2010 Ninth International Conference on Networks

An Approach for Automated Network-Wide Security Analysis

Miroslav Sveda, Ondrej Rysavy, Petr Matousek, Jaroslav Rab
Faculty of Information Technology
Brno University of Technology
Brno, Czech Republic
{sveda, rysavy, matousp, rabj}@fit.vutbr.cz

***Abstract*— This paper deals with an approach to security analysis of TCP/IP-based computer networks. The method developed stems from a formal model of network topology with changing link states, and deploys bounded model checking of network security properties supported by SAT-based decision procedure. Its implementation should consist of a set of tools that can provide automatic analysis of router configurations, network topologies, and states with respect to checked properties. While this project aims at supporting a real practice, it stems from the previous, more theoretical research designing the method in detail including its formal background.**

Keywords- TCP/IP networks; changing network topology; network security analysis; bounded model-checking; SAT-based decision procedure

I. INTRODUCTION

Network design is a complex task. Network specialists are expected to fulfill customers' requirements, while considering the limits of underlined technologies. The goal is to provide reliable network services as requested. Once the design is finished, the deployment phase is launched. It consists of installation and physical interconnection of the devices, setting up their configurations, and finally, network troubleshooting, in order to assure network functionality. Identification of potential problems as early as possible in the design phases is a serious argument for extra techniques and methodologies that verify and validate the results of the design process.

Suppose a small organization running a web server that provides information to their customers. The server is placed in the local network equipped with three routers. A path to the web server goes through router R2 that filters traffic as specified by filtering rules ACL1 (Access Control List) in its input, as in Figure 1.

There is a backup line between routers R1 and R3 with higher costs and lower priority. However, when the link between R2 and R3 goes down, the redirected traffic is not filtered any longer and the web server can be attacked from the outside network.

Another scenario can be the following. The priority line appears between routers R1 and R3. The line provides an access to the web site from the PC, as in Figure 1. When the link goes down, the traffic is automatically redirected by routing process through R2. However, the R2 entry interface is filtered by ACL1. The connection from PC to the web server is filtered out now, and the web services are no longer available. These two scenarios demonstrate a typical situation of a real-world network with dynamic behavior. While in this example all possible states of network behavior can be easily enumerated, a real network consisting of tens of routers poses a real challenge to prove that the network ensures designed security, safety and availability of network resources.

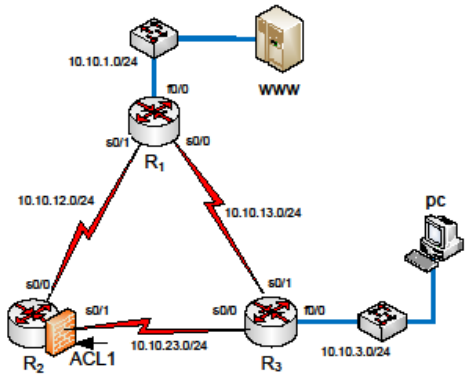

Figure 1. Example of a small network

Our approach focuses on the area of automatic analysis of a network that consists of L3 (Layer 3) devices (hosts, routers, firewalls, etc.) connected by links and, optionally, including firewall rules applied on device interfaces. Based on the network configuration and considering the dynamic behavior of the network, we ask (and answer) questions like "Is this network protected against P2P connections?", "What packets can be delivered to the given host?", or "Is this WWW service accessible under every configuration of the network?"

The current paper consists of six chapters with the following contents. After this introduction, the next chapter introduces briefly state of the art of the network security analysis domain from the viewpoint of support methods and tools. While the chapter III. discusses goals of the research, the chapter IV. presents research approach used. The last two chapters V. and VI. bring preliminary results including a

978-0-7695-3979-9/10 $26.00 © 2010 IEEE
DOI 10.1109/ICN.2010.69

demonstration example, and conclude with the project outcomes.

II. STATE OF THE ART

Research in the area of network security and vulnerability detection has been conducted since the beginning of the Internet. Many papers concentrate on detection of vulnerabilities of hosts and their protection against the network attack [14][17][13]. Most works follow the similar scheme: (i) The network is modeled as an entity that includes hosts, connections, user privileges, OS types, running services, and individual vulnerabilities of hosts. (ii) Host vulnerabilities are revealed by external automatic tools like Nessus, or by OVAL scanner [16]; then, detected vulnerabilities are expressed in the language of precondition and post-condition assertions, or rules. (iii) An important step is to determine the attacker goal – security violation (e.g., root access on the web server), which is often expressed by a predicate. (iv) After that, vulnerability analysis follows; it includes an application of derivation rules based on the initial assumptions, i.e., network configuration, in order to prove a predicate, i.e., security violation.

If the predicate is true, then the deduction path corresponds to the possible attack scenario. Despite the statement of authors in [13] that "this model lets automatically verify and proof network safety and vulnerability against the attack" (emphasis added), the method of logic deduction and proving requires good knowledge of logics and deductive systems, since the proof is constructive and it is made by human, not automatically.

In [16], an automatic deduction of network security executed in Prolog is introduced. The authors define reasoning rules that express semantics of different kinds of exploits. The rules are automatically extracted from OVAL scanner and CVE database [10].

Another approach is an automatic generation of network protection in the form of firewall rules as shown in [3]. The security policy is modeled using Model Definition Language as the first step. Then, the model of a network topology is translated into firewall-specific configurations. These configuration files are loaded into real devices (firewalls).

Ritchey and Amman [12] show how model checking can be used to analyze network vulnerabilities. They build a network security model of hosts, connections, an attacker and those exploits, which can be misused by the attacker. Security properties are described by temporal logics and verified using SMV model checker. However, their goal is different from ours. They verify if the hosts on the stable network are vulnerable to attacks. In our case, we concentrate on dynamically changing networks and reachability of their nodes.

From the approaches mentioned above, we take the following conclusions that are important for network security analysis: (1) a model of a network includes specification of hosts, their configurations, network topology, description of vulnerabilities; (2) a list of host vulnerabilities and network threats can be downloaded from open databases, or specified manually; (3) analysis can be manual or automatic, based on deductive systems or by model checking, respectively; (4) results of the analysis can either show specific vulnerabilities that require intervention of an administrator to generate a new safe configuration for network devices, or prove that the property is valid under every condition of the network.

III. GOALS OF THE RESEARCH

The goals of this research project consist of i) creation of a unifying model suitable for description of relevant aspects of real computer networks, including routing information, ACLs (access control lists), NAT (network address translation), dynamic routing policy and ii) delivering methods for automated verification of dependable properties (e.g., availability, security, survivability). The unique added value of the project is to specifically merge the research on formal methods with the research on network security to devise a new method for network security verification.

The recent work has focused on studying models and analysis techniques based on simulation and network monitoring. These models, nevertheless, do not take into consideration routing and packet filtering despite the fact that these aspects may significantly influence the traffic coverage observed in the network. The intensive research needs to be done in order to find new models that would include dynamic view on the network.

Similarly to hardware and software analysis based on simulation, the network simulation methods are useful mainly to observe properties given by normal behavior of the system. Simulation techniques are inefficient in catching "what if" cases that occur rarely in the system. However, the real world systems inevitably exhibit also the unusual behavior. The use of formal methods is better suited for checking these situations to uncover hidden problems.

The dynamics of current network models is most often limited to changes of actual data in time. The other dimension of dynamics of routed networks comes from dynamic routing protocols and topology changes based on the availability of links and link parameters, e.g. reliability, bandwidth or load. This kind of dynamics corresponds to the control and management timescales as classified by Hui [7]. The current project defines a novel approach in the area of network traffic analysis. The rest of this section lists the four topics that represent the basic inputs for the problem-driven research suggested in this proposal.

A. Rigorous Network Design

Various design methodologies for network architecture include a library of best practices in the form of design patterns or design invariants [1]. Nevertheless, mere application of a correct design pattern cannot guarantee that the designed network will work properly under all circumstances. Available simulation methods can help to increase the confidence in correctness of the network design but still, most notably for large networks, it is unfeasible to check more than several tens of possible cases.

The security requirements of the IT environment define the concept of Evaluation Assurance that specifies several levels of assurance validation. The highest level considered as the most secure requires usage of the formal methods for

presenting the evidence that the design satisfies functional and security requirements.

The method to be studied in the frame of the project is based on model-checking algorithm and formal verification of dependable properties of the design of network architecture. The properties include, for instance, survivability against a link failure, which means, that the network remains fully operational even if any link fails [6].

B. Safe Service Reconfiguration

Networks are designed to provide services. Once the network is deployed, it is carefully managed in order to preserve the intended functionality. However, a network administrator is often required to provide adjustments on the productive network. In order to meet new demands, migrations to newer technology or configuration modification become inevitable at some point. This can have, nevertheless, a significant impact on the availability of currently running services. In some cases, the impact of the migration can be hardly estimated. Network administrators mostly lack tools and methods that explore every eventuality that may happen. In the project, verification problem of safe replace ability, in terms of reconfiguration and topology changes, will be defined and the appropriate verification methods will be studied. This intention lies in the same research direction as the previously stated topic.

C. Inter-network Traffic Analysis

Network monitoring allows operators to see current state of the network and adjust routing protocol behavior such that it responds to network conditions. In the case of interconnection of autonomous systems, routing protocol BGP (Border Gateway Protocol) is deployed. It should be tuned by the operator, so that it adapts to link capacity and connectivity changes, routing updates, or failures. An operator should be given a tool to predict the effect of a new configuration before deployment in a productive network [5].

Another issue encountered in core networks is accountability. Using several interconnections among ISPs (Internet Service Provider) at peering points, the traffic can travel following more possible paths. The path prediction is difficult. Therefore, guarantee of service quality becomes very expensive. At the core level, it is difficult for ISPs to coordinate implementation of routing policies efficiently and clearly.

The lack of well-designed policies leads to introduction of conflicts, e.g., permanent route oscillations. The Routing Policy Specification Language [5] was introduced for this purpose, but it is too expressive to specify certain complex dynamic or multi-homing policies. As the high volume of data flows through ISP networks, different routing principles are applied. The problem synthesized for the project governs the research in the direction of exploring the models that would be expressive enough for capturing these policies. The working hypothesis is that formal methods based on model-checking are capable of verifying efficiently these complex models as well.

D. Increasing Accuracy of Intrusion Detection

Each network connected to the Internet is vulnerable to various attacks because of the services that the network offers but also due to potential contagion of a host computer. One of the greatest issues of the current Internet is called the denial of service attack (DoS). Particularly, it is a difficult task to protect network services to a distributed form of the DoS.

The architecture of IP networks is based on principles such as resource sharing, simple core and complex edge, multipath routing, traffic scalability, and decentralized management. It makes the networks survivable and vulnerable to the DoS attacks at the same time. In [11], Peng et al. survey DoS attacks, their detection and preventions. An efficient detection of DoS attacks has to deal with the separation of legitimate traffic from the attack traffic in order to reduce the rate of false positive results, hence improving the detection accuracy. Recently, the interest in mobile ad hoc networks brings a new kind of security issues [2]. In this kind of networks, topology changes prevent networks to organize in some well-defined security pattern. Instead, security must be imposed to every part of the network. The whole network is thus vulnerable as its weakest point. The dynamic nature of this kind of networks, redundancy of a path between nodes, and distribution of trust among the network nodes pose advantages for achieving availability. On the other hand, the use of wireless links makes the networks more susceptible to passive and active link attacks. Modeling both attacks and detection schemes on these networks may profit from utilization of formal methods as well as from given intrusion detection plan. The evaluation based on a model-checking method can be provided to determine a security level achieved and point out possible sources of security problems. The plan is to develop a network model and verification techniques to analyze a large number of different topologies specified by a predefined scheme and make security assessment on individual topologies with respect to the intrusion susceptibility.

Based on our bibliographic search, we argue that the current models and analysis techniques are not mature enough to guarantee the dependability properties in computer networks considering dynamic behavior. The research of new models and methods for verification is planned in the frame of the proposed approach. The method, which accommodates established model-checking algorithms, will be developed to solve verification problem for validation of security attributes in dynamic computer networks.

IV. RESEARCH APPROACH

The proposed work addresses a problem of automatic formal verification for dependable properties in models of dynamic computer networks. The goal is to develop a verification method for the problem and evaluate its benefits with respect to techniques currently used, e.g. monitoring and simulation. The viability of the approach based on the bounded model-checking algorithm has been demonstrated by the project proponents in [8] and [9] published in conference proceedings and as a technical report.

The proposed research approach is formulated with a strong evaluative component. The current models were found insufficient for modeling dynamic computer networks as discussed above. Since verification has not been extensively used in this area, the main purpose of this approach is to define a verification problem and to prove the existence of a feasible verification method by means of its construction.

We use the traditional four phase research approach to the problem being investigated. In general, it consists of informational, propositional, design and evaluation phases with activities mainly suggested by the names of these phases. The specific details on the work carried in each phase are briefly described in the rest of this section.

A. Informational Phase

Using consultation with networking experts, literature survey, and analysis of raw data from our campus network, we aim to increase knowledge on practical network issues related to design and security. The four particular areas of the project were identified in the previous section. The informational phase also serves to extensively examine particular aspects of all the four mentioned problems. The view on the relative impact of the state problems on network security will be given. We plan to carry out a deeper survey on the current analysis techniques that aim to the similar goal, e.g., verification and simulation methods.

B. Propositional Phase

Proposing and formulating theories and models, and the further refinement into methods and algorithms, is the main focus of the second phase. The outcomes of the informational phase will drive the formulation of the theory that lies behind the verification methods developed in the frame of the project. This theory will encompass real concepts such as dynamic routing protocols, filter lists, aggregated traffic, and packet transformations.

C. Design Phase

During the design phase the theories and methods will be transformed into prototypes of software tools. These tools enable us to perform case studies in order to measure and analyze attributes of the proposed verification methods. To shorten the design phases as much as possible the software libraries implementing verification procedures will be exploited. High-level programming techniques will be employed as the short run-time and a small footprint of the tools are not the primary concerns at this phase. Instead, the rapid development of tools allowing us to conduct experiments with the methods proposed is our priority.

D. Evaluation Phase

Evaluation of the approach will be based on the outputs from the experiments with the computer tools developed in the previous phase. The experiments are considered to be an inevitable part of the project. The evaluation can be split into the following steps:

1. Capability of the proposed methods will be demonstrated.

2. The comparison of methods based on simulation with methods based on verification in the domain of network analysis will be given.

3. Analysis performed on case studies will reveal how the methods can be applied in real conditions.

Note that several different methods may be suitable for modeling and analysis of the environment and properties in the domain of interest. Most often, the combination of several methods leads to better results. The emphasis of the project's research is put on the formal verification methods, but other methods are certainly worthwhile to explore as well. The other methods may be orthogonal with formal verification, or they may support the formal methods.

In particular, monitoring may provide a fruitful data for classification and definition of security-related properties based on the real traffic. Simulation serves as a useful tool to specify and replay possible dangerous scenarios found by the formal verification. Therefore, simulation and monitoring are seen as supporting methods for the network-wide analysis. Their study brings added-value insight with respect to the main research topic of the project. We plan to determine relative positions of all these methods in the evaluation report.

V. Preliminary Results

The approach aiming at applying formal verification methods based on automated techniques, classifying and representing security properties, and implementing experimental tools was currently launched by the both informational and propositional phases. Our launching research stems from the basic ideas presented by Xie et al. in [15], and further elaborated in our work [11, 12]. In those papers, we proposed a verification method that stems from bounded model-checking algorithm [4]. The network is modeled as a graph with dynamically changed links and filtering functions on edges. The model-checking algorithm is implemented as a SAT-based decision procedure and currently prototyped using generally available algorithm libraries. A modal logic language is used for description of dependability properties belonging to availability, safety and security classes.

A promising way of our research currently appears constructing a transition system describing the topology changes of a network to prop efficiency of the method when dealing with large networks. This transition system represents a subset of possible network states coping with reachability of nodes. As we ascertained, such an appropriately constructed transition system forms a lattice, for which various interesting network properties are closed under lattice operations and so can be represented as sets of states in form of sub-lattice. The following example demonstrates the approach.

A. Demonstration Example

The property *network reachability under prescribed packet assets* can be computed by a least fixed-point algorithm. For the example network on Figure 1. we used a language of modal logic to express security requirements based on or derived from this property. Modal logic allows

to reason with validity of packet properties (protocol = TCP, port = 80) in different network states. For example, a statement in modal logic is able to describe properties in different network states where links can change their status, which cannot be expressed by basic propositional logic. In modal logic, a network property can be specified using modal operators *box* (*[.]*, with the meaning "in any case") and *diamond* (*<>*, with the meaning "there is a case"). A modal formula with *box*, e.g., $[\alpha]\varphi$, is valid ("is valid" can be written as "|=") in the network state s_1, $s_1 \models [\alpha]\varphi$, if packet property φ is valid in the network state s_2, $s_2 \models \varphi$, and $s_1 \rightarrow^{\alpha} s_2$ for any α, where α is a label of the related transition. The *diamond* is dual operator to *box*, i.e., defined as $\langle\alpha\rangle \varphi \stackrel{def}{=} \neg[\alpha]\neg\varphi$. That language of modal logic enables to specify and verify various network properties, e.g., a network property saying that the problem with the link between routers R_1 and R_2 has no influence on the web traffic between host PC_1 and web server WWW.

A formula of modal language is interpreted in the network transition system T_N. For model checking, we can define a modal model on the network transition system T_N as a pair $M_N = < T_N , V_N >$, where V_N is a valuation which assigns to each atomic sentence Q a subset of states of T_N. The general decision procedure for the modal model introduced above in realm of the network transition system T_N can be based on small modal property of the logic, which guarantees the decidability of the procedure testing the satisfiability of a formula. We adopted bounded model checking that limits state space by reachability diameter; in this case, the reachability diameter equals to the number of network links.

Now it is possible to evaluate a property, e.g., reachability, in every state s. The SAT-based decision procedure evaluates related propositional formula, which consists of a propositional representation of the transition system T_N and the verified network property, by finding the satisfying permutation of possible valuations. There are standard implementations of such algorithms that appear effective enough to support model checking verification also for non-trivial networks.

VI. Conclusions and Project Outcomes

The approach stems from a formal theory of dynamic computer networks, formal verification methods based on automated techniques, classification and formal mathematical representation of security properties and aims at implementation of experimental tools, and assessment of the proposed approach and comparison with other methods.

The outcomes of the propositional activities of the project include delivering a collection of procedures and tools for:

- Performing automatic verification of properties in a model of local area network using model-checking algorithm,
- Identifying, defining and classifying dependable properties in dynamic computer networks,
- Formal description of the inter-networks and extract of models for automated analysis of aggregated traffic flows,
- Modeling ad-hoc networks and security properties in networks with variable topology and dynamic routing, and
- Classification of topologies according to vulnerability threads and security mechanisms involved.

The design of verification methods and experimental implementation of either standalone or integrated automated verification tools for each of the stated objective is an integral part of the project despite its theoretical nature. We are going to deploy the designed tools in real-size case studies and experiments in the cooperation with domain experts from the area of network design and administration. Based on the findings from the experiments and case-studies, the analysis and exploration of the methods will lead to a formulation of generalized principles. The outcomes of the analysis, exploration and evaluation activities will be the following:

- The determination of a class of models amenable to the automated formal verification by means of model-checking methods and the class of properties that can be verified in these models.
- The statistical results on the efficiency of implemented verification methods. The time/space consumption is measured and the definition of the practical issues is provided.
- The set of issues left as open problems for the further research that hamper the practical and large-scale application of the developed methods.
- The evaluation of the formal models of the inter-networks with respect to the notions captured and the size of a model that can be feasibly analyzed.
- The exploration of ad-hoc network topologies and their classification according to security attributes, such as availability, confidentiality, integrity, authentication, and non-repudiation.

The integrated framework employing the model-based design methods for dynamic computer networks description and model-checking methods for verification of security properties in computer networks should be the main contribution of this project. The outputs of the project will define the basis for the further analysis of security attributes in dynamically routed networks. The effect of routing in the computer networks was overlooked in the security analysis in the past. We aim to identify capabilities of the original idea that propose to use methods based on model-checking for verification of computer networks with dynamic routing.

Acknowledgment

This approach has been carried out in a project with a financial support from the Czech Republic state budget through the CEZ MMT project no. MSM0021630528: *Security-Oriented Research in Information Technology* and by the Grant Agency of the Czech Republic through the grant no. GACR 102/08/1429: *Safety and Security of Networked Embedded System Applications*. Also, the first

co-author was supported by the grant no. FR-TI1/037 of Ministry of Industry and Trade: *Automatic Attack Processing*

REFERENCES

[1] B. Ahlgren, M. Brunner, L. Eggert, R. Hancock, and S. Schmid, "Invariants: a new design methodology for network architectures," Proceedings of the ACM SIGCOMM workshop FDNA '04 on Future Directions in Network Architecture, pp. 65–70, 2004.

[2] Yian Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," Proceedings of the 1st ACM workshop SASN '03 on Security of Ad Hoc and Sensor Networks, pp. 135–147, 2003.

[3] Y. Bartal, A.J. Mayer, K. Nissim, and A. Wool. Firmato, "A Novel Firewall Management Toolkit," Proceedings of the IEEE Symposium on Security and Privacy, pp. 17–31, 1999.

[4] E.M. Clarke, O. Grumberg, and D.A. Peled. Model Checking. MIT Press, 1999.

[5] N. Feamster, J. Winick, and J. Rexford, "A model of bgp routing for network engineering," SIGMETRICS'04 / Performance'04: Proceedings of the Joint International Conference on Measurement and Modeling of Computer Systems, ACM, pp.331–342, 2004.

[6] K.S. Ho and K.W. Cheung, "Generalized survivable network," IEEE/ACM Transactions on Netw., Vol.15, No.4, pp.750–760, 2007.

[7] J.Y. Hui, "Resource allocation for broadband networks," IEEE/ACM Transactions on Netw., Vol.15, No.4, pp. 358–368, 1991.

[8] P. Matousek, J. Rab, O. Rysavy, and M. Sveda, "A formal model for network-wide security analysis," Proceedings of the 15th IEEE Symposium and Workshop on ECBS, pp.171-181, 2008.

[9] P. Matousek, J. Rab, O. Rysavy, and M. Sveda. Network security analysis using model checking. Technical report, Faculty of Information Technology BUT, 2008.

[10] Mitre. Common Vulnerabilities and Exposures Database. [Available from http://cve.mitre.org/; accessed on Feb 2009].

[11] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the dos and ddos problems," ACM Comput. Surv., Vol.39, No.3, 2007.

[12] R.W. Ritchey and P. Ammann, "Using Model Checking to Analyze Network Vulnerabilities," Presented on IEEE Symposium on Security and Privacy, Washington, USA, 2000.

[13] H.R. Shahriari and R. Jalili, "Modeling and Analyzing Network Vulnerabilities via a Logic-Based Approach," Proceedings of the 2nd Int. Symposium of Telecommunications, pp. 13–18, 2005.

[14] T. Tidwell, R. Larson, K. Fitch, and J. Hale, "Modeling Internet attacks," Proceedings of the IEEE Workshop on Information Assurance and Security, West Point, NY, 2001.

[15] Geoffrey G. Xie, J. Zhan, D.A. Maltz, H. Zhang, A.G. Greenberg, G. Hjalmtysson, and J. Rexford, "On static reachability analysis of IP networks," Proceedings of the INFOCOM, pp. 2170–2183, 2005.

[16] X. Ou, S. Govindavajhala, and A.W. Appel. MulVAL, "A logic-based network security analyzer," Proceedings of the 14th USENIX Security Symposium, Baltimore, 2005.

[17] R. Zakeri, H.R. Shahriari, R. Jalili, and R. Sadoddin, "Modeling TCP/IP Networks Topology for Network Vulnerability Analysis," Proceedings of the 2nd Int. Symposium of Telecommunications, pp. 653–658, 2005.