Automated Safety Analysis of Administrative Temporal Role-Based Access Control (ATRBAC) Policies using Mohawk+T

by

Jonathan Shahen

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Applied Science
in
Electrical and Computer Engineering

Waterloo, Ontario, Canada, 2016

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

This thesis consists of material that is published in the ACM Symposium on Access Control Models and Technologies (SACMAT) 2015, under the title of "Mohawk+T: Efficient Analysis of Administrative Temporal Role-Based Access Control (ATRBAC) Policies" [12] with the co-authors Jianwei Niu and Mahesh Tripunitara.

Abstract

Safety analysis is recognized as a fundamental problem in access control. It has been studied for various access control schemes in the literature. Recent work has proposed an administrative model for Temporal Role-Based Access Control (TRBAC) policies called Administrative TRBAC (ATRBAC). We address ATRBAC-safety. We first identify that the problem is **PSPACE**-complete. This is a much tighter identification of the computational complexity of the problem than prior work, which shows only that the problem is decidable. With this result as the basis, we propose an approach that leverages an existing open-source software tool called Mohawk to address ATRBAC-safety. Our approach is to efficiently reduce ATRBAC-safety to ARBAC-safety, and then use Mohawk. We have conducted a thorough empirical assessment. In the course of our assessment, we came up with a "reduction toolkit," which allows us to reduce Mohawk+T input instances to instances that existing tools support. Our results suggest that there are some input classes for which Mohawk+T outperforms existing tools, and others for which existing tools outperform Mohawk+T. The source code for Mohawk+T is available for public download [11].

Acknowledgements

I would like to thank my thesis advisor Mahesh Tripunitara for mentoring me and for co-authoring the paper that led to this thesis.

Table of Contents

List of Tables viii

List of Figures ix

1 Introduction 1

1.1 Prior work 4

1.2 Our work 5

2 ATRBAC-Safety 7

2.1 RBAC, ARBAC and ARBAC-Safety 7

2.2 TRBAC, ATRBAC and ATRBAC-Safety 9

3 ATRBAC-Safety is PSPACE-Complete 18

3.1 Expressive power of ATRBAC 20

4 The Reduction Toolkit 22

4.1 Compositions of Reductions 29

4.2 Reduction to AsaspTime-Nsa 29

4.3 Reduction to AsaspTime-Sa 29

4.4 Reduction to TredRole and TredRule 29

4.5 Reduction to Mohawk 30

5 Empirical Assessment **31**

6 Empirical Results **34**

7 Future Work **38**

8 Conclusions **39**

APPENDICES **40**

A Benchmark Results **41**

A.1 Large Images for Benchmark Class A 41

A.2 Large Image for Benchmark Class B and C 43

A.3 Large Image for Mohawk Benchmark 45

References **47**

List of Tables

5.1 Feature-support of the various existing tools, and our design choice for Mohawk+T. For Mohawk+T, we have chosen the most general version of a feature from amongst existing tools for ATRBAC-safety. We show also the support Mohawk offers. As a tool for ARBAC-safety only, Mohawk expectedly has no support for temporality. There is also no notion of enable/disable rules in ARBAC-safety. When we say "'true' only" for administrative roles, we mean that every rule is enabled in every state. 33

List of Figures

1.1 An example of the Start State component (referred to as *TUA*) of a TRBAC policy is the figure on top. We assume that no role is enabled. Ignoring the time periods on the edges gives us an example of the Start State component (referred to as *UA*) of an RBAC policy. Example ARBAC and ATRBAC administrative rules are in the table. Figure 1.2 and Figure 1.3 contain examples of safety queries. 2

1.2 An ARBAC safety query for the example in Figure 1.1. We ignore the labels on edges that pertain to time-intervals to get an example of *UA* in RBAC. The ARBAC safety query, "could Bob become a member of the role Consulting Physician?," is true. Alice first revokes him from the role Doctor and then assigns him to the role Consulting Physician. 3

1.3 An ATRBAC safety query for the example in Figure 1.1. The ATRBAC safety query "could Bob become a member of the role Consulting Physician between 8 am and noon?," is true, provided we adopt a version of the problem that does not require the Consulting Physician role to be enabled. The role Director is first enabled (shown shaded in the second state in the figure). This allows Alice to carry out administrative tasks. Alice then exercises the *t_can_revoke* rule so Bob is revoked from the Doctor role for 8 am – noon. She then is able to assign him to the Consulting Physician role for 8 am – noon. This last state-change is not shown in the above figure. "Could Bob become a member of the role Consulting Physician between 1 pm and 5 pm?," is an example of a safety query that is not true. 4

2.1 The relationship between RBAC, ARBAC, TRBAC and ATRBAC. TRBAC syntactically generalizes RBAC with temporal extensions. Similarly, ATRBAC syntactically generalizes ARBAC. ARBAC is used to administer RBAC, and ATRBAC is used to administer TRBAC. 8

4.1 The algorithm to break up input time-intervals into non-overlapping time-intervals is listed below. An example of an input and output is shown above. The algorithm is used by the non-deterministic Turing machine in Chapter 3, and as part of our Reduction Toolkit in Chapter 4. The algorithm takes as input S, a set of time-intervals. The algorithm is guaranteed to terminate as no entry is chosen more than once in Line (1), and at most a constant number of entries is added in Line (2) for every entry chosen in Line (1). The algorithm runs in time at-worst quadratic in the size of the input S because for every entry chosen in Line (1), each entry in S is broken up into at most a constant number of entries in Line (2). 27

4.2 Simple diagram showing which reductions are required to reduce from Mohawk+T's general version of ATRBAC to each version of ATRBAC from Ranise et al. [7] and Uzun et al. [13], and ARBAC from Mohawk. 28

6.1 Results on all tools for Benchmark Class (a). It comprises random input instances from a generator from Uzun et al. [13]. The curves interpolate averages, and the error-bars show the standard deviation. Larger images can be found: Figure A.1, Figure A.2, and Figure A.3. 34

6.2 Results for Benchmark Class (b) (two graphs to the left), and Benchmark Class (c) (right). These comprise input instances from the work of Ranise et al. [7]. Larger images can be found: Figure A.4, Figure A.5, and Figure A.6. 36

6.3 Trivially converted the Mohawk inputs [5] to ATRBAC-safety instances using one time-slot. Test Suite 1 is for inputs with non-negated preconditions only. Test Suite 2 is for inputs with no revoke rules. Test Suite 3 is for both positive and negated preconditions, and assign/revoke rules. Some of the curves are truncated because the corresponding tools crash at those inputs sizes and beyond. Larger images can be found: Figure A.7, Figure A.8, and Figure A.9. 37

A.1 Results on all tools for Benchmark Class (a). It comprises random input instances from a generator from Uzun et al. [13]. The curves interpolate averages, and the error-bars show the standard deviation. A larger version taken from Figure 6.1. 41

A.2 Results on all tools for Benchmark Class (a). It comprises random input instances from a generator from Uzun et al. [13]. The curves interpolate averages, and the error-bars show the standard deviation. A larger version taken from Figure 6.1. 42

A.3 Results on all tools for Benchmark Class (a). It comprises random input instances from a generator from Uzun et al. [13]. The curves interpolate averages, and the error-bars show the standard deviation. A larger version taken from Figure 6.1. 42

A.4 Results for Benchmark Class (b). These comprise input instances from the work of Ranise et al. [7]. A larger version taken from Figure 6.2. 43

A.5 Results for Benchmark Class (b). These comprise input instances from the work of Ranise et al. [7]. A larger version taken from Figure 6.2. 44

A.6 Results for and Benchmark Class (c). These comprise input instances from the work of Ranise et al. [7]. A larger version taken from Figure 6.2. 44

A.7 Results for inputs used in the empirical assessment of Mohawk [5]. We trivially converted the Mohawk inputs to ATRBAC-safety instances — there is one time-slot only. This graph is for inputs with non-negated preconditions only. Some of the curves are truncated because the corresponding tools crash at those inputs sizes and beyond. A larger version taken from Figure 6.3. . 45

A.8 Results for inputs used in the empirical assessment of Mohawk [5]. We trivially converted the Mohawk inputs to ATRBAC-safety instances — there is one time-slot only. This graph is for inputs with no revoke rules. Some of the curves are truncated because the corresponding tools crash at those inputs sizes and beyond. A larger version taken from Figure 6.3. 45

A.9 Results for inputs used in the empirical assessment of Mohawk [5]. We trivially converted the Mohawk inputs to ATRBAC-safety instances — there is one time-slot only. This graph is the hardest class, in which both negated and non-negated preconditions are allowed, as are revoke rules. Some of the curves are truncated because the corresponding tools crash at those inputs sizes and beyond. A larger version taken from Figure 6.3. 46

Chapter 1

Introduction

Access control deals with whether a principal may exercise a privilege on a resource; a user exercising a read privilege on a file. This is an important aspect of the security of a system. Whether an attempted access is permitted is customarily specified in a policy.

Effecting and intuiting the consequences of changes to an access control policy is called administration. An aspect of administration is **delegation**, with which a trusted administrator empowers another principal to change the policy in limited ways. Delegation is used so administrative efficiency can scale with the size of an access control system.

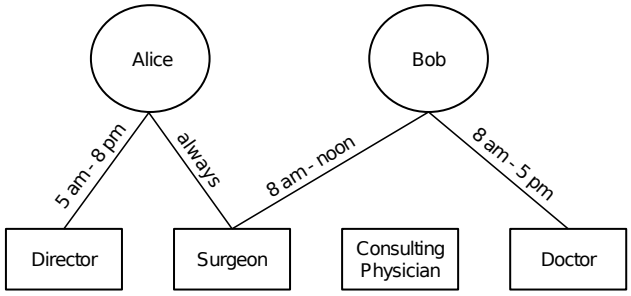
With delegation arises the need for safety analysis, which has been recognized as a fundamental problem in access control since the work of Harrison et al. [4]. The safety analysis problem takes three inputs:

(1) Start State – is an instance of an access control policy,

(2) State Change Rules – is the set of administrative rules by which a policy can change,

(3) Security Query – a statement that can judge if the system is secure; typically whether a particular user can obtain a particular privilege.

Safety Analysis returns 'TRUE' if the query can never become true, and 'FALSE' otherwise. That is, when the safety analysis returns 'FALSE', the system is deemed to be unsafe because there exists a reachable state in which the user indeed has the privilege. The reason is that the user's acquisition of the privilege is presumably undesirable.



Model	Rule Type	Rule
ARBAC	*can_assign*	⟨Director, Surgeon ∧ ¬Doctor, Consulting Physician⟩
	can_revoke	⟨Director, Doctor⟩
ATRBAC	*t_can_assign*	⟨Director, 8 am – 9 am, Surgeon ∧ ¬Doctor, 8 am – noon, Consulting Physician⟩
	t_can_revoke	⟨Director, 8 am – 9 am, true, 8 am – noon, Doctor⟩
	t_can_enable	⟨true, 6 am – 8 am, true, 8 am – 5 pm, Director⟩
	t_can_disable	*No Rules*

Figure 1.1: An example of the Start State component (referred to as *TUA*) of a TRBAC policy is the figure on top. We assume that no role is enabled. Ignoring the time periods on the edges gives us an example of the Start State component (referred to as *UA*) of an RBAC policy. Example ARBAC and ATRBAC administrative rules are in the table. Figure 1.2 and Figure 1.3 contain examples of safety queries.

An example of a security query is: *Can an 'External Consultant' user ever obtain read or write permissions to the Internal Documents Server?* A 'secure' policy would ensure that this state can never not occur by using the delegation rules provided in the policy.

Safety analysis has been addressed for various access control schemes in the literature. Our focus is safety analysis in the context of Administrative Temporal Role-Based Access Control (ATRBAC) [13]. ATRBAC is an administrative scheme for Temporal Role-Based Access Control (TRBAC). TRBAC is Role-Based Access Control (RBAC) with temporal-extensions. In RBAC, rather than assigning a user directly to a permission, we adopt the indirection of a role. A user is authorized to a role, which in turn is authorized to a permission. In TRBAC, a user's ability to use their permission is limited to within a certain time interval.

Furthermore, in TRBAC, a role may be annotated with time-intervals. The role is then

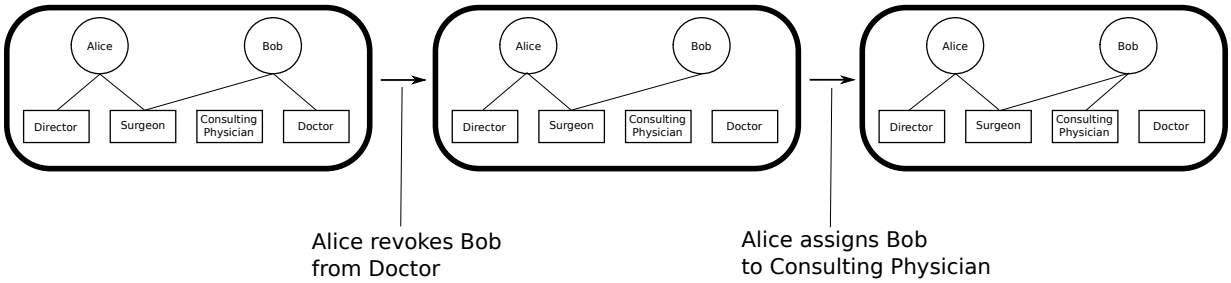


Figure 1.2: An ARBAC safety query for the example in Figure 1.1. We ignore the labels on edges that pertain to time-intervals to get an example of *UA* in RBAC. The ARBAC safety query, "could Bob become a member of the role Consulting Physician?," is true. Alice first revokes him from the role Doctor and then assigns him to the role Consulting Physician.

said to be active during those time-intervals. A user is able to exercise permissions she acquires via a role when the role is active only.

In Figure 1.1, we show an example of a TRBAC policy. It can be seen as an example of an RBAC policy by simply ignoring the references to time periods such as "5 am – 8 pm." We also show instances of administrative rules in ARBAC and ATRBAC syntax. We discuss ATRBAC more precisely in Chapter 2.1. ATRBAC is an extension of Administrative RBAC (ARBAC) [8]. ARBAC is used to administer RBAC, i.e., provides syntax for administrative delegation rules. ATRBAC specifies how two components of a TRBAC access control policy can change: (1) the temporal assignment of a user to a role, and, (2) the temporal activation/enablement of a role.

In the example in Figure 1.2, as the caption for the figure says, with the RBAC policy in the figure as the start-state, the ARBAC safety query, "could Bob become a member of Consulting Physician?" is true. However, the safety query, "could Bob simultaneously be a member of Consulting Physician and Doctor?" is false.

Also, for the example in Figure 1.3, with the TRBAC policy as the start-state, the ATRBAC-safety query, "could Bob become a member of Consulting Physician between 8 am and noon?" is true. The sequence of actions that must occur for that query to become true, however, is somewhat different from the ARBAC case. In particular, the Director role must first be enabled, as the *t_can_assign* and *t_can_revoke* rules that must be exercised to make that query true have Director as the administrative role.

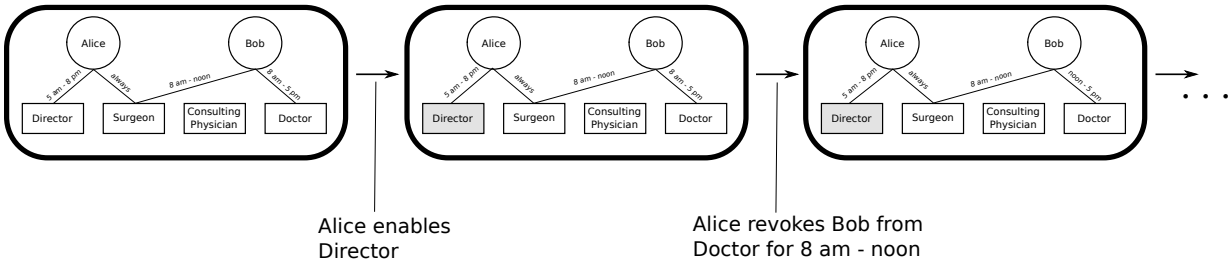


Figure 1.3: An ATRBAC safety query for the example in Figure 1.1. The ATRBAC safety query "could Bob become a member of the role Consulting Physician between 8 am and noon?," is true, provided we adopt a version of the problem that does not require the Consulting Physician role to be enabled. The role Director is first enabled (shown shaded in the second state in the figure). This allows Alice to carry out administrative tasks. Alice then exercises the *t_can_revoke* rule so Bob is revoked from the Doctor role for 8 am – noon. She then is able to assign him to the Consulting Physician role for 8 am – noon. This last state-change is not shown in the above figure. "Could Bob become a member of the role Consulting Physician between 1 pm and 5 pm?," is an example of a safety query that is not true.

1.1 Prior work

There is considerable prior work on safety analysis in various contexts. See, for example, the work of Harrison et al. [4]. It is beyond the scope of this paper to discuss all of those pieces of work. We are aware of two pieces of prior work on ATRBAC-safety. The work of Uzun et al. [13] is, to our knowledge, the first work to propose ATRBAC and pose the safety-analysis problem for it. In addition, that work discusses the design of two software tools, TredRole and TredRule to address instances in practice.

The work of Ranise et al. [7] syntactically generalizes some aspects of the version of ATRBAC from Uzun et al. [13]. It then presents a result on the computational-complexity of ATRBAC-safety — it proves that the problem is decidable. It then discusses the design, construction and evaluation of a different software tool, AsaspTime, to address problem instances in practice.

1.2 Our work

We make both theoretical and practical contributions in the context of ATRBAC-safety. We observe that prior work refers to a number of different versions of ATRBAC-safety. We carefully distinguish the various versions. This is important to validate prior claims regarding the non-existence of an efficient reduction from one version to another, and for a meaningful empirical assessment. For our theoretical analysis, for each feature of the problem, we adopt the more general form across the two versions from prior work [7, 13].

Our main theoretical result is a much tighter identification of the complexity-class in which ATRBAC-safety lies than prior work — we show that it is **PSPACE**-complete. **PSPACE** is the class of decision problems that can be solved by a (deterministic) Turing machine given space only polynomial in the size of the input.

We show the upper-bound, i.e., that the problem is in **PSPACE**, by constructing a non-deterministic Turing machine that decides instances and uses space only polynomial in the size of the input, and then leveraging the corollary to Savitch's theorem that **NSPACE** = **PSPACE** [10]. **NSPACE** is the class of decision problems that can be solved by a non-deterministic Turing machine given space only polynomial in the size of the input. We infer the lower-bound, i.e., that the problem is **PSPACE**-hard, by observing that ATRBAC generalizes ARBAC, and user-role safety in ARBAC is known to be **PSPACE**-hard [6].

Our result that ATRBAC-safety is **PSPACE**-complete is also of practical consequence. It immediately suggests to us an approach that we can use for instances that arise in practice — model-checking that is complete for **PSPACE**. Mohawk [5] is an open-source tool for ARBAC-safety that leverages a state of the art model checker, and has additional features that are customized for the ARBAC-safety problem. As ARBAC-safety is **PSPACE**-hard and ATRBAC-safety is in **PSPACE**, we know that there exists an efficient, i.e., polynomial-time, reduction from the latter to the former.

Mohawk has been shown to scale to problem-instances that comprise tens of thousands of roles and hundreds of thousands of administrative rules. A thesis we seek to validate empirically is that Mohawk can be extended via an efficient reduction from ATRBAC-safety to ARBAC-safety to address ATRBAC-safety with scalability similar to what it demonstrates for ARBAC-safety instances. We call the tool that we have constructed in this manner, Mohawk+T. The version of ATRBAC-safety that Mohawk+T supports is the most general for each feature across the different tools from prior work. Mohawk+T is available for public download [11].

We provide a thorough empirical assessment of Mohawk+T, and compare its perfor-

mance to tools from prior work*. The versions of the problem that the tools from prior work support are syntactically incomparable to one another. As we adopt the most general from across those tools for each feature for Mohawk+T, to be able to meaningfully empirically compare the different tools on the same inputs, we efficiently reduce the Mohawk+T version to the others. Towards this, we present a "reduction toolkit". The toolkit comprises mappings to efficiently reduce from a version of the problem to another.

A composition of steps from the toolkit is also an efficient reduction, and different such compositions reduce the version of the problem that Mohawk+T supports to the other versions. This includes the version of ARBAC-safety that Mohawk supports. In this manner, we are able to perform an apples-for-apples empirical comparison with prior tools.

*We thank the creators of the prior tools [7, 13] for making their tools available to us and helping us with their use. We thank also Ranise et al. [7] for making all of their inputs from their empirical assessment available to us.

Chapter 2

ATRBAC-Safety

In this section, we describe ATRBAC, and then pose the ATRBAC-safety problem. We do this in stages. We first introduce RBAC, ARBAC and a version of ARBAC-safety that is relevant to ATRBAC-safety. Then, we describe TRBAC, ATRBAC and ATRBAC-safety. Figure 2.1 shows the relationship between RBAC, ARBAC, TRBAC and ATRBAC.

We then clarify that various versions of ATRBAC- and ARBAC-safety are addressed in the literature, and discuss the choices we have made with regards to the various features of the problem. Specifically, that we have chosen the most general of each feature.

2.1 RBAC, ARBAC and ARBAC-Safety

ATRBAC addresses temporal extensions to RBAC and ARBAC. In this section we discuss RBAC, ARBAC and the version of safety analysis in ARBAC that we call ARBAC-safety that is relevant to our work on ATRBAC-safety.

RBAC RBAC is used to specify an authorization policy — who has access to what. An RBAC policy, in the context of this work, is a set UA, the user–role assignment relation. An instance of UA is a set of pairs of the form $\langle u, r \rangle$, where u is a user and r is a role. A user u is authorized to the role r if and only if $\langle u, r \rangle \in UA$. RBAC has other constructs, such as role-permission assignment and a role-hierarchy, that are not relevant to ATRBAC-safety with which we deal in this paper. Indeed, a role-hierarchy can be flattened as a pre-processing step without affecting the correctness or efficiency of our techniques.

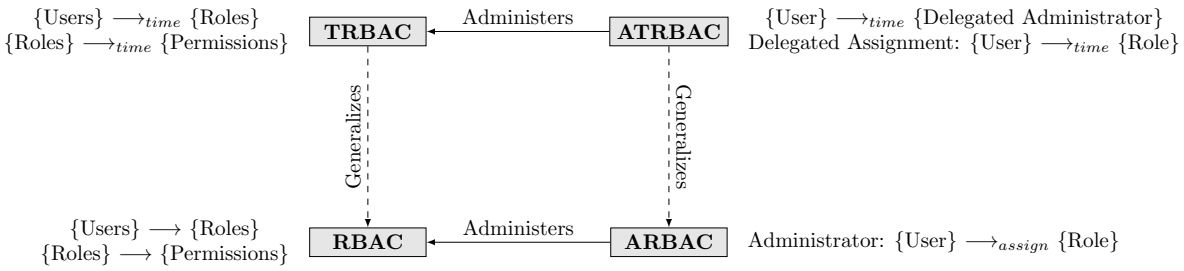


Figure 2.1: The relationship between RBAC, ARBAC, TRBAC and ATRBAC. TRBAC syntactically generalizes RBAC with temporal extensions. Similarly, ATRBAC syntactically generalizes ARBAC. ARBAC is used to administer RBAC, and ATRBAC is used to administer TRBAC.

ARBAC ARBAC is a syntax for specifying the ways in which an RBAC policy may change. As our work deals with the UA component of an RBAC policy only, by ARBAC we mean its URA portion [8], via which users are authorized to and revoked from roles.

There are only two ways in which an instance of UA may change. One is the addition of an entry $\langle u, r\rangle$ to UA, which is the authorization of u to r. The other is the removal of an entry $\langle u, r\rangle$, which is the revocation of u's authorization to r. An instance of ARBAC is a collection of *rules*, and addresses two issues with regards to such changes to UA: who may carry out one of those operations, and under what conditions.

A set of *can_assign* rules controls additions to UA, and a set of *can_revoke* rules controls removals from UA. A
can_assign rule is of the form $\langle a, C, t\rangle$, where a, t are roles and C is a precondition. The precondition C is a set in which each entry is either a role r, or its negation, $\neg r$. The semantics of the *can_assign* rule $\langle a, C, t\rangle$ is that a member of the role a may assign a user u to the role t provided u is already a member of every non-negated role in C and is not a member of any negated role in C.

In the *can_assign* rule in Figure 1.1 for example, a member of the role Director, e.g., Alice, may assign another user, e.g., Bob, to the role Consulting Physician provided he is already a member of the role Surgeon and is not a member of the role Doctor.

In a *can_assign* rule $\langle a, C, t\rangle$, the role a is called an administrative role and the role t is called a target role. A *can_revoke* rule has the form $\langle a, t\rangle$ where both a and t are roles. The semantics is that a member of the administrative role a is allowed to revoke a user's

authorization from the target role t. The reason that a *can_revoke* rule has no precondition is that revocation is seen as an inherently safe operation [8].

ARBAC-safety We now discuss a version of safety analysis in ARBAC that is relevant to our work. We call it ARBAC-safety. As our work deals with user-role authorization only, ARBAC-safety refers to that aspect only. More general versions of safety analysis for ARBAC have been considered in the literature [9], that reconcile not only the user-role authorizations, but also role-role relationships. Nevertheless, all the versions of safety analysis in ARBAC of which we are aware lie in the same complexity-class — they are all **PSPACE**-complete.

ARBAC-safety is a state-reachability problem. It takes three inputs:

(1) A *query*, which is a pair $\langle u, r \rangle$, where u is a user and r is a role.

(2) A current- or start-state, which is an instance of UA.

(3) A state-change specification, which is an instance of ARBAC, i.e., instances of *can_assign* and *can_revoke* rules.

The output of the ARBAC-safety instance is 'false,' if there exists a state that is reachable from the start-state in which the user u from the query is a member of the role r from the query. Otherwise, the output is 'true.' Figure 1.2 extends the example from Figure 1.1 with an example of ARBAC-safety.

ARBAC-safety is known to be **PSPACE**-complete [6]. Several techniques have been proposed to address instances that are likely to arise in practice. For example, Gofman et al. [3] propose a tool called RBAC-PAT, and Jayaraman et al. [5] propose a tool called Mohawk. We adopt the latter as the basis for the tool we build for ATRBAC-safety as it has been shown to scale well with the size of the input.

2.2 TRBAC, ATRBAC and ATRBAC-Safety

We now discuss the temporal extensions to RBAC and ARBAC that give us TRBAC and ATRBAC respectively. We discuss also the problem we address, ATRBAC-safety. We first present a model and encoding of time that is the basis for the syntax for temporality in ATRBAC. The version we adopt is the same as prior work [13].

Time An instant in time, m, can be thought of as represented by a real number. A time-slot represents some duration of time, and is represented as a non-negative integer. In an

instance of ATRBAC-safety, no two distinct time-slots overlap in time. Given time-slots i, j where $i < j$, the time-slot j is associated with a duration of time that occurs later than time-slot i. A time-instant m falls within a time-slot.

We assume that the earliest time-slot with which an instance of ATRBAC-safety is associated is 0, and there is some integer, $T_{\max}$, such that $T_{\max} - 1$ is the latest time-slot that pertains to the ATRBAC-safety instance. We discuss how time progresses under ATRBAC-safety below.

A generalization of a time-slot is a time-interval. A time-interval is a pair of integers $\langle i, j \rangle$ where $i \leq j$. It represents the set of time-slots $\{i, i+1, \ldots, j\}$. We say that a time-instant m falls within a time-interval if m falls within one of the time-slots in that time-interval.

The mindset that underlies the above notions for time is that each time-slot represents some realistic, recurring, fixed time period, such as "9 AM – 10 AM." The particular such actual time periods to which time-slots in an instance of ATRBAC-safety map is irrelevant to the analysis.

TRBAC From the standpoint of our work, TRBAC generalizes RBAC in two, temporal ways. (1) The set UA is generalized to TUA, each of whose elements is a triple $\langle u, r, l_{u,r} \rangle$, where $l_{u,r}$ is a time-interval. The semantics is that u is a member of r during the time-interval $l_{u,r}$ only. (2) Each role r that appears in TUA is annotated with a time-interval, l_r. We say that l_r is the time-interval during which the role r is active. The semantics is that outside of the time-interval l_r, no user can exercise a permission that she acquires via the role r. The set of all pairs, $\langle r, l_r \rangle$, is denoted RS.

Thus, a TRBAC policy, and therefore a state in the verification problem we consider, is a 3-tuple, $\langle TUA, RS, m \rangle$, where TUA and RS are as described above, and m is a time-instant. A user u is authorized to a role r at the time-instant, m, if and only if there exists an entry $\langle u, r, l_{u,r} \rangle \in TUA$ such that m is within $l_{u,r}$. The entries in RS matter when a user attempts to make an administrative change, i.e., a change to the authorization state. We discuss this under ATRBAC below.

ATRBAC ATRBAC generalizes ARBAC by providing rules for changes to TRBAC policies. As we discuss under "Versions of the problem" below, the version we discuss generalizes prior versions. Under ATRBAC, there are two ways in which a state, which is a TRBAC policy, can change: (1) via an administrative action, or, (2) the passage of time.

Under (1), four kinds of administrative actions are possible to a TRBAC policy, $\langle TUA, RS, m \rangle$. It is possible to add an entry to, and remove an entry from TUA, and

it is possible to add an entry to, and remove an entry from RS. The first two kinds of changes are called assign and revoke administrative actions, and the next two are called role enabling and disabling administrative actions. We have the corresponding sets of tuples *t_can_assign*, *t_can_revoke*, *t_can_enable*, and *t_can_disable*. (As in Uzun et al. [13], we employ the prefix "*t_*" to distinguish clearly that these are rules for ATRBAC, rather than ARBAC.)

Each such set contains 5-tuples. Each tuple is of the form $\langle C_a, L_a, C_t, L_t, t\rangle$. The first two components, C_a, L_a are conditions on the administrator that seeks to effect the action. The next two components, C_t, L_t, are conditions on the user or role to which the rule pertains. The last component, t, is the target-role; the role that is affected by the action. C_a is either the mnemonic 'true,' or a condition, i.e., a set of negated and non-negated roles. L_a is a set of time-intervals. We specify their semantics below for each kind of administrative rule. The entry t is the target role, i.e., the role that is affected by the firing of the rule. C_t is a role-condition similar to C_a above. There are some important differences between C_a and C_t, however, and we discuss these below for each kind of rule. L_t is a set of time-intervals, similar to L_a above. We discuss the semantics of L_t below for each kind of rule as well.

Such a 5-tuple $\langle C_a, L_a, C_t, L_t, t\rangle$ applies when an administrator, say, Alice, attempts an administrative action at a particular time-instant, m. Each administrative action takes inputs, one of which is the administrator that attempts it, i.e., Alice, and others that we discuss below.

Role enabling: the inputs are Alice, a target role t, and a set of time-intervals, L. Alice succeeds in her attempt at enabling the role t if and only if there exists an entry $\langle C_a, L_a, C_t, L_t, t\rangle \in$ *t_can_enable* for which all of the following are true.

(1) The time-instant, m, at which Alice attempts the action falls within some time-interval in L_a.

(2) Alice and the current time-instant m together satisfy the administrative condition, C_a. That is, if p is a non-negated role in C_a, then Alice is a member of p at time-instant m in the current state, $\langle TUA, RS, m\rangle$, and p is active at the time-instant m. If n is a negated role in C_a, then either Alice is not a member of n at time-instant m in the current state, or the role n is not active, or both. If C_a is the mnemonic 'true,' then the rule may fire provided m is within some time-interval in L_a.

(3) The set of time-intervals L is contained within the set of time-intervals L_t. That is, for every time-interval $l \in L$, there exists a time-interval $l_t \in L_t$ such that l is within l_t.

(4) The set of time-intervals L satisfies the target condition C_t for every $l \in L$. That is, if p is a non-negated role in C_t, then for every $l \in L$, p is active during the time-interval l, in the current-state, i.e., RS. And if n is a negated role in C_t, then for every $l \in L$, n is not active during l, in the current-state.

The effect of a successful role enabling by Alice is that the component RS of the current-state is updated as follows to get a new state: $RS \leftarrow RS \cup \{\langle t, l\rangle : l \in L\}$.

Example: In Figure 1.1 Alice must first enable the role of "Director" so that she can later be allowed to exercise rules where the "Director" role is required by the administrative condition, C_a. Alice may exercise the *t_can_enable* rule during 6 am – 8 am as she satisfies C_a during that time. Once she enables it, Alice must wait before she exercises the *t_can_revoke* rule, where the "Director" role is required by *t_can_revoke*'s C_a, until the current time falls within 8 am – noon.

Role disabling: the inputs are Alice, a target role t, and a set of time-intervals, L. Alice succeeds in disabling t via her action at time-instant m if and only if there exists an entry $\langle C_a, L_a, C_t, L_t, t\rangle \in$ *t_can_disable* for which all of the following are true.

(1) The current time-instant, m, falls within some time-interval in L_a.

(2) Alice and the current time-instant, m, together satisfy the administrative condition, C_a.

(3) The set of time-intervals, L, is contained within the set of time-intervals, L_t.

(4) The set of time-intervals L satisfies the target condition C_t for every $l \in L$.

The effect of a successful role disabling by Alice is that the component RS of the current-state is updated as follows to get a new state: $RS \leftarrow RS \setminus \{\langle t, l\rangle : l \in L\}$.

Example: Figure 1.1 does not provide a rule for *t_can_disable*. But an example case of this rule is to have a *t_can_disable* rule: ⟨true, 6 am – 6 pm, true, noon – 1 pm, Director⟩. This rule allows for the "Director" role to be disabled during lunch time, which means that no changes to *TUA* can be done during lunch. Exercising the *t_can_enable* rule after this *t_can_disable* rule will overwrite the changes and have the "Director" role enabled during noon – 1 pm.

User-role assignment: the inputs are the administrator, Alice, a user u, a target role t to which she seeks to assign u, and a set of time-intervals L. The assignment action that she

attempts at time-instant m succeeds if and only if there exists an entry $\langle C_a, L_a, C_t, L_t, t\rangle \in$ *t_can_assign* for which all of the following are true.

(1) The current time-instant, m, falls within some time-interval in L_a.

(2) Alice and the current time-instant, m, together satisfy the administrative condition, C_a.

(3) The set of time-intervals, L, is contained within the set of time-intervals, L_t.

(4) The user u and the set of time-intervals L satisfy the target condition C_t for every $l \in L$. That is, if p is a non-negated role in C_t, then u is a member of p during every time-interval $l \in L$. If n is a negated role in C_t, then u is not a member of n in any time-interval $l \in L$. If C_t is the mnemonic 'true,' then there are no constraints on the current role-memberships of the user u.

The effect of a successful assignment by Alice is that the component TUA of the current-state is updated as follows to get a new state: $TUA \leftarrow TUA \cup \{\langle u, t, l\rangle : l \in L\}$.

Example: The example in Figure 1.1 shows that Alice is able to assign the "Consulting Physician" role to Bob during 8 am – noon. She is able to exercise this rule because Bob has the role "Surgeon," and does not have the role "Doctor" during 8 am – noon, and Alice satisfies the administrative condition by having the role "Director."

User-role revocation: the inputs are an administrator Alice, a user u that she seeks to revoke from a role, a target role, t from which she seeks to revoke u, and a set of time-intervals, L. The revocation action she attempts at some time-instant m succeeds if and only if there exists an entry $\langle C_a, L_a, C_t, L_t, t\rangle \in$ *t_can_revoke* for which all of the following are true.

(1) The current time-instant, m, falls within some time-interval in L_a.

(2) Alice and the current time-instant, m, together satisfy the administrative condition, C_a.

(3) The set of time-intervals, L, is contained within the set of time-intervals, L_t.

(4) The user u and the set of time-intervals L satisfy the target condition C_t for every $l \in L$.

The effect of a successful revocation by Alice is that the component TUA of the current-state is updated as follows to get a new state: $TUA \leftarrow TUA \setminus \{\langle u, t, l\rangle : l \in L\}$.

Example: Alice may revoke Bob from the "Doctor" role during 8 am – noon using the *t_can_revoke* rule in Figure 1.1. If she does so, Bob retains membership of "Doctor" during noon – 5 pm, as we show in Figure 1.3.

Time-change: Another way that a state, $\langle TUA, RS, m\rangle$, can change is in its time component, m. The manner in which passage of time is modelled [7, 13] is simply by allowing the m component to increase without any change to the other two components, TUA and RS. That is, a possible state-change is from $\langle TUA, RS, m\rangle$ to a new state, $\langle TUA, RS, m'\rangle$, where $m' > m$.

An issue we clarify in this regard of passage of time is whether, once we reach the time-slot $T_{\max} - 1$ to which an instance of ATRBAC-safety pertains, the time-slot 0 recurs, followed by time-slot 1 and so on, forever. The assumption in prior work [13] is that it does. The reason regards the semantics of a time-slot — it maps to some realistic, recurring period of time. We refer to this property as periodicity, and revisit it in the context of the software tools.

Example: Time periodicity is what allows the rules in Figure 1.1 to be described by just the time of day. The intention of the rules is that they are contained within a day. Thus when a day ends and the next day begins, the rules should still apply to the new day.

ATRBAC-safety The safety analysis problem for ATRBAC takes three inputs. (1) A query, $\langle u, C, L, t\rangle$, where u is a user, C is a condition (set of negated and non-negated roles), L is a set of time-intervals and t is some units of time. (2) A start-state, $\langle TUA, RS, m\rangle$, which is an instance of TRBAC. (3) A state-change specification, which is an instance of ATRBAC, i.e., four sets of rules, *t_can_assign*, *t_can_revoke*, *t_can_enable*, and *t_can_disable*.

The output is 'false,' if there exists a TRBAC state $\langle TUA', RS', m'\rangle$ that is reachable from the start-state in which:

(i) the user u is a member of every non-negated role in C in every time-interval in L, and is not a member of any negated role in C in any time-interval in L,

(ii) every non-negated role in C is active for every time-interval in L, and no negated role in C is active in any time-interval in L, and,

(iii) the time-instant m' of this state is within t time-units of the time-instant of the start-state. Otherwise, the output is 'true.' We point out that it is possible to specify t

that is large enough that the query pertains to any time-slot that pertains to the problem instance.

In Figure 1.3 we discuss two ATRBAC safety questions: "could Bob become a member of the role Consulting Physician between 8 am and noon?" and "could Bob become a member of the role Consulting Physician between 1 pm and 5 pm?". As the caption of the figure discusses, the former is true, provided we do not require the role Consulting Physician to be enabled when Bob becomes a member of it. The latter question is not true.

Versions of the problem Prior work that is relevant to our work refers to different versions of ATRBAC-safety. We broadly classify the various versions along two axes. One comprises the versions that are discussed theoretically, i.e., in prose, assertions and proofs only. The other comprises versions supported by software tools.

Correspondingly, from the work of Uzun et al. [13] we have the versions of ATRBAC-safety that we call Tred–Theory, and the versions supported by their tools, TredRole and TredRule. They are so named because Ranise et al. [7] refer to their two software tools with the prefix Tred. Similarly, from Ranise et al. [7] we have AsaspTime–Theory, and the versions supported by their tools AsaspTime-Nsa and AsaspTime-Sa. The acronym "NSA" stands for Non-Separate Administration, and "SA" for "Separate Administration." They pertain to whether administrative roles are distinct from user roles. Finally, we refer to the version of ATRBAC-safety we discuss above as Mohawk+T–Theory. We also have the version that is supported by our tool, Mohawk+T.

We address the differences between AsaspTime–Theory and Tred–Theory, and our choices for Mohawk+T–Theory here. We address the differences between the versions of the software tools in Chapter 5. A recognition of the differences of the theoretical versions is important from two standpoints. One is that Mohawk+T–Theory syntactically generalizes both AsaspTime–Theory and Tred–Theory. Thus, an upper-bound for the computational complexity of ATRBAC-safety for Mohawk+T–Theory is an upper-bound for each of the other two as well.

Another reason a recognition of these different versions is important regards an assertion about the non-existence of an efficient reduction from AsaspTime–Theory to Tred–Theory in prior work [7]. As we point out in the next section on computational complexity, the assertion is in error.

The differences between AsaspTime–Theory and Tred–Theory pertain to (1) whether time-intervals are allowed, or only time-slots, (2) whether an administrative condition may

be specified in a rule, or an administrative role only, and, (3) the kind of query that may be specified in an instance of safety. The differences are the following.

1. AsaspTime–Theory allows time-slot only, and not time-intervals. Tred–Theory allows time-intervals. So, for this feature, AsaspTime–Theory is less general than Tred–Theory. We point out that naively encoding a time-interval as a set of time-slots is inefficient in the worst-case. Recall from our discussion above under "Time" that a time-interval is a set of consecutive time-slots $\{i, i+1, \ldots, i+n\}$, where $n \geq 0$. Encoding a time-interval as the pair $\langle i, i+n \rangle$ takes space $\leq 2\log(i+n)$ only. Encoding it as the set $\{i, i+1, \ldots, i+n\}$, however, takes space $\geq (n+1)\log(i)$. The latter is exponential in the former, in the worst-case.

2. AsaspTime–Theory allows a condition for the administrator in a rule, rather than an administrative role only. Tred–Theory allows an administrative role only. For this feature, therefore, AsaspTime–Theory generalizes Tred–Theory.

3. A query in AsaspTime–Theory is of the form $\langle u, C, L \rangle$ where u is a user, C is a role condition, and L is a set of time-slots. The semantics is: does there exist a reachable state in which (1) u satisfies C for L, i.e., is a member of every non-negated role for every time-slot in L and not a member of any negated role in C for any time-slot in L, and, (2) roles are enabled and disabled as C specifies for the time-slots in L.

   Tred–Theory proposes two kinds of queries. One is of the form $\langle u, r, L \rangle$, which asks whether u can become a member of r in all the time-intervals L. This is less syntactically general than AsaspTime–Theory in that C is allowed to be a role only, but more general in that L is allowed to be a set of time-intervals, and not only a set of time-slots. The other kind of query is of the form $\langle u, r, L, t \rangle$, which asks whether u can become a member of r in all the time-intervals in L within t time-units of the start-state. This syntactically generalizes the version of the safety problem that allows the first kind of query only — there is a straightforward reduction from the safety problem that allows the first kind of query only, to one that allows the second kind of query.

   Thus, from the standpoint of the query, the two versions are incomparable to one another.

For Mohawk+T–Theory that we describe earlier, for each of the three features above, we have chosen the more general. For example, the query allows a role condition, a set of time-intervals and the extra parameter t that limits the number of time units in which the

query must become true. Also, we assume that all possible users that are allowed to exist in the system are part of the TUA component in the start-state. (It is easy to incorporate users that are not assigned to any role into TUA. Create a "dummy" role that does not appear in any of the administrative rules and assign all users to it in the start-state.)

The reason we have adopted such a general version is to emphasize our complexity result that we present in the next section — such a choice has no consequence to the upper-bound computational complexity of ATRBAC-safety.

Chapter 3

ATRBAC-Safety is PSPACE-Complete

We now identify the computational complexity of ATRBAC-safety, for the version we call Mohawk+T–Theory. In Theorem 1 below, we identify an upper-bound. Then, in Theorem 2, we identify a tight bound. We then identify that all versions of ATRBAC-safety we address are **PSPACE**-complete. We then address the expressive power of ATRBAC and an assertion in prior work on the non-existence of a reduction.

Theorem 1 *ARBAC-safety for Mohawk+T–Theory is in* ***PSPACE****.*

The above theorem asserts an upper-bound on the hardness of safety analysis in ATRBAC. To prove it, we construct a non-deterministic Turing machine that terminates on every input with the correct 'safe' or 'unsafe' output, and runs with space only polynomial in the size of the input. Then, from the fact that **PSPACE** = **NSPACE**, which is a corollary to Savitch's theorem [10], we immediately infer that the problem is in **PSPACE**.

We point out that a similar non-deterministic Turing machine is constructed by Jha et al. [6] to show that their version of ARBAC-safety is in **PSPACE**. A main difference for us is that we need to reconcile the temporal aspect of ATRBAC-safety as well. Our non-deterministic Turing machine, M, is provided the three inputs:

(1) Query, $q = \langle u, C, L, t \rangle$,

(2) Start State, $\langle TUA, RS, m \rangle$, and,

(3) State Change rules in ATRBAC, i.e., the four sets *t_can_assign*, *t_can_revoke*, *t_can_enable* and *t_can_disable*.

M first assembles a set S of all the time-intervals (some of which may be time-slots) that appear in any of the three components of the input. M then breaks up the time-intervals in S so none of them overlaps with any other. It does this using the algorithm in Figure 4.1. The input set S is at worst linear in the size of the input ARBAC-safety instance. The output from the algorithm in Figure 4.1, call it S', is at worst quadratic in the size of input S – the caption in Figure 4.1 provides a reasoning.

The reason M does this is that it only has to maintain one of these time-intervals as the current time. The exact value of the current time, or even time-slot, no longer matters. For convenience, M could rewrite the input ATRBAC rules so each mentions only entries from S' and not S. M then maintains the following state:

(1) The current values for the sets TUA and RS.

(2) The current time-interval from S' within which the current time instant falls.

(3) The number of time units that have elapsed.

M performs its moves as follows. M first checks whether the query q is satisfied. It can do so from the state information it maintains. If yes, it halts with output 'unsafe.' If not, it checks whether it has exceeded t from the query q. If yes, it halts with output 'safe.' Otherwise, it assembles all the administrative rules that are enabled, i.e., for which the administrative and role conditions are met. It also includes an update of the current time-interval to the next time-interval as an option. It non-deterministically picks an option from those, updates its state, and continues.

M ensures that it terminates — we know that the input instance is unsafe if and only if the non-deterministic Turing machine halts with an output of 'unsafe' within 2^n transitions, where n is the size of the input. The Turing machine can keep a count of its transitions with space $\log_2(2^n) = n$. Thus, if M has not determined that the instance is unsafe after 2^n transitions, it outputs 'safe' and halts. We point out also that M maintains state that is at worst quadratic in the size of the input.

Theorem 2 *ATRBAC-safety for Mohawk+T–Theory is* ***PSPACE****-complete.*

We infer the above theorem from the fact that ARBAC-safety is **PSPACE**-hard [6]. As ATRBAC-safety forMohawk+T–Theory generalizes that version of ARBAC-safety, the **PSPACE**-hard lower bound applies to ATRBAC-safety for Mohawk+T–Theory as well. Given Theorem 1, we thus prove Theorem 2.

Theorem 3 *All the versions of ATRBAC-safety we consider in this paper are **PSPACE**-complete. They are: AsaspTime–Theory, Tred–Theory, Mohawk+T–Theory, and the versions supported by the tools AsaspTime-Nsa, AsaspTime-Sa, TredRole, TredRule, Mohawk+T, and Mohawk.*

To prove the theorem, we first observe that the version of ARBAC-safety, which can be perceived as a special case of ATRBAC-safety with only 1 time-slot, supported by Mohawk, is **PSPACE**-complete. We comment on this more in Chapter 5 under Item (4), "Admin role is 'true' only," in our Reduction Toolkit. All the other versions generalize the version supported by Mohawk, and therefore are **PSPACE**-hard. And, all the versions are at most as general as Mohawk+T–Theory, and therefore are in **PSPACE**.

3.1 Expressive power of ATRBAC

We can interpret the hardness of ATRBAC-safety as a measure of the expressive power of ATRBAC. The fact that ATRBAC-safety is no harder than ARBAC-safety, within a polynomial factor, suggests that ATRBAC is no more expressive than ARBAC.

Indeed, in this context, one can point to some seeming deficiencies in the syntax of ATRBAC. It is not possible, for example, to directly express a rule such as the following: "if a user is a member of the role Surgeon between 8 am and 9 am, then allow the user to be assigned to the role Consulting Physician between noon and 5 pm." The reason is that the set of time-intervals L_t in a rule $\langle C_a, L_a, C_t, L_t, t\rangle$ serves two purposes. It is used as a precondition to check the current temporal role-memberships of the user along with C_t, and, it is used to limit the time-intervals for which the user can acquire membership in the target role t.

A straightforward way to extend the syntax of ATRBAC to account for such use cases is to allow C_t to be a set of pairs, each of the form $\langle c, l\rangle$, where c is either a non-negated or negated role, and l is a time-interval. This separates the two purposes mentioned above. Nonetheless, ATRBAC-safety for this version of ATRBAC is also **PSPACE**-complete. That is, from the standpoint of computational complexity of safety analysis, nothing has changed. This means that this new version can be reduced efficiently to the original.

Another issue in this context regards an assertion from prior work [7] regarding the non-existence of an efficient reduction from AsaspTime–Theory to Tred–Theory. Theorem 3 invalidates the assertion. The erroneous reasoning in that work is that to support an administrative condition in an ATRBAC rule rather than only an administrative role, one must introduce exponentially many new roles.

An efficient reduction, however, can be constructed as follows. We introduce a new role for every administrative condition. Thus, the number of new roles is at worst linear in the ATRBAC-safety instance. We then introduce *t_can_assign* rules with the condition as a role precondition to assign a user to the new role. There are additional details we need which we omit here, for example to account for when a user no longer satisfies a condition in a future state.

Chapter 4

The Reduction Toolkit

There are some common transformations we effect in our efficient reductions from Mohawk+T to AsaspTime-Nsa, AsaspTime-Sa, TredRole/TredRule, and Mohawk. In this section, we discuss six mappings, each of which transforms some component of the problem efficiently (in polynomial time). Then, in subsequent sections, we mention which ones we need for each of the four reductions. Each of our reductions, from an input Mohawk+T to one of the other tools, is composed of a subset of transformations from our toolkit. As each of these transformations is an efficient reduction, so is any of those compositions. The compositions for each reduction is provided in Section 4.2, 4.3, 4.4, and 4.5.

Reduction (1) Query The safety query syntax provided by the AsaspTime-Nsa/Asasp Time-Sa, TredRole/TredRule, and Mohawk are all different thus we provide three kinds of mappings, which we call Type 1, 2, and 3.

Type 1 For AsaspTime-Nsa and AsaspTime-Sa, we need to map a Mohawk+T query $q = \langle R, l\rangle$ to a query $q' = \langle r', l'\rangle$, where r' is a single role while R is a set of roles. For this, we do the following. We first determine to what time-slot the time-slot l is mapped. This may be the result, for example, from applying Reduction (2) below, "time-intervals to time-slots." This mapped-to time-slot is l'. We create a new role r'. We add a *t_can_assign* rule, $\langle \text{true}, L'_{\text{all}}, r_1 \wedge \ldots \wedge r_n, l', r'\rangle$, where $R = \{r_1, \ldots, r_n\}$. And L'_{all} is the set of all mapped-to time-slots. Note that enumerating them does not affect the fact that the mapping is efficient. Now, our mapped-to query is $\langle r', l'\rangle$.

Type 2 For TredRole and TredRule, we need to map a Mohawk+T query, $q = \langle R, l\rangle$ to a query of the form $q' = \langle R'\rangle$. That is, a set of roles only. For this, we first do exactly what we do for AsaspTime-Nsa and AsaspTime-Sa. That is, we create a new role, r'. We

add a new *t_can_assign* rule: $\langle \text{true}, l_0 - l_{T_{\max}}, r_1 \wedge \ldots \wedge r_n, \{l\}, r' \rangle$, where $R = \{r_1, \ldots, r_n\}$. The mapped-to query is $q' = \langle \{r'\} \rangle$.

Type 3 For Mohawk, we need to map a Mohawk+T query $q = \langle R, l \rangle$ to a query $q' = \langle u', r' \rangle$, where u' is a user and r' is a single role. Assume that $R = \{r_1, \ldots, r_n\}$ and that set of roles maps to the non-temporal roles $\{\langle r_1, l \rangle, \ldots, \langle r_n, l \rangle\}$ by applying Reduction (5), "remove temporality." We create a new role r'. We add a *can_assign* rule, $\langle \text{true}, \langle r_1, l \rangle \wedge \ldots \wedge \langle r_n, l \rangle, r' \rangle$. We also ensure that a user u' exists in the system by specifying that as part of the input to Mohawk. Our output query is now $\langle u', r' \rangle$.

Reduction (2) Time-intervals to time-slots This reduction maps time-intervals to time-slots only. Recall from our discussion in Chapter 2.2 that naively enumerating the time-slots that comprise a time-interval is not efficient. For this reduction, we run the algorithm from Figure 4.1. We then adopt each time-interval in the output as a time-slot.

Run the algorithm in Figure 4.1. Let $i_1, \ldots, i_n$ be all the time-intervals, some of which may be time-slots, that appear in an input instance to Mohawk+T. We first reconcile overlapping intervals by breaking intervals up into largest possible intervals that do not overlap.

Now suppose the resultant set of intervals is $j_1, \ldots, j_k$. We associate each of these intervals with a time-slot in the output of the mapping. Note that this affects the query as well. That is, if $\langle R, l \rangle$ is the query in the input to Mohawk+T, the query $\langle r, l' \rangle$ in the output may be such that $l \neq l'$.

The example in Figure 4.1, the input is 5 time-intervals: $\{\langle 0, 3\rangle, \langle 1, 4\rangle, \langle 5, 8\rangle, \langle 6, 6\rangle, \langle 8, 10\rangle\}$. The output is 8 non-overlapping time-intervals: $\{\langle 0, 0\rangle, \langle 1, 3\rangle, \langle 4, 4\rangle, \langle 5, 5\rangle, \langle 6, 6\rangle, \langle 7, 7\rangle, \langle 8, 8\rangle, \langle 9, 10\rangle\}$. To represent the time interval $\langle 0, 3\rangle$, from the input set S, in non-overlapping time intervals we would use: $\{\langle 0, 0\rangle, \langle 1, 3\rangle\}$. Converting the non-overlapping time intervals to time-slots is trivial, as we have a strict ordering that we use as the time-slot ordering. The example 8 non-overlapping time intervals: $\{\langle 0, 0\rangle, \langle 1, 3\rangle, \langle 4, 4\rangle, \langle 5, 5\rangle, \langle 6, 6\rangle, \langle 7, 7\rangle, \langle 8, 8\rangle, \langle 9, 10\rangle\}$, gets trivially converted to 8 time-slots: $\{\langle 0, 0\rangle, \langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 4, 4\rangle, \langle 5, 5\rangle, \langle 6, 6\rangle, \langle 7, 7\rangle\}$.

Reduction (3) Remove *t_can_enable* and *t_can_disable* rules This reduction produces an output with no *t_can_enable* or *t_can_disable* rules. This is needed to map Mohawk+T inputs to AsaspTime-Sa, TredRole, TredRule, and Mohawk.

Our strategy behind eliminating *t_can_enable* and *t_can_disable* rules is to capture the constraints they represent in role-conditions in *t_can_assign* and *t_can_revoke* rules. For each role r, we introduce a new role r_e. The semantics of r_e is that the role r is enabled if

and only if r_e is assigned the user for whom we seek to exercise a *t_can_assign* or *t_can_revoke* rule. We need to also consider the enabling of the administrative role in a rule.

We transform rules as follows. We change a *t_can_assign* or *t_can_revoke* rule $\langle a, \cdot, C, \cdot, t\rangle$ to the rule $\langle a, \cdot, a_e \wedge C, \cdot, t\rangle$, if a is a role. If a is the mnemonic 'true,' then we do not add the extra role-condition 'a_e.'

We transform a *t_can_enable* rule $\langle a, \cdot, p_1 \wedge \ldots \wedge p_k \wedge \neg n_1 \wedge \ldots \wedge \neg n_m, \cdot, t\rangle$ as follows. In its place, we have a *t_can_assign* rule $\langle a, \cdot, a_e \wedge p_{1_e} \wedge \ldots \wedge p_{k_e} \wedge \neg n_{1_e} \wedge \ldots \wedge \neg n_{m_e}, \cdot, t_e\rangle$. Similarly, we change a *t_can_disable* rule with target role t to a *t_can_revoke* rule with target role t_e. As with *t_can_assign* and *t_can_revoke* rules above, if a is 'true,' then we do not add the extra role pre-condition 'a_e.'

There is special thought that goes into the role 'a_e.' Given a rule: $\langle a, ti_a, C, ti_t, t\rangle$, the administrator role a must be enabled and assigned for the time ti_a, the user that might receive the target role t must have the role-condition satisfied for time ti_t; ti_a and ti_t are time-intervals or time-slots. When $ti_a == ti_t$ no special thought is required and a_e can be added directly to the pre-condition.

When $ti_a \neq ti_t$, for any rule in the input, we require a_e to reflect the time-interval ti_a for each specific rule instance, i.e. a_{ti_a}.

For *t_can_assign* and *t_can_enable* rules, $\langle a, ti_a, C, ti_t, t\rangle$, we need to add a new *t_can_assign* rule: $\langle true, L_{all}, a \wedge a_e, ti_a, a_{ti_a}\rangle$. This rule properly reflects *t_can_enable* for the role a.

For *t_can_revoke* and *t_can_disable* rules, $\langle a, ti_a, C, ti_t, t\rangle$, we need to add 2 new *t_can_revoke* rules: $\langle true, L_{all}, a, ti_a, a_{ti_a}\rangle$, and $\langle true, L_{all}, a_e, ti_a, a_{ti_a}\rangle$. These two rules allow for removing the role a_{ti_a} if either a_e or a is removed. This properly reflects *t_can_revoke* and *t_can_disable* of the role a.

Reduction (4) Admin role is 'true' only In this version of the problem, a state-change rule must always be of the form $\langle$true, ...$\rangle$. (The specific format may be different from this, but the semantics is this.) AsaspTime-Sa, TredRole, and TredRule support only such rules. Mohawk also supports only 'true' for the administrative role in a rule, and furthermore, does not have the constraints related to time-intervals for the rule to fire. We first address the tools that support temporality, i.e., AsaspTime-Nsa, TredRole, and TredRule. Then we address Mohawk.

It may seem surprising that a reduction exists from Mohawk+T to this version of the problem. Indeed, Ranise et al. [7] do not attempt what they call Benchmark class (c) on TredRole and TredRule because those tools only support rules with 'true' for the

administrative role, unlike AsaspTime-Nsa. We point out the reduction in Jha et al. [6], that establishes that ARBAC-safety is **PSPACE**-hard, is to the version that requires only 'true' for the administrative role. More precisely, every rule in the ARBAC-safety instance produced by the reduction in that work has the same administrative role, which, at the start, is assigned a user that is distinct from the user in the query. This user-role membership does not change. Thus, every rule is enabled in every state, which is exactly the semantics of 'true' for the administrative role.

To reduce to a version that supports only such rules, we first apply the Reduction (3) "remove *t_can_enable* and *t_can_disable* rules" from above, so that the only rules we have are *t_can_assign* and *t_can_revoke* rules.

Then, we adopt the strategy of moving an admin role in a rule to a precondition. That is, what we broadly seek is to change a rule $\langle a, \cdot, C, \cdot, t\rangle$ to $\langle \text{true}, \cdot, a \wedge C, \cdot, t\rangle$. However, we need to be careful regarding situations such as the following. Suppose we have an admin role a that, to be assigned a user, has precondition role x. Then, we have a role q that appears in the query, and the only way to assign a user to q is with a rule that has admin role a and precondition $\neg x$.

Thus, if we have two different users, then one of them can act as admin, and the other as the user that is assigned to q to make the query true. However, if we have one user only, then q cannot be assigned a user. If we move an admin role to be a precondition role, then it is as though we seek to simulate a system with several users, using only one user. We deal with this by introducing new roles and rules. Our reduction is as follows. We replace the original input with the input we specify below.

Let $A = \{a_1, \ldots, a_{|A|}\}$ be the set of all admin roles, i.e., roles that appear as the first component of any rule. Let L be the set of all time-intervals (some of which may be time-slots) that appear in the input. For every role (i.e., both admin and non-admin roles), we create $|A| \cdot |L| + 1$ copies of it. We denote the copies using a subscript. That is, for $j = 0, \ldots, |A| \cdot |L|$, the j^{th} copy of role r from the original system is r_j. The j^{th} copy of a role r_i from the original input is designated $r_{i,j}$.

For the admin roles, we create an additional $|A| \cdot |L|$ copies. Designated as $a'_{i,j}$; the j^{th} such copy of the role a_i, for $j = 1, \ldots, |A| \cdot |L|$. Now, we make copies of the rules as follows.

Corresponding to subscript $j = 0$, we create copies of all *t_can_assign* and *t_can_revoke* rules, but for the 0^{th} copy of the roles. Then, we retain only those rules that have 'true' as the first component, i.e., the rules in which the admin role is the mnemonic 'true.' We do not include any other rules in the set of rules that corresponds to the index 0. That is, if we have a rule $\langle a, l_a, C, l_t, t\rangle$, we do not create a copy of this rule if $a \neq$ true. However, if

$a = \text{true}$, we create a copy $\langle \text{true}, l_a, C_0, t_0 \rangle$, where C_0 indicates every role r_i (negated and non-negated) in the precondition replaced by $r_{i,0}$.

For the remainder of the subscripts, $j = 1, \ldots, |A| \cdot |L|$, we make a copy of all the rules as follows. For a rule $\langle a_i, l_a, C, l_t, t \rangle$ in the original input, we create a rule $\langle \text{true},\ l_a,\ a'_{i,j} \wedge C_j,\ l_t,\ t_j \rangle$.

Finally, we add the following two sets of rules.

(i) For every $j = 1, \ldots, |A| \cdot |L|$, we add a *t_can_assign* rule $\langle \text{true},\ L_{\text{all}},\ a_{i,j-1},\ L_{\text{all}},\ a'_{i,j} \rangle$.

(ii) For every $j = 1, \ldots, |A| \cdot |L| - 1$, we add a *t_can_assign* rule $\langle \text{true}, L_{\text{all}}, a'_{i,j}, L_{\text{all}}, a'_{i,j+1} \rangle$.

Finally, consider that the query is $\langle R, l \rangle$ where $R = \{r_1, \ldots, r_k\}$. We adopt as query $\langle R_{|A|\cdot|L|}, l \rangle$ instead, where $R_{|A|\cdot|L|} = \{r_{1,|A|\cdot|L|}, \ldots, r_{k,|A|\cdot|L|}\}$.

The idea behind the above mapping is the following. If indeed the query can become true in the original system, then we require at most $|A| \cdot |L|$ administrators to make it true. Thus, the maximum number of users we need in the system is $|A| \cdot |L| + 1$. (The "+1" is the user that is assigned to roles to make the query true.) In the new system, we simulate the actions of all these users using a single user. The assignment of a, possibly distinct, administrator to an admin role a_i in the original system is simulated by assigning the single user to $a'_{i,j}$ for some j.

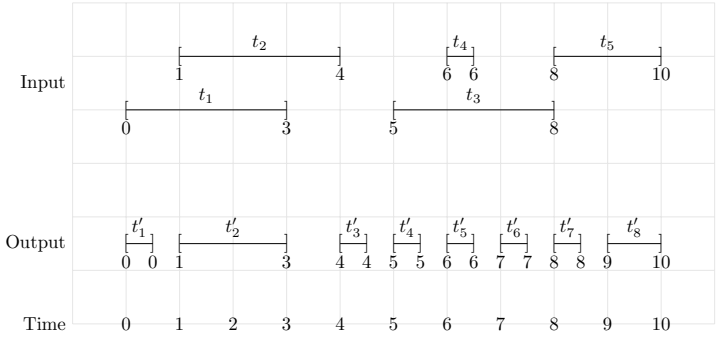
Reduction (5) Remove temporality Reduction (5) produces an output with no temporality. This can be seen as a version of the problem with one time-slot only. We need this to reduce to Mohawk's version, which is for ARBAC-safety. We map every entry in $R \times L$ to a role in Mohawk, where R is the set of all roles and L is the set of all time-intervals in the Mohawk+T input.

Suppose R is the set of all roles that appear in the input. This includes roles in the state-change rules, and the query (or goal). Also suppose that L is the set of all time-intervals (some of which may be time-slots) that appear in the input. We compute $R \times L$, where '$\times$' is the cartesian product of those two sets. We adopt $R \times L$ as our new set of roles.

We change the rules as follows. Suppose in the original input that allows temporality, we have $r \in R$, and $l \in L$. Then we denote as $\langle r, l \rangle$ the corresponding member of $R \times L$. Suppose we have a rule $\langle a,\ l_a,\ p_1 \wedge \ldots \wedge p_k \wedge \neg q_1 \wedge \ldots \wedge \neg q_j,\ l_t,\ t \rangle$, where l_a, l_t are time-intervals (either or both of which may be time-slots). Note that we have broken up the rules so that only one admin and one role-condition time-interval appears in the rule.

We replace this rule with the following rule: $\langle\langle a, l_a\rangle, \langle p_1, l_t\rangle \wedge \ldots \wedge \langle p_k, l_t\rangle \wedge \neg\langle q_1, l_t\rangle \wedge \ldots \wedge \neg\langle q_j, l_t\rangle, \langle t, l_t\rangle\rangle$.

If the administrative role, a, is the mnemonic 'true' in the original input, then we map this to $\langle \text{true}, \ldots\rangle$, immaterial of what l_a is. Similarly, if the role pre-condition is 'true,' then we map the rule to $\langle \cdot, \text{true}, \langle t, l_t\rangle\rangle$.



`Input: a set of time-intervals,` S

`1: From the entries of` S `that have not been considered before, pick one of smallest duration.`
`2: If any entry in` S `overlaps with the entry chosen in Line (1) other than itself, break it up into at most 3 non-overlapping entries and add those back to` S`.`
`3: If all entries have been considered, halt.`
`4: Else goto Line 1.`

Figure 4.1: The algorithm to break up input time-intervals into non-overlapping time-intervals is listed below. An example of an input and output is shown above. The algorithm is used by the non-deterministic Turing machine in Chapter 3, and as part of our Reduction Toolkit in Chapter 4. The algorithm takes as input S, a set of time-intervals. The algorithm is guaranteed to terminate as no entry is chosen more than once in Line (1), and at most a constant number of entries is added in Line (2) for every entry chosen in Line (1). The algorithm runs in time at-worst quadratic in the size of the input S because for every entry chosen in Line (1), each entry in S is broken up into at most a constant number of entries in Line (2).

Reduction (6) Remove pre-conditions in *can_revoke* rules ARBAC does not support role pre-conditions in *can_revoke* rules. That is, a *can_revoke* rule is of the form $\langle a, t\rangle$, where a is a role that acts as the administrative role for this rule, or the mnemonic 'true,' and t is the target role from which the user is to be revoked. There are no conditions on the user's current role memberships and non-memberships. However, this does not affect the fact that safety analysis in ARBAC is **PSPACE**-hard. As one would expect, Mohawk, which deals with ARBAC-safety, does not support pre-conditions on *can_revoke* rules.

We reduce the version of ARBAC-safety that supports pre-conditions in *can_revoke* rules, to one that does not, as follows. We first ensure that there is no rule in whose precondition we have both a role and its negation: $\langle \cdot, p \wedge \ldots \wedge \neg p, t\rangle$. If we have such a rule, we can simply remove it — it can never fire; i.e no user can have and not have a role p. Now, let $\langle a, C, t\rangle$ be a *can_revoke* rule in the original system. We map it as follows.

We change the rule to $\langle a, t\rangle$, which has the same meaning as $\langle a, \text{true}, t\rangle$. That is, a member of a can freely revoke users from t. Then, we introduce a new role that corresponds to t, call it t'. We introduce a new *can_assign* rule: $\langle a, \neg t \wedge C, t'\rangle$. We replace any occurrence of a role pre-condition $\neg t$ with the pre-condition $\neg t \wedge t'$.

The mindset behind the above reduction is that a user is considered to be assigned to t if he is a member of t, immaterial of his membership in t'. He is thought of as not assigned to t if he is not a member of t and is a member of t'.

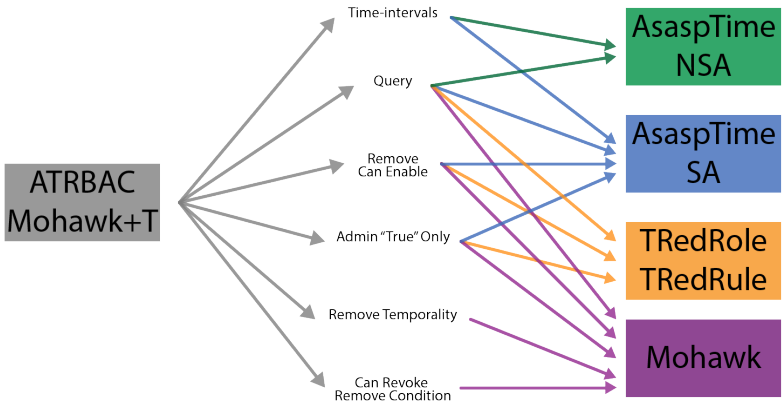


Figure 4.2: Simple diagram showing which reductions are required to reduce from Mohawk+T's general version of ATRBAC to each version of ATRBAC from Ranise et al. [7] and Uzun et al. [13], and ARBAC from Mohawk.

4.1 Compositions of Reductions

Figure 4.2 shows an overview of what reductions are required for each version of ATRBAC and ARBAC that we have considered in this work. Below is a more detailed list of the reductions and the order in which the reductions are executed.

4.2 Reduction to AsaspTime-Nsa

To reduce the Mohawk+T version to AsaspTime-Nsa, we need the following steps from the reduction tool-kit.

1. Reduction (2) Time-intervals to time-slots
2. Reduction (1) Query, Type 1

4.3 Reduction to AsaspTime-Sa

To reduce Mohawk+T to AsaspTime-Sa, we need the following steps.

1. Reduction (3) Remove *t_can_enable* and *t_can_disable* rules
2. Reduction (4) Admin role is 'true' only
3. Reduction (2) Time-intervals to time-slots
4. Reduction (1) Query, Type 1

4.4 Reduction to TredRole and TredRule

To reduce Mohawk+T to TredRole and TredRule, we need the following steps from the toolkit.

1. Reduction (3) Remove *t_can_enable* and *t_can_disable* rules
2. Reduction (4) Admin role is 'true' only
3. Reduction (1) Query, Type 2

4.5 Reduction to Mohawk

To reduce Mohawk+T to Mohawk, we need the following steps from the toolkit.

1. Reduction (3) Remove *t_can_enable* and *t_can_disable* rules
2. Reduction (4) Admin role is 'true' only
3. Reduction (1) Query, Type 3
4. Reduction (5) Remove temporality
5. Reduction (6) Remove pre-conditions in *can_revoke* rules

Chapter 5

Empirical Assessment

We have designed and built a software tool that we call Mohawk+T for ATRBAC-safety. Mohawk+T has been built as a wrapper to Mohawk [5], an open-source tool for ARBAC-safety. Mohawk reduces ARBAC-safety to model-checking and employs an off-the-shelf model checker, NuSMV [1]. In addition, Mohawk employs within it domain-specific heuristics called abstraction-refinement and bound-estimation for increased efficiency. The empirical results that have been reported for Mohawk suggest that it scales well for large input instances, for example, $40,000$ roles and $200,000$ rules.

Our intent here is to validate the thesis that we can wrap Mohawk in a manner that we preserve its scalability for ATRBAC policies. Thus, Mohawk+T would scale significantly better than what has been shown for existing tools for ATRBAC-safety [7, 13]. The manner in which Mohawk+T wraps Mohawk is an efficient reduction from ATRBAC-safety to ARBAC-safety. That is, given as input an instance of ATRBAC-safety, the wrapper in Mohawk+T maps this to an instance of ARBAC-safety that it provides as input to Mohawk. The mapping is a reduction, and therefore Mohawk's 'safe' or 'unsafe' output can immediately be adopted as Mohawk+T's output.

We had to address some technical challenges in realizing and assessing Mohawk+T. One is that we had to choose a version of ATRBAC-safety that Mohawk+T would support. So far in this paper, we have discussed what we have called theoretical versions of ATRBAC-safety. None of the prior tools, AsaspTime-Nsa, AsaspTime-Sa, TredRole and TredRule supports its corresponding theoretical version. AsaspTime-Nsa, for example, supports administrative roles only, and not administrative conditions. Another example is that TredRole allows only a set of time-slots, and not a time-interval, as the role condition.

As with their theoretical counterparts, the two sets of existing tools are incomparable

to one another from the standpoint of generality. We have investigated the various features that the existing tools allow for their input, and chosen for Mohawk+T the more general for each feature. We discuss this in more detail below.

Another technical challenge we had to address is that we had to devise an efficient reduction from the version of ATRBAC-safety that Mohawk+T supports to the version of ARBAC-safety that Mohawk supports. In this context, we point out that Mohawk also has a corresponding theoretical version [6] that is more general. Mohawk, for example, allows only 'true' for the administrative role in a rule. We discuss our reduction in Chapter 5, once we introduce our Reduction Toolkit.

We devised our Reduction Toolkit not only to reduce the version of ATRBAC-safety that Mohawk+T supports to the version of ARBAC-safety that Mohawk supports, but also so we can conduct a meaningful empirical comparison with existing tools for ATRBAC-safety. As Mohawk+T syntactically generalizes all existing tools, we cannot directly provide as input to an existing tool an input designed for Mohawk+T.

So we can perform apples-for-apples comparisons on inputs, we have devised and implemented efficient reductions from the version of ATRBAC-safety that Mohawk+T supports to the version that each of the existing tools supports. Thus, we need 4 reductions in total — to (1) AsaspTime-Nsa, (2) AsaspTime-Sa, (3) TredRole and TredRule, and, (4) Mohawk. We observed that the reductions have commonalities, which motivated us to devise our Reduction Toolkit. Composing particular reductions from the toolkit provides us with each of the 4 reductions we seek.

Versions that tools support Table 5.1 expresses the support for various features in existing tools, and our design choice for Mohawk+T. We list only those features for which the tools differ. As the table shows, for Mohawk+T, we have chosen the most general for each feature in existing tools. We show in the table also the support in Mohawk. We show this to indicate what our reduction from Mohawk+T's version of ATRBAC-safety must address. We point out, in addition to the information in the table, that none of the existing tools for ATRBAC-safety supports administrative conditions. They also do not support periodicity of time. Therefore, neither does Mohawk+T. These are features that are supported by the theoretical versions we discuss earlier in the paper.

	Time-intervals or time-slots only	Enable/ Disable rules supported	Query	Administrative roles supported or 'true' only
AsaspTime Nsa	Time-slots only	Yes	$\langle r, l\rangle$ — can some user become a member of r in time-slot l?	Yes
AsaspTime Sa	Time-slots only	No	$\langle r, l\rangle$ — see above	No — 'true' only
TredRole, TredRule	Allows time-interval in administrative condition	No	$\langle R\rangle$ — can the same user become a member of all roles in R in the same time-slot?	No — 'true' only
Mohawk+T	Allows time-interval in administrative condition	Yes	$\langle R, l\rangle$ — can the same user become a member of all roles in R in the time-slot l?	Yes
Mohawk	No temporal support	No	$\langle u, r\rangle$ — can the user u become a member of role r?	No — 'true' only

Table 5.1: Feature-support of the various existing tools, and our design choice for Mohawk+T. For Mohawk+T, we have chosen the most general version of a feature from amongst existing tools for ATRBAC-safety. We show also the support Mohawk offers. As a tool for ARBAC-safety only, Mohawk expectedly has no support for temporality. There is also no notion of enable/disable rules in ARBAC-safety. When we say "'true' only" for administrative roles, we mean that every rule is enabled in every state.

Chapter 6

Empirical Results

We have conducted empirical assessments on the three benchmark classes from prior work [7]. In addition, we have converted the input instances that were used in the empirical assessment of Mohawk [5] to ATRBAC-safety instances, and tried them as well on the tools. The conversion of Mohawk inputs is trivial — we adopt a single time-slot for the policy. Our results are shown in Figure 6.1, Figure 6.2, and Figure 6.3. The curves interpolate the average of 5 runs. The error-bars show the standard deviation from the average.

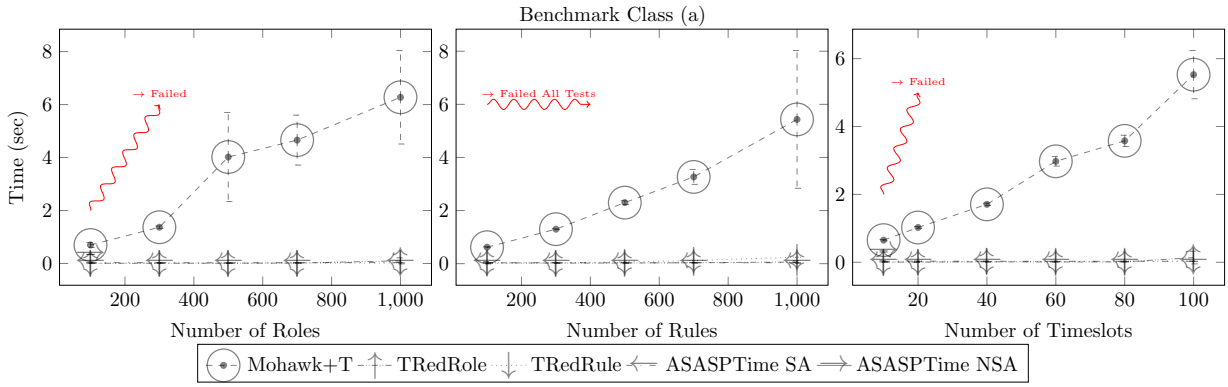


Figure 6.1: Results on all tools for Benchmark Class (a). It comprises random input instances from a generator from Uzun et al. [13]. The curves interpolate averages, and the error-bars show the standard deviation. Larger images can be found: Figure A.1, Figure A.2, and Figure A.3.

Benchmark Class (a) in Figure 6.1, first presented by Uzun et al. [13] but altered here, are randomized test-cases where:

- For the Roles subplot: the number of Rules are fixed at 200 and Timeslots at 20.
- For the Rules subplot: the number of Roles are fixed at 200 and Timeslots at 20.
- For the Timeslots subplot: the number of Rules and Roles are fixed at 200.

Everything about the rules created in the Benchmark Class (a) rules are randomized:

- Random start and end times for the administrator time-interval, where start $\leq$ end time.
- For every role that exists there is a $\frac{1}{5}$ chance that it will be added to the rule's pre-condition as a positive role condition, and $\frac{1}{5}$ chance for a negative pre-condition. These factors differ from the original code in [13] where there was an equal probability of $\frac{1}{3}$ for each case. The change is to reduce the number of role-pre-conditions is to allow for more rules that have zero pre-conditions, and thus are allowed to be executed. Without rules with empty pre-conditions the query will always be unreachable and thus a safe system.
- The target role is randomized.
- The target time-interval is a set of time-slots and there is a $\frac{1}{2}$ probability of a time-slot being added to the "role-schedule".
- The type of rule is randomized with a $\frac{1}{2}$ probability for *t_can_assign* or *t_can_revoke*.
- The administrator is "TRUE".

We observe that the results are mixed with regards to favouring Mohawk+T. For Benchmark Class (a), which is shown in Figure 6.1, the existing tools for ATRBAC-safety outperform Mohawk+T. Mohawk+T completes in a few seconds, while existing tools complete in less than a second each. Our investigation reveals that the policies in this benchmark are almost always safe, given the way they are generated. Mohawk's static slicing does a good job of paring large policies (e.g., 2,000 roles, 100,000 rules) down to a much smaller size (e.g., 150 roles and rules). However, its bound estimator estimates a bound that is linear in the number of roles for these policies, e.g., 150. While this is certainly much better than the worst-case estimate of 2^{150}, it still results in Mohawk+T taking several seconds.

Benchmark Class (b) in Figure 6.2, presented by Ranise et al. [7], are ARBAC policies that have "temporality" randomly added to them. We would like to thank Ranise et al.

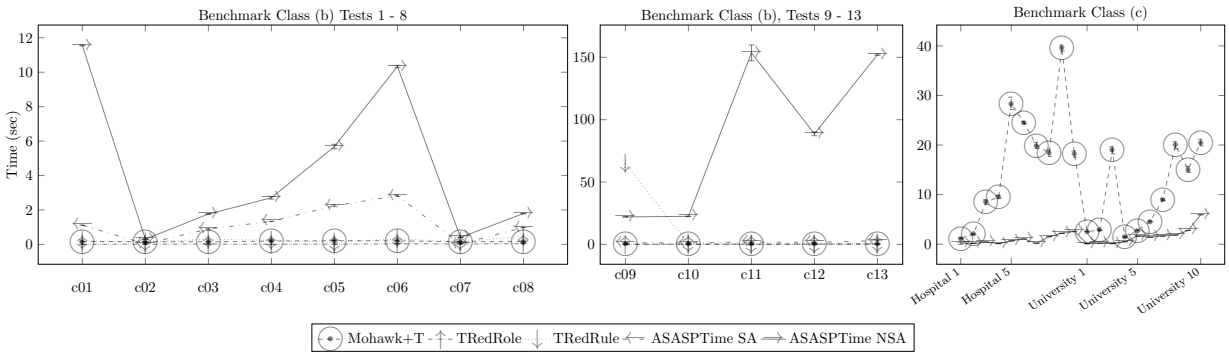


Figure 6.2: Results for Benchmark Class (b) (two graphs to the left), and Benchmark Class (c) (right). These comprise input instances from the work of Ranise et al. [7]. Larger images can be found: Figure A.4, Figure A.5, and Figure A.6.

for providing these test-cases for us to use. This set of 13 policies all have "TRUE" as the administrator and only contain *t_can_assign* and *t_can_revoke* rules.

Benchmark Class (c) in Figure 6.2, presented by Ranise et al. [7], is generated similarly to Benchmark Class (b) but these rules allow for arbitrary administrator roles.

In Figure 6.3, we present testcases taken from Jayaraman et al. [5], which are ARBAC policies and we trivially convert them to ATRBAC policies by introducing 1 time-slot and having every rule associate with that time slot. Given an example ARBAC rule: $\langle a, C, t\rangle$, we can trivially convert it with a single time-slot ts such that the policy still reflects it's original guarantees on safety: $\langle a, ts, C, ts, t\rangle$. The Mohawk test-cases are split into 3 complexity classes: polynomial time, NP-Complete, and PSPACE-Complete. This reflects what is contained within the test-cases:

- Polynomial Time: *can_assign* and *can_revoke* rules where the administrator is "TRUE", all pre-conditions for *can_assign* rules are positive or "TRUE", and *can_revoke* rule's pre-conditions are "TRUE".
- NP-Complete: *can_assign* rules where the administrator is "TRUE" and pre-conditions can include positive or negative roles, or be "TRUE".
- PSPACE-Complete: *can_assign* and *can_revoke* rules where the administrator is "TRUE" and pre-conditions can include positive or negative roles, or be "TRUE".

For Benchmark Class (b), shown in Figure 6.2, and Mohawk inputs, which is shown in Figure 6.3, however, Mohawk+T significantly outperforms the existing tools. Furthermore,

the existing tools are unable to withstand the input instances from Mohawk [5] beyond a certain threshold. For the polynomial-time verifiable sub-class, for example, which is Test Suite 1 in Figure 6.3, none of the existing tools is able to handle inputs beyond 20,000 roles and 80,000 rules.

For Benchmark Class (c), which is shown in Figure Figure 6.2, AsaspTime-Nsa outperforms Mohawk+T. Note that as in prior work [7], we did not try this Benchmark Class on the other existing tools.

Thus, we have the somewhat interesting situation that no single tool can be said to be good with all the input ATRBAC-safety instances we have tried. Further investigation is warranted to carefully identify the structure of input instances, and what features a universally good tool needs to have.

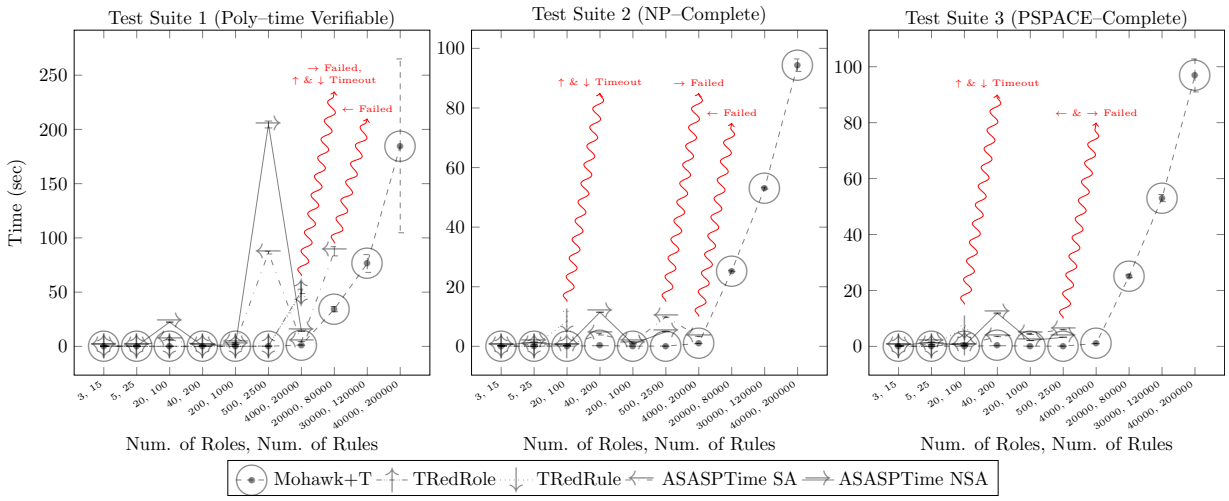


Figure 6.3: Trivially converted the Mohawk inputs [5] to ATRBAC-safety instances using one time-slot. Test Suite 1 is for inputs with non-negated preconditions only. Test Suite 2 is for inputs with no revoke rules. Test Suite 3 is for both positive and negated preconditions, and assign/revoke rules. Some of the curves are truncated because the corresponding tools crash at those inputs sizes and beyond. Larger images can be found: Figure A.7, Figure A.8, and Figure A.9.

Chapter 7

Future Work

Mohawk+T currently does two polynomial reductions to two separate PSPACE-Complete problems: the first is from ATRBAC-Safety to ARBAC-Safety, and the second is from ARBAC-Safety to a Model Checking. It would be interesting to see the performance increase from converting ATRBAC-Safety directly to a Model Checking.

For large test cases, Mohawk [5] performs abstraction-refinement to remove elements of the ARBAC-policy to reduce its size and keep the errors one sided. They also present bounded estimation that assures one sided errors for the model checker. This increases the performance of the model checker. Future work into adapting abstraction-refinement and bounded estimation for ATRBAC-Safety.

NuSMV has had some problems with performance that might be fixed by switching to nuXmv [2]. A comparison of performance would be interesting to see.

Chapter 8

Conclusions

We have addressed the safety analysis problem in the context of Administrative Temporal Role-Based Access Control (ATRBAC-safety). We have shown that the problem is **PSPACE**-complete, and also that various versions of the problem from the literature are **PSPACE**-complete. As the complexity class is the same as ARBAC-safety, we have investigated an approach to dealing with practical instances of ATRBAC-safety via a reduction to ARBAC-safety, and then leveraging an existing tool that has been shown to scale well — Mohawk. For an apples-for-apples comparison with existing tools, we have also come up with a Reduction Toolkit. Compositions of reductions from the toolkit allow us to reduce Mohawk+T's more general version of ATRBAC-safety to other versions. We have conducted a thorough empirical assessment. Our results are that there are some classes of inputs for which exiting tools outperform Mohawk+T, and others for which Mohawk+T outperforms existing tools.

APPENDICES

Appendix A

Benchmark Results

A.1 Large Images for Benchmark Class A

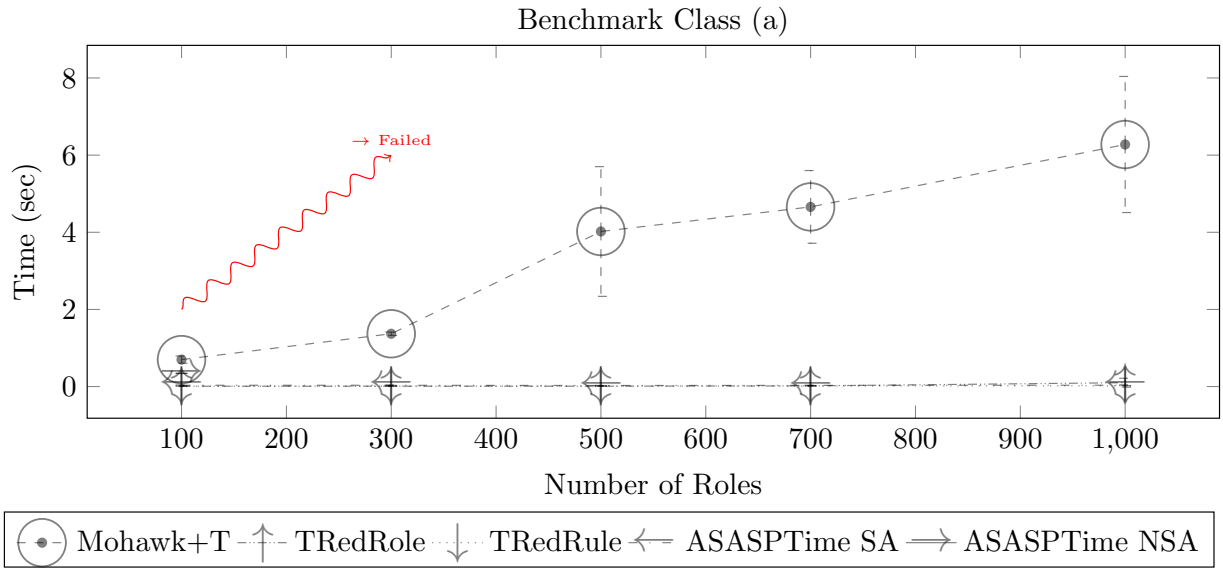


Figure A.1: Results on all tools for Benchmark Class (a). It comprises random input instances from a generator from Uzun et al. [13]. The curves interpolate averages, and the error-bars show the standard deviation. A larger version taken from Figure 6.1.

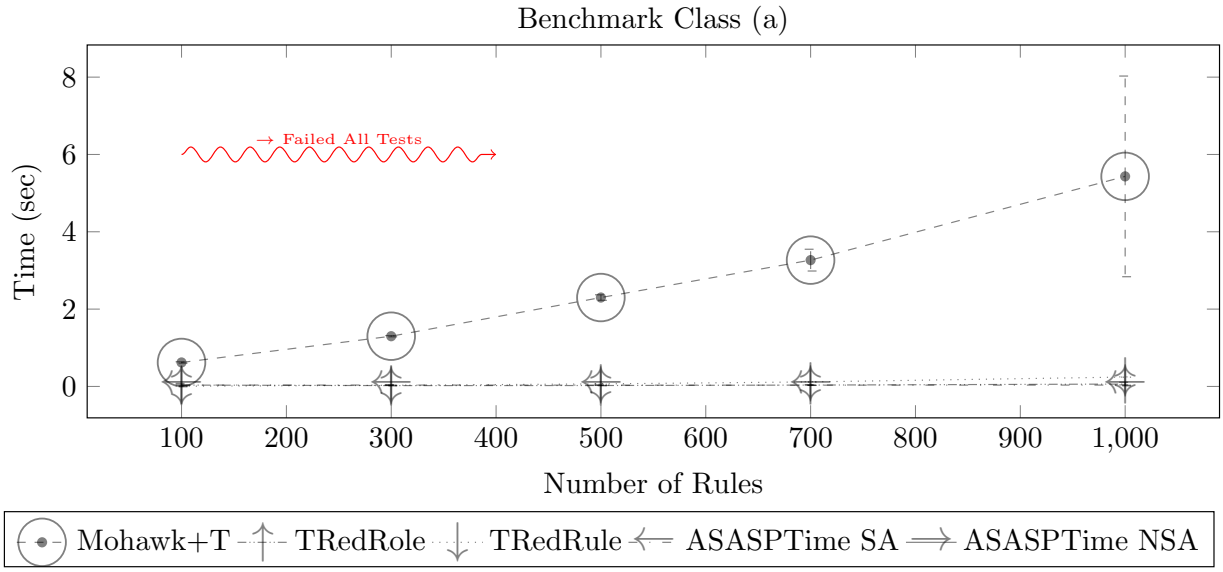


Figure A.2: Results on all tools for Benchmark Class (a). It comprises random input instances from a generator from Uzun et al. [13]. The curves interpolate averages, and the error-bars show the standard deviation. A larger version taken from Figure 6.1.

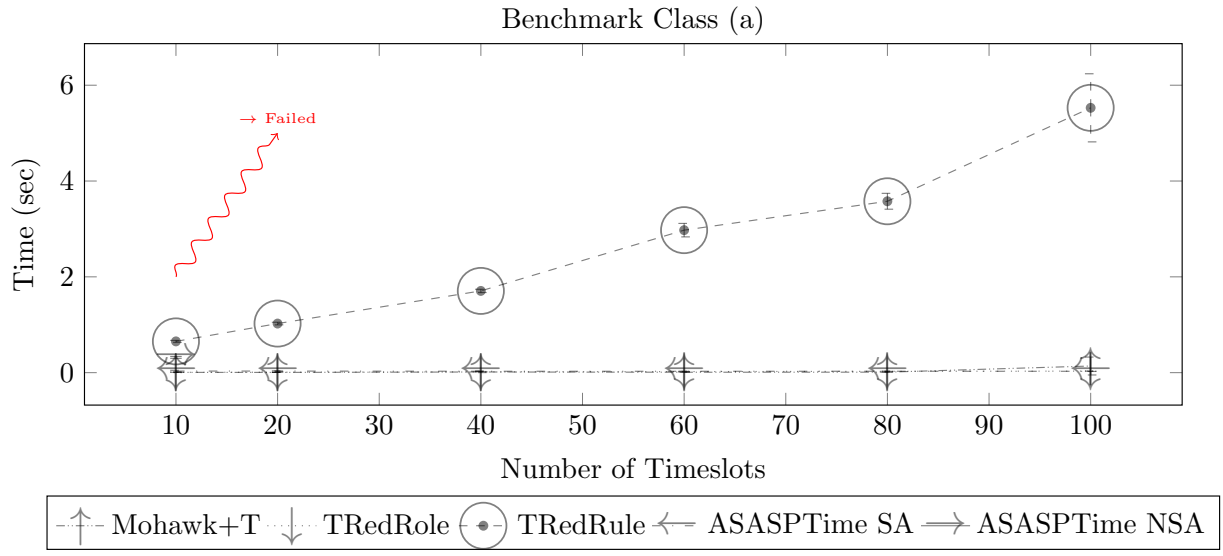


Figure A.3: Results on all tools for Benchmark Class (a). It comprises random input instances from a generator from Uzun et al. [13]. The curves interpolate averages, and the error-bars show the standard deviation. A larger version taken from Figure 6.1.

A.2 Large Image for Benchmark Class B and C

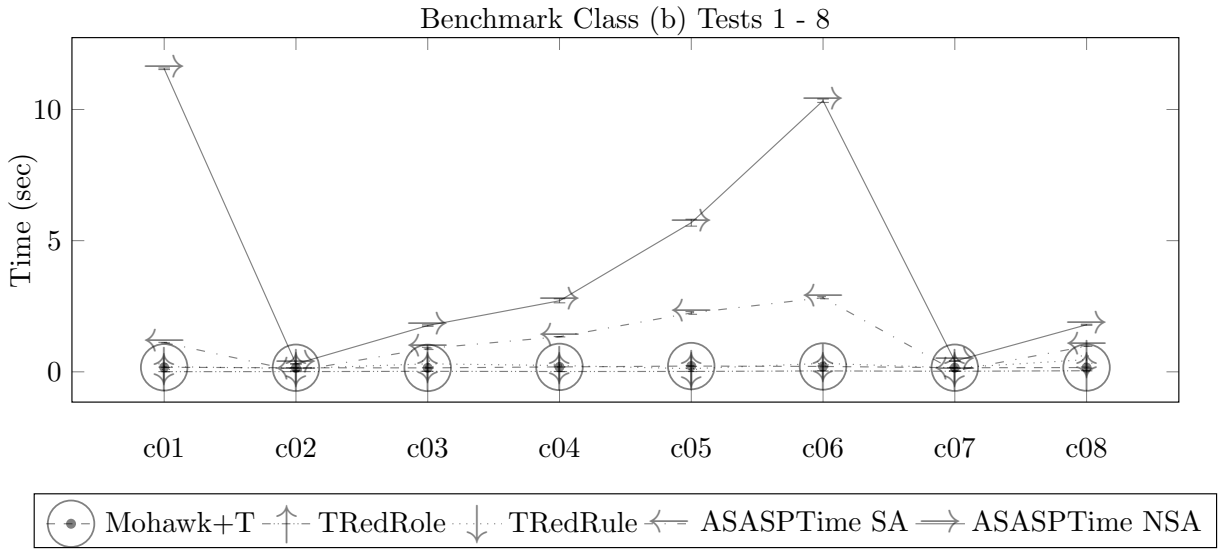


Figure A.4: Results for Benchmark Class (b). These comprise input instances from the work of Ranise et al. [7]. A larger version taken from Figure 6.2.

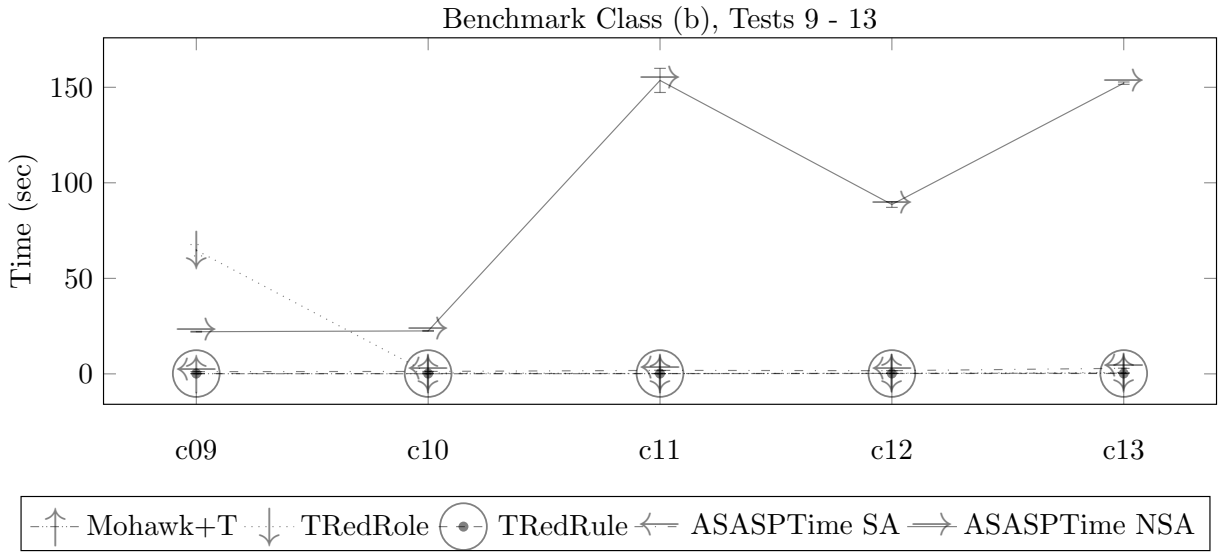


Figure A.5: Results for Benchmark Class (b). These comprise input instances from the work of Ranise et al. [7]. A larger version taken from Figure 6.2.

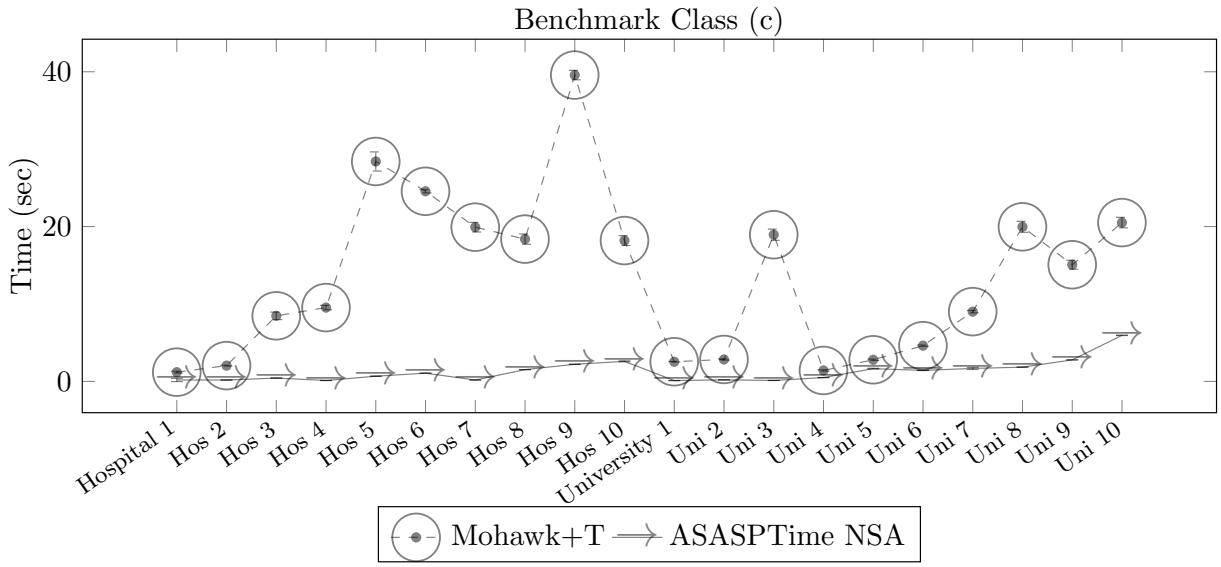


Figure A.6: Results for and Benchmark Class (c). These comprise input instances from the work of Ranise et al. [7]. A larger version taken from Figure 6.2.

A.3 Large Image for Mohawk Benchmark

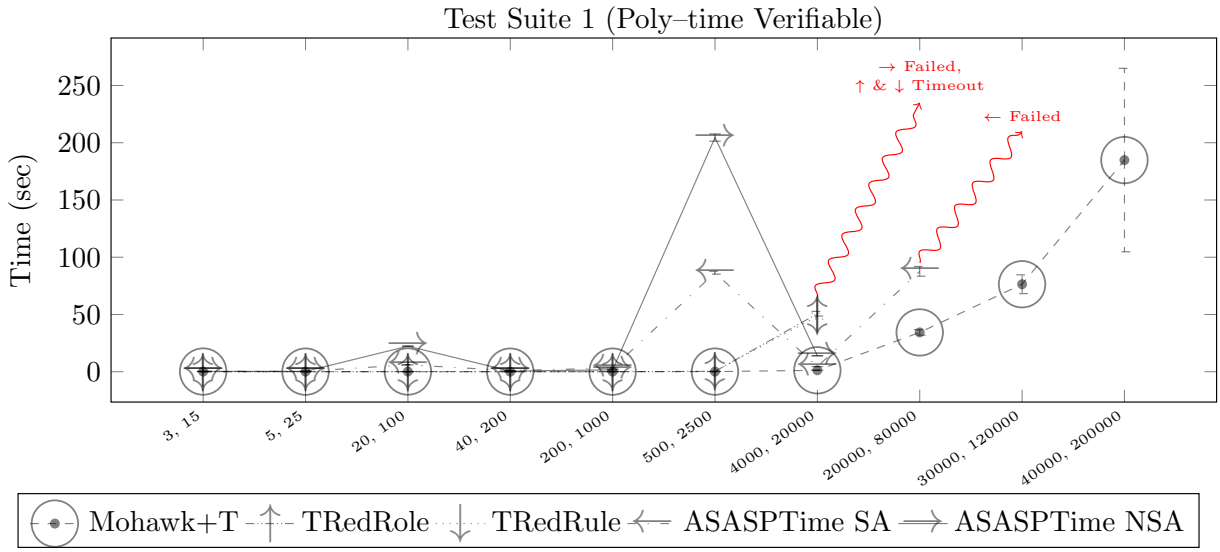


Figure A.7: Results for inputs used in the empirical assessment of Mohawk [5]. We trivially converted the Mohawk inputs to ATRBAC-safety instances — there is one time-slot only. This graph is for inputs with non-negated preconditions only. Some of the curves are truncated because the corresponding tools crash at those inputs sizes and beyond. A larger version taken from Figure 6.3.

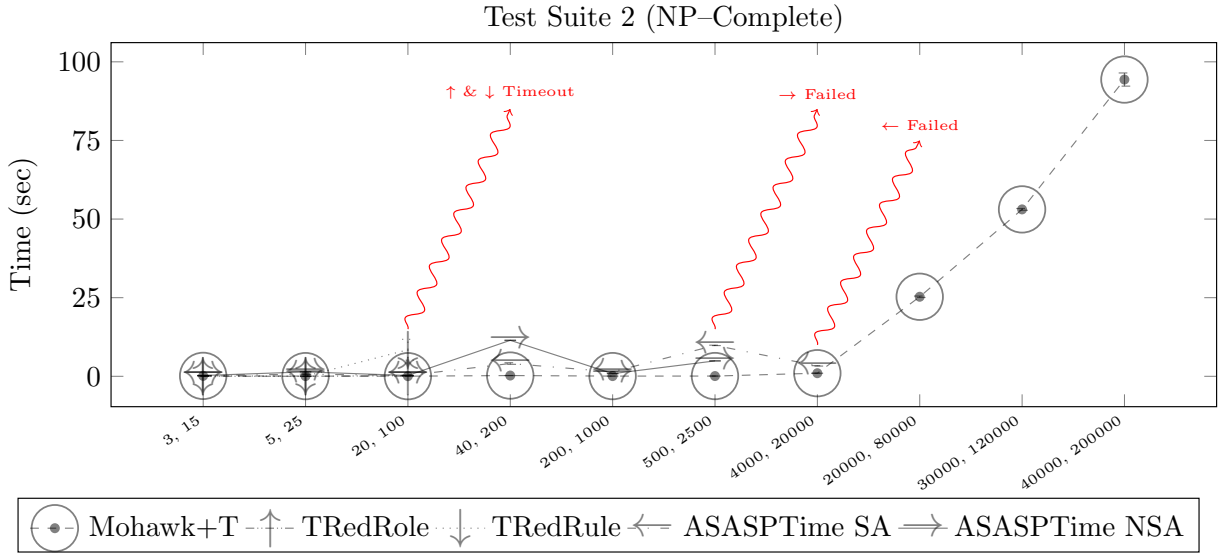


Figure A.8: Results for inputs used in the empirical assessment of Mohawk [5]. We trivially converted the Mohawk inputs to ATRBAC-safety instances — there is one time-slot only. This graph is for inputs with no revoke rules. Some of the curves are truncated because the corresponding tools crash at those inputs sizes and beyond. A larger version taken from Figure 6.3.

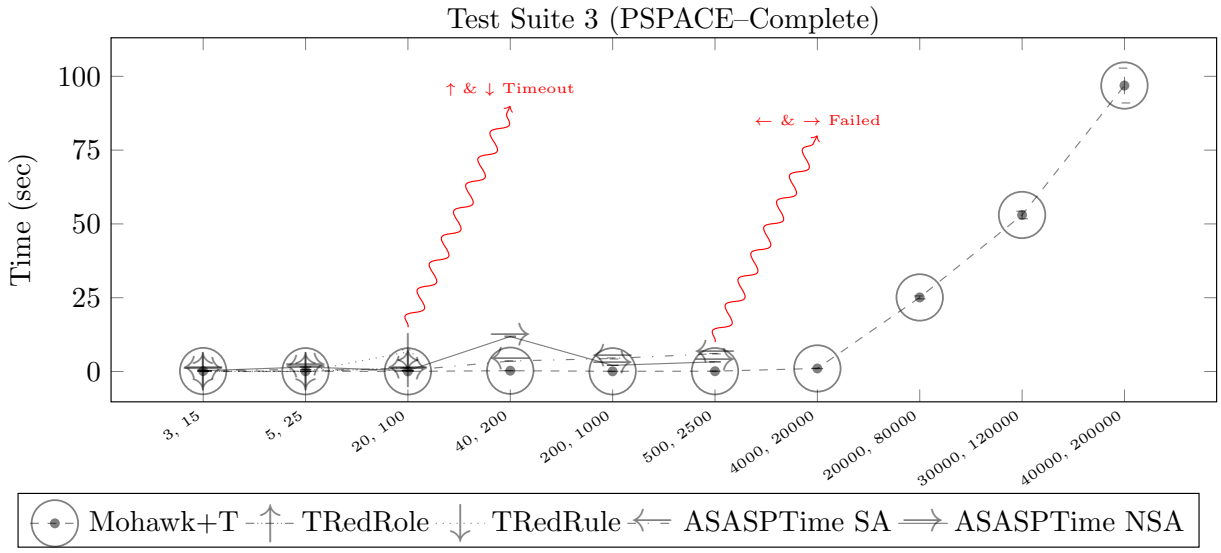


Figure A.9: Results for inputs used in the empirical assessment of Mohawk [5]. We trivially converted the Mohawk inputs to ATRBAC-safety instances — there is one time-slot only. This graph is the hardest class, in which both negated and non-negated preconditions are allowed, as are revoke rules. Some of the curves are truncated because the corresponding tools crash at those inputs sizes and beyond. A larger version taken from Figure 6.3.

References

[1] NuSMV. http://nusmv.fbk.eu/, Jun 2016.

[2] Roberto Cavada, Alessandro Cimatti, Michele Dorigatti, Alberto Griggio, Alessandro Mariotti, Andrea Micheli, Sergio Mover, Marco Roveri, and Stefano Tonetta. The nuxmv symbolic model checker. In *CAV*, pages 334–342, 2014.

[3] Mikhail I. Gofman, Ruiqi Luo, Ayla C. Solomon, Yingbin Zhang, Ping Yang, and Scott D. Stoller. *RBAC-PAT: A Policy Analysis Tool for Role Based Access Control*, pages 46–49. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[4] Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman. Protection in operating systems. *Commun. ACM*, 19(8):461–471, August 1976.

[5] Karthick Jayaraman, Mahesh Tripunitara, Vijay Ganesh, Martin Rinard, and Steve Chapin. Mohawk: Abstraction-refinement and bound-estimation for verifying access control policies. *ACM Trans. Inf. Syst. Secur.*, 15(4):18:1–18:28, April 2013.

[6] S. Jha, Ninghui Li, M. Tripunitara, Qihua Wang, and W.H. Winsborough. Towards formal verification of role-based access control policies. *Dependable and Secure Computing, IEEE Transactions on*, 5(4):242–255, Oct 2008.

[7] Silvio Ranise, Anh Truong, and Alessandro Armando. Scalable and Precise Automated Analysis of Administrative Temporal Role-based Access Control. In *Proceedings of the 19th ACM Symposium on Access Control Models and Technologies*, SACMAT '14, pages 103–114, New York, NY, USA, 2014. ACM.

[8] Ravi Sandhu, Venkata Bhamidipati, and Qamar Munawer. The arbac97 model for role-based administration of roles. *ACM Trans. Inf. Syst. Secur.*, 2(1):105–135, February 1999.

[9] Amit Sasturkar, Ping Yang, Scott D. Stoller, and C. R. Ramakrishnan. Policy analysis for administrative role based access control. *Theoretical Computer Science*, 412(44):6208–6234, October 2011.

[10] Walter J. Savitch. Relationships between nondeterministic and deterministic tape complexities. *Journal of Computer and System Sciences*, 4(2):177 – 192, 1970.

[11] Jonathan Shahen. Mohawk+T: Source Code. https://ece.uwaterloo.ca/~jmshahen/mohawk+t/, Jun 2015.

[12] Jonathan Shahen, Jianwei Niu, and Mahesh Tripunitara. Mohawk+t: Efficient analysis of administrative temporal role-based access control (atrbac) policies. In *Proceedings of the 20th ACM Symposium on Access Control Models and Technologies*, SACMAT '15, pages 15–26, New York, NY, USA, 2015. ACM.

[13] Emre Uzun, Vijayalakshmi Atluri, Shamik Sural, Jaideep Vaidya, Gennaro Parlato, Anna Lisa Ferrara, and Madhusudan Parthasarathy. Analyzing Temporal Role Based Access Control Models. In *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies*, SACMAT '12, pages 177–186, New York, NY, USA, 2012. ACM.