SANDIA REPORT
SAND2018-8199
Unlimited Release
Printed July 2018

Leveraging Technology Services for Public Good

Ian Phillip Miner, Troy Stevens, and Thushara Gunda

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone:	(865) 576-8401
Facsimile:	(865) 576-5728
E-Mail:	reports@osti.gov
Online ordering:	http://www.osti.gov/scitech

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone:	(800) 553-6847
Facsimile:	(703) 605-6900
E-Mail:	orders@ntis.gov
Online order:	https://classic.ntis.gov/help/order-methods/

SAND2018-8199
Printed July 2018
Unlimited Release

Leveraging Technology Services for Public Good

Ian Phillip Miner, Troy Stevens, and Thushara Gunda
Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185-MS1137

Abstract

As the technological world expands, vulnerabilities of our critical infrastructure are becoming clear. Fortunately, emerging services provide an opportunity to improve the efficiency and security of current practices. In particular, serverless computing (such as Amazon Web Services and REDFISH’s Acequia) provide opportunities to improve current practices. However, the critical infrastructure needs to evolve and that will require due diligence to ensure that transferring aspects of its practices onto the internet is done in a secure manner.

TABLE OF CONTENTS

NOMENCLATURE

Abbreviation	Definition
AWS	Amazon Web Services
SCADA	Supervisory Control and Analysis

1. MOTIVATION

As technology expands over the globe, cyber security, especially surrounding our critical infrastructure, is becoming more important. There have been countless attacks on our power plants and banks from countries abroad. Not long ago it was reported that hackers gained access to multiple power plants at once, across the globe, and had the ability to turn power off at will[1]. Countries all over the world are creating cyber security teams as well as hacking teams; some are being created to defend, while others are being made to attack. There are even hacker teams (such as grey hat hackers and criminals) that are not connected to a country. Nonetheless, this emphasis on cyber defense puts even more importance on cyber security for critical infrastructure.

2. CRITICAL INFRASTRUCTURE & SCADA

Some of the key parts of critical infrastructure are the control and operation of water and power plants. Today a system called supervisory control and analysis (SCADA) is used to control many water treatment plants, electrical systems, and nuclear power plants. Unfortunately, SCADA has vulnerabilities that cause utilities to not be as secure as they could be. This is due to many factors, the main one being lack of funding[2]. This is a big issue because with limited funding there is a lack of training on and maintaining of the SCADA systems. There have also been cases of SCADA systems being hacked due to negligent practices such as failure to change the default password. Even if there was enough funding and personnel properly installed and configured SCADA, the largest issue is the centralization of all the data coming from the power plant to one point. This creates a single point of failure that if a hacker exploited would gain vast control and information into a plant.

Two distinct vulnerabilities exist in modern SCADA systems. The first is unauthorized access to the control software, whether it is human access or changes made deliberately or unintentionally by a virus or other malware on the control host machine. Whether intentional or not, this issue highlights SCADA's vulnerabilities to insider threats[2]. The second is the threat of packet access to the network segments hosting SCADA devices. This is because SCADA packets differ from normal network packets. For instance, they sometimes SCADA uses a simple light weight internet protocol that uses a different port, and they believe that this is efficient security through obscurity but using an abstract packet and protocol can sometimes make the packet easier to track and find. People believe that SCADA systems are secure through obscurity by using specialized protocols and proprietary interfaces. This leads to other security oversights, which is particularly problematic given increasing awareness among the hacker community about the vulnerability of this important software[2]. This leaves the world stumbling for a better way to secure and control their power systems, and the answer just might be using the cloud such as Amazon Web Services (AWS).

3. PROPOSED SOLUTION: SERVERLESS COMPUTING

Given the rapid growth of large technology companies, new opportunities for helping protect critical infrastructure now exist. Companies such as Google and Facebook are buying massive chunks of land across the United States and even the globe to create data centers with computing power that has never been seen before[3].

These companies never want to have their servers crash due to lack of capacity. Therefore, they plan for the largest spikes possible and create 50, even 100 times more server capacity than they need. This leads to an excess of computing power on any given day. To not waste this excess computing power, these companies (such as Google, Facebook, Amazon, and Alibaba) have begun offering their computing power to others in the form of a service known as ‘serverless computing’. This name is slightly misleading because it is only serverless to the user. They call it serverless computing because the user does not need to worry about maintenance, up keep, or updating the server - all of those responsibilities fall upon the company providing the service. Thus, the user only pays for the server resources they use and the extra company services they apply to their project.

This use of excess computing power is more efficient, cheaper, and more secure than setting up an individual server[4]; a server used for computing power can be located anywhere and be combined with other servers as well. Therefore, there is a chance that it may expand into controlling water and energy plants. For the rest of the report, we will refer to the services available through one particular company (AWS was the company chosen) to highlight the capabilities that can be leveraged in serverless computing for critical infrastructure needs. Services of particular interest in this domain are AWS Kinesis (which organizes and analyzes data)[5], AWS Machine Learning (which can track the data from Kinesis and look for user specified events)[6], and AWS Lambda (which is AWS’ serverless computing and would execute protocols to control the pumps, valves, or whatever else needs to be controlled at a plant)[7]. This combination of AWS services creates a harder to hack, more secure version of SCADA, because it is running through three different services with different languages and can be bounced across multiple servers across the world. It also decentralizes the information from one building into the cloud. Using multiple servers in real-time, serverless computing also addresses security and synchronicity issues by spreading out the services across units.

The benefits of AWS do not stop there. A higher level of security can be achieved through AWS CloudWatch (which monitors and manages services and collects logs and data)[8], AWS CloudTrail (which enables governance compliance, operational auditing and risk auditing for your AWS services)[9], AWS GuardDuty (which detects threats and continuously monitors for malicious or unauthorized behavior)[10], and many more[11]. An additional level of security can be achieved through Amazon Macie. Amazon Macie is an AWS machine learning service applied to cyber security logs and events[12]. Due to the magnitude of logs that can pile up on a big project, using machine learning to sort through them is a great way to be as secure as possible. Any of these services would increase the security assuming the user is willing to spend the requisite amount of time to learn how to configure and implement the services correctly.

Furthermore, a company in Santa Fe, New Mexico is creating the first version of truly serverless computing. The company is called REDFISH and their idea is to use dormant devices to simulate a server. They call this idea Acequia, and it could be a major breakthrough in the computing world. The advent of REDFISH’s Acequia introduces large amounts of efficiency improvements by allowing individual participants’ (people or companies) dormant devices to be used for computing power[13]. But it also adds to the security because different devices are being used, making packets far harder to find much less hack. The participants can note which devices they allow

REDFISH to use for a specified project. These capabilities allow Acequia to leverage excess computing power in a similar manner that big technology companies have, essentially creating a new resource through dormant devices that has not been utilized in this way before.

4. CONCLUSION

A combination of AWS services and REDFISH's Acequia would create a system very similar to SCADA except with much more security. The level of security also increases as more serverless computing is done. In addition to tackling huge projects and issues constantly, the more serverless computing actions that are fired across the country the more secure each piece of information becomes. Soon trying to fine one piece of information is like trying to find a needle in a haystack, and once you find the needle, it is encrypted and protected by AWS security protocols. This use of computing power would create a new age of tackling issues of security at critical infrastructure plants on a national or global scale, in a potentially more secure way.

REFERENCES

1. Perlroth, N. & Sanger, D. (2018, March 15). Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says. *New York Times.* Retrieved from: https://www.nytimes.com/2018/03/15/us/politics/russia-cyberattacks.html

2. Kim H. (2012, November 25). Security Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks. http://journals.sagepub.com/doi/full/10.1155/2012/268478

3. Horowitz K. (2017, August 15). Facebook is building a new $750 million data center in Ohio. *CNN*. Retrieved from: https://money.cnn.com/2017/08/15/technology/facebook-ohio-data-center/index.html

4. Gancarz R. (2017, March 23). The Economics of serverless computing: A real-world test. *TechBeacon*. Retrieved from: https://techbeacon.com/economics-serverless-computing-real-world-test

5. Amazon Kinesis. Retrieved from: https://aws.amazon.com/kinesis/

6. Amazon Machine Learning. Retrieved from: https://aws.amazon.com/machine-learning/

7. Amazon Lambda. Retrieved from: https://aws.amazon.com/lambda/

8. Amazon CloudWatch Retrieved from: https://aws.amazon.com/CloudWatch/

9. Amazon CloudTrail Retrieved from: https://aws.amazon.com/CloudTrail/

10. Amazon GuardDuty Retrieved from: https://aws.amazon.com/GuardDuty/

11. Amazon Security. Retrieved from: https://aws.amazon.com/products/security/?nc2=h_l3_db

12. Amazon Macie. Retrieved from: https://aws.amazon.com/macie/

13. Guerin S. About Stephen Guerin. http://www.redfish.com/stephen.htm

DISTRIBUTION

1	MS1137	Troy Stevens	6617
1	MS1137	Thushara Gunda	8825
1	MS1138	Stephanie Kuzio	8825
1	MS1138	Katherine Klise	8825
1	MS1138	Marjorie McCornack	6616
1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories