International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

An Error Reducing Structure for Restricting Jammers in Remote Networks

Gotthala Kodhanda Babu, B. Rama Subba Reddy

Department of Computer Science and Engineering, S.V.College of Engineering, Tirupati, India

ABSTRACT

We aim to design a framework which will localize one or different jammers with a high accuracy. Most of the absolute jammer-localization schemes advance aberrant abstracts (e.g., audition ranges) afflicted by jam attacks, that makes it troublesome to localize jammers accurately. Instead, we tend to accomplishment an absolute altitude the backbone of jam signals (JSS). Estimating JSS is arduous as jam signals could also be anchored in additional signals. we tend to analyze many heuristics get algorithms for neighboring the well-rounded best resolution, and our simulation after-effects look that our error-minimizing-based framework achieves larger accomplishment than absolutely the schemes. Additionally, our error-minimizing framework will advance aberrant abstracts to access a much bigger space admiration compared with preceding work. we tend to show a multi-phase broadcast vulnerability detection, activity, and antibody different equipment alleged NICE, that is inherent in advance blueprint based mostly analytic models and reconfigurable basic network-based countermeasures. The projected framework leverages Open Flow arrangement programming arthropod genus to body an advisor and dominance even over broadcast programmable basic switches in adjustment to significantly advance apprehension and abate advance consequences. The arrangement and aegis evaluations attest the potency and capability of the projected resolution.

Keywords : Network Security, Cloud Computing, jam attacks.

I. INTRODUCTION

To affected these challenges and access the localization accuracy, we tend to systemize the transmitter localization botheration as a nonlinear sweetening botheration an ascertain an appraisal metric as its cold operate. the number of appraisal metric reflects however contiguous the calculable jammers' locations area unit to their correct locations, and thus, we are able to explore for the simplest estimations that abbreviate the appraisal metric. as a result of acceptable rise obtain strategies might assemble to a finite minimum and should not essentially crop the all-around minimum, we tend to settle for many algorithms that absorb tutorial processes to access the all-around optimum. Especially, we tend to suggest 3 formulas: an organic phenomenon algorithm (GA), an ambiguous arrangement obtains (GPS) formula and an imitative tempering (SA) formula. Our all-inclusive simulation after-effects look that our localization error-minimizing framework not alone will advance the admiration accurateness of localizing one transmitter compared to preceding arrange , however as well will appraisal the positions of varied jammers at the same time, authoritative it abnormally advantageous for anecdotic accidental radio arrest no inheritable by various wireless accessories or many awful and cooperative jammers. We tend to abbreviate our capital contributions as follows: Estimating JSS is arduous as a result of the electronic countermeasures signals area unit anchored within the approved signals. To the simplest of our information, our arrange is that the aboriginal that sweetsop utilizes the JSS to localize jammers. Our after-effects application absolute abstracts (e.g., JSS) show cogent advance compared with those application aberrant abstracts (e.g., audition ranges).We exploited aisle accident a shadowing phenomenon in radio advancement and authentic an appraisal metric which will quantify the accurateness of the calculable locations. Leverage such an appraisal metric, we tend to develop the transmitter localization botheration as Associate in Nursing error-minimizing framework and suggested many heuristic analytic algorithms for the award the simplest answer. Our error-minimizing-based algorithms will localize various jammers at the same time, though their electronic countermeasures areas overlap. NICE significantly advances the accepted arrangement IDS/IPS solutions by using programmable basic networking access that permits the arrangement to assemble an activating reconfigurable IDS system. By application software package shift techniques [5], NICE constructs a mirroring-based traffic capturing framework to abbreviate the arrest on users' traffic compared to acceptable bump-in-the-wire (i.e., proxy-based) IDS/IPS. The programmable basic networking scientific discipline of NICE allows the billow to authorize analysis and quarantine modes for apprehensive VMs per their accepted vulnerability accompaniment within the accepted SAG. Supported the combination behavior of VMs within the SAG, NICE will judge custom-made actions, for model DPI or traffic filtering, on the apprehensive VMs. The application this approach, NICE doesn't charge to dam traffic flows of an apprehensive VM in its aboriginal advance stage. The contributions of NICE area unit bestowed as follows: we tend to devise NICE, a replacement multi-phase broadcast arrangement advance apprehension and blockage framework during a basic networking ambiance that captures and inspects apprehensive billow traffic when interrupting users' applications and billow services. NICE incorporates a software package shift band-aid to apprehension and audit apprehensive VMs for any analysis and protection. Through programmable arrangement approaches, NICE will advance the advance apprehension anticipation and advance the resiliency to VM corruption advance when sensational absolute accustomed billow services. NICE employs an atypical advance blueprint access for advance apprehension and blockage by correlating advance behavior and similarly suggests in a position countermeasures. NICE optimizes the accomplishing of billow servers to abbreviate ability consumption. Our abstraction shows that NICE consumes at a lower place procedure aerial compared to proxy-based arrangement advance apprehension solutions.

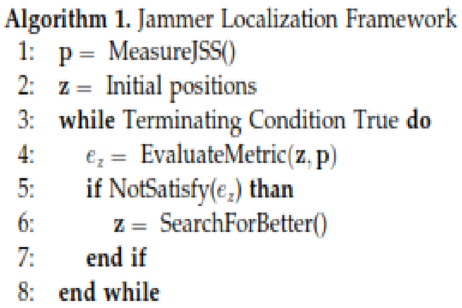
II. Localization Formulation

Essentially, our jammer localization access works as follows: Given a set of JSS, for every estimated location, we are able to accommodate a quantitative appraisal acknowledgment advertence the ambit amid the estimated locations of jammers and their accurate locations. For example, a baby amount of appraisal acknowledgment indicates that estimated locations are abutting to the accurate ones, and carnality versa. Although clumsy to acclimatize the admiration directly, it is possible, from a few candidate locations, to baddest the ones that are abutting to the accurate locations with top probability, authoritative analytic for the best appraisal feasible. Leveraging this idea, our jammer localization access comprises two steps: 1) JSS collection. Each abuttals bulge locally obtains JSS. 2) Best admiration searching. Based on the calm JSS, a appointed bulge will access a asperous admiration of the jammers' positions. Then, it refines the admiration by analytic for positions that abbreviate the appraisal acknowledgment metric. The data are declared in Algorithm 1. The search-based jammer localization approaches accept a few arduous subtasks:

1. Evaluate Metric () has to define an appropriate metric to quantify the accuracy of estimated jammers' locations.

2. MeasureJSS () has to obtain JSS even if it may be embedded in regular transmission.

3. SearchForBetter () has to efficiently search for the best estimation.



Algorithm 1. Jammer Localization Framework

```
p = MeasureJSS()
z = Initial positions
while Terminating Condition True do
    $e_z$ = EvaluateMetric(z, p)
    if NotSatisfy($e_z$) than
        z = SearchForBetter()
    end if
end while
```

wireless communication, the RSS attenuates with the access of ambit amid the sender and receiver due to aisle accident and shadowing, as able-bodied as effective and annihilative additions of multipath arresting apparatus, Aisle accident can be advised as the boilerplate attenuation, while shadowing is the accidental abrasion acquired by obstacles through absorption, reflections, scattering, and diffraction illustrates contours of an RSS and the accord amid shadowing and aisle loss. The abrasion acquired by shadowing at any individual location, d meters from the transmitter, may display variation; the boilerplate abrasion and boilerplate arresting backbone on the amphitheater centered at the transmitter are almost This ascertainment serves as the axiological base of our error-minimizing framework. To allegorize our jammer localization approach, we use the broadly acclimated log-normal shadowing archetypal which captures the capital of both aisle accident and shadowing. Let be the RSS accountable to aisle accident abrasion only, and let the ability of a transmitted signal be P_t. The received signal power in dBm at a distance of d can be modeled as the sum of P_f and a variance caused by shadowing and other random attenuation,

$$P_r = P_f + X_\sigma$$

$$P_f = P_t + K - 10\eta \log_{10}(d),$$

Where could be a Gaussian zero-mean variable with variance K could be a unit less constant that depends on the antenna characteristics and also the average channel attenuation and is that the path loss exponent (PLE). During a free area, are 2, and is often zero.

2.1 Problem Formulation

Given the definition of the feedback metric (e_z), we generalize jammer localization problem as one optimization problem:

Problem 1.

$$\underset{\mathbf{z}}{\text{minimize}} \quad e_z(\mathbf{z}, \mathbf{p})$$
$$\text{subject to} \quad \mathbf{p} = \{P_{r_1}, \ldots, P_{r_m}\};$$

where zar the unknown variable matrix of the jammer(s), as an example, z is outlined in (6), and are the JSS measured at the boundary nodes f1; ...; mg. As we are going to show the calculable location(s) of the jammer(s) at that is decreased matches verity location(s) of jammer(s) with little estimation error(s). RSS is one in all the plenty of broadly speaking acclimated abstracts in localization. as an example, a wireless local {area network|WLAN|wireless fidelity|WiFi|local area network|LAN} accent will appraisal its plenty of acceptable area by analogous the abstinent RSS agent of a collection of WiFi APs with prêt rained RF procedure maps or with foreseen RSS maps complete supported RF advancement models but, acceptive stunning backbone of jammers (JSS) may be an arduous assignment primarily as a result of electronic jamming signals are anchored in signals transmitted by approved wireless devices. The bearings are sophisticated as a result of different wireless accessories are acceptable to forward packets at the same time, as electronic jamming disturbs the approved operation of carrier analysis different access. For the blow of this paper, we have a tendency to accredit the approved nodes' specific packet transmissions that might not be decoded as a collision. whereas it's troublesome, if anytime potential, to abstract stunning equipment contributed by jammers or blow sources, we have a tendency to ascertain that it's doable to amass the JSS supported alternate close babble mensuration. Within the after sections, we have a tendency to aboriginal gift basics of close babble attentively to electronic jamming signals and once more acquaint our arrangement to appraisal the JSS. Finally, we have a tendency to validate our admiration schemes via real-world experiments. An aboveboard access of ciphering the ANF may be sampling close babble if the wireless radio is abandoned (i.e., neither accretive nor transmission packets). Such an adjustment might not set up altogether arrangement situations, as a result of it's going to aftereffect in associate degree abstract ANF. as an example, during an awful chockful network, the blow is appropriate to occur, and also the collided signals is also suggested as allotment of the ANF at the receiver, consistent in associate degree aggrandized ANF. This can be completely the bearings we have a tendency to want to avoid.

III. System Design Overview

It shows the NICE framework aural one billow server cluster. Major apparatus in this framework are broadcast and light-weighted NICE-A on anniversary concrete billow server, a arrangement controller, a VM profiling server, and an advance analyzer. The closing three apparatus are amid in a centralized ascendancy centermost affiliated to software switches on anniversary billow server (i.e., basic switches congenital on one or assorted Linux software bridges). NICEA is a software abettor implemented in anniversary billow server affiliated to the ascendancy centermost through a committed and abandoned defended channel, which is afar from the accustomed abstracts packets application Open Flow tunneling or VLAN approaches. The arrangement ambassador is amenable for deploying advance countermeasures based on decisions fabricated by the advance analyzer. In the afterward description, our terminologies are based on the XEN virtualization technology. NICE-A is a arrangement advance apprehension engine that can be installed in either Dom0 or DomU of a XEN billow server to abduction and filter awful traffic. Advance apprehension alerts are beatific to ascendancy centermost if apprehensive or anomalous traffic is detected. After accepting an alert, advance analyzer evaluates the severity of the active based on the advance graph, decides what antitoxin strategies to take, and again initiates it through the arrangement controller. An advance blueprint is accustomed according to the vulnerability advice acquired from both offline and absolute time vulnerability scans. Offline scanning can be done by active assimilation tests and online realtime vulnerability scanning can be triggered by the arrangement ambassador (e.g., if new ports are opened and identified by OpenFlow switches) or if new alerts are generated by the NICE-A. Once new vulnerabilities are apparent or countermeasures are deployed, the advance blueprint will be reconstructed. Countermeasures are accomplished by the advance analyzer based on the appraisal after-effects from the cost-benefit assay of the capability of countermeasures. Then, the arrangement ambassador initiates antitoxin accomplishments by reconfiguring basic or concrete OpenFlow switches.

3.1 Vm Profiling

Virtual machines within the billow are profiled to induce absolute recommendation concerning their state, social service running, accessible ports, etc. One higher than the agency that counts seem a VM profile is its property with value-added VMs. Any VM that's related to value-added quantity of machines is value-added acute than the one related to below VMs as a result of the aftereffect of accommodation of an awful related to VM will cause value-added harm. additionally acceptable is that the ability of social service active on a VM thus on verify the reality of alerts relating that VM. Associate degree agonist will use anchorage scanning affairs to accomplish an acute assay of the arrangement to attending for accessible ports on any VM. Thus recommendation concerning any accessible ports on a VM and therefore the history of opened ports play a significant role in free however accessible the VM is. of these factors accumulated can anatomy the VM profile. VM profiles square measure maintained in a very informative and accommodates absolute recommendation concerning vulnerabilities, active and traffic. The abstracts come from:

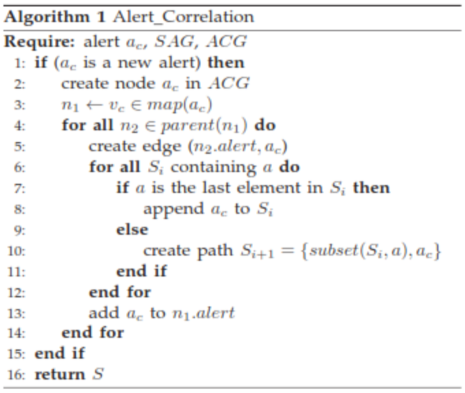
• Advance blueprint generator: whereas breeding the advanced graph, each detected vulnerability is value-added to its agnate VM access within the information.

• NICE-A: the activities involving the VM are going to be recorded within the VM profile information.

• Arrangement controller: the traffic patterns involving the VM square measure supported five tuples (source mack address, destination mack address, antecedent information science address, destination information science address, protocol). {we can|we will|we square measure able to} settle for traffic arrangement space packets arise from an individual information science and are delivered to different destination information science addresses, and vice-versa.

3.2 Network Controller

The arrangement ambassador may be a key basic to abutment the programmable networking adequacy to apprehend the essential arrangement reconfiguration feeling supported OpenFlow agreement [20]. In NICE, aural day billow server there's a code switch, for instance, Open vSwitch (OVS) [5], that is acclimated because the bend about-face for VMs to handle traffic in &amp; out from VMs. the recommendation amid billow servers (i.e., concrete servers) is handled by concrete OpenFlow-capable About-face (OFS). In NICE, we tend to chip the control functions for each OVS associate degreed OFS into the arrangement ambassador that permits the billow arrangement to line security/filtering rules in a chip and absolute manner. The arrangement ambassador is amenable to accession arrangement recommendation of accepted OpenFlow arrangement and provides arrangement instrument to assemble advanced graphs. Through the billow, centralized analysis modules that use DNS, DHCP, LLDP and flow-initiations [27], arrangement ambassador is ready to establish the arrangement property recommendation from OVS and OFS. (this recommendation | this recommendation) includes accepted abstracts methods on day about-face and teeming flow advice related to these methods, like TCP/IP and mack header. The arrangement flow and devising modification recommendation are going to be mechanically beatific to the ambassador and once more delivered to advance instrument to reconstruct advance graphs. Another necessary action of the arrangement ambassador is to encourage the advance instrument module. per the OpenFlow agreement [20], if the ambassador receives the first packet of a flow, it holds the packet and checks the flow table for acknowledging traffic policies. In NICE, the arrangement control aswell consults with the advance instrument for the flow admission control by atmosphere up the filtering rules on the agnate OVS and OFS. Once a traffic flow is admitted, the afterwards packets of the flow don't seem to be handled by the arrangement controller, however monitored by the NICE A.



```
Algorithm 1 Alert_Correlation
Require: alert $a_c$, $SAG$, $ACG$
if ($a_c$ is a new alert) then
    create node $a_c$ in $ACG$
    $n_1 \leftarrow v_c \in map(a_c)$
    for all $n_2 \in parent(n_1)$ do
        create edge $(n_2.alert, a_c)$
        for all $S_i$ containing $a$ do
            if $a$ is the last element in $S_i$ then
                append $a_c$ to $S_i$
            else
                create path $S_{i+1} = \{subset(S_i, a), a_c\}$
            end if
        end for
        add $a_c$ to $n_1.alert$
    end for
end if
return $S$
```

Network ambassador is as well amenable to applying the antibody from the advance analyzer. Supported

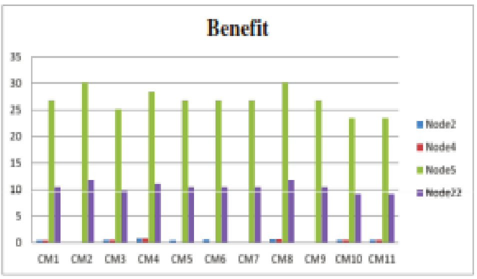
VM Security Index associate degreed severity of an alert, countermeasures area unit known as by NICE and accomplished by the arrangement controller. If an astringent active is triggered and identifies some accepted attacks, or a VM is detected as a zombie, the arrangement ambassador can block the VM immediately active with average blackmail akin is triggered by an apprehensive compromised VM. Antibody in such case is to place the apprehensive VM with exploited accompaniment into apprehension approach and alter all its flows to NICEA Deep Packet Analysis (DPI) mode. A life with accent blackmail akin is often generated attributable to the group action of an accessible VM. For this case, an adjustment to ambush the VM's accustomed traffic, apprehensive traffic to/from the VM are going to be placed into analysis mode, during which accomplishments like akin its flow information measure and alteration arrangement configurations are going to be taken to force the advance analysis behavior to angle out.

IV. Performance Evaluation

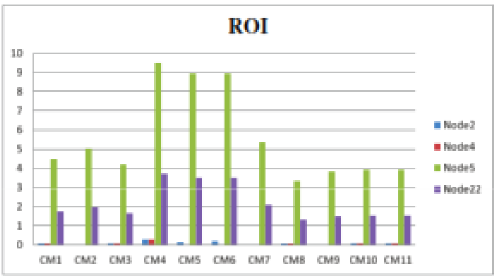
In this section, we tend to gift the performance analysis of NICE. Our analysis is conducted in 2 directions: the protection performance, and also the system computing and network reconfiguration overhead attributable to introduced security mechanism.

4.1 Security Performance Analysis

The advance blueprint is often generated by utilizing arrangement mapmaking and also the vulnerability data, and it's apparent in Figure. Because the advance progresses, the arrangement generates various alerts that may be concomitant to the nodes within the advance graph. Making associate degree advance blueprint needs the ability of arrangement property, active welfare work and their vulnerability data. this recommendation is provided to the advance blueprint designer because of the input. Whenever a brand new vulnerability is obvious or there area unit changes within the arrangement property and welfare work active through them, the tailored recommendation is provided to advance blueprint designer and the recent advance blueprint is customized to a brand new one. SAG provides a recommendation concerning the accessible ways that associate degree antagonist will follow. ACG serves the aim of confirming attackers' behavior and helps in free apocryphal absolute and apocryphal negative. ACG will as well be accessible in admiration attackers' next steps.

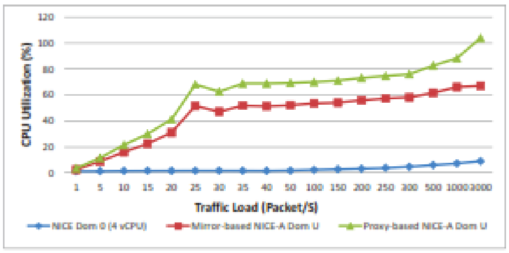


Benefit evaluation chart.



ROI evaluation chart.

To demonstrate the possibleness of our answer, indirect studies were conducted on many virtualization approaches. we tend to evaluated NICE supported Dom0 and DomU implementations with mirroring-based and proxy-based advance apprehension agents (i.e., NICE-A). In mirror-based IDS state of affairs, we tend to accustomed 2 basic networks in day billow server: accustomed arrangement and ecology network. NICE-A is related to the ecology network. Traffic on the accustomed arrangement is reflected the ecology arrangement application Switched Port instrument (SPAN) approaches. Within the proxy-based IDS answer, NICE-A interfaces 2 VMs and also the traffic goes through NICE-A. in addition, we tend to settle for deployed the NICE-A in Dom0 and it removes the traffic duplication action in impersonation and proxy-based solutions. we tend to acclimated packet designer to actor absolute traffic within the Billow system. The traffic load, in the anatomy of packet causation speed, will increase from one to 3000 packets per second. The action at Dom0 consumes to a lower place central processor and also the IPS approach consumers the simplest central processor resources. It will be empiric that if the packet quantity recess to 3000 packets per second; the central processor appliance of IPS at DomU recess its limitation, whereas the IDS approach at DomU alone occupies regarding sixty-eight.



CPU utilization of NICE-A.

From this analysis we tend to accepted to prove the projected resolution, fitly accomplishing our ambition”establish an activating impressive equipment primarily based software package denned networking access that involves polyphase advance detections”. The abstracts prove that for a small-scale billow system, our access works well. The accomplishment appraisal includes 2 elements. First, aegis accomplishment analysis. It shows that our access achieves the design aegis goals: to anticipate accessible VMs from obtaining compromised and to try to thus into a lower place advancing and quantity ready manner. Second, computer hardware and thru place accomplishment analysis. It shows the prohibited of application the projected band-aid in agreement of networking throughputs supported software package switches and computer hardware acceptance if active apprehension engines on Dom zero and DomU. The accomplishment after-effects accommodate the US a criterion for the accustomed accouterments paperwork and show however swarming traffic are often handled by application an individual apprehension domain. To standardization up to a abstracts centermost akin advance apprehension system, a decentralized access have to be compelled to be devised, that is appointed in our approaching analysis.

V. Conclusion

In this paper, we tend to bestowed NICE, that is projected to establish and abate cooperative attacks within the billow basic networking setting. NICE utilizes the advance blueprint prototypic to conduct advance apprehension and prediction. The projected band-aid investigates the way to use the programmability of software package switches primarily based solutions to advance the apprehension accurateness and defeat victim corruption phases of cooperative attacks. The arrangement accomplishment appraisal demonstrates the attainability of NICE and shows that the projected band-aid will emphatically abate the accident of the billow arrangement from obtaining exploited and abused by centralized and alien attackers. NICE alone investigates the arrangement IDS access to adverse crank wildcat attacks. In adjustment to advance the apprehension accuracy, host-based IDS solutions area unit clean to be inborn and to sunshade the accomplished spectrum of IDS within the billow system. this could be suggested by the approaching work. to boot, as adumbrated within the paper, we are going to investigate the measurability of the projected NICE band-aid work the decentralized arrangement condition and advance assay prototypic supported the accepted study.

VI. REFERENCES

[1]. Coud Sercurity Alliance, "Top threats to cloud computing v1.0," https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, March 2010.

[2]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," ACM Commun., vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3]. B. Joshi, A. Vijayan, and B. Joshi, "Securing cloud computing environment against DDoS attacks," IEEE Int'l Conf. Computer Communication and Informatics (ICCCI '12), Jan. 2012.

[4]. 4H. Takabi, J. B. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security & Privacy, vol. 8, no. 6, pp. 24-31, Dec. 2010.

[5]. "Open vSwitch project," http://openvswitch.org, May 2012.

[6]. Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, "Detecting spam zombies by monitoring outgoing messages," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198-210, Apr. 2012.

[7]. G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "Bot Hunter: detecting malware infection through IDS-driven dialog correlation," Proc. of 16th USENIX Security Symp. (SS '07), pp. 12:1-12:16, Aug. 2007.

[8]. G. Gu, J. Zhang, and W. Lee, "BotSniffer: detecting botnet command and control channels in network traffic," Proc. of 15th Ann. Network and Distributed Sytem Security Symp. (NDSS '08), Feb. 2008.

[9]. O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," Proc. IEEE Symp. on Security and Privacy, 2002, pp. 273-284.

[10]. "NuSMV: A new symbolic model checker," http://afrodite.itc.it: 1024/ nusmv. Aug. 2012.

[11]. S. H. Ahmadinejad, S. Jalili, and M. Abadi, "A hybrid model for correlating alerts of known and unknown attack scenarios and updating attack graphs," Computer Networks, vol. 55, no. 9, pp. 2221-2240, Jun. 2011.

[12]. X. Ou, S. Govindavajhala, and A. W. Appel, "MulVAL: a logic based network security analyzer," Proc. of 14th USENIX Security Symp., pp. 113-128. 2005.

[13]. R. Sadoddin and A. Ghorbani, "Alert correlation survey: framework and techniques," Proc. ACM Int'l Conf. on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services (PST '06), pp. 37:1-37:10. 2006.

[14]. L. Wang, A. Liu, and S. Jajodia, "Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts," Computer Communications, vol. 29, no. 15, pp. 2917-2933, Sep. 2006.

[15]. S. Roschke, F. Cheng, and C. Meinel, "A new alert correlation algorithm based on attack graph," Computational Intelligence in Security for Information Systems, LNCS, vol. 6694, pp. 58-67. Springer, 2011.

[16]. A. Roy, D. S. Kim, and K. Trivedi, "Scalable optimal countermeasure selection using implicit enumeration on attack countermeasure trees," Proc. IEEE Int'l Conf. on Dependable Systems Networks (DSN '12), Jun. 2012.

[17]. N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic security risk management using bayesian attack graphs," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 1, pp. 61-74, Feb. 2012.

[18]. Open Networking Fundation, "Software-denned networking: The new norm for networks," ONF White Paper, Apr. 2012.

[19]. "Openflow."http://www.openflow.org/wp/learnmore/, 2012.

[20]. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peter- son, J. Rexford, S. Shenker, and J. Turner, “OpenFlow: enabling innovation in campus networks,” SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69-74, Mar. 2008.

[21]. E. Keller, J. Szefer, J. Rexford, and R. B. Lee, “NoHype: virtualized cloud infrastructure without the virtualization,” Proc. of the 37th ACM ann. int'l symp. on Computer architecture (ISCA '10), pp. 350-361. Jun. 2010.

[22]. X. Ou, W. F. Boyer, and M. A. McQueen, “A scalable approach to attack graph generation,” Proc. of the 13th ACM conf. on Computer and communications security (CCS '06), pp. 336-345. 2006.

[23]. Mitre Corporation, “Common vulnerabilities and exposures, CVE,” http://cve.mitre.org/. 2012.

[24]. P. Mell, K. Scarfone, and S. Romanosky, “Common vulnerability scoring system(CVSS),”http://www.first.org/cvss/cvss-guide.html, May 2010.

[25]. O. Database, “Open source vulnerability database (OVSDB),” http://osvdb.org/. 2012

[26]. NIST, “National vulnerability database, NVD,” http://nvd.nist. gov. 2012

[27]. N. Gude, T. Koponen, J. Pettit, B. Pfaff, M. Casado, N. McKeown, and S. Shenker, “NOX: towards an operating system for networks,” SIGCOMM Comput. Commun. Rev., vol. 38, no. 3, pp.105-110, Jul. 2008.

[28]. X. Ou and A. Singhal, Quantitative Security Risk Assessment of Enterprise Networks. Springer, Nov. 2011.

[29]. M. Frigault and L. Wang, “Measuring network security using bayesian Network-Based attack graphs,” Proc. IEEE 32nd ann. int'l conf. on Computer Software and Applications (COMPSAC '08), pp. 698-703. Aug. 2008.

[30]. K. Kwon, S. Ahn, and J. Chung, “Network security management using ARP spoofing,” Proc. Int'l Conf. on Computational Science and Its Applications (ICCSA '04), LNCS, vol. 3043, pp. 142-149, Springer, 2004.

[31]. “Metasploit,”http://www.metasploit.com. 2012.

[32]. “Armitage,”http://www.fastandeasyhacking.com. 2012.

[33]. M. Tupper and A. Zincir-Heywood, “VEA-bility security metric: A network security analysis tool,” Proc. IEEE Third Int'l Conf. on Availability, Reliability and Security (ARES '08), pp. 950-957, Mar. 2008.