Requirements and Challenges for Building a National Open Security Lab

Conference Paper · October 2015

CITATION
1

READS
634

3 authors:

Izzat Alsmadi
Yarmouk University
284 PUBLICATIONS **1,559** CITATIONS

SEE PROFILE

Mohammed N. Al-Kabi
Zarqa University
123 PUBLICATIONS **1,396** CITATIONS

SEE PROFILE

Emad Abu-Shanab
Yarmouk University
182 PUBLICATIONS **1,897** CITATIONS

SEE PROFILE

Requirements and Challenges for Building a National Open Security Lab

Izzat M. Alsmadi
Computer Science Department
Boise State University
Boise, ID 83725, USA
izzatalsmadi@boisestate.edu

Mohammed N. Al-Kabi
Faculty of Sciences and Information Technology
Zarqa University, P.O. Box 132222
13132 Zarqa, Jordan.
malkabi@zu.edu.jo

Emad Abu-Shanab
Management Information Systems Department
IT & CS Faculty
Yarmouk University, 21163 Irbid – Jordan
abushanab@yu.edu.jo

Abstract

The evolution of Internet, networking and security continue through the recent years. Such evolution in those fields or technologies expand significantly their rules and usage in our life. The world is now connected through the Internet not only within computers, laptops, etc. but also within smart phones, tablets, smart devices, etc. The Internet of Things (IoT) envisions that eventually everything around us (i.e. cars, refrigerators, homes, etc.) will be part of the Internet and send/receive information in one way or another. On the other hand, security continues to evolve and intruders of security in networks and users' private information try always to find new methods and techniques to hack into those resources. As a result investing in security assessment and protection methods become a national priorities for all countries around the world. In this paper, we present a proposal to develop a security open test lab as a national project. We present major requirement and design issues. We present also some of the significant security issues or challenges that should be handled to be able to successfully design and operate such labs.

Keywords: Open labs, security experiments, network security.

1. Introduction

Users try to illegally access illegitimate resources for a wide variety of purposes. Despite the fact that most countries continue to push serious sanctions on such acts, yet such hacking schemes and breakouts continue to appear in almost all countries around the world. There is no doubt that

the financial return from some hacking methods is considered significant. This is particularly true in countries that e-commerce becomes more popular than real or physical commerce. Information of credit cards, bank accounts, etc. are all transferred or exchanged between buyers and sellers online. This can be seen as a significant source of income for hackers specially where such hackers can be in different countries that have less rigorous sanctions. For example areas in Africa and east Europe are often seen to be sources for financially hacking schemes. In addition to hacking for financial information, passports and different identity information can be found in such black market websites where buyers can buy such information and can possibly use it in physical, rather than only in cybercrimes.

Recently, we witness several cases of large hacking schemes for political purposes. For example, “Anonymous” is a name that is used in many different websites to refer to a large group of hackers who are joining efforts to attack a particular country based on political reasons. Those hackers try to use a large spectrum of hacking methods and tools to target many websites in targeted country. Their goals are not monetary related but rather to bring the websites and the networks of such country down, causes significant breakouts and embarrassments. They also often post their political messages through hacked websites. Political purposes in such cases are often combined with looking for popularity of fame. This is despite the fact that they want to stay “anonymous”. In additional to having technical skills, such teams are usually profiled as young males; chasing adrenaline motives and caring less for possible consequences.

Security controls and mechanisms continue to grow in technology and schemes. In parallel hacking schemes continue to grow and become more serious and complex. It is envisioned that in future some cyber security crimes may impact deeply and significantly human life and may seriously disrupt daily activities especially as smart cities are growing around the world. Those

smart cities typically use SCADA (supervisory control and data acquisition) system. Those systems can be typically monitored, accessed and controlled online and/or from remote location. In that sense, the challenge of trade-off between security and many other quality aspects of technology and life exist. In such trade-off tightening security requirements may come at the cost of having less convenient, time consuming systems, processes, etc.

Open test labs allow physical labs from different locations to integrate and share resources. Eventually, users from those labs and elsewhere can have access to those resources and be able to conduct experiments on resources that they can't have locally. In comparison with simulation, open test labs allow users to *emulate* remotely computer and network resources; which is more realistic.

In the last few years many large scale national or regional labs were established around the world. The largest and most significant ones are GENI (https://www.geni.net) in USA and OFELIA (http://www.fp7-ofelia.eu/) in Europe. GENI is planned to host experiments for the future Internet. Currently, major Universities in US form the infrastructure of the open lab where they have Software Defined Networking (SDN) open labs. SDN evolves as a recent networking architecture to make networks more open and programmable. In SDN, controller is taken from switches and allocated remotely in a software called the controller. OpenFlow protocol is designed and used to define the communication between the controller and its switches.

Branching from GENI, many customized open labs exist to serve certain focuses. Examples of those focused open labs are: Emulab (https://www.emulab.net), CloudLab (https://www.cloudlab.us), Aptlab (https://www.aptlab.net/) and Deterlab (https://www.isi.deterlab.net). Deterlab in particular focus on security related experiments. It tries to emulate real world security complexity and experiments. The Lab allows running

different security experiments despite that some experiments may require special security control mechanisms to ensure a resilient system protected against crashes or breakouts.

In this paper, we propose a cyber-security open testing lab. We will evaluate requirements to build such lab. We will also describe some of the technical challenges and how such issues should be handled. We think that such labs are important and necessary and can form a strong cooperation between different University and research facilities at the national level. Such cooperation can be beneficial not only for resources' sharing but also for knowledge sharing and dissemination.

The rest of the paper is organized as the following: In section 2, we will present a general information background about security open labs. In section three we will introduce examples of relevant research contributions. In section four we will present requirement and design issues for security open labs. Challenges in such labs are presented in section five, Paper is concluded in section 7.

2. Background

Conducting experiments for research and education is a major activity in terms of amount of resources required to have the right tools and equipment. While large Universities in major cities may afford acquiring or having labs for such experiments, however, most small Universities, community colleges, schools, etc. lack the ability to have or afford such resources. In addition, researchers or students who are not affiliated with Universities or research institution may want also to be able to conduct such experiments. Those are only examples of situations where the case for having a national open test bed is important and should be one of the major national interests from both research and education perspectives.

As an alternative to conducting experiments on real systems, many students and educators use simulation labs and tools as an alternative. For example, simulation tools such as Matlab, NS2, NS3, Qual, Labview, etc. are widely used. Those tools allow designing and building virtual environments that simulate real environments. How much those simulations are realistic or close to real situations?! This can vary from one tool to another or even from one experiment to another. Nonetheless, this has been a very convenient and affordable alternative to real labs.

Emulation can somewhat falls in the middle between real or physical labs and simulation. Users can have remote access to real or physical equipment. If sufficient resources exist and if Internet connections provided between users and lab resources are reliable, those open labs or test beds become to users real labs. In addition, those open labs optimize the usage of such resources. Management of such labs should have effective schemes to guarantee that time and scheduling schemes are in place. Those schemes should best distribute resources where all users or service requesters can allocate required resources. Resources should not be left idle for a long time in experiments. This will ensure that resources can be always available for service requesters.

Deterlab is an example of open test bed dedicated for conducting security experiments (USC/ISI's DeterLab, 2015). The lab is open for all users, educators and students in US. Instructors can create courses and experiments in Deterlab. Students can reserve resources (e.g. computers, network equipment). They can specify in details for example what operating system should run on each allocated machine, what software to install on each host, what kind of connections to have between different reserved hosts, topology, etc. All those experiment specification can be specified typically using scripts (e.g. .NS). Users can then swap in their experiments. Deterlab will try then to reserve requested resources. Once those resources are reserved, users can remotely login to those resources and start conducting their experiments.

3. Literature Review

The architecture for security in Open Grid Services Architecture (OGSA) has been has been presented by (Nagaratnam et. al., 2003), and a security model is exhibited by in their paper. OGSA specifies the Standard policy management for Grids, and shows how Grids can employ Web services techniques to specify, publish and enforce security policies.

Students of Information Security curriculum should gain an essential experience to install software, setup software and hardware, but students may find it hard. Therefore many propose the use of virtual machines (VMs) to train students. Furthermore to avoid the numerous problems generated by those students that include network security penetration testing, session hijacking, injection attacks, and spoofing (Bulbrook, 2006) proposes a method to isolate these problems into a virtual environment. He developed a security lab on VMware that supports Windows systems, where the students have to configure these VMs manually to understand the effect of proper configuration and attacks. Furthermore, VMs help students to train with the same computer configuration, and allow for the standardization of the initial work environment (Kneale et. al., 2004)(Damiani et. al., 2006).

This part of the this section is dedicated to public testbed called Global Environment for Network Innovations (GENI)that funded by National Science Foundation (NSF). Therefore in this part we present one of the studies related to GENI project. GENI testbed is used by (Edwards, Liu, and Riga, 2015) to illustrate and present their methodology for experimenters to write and deploy duplicated and sharable experiments that deal with these problems. Also best practices about deploying an experiment in a community testbed are described.

Deterlab is an infrastructure designed to support large-scale security experiments. In this part of literature review section we present few papers that use or propose an improvement to DeterLab.

(Benzel, 2011) study presents the evolution of experimentation science and a transformed facility for cyber security research development and evaluation using DeterLab infrastructure. (Murillo and Duarte, 2013) study suggests an improvement to the capabilities of DeterLab, and propose the use of virtual networks developed in the Future Internet Testbed with Security (FITS) technologies. The feasibility of capturing and fitting Internet's topology snapshots to Deterlab is studied by (Perera, Miller, Mela, McGarry, and Acosta, 2013). They successfully found a scalable way to represent Internet's topology snapshot in Deterlab, and their work is accompanied by proving the usefulness of their solution. (Hussain and Amin, 2012) study exhibits an experimentation framework for the evaluation of Networked Control Systems (NCS) on Deterlab infrastructure. The experimentation framework they presented consists of three major components: a physical-to-cyber interface, physical dynamics, and a cyber network model. To evaluate the impact of denial of service (DoS) attacks on scalar linear systems they develop several attack scenarios, where the results of these attack scenarios yield novel insights about the network-induced security and reliability failures in large scale NCS.

4. Open Security Lab Design and Requirements

An open lab includes an aggregation of several labs hosted by different Universities, research institutions, etc. Top level software management programs should have control and management on all those resources. Typically there are two connections to local labs, one for management and the other one for experiments. Figure 1 shows a high level data flow diagram for Deterlab (USC/ISI's DeterLab, 2015). Experiment details and topology are sent to the lab as a request. A container allocation system receives the request to evaluate required resources. The container communicates also with Lab resource allocation system to request resources reservation. Physical resources receive both configuration and resource allocation information as inputs.

Logical resources are reserved part of the physical resources. The same physical lab can provided services to many experiments simultaneously. In addition, one experiment can span more than one physical lab based on experiment details or constraints.

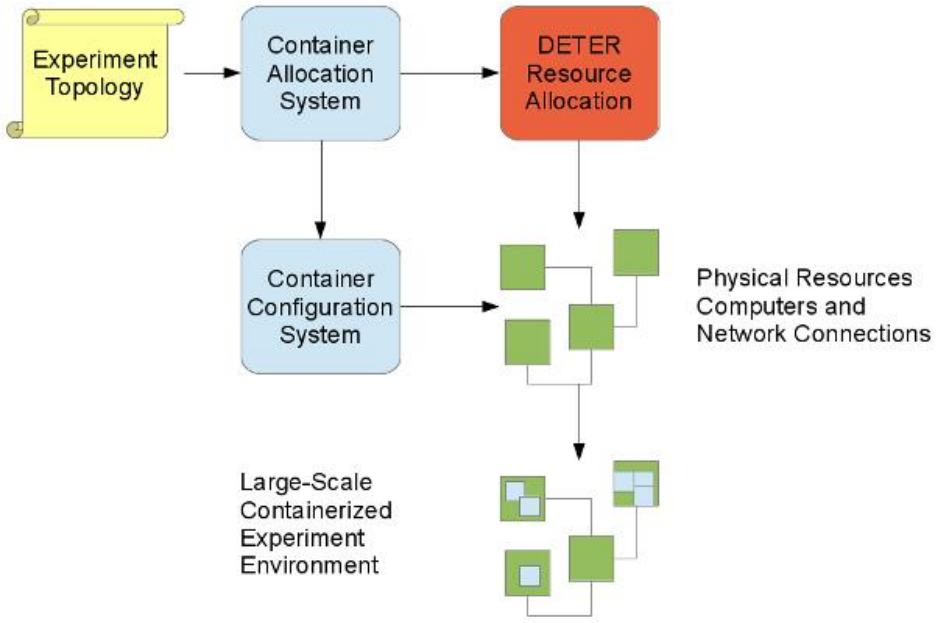

Figure 1. High level data flow diagram; Deterlab (USC/ISI's DeterLab, 2015)

A major enabler to open labs in general is Software Defined Networking (SDN) and its instance OpenFlow protocol (Casado et. al., 2006)(Casado et al., 2007)(Casado et al., 2009). SDN is a recent networking architecture that tackles issues related to the need for flexible, open and programmable networks. SDN separates control from data in network switches and allocate control centrally in a software controller. Software controller can then communicate with its switches for flow and access control rules. OpenFlow; as a protocol instance of SDN, defines communication between controller and its switches. Users and their applications can communicate with the network indirectly through the controller. Traditionally, network

switching and routing protocols are closed and vendor specific where users and their top applications have little control on those protocols.

There are many examples of open source and commercial controllers. Each networking company has its controller while there are many controllers for new startups. Examples of open source controllers include: Opendaylight, Floodlight, Ryu, Pox, Nox, etc. Those controllers typically allow access to their controller and network resources through standard REST interfaces. Users can also develop their own application on top of those controllers to manipulate networks. They can see flows in switches flow tables reactively added in real time based on traffic and control.

There are several design issues that should be discussed and planned prior to building open security labs. Here, we describe examples of those design issues:

- **Local and Remote Control and Management Issues**

In open labs, control and management can and should exist in each local physical lab. Additionally a central control, maintenance and management should exist for the whole national or regional testing lab. Rules and regulations should be put in place to ensure the avoidance of conflict decisions. Ultimately and similar to SDN architecture, a controller should exist to monitor and control all physical labs centrally. For failure and reliability issues, this controller can have backups, or its core tasks can be distributed across several controller instances. Communication for control and management should be separated from the normal communication channel that is used between users and experiments.

- **Time and Resources' Allocation Schemes**

Certain programmable controller modules or software applications should be dedicated for the tasks of time and resources' allocation. It is expected that in certain times resources may not be available to provide services to all experiments or service requesters. An optimized scheme

should exist to ensure that will not have idle experiments or wait for a long time till acquiring their requested resources. Experiments in general can be given two types of expiration schemes; idle expiration scheme where experiment resources can be de-allocated when a certain idle time passes. Hard expiration times should also exist where regardless of usage, resources will be released at this time. In both cases, users should be continuously notified that their resources' allocation will expire soon. They should be also given the option to back up certain resources or their content. Many open labs allow permanent offline storage for users per their requests.

- **Scheduling Schemes**

In integration with allocation schemes, scheduling schemes should track and monitor different experiments. Different experiments should be logically separated. Users can have the ability to swap in and out their experiments. Users will be also warned by emails that their experiments are about to expire. Scheduling and resource allocation schemes should consider the availability of resources in each physical lab. They should also consider any constraints. Those constraints can be permanent (e.g. bandwidth limitation, throughput, etc.) or can be temporary such as temporary blackout or maintenance times. Users or experiments who/that will be possibly impacted by any non-periodic resource problems should be informed.

- **Future Lab Expansions**

There is no one or single standard scheme on how open labs should start or expand. They can start through integrating several existing physical labs. They can also start from new labs built using new SDN-supporting equipment. Most current SDN open labs require switches or network equipment that support OpenFlow protocol. In addition bandwidth and capacity of either channels or network equipment should be considered in each physical labs. Experiments that

may span more than one physical lab can significantly impacted, if the different physical labs have different bandwidth capacities or capabilities.

5. Open Security Lab Challenges

As a new and evolving architecture, SDN presents both security challenges and risks. Both SDN and open security labs can help experimentations on new security features and controls. For example, future security controls may see programmable firewalls, IDS, etc. where such security controls are completely programmable. In such sense, access control rules can be added/modified/deleted in those security controls based on real time traffic, network topology changes or malware breakouts. A future resilience network may possible exist where the network is adaptable to its environment without or with the least human or manual intervention.

From security concern perspectives, research investigations showed that SDN networks have their own vulnerabilities. The flexibility offered in SDN networks can be abused or misused by users. For example, an application that is developed on top of an SDN controller can interact with the network and its flows. Such application can have its own vulnerabilities. Vulnerabilities can also come from the host operating system, users, authentication systems, etc. Eventually, such application can be used as an entry for illegitimate access to the controller or the network.

Unlike other experiments, security experiments can have significant security concerns. Security experiments may cause the whole network or part of it to be idle, crash, or be corrupted. Denial of Service (DoS) or flooding attacks may impact other experiments currently running in the open lab. We conducted several experiments for such kind of resource exhausting experiments. Results showed that other experiments can be significantly impacted. There are risks of possible malware or worm breakouts. Such labs can be a rich source of worm’s creation and expansion.

We explicitly described the following challenges as the most significant to be handled for an open security lab to run without serious problems.

We described few examples of security concerns that may arise when building open security labs:

- **Resources and Logical Isolation between Different Experiments**

With SDN and virtualization, the line between physical and logical or virtual resources is very thin. From users' views or perspectives, we may not be able to distinguish that our allocated resources are physical or logical. In open test beds, for security, privacy and integrity reasons, it is very important to ensure that different experiments do not interfere with each other. Security controls should exist to ensure such isolation. While the issue with security test beds can be less sensitive to the same issue in the cloud for example, where financial and personal information may exist from different cloud users, nonetheless, the issue can still be important and relevant. There are many machines that support dual or multi-core systems. Such systems may provide resources for different experiments where those experiments share same physical resources.

- **Constraints on Security Experiments**

Many open test beds have their constraints and regulations on users and what are the limits of the kinds of experiments they can conduct. By far, Deterlab as an open security test lab, has the most flexible constraints on security experiments that can be conducted. This is since many security experiments by nature violate rules in normal networks and usage. For example, security experiments maybe conducted to perform MAC, IP or ARP spoofing, DoS and flooding attacks, etc. Such security related experiments can be typically banned or prevented on most physical experiments. However, this is not and should not be open. Both regulations and tools should exist to monitor and control how far such experiments can go. Fear that breakouts may happen

where for example an experiment may cause a worm to be launched within and beyond lab resources.

- **Security Controls and Mechanisms**

Open security lab should have its own security control mechanism. They should have firewalls and intrusion detection/protection systems. Identity management and access control are very important security measures to have. Typically those labs allow only registered users to access lab resources. After registration, users are expected to verify computers that they are going to use the lab through. For example, keys are used to perform handshaking between lab and user computer. Users are required to upload their public key to the lab and keep a pair of their public and private key locally. Users may have local security controls that prevent remote access. The lab should have firewalls and other security mechanisms to ensure that illegitimate users are prevented from using or accessing the lab. Due to its open nature, the lab should expect that some intruders may masquerade legitimate users (e.g. through stolen keys). Security and audit mechanisms should be able to identify the possible of such situations and limit them.

- **Security Monitoring and Auditing**

Breakouts, failures or problems are expected to occur in security open labs. Monitoring and auditing systems are important to be important to trace back such problems for future preventions and fixes. Logging information should distinguish information or data from different users although they may be using the same physical resources. Those monitoring and auditing systems should be also transparent as much as possible to reduce the amount of overhead on the network. As described earlier, typically such activities should have a separate dedicated communication line and network other than the main network that is used by the users and their experiments.

6. Conclusion

In this paper, we presented a high level proposal to build a national or regional security open labs. The justifications for having such labs are enormous. This include for example resources optimization and the ability to serve educators, students and researchers all over the country or region regardless of their location (e.g. in a major city, University or rural area). Current technologies open the possibility for having such labs. For examples, Networks now have fast and reliable speeds that spread across most countries. In addition, technologies such as SDN makes it possible to manage and orchestrate centrally many physical labs that exist in different locations. We showed major design and security challenges that should be handled in order to build such labs.

References

Benzel, T. (2011). The science of cyber security experimentation: the DETER project. In Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC '11). ACM, New York, NY, USA, pp.137-148.

Bulbrook, H. (2006). Using virtual machines to provide a secure teaching lab environment. [White Paper]. Durham Technical College. Durham.

Casado, M., Garfinkel, T., Akella, A., Freedman, M. J., Boneh, D., McKeown, N. and Shenker, S. (2006). SANE: a protection architecture for enterprise networks. In Proceedings of the 15th conference on USENIX Security Symposium - Volume 15 (USENIX-SS'06), Vol. 15. USENIX Association, Berkeley, CA, USA.

Casado, M., Freedman, M. J., Pettit, J., Luo, J., McKeown, N. and Shenker, S. (2007). Ethane: taking control of the enterprise. In Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '07). ACM, New York, NY, USA, pp. 1-12.

Casado, M., Freedman, M. J., Pettit, J., Luo, J., Gude, N., McKeown, N., Shenker, S. (2009). Rethinking enterprise network control. IEEE/ACM Trans. Netw. 17, 4 (August 2009), pp. 1270-1283.

Damiani, E., Frati, F., and Rebeccani, D. (2006). The Open Source Virtual Lab: a Case Study. In: Proceedings of the Workshop on Free and Open Source Learning Environments and Tools FOSLET06, Lugano, Switzerland.

Edwards, S., Liu, X., and Riga, N. (2015). Creating Repeatable Computer Science and Networking Experiments on Shared, Public Testbeds. SIGOPS Oper. Syst. Rev. 49, 1 (January 2015), pp. 90-99.

Hussain, A. and Amin, S. (2012). NCS security experimentation using DETER, in Proceedings of the First Conference on High Confidence Networked Systems.

Kneale, B., Horta, A. Y. De, and Box, I. (2004). Velnet: virtual environment for learning networking," in ACE '04: Proceedings of the sixth conference on Australasian computing education, pp. 161-168, Darlinghurst, Australia, Australia, 2004. Australian Computer Society, Inc.

Murillo, A., and Duarte, O. C. M. B. (2013). Virtual Networks for Cyber Security Testing of Future Internet Proposals, in Second Workshop on Network Virtualization and Intelligence for the Future Internet - WNetVirt'2013, Angra dos Reis, RJ, Brazil, October 2013. English, A4 size, 1p.

Nagaratnam, N., Janson, P., Dayka, J., Nadalin, A., Siebenlist, F., Welch, V., Foster, I. and Tuecke, S. (2003). The Security Architecture for Open Grid Services. In: OGSA Security WG, Global Grid Forum.

Perera, G., N. Miller, N., Mela, J., McGarry, P. M. and Acosta, J. C. (2013). Emulating internet topology snapshots in Deterlab. In Proceedings of the third ACM conference on Data and application security and privacy (CODASPY '13). ACM, New York, NY, USA, pp.165-168.

USC/ISI's DeterLab (cyber DEfense Technology Experimental Research Laboratory), http://deter-project.org/about_deterlab.