Assignment 5

CPSC – 59700, Spring 2017

Richard P. Givens
Student, College of Arts and Sciences
Lewis University
Romeoville, IL, USA

***Abstract*— This document is a review of two papers presented for study in Week 6, Automated Theorem Proving with SMT [1], and Problem-Oriented Applications of Theorem Proving [2]. Each paper is summarized, and the final section discusses a relevant practical problem related to the final course project, that can be formalized in logical language which can then be utilized by Automated Theorem Proving (ATP) for verification.**

Keywords— Automated Theorem Proving, Satisfiabiliy-Modulo-Theories, Internet of Things, Vulnerability

I. Introduction

Week Six continues the topic of Formal Verification, its logical and computational methods, and how it expresses the various actions or interactions of an application in mathematical terms. This paper is a summary of two papers, [1], and [2], which discuss Automated Theorem Proving, and its use in formal verification methods. Section II discusses [1], and how automated proofing assistants may play a key role in future development. Section III discusses [2], which is an in-depth presentation of one company's approach to developing an Automated Theorem Proving system, and the results from research which attempt to automate both classical and non-classical logic. Finally, Section IV discusses the application of ATP to a relevant problem related to the research project required in CPSC 59700. This project addresses the vulnerabilities of certain Wi-Fi connected devices, and this paper will address how developers may eliminate these vulnerabilities, or avoid creating them in future development projects.

One important clarification is required; though the specific research project touches upon the methods attackers may use to circumvent security measures, or exploit vulnerabilities, neither this paper, nor the final project, will contain specific instructions enabling one to achieve these goals. Testing, implementation and research is conducted using legally owned equipment, with open source tools, and within the scope of all applicable legal constraints.

Similarly, the use or mention of any company's name, product, or device is not a challenge to any trademark, patent or copywrite claim of that company, nor any organization, individual, or individuals affiliated with it. All research is conducted independently, with no sponsorship, consideration or expectation on the part of the author or other parties.

II. Summary of Problem-Oriented Applications of Automated Theorem Proving

Reference [1] is a presentation paper authored by W. Bidel, D. Korn, and S. Schmidt of Fachgebiet Intellektik, Fachbereich Informatik, located in Darnstadt, Germany. It is a view of the organization's "approach to developing a coherent ATP-system, which can deal with a variety of logics," [1].

In most cases, Automated Theorem Proving (ATP) is utilized whenever a problem is formalized in First Order, or Classical, Logic, as well as other problems which rely on mathematical reasoning. It is difficult, however, to formulate solutions for problems which are outside these methods. Additionally, the proofs and outputs of standard ATP systems are technical in nature, and often require translation so they are easily readable. The effect of reading untranslated ATP output is like a person unfamiliar with any programming language attempting to read C++ for the first time. Though there may be some discernible details, the information will be of little value to the reader.

The answer to this problem, as approached by [1] is to design a system that incorporates aspects of several different ATP machines or applications in a system, interconnected and operating cooperatively within itself to translate, infer or guess logical arguments, and then present the output in a human readable form.

While the overall concept of the organization's efforts is understandable, the presentation of the logical calculi is difficult to comprehend. Reference [1] does not provide enough background detail, nor explanation of concepts, which enable clear understanding of its content. However, one can see that the use of this form of ATP system will enable productive research with higher accuracy, which will result in efficient development with lower costs. The methods discussed in [1] seem to touch upon the realms of Artificial Intelligence and Neural Networks, however further research into, and clarity regarding, the background topics discussed in [1] is required to appreciate its content.

that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

III. Summary of Automated Theorem Proving with SMT

Reference [2] is a presentation paper by K. Rustan, and M. Leino from Microsoft, discussing the use of satisfiability-modulotheories, (SMT) in automated or mechanized formal

theorem proving. Utilizing the SMT based verifier Dafny, the authors demonstrate the evolution of SMT tools, which allows testers to focus on other areas of the project while the verifier assumes responsibility for numerous mundane tasks.

Many dedicated verification tools, designed for programs, utilize SMT as the underlying logic, and are accessed via an intermediate programming language designed specifically for the tool or a set of tools. Because of the incorporation of this language, users may automate many of the necessary tasks and focus on the development of specific preconditions, which enable robust testing of applications.

The authors demonstrate the effectiveness of Dafny's proof features by providing "examples inductive and co-inductive definitions proofs by induction and by co-induction, as well as human-readable proofs," which are all recent improvements and supported by what the authors define as "auto-active verifiers," or automated verifiers which work interactively with user input and guidance [2].

The level of automation and accuracy inherit in auto-active verifiers allows comprehensive, rapid verification of programs. Methods and functions, which previously required manual verification over a substantially long period, complete in seconds, freeing the user or tester to concentrate on other tasks, create new methods which explore the application thoroughly, and complete the verification process in a period shorter than previous projects.

As with the techniques and methods presented in [1], [2] demonstrates these tools are evolving, which will result in efficient product development lifecycles, and contribute to advancing the scope and pace of Computer Science.

IV. Applications Involving the Current Research Project

This section will discuss the current research project for CPSC 59700, and how formalizing the project in logical language assists in its formal verification. Since the research project uncovered multiple vulnerabilities, comprehensive detail is not possible due to guideline constraints. One process, user authentication, which accounts for several vulnerabilities, is examined; the final section discusses this process and how ATP may assist in its remedy.

A. Overview of Project

The final research project for this course is a demonstration of vulnerabilities common to many "Internet of Things" (IoT) devices. The reasoning behind the selection of the product involved in the research project is a question asked incessantly, sometimes multiple times daily, by various parties. The main criterion for selection is originality. Importance of original work is paramount; and through research the author has identified one device with no disclosed vulnerabilities, the Black and Decker Wi-Fi Enabled Slow Cooker. This device, through a variety of advanced methods, is usable as a stepping stone into a private communication network, allows access to a user's smartphone. The device serves as an effective attack vector, through which an attacker may steal sensitive account information from anyone attempting to access it. The project does not provide specific methods, but merely highlights certain vulnerabilities that are present in the device, and discusses how these vulnerabilities pose a threat to an individual's privacy or data security.

B. Recent Findings

The core vulnerabilities affecting the Black and Decker Wi-Fi Slow Cooker are systemic, rather than relating solely to the device itself. The slow cooker connects to a network, through which users may control it remotely via an application installed on a compatible smart device using Apple iOS or Android. When configuring the device of remote access, the slow cooker broadcasts an SSID. Though the connection is encrypted, the password for the slow cooker is published on a publicly viewable webpage on Black and Decker's website. There, Black and Decker states the default password for all devices is "12345678" and that users are unable to change it.

Further research reveals that the smart device application, used to interact with the slow cooker remotely, requires no authentication beyond an initial setup of an email address and password. The password may be any six characters, and there is no enforcement policy requiring capital letters, special characters, or numbers. Black and Decker does send a notification email to the address entered in the application, but there is no verification of information required, thus exposing users to possible fraudulent communications from an attacker posing as the company.

The slow cooker, when broadcasting its publicly viewable SSID, will accept a network connection from any device which authenticates using the default password. Additionally, it will accept concurrent connections from multiple devices, exposing it and anyone connecting to attacks from a third party. Though the information between the slow cooker and any connected devices is encrypted, tools exist which allow viewing and decryption of Internet traffic.

Finally, there are no secure protocols preventing the smart device accessing the slow cooker connecting to a device posing as the slow cooker. By using commonly available tools, an attacker is capable of creating a fake access point which broadcasts the same SSID as the slow cooker. This includes the capability of cloning the MAC address, and subverting the channel communications of the actual slow cooker using a higher power rating for transmission. Using this method, an attacker is able to force a user to connect to the fake slow cooker, intercept and decrypt all information sent to it, and then steal sensitive information through a fake web portal. Though considerably less damaging, though infuriating, the attacker may also deny the user any Internet access for as long as they remain connected to the fake access point. Even this simple mischief may serve as the starting point of other attacks, distracting users from the attacker or attackers' other efforts.

C. What Variables Require Optimization

In Security Research and Penetration Testing, most verification occurs through trial and error. The researcher or tester utilizes known methods to simulate an attack or exploit. However, patching vulnerabilities is the responsibility of the

development team or a specialized team tasked with eliminating exposed vulnerabilities.

A comprehensive description of variables named in the previous section requires greater detail than is permitted within this assignment, therefore this section will address one specific vulnerability, the smart device application's authentication methods, and describe how ATP will be utilized during any subsequent patching.

As mentioned previously, the application which interfaces with the slow cooker requires a user email address, and a password consisting of any six characters. The variable requiring correction, in this case, is the initial authentication of the user, when first logging into the application, which within the scope of this paper is termed first_Login.

D. What Variables Affect the Solution?

One of the variables affecting the solution is subsequent logins by the same user over time. Very few applications require users to login every time, when opened on a smart device, and instead save the credentials for subsequent logins. Applications used by professional enterprises, such as large corporations, may have additional authentication or require users to login each time the application is opened, but these examples are few. The developer team must decide if users will remain logged in after first_Login, or if a time limit will determine requirements remaining logged in.

Another variable is the number of users accessing the application. Should the application sync with one account, or remain as it is, allowing to sync with multiple accounts? Ideally, one account for one device is the solution selected by the development team.

A final variable is authentication of the account post creation. In its current state, the smart device application allows full functionality after a potential user enters an email and password. An automated email from Black and Decker is sent to the user, but requires no further action from the user. A potential user may enter any email address, or enter a fake email address, with no requirement for verifying if the account exists. To address this shortfall, the automated email should either prompt the user for additional information or require the user to select a hyperlink, which verifies the user's identity.

E. What are the Benefits of Applying ATP to this Problem?

The benefits of applying ATP to addressing the inherit vulnerabilities of the slow cooker are the same as the benefits of using automated tools to explore and exploit those vulnerabilities. Manual interaction with penetration testing tools is time consuming and prone to error, this is the same issue facing verification of any product pre-release. By automating the testing or verification of the system, teams will save time and experience less errors. Declaring or programming all of the variables will take time, however once the initial scripting or compiling completes, the tools will operate at a pace that is faster than a human is capable of. Additionally, development teams may miss a variable, or an instance of a variable, while automated tools utilize methods which address those potential errors.

The vulnerabilities of the Black and Decker Wi-Fi Enabled Slow Cooker are systemic, and indicative of a lack of focus on application, device, and user security. Though the original developers of the slow cooker, who will be discussed in the final project, may have invested substantial effort in its operability, it is obvious the device did not undergo security verification, and as such the final product verification is lacking. In time, these vulnerabilities may pose a substantial risk to users, but the likelihood of the manufacturer addressing them is slim.

V. CONCLUSION

This paper summarized two presentation papers, [1], and [2], proving automated tools used in formal verification are evolving. As these tools continue to evolve, they will contribute to the development of advanced projects. These projects will similarly evolve, increasing in scope, complexity, and require greater care in verification. Eventually the pace of product development will demand further innovation in verification development, resulting in the discipline's advancement.

This paper also presented a case for using ATP tools as they relate to the upcoming course research project, the exploration of vulnerabilities present in an IoT device. The number of vulnerabilities associated with the device prohibits a comprehensive use case, so this paper focused on user authentication between the smart device application, the user, and the IoT device. Given the extent of the vulnerabilities discussed, and those still undiscovered, it is apparent the manufacturer of the device failed to conduct a comprehensive formal verification, thus highlighting the importance of these tools and methods, as well as the tools and methods of previous research papers presented throughout this course, in software and hardware development.

REFERENCES

[1] W. Bibel, D. Korn, C. Kreitz, and S. Schmitt, "Problem-Oriented Applications of Automated Theorem Proving," Fachgebiet Intellektik, Fachbereich Informatik Technische Hochschule Darmstad, Germany

[2] K. Rustan, and M. Leino, Automating Theorem Proving with SMT , Microsoft Research

[3] Consumer Support Center, Black and Decker| Specturm Home Appliances Consumer Support. http://www.userandcaremanuls.com/pdf/scw3000s.pdf