U.S. DEPARTMENT OF ENERGY

PNNL-18252

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

GridStat – Cyber Security and Regional Deployment Project Report

SL Clements

December 2008

Pacific Northwest
NATIONAL LABORATORY

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY

operated by

BATTELLE

for the

UNITED STATES DEPARTMENT OF ENERGY

under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401, fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847, fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

This document was printed on recycled paper.
(8/00)

PNNL-xxxxx

GridStat – Cyber Security and Regional Deployment Project Report

SL Clements

January 2009

Prepared for
U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

Executive Summary

GridStat is a developing communication technology to provide real-time data delivery services to the electric power grid. It is being developed in a collaborative effort between the Electrical Power Engineering and Distributed Computing Science Departments at Washington State University. Improving the cyber security of GridStat was the principle focus of this project. A regional network was established to test GridStat's cyber security mechanisms in a realistic environment. The network consists of nodes at Pacific Northwest National Laboratory, Idaho National Laboratory, and Washington State University. Idaho National Laboratory (INL) was tasked with performing the security assessment, the results of which detailed a number or easily resolvable and previously unknown issues, as well as a number of difficult and previously known issues.

Going forward we recommend additional development prior to commercialization of GridStat. The development plan is structured into three domains: Core Development, Cyber Security and Pilot Projects. Each domain contains a number of phased subtasks that build upon each other to increase the robustness and maturity of GridStat.

Table of Contents

Figures

Tables

Overview of GridStat Technology

GridStat is an information sharing framework that overcomes the inadequacies and limitations of current control system device communications. Washington State University (WSU) developed this framework for use in the electric power industry. GridStat belongs in a class of software called *middleware*, which functions between the operating system and the application software. GridStat facilitates the communications between control system devices and adds additional capabilities to improve the quality of service (QoS) of inter-device communications. GridStat handles network resource allocations, redundant communications pathways, secure links and protocol translations in a way that is transparent to the control system devices.

Compared to today's control system technology, GridStat's flexibility allows better performance, robustness, and security. GridStat lets data be delivered flexibly in a peer-to-peer fashion without requiring a centralized collection point, thus reducing latency and eliminating a single point of failure. GridStat has a *hierarchical management infrastructure* that maps onto the natural hierarchy in the grid. This enables utilities and other participants in the power grid to configure their own security policies to control access and resource usage to meet their own security requirements.

The GridStat project began in 2000 (Bakken et al. 2000). Its first funding came from the National Institute of Standards and Technology and since that time has had involvement from Schweitzer Engineering Laboratories, the University of Idaho, Avista Utilities, the National Science Foundation, the Department of Energy, and the Department of Homeland Security. Their involvement and funding has produced a number of doctoral dissertations (Dionysiou 2006, Gjermundrød 2006, Irava 2006) and masters theses (Ping 2004, Johnston 2005, Helkey 2007, Abelsen 2007, Viddal 2007, Solum 2007, Muthuswamy 2008).

The code developed by these students was not intended to be production quality, or designed for long-term maintainability or reliability. Rather, as is the case with graduate research everywhere, the code was developed to demonstrate the feasibility of particular mechanisms, and to provide an experimental evaluation of them. Such code was crucial for developing the underlying technology. However, as GridStat moves towards being used in wide-area pilot projects, its code needs to be matured, and configuration and testing tools need to be developed.

Project

The Cyber Security and Regional Deployment project had three objectives: first to create a regional deployment of GridStat, second to test the cyber security of GridStat on the regional network, and third to develop and integrate a visualization tool into the Electricity Infrastructure Operations Center (EIOC) at Pacific Northwest National Laboratory (PNNL).

Regional Deployment

The project team designed and implemented a regional deployment of GridStat to test its security features. The GridStat network consists of nodes at PNNL, Idaho National Laboratory (INL) and WSU. Each node is linked to each of the other nodes such that if one link fails, there is a redundant communication path [see Figure 1]. Optimally this network would be built on dedicated fiber-optic cables, but the versatility of GridStat allows it to run across various types of physical media. It is currently configured using virtual private network tunnels across the public Internet. This phase of the project was completed March 2008.

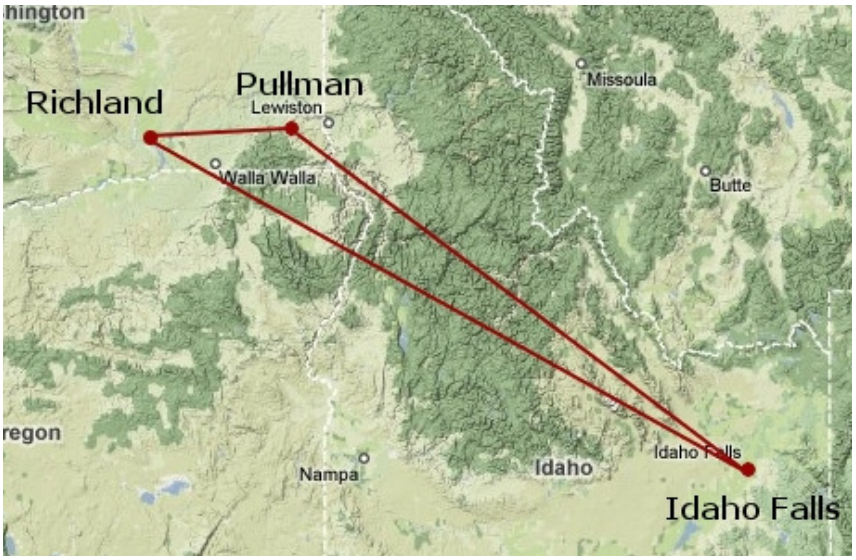

Figure 1: Regional GridStat Deployment

Cyber Security Assessment

As previously noted, GridStat has been developed in an academic environment, where the code produced was intended to demonstrate feasibility of mechanisms, not provide production quality code. Knowing that there were a number of security issues associated with GridStat, and understanding that building security into a product is easier and more effective than trying to add it on later, this project was designed to do an assessment to ensure all security mechanisms were considered at an early stage in the development lifecycle. This was done with the confidence that an early assessment would aid in developing a more secure and robust communication system.

Idaho National Laboratory was tasked to perform the cyber security assessment of GridStat. The assessment (Hall et al. 2008) provided the desired information. It detailed eight security issues or concerns. Some of these issues were known issues that have yet to be addressed, and others were common security errors that are relatively easy to fix now but would have been more difficult to address later in the development cycle. The issues, summarized below in order of increasing time/difficulty to mitigate, range from minor programming errors taking a couple of months to unfunded research areas that could take a year or more.

1. The assessment listed logging as an area of concern. The logging mechanisms of GridStat allow logging of events at varying levels of granularity. In the current iteration of GridStat, much of this capability is not enabled. The project team discussed this concern and determined that the existing logging mechanisms are adequate and that the amount and type of logging should be determined by the vendor of the system. Therefore, it is left to the vendor to implement logging as best suites them and their customers.
2. Three vulnerabilities identified contain previously unknown coding errors. Fortunately at this stage of development, they are relatively easy to fix. Finding and mitigating such problems was a primary purpose for this project. All three vulnerabilities have resources allocated to make the necessary coding changes.
    a. Encryption Errors: It was noted that encryption did not always function correctly and when it failed, it defaulted to an unencrypted state. Thus, any message encrypted or not could be sent to a receiver claiming to be encrypted. When the receiver attempted to decrypt the message, the decryption would fail and the original message would be forwarded on as if it had successfully been decrypted. This type of response, known as fail-open, sends a message even when an error occurs. To resolve this issue, GridStat will be reconfigured to fail-close, causing the function to drop the packet when an error occurs, thus forcing the encryption to function as it should.
    b. Replay Attacks: Each packet in the GridStat protocol contains a timestamp that makes each packet unique. The problem identified is that the timestamp is not encapsulated inside the encrypted section of the packet. This allows an attacker to capture encrypted packets, replace the timestamp with any timestamp desired, and then replay the packets, which will be accepted as valid. The code will be modified to move the timestamp inside the encrypted section of the packet to mitigate this vulnerability.
    c. Message Spoofing: The report states that the “Client Information Is Not Retained”. When a message is received there is not a binding tie between the sender and the message thus allowing a rogue sender to claim the message is from a legitimate sender and the receiver will accept it as such. The code will be updated to tie the sender’s information to each message.

3. Two vulnerabilities were listed that relate to the lack of security mechanisms in the management plane. This was a known issue and is currently the topic of ongoing research.

    a. Identity Spoofing: The lack of an authentication mechanism on messages allows an attacker to arbitrarily identify itself as any publisher or subscriber. Allowing the attacker to send or receive information that otherwise may not be allowed. The research currently underway is to determine the best methods for ensuring authenticity of messages and incorporating them into GridStat.

    b. Unsecured Management Plane: Throughout the report it is noted that there is a lack of authentication mechanisms. At the time of the assessment, there were no security mechanisms developed for the management plane. Up to this point the research had been on proof-of-concept and getting the functionality working. Now that the code is operational, the research has moved to securing the communication channels between management plane nodes.

4. Authorization Mechanism Needed: In a production environment of GridStat there would be data with varying levels of sensitivity. Users would need access to different data. Currently GridStat does not have any mechanism for limiting access to data. This is a known issue and needs to be addressed. It is anticipated that basic mechanisms could be designed and implemented in 6 months with a full-time experienced programmer. Currently there is not a funding source for this task.

5. Dynamic Port Allocation: GridStat is designed using CORBA, which utilizes dynamic port allocation. The assessment noted that it would be difficult to implement GridStat into existing network infrastructure because it uses dynamic ports. Creating firewall rules on such a system is unmanageable. This was a known issue to the development team. A number of options are available to mitigate this concern, but all would require an overhaul of the existing code. This is a significant effort that will need to occur before commercialization of GridStat. It is estimated that an experienced full-time programmer could accomplish this in 6 months. Currently there is not funding for this effort

The details of the report helped guide GridStat's development work. As described above, a number of unknown issues were found at this early stage of development and will be quickly resolved. The testing and exploit-demonstration code modules that were developed in the assessment are being incorporated into the GridStat test harness to ensure that regression does not occur on the corrected problems. A number of known issues were reconfirmed to the development team, some of which have funding and others do not. Table 1 below gives a quick summary of the issues, WSU's response and timeline for resolution. The sections are listed where the vulnerability findings are located in INL's assessment report (Hall et al. 2008).

Section	Vulnerability or Concern	Response	Timeline
2.3.3.1	Lack of authentication allows spoofing of publishers and subscribers	Related to lack of security mechanisms in the management plane (see section 2.5 entry below)	Summer 2009
2.3.3.2	Client Identification Not Retained	Unknown but easily resolved bug	Fall 2008
2.3.4	No authorization mechanism	Prototype authorization mechanism has been demonstrated using TrustBuilder2 yet a full solution requires developing greater understanding of requirements	Not a current research activity in the project. 6 months of programmer time would provide basic mechanisms. Research needed to map into power nomenclature.
2.4.4.1	Encryption is optional	Unknown but easily resolvable bug	Fall 2008
2.4.4.2	Data point replay	Protocol design issue	Explore possible solution in research prototype Fall 2008
2.5	Management plane vulnerabilities	No management plane security mechanisms in current GridStat	Summer 2009
2.6	Lack of logging	Logging mechanism is present but largely unused	Mapping requirements onto the mechanism is a implementation activity
2.7	Network security	Tension between providing better, more interconnected communication and providing protection from attack using isolation	Needs significant research but not a currently funded activity

Table 1: Response to Vulnerabilitiy Assessment

The GridStat team at WSU identified two additional concerns that need to be part of the long-term outlook for GridStat research and development. First, GridStat's security design implicitly relies on the ability of individual entities to securely hold secrets. While GridStat's current design uses symmetric-key cryptography, this requirement would not be reduced by using public-key techniques. Either way, entities can only be identified by the secrets that they know and use while they are in operation. Research is needed to identify and implement host security

mechanisms to protect these secrets while meeting operational requirements in a widely-dispersed infrastructure.

Second, GridStat and the applications that use it require robust distributed time synchronization and rely on the accuracy of timestamps carried in messages. Research is needed to quantify the security vulnerabilities related to attacks on timekeeping and distribution services, to understand what forms those attacks might take, and to devise mechanisms to mitigate the effects of attacks on applications.

Visualization Integration

Integrating a visualization tool of GridStat into the Electricity Infrastructure Operations Center (EIOC) at Pacific Northwest National Laboratory (PNNL) was an important aspect of this project. The EIOC is a laboratory specifically created for researching the power grid. Integrating GridStat into this environment was beneficial both from research and awareness perspectives. Initially the visualization tool was going to be a standalone application but after further analysis, it was determined that for maintenance and ease of upgrades utilizing the same demonstration tool available at www.gridstat.net/demo would be superior to the standalone application. The current version of this tool was completed in September 2008.

Figure 2 below shows some of the capabilities of GridStat. The left box contains both power generation statistics from a number of Avista's generators and latency statistics between nodes in the network. The sudden increase in latency on the yellow line illustrates a failed link. The right box contains frequency data from PNNL, INL and WSU as well as a grey trending line.

Continued Effort / Future Work

There is significant work left to commercialize GridStat. The recommended commercialization plan is structured into three domains: Core Development, Cyber Security and Pilot Projects. Each domain contains phased subtasks, which can be funded individually or in concert with other tasks within the same phase. Each phase builds upon its predecessor(s) to increase the robustness and maturity of GridStat. Table 2 briefly defines the subtasks and anticipated funding required. For more information, see the GridStat Capability Development Roadmap (Bakken and Hauser 2008).

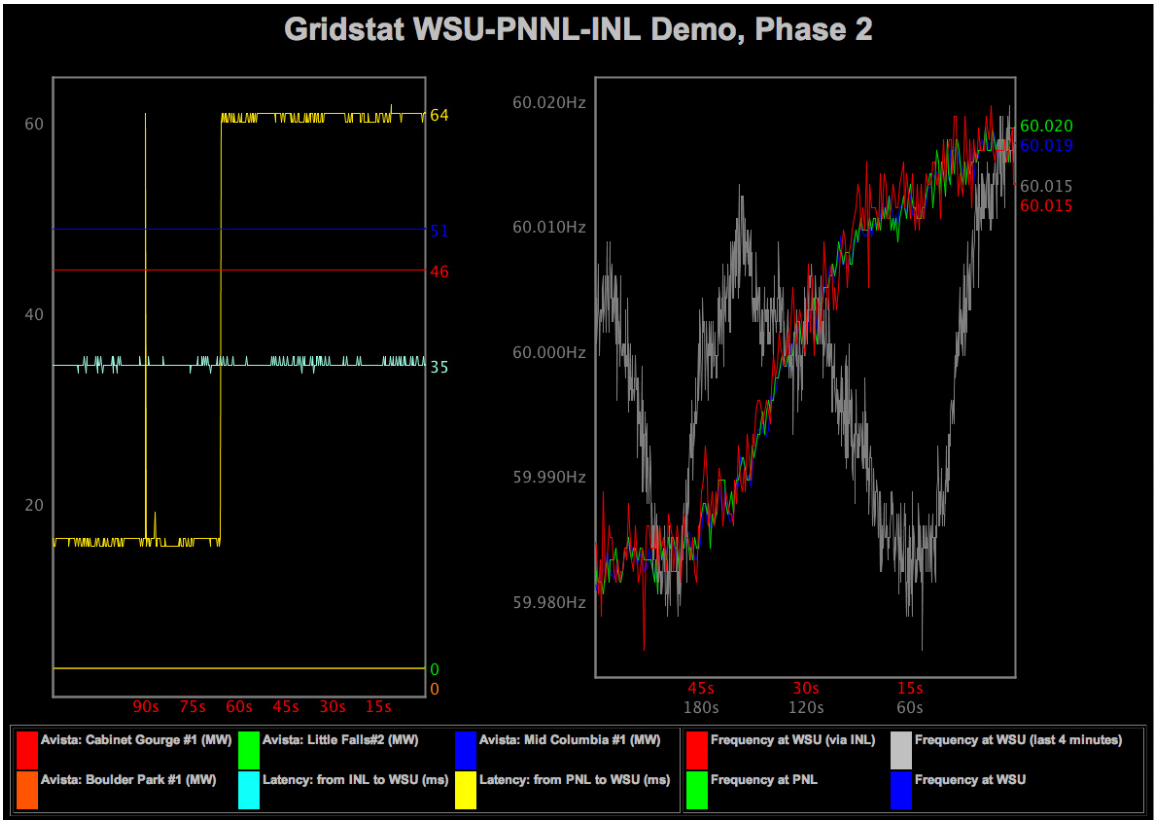

Figure 2: GridStat Visualization

	Core Development ~2.4 Million				Cyber-Security ~600K	Pilot Projects: ~1.2 Million	
Phase	**Config Tools**	**Policy Support**	**Verf. Suite**	**Instrument**	**Baseline Security**	**# of Sites**	**Kind of Communication**
1	Basic 150K	Hard-coded	Build regres-sion	Link-level & path QoS logging	Address INL-identified vulnerabilities	7	Phasor Measurement Unit (PMU) data between control centers
2	More powerful	Simple	Base-line	Report violations	Simple Trust-Builder policies	2–10 more	PMU & other data between substations: simple Special Protection Scheme
3	Reason-able	Reason-able	Basic	Simple health dashboard	Reasonable Trust-Builder policies	10–20 more	PMU & other data between substations: generalized Special Protection Scheme
4	Mature	Mature	Reason able	Complex health dashboard	More trust mgmt. TBD	20–50 more	PMU and other data (incl. actuator cmds) to substation for control

Table 2: GridStat Development Plan

Conclusion

A successful collaboration between WSU, INL and PNNL has evaluated the security attributes of GridStat over a regional network, which brought to light unknown issues and emphasized known security deficits. The GridStat development team took the information learned and has allocated resources to many issues and is actively seeking funding sources for the remainder. This project has helped GridStat become a more robust and secure real-time data delivery framework.

References

Abelsen, Stian Fedje, 2007. "Adaptive GridStat information flow mechanisms and management for power grid contingencies." *Thesis (M.S. in computer science)*, School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA August 2007. Available via http://www.dissertations.wsu.edu/Thesis/Summer2007/s_abelsen_120707.pdf.

Bakken, D., A. Bose, and S. Bhowmik. 2000. "Survivability and Status Dissemination in Combined Electric Power and Computer Communications Networks." In *Proceedings of the Third Information Survivability Workshop* (ISW-2000), CERT, October, 2000, Boston, MA.

Bakken, David and Carl Hauser. 2008. "GridStat Capability Development Roadmap." Washington State University, Pullman, WA September 30, 2008.

Dionysiou, Ioanna. 2006. "Dynamic and composable trust for indirect interactions." *Thesis (Ph. D. in computer science)*, School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA, August 2006. Available via http://www.dissertations.wsu.edu/Dissertations/Summer2006/i_dionysiou_072406.pdf.

Gjermundrød, Kjell Harald. 2006. "Flexible QoS-managed status dissemination middleware framework for the electric power grid." *Thesis (Ph. D. in computer science)*, School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA August 2006. Available via http://www.dissertations.wsu.edu/Dissertations/Summer2006/k_gjermundrod_072406.pdf.

Hall, Chuck, Michael Milvich, and David Kuipers. 2008. "GridStat Cyber Security Assessment Report." INL/EXT-08-15041 November, Idaho National Laboratory, Idaho Falls, ID.

Helkey, Joel Norman. 2007. "Achieving end-to-end delay bounds in a real-time status dissemination network." *Thesis M.S. in computer science)*, School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA May 2007.

Irava, Venkata Srinivas. 2006. "Low-cost delay-constrained multicast routing heuristics and their evaluation." *Thesis (Ph. D. in computer science)*, School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA August 2006. Available via http://www.dissertations.wsu.edu/Dissertations/Summer2006/v_irava_072106.pdf.

Johnston, Ryan Andrew. 2005 "Obtaining high performance phasor measurements in a geographically distributed status dissemination network." *Thesis (M.S. in computer science)*, School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA May 2004. Available via http://www.dissertations.wsu.edu/Thesis/Summer2005/r_johnston_072905.pdf.

Muthuswamy, Sunil Karthik. 2008. "System implementation of a real-time, content based application router for a managed publish-subscribe system." *Thesis (M.S. in computer science)*, School of Electrical Engineering and Computer Science, Washington State University, Pullman,

WA August 2008 Available via
http://www.dissertations.wsu.edu/Thesis/Summer2008/S_Muthuswamy_080408.pdf

Ping, Jiang. 2004. “A naming and directory service for publisher-subscriber's status dissemination.” *Thesis (M.S. in computer science)*, School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA May 2004. Available via http://www.dissertations.wsu.edu/Thesis/Spring2004/P_Jiang_050504.pdf.

Solum, Erik. 2007. “Achieving over-the-wire configurable confidentiality, integrity, authentication and availability in GridStat's status dissemination.” *Thesis (M.S. in computer science)*, School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA December 2007. Available via http://www.dissertations.wsu.edu/Thesis/Fall2007/e_solum_121807.pdf.

Viddal, Erlend Smørgrav. 2007. “Ratatoskr : wide-area actuator RPC over gridstat with timeliness, redundancy, and safety.” *Thesis (MS. in computer science)*, School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA December 2007. Available via http://www.dissertations.wsu.edu/Thesis/Fall2007/e_viddal_081407.pdf.