Research Proposal

Implementation of Formal Semantics and the Potential of Non-Classical Logic Systems for the Enhancement of Access Control Models

Alvin Tang

Introduction

Cyber security has been a significant branch of computer science as digital systems have been critical in people's lives since the extensive digitisation of our daily tasks and businesses in modern society. The importance of protecting digitally-stored data and ensuring the integrity of access control have been more important than ever before. Inadequate level of awareness towards computer security and poor implementations of cyber security protocols in the industry, however, are posing risks that may undermine the integrity of software systems. Whilst there is an growing occurrence of data breaches in the industry, it is imperative for researchers to discover the prevention thereof. [1]

From the practical data breach detection with zero persistent secret state [2] to the semantics for a logic of authentication [3], formal methods and logic have been asserted to be just as crucial as the implementations of computing with programming and software design. The underlying mathematical principles of computation play a notable role in ensuring that our encryption and validation protocols are resilient to security attacks. Access control, in particular, is an essential component of computer systems to manage the permissions of users and processes to retrieve and manipulate data.

In this proposed research, we shall analyse the roles of logic and semantics in systematising the foundational concepts of access control models, their consequent limitations arising from the essence of classical logic and potential solutions with alternative logic systems. Envisioning to focus on the utilisation of set theory and sequents to convey the semantics in these models, we will, for instance, study the significance of modal logic in role-based access control (RBAC) policies due to its value in displaying how the completeness and consistency of cyber security protocols can be proven theoretically. [4] We should subsequently reveal the prevalent vulnerabilities and concerns regarding current theories, as well as how alternative logic systems can form the foundation of refined models to encounter the challenges.

Linux and plenty of Unix-based systems, being common options of operating systems for server hosting, implement simple access control models by default. The management of permissions to read, write and execute files and directories are performed by identifying users with a numerical system. [5] Notwithstanding the fact that a simple access control model provides the advantages of being lightweight and uncomplicated to manage, it may not offer the most advanced features or the most granular control in more complex systems. Role-based access control (implemented in SELinux, for example), on the other hand, maximises the flexibility and effectiveness to manage permissions based on the principle of least privilege and consideration of users' roles, job functions and other attributes. The foundation of this concept is primarily attributed to formal logic as we use relations and sequents to coherently express role hierarchies, users' attributions and decision methods. [6]

Whilst the majority of theoretical computer science concepts are derived from classical logic, with binary truth values and the principle of explosion as some of its major characteristics, we shall reckon the potential of applying non-orthodox logic systems, including fuzzy logic and paraconsistent (e.g. relevant) logic, in cyber security to model and reason about systems where uncertainty or inconsistency are present. As another major focus of the study, we anticipate elucidating the potential vulnerabilities of popular access control

systems and how non-classical logic systems may contribute to resolutions of the most prevalent issues in current technologies.

Research Problem

Defining Key Terms

In order to succinctly identify the focus of the research, we should begin by clearly defining *cyber security*, *access control* and how the principles of the former are fulfilled by the objectives of the latter. This enables us to better achieve the purposes of investigating existing access control models and proffering improvements with new models.

The common definition of *cyber security* refers to "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets". [7]

There are plenty of cyber security principles, including open design, least privilege and compartmentalisation. [8] [9] The principle of open design affirms that the security of a system should not depend on the secrecy of its protection mechanisms. The concept of least privilege ensures that any component of a system should operate using the least set of permissions to complete its job. Compartmentalisation organises resources into isolated groups of similar needs. These are all features which help achieve the security of data and systems.

Meanwhile, *access control* is a strategy to limit access to a computing system by [10]

- deciding whom they would like to give access privileges to,
- determining which roles require what access, and
- enforcing access control limits.

The objective of implementing access control is to minimise the risk of unauthorised access to important information.

Access control in digital systems ensures cyber security with a set of rules to determine roles and privileges. Given this nature, access control theories may be classified as *tools and foundations of technologies based on the enforcement of policies.*

Modern access control theories comprehensively fulfil the principles of cyber security. The implementation of discretionary access control, for example, is publicly scrutinised by academics [11] [12] for its safety while the use of one-time passwords in multi-factor authentication is developed from the knowledge of hash chains. The successful deployment of these technologies can be attributed to the fact that they are secure even if their underlying mechanisms are publicly known. A well-implemented access control system, furthermore, ensures security by offering minimal privileges to users and processes. [13] This fulfils the principle of least privilege.

Research Questions

With the above key terms and concepts well-delineated, the research can accordingly be tersely summarised as the following inquiries.

1. How are formal logic and semantics applied in the principles of existing access control models?
2. How do the features of classical logic lead to limitations in existing access control models?
3. How can non-orthodox logic systems contribute to the development of more expressive, flexible and comprehensive access control models?

Roles and Importance of Logic in Access Control Models

Whilst the development of access control systems are chiefly concentrated on software engineering and operating systems design, formal logic and semantics are equally indispensable for their underlying foundations as theoretical models as they provide rigorous modalities to reason about the correctness and integrity of these systems.

Experts have developed a wide variety of ideas using axioms and sequents to represent the role hierarchies and user attributes, as well as the resultant reasoning services, to define the policies in the access control system.[6]

In addition to the role-based access control model as aforementioned, researchers have developed the attribute-based access control model (ABAC) with a logic-oriented framework. Unlike RBAC, which restricts access to resources dependent on the roles assigned to users, ABAC uses attributes of users, resources and the environment to render access control decisions.[14] Both frameworks rely on expressions of policies with set, relations and sequents.

An approach to define ABAC policies suggested by researchers, as a concrete example, is to construct rules using constraint predicates. `cando(X,Y,±,Z)` is a basic example. The 4-ary predicate where X and Y are attribute and service set terms, intuitively meaning that set X is authorised/prohibited in using services Y.[15]

Hence, we may clearly observe that formal logic and semantics are critical tools to help us ensure that the designs of access control systems provide the necessary level of security and protection for sensitive information and resources. In this research, therefore, we will ascertain and analyse how logic and semantics are applied in existing access control models.

Research Significance and Potential Achievements

The vast majority of theories relevant to access control models and, in general, cyber security are grounded on classical (orthodox) logic. Modal logic adopted for RBAC, for instance, is an extension of classical logic that adds operators to express modalities such as necessity and possibility. Nevertheless, there are concerns arising from the characteristics of orthodox logic. The features of this traditional logic system include but are not exclusive to:[16]

1. Having exactly two truth values (i.e. true/false);
2. The law of excluded middle: the negation of a true statement is false, and vice versa;
3. The principle of identity: every object is identical to itself;
4. The principle of non-contradiction: a proposition and its negation cannot be true at the same time.

There are moreover some potentially undesirable attributes from the most elementary definitions of logical connectives. Consider the propositional formula $p \rightarrow q$. When premise p is false, the whole implication statement is true by definition. In fact, there is no requirement that p and q have to be related to each other in any respect. This is regarded as the principle of explosion (*ex falso quodlibet*).

Such definitions and their resultant phenomena, however, may be concerns when we use this logic system in practical situations to express and validate access control models. In actual cyber security implementations, indeterminate or insufficient information is often dealt with. For example, in RBAC systems, it may not always be possible to determine all the permissions that a user/role has or all the resources that a user/role can access owing to the proscription of uncertainty in classical logic.

To tackle these concerns, alternative logic systems such as fuzzy logic, relevant logic and intuitionistic logic may be considered for creating ameliorated access control policies. These logics can allow for reasoning about uncertain or incomplete information and provide more flexible and expressive ways for the design and analysis of new models.

Hence, the final objective of this research is to unearth the possibility of using unconventional logic systems and to investigate the advantages or otherwise thereof.

Benefiting from the outcomes of this research, designers of computer systems, especially contemporary types of architectures (e.g. distributed systems) may address prevalent issues with existing access control models.

Methodology

Based on the three main research questions specified above, the inquiry shall be conducted in various approaches in order to obtain a comprehensive understanding of existing access control models and to uncover possible ways to develop more enhanced models with non-classical logic systems.

Understanding Logic in Existing Models

The project shall begin by exploring the ongoing work of scholars in expressing popular access control models with formal logic. In particular, it is proposed that the previous research papers relevant to the following models should be analysed:

1. Discretionary Access Control (DAC)
2. Role-Based Access Control (RBAC)
3. Attribute-Based Access Control (ABAC)
4. Bell-LaPadula Model (BLP)

These models are valued in a diverse set of situations inasmuch as their characteristics cater to various needs. DAC is commonly operationalised in personal computer systems, where users should have complete control over their machines. RBAC and ABAC are applied in more complex systems whilst BLP is utilised when strict confidentiality of data is necessary. We will examine how these models apply formal logic in different ways in order to suit their specifications.

Since formal language and grammar are major parts of logic and semantics in access control models, we may perform investigations of languages for access control, such as the one researched by Kumar Avijit. [17]

As an example, suppose $\mathbf{w}$ and R are a user and an object (file/process) in this language respectively. Predicates are developed to articulate ownership and permissions, such as follows.

- $\texttt{owns}(\mathbf{w}, R)$ means $\mathbf{w}$ possesses ownership of R.
- $\texttt{mayrd}(\mathbf{w}, R)$ denotes $\mathbf{w}$ has the permission to read the file R.
- $\texttt{maywt}(\mathbf{w}, R)$ indicates $\mathbf{w}$ has the permission to write the file R.

Subsequently, we are able to formulate axioms, such as

$$\forall w.\forall R.\texttt{owns}(\mathbf{w}, R) \supset \texttt{mayrd}(\mathbf{w}, R)$$

which refers to the rule that ownership implies permission to read. (Note that this is an *axiom* defined in this language, which is not always true in reality.)

The language is then introduced to be expressed in sequents for better coherency and static typing, which ensures that the logic is consistent. Here is an example of a deduction rule defined by the author:

$$\frac{\pi \vdash_{\mathcal{L}} m : p_1 \wedge p_2}{\pi \vdash_{\mathcal{L}} \texttt{fst}_{\mathcal{L}} m : p_1}(\wedge E1)$$

The symbol π refers to a hypothesis while p_1 and p_2 are propositions. $\texttt{fst}_{\mathcal{L}} m$ is a proof term. This rule closely resembles conjunction elimination in natural deductions and sequent calculus, which are important formal proof methods.

By using static typing, the researcher is able to prove that the language is type-safe, which assures the security of the model by preventing security vulnerabilities caused by misconfigured policies. Rules for formal proofs with sequents also enable developers of the models to better maintain the system. [17]

There is a considerable variety of languages and formal grammar proposed by academics. In this research, they can be compared for similarities and characteristics in order to understand how precisely logic plays a critical role.

Investigating the Limitations of Existing Models

To explore the shortcomings of existing access control models, we shall focus on the fundamental causes attributed to the distinctive qualities of classical logic.

As an illustration, a feature in RBAC is that the user is either granted or denied access to a file predicated on their roles and permissions. This is consistent with the prominent property of orthodox logic that each statement has a truth value, which can only be either true or false. In practical situations, nonetheless, binary truth values may not be sufficient to express the decisions for managing permissions.

Role explosion is another concern in RBAC. As the complexity of a system increases, the number of roles and permissions may grow exponentially. This can lead to a combinatorial explosion in the number of possible access control configurations, making it arduous to manage and verify the policies. [18]

In addition, RBAC may be susceptible to insider threat, where a user with legitimate access may abuse their privileges to access sensitive resources. [19]

There are plenty of models in addition to RBAC. Each option has advantages and drawbacks. In this research project, we should conduct analyses to discover the limitations of the four models as stated discussed, as well as how classical logic is attributed to their constraints.

Discovering the Potential of Non-Classical Logic for Enhanced Models

There are plenty of alternative logic systems, including the following options.

1. Fuzzy logic: a continuous range of truth values between 0 and 1 replaces bivalance. [20]
2. Relevant logic: avoids the sorites paradox by requiring relationship between premises and conclusions in implication statements. [21]
3. Intuitionistic logic: avoids the law of excluded middle and double negation elimination. $(\neg\neg p \not\equiv p)$ [22]

Again, as an illustration, we can demonstrate how in this research these three logic systems may resolve the above issues in RBAC respectively.

To address the limitation that access can only be either granted or denied, fuzzy logic may instead be used to assign probabilities to users based on their credentials and behaviour. This approach, rather than by defining the roles of users explicitly, resembles a "credit system" which may possibly be used in situations when access is determined according to the level of trustworthiness.

In the meantime, relevant logic may be used to resolve the issue of role explosion. [18] By providing a framework for expressing and comparing roles and permissions in terms of their relevance and redundancy, this logic system can reduce the number of roles needed and simplify the management of RBAC policies, leading to a more efficient and effective access control system.

Intuitionistic logic can attend to the concern of insider threat by providing a framework for expressing uncertainty and ambiguity in access control decisions. The strict requirement not to allow the principle of excluded middle or non-contradiction may reduce unnecessary authorisations of file access, upholding the principle of least privileges in cyber security.

The methodology of this research is to discover the potential of non-orthodox logic for enhanced access control models, done by proposing models based on these logic systems substitution options. We shall in turn investigate the advantages and concerns of these proposals with the comparison of one another.

Limitations of the Research

A potential limitation of this research is the challenge of providing an all-round solution addressing all problems in the existing access control models concurrently.

Different logic systems are innovated to resolve paradoxes and drawbacks of classical logic. Therefore, when new models are proposed with various logic systems, we may likely only resolve some issues at a time.

The benefits of this project can be retained as we overcome such challenge by specifying the intended purposes of all kinds of access control models. Upon the successful development of multiple alternative access control models, they can be utilised for different situations according to the relevant needs.

Evaluation Criteria

The outcomes of this research project can be evaluated with various techniques corresponding to the three main research questions.

In connection with analysing the functions of formal logic in existing access control models, we will attempt to perform formal logic proofs based on the languages and grammar developed by researchers. The method of analysis shall be modelled after the proof examples in *Access Control, Security and Trust: A Logical Approach* by S. K. Chin and S. Older [23], where abstractions of modern access control models are formalised by sequents and rules for natural deduction or sequent calculus. The completeness and soundness of the logic system are then taken into consideration to determine the comprehensiveness of each model.

Regarding the limitations of existing access control models built upon orthodox logic, we shall attempt to discover their vulnerabilities and concerns. We should try to exploit the vulnerabilities in the models proposed by researchers, which demonstrates the level of inadequacy in terms of the models' articulacy, scalability [24] and flexibility. This can be evaluated by mathematically (or with actual access control systems, if applicable) demonstrating that the existing logical models are not able to fulfil some specifications for an access control solution.

For instance, we shall create a scenario of access model usage in industrial applications where bivalent truth values are not sufficient for the management of users' roles and permissions. We may also conduct complexity analyses on how the existing models perform when there is a large number of roles and permissions required in an extensive database. As case studies with some exploitation of access control models are done, the limitations can be evaluated.

For the discovery of improved models founded on non-classical logic, it is understood that these concepts should not only be rigorous theoretically but also be feasible practically. Therefore, it is proposed that, upon the exploration of conceptual models, we shall develop simulations of the proposed access control systems to demonstrate the possibility of real-world applications.

Type checking, as mentioned above in the example of the RBAC language, is an vital element to ensure the correctness of model axioms. A strongly-typed functional programming language (e.g. Haskell) is therefore preferred for the coding demonstration.

Depending on the extensiveness of the research, the project shall last for at least a semester. The initial weeks should be dedicated to theoretical proofs and review of previous literature while the subsequent time will be used for the realisation of access model proposals with a gradual increase of time and dedication to the development of simulation programs.

References

[1] R. von Solms and J. van Niekerk, "From information security to cyber security," in *Computers & Security*. Elsevier, 2013, vol. 38, pp. 97–102, accessed on 5 April 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404813000801

[2] A. Dionysiou and E. Athanasopoulos, "Lethe: Practical Data Breach Detection with Zero Persistent Secret State," in *IEEE 7th European Symposium on Security and Privacy (EuroS&P)*, 2022, accessed on 5 April 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9797372

[3] M. Abadi and M. R. Tuttle, "A Semantics for a Logic of Authentication (extended abstract)," in *PODC '91: Proceedings of the tenth annual ACM symposium on Principles of distributed computing*, July 1991, pp. 201–216, accessed on 5 April 2023. [Online]. Available: https://dl.acm.org/doi/pdf/10.1145/112600.112618

[4] T. Kosiyatrakul, S. Older, and S. K. Chin, "A Modal Logic for Role-Based Access Control," in *Computer Network Security*, V. Gorodetsky, I. Kotenko, and V. Skormin, Eds. Berlin, Heidelberg: Springer, 2005, pp. 179–193, accessed on 5 April 2023. [Online]. Available: https://link.springer.com/chapter/10.1007/11560326_14

[5] E. Raggi, K. Thomas, and S. van Vugt, *Beginning Ubuntu Linux*, 6th ed. Apress, October 2011, accessed on 5 April 2023. [Online]. Available: https://learning.oreilly.com/library/view/beginning-ubuntu-linux/9781430236269/Chapter21.html

[6] F. Massacci, "Reasoning About Security: A Logic and a Decision Method for Role-Based Access Control," in *Qualitative and Quantitative Practical Reasoning*, D. M. Gabbay, R. Kruse, A. Nonnengart, and H. J. Ohlbach, Eds., 1997, pp. 421–435, accessed on 5 April 2023. [Online]. Available: https://link.springer.com/chapter/10.1007/BFb0035639

[7] International Telecommunication Union, "ITU-T Recommendation X.1205: Overview of Cybersecurity," April 2008, accessed on 5 April 2023. [Online]. Available: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[8] D. Basin, P. Schaller, and M. Schläpfer, *Applied Information Security: A Hands-on Approach*. Springer, October 2011, accessed on 5 April 2023.

[9] D. Gollmann, *Computer Security*. Wiley, September 2010, accessed on 5 April 2023. [Online]. Available: https://wires.onlinelibrary.wiley.com/doi/full/10.1002/wics.106

[10] Australian Cyber Security Centre (Australian Signals Directorate), "Access control," accessed on 5 April 2023. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/guidance/access-control

[11] A. Valenzano, "Industrial Cybersecurity: Improving Security Through Access Control Policy Models," *IEEE Industrial Electronics Magazine*, vol. 8, no. 2, pp. 6–17, June 2014, accessed on 5 April 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6839138

[12] N. Li and M. V. Tripunitara, "On safety in discretionary access control," in *2005 IEEE Symposium on Security and Privacy (S&P'05)*, 2005, pp. 96–109, accessed on 5 April 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1425061

[13] D. E. R. Denning, *Cryptography and Data Security*. Addison-Wesley, 1982, accessed on 5 April 2023. [Online]. Available: http://faculty.nps.edu/dedennin/publications/Denning-CryptographyDataSecurity.pdf

[14] U.S. National Institute of Standards and Technology (Computer Security Resource Center), "Role Based Access Control," accessed on 5 April 2023. [Online]. Available: https://csrc.nist.gov/projects/role-based-access-control

[15] L. Wang, D. Wijesekera, and S. Jajodia, "A logic-based framework for attribute based access control," in *FMSE '04: Proceedings of the 2004 ACM workshop on Formal methods in security engineering*, 10 2004, pp. 45–55, accessed on 5 April 2023. [Online]. Available: https://dl.acm.org/doi/10.1145/1029133.1029140

[16] J.-Y. Béziau, "Bivalence, Excluded Middle and Non Contradiction," January 2003, accessed on 5 April 2023. [Online]. Available: http://wwwa.unine.ch/unilog/jyb/newprincipleofbivalence.pdf

[17] K. Avijit, "A language for access control," July 2007, accessed on 6 April 2023. [Online]. Available: https://www.cs.cmu.edu/~rwh/papers/accctl/paper.pdf

[18] A. A. Elliott and G. S. Knight, "Role Explosion: Acknowledging the Problem," in *Software Engineering Research and Practice*, 2010, accessed on 6 April 2023. [Online]. Available: http://knight.segfaults.net/papers/20100502-AaronElliott-WOLRDCOMP2010Paper.pdf

[19] N. Baracaldo and J. Joshi, "A trust-and-risk aware RBAC framework: tackling insider threat," in *SACMAT '12: Proceedings of the 17th ACM symposium on Access Control Models and Technologies*, June 2012, accessed on 6 April 2023. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/2295136.2295168

[20] L. A. Zadeh, "Fuzzy Logic," 1988, accessed on 6 April 2023. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=53&tag=1

[21] E. D. Mares, *Relevant Logic: A Philosophical Interpretation*. Cambridge University Press, 2004.

[22] "Stanford Encyclopedia of Philosophy: Intuitionistic Logic," revised on 16 December 2022, accessed on 6 April 2023. [Online]. Available: https://plato.stanford.edu/entries/logic-intuitionistic

[23] S. K. Chin and S. Older, *Access Control, Security and Trust: A Logical Approach*. CRC Press, 2011, accessed on 5 April 2023. [Online]. Available: https://wires.onlinelibrary.wiley.com/doi/full/10.1002/wics.106

[24] M. Abadi, M. Burrows, B. Lampson, and G. Plotkin, "A calculus for access control in distributed systems," in *ACM Transactions on Programming Languages and System*, vol. 15, September 1993, accessed on 6 April 2023. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/155183.155225

Acknowledgements

During the process of writing this research proposal, the generative AI results produced by ChatGPT is taken as reference to gain directions for searching suitable reference materials, to refine the language, and to obtain guidance regarding LaTeX syntax and citation styles.