailed information including information about the vendor's intellectual property. The vendor, in response to this RFI, **should not provide information that requires the protection of a nondisclosure agreement.***

*It is anticipated that an understanding of the capabilities of vendor technologies, gleaned from the response to this RFI, will be communicated to organizations affiliated with the Joint Committee of the Higher Education and Entertainment Communities. The vendors may or may not be given the opportunity to review and comment upon the documentation of **its individual technologies** prior to the release of such documentation, so the vendors' response to this RFI should be as complete as possible. Material that is considered proprietary or confidential can be referred to, but not included in the vendor's response to this RFI.*

Red Lambda acknowledges and accepts the Confidentiality information in this section.

4 Conflicts of Interest

The vendor should disclose any potential or existing conflict of interest that it may have in either its response to this RFI or in the conduct of pilot testing at campuses that elect to participate in such tests. Conflicts of interest should also be noted with respect to any other products or services that may be required in order to deploy the vendor's technology for this project.

Red Lambda has no conflicts of interest concerning its technology or implementation.

5 Readership and Dissemination

*The results of documenting the responses to this RFI will be reported by the Technology Task Force to the Joint Committee of the Higher Education and Entertainment Communities. The committee will share the information more widely in the form of a knowledge base. **It cannot be guaranteed that the information in the knowledge base concerning the technology responses to this RFI will be limited to those parties.***

Red Lambda acknowledges and accepts the Readership and Dissemination information in this section.

6 Miscellaneous

6.1 No Obligations

The Technology Task Force of the Joint Committee of the Higher Education and Entertainment Communities reserves the right to cancel this RFI at any time. Technologies may or may not be selected for pilot or evaluation testing at the discretion of individual campuses.

Red Lambda acknowledges and accepts the Obligation information in this section.

6.2 Neutrality

The Technology Task Force of the Joint Committee of the Higher Education and Entertainment Communities will neither recommend nor approve any response to this RFI. The task force will not endorse specific business models or technologies. Evaluation and testing that may be conducted by individual campuses of selected technologies will in no way indicate a preference for any technology or vendor over another competing technology or vendor.

Red Lambda acknowledges and accepts the Neutrality information in this section.