

# Grid Enabled Internet Instruments

Peter Komisarczuk, Christian Seifert, Dean Pemberton, Ian Welch  
School of Mathematics, Statistics and Computer Science,  
Victoria University of Wellington,  
Wellington, New Zealand

{Peter.komisarczuk Ian.Welch Christian.Seifert Dean.Pemberton} @mcs.vuw.ac.nz

*This paper introduces the Grid Enabled Internet Instrument concept and discusses instruments that are being developed at Victoria University to measure Internet quality. The first instrument is a Grid version of the network telescope for studying Internet Background Radiation (IBR) and the second is a hybrid client honeypot system using high and low interaction devices for scanning the web for malicious content and servers. A third instrument on VOIP quality has been approached through simulation. The GEII framework is a work in progress and the initial design is introduced in this paper as the basis of a new Grid of Internet sensors that could be deployed to improve Internet measurement and gain a global insight to Internet quality.*

*Keywords-component; IBR, honeypot, measurement, Grid*

## I. INTRODUCTION

The current and Next Generation Internet (NGI) support an increase in the number of offered services, bandwidth, systems, and managed devices. These network developments drive the need to protect users, measure/detect and determine the quality of the Internet using new network instruments, defences and quality measures. We are developing an Internet-scale quality of service measurement framework using Grid technology combined with emerging Internet instrumentation. Our proposed quality of service measures include: a “Safety Index” or “Compromise Index” measuring the potential for a vulnerable computer to be compromised; a “Malicious Web Server Index” measuring the percentage of malicious web servers on the Internet; a “Background Traffic Intensity” measuring the volume of unsolicited non productive traffic; and the mean R factor [17] of a network for VOIP traffic transmission quality.

The Grid Enabled Internet Instruments (GEII, see <http://www.mcs.vuw.ac.nz/~peterk/geii/>) project is developing a set of cooperative instruments that measure or scan components of the Internet and uses Grid technology [4] to enable storage [10], sharing and analysis of the resulting data set. Our initial framework uses two experimental Internet instruments as the basis for implementation and validation of the approach. These prototype instruments being developed at Victoria University scan for malicious Internet content/servers [1,2] using a client honeypot architecture that can be Grid deployed and capture and analyse Internet Background Radiation (IBR) using network telescopes and a Grid based analysis engine for traffic analysis computation [3]. The network telescope is shown in Figure 1 and the client honeypot in Figure 4.

The GEII concept has potential applications beyond a wider scale IBR measurement or a scan of web quality and web server maliciousness. The use of Grids for large scale instrument creation through sensor Grids has emerged and the Next Generation Network (NGN) for converged voice, entertainment and data services could be considered a large scale instrument. We outline the initial GEII instruments in section 2. Then in section 3 we discuss the GEII framework and then in section 4 a brief conclusion.

## II. EXAMPLE GEII INSTRUMENTS

IBR [3] and client honeypot [1,2] Internet instruments are being developed at Victoria University and the NGN VOIP quality monitoring concept has been simulated [16]. These are examples of Internet Grid instruments that could be used to capture network information for improving the Internet experience for users and Service Providers (SP) through detection, data analysis to diagnose and prevent malicious activity such as denial-of-service or intrusions. Candidate data analysis techniques include metadata generation, pattern matching, trend/time series analysis, network mapping, attack analysis such as the spread of the new contagion worm attacks.

### A. Network Telescopes for IBR Detection

To determine the applicability of Network Telescopes to Internet quality measurement we deployed a standard Network Telescope sensor, consisting of an advertising router connected to the Internet. In this experiment a dark /16 network was advertised for a period of 15 months, a VLAN (802.1q) constrained traffic routed to this /16 to the capture server, where all traffic was captured and stored. The key interfaces for the network telescope are shown in figure 1.

The role of the Advertising Router is twofold. Firstly to advertise the IP address space monitored by the telescope to the Internet through BGP. Secondly to forward any IBR packets which are destined for the advertised address range to the Capture Server. Static routing across a private address space is then used to direct traffic to the capture server. Capture Server integrity is maintained by using tcpdump to capture all packets to disk (in standard PCAP format) and then using netfilter rules to drop all traffic from the telescope using the VLAN identifier to remove 100% of the IBR traffic before it could be processed. The tcpdump process is monitored by the “init” process to ensure that a tcpdump process is kept alive. All data was captured and stored in 100MB files which were compressed along with identifying metadata. Data processing is accomplished using a tool

---

The client honeypot, IBR and GEII projects are supported by the Victoria University Research Fund and Science Faculty Research Grants. We wish to thank Juniper for their donation of a J6300 router for the IBR tool and support from the HoneyNet Alliance.

called pcapstat written in C using the libtrace library [14]. Pacpstat was deployed on a GT2 Grid and the resulting output analysed with the statistical analysis package R. This allows processing of the current 15 month, 210GByte dataset in a few hours, on our GT2 grid where currently any one job can use up to 90 computers in parallel. The computations would take around a week on a single computer [3]. This allows near real time analysis of the data collected. In the GEII framework the output from multiple network telescopes is expected to be collated and analysed in zones. Our current work is looking into controlling such instrument in a Grid infrastructure. In figure 1, we have identified at a high level the interfaces that are required to integrate and control this sensor as part of a virtual organization. These are:

- Router Control – configuration such as router advertising, filtering and management.
- Router Management – notification/management events and statistics (e.g. NetFlow data).
- Network Control – control of VLANs required.
- Capture Control – data capture, data filtering and capture process management.
- Storage Control – manages the storage of IBR data over the Grid interface, e.g. interworking with a SRB (Storage Request Broker) [10].
- Telescope Control – access control, top level data management and policy management.

The development of these web service based interfaces to the Network Telescope is part of an ongoing project.

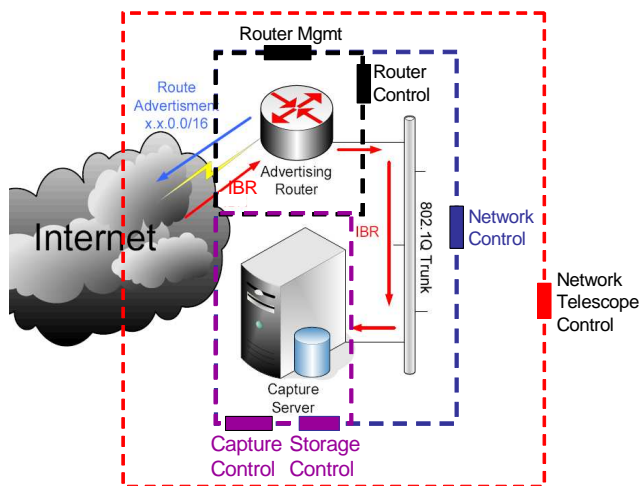


Figure 1 Network telescope for IBR detection [3]

The network telescope for IBR capture is relatively straight forward for a /16 network with today's level of background radiation. However, from a data storage and analysis perspective the Grid provides mechanisms essential for large scale instruments and provides useful mechanisms for sharing data between institutions and instruments. For a larger network telescope we have significant packet processing issues, with 20-30K packets per second received

in a /8 network [19]. Pemberton [3] shows that we should deploy many smaller network telescopes and aggregate their results to obtain a good estimate of the IBR hitting a /16 network. He shows that with as few as 30 random addresses in a /16 address space we can obtain a realistic measure of the IBR for the /16 as a whole, although the detection speed of attacks is reduced [5].

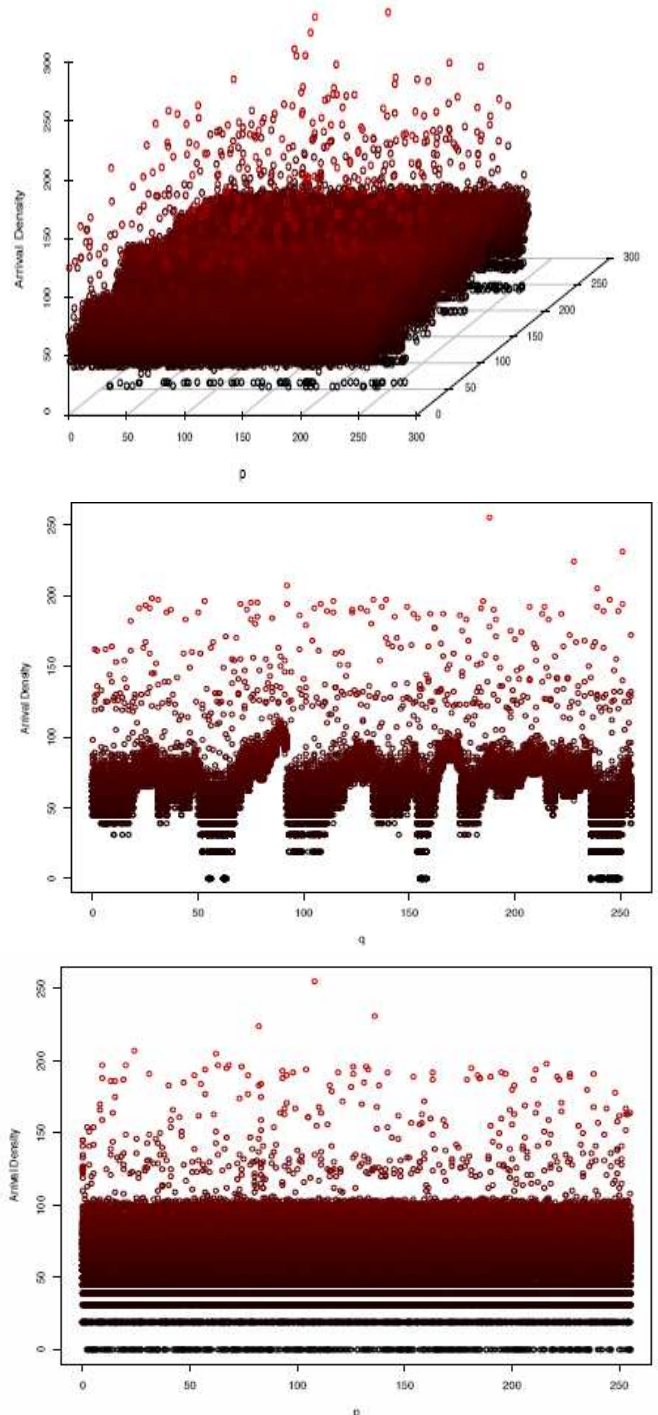
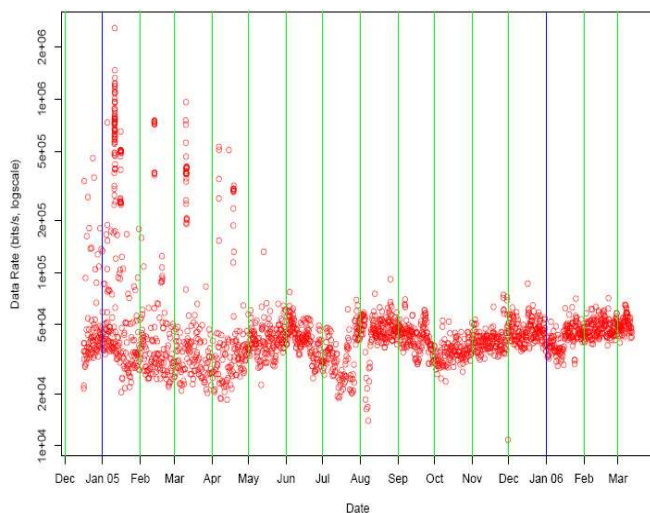


Figure 2 Scatter graphs of IBR arrival density across the /16 address space, aaa.bbb.q.p and a slice along the p and q axes, for 100MB of IBR traffic [3]

Figures 2 and 3 show a 100Mbyte sample of Network Telescope traffic activity and a 15-month sample of traffic activity respectively. The key data used in this analysis are the arrival characteristics of the IBR traffic although every packet is captured and processed. The arrival characteristics are the arrival rate, arrival, types of packet (ICMP, TCP or UDP), and destination ports. These allow calculation of the wasted bandwidth caused by IBR, the IBR arrival rate and basic diagnosis of the cause of the IBR. The IBR arrival rate is seen as a key research metric in many current projects [9, 19].

Figure 2 shows the /16 address space shown as 256x256 addresses p and q within the /16; a total of 65536 addresses. Given this /16 we are able to look at selected addresses within it to determine whether they will be good predictors of the overall IBR incident upon the /16 network as a whole. That is, are we able to generate statistics from a subset of these addresses to accurately predict the IBR traffic which was destined to the Network Telescope as a whole [3].

We see in Figure 2 that there is great arrival density variability in the q axis than the p axis. This representation makes it difficult to see the characteristics over the full address range. The data indicates that at this sampling unit the IBR is not uniformly distributed across the /16. In Figure 3 we see the traffic hitting the network telescope over a 15 month period up to March 2006. Each circle indicates a 100MByte sample. Measurements show a /16, a typical university network in New Zealand, receives approximately 14GB of IBR traffic per month [3], which reduces the network capacity available for legitimate Internet users, furthermore the IBR is usually of a malicious nature consisting of elements such as port scans, worm attacks etc. For New Zealand international connectivity is relatively expensive so the cost of IBR is high compared to other countries, thus enabling strategies to reduce IBR benefits all by allowing optimal use of the Internet infrastructure.



**Figure 3** Network Telescope traffic arrival rate for a /16. Each dot represents 100Mbytes collected over a 15 month period to March 2006 [3]

The IBR telescope produces large data sets from passive data capture [3] which may benefit from the use of storage brokers [10] and computational Grid resources for analysis – such as our GT2 prototype. Our intention is to create a collaborative grid of network telescopes around New Zealand as a proof of concept, creating an instrument zone using storage and computation resources to analyse wide area IBR. A /16 Network Telescope attracts around 0.5GB of IBR per day, thus if the 7 universities in New Zealand shared IBR data we would typically store and analyse around 3.5GB of data per day. Using the current pcapstat analysis tool that would require approximately 120 hours of computation to generate aggregated data. Looking at the data in figure 3 we can see that this arriving data rate can be greatly exceeded and periodically will require significantly more processing.

One of the other issues with this approach is that different universities have different ethic committee requirements on the captured data. At Victoria University a separate /16 network is used and all traffic can be captured, analysed and shared. Whereas for example at the University of Waikato, IBR measurement is made as part of the university –wide network monitoring system. Their network has some externally exposed addresses with the remaining hosts behind proxies. Thus traffic entering the network for the hidden hosts is IBR and is captured. However the Waikato ethics committee requires the data to be anonymised and only the first 40 bytes of each packet to be captured, stored and shared. This limits the data that can be extracted from this network telescope and indicates requirements on the filtering of traffic to be carried out before storage in the Grid.

### B. Client Honeypots for Web Content Classification

Millions of computers are infected by malicious web servers per year. This can result in crippled computers that need rebuilding. Worse still, hackers may use these compromised computers to send spam, relay or launch attacks on other users of the Internet. Our client honeypot system can detect exploits hosted on malicious web sites and create rules for content filters and IDS. Furthermore, lists of malicious URLs generated by client honeypot systems could be used by existing mechanisms such as black holes in DNS and filters in proxies to block or filter content. This would typically protect the most vulnerable users on the Internet.

We have developed open source client honeypot implementations [13, 23] that have been positively received by the HoneyNet Alliance [12]. The client honeypot architecture is shown in Figure 4 consisting of a two-level client architecture consisting of a low interaction honeypot and a high interaction client honeypot.

The low interaction honeypot uses heuristics to identify websites hosting malicious exploits. This has a high false positive rate so we pass the URLs of potentially malicious websites to our high interaction client honeypot that has a low false positive rate but is much slower than our low interaction client honeypot. To address potential false negatives, a random proportion of non-malicious URLs are also passed to the high interaction client honeypot systems.

Should these URLs be shown to be malicious, the heuristics of the low interaction client honeypot are updated.

The high interaction client honeypot utilises a dedicated host operating system that currently runs a VMware instance of the Microsoft XP operating system. Within the VMware instance, Internet Explorer 6, downloads web content for analysis. The XP environment uses Capture BAT - a behavioral analysis tool developed at Victoria University of Wellington to detect anomalous system events that compromise the environment which are reported to the host system. This high interaction client honeypot instrument allows us to detect unknown exploits. Note that some malware detects the presence of emulated or virtual environments and avoids instantiation, so work is progressing to move from the VMware based solution to maximise detection. The system uses special purpose web and DNS proxies between the client honeypots and the servers on the Internet and the Honeypot controller which provides an optimisation of Internet connectivity and allows repeated experiments on suspected data as malicious web servers to not always replicate attacks regularly.

We have developed our own open source client honeypot instrument because existing instruments such as HoneyMonkey from Microsoft [20] are either closed source or limited in functionality [2]. We envisage using our client honeypot in a larger system consisting of hundreds cooperating low and high interaction client honeypots scanning web content over a Gigabit Internet connection.. Our investigation into the “.nz” domain [21] and queuing theory models indicate a scan of the “.nz” domain could be achieved within a week using the 2000 or so available Grid machines at Victoria University [22]. In a recent test, we identified over 300 malicious web sites out of a sample of 300,000 web pages that had a higher likelihood of maliciousness than a purely random sample.

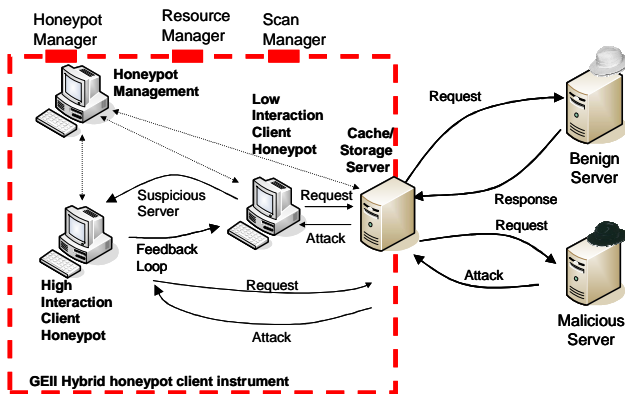


Figure 4 Hybrid client honeypot architecture [23]

The IBR telescope produces reasonably large data sets from passive data capture [3] that may require the use of storage brokers [10] and computational Grid resources for analysis. However, the client honeypot downloads a much larger quantity of web content, thus requiring a much larger computational infrastructure to analyse the uploaded

malicious server data. Localising client honeypot clusters around the world minimises latency and optimises client honeypot performance whereas locating standardised telescopes worldwide allows global IBR mapping. Grid efficiency is enabled by migrating analysis code to IBR data sets whereas the client honeypot system gains efficiency through deployment of individual client honeypot virtual machine images to compute clusters. Currently, as proof of concept we have deployed our client honeypots using the Amazon EC2 service [11] and low interaction client honeypots (HoneyC) on our GT2 grid. HoneyC is being extended with full JavaScript engine, more obfuscation functionality and enhanced ability to follow redirects.

### C. VoIP and NGN Quality Monitor

The GEII concept has potential applications beyond a wider scale IBR measurement or a scan of web quality and web server maliciousness. The use of Grids for large scale instrument creation through sensor Grids has emerged and the Next Generation Network (NGN) for converged voice, entertainment and data services could be considered a huge scale instrument with millions of potential sensors. In the case of voice services, each end point running the RTP (Real Time Protocol) could deliver RTCP XR (Real Time Control Protocol eXtended Record) information every 10 seconds during a voice call [18]. The R factor [17] is directly related to the end-to-end delay, jitter, voice codec etc. and changes during the duration of a call as the network characteristics change, e.g. congestion pinch points, reconfiguration due to network failures etc. [16]. The XR format provides the information from each end point that can be used to determine the quality of the network and importantly contains a voice quality measure as shown in figure 5 [17].

Loss Rate	Discard Rate	Burst Density	Gap Density
Burst Duration (mS)		Gap Duration (mS)	
Round Trip Delay (mS)		End System Delay (mS)	
Signal level	RERL	Noise Level	Gmin
R Factor	Ext R	MOS-LQ	MOS-CQ
Rx Config	-	Jitter Buffer Nominal	
Jitter Buffer Max		Jitter Buffer Abs Max	

Figure 5 RTCP eXtended Record (XR) data

The set of information provided for a call thus determining the perceived quality of the network from longterm measurement end points [16] and short term voice calls. For a given network there may be thousands to millions of calls occurring each hour between network regions, which is a large data processing load that could be processed and stored on a Grid and the call quality record data could be placed in a data warehouse for network analysis. The data needs to be sorted, aggregated and processed, to develop the call quality for the network per codec type  $c$ ,  $R_{Tc}$ , and the call quality per source and destination region (voice calls XR

data is sorted by source  $s$  and destination  $d$  regions and by codec type)  $R_{Tc,s,d}$ .

$$R_{Tc} = \sum_{i=1}^n R_i / i \quad (1), \text{ and}$$

$$R_{Tcsd} = \sum_{i=1}^k R_{icsd} / i \quad (2)$$

For a country like New Zealand with 4.1 million people we would expect over 10GB of XR records to be created with thousands of XR events per second. During peak hours tens of thousands of XR events per second are likely to be received. Again using a Grid for storage and analysis of this data and quality computation is feasible.

The top level view of the GEII solution for NGN quality measurement is shown in figure 6. Long Term Sensors are deployed in a sensor grid similarly to the simulated VoIP sources and destinations of the simulation studies undertaken [16], using long term measurements flows, across the NGN able to detect outages effectively. These sensors create a Grid across the network, typically deployed on a regional basis. Transient sensors are those in consumer service nodes that are enabled and opted in to provide measurement data to the regional DCAS (Data Collector Aggregator and Sorters). The consumer nodes make a call and produce XR's for the duration of the call; these are sorted into source and destination regions and augment the Long Term Sensor data. These provide sorted data to the Analysis Engine and long term storage, e.g. using an SRB [10].

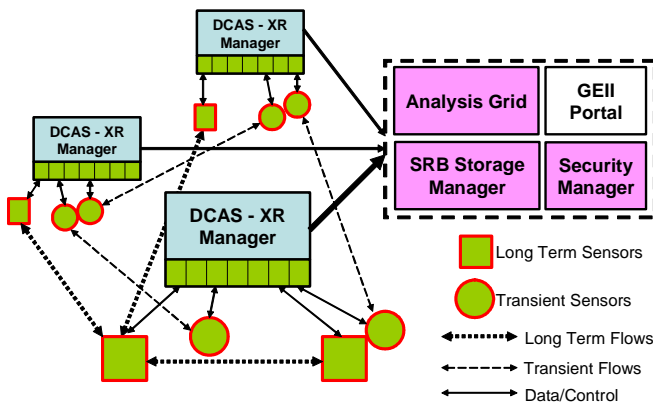


Figure 6 GEII NGN architecture

### III. THE GEII FRAMEWORK

The GEII framework is based on Grid technology [4] with our current network telescope analysis engine based on GT2. The initial controller model for these instruments aims to use the existing Grid instrument R&D to create a framework that is appropriate to the GEII concept. There are several key Grid instrumentation projects that have been developed in the last year or two. The Common Instrument Middleware Architecture (CIMA) [6,7,8] provides one

framework which has developed implementations from low power wireless sensors through to collaboration and control of large physical sciences instruments. Another approach is taken with the GRIDCC project [24, 25] that has developed a number of instruments based on the EGEE Grid implementation. This project has implementations that encompass instrumentation on the Electrical power grid, geohazard monitoring, meteorology, medical instruments and telecommunications – specifically in Intrusion Detection Systems (IDS) [25].

CIMA allows scientists to access, store and transport data and remotely control scientific instruments and sensor in Grids. The emerging CIMA framework provides the basis to encapsulate several of the Internet instruments envisaged for GEII and develop wide scale Internet measurement systems. CIMA projects have included the use of Kepler workflows (<http://kepler-project.org/>) for scientific applications and includes GridSphere portal and Storage Request Broker. However the architecture may require extensions in security/privacy, metadata for Internet measurements, enhanced business process execution and data normalisation services for these Internet measurement instruments.

GRIDCC provides a similar solution, based on EGEE/gLite middleware (<http://www.glite.org>), comprising a Virtual Control Room (VCR), Virtual Instrument Grid Service (VIGS). Again the focus is on scientific workflows executed through Execution Services (ES) using the Workflow Management Systems (WfMS) based on BPEL with QOS constraints to manage Compute Elements (CE) and Storage Elements (SE) as well as Instruments Elements (IE).

Our framework is investigating the use of these two approaches and their workflow systems as a basis for GEII. The emerging Grid component model (GRIDCOMP[15]) may also be of interest within the framework to develop Internet measurement application components; employing asynchrony, group and migration services, as well as service composing. To date the prototype instruments discussed and the initial IBR analysis software have been developed but not integrated into the GEII framework. Current work is looking at defining workflows for our instruments and analysis software.

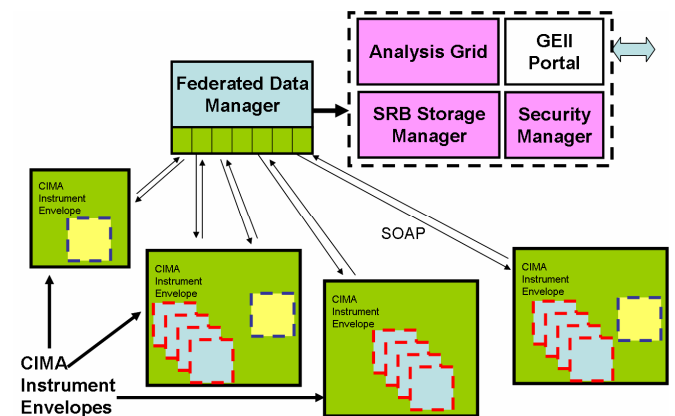


Figure 7 Top level of GEII framework

To date there has been little input from the Service Provider perspective into the GEII project. Including the SP requirements could lead to a more inclusive GEII architecture implementation, with SP instrument configurations, analysis tools and Grid components. The SP can develop closed measurement systems or federated instrumentation with different scope for data exchange. There may be several different aspects to a GEII Virtual Organisation related to the SP relationships and depending on what a SP wishes to gain from such a system.

#### IV. CONCLUSIONS

We have described two Internet instruments that we have been developed, and outlined the GEII concept and framework. We intend to use the Internet instruments to evaluate the usefulness of the GEII concept and framework. The client honeypot is indicative of an instrument that requires provision of large compute resources, working on a large data set, whereas the network telescope requires storage and federated data access and could be used for near real time network attack identification. The VOIP quality measure indicates near real time network quality and may be useful as a tool in optimizing NGN configuration through using this data to optimize link weight settings through the application of linear programming techniques. This would add a real time element to the data analysis [26].

These and other instruments deployed in a Grid, utilizing the compute power available can provide Internet measurements and analysis to improve the quality of the Internet. The IBR sensors may also be used within the Grid infrastructure as part of the security services and Grid measurement systems. Similarly the VOIP quality measures could be utilised as part of the real time interactive services for collaboration services delivered in a Grid.

#### REFERENCES

- [1] C. Seifert, I. Welch, P. Komisarczuk, HoneyC - The Low-Interaction Client Honeypot, 2006. URL <http://www.mcs.vuw.ac.nz/~cseifert/blog/images/seifert-honeyc.pdf>; last accessed 2/2/2007.
- [2] C. Seifert, I. Welch, P. Komisarczuk, Taxonomy of Honeypots, July 2006. URL <http://www.mcs.vuw.ac.nz/comp/Publications/index-byyear-06.html>, last accessed 2/2/2007.
- [3] D. S. Pemberton, An Empirical Study of Internet Background Radiation Arrival Density and Network Telescope Sampling Strategies, MSc Thesis, Victoria University, January 2007.
- [4] The Globus Toolkit, <http://www.globus.org/>, last accessed 2/2/2007.
- [5] D. Moore, C. Shannon, G. M. Voelker, and S. Savage. Network telescopes. Technical report, CAIDA, 2003. URL <http://www.caida.org/outreach/papers/2004/tr-2004-04/tr-2004-04.pdf> last accessed 25 Dec 2006.
- [6] D. F. McMullen, T. Devadithya, Integrating Instruments and Sensors into the Grid with CIMA Web Services, Proceedings of the Third APAC Conference on Advanced Computing, Grid Applications and e-Research (APAC05), Gold Coast, Australia, 2005.
- [7] A Bagnasco, A Poggi, A. M. Scapolla, A Grid-Based Architecture for the Composition and the Execution of Remote Interactive Measurements, Second IEEE International Conference on e-Science and Grid Computing (e-Science'06), Amsterdam, December 2006
- [8] G. Aloisio, D Conte, C. Elefante, I Epicoco, G. P. Marra, G. Mastrantonio, G. Quarta, SensorML for Grid Sensor Networks, Proceedings of The 2006 International Conference on Grid Computing & Application, Las Vegas, June 2006
- [9] R. Pang, V. Yegneswaran, P. Barford, V. Paxson, and L. Peterson. Characteristics of Internet Background Radiation. In Proceedings of the 4th ACM SIGCOMM conference on Internet measurement, pages 27–40. ACM Press, October 2004. ISBN 1-58113-821-0.
- [10] IBM, Build a data Grid with the Storage Resource Broker, June 2006, <http://www-128.ibm.com/developerworks/Grid/library/gr-srb/index.html>, last accessed 3/2/2007.
- [11] S. Garfinkel, Commodity Grid Computing with Amazon's S3 and EC2, UESNIX February 2007, pp7-13.
- [12] The HoneyNet Alliance, <http://www.honeynet.org/alliance/>, last visited 3/2/2007 and the New Zealand HoneyNet organisation <http://www.nz-honeynet.org/> last accessed 3/2/2007.
- [13] HoneyC, <http://honeyc.sourceforge.net/>, last visited 3/2/2007. Capture, A Honeypot Client, <http://capture-hpc.sourceforge.net/>, last accessed 3/2/2007.
- [14] WAND Network Research Group. libtrace packet library. <http://research.wand.net.nz/software/libtrace.php> [Accessed 25 Dec 2006]
- [15] GridCOMP, Grid Programming with Components, An Advanced Component Platform for an Effective Invisible, IST programme of the European Commission (DG Information Society and Media, project n°034442), <http://Gridcomp.ercim.org/>, last accessed 3/2/2007.
- [16] A. Koudrin, Network Reliability and Resiliency in Next Generation Networks, MSc Thesis, Victoria University, June 2006.
- [17] ITU-T, G.114, One-way transmission time SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS International telephone connections and circuits – General Recommendations on the transmission quality for an entire international telephone connection, May 2003.
- [18] T. Friedman, R. Caceres, A. Clark, RFC 3588, RTP Control Protocol Extended Reports (RTCP XR), IETF, November 2003.
- [19] V. Yegneswaran, P. Barford, and D. Plonka. On the design and use of internet sinks for network abuse monitoring. In Proceedings of Symposium on Recent Advances in Intrusion Detection, 2004. Available from <http://www.cs.wisc.edu/~vinod/raid-paper.pdf>, accessed 22 February 2007.
- [20] Y.-M. Wang, D. Beck, X. Jiang, R Rousev, C. Verbowski, S. Chen, and S. King. Automated Web Patrol with Strider HoneyMonkeys: Finding Web Sites That Exploit Browser Vulnerabilities . In 13th Annual Network and Distributed System Security Symposium (San Diego, 2006), Internet Society.
- [21] N. Bertram, The New Zealand Internet Landscape: An analysis of peering, content and scalability, Victoria University, October 2006, available from <http://www.mcs.vuw.ac.nz/~peterk/index.shtml>, accessed on 22 February 2007.
- [22] C. Seifert, Improving Detection Accuracy and Speed with Hybrid Client Honeypots, PhD Proposal, Victoria University of Wellington, Wellington, New Zealand, Available from [http://www.mcs.vuw.ac.nz/~cseifert/publications/publications/Cseifert\\_phd\\_proposal-Hybrid\\_Client\\_Honeypots.pdf](http://www.mcs.vuw.ac.nz/~cseifert/publications/publications/Cseifert_phd_proposal-Hybrid_Client_Honeypots.pdf), accessed on 22 February 2007.
- [23] C. Seifert, C., I. Welch, and P. Komisarczuk. HoneyC - The Low-Interaction Client Honeypot, Proceedings of the 2007 NZCSRCS, Waikato University, Hamilton, New Zealand, April 2007.
- [24] Grid Enabled Remote Instrumentation with Distributed Control and Computation, <http://www.gridcc.org/>, last accessed 3/2/2007.
- [25] E. Frizziero1, M. Gulmini1, F. Lelli, G. Maron, A. Oh, S. Orlando, A. Petrucci, S. Squizzato, S. Traldi1, Instrument Element: a new Grid component that enables the control of remote instrumentation, Workshop on Scientific Instruments and Sensors on the Grid, Trieste - Italy, 23 - 28 April 2007.
- [26] R. Suryasaputra, Congestion Removal in the Next Generation Internet, Thesis, Doctor of of Philosophy, 2007, RMIT.