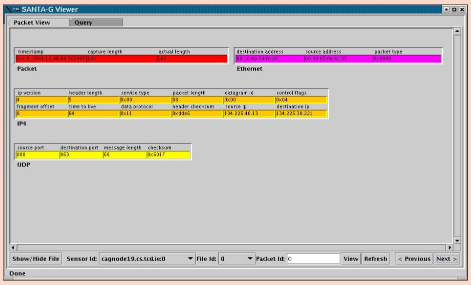
SANTA-G: Grid-enabled System Area Networks Trace Analysis

crossgrid

www.eu-crossgrid.org



SANTA-G Viewer

Packet View | Query

timestamp	capture length	actual length
Oct 8, 2001 12:04:48.363987	102	102

Packet

destination address	source address	packet type
00:10:4b:3d:fd:b5	00:30:05:0e:4c:35	0x0800

Ethernet

ip version	header length	service type	packet length	datagram id	control flags
4	5	0x00	88	0x00	0x04
fragment offset	**time to live**	**data protocol**	**header checksum**	**source ip**	**destination ip**
0	64	0x11	0xdde6	134.226.40.13	134.226.38.221

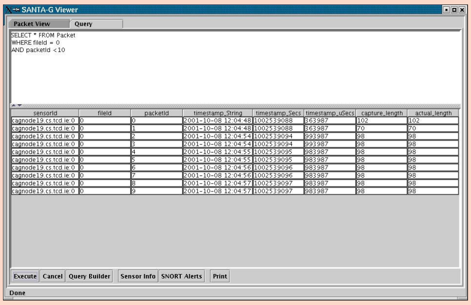
IP4

source port	destination port	message length	checksum
888	863	68	0x6017

UDP

Sensor Id: cagnode19.cs.tcd.ie:0
File Id: 0
Packet Id: 0

Detailed Graphical Packet Display



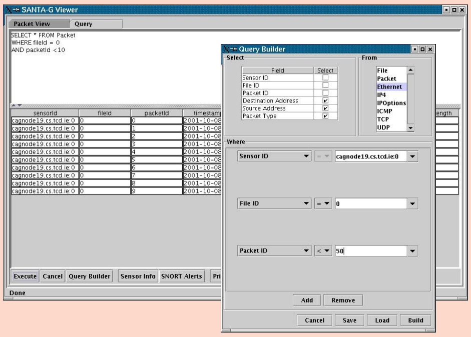
SANTA-G Viewer

Packet View | Query

```
SELECT * FROM Packet
WHERE fileId = 0
AND packetId <10
```

sensorId	fileId	packetId	timestamp_String	timestamp_Secs	timestamp_uSecs	capture_length	actual_length
cagnode19.cs.tcd.ie:0	0	0	2001-10-08 12:04:48	1002539088	363987	102	102
cagnode19.cs.tcd.ie:0	0	1	2001-10-08 12:04:48	1002539088	363987	70	70
cagnode19.cs.tcd.ie:0	0	2	2001-10-08 12:04:54	1002539094	993987	98	98
cagnode19.cs.tcd.ie:0	0	3	2001-10-08 12:04:54	1002539094	993987	98	98
cagnode19.cs.tcd.ie:0	0	4	2001-10-08 12:04:55	1002539095	983987	98	98
cagnode19.cs.tcd.ie:0	0	5	2001-10-08 12:04:55	1002539095	983987	98	98
cagnode19.cs.tcd.ie:0	0	6	2001-10-08 12:04:56	1002539096	983987	98	98
cagnode19.cs.tcd.ie:0	0	7	2001-10-08 12:04:56	1002539096	983987	98	98
cagnode19.cs.tcd.ie:0	0	8	2001-10-08 12:04:57	1002539097	983987	98	98
cagnode19.cs.tcd.ie:0	0	9	2001-10-08 12:04:57	1002539097	983987	98	98

SQL Query Submission and ResultSet View



SANTA-G Viewer

Packet View | Query

```
SELECT * FROM Packet
WHERE fileId = 0
AND packetId <10
```

sensorId	fileId	packetId	timestam
cagnode19.cs.tcd.ie:0	0	0	2001-10-08
cagnode19.cs.tcd.ie:0	0	1	2001-10-08
cagnode19.cs.tcd.ie:0	0	2	2001-10-08
cagnode19.cs.tcd.ie:0	0	3	2001-10-08
cagnode19.cs.tcd.ie:0	0	4	2001-10-08
cagnode19.cs.tcd.ie:0	0	5	2001-10-08
cagnode19.cs.tcd.ie:0	0	6	2001-10-08
cagnode19.cs.tcd.ie:0	0	7	2001-10-08
cagnode19.cs.tcd.ie:0	0	8	2001-10-08
cagnode19.cs.tcd.ie:0	0	9	2001-10-08

Query Builder

Select

Field	Select
Sensor ID	□
File ID	□
Packet ID	□
Destination Address	☑
Source Address	☑
Packet Type	☑

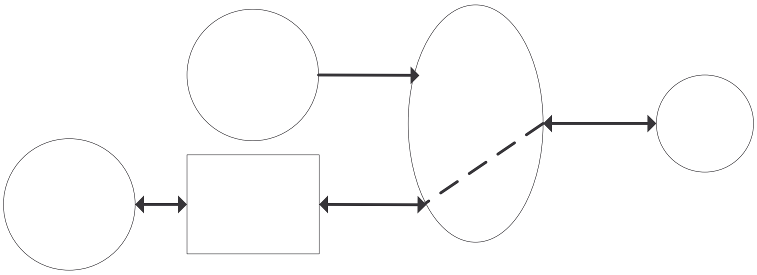
From: File, Packet, Ethernet, IP4, IPOptions, ICMP, TCP, UDP

Where

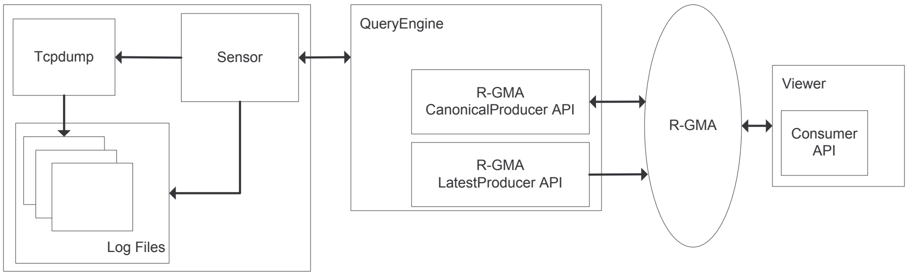
Sensor ID = cagnode19.cs.tcd.ie:0
File ID = 0
Packet ID < 50

SQL SELECT statement builder to easily construct SQL queries

Typically with Grid Information Systems an information provider inserts data to the system at regular intervals. The user can then retrieve this data using the information system client (e.g. API, GUI). A difficulty arises when dealing with information sources that generate a large amount of data at a very fast rate in a form unsuitable for direct insertion to the information system, for example instrument monitors (e.g. logic analysers). SANTA-G is a framework that supports monitoring with this type of information source in the Grid environment by allowing access to data *through* the Grid Information System. The monitoring data, rather than being inserted into the information system, is left in its raw form at the location where it was created.



The demonstrator of this, developed within the EU CrossGrid project, is the SANTA-G NetTracer, a network monitor that allows users to access log files stored in *libcap* (a network packet capture library) format through the EU DataGrid's (EDG) Relational Grid Monitoring Architecture (R-GMA) monitoring and information system. Examples of tools that generate logs in this format are Tcpdump, and SNORT (a network intrusion detection system). It is aimed at system administrators for network traffic analysis across multiple sites within a Grid, and also for performance analysis. It is also intended to use the SNORT functionality of the NetTracer to construct a Grid-wide intrusion detection system. The NetTracer is written entirely in Java, and has been tested on Redhat Linux 7.3. It is covered under the EDG License.

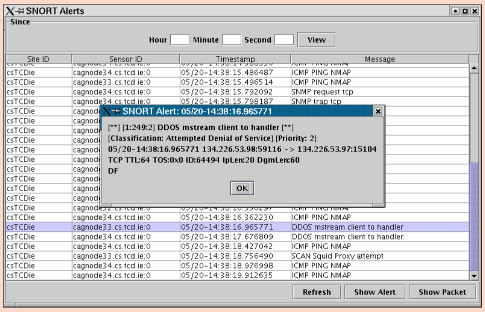


The SANTA-G NetTracer is composed of three components: a Sensor (which is installed on the node(s) to be monitored), a QueryEngine, and a Viewer GUI. The Sensor invokes Tcpdump (an open-source packet capture application), and then monitors the log files created. The Sensor notifies the QueryEngine when new log files are detected. The QueryEngine records these events and publishes them to users through the R-GMA. The QueryEngine also forms the interface to the R-GMA by using the R-GMA's CanonicalProducer API.

The Viewer GUI presents a graphical interface to users (see left), through which they may present queries and view results. Through the Canonical Producer their query is forwarded to the Query Engine, which then parses the query, searches the appropriate log file to obtain the data required to satisfy the query, and returns the dataset to the Viewer GUI through the R-GMA.

Information Society Technologies

IST-2001-32243



Site ID	Sensor ID	Timestamp	Message
csTCDie	cagnode34.cs.tcd.ie:0	05/20-14:38:15.486487	ICMP PING NMAP
csTCDie	cagnode33.cs.tcd.ie:0	05/20-14:38:15.496514	ICMP PING NMAP
csTCDie	cagnode34.cs.tcd.ie:0	05/20-14:38:15.792092	SNMP request tcp
csTCDie	cagnode34.cs.tcd.ie:0	05/20-14:38:15.798187	SNMP trap tcp
csTCDie	cagnod		
csTCDie	cagnod		
csTCDie	cagnod		
csTCDie	cagnod		
csTCDie	cagnod		
csTCDie	cagnod		
csTCDie	cagnod		
csTCDie	cagnod		
csTCDie	cagnod		
csTCDie	cagnod		
csTCDie	cagnode32.cs.tcd.ie:0	[illegible]	ICMP PING NMAP
csTCDie	cagnode34.cs.tcd.ie:0	05/20-14:38:16.362230	ICMP PING NMAP
csTCDie	cagnode33.cs.tcd.ie:0	05/20-14:38:16.965771	DDOS mstream client to handler
csTCDie	cagnode34.cs.tcd.ie:0	05/20-14:38:17.676809	DDOS mstream client to handler
csTCDie	cagnode34.cs.tcd.ie:0	05/20-14:38:18.427042	ICMP PING NMAP
csTCDie	cagnode33.cs.tcd.ie:0	05/20-14:38:18.756490	SCAN Squid Proxy attempt
csTCDie	cagnode34.cs.tcd.ie:0	05/20-14:38:18.976998	ICMP PING NMAP
csTCDie	cagnode34.cs.tcd.ie:0	05/20-14:38:19.912635	ICMP PING NMAP

SNORT Alert: 05/20-14:38:16.965771

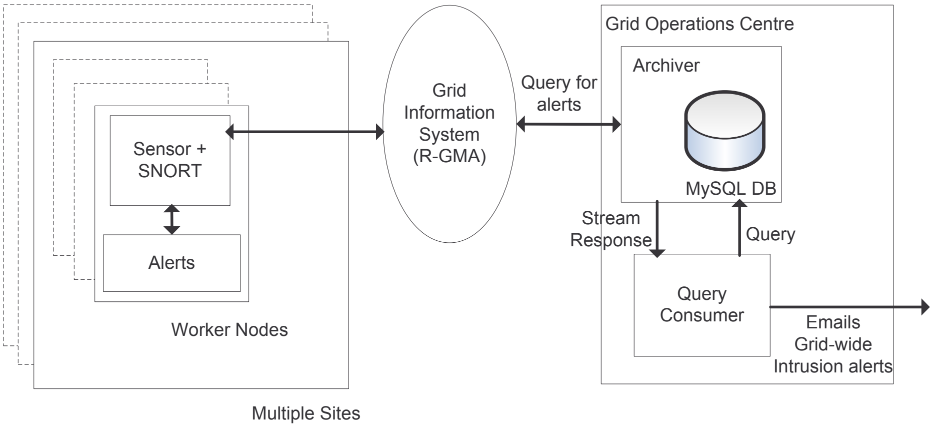
```
[**] [1:249:2] DDOS mstream client to handler [**]
[Classification: Attempted Denial of Service] [Priority: 2]
05/20-14:38:16.965771 134.226.53.98:59116 -> 134.226.53.97:15104
TCP TTL:64 TOS:0x0 ID:64494 IpLen:20 DgmLen:60
DF
```

SNORT Alerts Display

Grid-wide Intrusion Detection

The SNORT functionality of the SANTA-G NetTracer will be used as the basis of a Grid-wide intrusion detection system. SNORT logs alerts to a file when suspect packets are detected on the network. The Sensor component monitors this alerts file and when a new alert is detected its details are sent to the QueryEngine, which then *streams* them to the R-GMA. Users can then view these alerts using the Viewer GUI.

It is envisaged that each site within a Grid will run a set of SNORT sensors publishing alerts to the R-GMA. By using other R-GMA components, such as an Archiver, alerts published from multiple sites can be aggregated to form a Grid-wide intrusion log. A high level incident detection, tracking and response platform can then be created by using custom coded Consumers to filter and analyse this log in order to detect patterns that would signify an attempted distributed attack on the Grid infrastructure. If such a pattern is found the Consumer would trigger a pattern-specific alert, and thereby generate Grid-wide intrusion alerts.



Documentation:

Documentation for the NetTracer, including Installation, User, and Developer guides can be downloaded from the following address:

http://gridportal.fzk.de/autobuild/i386-rh7.3-gcc3.2.2/AutoDoc.html

CrossGrid deliverables, including a Software Requirements Specification and Software Design Document can be obtained from the CrossGrid website:

http://www.eu-crossgrid.org/deliverables_all.htm

References:

The CanonicalProducer, an instrument monitoring component of the EDG R-GMA. *Proceedings of the ISPDC*, Cork, Ireland, July 2004. Stuart Kenny, Brian Coghlan, and EDG WP3.

Grid-wide Intrusion Detection System. *Cracow Grid Workshop*, Cracow, Poland, December 2004. Stuart Kenny, Brian Coghlan.

Contact:

CYFRONET
Prof.Michal Turala
M.Turala@cern.ch

Algosystems S.A.
Yannis Perros
yperros@algosystems.gr

Trinity College Dublin
Dr.Brian Coghlan
<coghlan@cs.tcd.ie>
Stuart Kenny
<Stuart.Kenny@cs.tcd.ie>

IST-2001-32243