atsec information security corporation
4516 Seton Center Pkwy, Suite 250
Austin, TX 78759
Tel: +1 512 615 7300
Fax: +1 512 615 7301

Author: Yi Mao (yi@atsec.com), Ph.D., CISSP

Organization: atsec information security corporation

Short biography

Yi Mao, CISSP, holds a Ph.D. in Mathematical Logic (2003) and a Master's degree in Computer Science (2000) from the University of Texas at Austin. She graduated from Peking University in China with a B.A. (1991) and an M.A. (1994). Dr. Mao is the CEO and Managing Director of atsec U.S.A. She oversees the business operation, including but not limited to the Cryptographic Security Testing compliant with the FIPS 140 related standards and the Common Criteria (CC) evaluation. She coordinates with atsec sibling offices in Europe and Asia. Dr. Mao contributes to ISO/JTC1/SC27/WG3 and is a liaison officer representing CMUF at the ISO expert editing sessions that develop the international standard counterparts (ISO/IEC 19790, 24759, 15408, and 18045) of FIPS 140-3 and CC. She is a frequent conference presenter in the area of information security.

Presentation Title for 2024 NCCoE FMCP Workshop:

Which one to apply: formal methods or machine learning?

Extended Abstract

The presenter will share her knowledge of formal methods and experience in applying formal methods to Common Criteria evaluation and FIPS validation. She doubts the applicability of formal methods to ACVP and AMVP. Alternatively, she proposes to adopt machine learning techniques to facilitate the cryptographic module review process.

While studying at UT-Austin, the presenter took classes from Professors Robert Boyer [1] and J. Moore [2]. She was familiar with the Boyer-Moore Theorem Prover family and their latest industrial-strength automated reasoning system ACL2 [3]. "ACL2" denotes "**A** **C**omputational **L**ogic for **A**pplicative **C**ommon **L**isp". ACL2 is an interactive system consisting of a logic and programming language in which you can model computer systems and their digital artifacts and guide the system to mathematical proofs about the behavior of those models. It has been used at AMD, Centaur, IBM, and Rockwell Collins to verify properties of commercially designed microprocessors, microcode, the Sun Java Virtual Machine, and operating system kernels. Some industrial examples of ACL2 use are the following:

- Verify the compliance of **AMD Athlon's** (TM) elementary floating point

operations with their IEEE 754 specifications
- Verify the floating point divide and square root on the **IBM Power 4**
- Verify floating-point addition/subtraction instructions for the **media unit** from **Centaur Technology's** 64-bit, X86-compatible microprocessor
- Prove information flow properties about **Rockwell Collins's Advanced Architecture MicroProcessor 7 Government Version (AAMP7G)**, a Multiple Independent Levels of Security (MILS) device for cryptographic applications. The AAMP7G provides MILS capability via a verified secure hardware-based separation kernel. The AAMP7G's design was proved to achieve MILS using ACL2, per the standards set by EAL-7 of the Common Criteria. Rockwell Collins has received National Security Agency (NSA) certification for the device based on this work.

Also, during her UT years, the presenter was very fortunate to take small-size seminars with Professor Allen Emerson [4] and gained a thorough understanding of his seminal work on formal verification and model checking, which is an algorithmic method of verifying nominally finite-state concurrent programs. These ongoing finite-state programs correspond to the synchronization skeletons of many concurrent, distributed, or reactive programs comprised of multiple processes that must synchronize or coordinate their behavior. Emerson uses a temporal logic, CTL (Computation Tree Logic), to describe correct behavior, permitting behavior specification along all futures versus some futures. His model checking theory has become a viral and successful approach to formal verification, such as verification of parameterized systems and reasoning about data structures. Emerson won the Turing Award in 2007 for his groundbreaking work and significant contributions to model checking [5].

Being rigorously trained in academia for more than a decade in mathematical logic and its applied areas, such as theorem provers, formal verification, and model checking, the presenter attempted to promote the use of formal methods whenever possible. At ICCC 2007 in Rome, Italy, she presented "Economical Use of Formal Methods" [6]. Gemalto used formal methods for a smart card CC certificate at EAL7 in 2008 (see "About the world-first smart card certificate with EAL7 formal assurances" [7]), and the presenter worked from 2000-2006 on the smart card subject to the certification. The presenter closely worked with IBM using their SPIN model checker to prove the security features of their HSM module to fulfill the FIPS 140-2 level 4 validation requirements [8].

The recent survey on formal methods [9] summaries the following challenges for deploying Formal Methods:

- Complexity: Applying formal methods can be complex and require specialized knowledge.

- Scalability: Formal methods may struggle with scalability when applied to large and complex systems.
- Resource Intensive: The process can be time-consuming and resource-intensive, which might be a barrier for some projects.

Due to the challenges of using formal methods, both the CC and FIPS standards have removed the requirements for using formal methods. NIAP has long moved away from high Evaluation Assurance Levels (EALs) that require formal methods but promote a Protection-Profile-centric approach, and the CCRA (CC Mutual Recognition Agreement) downgraded from EAL4 to EAL2 a decade ago. CC:2022 adopted NIAP's approach and promoted exact conformance to Protection Profiles (PPs), which specify evaluation activities for each security requirement for a type of product (e.g., Operating System, Software Application, Network Devices, Mobile Devices). Still, none of the PPs requires Formal Methods. FIPS 140-3 is an adoption of ISO/IEC 19790, which does not require Formal Methods for any modules at all security levels. The presenter questions the feasibility of imposing Formal Methods while FIPS 140-3 does not require it.

In the age of Machine Learning and AI, it may be more promising to use ML-based or AI-assisted tools to expedite the CMVP certification process. The presenter participated in the UT 2024 ML Symposium [10] and learned that there were some ML-based tools for code review/editing [11]. The research work in this area, computational linguistics, heavily references DRT (Discourse Representation Theory) and SDRT (Segmented Discourse Representation Theory). The co-author of DRT, Hans Kamp, was recently awarded the Schock Prize [12]. The co-author of SDRT, Nicholas Asher, was the speaker's Ph.D. thesis advisor. Asher is the director of a national AI lab in France. His team created the STAC corpus [14], the only dataset annotated for discourse relations and the most cited dataset in computational linguistics. Asher is regarded as the "Godfather" of this field. The presenter knew DRT and SDRT by heart, upon which she developed her Ph.D. dissertation [15].

From now to the workshop in July, the presenter plans to study and catch up with the latest research results that apply to the crypto module certification program when her time permits. The NCCoE may also consider to collaborate with UT-Austin. The presenter's vision of the future AI-assisted certification program is depicted in the ICMC 2023 clip [16].

Key Words:

Formal Verification, Theorem Prover, Formal Method, Machine Learning, AI-based code review, AI-based report review, AI-assisted evidence review.

atsec information security corporation
4516 Seton Center Pkwy, Suite 250
Austin, TX 78759
Tel: +1 512 615 7300
Fax: +1 512 615 7301

References:

[1] Robert Boyer: https://www.cs.utexas.edu/users/boyer/
[2] J. Moore: https://www.cs.utexas.edu/users/moore/
[3] ACL2: https://www.cs.utexas.edu/users/moore/acl2/
[4] Allen Emerson: https://www.cs.utexas.edu/~emerson/
[5] Allen's 2007 Turing Award: https://amturing.acm.org/award_winners/emerson_1671460.cfm
[6] Yi Mao's presentation at ICCC 2007 in Rome, Italy: https://drive.google.com/file/d/10M5fbwI4iYbsa5Xa2R7ObAvCelC0jNKd/view
[7] Gemalto's world-first smart card CC certificate at EAL7: https://www.commoncriteriaportal.org/iccc/9iccc/pdf/B2404.pdf
[8] IBM HSM module at FIPS level 4; https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/4558
[9] A Survey of Practical Formal Methods for Security: https://dl.acm.org/doi/pdf/10.1145/3522582
[10] UT 2024 ML Symposium: https://cns.utexas.edu/events/public-event/2024-machine-learning-lab-research-symposium
[11] CoditT5: Pretraining for Source Code and Natural Language Editing, by Jiyang Zhang et. Al: https://dl.acm.org/doi/pdf/10.1145/3551349.3556955
[12] Hans Kamp and his DRT (Discourse Representation Theory) recently awarded the Schock Prize: https://www.kva.se/en/prizes/rolf-schock-prizes/ and https://liberalarts.utexas.edu/news/linguist-and-philosopher-hans-kamp-awarded-schock-prize
[13] Nicholas Asher (https://www.irit.fr/~Nicholas.Asher/) and his SDRT (Segmented Discourse Representation Theory): https://www.researchgate.net/profile/Nicholas-Asher/publication/226373693_Segmented_Discourse_Representation_Theory_Dynamic_Semantics_With_Discourse_Structure/links/0fcfd50ad08ae189ec000000/Segmented-Discourse-Representation-Theory-Dynamic-Semantics-With-Discourse-Structure.pdf
[14] Strategic Conversation (STAC): https://www.irit.fr/STAC/index.html
[15] Yi Mao's Ph.D. dissertation: https://repositories.lib.utexas.edu/items/8e141545-2520-4491-90cd-7dbdf0ad3cb1
[16] ICMC 2023 clip: https://vimeo.com/864916383