Creation of Test Bed Security using Cyber-Attacks

[1]Dr.S.Kannan, [2]Mr.T.Pushparaj
Research Supervisor, Research Scholar,
Madurai Kamaraj University, Madurai

Abstract

Cyber-attacks requiredevelop ubiquitous and in directionto face current threats it is significant to understand them. Studying occurrences in a real environment however, is not viable and therefore it is essential to find other approaches how to inspect the nature of attacks. Achievementcomplete knowledge about them assists designing of novel detection approaches as well as considerate their influence. In this paper we present a testbed framework to simulate attacks that permits to study a wide varietyof security states. The framework deliversanidea of real world preparations, yet it keeps full control over all the activities achieved within the simulated infrastructures. Developing the sandbox environment, it is conceivable to simulate numerous security attacks and assess their effects on real infrastructures. In this paper the design of the framework assistancesfrom IaaS clouds. Therefore its deployment does not needenthusiastic facilities and the testbed can be organized over variousmodern clouds. The feasibility of the testbed has been confirmed by a simulation of specific DDoS attack.

Keywords

Testbed, cyber-attack, security, framework, security testbed.

I. INTRODUCTION

In instruction to be competent to face the threats modeled by modernattackers, it is critical tofrequently develop techniques and methods for detection and deterrence of attacks. Also, the nature of cyber-attacks is developing, so is the focus of attackers. This unstable character of computer attacks kindsit inspiring to catch up with current developments in the area. The condition is also difficult by the closed nature of the area, where attackers certainly do not discloseparticularsabout their methods, which often essential to be originate out only through real security events. In order to competentlyopposecontemporary attacks it is unavoidable to understand their nature and to grow mechanisms for their detection.Non-virtualized physical testbeds are expensive and inaccessible, and are often position constrained.

As such, present education and research for control system security is becoming progressivelydependent on virtualized labs and tools. Any learning or investigation undertaken using these tools, though, is established around the restrictions and appearances of such tools, as well as any expectations made by their designers. Additionally, the correctness of data subsequent from competitions and models may be further reduced if used outside of their proposed usage scenario. It is for that motive that projects such as SCADAVT suggest testbed frameworks for cyber-security research, based on a simulation method.

A virtualizedmethod offers important cost reserves and a self-paced and active method to learning. However, it also has numerous key restrictions including: no hands-on involvement, no real-world preparation with exact equipment and no involvement in recognizing and understandingimproper or uncharacteristic data. Simulation is active at signifying “correct” performance. However, critical substructure systems need to be protected against conditions where they are unprotected to extreme irregularproceedings. Inappropriately, in such conditions, schemes do not continuallyperform in the way predictable or answer in the same reliable manner. Correspondingly, it is consequently difficult to exactly model how a system’s erratic performance might cascade and influence other amounts of the infrastructure.The research obtainable in this paper deliversaperfect solution. The usefulcomponentcomplicated in the Micro-CI project announces a level of practicality that is problematic to match through simulation alone. It permits for the benefits of both physical and effective tools to be joined, and some of these are conversedunderneath.

A) Pedagogical benefits:

The Micro-CI method offers students and researchers hands-on involvement and first-hand knowledge of the irregularity of a system under occurrence or pressure. It will also help them to improve their difficult solving and applied skills.

B) *Cost effectiveness:*

The Micro-CI development has been intended to be as cost operative as conceivable. For example, at the time of writing, we assessment that at the time of writing, the design obtainable in this paper can be simulated at low cost.

C) *Portability:*

As the project apparatuses are on a reduced bench top scale, it permits them to be packed away, deposited and transported with ease. Schemes can still be enthused and/or deposited whilst partially collected.

D) *Platform independency:*

The Micro-CI project prepares not need any particularnecessities, dependencies or workingorganizations to connect with the testbeds established. Additionally, it is not tied or limited by any certifying model, so it can be used on an endless number of dissimilar machines, without experiencing additional costs.

II. INTENDED TESTBED ARCHITECTURE

Considering the determination and predicted use of the proposedtestbed organization we have recognized a set of necessitiesthat the testbed must fulfill to happen our requirements. For the sake of clarity, we divide these necessities into five groupsnetwork-related, hosts-related, monitoring, testbed control, and deployment desires. Concerning the network-related requirements, the testbed's capability to describe and run any network topology is perceptiblyrequired, whether it is a single node or numerous interconnected networks. The testbed has to permit users to have wholecontrol over the system Layer 3 arrangement. This feature, which is not obtainable in most of the prevailing security-related testbed answers that we studied, is essential to use an arbitrary L3 protocol and/or an addressing schema, comprising public IP discourseswithin a sandboxed environment. In order to technique real-world arrangements, additional network characteristics should bepreserved. To pretendnumerousnetworking kinds, like ADSL modems or mobile procedures, the testbed mustprovidecapability to emulate frequent network possessions, such as incomplete bandwidth, delays, packet drop rate, or connectiondisappointments. While we predict an inaccessible environment is used for most imitations, the testbed must also sustenancescenarios which necessitateassociates to real Internet servers. An example of such a scenario is an examination of the procedurebetween an infected computer and a real malicious server.

Such traffic must be filteredcorrectly using firewall rules.The hosts-related necessities concern the possibilities to sustenancenumerous hosts' formations. To deliveradequateflexibility, the testbed has to be able to create nodes running mutual operating systems and architectures. To deliverobserving features, the testbed is essential to display network links among any two nodes in the defined virtual topology and gatherchecking data about network movements or even packet dumps of the whole communication accepted over the emulated wires. Besides network-based probes, host-based probes eg. CPU and memory usage monitoringmust also be provided. Obviously, all the checking functionality has to be achievedclearly, so it cannot be noticed or even consequences could not be partial. The testbed control necessitiesbasically include potentialsto arrange the testbed and to control all its components easily. The testbed has to depiction a user interface that is overall enough yet informal to use for users so that they do not essential to cope with internal arrangementparts.

The testbed mustadditional give andchoice to achieve a defined set of processes in real time, permittingfor acommunicatinginterferenceto and/or control of consecutively attacks. Correspondingly, attack situationsthemselves must also be informal to set-up, organize and implement. The testbed mustprovisionrecurrences of the same experimentsnumerous times, which is essential, for occurrence, when tuning and assessing a specific detection mechanism.

Concerning the placementnecessities, the testbed must imagine just widely-used middleware for testbed processes so that one is capable to establishit completed an existing cloud-based substructureproviding maintained interfaces. Assumed the features we necessitate from such a security-related testbed, competences of the existinganswers, as well as profitsof the cloud-based infrastructures, we absolute to propose a new testbed retaining cloud infrastructures providing an substructure as a service IaaS clouds. Afterexpending well recognizedcloud interfaces, the testbed essential not rely on a specificcloud provider but can be certainlymodified to any of them, declaringequitable costs and providing suppleness when essential. Unlike to other answers, we deliver a general framework to build own testbeds, which can organized in dissimilar environments. This method has its restriction, with the central one being the arrangement of networks. Solely using widely-used networking devices, we present a newmethod to building flexible virtualized systems.

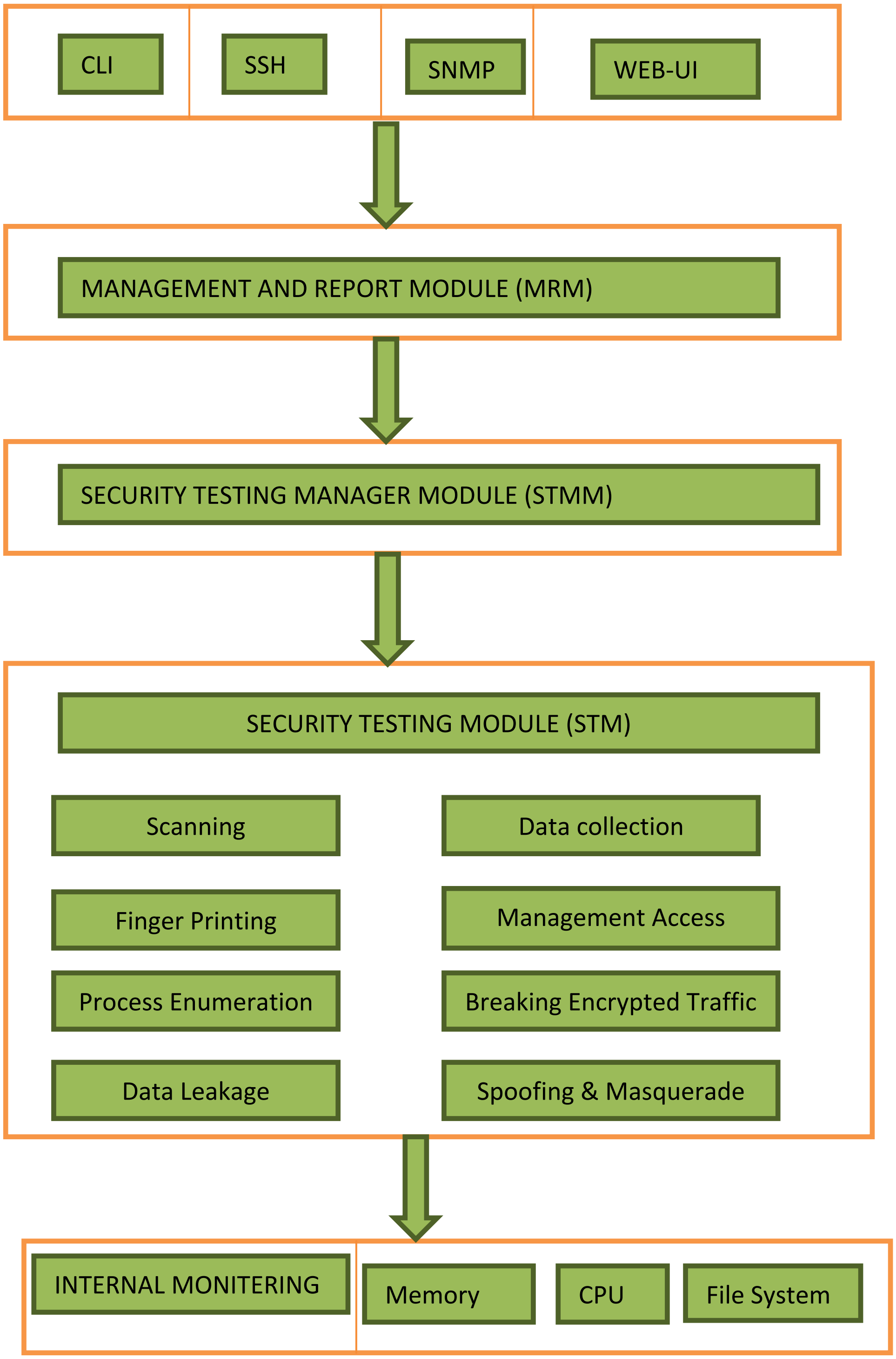


FIG 1 Retreat testbed structure

III. THE CYBER THREAT

Control system data is coded in protocol format to altercation information with apparatuses and RTUs. The protocol arrangementsdeliver automation and send information back to the control user interface to distribute a position of system operations. Communication procedures are intended for real-time operation. Two instances of industrial control network protocols contain Modbus and DNP3 Distributed Network Protocol. They are usually used in present day critical infrastructures and able to match the exactnecessities of the system. However, they are vulnerable to interruption and security breaches. One of the most common approaches of attack is the Distributed Denial of Service (DDoS) attack, where schemes are directed large volumes of traffic that is envisioned to make the scheme fail by congestion it. This attack is effective. It is a challenge to differentiateamong good and bad needs, making attacks difficult to block. Often cyber-attacks are exactly targeted at separate parts of substructures.

Numerous attacks are intended with the detailedpurpose of disorderly orthorough SCADA systems. One such attack is recognized as a Procedure Network Malware Infection (PNMI), which includes injecting a worm into the procedure network. The procedure network is frequently used for presenting the whole of the SCADA where statement is directed through procedures like Modbus or DNP3. Extracommonmethod is the Man in the Middle attack (MITM) where false commands or system directions and fake answers are introduced into the system. Not only can a MITM attack be used to reasondisturbance; it can also be used to deliver a way of eavesdropping; creation it significant to use verificationprocedures to ensure the confidentiality and integrity of the communications.The Cybernetic Verifying Ground allows users to generatevirtual surroundings that can be used for many doings likethorough forensics analysis of malware or security hands-ontrainings.

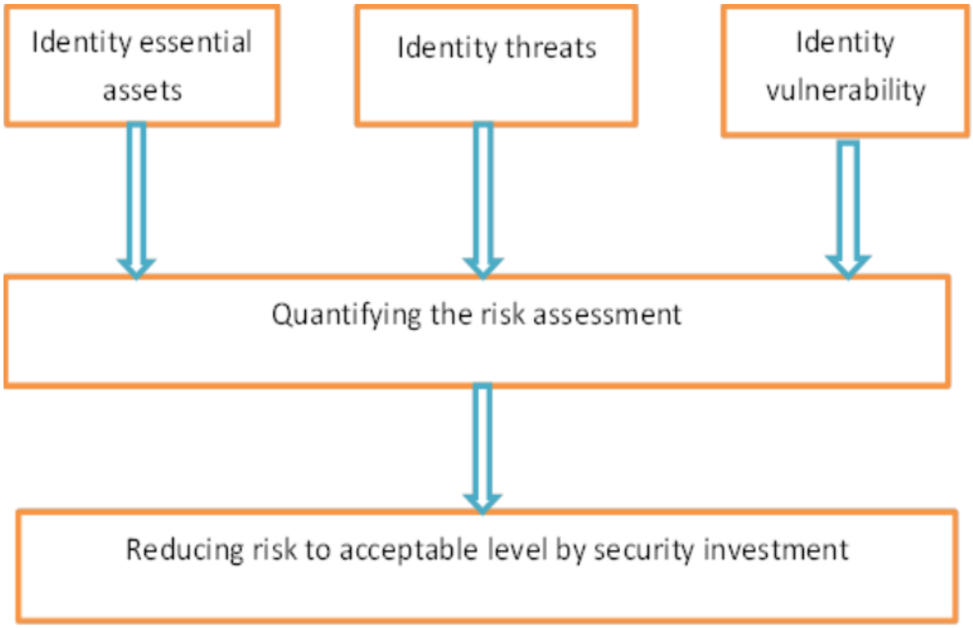

Identity essential assets
Identity threats
Identity vulnerability
Quantifying the risk assessment
Reducing risk to acceptable level by security investment

FIG 2the cyber thread security

IV. MODELING SECURITY SCENARIOS

An experiment is totallydefined by a scenario andprocedure of its recognition. The scenario is defined as a collection of nodes, logical and network topologies, monitoring rules, and a depiction of three stages of an attack simulation. Individually of these portionshave many obtainableconformationlimitations which regulate the network environment. Node is a machine which is a member of the logical substructure and it is associatedto the network substructure via its configurable interface. It is conceivable to define node's hardware (CPUs and RAM), its operating system, and application software. Network topology designates interconnections among all nodes in a situation. In order to pretend various networking preparations, such as ADSL modems or mobile devices, this topology is also configurable in numerous parameters such as packet loss and bandwidth. Logical topology designates the role reflector, attacker, victim, etc. of each node and network in the scenario. Once the scenario is wholly defined, the Scenario Organizationnode can implement the first of three phases' initialization, run, and evaluation ofthe attack simulation.

In the first phase, the initialization, network and logical topologies of the situation are recognized and parameters of the attack are set. This initialization is controlled by scenario organizationwhich instantiates the testbed in the Cybernetic Substantiating Ground.

The testbed delivers the network topology defined in the situation with all demanded monitoring rules applied in the second phase, the scenario run, the definite experiment is done. The attack is implementedconferring to the scenario. Both network and host observing infrastructures capture data such as NetFlow, IPFIX and host information from particular nodes and networks. The collector captures established data and permitsit to the Scenario Management Node for storage and extraanalysis.

All data and appearances are incessantlyremovedfrom the Scenario Management node to a conceptioninfrastructure where they are presented in accordance with necessitiesquantified by the scenario. A further description of conception is out of the scope of this paper.

The third phase, the evaluation, serves for an analysis of the experiment. Captured data is stored for advanced work, scenario alterations and it's re-run. The research can also be repeated by the imaginingorganization in dissimilar speeds. It is particularly useful in case of security training, where it is conceivable to use this functionality for detail interrogation of the exercise.The requirement is modest, denotation there is scope for future development; yet is enough in size to produce realistic substructureperformance datasets for research determinations.

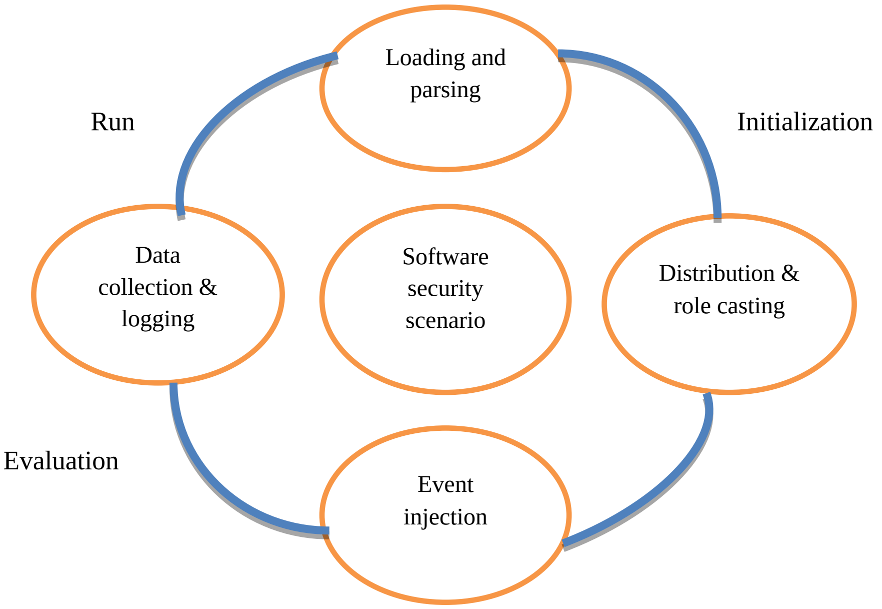

Loading and parsing
Run
Initialization
Data collection & logging
Software security scenario
Distribution & role casting
Evaluation
Event injection

FIG 3 Security Scenarios

V. SECURITY ISSUES

Security is not only the object of exploration using the testbed;it is likewise a vital necessity for the testbed itself. Security for the DETER testbed is dangerous, and the intimidations are both internal and external. Internal threats come from infectiouscode that is tested within DETER and portends to take control of the testbed or discharge into the Internet. Extrainternal threats come from experimenters who effort to steal test data or results prior to publication. The external threats come from those who see the testbed as a tempting target for exploit; thus, penetrationdefense is required.

Like any network infrastructure associated to the Internet, the DETER testbed is subject to attack; this is particularlyacute because a security testbed forms an attractive target. Both experiments consecutively in DETER and the testbed control plane must be endangered. Because of DETER's mission, DETER security has a major extra module: the public Internet as well as the testbed control plane and other experiments must be protected from attack by experiments running in DETER. Whereas security in most schemes is disturbed only with the problem of *infiltration*, DETER is moreover concerned with the problem of *exfiltration*.

The resolved of the testbed is to deliver containment for security experiments, to sustenance safe experiments that present a wide range of danger levels.

The highest dangerous level might be live testing of a communicable attack program whose potentials are totally unknown, for example an definitemischievous worm or virus. The traditional method to testing such dangerous programs has used atotally isolated laboratory containing of dedicated systems whose disk efforts and memory chips never consent the laboratory. Experimenters necessity be physically current in these laboratories and must be particularly trained.

Not all experiments necessitate complete separation from the rest of the internet, and in fact, it is a goal of our effort to delivervariable degrees of isolation depending on what is known about researchthat is to run. The method of the DETER project, is to build a solitary safe testbed that can alteration its operational mode to competition the danger level of the experiments. DETER delivers a shared laboratory capability for those experiments whose threat level is low sufficient to allow distribution, but it can be reconfigured for limited use for more hazardous experiments.

The testbed permits remote experimenter access for all but the most dangerous experiments. Additional paper in these workshop proceedingsdesignates techniques under progressfor stronger isolation and repression of real malware whose possessions are known, without the essential for a complete disconnection from the rest of the internet.

A) *Containment*

Containment addresses the essential to prevent exfiltration ofpackages from the testbed. The worst breach of repressionwould be announcement of a beforeinvisible virus or worm into the public Internet. In totaling to comprisinghateful code, the testbed comprises the effects of malicious software and extreme traffic that are produced by an experiment. The DETER testbed delivers containment done several resources. The first is the use of a physicallydiscreteexperimental network on which the nodes of an experiment interconnect. This network is incapable to route packagesbeyond the nodes that are part of the experiment. Second, as shown in figure 4, firewalls are located at several sites in the testbed and on the interface among the user machine and the open Internet. The problem of containment is a little more difficultwhen considering distribution of malicious code that has been consecutively within aresearch. While active exfiltration can be prohibited by the methods just definedi.e. no route for envelopes to leave the testbed, malicious code can escape by hiding itself in data repossessedto the outside by an experimenter upon deduction of an experiment.

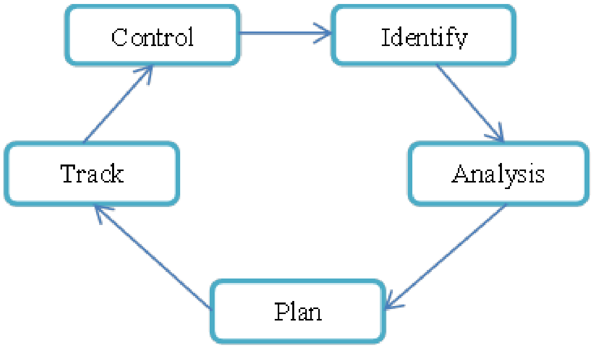


FIG 4 Risk management process

B) *Isolation*

We deliver physical link separation to address the essential toprevent experiments from interfering with one another, or for actions external to the experiment or the testbed to delay with the results of an experiment. Such interference could be inadvertent, such as the congestion of amutual network link by additionalexperiment, or deliberate such as from of a denial of service attack. A programmable VLAN switch is used to map physical influences between nodes, so there is efficiently no interferingamong links of the same or dissimilarexperiments, as long as the nodes are allocated on the same switch.

Because multiple switches are needed to handle the total number of nodes in the testbed, as well as to handle nodes at different physical sites, the testbed contains multiple switches connected by turning links, some of which are used within a site, and some of which are wide area. These relations may be over-subscribed by the rationalrelations crossing them, which can reason experimental artifacts varying performance when a single experiment uses nodes on multiple switches. Careful observing of joining bandwidth is used to attentivedetectives if interference or even just basic over distributionhas happened.

C) Confidentiality and Integrity

The confidentiality and integrity necessities of theDETER network midpoint around the defense of the data used by an research, the code and nature of the research, and the results of the experiment until such time as the consequences are available. Often aresearch will use input data such as movementsuggestions that are subject to nondisclosure contracts. Discretion must be providing while data is occupant in the performance area for aresearchdatabases and file systems, in place on nodes allocated to atesting, and while transiting the network. Confidentiality of the data thoughoccupant on the performancefile system, and while it is in passage to an allocated new node is providingfinished the use of the Cryptographic File System Integrity of the data used as inputs to and shaped by experiments is also dangerous. The reliabilityconcern is also addressed finished the use of a cryptographic file system.

VI. PROPOSED SYSTEM

A simple testbed can be created by manually wiringcomposed and arranging a committed set of machines; however, such a testbed lacks generalization and share-ability. Like Emulab, DETER belongs to the extravaluable class of testbeds that are general-purpose, shared, and distantlyavailableby experimenters. To support a large community of users, the testbed hardware can be separatedinto independent and inaccessibleexperimental testbeds, which can be used concurrently. Just as a main particle accelerator has numerous beam-lines, so the DETER testbed supports multiple concurrentexperiments. Emulab uses high-performance VLAN accomplishedchanges to dynamically make nearly arbitrary topologies between the nodes. Remote availability for beginning and monitoring of experiments is significant, but it may clash with security and repression requirements.

A main challenge of the DETER enterprise was to permit remote access for all but the most hazardous security experiments thoughpossession the experiments themselves limited within the testbed. Because DETER is envisioned to support security-related experiments, containment andsecurity were simplenecessities. Other goals for DETER were experimental fidelity, repeatability, programmability, and research functionality.

A) Fidelity

Fidelity to “real” networks, and in detailed to the realInternet, is significant. Dimensions to fidelity include:

(1) large sufficient number of nodes,
(2) realistic router and endsystemperformance,
(3) realistic heterogeneity of hardware andsoftware, and
(4) Realistic mix of link bandwidth and delay.

B) Repeatability

A dominant objective of DETER is to development the science ofcyber security, which needs repeatable experiments. The dynamics of the real Internet cover a wide range of circumstances, and Internet capacitiesdifferextensively in time and position. Internet topology, obtainable bandwidth and software forms, as well as the background “attacks” and user traffic that are present, are repeatedlydeveloping. It would be unbearable to truly recurrence a security experiment in the real Internet even if it were prudent to conduct such investigates.

C) Programmability

Some DETER experiments concern new networkmechanisms for observing, filtering, and analysis, which suggeststotaling or altering router algorithms. Router vendors are not anxious to open their platforms to newalterations, so the basic DETER node is programmable for this purpose. The experimenter can load particular PC router software such as Click or Zebra. Using software routers in DETER adds supplenessand programmability, butexpensesreliability. To regain some fidelity, the DETER testbed comprises a small number of commercial routers that can be linked into anew topology.

D) Research Functionality

The DETER testbed was made to sustenance research in aspecific topic area, security.

In calculation to the hardware and control software itself, that delivers a technical and social situation for security experimenters.

Proceduralsustenancecomprises a rich set of traffic and topology producers and experimental outlines, and tools for arrangement, conception, and analysis of results. As part of the exertion, have also established a powerful software environment for generating, monitoring, and controlling specific kinds of security experiments.

VII. PERFORMANCE ANALYSIS

As such, for the primaryportion of this case study, data for the watercirculation plant is recorded whilst operating under usualsituations. This allows the structure of aninteractive norm profile for the system.

Within the testbed, during the DDoS attack, only recurrentanalyses from the sensors are established, forcing it to make drastic and therefore uncharacteristicvariations to the testbed speeds, rather than regular as when operating usually. A small section of the data achieved at 00:10.5 in run time is shown in Table 1. There is no importantdifference present in the data. All the metrics maintain consistent trends in process.

Table 2 represents the delivery of standards for each of the modules over the 1 hour simulation. The unique value, max, min, median, mean and standard deviation of the values are established.

The DDoS attack on the system, which is thrown beside the RTU’s communications channel, results in recurrent sensor analyses.

Sample(t)	C1	C2	C3	C4	C5	C6
00:10.7	64	68	46.5	54.6	80.1	84.2
00:10.9	64	68	38.7	47.9	73.2	77.9
00:10.0	64	68	38.7	52.8	73.5	82.3

TABLE 1 Normal physical testbed data sample

Within Table 1, C1 to C6 signify the system modules used for data collection. As such, C1 and C2 signify the water level in speed 1 and 2 respectively; C3 and C4 indicate the water levelsin tank 2 and 3; C4 signifies the flow from test bed 2; C5 represents the speed of testbed 1 and C6 indicates the speed of testbed 2.

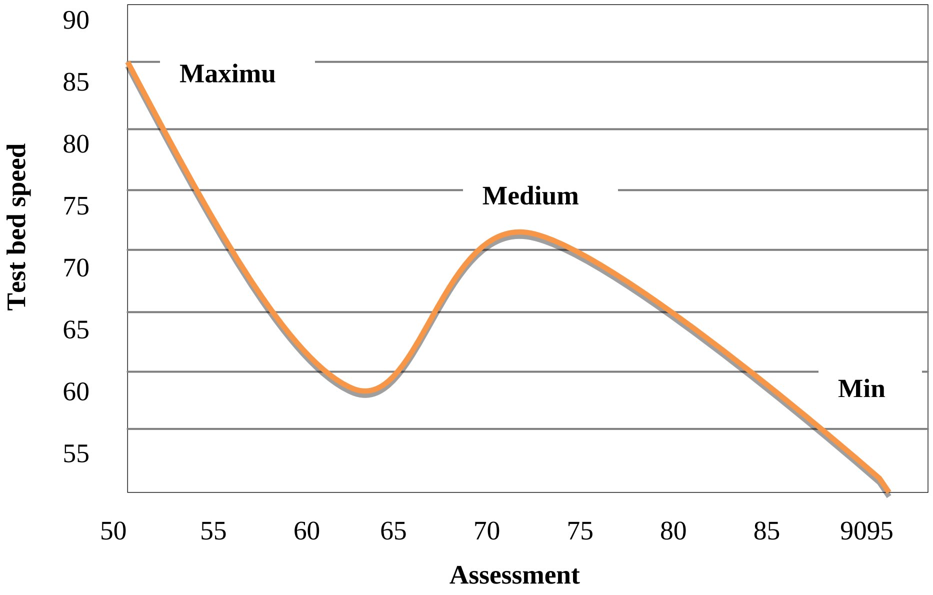
Assessment	C1	C2	C3	C4	C5	C6
Unique	22.00	3.00	54.00	51.00	50.00	52.00
Min	64.00	68.00	33.82	43.86	67.65	73.74
Max	65.22	68.45	36.35	45.65	70.65	75.85
Median	63.85	68.352	34.25	44.35	69.58	74.58
Mean	64.27	69.35	34.27	45.58	70.45	75.69
Std	0.258	0.053	0.578	0.575	0.697	0.584

TABLE 2 Distribution values for normal data

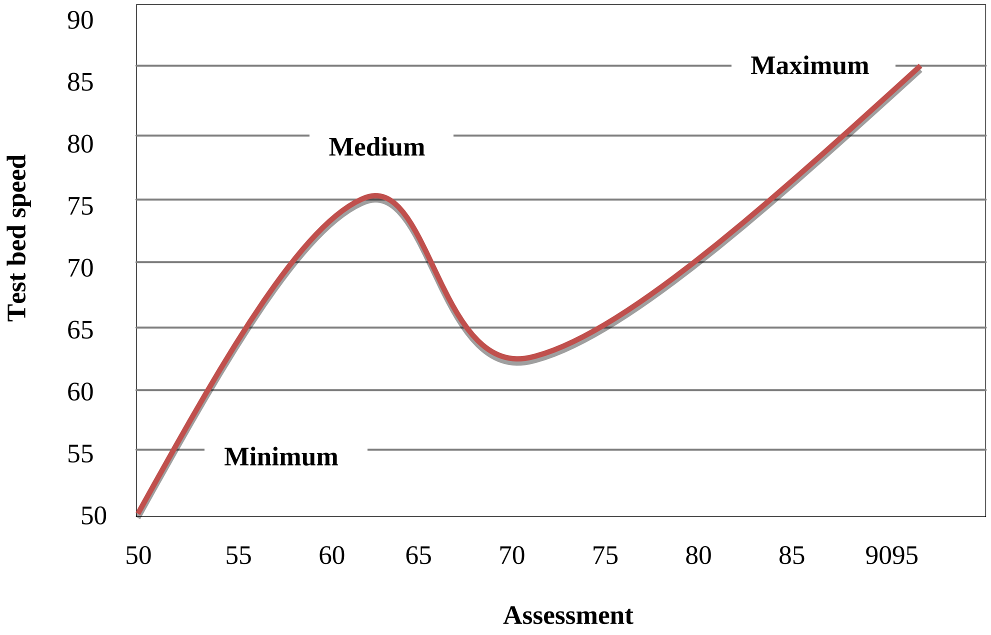
While no new standards are willinglyobtainable, the RTU sustains to domain the previous testbed speed. As before, Table 3 indicates the distribution of values for each of the apparatuses over the one hour simulation through the situation. The unique value, max, min, median, mean and normaldeviation of the values is again established.

Assessment	C1	C2	C3	C4	C5	C6
Unique	24.00	6.00	51.00	50.00	57.00	58.00
Min	64.00	68.74	33.87	43.47	55.87	55.78
Max	65.45	69.58	37.87	46.48	84.04	90.74
Median	64.75	68.11	35.27	45.73	71.06	73.76
Mean	64.55	68.84	35.64	45.48	70.07	73.82
Std	0.25	0.014	0.578	0.624	5.721	6.216

TABLE 3Distribution values for attack data



GRAPH 1 Scatter Plot for normal and abnormal operation of test bed



GRAPH 2 test bed speed variations of maximum and minimum

While under attack, the testbed continues to function, facility is disturbed and the output is noticeable in the dataset constructed. For example, the min and max standards from C5 are significantlydissimilar.

This change is data is identifiable in a visual assessment of the pump speeds. A two feature scatter plot of the normal and irregular operation of the two testbed pumps. Pump speed 2 is presented along the y-axis with pump speed 1 detailed on the x-axis.

VIII. CONCLUSION

In this paper we have obtainable a testbed for simulation ofcyber-attacks. The testbed delivers a generic way to pretendand study a wide range of cyber-attacks, and enables an establishingof isolated virtual environments that researches can use to pursue controlled analysis of attacks. The paper proves the feasibility of the solution, especially it answers the three questions raised in the introduction real-world environment, flexibility vs. usability and authentic attack modeling.Using virtualization and clouds we achieved to deliverasetting where it is conceivable to arrange any common network arrangement and therefore we are able to achievedesires of numeroustypes of security scenarios. The testbed clearly monitors all modules and delivers its users with thorough information about doingsachieved inside the environments as demanded by them.

The user can use the Cybernetic Verifying Ground to set up isolated surroundingsactualrapidly without the requirement to know particulars about how to arrange networking or organize auxiliary services like monitoring infrastructure. Instead, users can essence solely on the work with the recognized environment. Being created on a mutual cloud solution, the framework to create the environments can be organized on anextensive range of modern clouds. The underlying technology also deliversadequate scalability. We also presentedanidea of security situations, which delivers a common way to designate an attack and allowsrunning its simulation implemented in a controlled way. Finally, the feasibility of the solution was established by a simulation and monitoring of a specific DDoS attack.

REFERENCE

[1] "Prolexic Quarterly Global DDoS Attack Report Q2 2013," ProlexicTechnologies. Accessed on 6 Sep 2013. [Online]. Available: http:// www.prolexic.com/knowledge-center-ddos-attack-report-2013-q2.html

[2] "Worldwide Infrastructure Security Report," Arbor Networks. Volume VII, 2012. Accessed on 6 Sep 2013. [Online]. Available: http: //pages.arbornetworks.com/rs/arbor/images/WISR2012 EN.pdf.

[3] K.pavya "Secure Multicast Transmission Scheme for Overlay Networks" Volume 12 Number 1 – Sep 2014.

[4] L. Chen, "Construction of the New Generation Network Security Testbed-Testbed@ TWISC: Integration and Implementation on Software Aspect," 2008, Institute of Computer & Communication, National Cheng Kung University, Tainan, Taiwan.

[5] B. White, J. Lepreau, L. Stoller, R. Ricci, S. Guruprasad, M. Newbold, M. Hibler, C. Barb, and A. Joglekar, "An Integrated Experimental Environment for Distributed Systems and Networks," Boston, MA, Dec. 2002, pp. 255–270.

[6] A. Arnes, P. Haas, G. Vigna, and R. A. Kemmerer, "Using a virtual security testbed for digital forensic reconstruction." Journal in Computer Virology, vol. 2, no. 4, pp. 275–289, 2007.

[7] NikithaBhasu1 , Raju. K. Gopal, Enhanced Security Solution to Prevent Online Password Guessing Attacks, volume1 issue6 August 2014.

[8] K. Krishna, W. Sun, P. Rana, T. Li, and R. Sekar, "V-Net Lab: a cost effective platform to support course projects in computer security," in Proceedings of 9th Colloquium for Information Systems Security Education, 2005.

[9] D. Duchamp and G. De Angelis, "A hypervisor based security testbed," in Proceedings of the DETER Community Workshop on Cyber Security Experimentation and Test on DETER Community Workshop on Cyber Security Experimentation and Test 2007, ser. DETER. Berkeley, CA, USA: USENIX Association, 2007.

[10] Open vSwitch, "Open vSwitch: An Open Virtual Switch," accessed on 30 August 2013. [Online]. Available: http://openvswitch.org/

[11] M.Priyanka ,G.PremaPriya, Dectecting the Data Injection Attack Through Multiple Relay Network using the Security Code, volume 2 issue 4 April 2015.

[12] P. Velan, T. Jirsik, and P. Cˇ eleda, "Design and Evaluation of HTTP Protocol Parsers for IPFIX Measurement," in Advances in Communication Networking, Lecture Notes in Computer Science, Vol. 8115, T. Bauschert, Ed. Heidelberg: Springer Berlin / Heidelberg, 2013, pp. 136–147.

[13] P. Cˇ eleda, P. Velan, M. Rabek, R. Hofstede, and A. Pras, "Large-Scale Geolocation for NetFlow," in IFIP/IEEE International Symposium on Integrated Network Management (IM 2013). Ghent, Belgium: IEEE Xplore Digital Library, 2013, pp. 1015–1020.

[14] Sujee.R1 , Kannammal.K.E, Routing protocols based on network structure in wireless sensor networks -A survey, volume 2 issue 4 April 2015.

[15] "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information," RFC 5101 (Proposed Standard), Internet Engineering Task Force, 2008.

[16] S.Kokila1 , T. Princess Raichel, Software as a Service, a Detailed Study on Challenges and Security Threats, – volume 2 issue 12 December 2015.

[17] L. Hellemons, L. Hendriks, R. Hofstede, A. Sperotto, R. Sadre, and A. Pras, "SSHCure: A Flow-Based SSH Intrusion Detection System," in Dependable Networks and Services, ser. Lecture Notes in Computer Science, R. Sadre, J. Novotny´, P. Cˇ eleda, M. Waldburger, and B. Stiller,Eds. Springer Berlin Heidelberg, 2012, vol. 7279, pp. 86–97.

[18] R. Moreno-Vozmediano, R. S. Montero, and I. M. Llorente, "IaaS Cloud Architecture: From Virtualized Datacenters to Federated Cloud Infrastructures," Computer, vol. 45, no. 12, pp. 65–72, 2012.

[19] S. Shekyan, "slowhttptest - Application Layer DoS attack simulator," accessed on 8 August 2013. [Online]. Available: http://code.google.com/p/slowhttptest/

[20] A. Abdulmohsen., Z. Tari., I. Khalil., and A. Fahad., SCADAVT-A framework for SCADA security testbed based on virtualization technology, Proceedings of the 38th IEEE Conference on Local Computer Networks (LCN), pp639-646, 2013

[21] L. Topham, K. Kifayat, Y. A. Younis, Q. Shi and B. Askwith, Cyber Security Teaching and Learning Laboratories: A Survey, Information & Security: An International Journal, vol. 35, 2016.

[22] D. Lewis, The pedagogical benefits and pitfalls of virtual tools for teaching and learning laboratory practices in the Biological Sciences, HE Academy, 2014

[23] L. H. de Melo Leite, L. de Errico, and W. do Couto Boaventura, Criteria for the selection of communication

infrastructure applied to power distribution automation, Proceedings of the IEEE PES Conference on Innovative Smart Grid Technologies (ISGT Latin America), pp. 1–8, 2013.

[24] O. Gerstel, AControl Architectures for Multi-Layer Networking: Distributed, centralized, or something in between? Optical Fiber Communications Conference and Exhibition (OFC), pp 1-16, 2015.

[25] C. Esposito, D. Cotroneo, R. Barbosa, and N. Silva, Qualification and Selection of Off-the-Shelf Components for Safety Critical Systems: A Systematic Approach, Proceedings of the Fifth Latin-American Symposium on Dependable Computing Workshops, pp. 52–57, 2011.

[26] V. Urias, B. Van Leeuwen, and B. Richardson, Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed, Proceedings of the IEEE Military Communications Conference, (MILCOM), pp. 1–8, 2012.

[27] Z. Liu., D. Li., L. Yun., and S. Xu., An assessment method for reliability of distributed control system, Proceedings of the IEEE International Conference on Information and Automation, pp. 1300-1304, 2015.

[28] H. Fayyaz Abbasi., N. Iqbal., M. Rehan, Distributed Robust Adaptive Observer-Based Controller for Distributed Control Systems with Lipschitz Nonlinearities and Time Delays, Proceedings of the 13th International Conference on Frontiers of Information Technology (FIT), pp. 185–192, 2015.

[29] J. Adrian Ruiz Carmona., J. César Muñoz Benítez and J. L. García-Gervacio., SCADA system design: A proposal for optimizing a production line, Proceedings of the International Conference on Electronics, Communications and Computers (CONIELECOMP), pp. 192-197, 2016.

[30] R. Gao and C. Hwa Chang, A scalable and flexible communication protocol in a heterogeneous network, Proceedings of the 13th International Conference on Computer and Information Science (ICIS), pp 49-52, 2014.

[31] Y. Zhang., L. Wang., Y. Xiang and C. Ten, Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation. IEEE Transactions on Power Systems, Vol:PP, No 99, pp 1-16, 2016.

[32] Q. Yan., F. R. Yu., Q. Gong., and J. Li., Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges, IEEE Communications Surveys & Tutorials, Vol. 18 No. 1, pp. 602–622, 2015.

[33] A. Sahi Khader., and D. Lai., Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol, Proceedings of the 22nd International Conference on Telecommunications (ICT), pp. 204–208, 2015.

[34] R. Divya., and S. Muthukumarasamy., An impervious QR-based visual authentication protocols to prevent black-bag cryptanalysis, Proceedings of 9th IEEE International Conference on Intelligent Systems and Control (ISCO), pp. 1–6, 2015.

[35] T. Benzel, R. Braden, D. Kim and C. Neuman, Experience with DETER: a testbed for security research, in Proceedings of the 2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, 2014.

[36] Z. L. H. Wei, G. Yajuan, and C. Hao, Research on information security testing technology for smart Substations, in Proceedings of the International Conference on Power System Technology (POWERCON), pp. 2492–2497, 2014.

[37] M. Ficco, G. Avolio, L. Battaglia, and V. Manetti, Hybrid Simulation of Distributed Large-Scale Critical Infrastructures, Intell. Netw. Collab. Syst., pp. 616–621, 2014.