Assignment 4

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 Weeks Four and Five, Formal Methods: Practice and Experience [1], and Survey of Existing Tools for Formal Verification [2]. This work contains a summary of each paper, as well as additional research and detail regarding one of the tools or applications presented.**

Keywords—Formal Verification, Formal Methods, Mondex, Smart Card.

I. Introduction

The assignments for Weeks 4 and 5 involve the summary of two papers, [1], and [2], as well as further research into one of the applications mentioned within these two papers, drawing from [3]. Reference [1] is a paper which discusses the uses of formal verification methods across a wide array of development projects, which occurred over the course of several years, while [2] discusses some of the same tools utilized in [1] as well as several others. Finally, this paper discusses further research on a specific development project reported by [1], the Mondex Smart Card.

II. Summary of Formal Methods: Practice and Experience

A. The Early Days: Difficulties in Implementation

The largest challenge facing the widespread adoption of formal methods in software development was the complexity of systems (or lack thereof). Formal methods worked primarily with smaller systems, or subsystems within a larger system, because they were unable to handle larger than a few thousand lines of code. However, as the technology and hardware in computing grew in scope and capability, the ability to address systems containing larger amounts of code became easier. Soon, the capabilities of commercial systems surpassed that of earlier industrial systems, and the feasibility of applying formal verification methods to development matched pace.

B. The Survey: Wide in Scope, But Possibly Biased

The main portion of the paper discusses a survey of several projects, spanning multiple years and at separate phases of formal method adoption. In all, sixty-two projects comprise the survey, however it may contain some bias, as admitted by the authors, due to the respondents' familiarity with the authors. The data is self-reported, and the respondents themselves are from diverse backgrounds among the projects, some being on the development team, and others within the management team, or some other stakeholder. The lack of continuity among the respondents' backgrounds, and the inability to determine veracity of the self-reported data, does pose problems for the research; however, as the point of the survey appears to not only collect facts about the development projects themselves, but also the general impressions of those respondents regarding the use of formal methods and their future utility, as well as potential buy-in among other stakeholders for future projects.

C. Scope of Projects Surveyed

The scope of the various projects surveyed varied. Of single applications, Transport was the largest represented industry, followed by the Financial industry, and then Defense (or Defence, as spelled in the paper). Among the applications, the types surveyed included real time, high data volume, parallel processing, distributed systems, transaction processing, and several others with some projects crossing over from one application type to another.

Figure 3 in [1] shows a timeline of the projects surveyed, with the first date being 1984. What is most interesting regarding this figure is the pace of development is its increase in quantity, with shorter breaks in between projects. Other figures show approximations of the amount of code, which remained consistent within a curve favoring the median, and the techniques used, which included Modelling, Proofs, and Model Checking.

D. The Takeaway

While the paper does go into a high-level detail of each project, the main takeaway is the respondents' conclusions. When asked if the tools could cope with the tasks at hand, 84% responded favorably. Among the respondents, 75% stated they will use a similar technology or method in the future, while 25% stated they will possibly use a similar method in the future. Since there were no respondents who stated other than they would, or may use a similar technology, it is safe to assume that those who felt the tools were not up to the challenges of their project will seek a robust tool or method that is in line with their needs.

III. Summary of Survey of Existing Tools for Formal Verication

Reference [2] discusses the challenges of formal verification, specifically listing a bug in the Intel Pentium Processor, which although it underwent rigorous testing, manifested within a year of release.

Though numerous tools for formal verification exist, many address a single problem or problem domain, with very little customization options, and no utility beyond their immediate scope. As such, their utility for full formal verification is limited to debugging. As stated in the paper, most professionals who have need of specific checking of their unique problem domains either design a tool themselves or modify open source tools to fit their needs.

A. No Tool Covers Everything

By necessity, and complexity, it is impossible for any tool to comprehensibly cover every scenario. Testing and simulations of applications may show expected outputs in response to inputs, but they will not check for methods, inputs, or other issues which make an application unsafe. Even the most robust tools will be unable to predict every combination, input or action by a user, nor will developers and testers successfully predict users' inputs or actions. Formal methods may, through mathematical analysis, be able to fill in some of the gaps left by standard testing and simulations.

B. The Two Types of Tools

- Model Checkers utilize special programming languages, which vary according to the tool, to step through an application with little human interaction. They will return one of three results: Satisfied, Not Satisfied, or Indeterminate.
- Theorem Provers are semi-automated, and work under the manual guidance of a developer or tester, who utilizes adaptability, and experience in order to create a robust testing method with greater accuracy than Model Checkers.

C. The Three Classifications of Tools

Just as there are two types of tools, there are three classifications as well. Tools that verify the correctness of a model, either through model checking or theorem, may work with abstract models, or utilize specialized programming languages to verify the design descriptions to verify the design of software or hardware involved. The final classification of tools assist in creating provably correct designs, which prove the properties of the system.

It is important to note that these classifications and types of tools are by no means exclusive of one another. In any design or development of a project, it will be important to utilize a robust testing method, which will require these classifications and types at various times.

D. The Need for Testing

Reference [2] correctly states the need for testing at the onset of development will reduce the costs of projects, both in billable man hours and in debugging post-release. Also, [1] surveys its respondents, who in many cases pointed to actual cost and time savings because of a rigorous testing method with the correct tools. In any project which experienced no quantifiable savings in either time or money during development, it is certain savings the project experienced savings after release, simply because of fewer issues experienced by users.

The need for using formal verification methods in future development is unquestionable. Advances in computing, the complexity of the hardware and tools available, ensure the ability to comb through immense amounts of code, while the availability of development tools to anyone promotes an atmosphere of creativity, which balance with feasibility.

IV. In Depth Research of the Mondex Smart Card

One of the projects mentioned in [1] is the Mondex Smart Card, developed by the National Westminster Bank and Platform Seven[2].

A. Rationale for Choice

The Mondex Smart Card represented a dramatic leap ahead in terms of development and testing. The rigorous standards to which the developers adhered serve as a model for future products. Furthermore, the underlying technologies of the Mondex Smart Card manifest throughout society, and are integral to the function of industry, medicine, business, and finances. It is impossible to interact with any level of society today, without interacting at some point with a device, card, or application that uses technology like the Mondex Smart Card.

B. What is the Mondex Smart Card?

According to Reference [3], the Mondex Smart Card began in 1990. It served as a form of electronic cash and consisted of an embedded chip on an ATM style card with a magnetic strip.

Various Science Fiction and Cyberpunk style stories mention "cred cards" or "credsticks" and are identical in their description to the Mondex Smart Card. Indeed, one might think of the technology behind the Mondex Smart Card as the precursor, or the catalyst of, modern banking cards. Like modern banking cards, the Mondex Smart Card contains a microchip, encoded with financial information. This information serves as a balance of sorts, and allows the card to store many times more information than found on a standard magnetic stripe card [4].

Though the apparent original intent of the Mondex Smart Card was to serve as a secure means of carrying a form digital or electronic currency, it has evolved from that into various forms.

C. Pitfalls

Originally, if a cardholder lost their Mondex Smart Card, the ability to recover the funds or transactional information on the card faced limitations [4]. While purchases on the card worked similarly to pre-paid debit cards, the Smart Card contained a small microprocessor. So, the Mondex Smart Card has the advantage of acting as a private means of carrying digital currency, and the ability of conducting card to card transfers, but losing a Mondex Smart Card poses as many challenges to a cardholder as losing a wallet full of cash. Without strong security protocols, which are impractical for most devices of this size and complexity, the Mondex Smart Card is usable by any person finding it.

Other potential issues with the Mondex Smart Card are due to its complexity as an electronic device. One avenue of fraud exists in the limited memory present in the card. Repeated transactions may create an overflow, causing significant data loss which may be irretrievable [4]. Also, none of the resources found, of which there are very few, mention how the device maintains its memory; meaning it is impossible to determine if the encoded memory is volatile, and would erase if exposed to any form of power surge or power loss. Nor do the resources mention if there is any power requirement, such as a rechargeable micro-battery or solar cell, which supplies the Mondex Smart Card with the necessary power to maintain its encoded data.

Other forms of digital currency rely upon the transmission of data over standard means, usually via the Internet. Because of this transmission of data, modern banking cards and other forms of electronic or digital currency are less prone to fraud. In the case of a cardholder losing their card, calling the financial institution, and reporting a loss or stolen card is sufficient to ward off potential fraud, or recoup losses suffered because of the loss. The anonymity of carrying one's entire financial purse on a card may seem tempting, but losing that purse is sure to set one against it.

D. Where It Stands Now

Mondex does serve as an example of refined development, having earned an ITSEC Level 6 certificate in 1999 [1]. As part of this certification, a team audited the entire development process, and the formal methods used detected no errors [1]. Evaluation of the project occurred again in 2006, subjected to numerous methods to evaluate the current progress in modern verification tools, and how they improved during the time since the original project [1].

The surest indicator of the success of the Mondex Smart Card, and its underlying technology, is its acquirement by MasterCard, in 1997 [4].

Though a few agencies only use the actual Mondex Smart Card currently, the underlying technology is in many devices, cards, and technologies in use every day. Faults in the original design, such as the ability to lose the card and all the information on it, underwent improvement, and we utilize in modern banking cards. Smart card technology is in use today in cell phones, TV digital set top boxes, pre-paid credit cards, access control cards, employee identification cards, government issued IDs, and in medical devices such as the CPAP. "The chip" is ubiquitous in all physical purchases using electronic forms of payment. Many retailers have implemented the EMV standard, as it is known now, with many working towards full compliance in all purchases.

E. Conclusion

The Mondex Smart Card was a revolutionary step ahead in the development, design, and testing process, using advanced tools for its time that many chose to ignore. The necessity of providing secure financial information, safe from fraud, demanded a rigorous development and testing process, which served as the gold standard for many applications. Because of the ingenuity behind some of its designs, modern society will be using derivatives of the technologies involved for the foreseeable future.

F. Cautionary Note

Those researching the Mondex Smart Card must exercise caution. Several sources of potential research may be fraudulent, and intended to entice a potential victim to purchase a card, or the equipment necessary to utilize the Mondex system. MasterCard purchased Mondex in 1997, absorbing and incorporating it into their business operations. Current information regarding the Mondex Smart Card is sparse; and searching MasterCard's business site reveals no information pertaining to the subject. It is recommended that anyone researching the topic remain alert for indications of fraudulent or misleading information. In particular, though [2] appears legitimate, [3] has several indications of possible fraudulent, or misleading information.

REFERENCES

[1] J. Woodcock, P. G. Larsen, J Bicarregui, and J Fitzgerald, Formal Methods: Practice and Experience.

[2] R. C. Armstrong, R. J. Punnoose, M. H. Wong, and J. R. Mayo, Survey of Existing Tools for Formal Verification..

[3] "Mondex Smart Card." Tech-FAQ, www.tech-faq.com/mondex-smart-card.html. Accessed 25 Apr. 2017.

[4] "Mondex® | MasterCard®." Mondex® | MasterCard®, www.mondexusa.com/index.html. Accessed 25 Apr. 2017.