Evaluating Finite State Machine-Based Testing Methods on RBAC systems

Carlos Diego Nascimento Damasceno – damascenodiego@usp.br

Advisor: Prof. Dr. Adenilso da Silva Simão

Laboratory of Software Engineering – LabES

Institute of Mathematics and Computer Science – ICMC

University of Sao Paulo – USP

Sao Carlos – SP – Brazil

Agenda

1. Context, Motivation and Objectives
2. Role-Based Access Control (RBAC) Testing
3. Comparing FSM-Based Testing Methods on RBAC
4. Investigating Test Prioritization on RBAC
5. Conclusion, Limitations, Results and Future work

Context

- Software security is a *major requirement* of industrial-scale IT systems
  - Confidentiallity information
- Access control systems
  - Mediates user access to resources
  - Role-Based Access Control **(RBAC)**
    - Organizational roles ↔ Privileges assignment

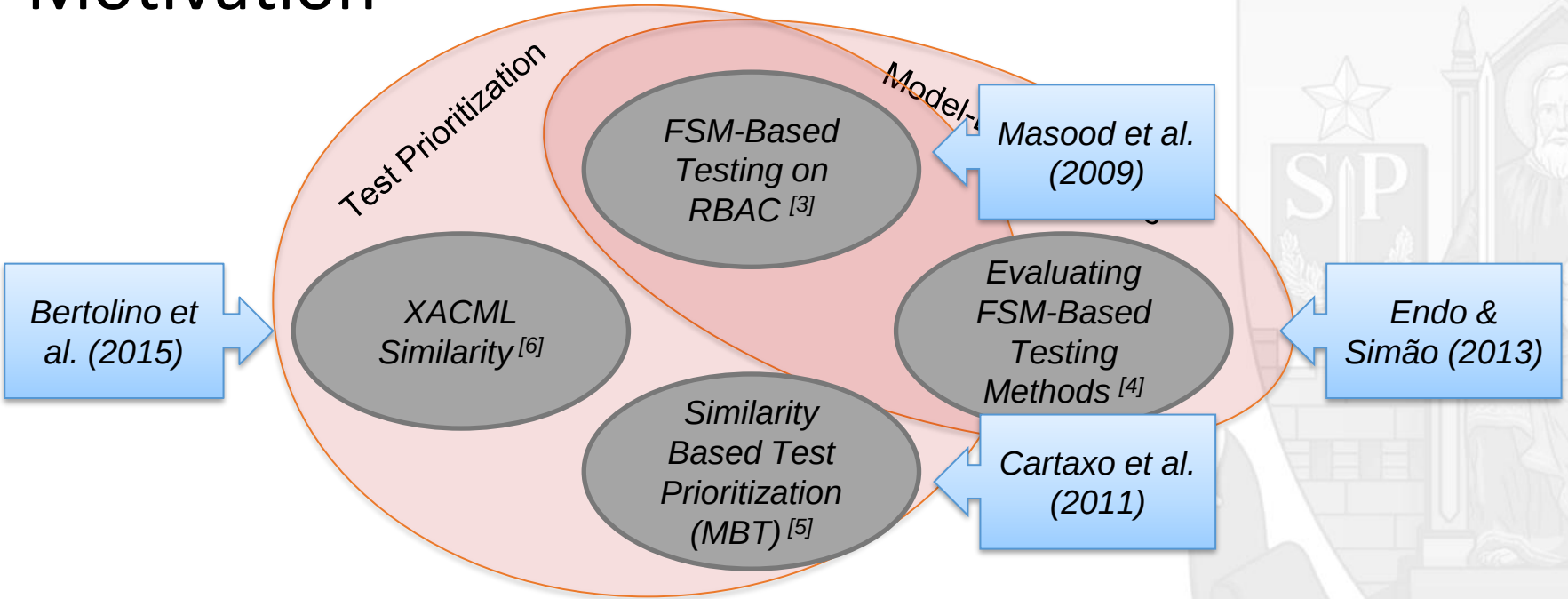
Motivation

- Faults on RBAC systems can threat user's privacy
- Software testing is necessary!
  - Model Based Security Testing
    - State based models (e.g. Finite State Machines - FSM) [1,2]

[1] FELDERER, M.; ZECH, P.; BREU, R.; BÜCHLER, M.; PRETSCHNER, A. Model-based security testing: a taxonomy and systematic classification. Software Testing, Verification and Reliability, p. n/a–n/a, 2015.

[2] **DAMASCENO, C. D. N.**; DELAMARO, M. E.; SIMÃO, A. d. S. Uma revisão sistemática em teste de segurança baseado em modelos. In: Anais do Workshop Brasileiro de Testes de Software Automatizados e Sistemático - CBSoft - Congresso Brasileiro de Software: Teoria e Prática. Porto Alegre: SBC, 2014. p. 31–40.

Motivation



[3] MASOOD, A.; BHATTI, R.; GHAFOOR, A.; MATHUR, A. P. Scalable and effective test generation for role-based access control systems. IEEE Transactions on Software Engineering, IEEE Press, Piscataway, NJ, USA, v. 35, n. 5, p. 654–668, Sep. 2009.

[4] ENDO, A. T.; SIMAO, A. Evaluating test suite characteristics, cost, and effectiveness of fsmbased testing methods. Information and Software Technology, v. 55, n. 6, p. 1045 – 1062, 2013.

[5] CARTAXO, E. G.; MACHADO, P. D. L.; NETO, F. G. O. On the use of a similarity function for test case selection in the context of model-based testing. Software Testing, Verification and Reliability, John Wiley & Sons, Ltd., v. 21, n. 2, p. 75–100, 2011.

[6] BERTOLINO, A.; DAOUDAGH, S.; KATEB, D. E.; HENARD, C.; TRAON, Y. L.; LONETTI, F.; MARCHETTI, E.; MOUELHI, T.; PAPADAKIS, M. Similarity testing for access control. Information and Software Technology, v. 58, p. 355 – 372, 2015.

Research Objectives

1. Compare recent and traditional FSM-based testing methods on RBAC domain
    a. Test characteristics and Effectiveness
        i. ***number of resets***, ***avg. test case length*** and ***test suite length***
        ii. ***RBAC fault domain***

Resemblance between FSMs expressing RBAC policies and random FSM models is unclear [1]

[4] ENDO, A. T.; SIMAO, A. Evaluating test suite characteristics, cost, and effectiveness of fsmbased testing methods. Information and Software Technology, v. 55, n. 6, p. 1045 – 1062, 2013.

Research Objectives

2. Investigate and compare test prioritization approaches for RBAC testing
    a. Similarity-based test prioritization for RBAC domain
        a. Simple similarity [5]
        b. XACML similarity [6]

Effectiveness of test criteria → Ability to represent specific-domain faults [1]

[1] FELDERER, M.; ZECH, P.; BREU, R.; BÜCHLER, M.; PRETSCHNER, A. Model-based security testing: a taxonomy and systematic classification. Software Testing, Verification and Reliability, p. n/a–n/a, 2015.

[5] CARTAXO, E. G.; MACHADO, P. D. L.; NETO, F. G. O. On the use of a similarity function for test case selection in the context of model-based testing. Software Testing, Verification and Reliability, John Wiley & Sons, Ltd., v. 21, n. 2, p. 75–100, 2011.

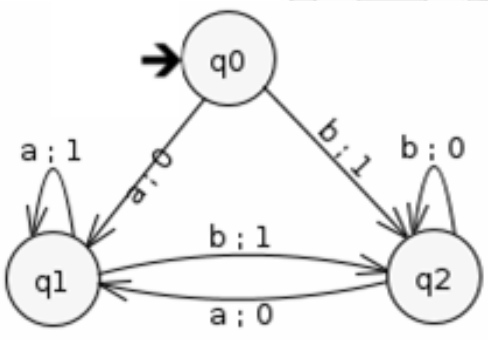
[6] BERTOLINO, A.; DAOUDAGH, S.; KATEB, D. E.; HENARD, C.; TRAON, Y. L.; LONETTI, F.; MARCHETTI, E.; MOUELHI, T.; PAPADAKIS, M. Similarity testing for access control. Information and Software Technology, v. 58, p. 355 – 372, 2015.

Role-Based Access Control Testing

Role-Based Access Control Testing

(FSM-Based Testing)

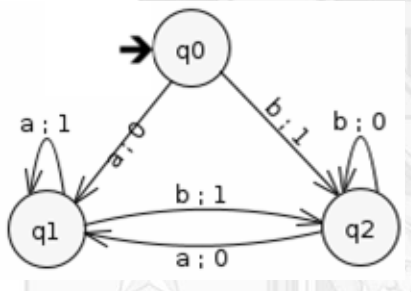
- Finite state machines (FSM) are widely used for modeling **reactive systems** [7]
- FSM-Based Testing → Check that an FSM behavior conforms to given specifications
- Mealy Machine is a 5-tuple M = <I , O , S , δ, λ>
- Mutation Analysis
  - Model faults in SUTs
  - Mutation operators
    - Represent typical faults



[7] BROY, M.; JONSSON, B.; KATOEN, J.-P.; LEUCKER, M.; PRETSCHNER, A. Model-Based Testing of Reactive Systems: Advanced Lectures (Lecture Notes in Computer Science). Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2005. I

Role-Based Access Control Testing

(FSM-Based Testing)



state \ input	a	b
q0	0	1
q1	1	1
q2	0	0

Characterization Set

- FSM-Based Testing Methods [7]
  - Traditional methods (W and HSI)
    - State and transition cover sets
    - Characterization set (W set) / Harmonized Identifiers (H_i)
  - Recent methods (SPY method)
    - Sufficient conditions and on-the-fly test sequence generation
      - Reduces test tree branching → On average 40% shorter than HSI
    - Higher fault detection effectiveness (underestimating extra states)
    - *Recent test methods rely on **fewer** and **longer** test cases **(random FSMs)**[4]*

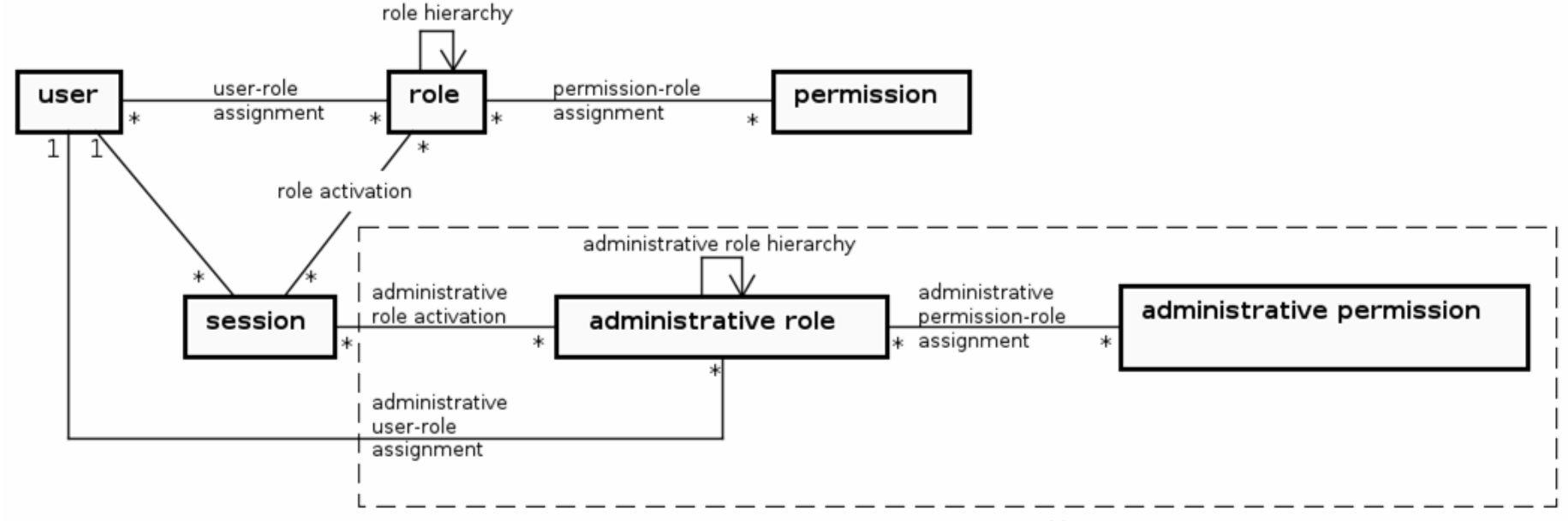
[7] BROY, M.; JONSSON, B.; KATOEN, J.-P.; LEUCKER, M.; PRETSCHNER, A. Model-Based Testing of Reactive Systems: Advanced Lectures (Lecture Notes in Computer Science). Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2005. I

[4] ENDO, A. T.; SIMAO, A. Evaluating test suite characteristics, cost, and effectiveness of fsmbased testing methods. Information and Software Technology, v. 55, n. 6, p. 1045 – 1062, 2013.

Role-Based Access Control Testing

(RBAC model)

- **RBAC**: ***Users*** *receive* ***privileges*** *through* ***role assignments***



ANSI RBAC and Administrative RBAC models [8]

[8] FADHEL, A. B.; BIANCULLI, D.; BRIAND, L. A comprehensive modeling framework for role-based access control policies. J. Syst. Softw., Elsevier Science Inc., New York, NY, USA, v. 107, n. C, p. 110–126, Sep. 2015.

Role-Based Access Control Testing

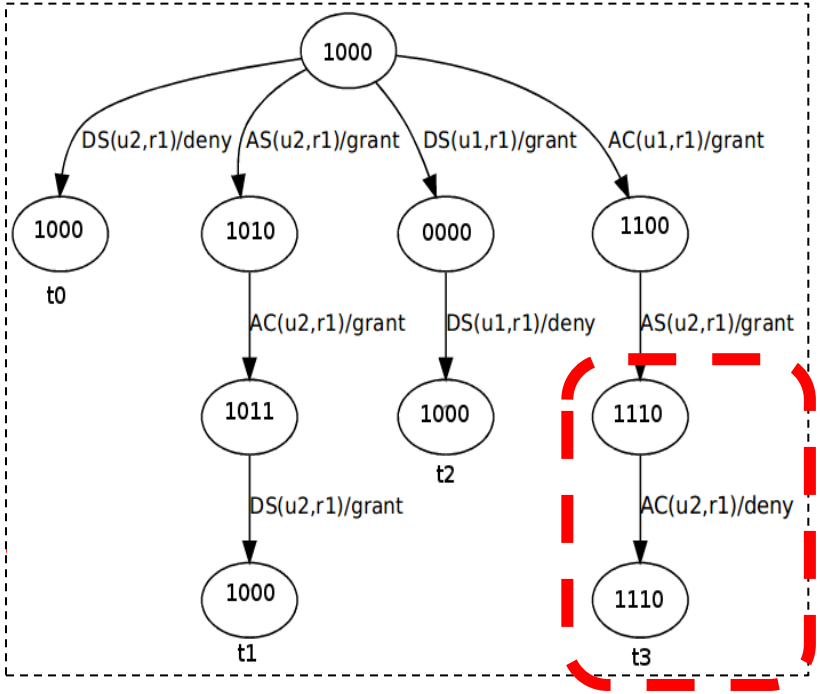
(RBAC constraints)

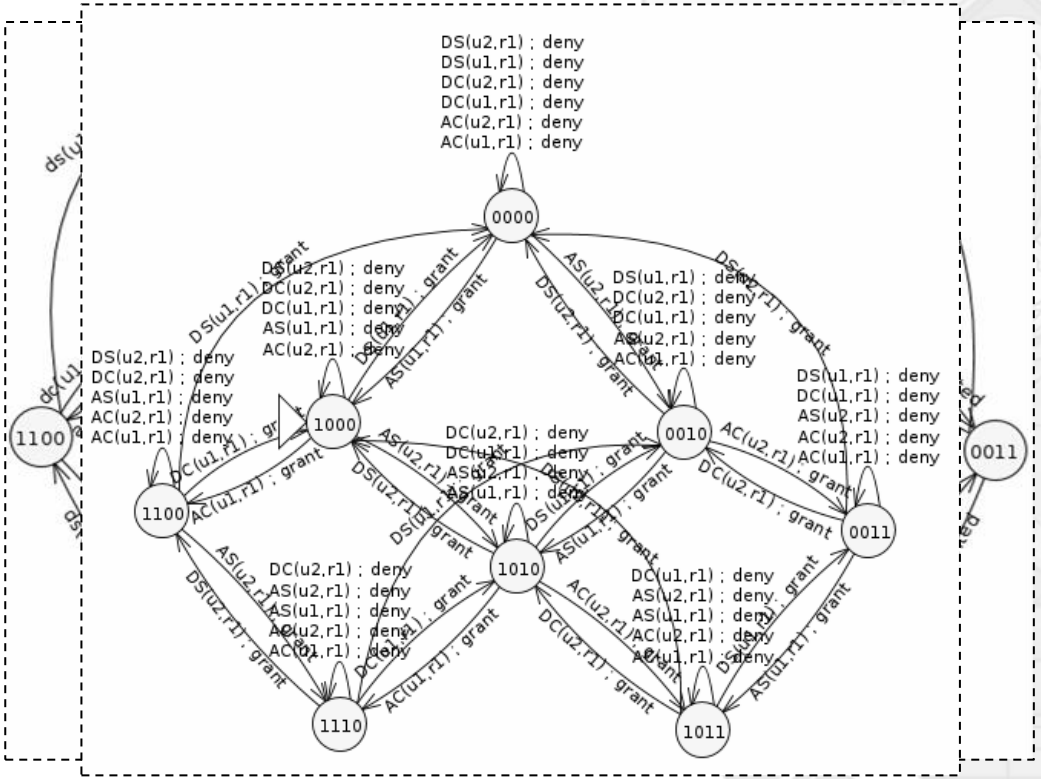
- **RBAC constraints** [8]
  - *Cardinality constraints*
  - *Separation of duty (SoD) constraints*

[8] FADHEL, A. B.; BIANCULLI, D.; BRIAND, L. A comprehensive modeling framework for role-based access control policies. J. Syst. Softw., Elsevier Science Inc., New York, NY, USA, v. 107, n. C, p. 110–126, Sep. 2015.

Role-Based Access Control Testing

(FSM-Based Testing of RBAC systems) [3]





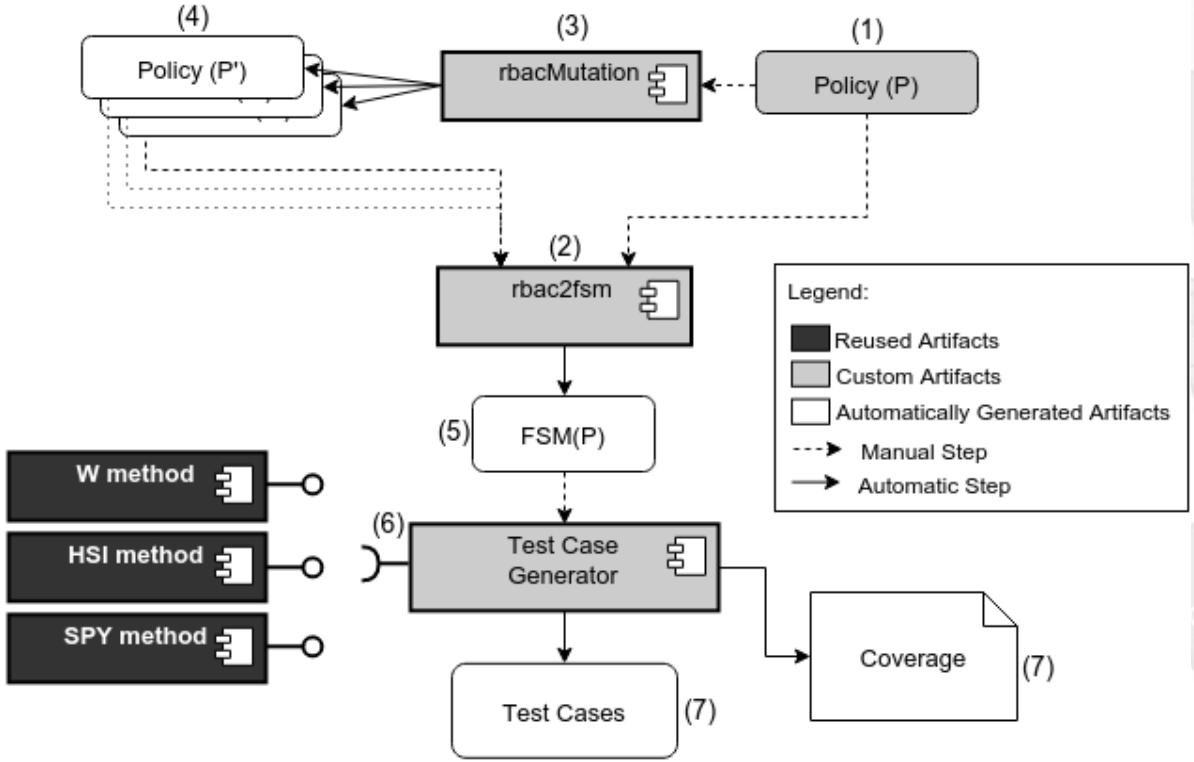
[3] MASOOD, A.; BHATTI, R.; GHAFOOR, A.; MATHUR, A. P. Scalable and effective test generation for role-based access control systems. IEEE Transactions on Software Engineering, IEEE Press, Piscataway, NJ, USA, v. 35, n. 5, p. 654–668, Sep. 2009.

Comparing FSM-Based Testing Methods on RBAC

Comparing FSM-Based Testing Methods on RBAC

1. Compare recent and traditional FSM-based testing methods on RBAC domain
    a. Recent **(SPY)** and Traditional **(W and HSI)** methods
    b. Test characteristics and Effectiveness
        i. ***number of resets**, **avg. test case length** and **test suite length***
        ii. ***RBAC fault domain***

Comparing FSM-Based Testing Methods on RBAC



Comparing FSM-Based Testing Methods on RBAC

(Selection of RBAC policies)

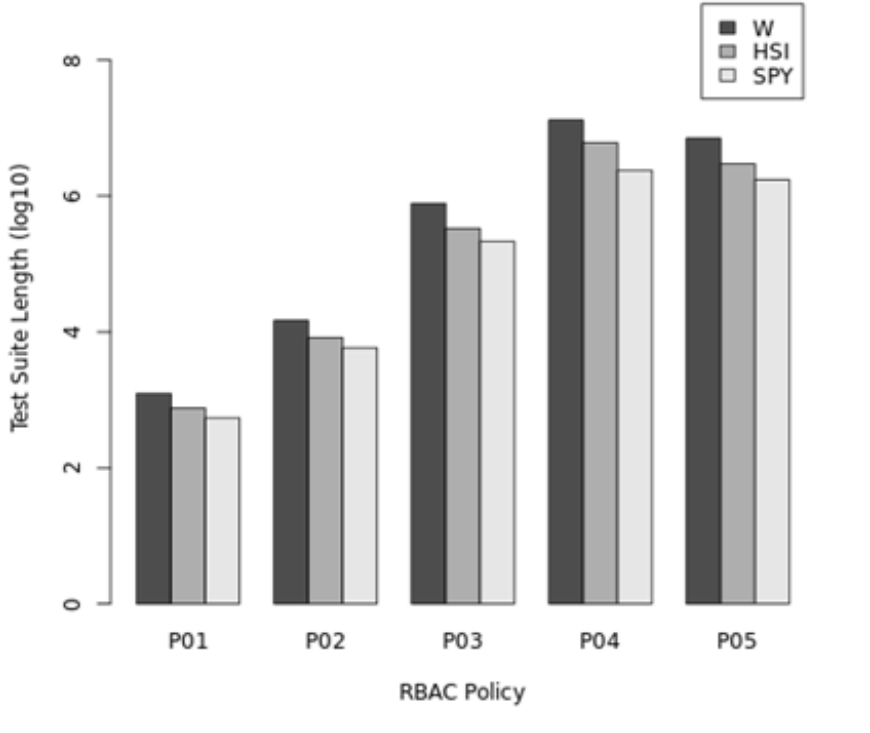
Policy name	U	R	$log_{10}(3^{UR})$	States	Transitions	Mutants
01_Masood2010Example1	2	1	0.9542	8	64	9
02_SeniorTraineeDoctor	2	2	1.9084	21	336	17
03_ExperiencePointsv2	2	4	2.7092	203	6496	11
04_users11roles2_v2	11	2	10.4966	485	42680	28
05_Masood2009P2v2	2	5	3	857	34280	48
06_Masood2009P1v2	3	4	3.2375	1880	90240	40
07_ProcureToStockv2	3	5	3.5282	5859	351540	14

15 test scenarios: {W,HSI,SPY} ⨯ {P01,P02,P03,P04,P05}

Comparing FSM-Based Testing Methods on RBAC

(***Test Suite Length***)

- Test generation duration
  - Total: 63 hours
  - *Min: 5 ms / Max: 24 h*
- Strong positive correlation [4]
  - |Users|×|Roles|
- *SPY test suite length (average)*
  - ***61%** of HSI*
  - ***31%** of W*

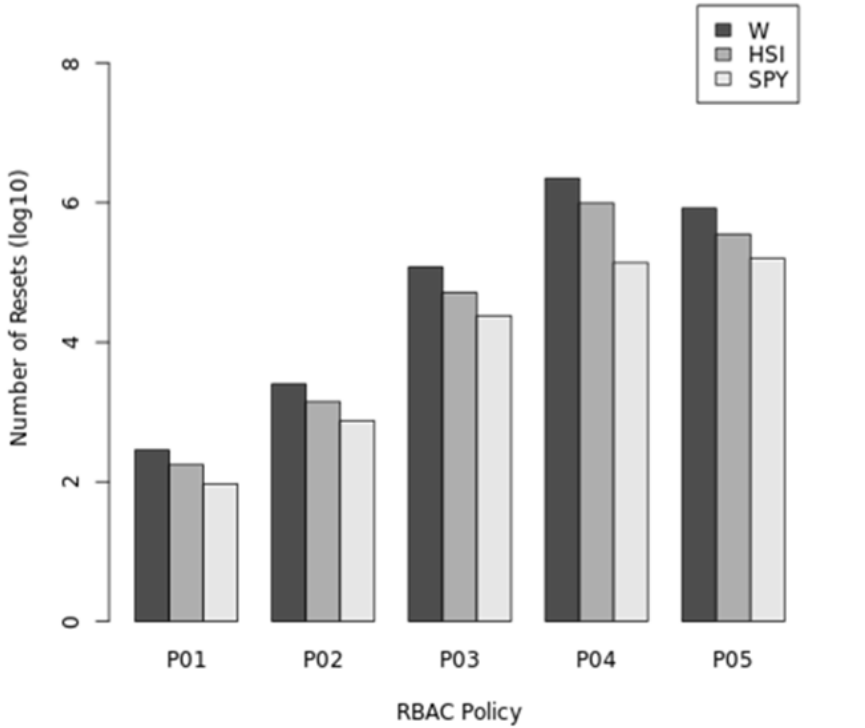


[4] ENDO, A. T.; SIMAO, A. Evaluating test suite characteristics, cost, and effectiveness of fsm based testing methods. Information and Software Technology, v. 55, n. 6, p. 1045 – 1062, 2013.

Comparing FSM-Based Testing Methods on RBAC

(***Number of Resets***)

- Strong positive correlation [4]
- SPY number of resets (average)
  - ***42.3%*** *of HSI*
    - Corroborated SPY's paper [9]
  - ***21.5%*** *of W*



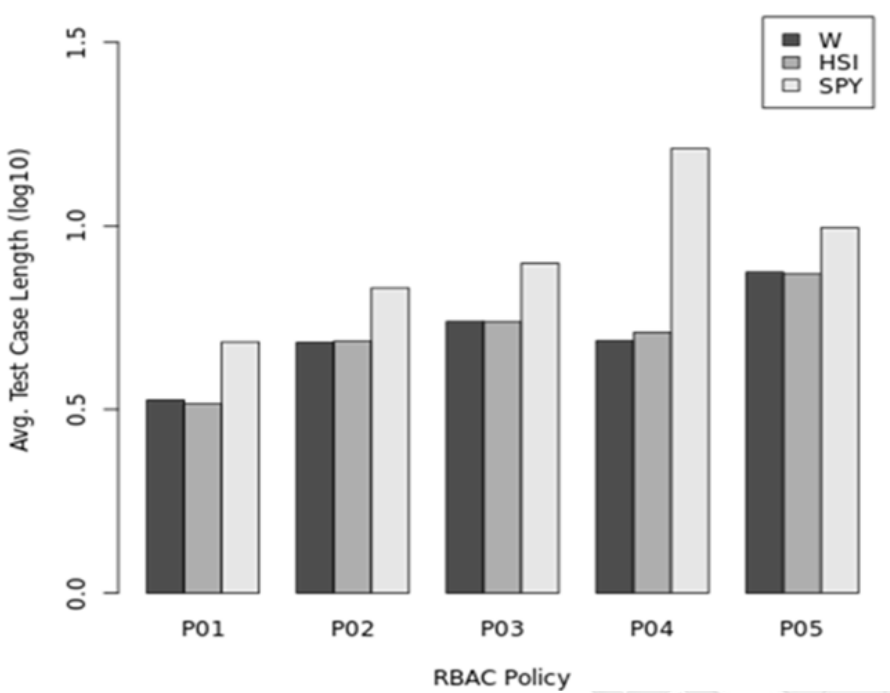
[4] ENDO, A. T.; SIMAO, A. Evaluating test suite characteristics, cost, and effectiveness of fsmbased testing methods. Information and Software Technology, v. 55, n. 6, p. 1045 – 1062, 2013.

[9] SIMÃO, A.; PETRENKO, A.; YEVTUSHENKO, N. Generating reduced tests for fsms with extra states. In: NUNEZ, M.; BAKER, P.; MERAYO, M. (Ed.). Testing of Software and Communication Systems. Springer Berlin Heidelberg, 2009, (Lecture Notes in Computer Science, v. 5826). p. 129–145.

Comparing FSM-Based Testing Methods on RBAC

(***Average Test Case Length***)

- No negative correlation [4]
- Average test case length
  - W and HSI were similar
  - SPY ~**78%** longer than {W, HSI}
- Maximum test case length
  - SPY was 14 times longer
- Test case length tends to increase
  - SPY method



[4] ENDO, A. T.; SIMAO, A. Evaluating test suite characteristics, cost, and effectiveness of fsmbased testing methods. Information and Software Technology, v. 55, n. 6, p. 1045 – 1062, 2013.

Comparing FSM-Based Testing Methods on RBAC

(Test analysis)

- The SPY testing method enabled significant reduction of the overall test costs
  - *Lower: Test Suite Length*, *Number of Resets*
  - *Greater: Average Test Case Length*
- 100% of effectiveness on all 15 scenarios: *{W,HSI,SPY} ⨯ {P01,P02,P03,P04,P05}*
  - *State and transition coverage* [4]
- ***Order of dominance: SPY > HSI > W***
- *A large amount of test cases tends to be generated on RBAC domain*
  - |Users|×|Roles|

[4] ENDO, A. T.; SIMAO, A. Evaluating test suite characteristics, cost, and effectiveness of fsmbased testing methods. Information and Software Technology, v. 55, n. 6, p. 1045 – 1062, 2013.

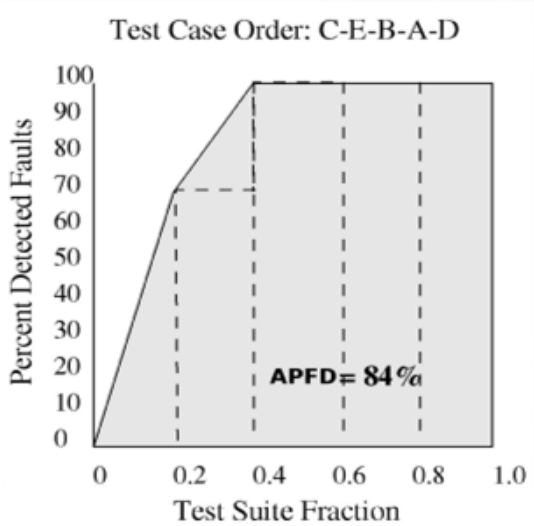
Investigating Test Prioritization on RBAC

Investigating Test Prioritization on RBAC

(Test Prioritization) [10]

- Time and resources constraints
- Identify an efficient ordering of the test cases to maximize certain properties
- Average Percentage Fault Detected (APFD)

test	fault									
	1	2	3	4	5	6	7	8	9	10
A	x				x					
B	x				x	x	x			
C	x	x	x	x	x	x	x			
D					x					
E								x	x	x



[10] ELBAUM, S.; MALISHEVSKY, A. G.; ROTHERMEL, G. Prioritizing test cases for regression testing. SIGSOFT Softw. Eng. Notes, ACM, New York, NY, USA, v. 25, n. 5, p. 102–112, Aug. 2000.

Investigating Test Prioritization on RBAC

(Test Similarity)

- Similar test cases are redundant [6]
  - Resembling fault detection capabilities → No additional gain
- Test similarity on XACML and MBT domains
  - On MBT, test similarity can be more effective than random approaches [5]
  - XACML prioritization effectiveness is higher than of random prioritization [6]

[5] CARTAXO, E. G.; MACHADO, P. D. L.; NETO, F. G. O. On the use of a similarity function for test case selection in the context of model-based testing. Software Testing, Verification and Reliability, John Wiley & Sons, Ltd., v. 21, n. 2, p. 75–100, 2011.

[6] BERTOLINO, A.; DAOUDAGH, S.; KATEB, D. E.; HENARD, C.; TRAON, Y. L.; LONETTI, F.; MARCHETTI, E.; MOUELHI, T.; PAPADAKIS, M. Similarity testing for access control. Information and Software Technology, v. 58, p. 355 – 372, 2015.

Investigating Test Prioritization on RBAC

2. Investigate and compare test prioritization approaches for RBAC testing

    a. ***Simple similarity***

    b. ***RBAC similarity***

    c. ***Random prioritization***

Investigating Test Prioritization on RBAC

(RBAC Similarity)

1. Simple similarity **(d_{sd})**: ***n****umber of* ***d****istinct* ***t****ransitions*

$$d_{sd}(t_i, t_j) = \frac{ndt(t_i, t_j)}{avg(length(t_i) + length(t_j))}$$

2. Applicability degree **(AppValue)**
   a. Policy Applicability Degree **($pad_{P(t)}$)**
   b. *Assignment Applicability Degree* ***($asad_{P(t)}$)***
   c. *Activation Applicability Degree* ***($acad_{P(t)}$)***
   d. *Permission Applicability Degree* ***($prad_{P(t)}$)***

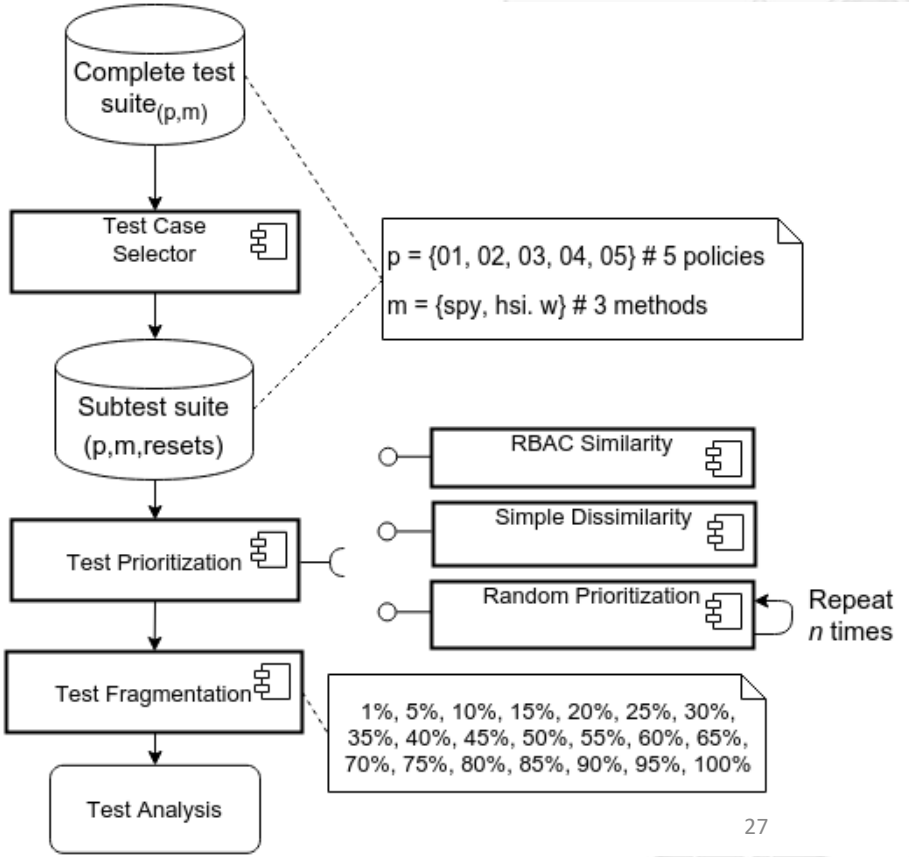
$$d_{rs}(P, t_i, t_j) = \begin{cases} 0 & \text{if } d_{sd}(t_i, t_j) = 0 \\ d_{sd}(t_i, t_j) + & \\ AppValue_{(P,t_i,t_j)} + & \\ PriorityValue_{(P,t_i,t_j)} & \text{otherwise} \end{cases}$$

3. Priority value **(PriorityValue)**
   a. *alpha > beta > gamma > delta*

$$PriorityValue_{P(t_i,t_j)} = \begin{cases} \alpha \text{ if } (pad_{P(t_i)} = pad_{P(t_j)} = 1) \\ \beta \text{ if } (pad_{P(t_i)} \; XOR \; pad_{P(t_j)}) \\ \gamma \text{ if } (0 < pad_{P(t_i)}, pad_{P(t_j)} < 1) \\ \delta \text{ otherwise} \end{cases}$$

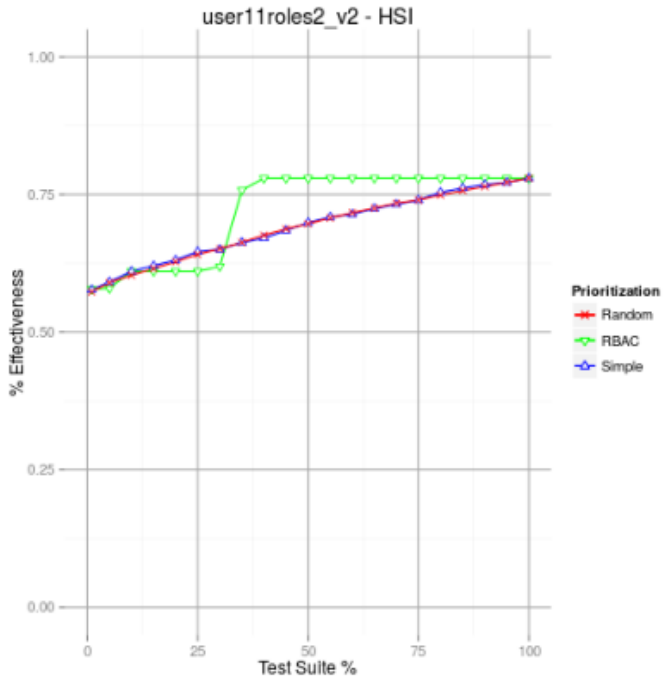
Investigating Test Prioritization on RBAC

1. Test Prioritization methods
    a. RBAC similarity
    b. Simple similarity
    c. Random prioritization
2. Test fragmentations
    a. 21 fragments
3. Test analysis
    a. Test effectiveness
    b. APFD metric

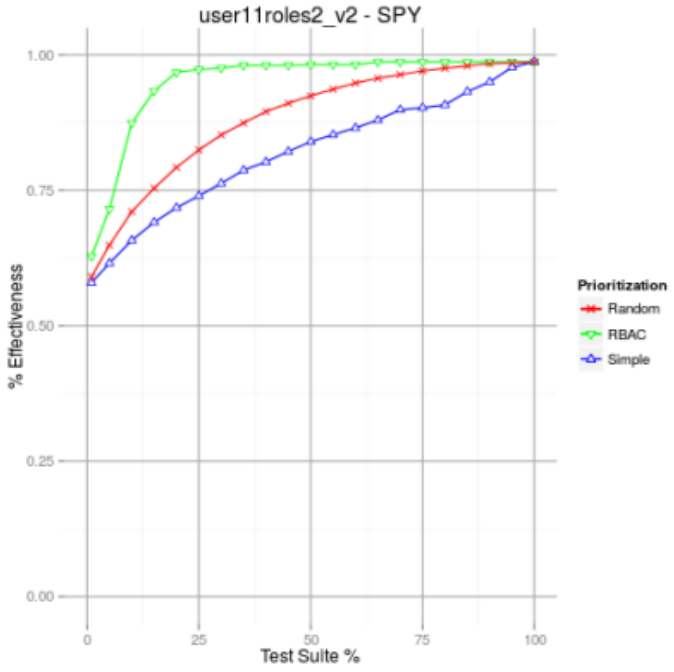


Investigating Test Prioritization on RBAC

(e) P04 + HSI



(f) P04 + SPY



Investigating Test Prioritization on RBAC

(Test analysis)

- RBAC presented better APFD
  - Issues on {P02,P03} + HSI
- Good prioritization: W and SPY
  - Some “oscillations”
  - 5 to 25% test suite → Max. effectiv.
- Test prioritization methods
  - ***RBAC > Random > Simple***

Table 21 – APFD of the complete test suites

Scenario	$APFD_{RBAC}$	$APFD_{Simple}$	$APFD_{Random}$
P01 + W	**0.964**	0.857	0.95
P02 + W	**0.969**	0.874	0.965
P01 + HSI	**0.952**	0.726	0.917
P02 + HSI	0.921	0.778	**0.959**
P01 + SPY	**0.916**	0.785	0.907
P02 + SPY	**0.962**	0.826	0.957

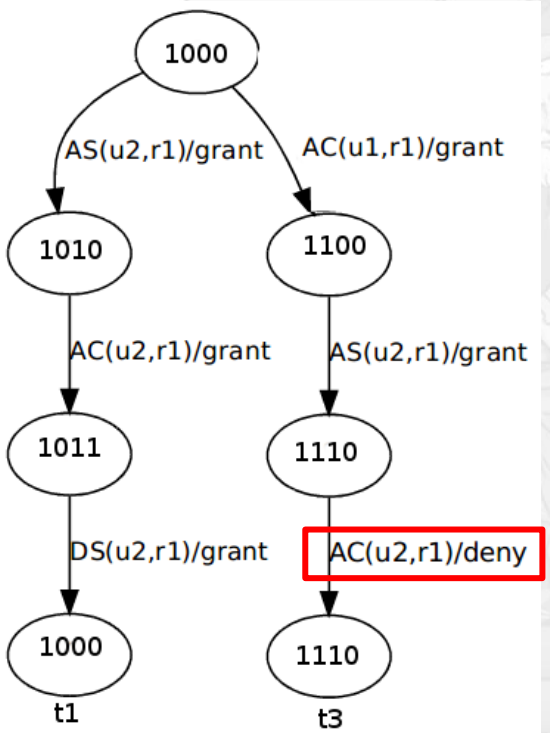
Table 25 – APFD of the subtest suites

Scenario	$APFD_{RBAC}$	$APFD_{Simple}$	$APFD_{Random}$
P03 + W	**0.973**	0.97	0.97
P04 + W	**0.646**	0.641	0.638
P05 + W	**0.811**	0.788	0.797
P03 + HSI	0.96	**0.967**	0.966
P04 + HSI	**0.706**	0.676	0.675
P05 + HSI	**0.797**	0.772	0.777
P03 + SPY	**0.974**	0.969	0.97
P04 + SPY	**0.922**	0.794	0.856
P05 + SPY	**0.819**	0.794	0.801

Investigating Test Prioritization on RBAC

(Test analysis)

- Random prioritization outperformed Simple similarity
  - Similar tests have resembling effectiveness
  - RBAC fault domain
    - One RBAC fault → Many *FSM(P)* transitions
    - Dissimilarity ⇏ Applicability
- Applicability degree can improve RBAC prioritization
  - Similarity + Applicability



Distinct test cases but with different AppValue (e.g. Sr(r1)=1)

Conclusion, Limitations, Results and Future work

Conclusion

- **On comparing FSM-based testing methods on RBAC**
  - Recent FSM testing methods can be mode adequate on RBAC testing
    - Less resets (test cases)
    - Shorter test suites
    - Longer test cases
  - Fault detection does not change (100% effective)

Conclusion

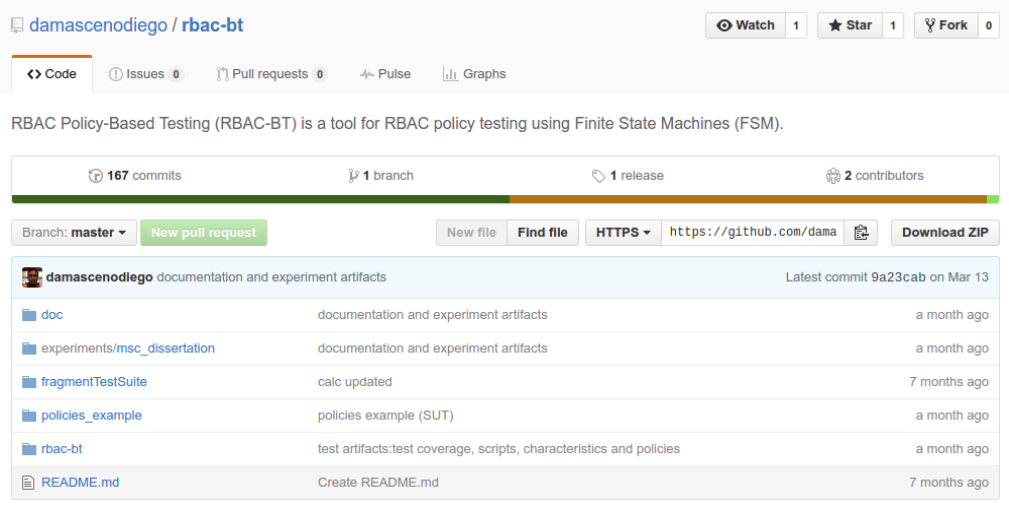
- **On investigating test prioritization criteria on RBAC**
  - Random prioritization outperformed simple similarity
    - *Distribution of RBAC faults along FSM(P)*
  - On average, the proposed **RBAC similarity**
    - Outperformed simple similarity and random prioritization

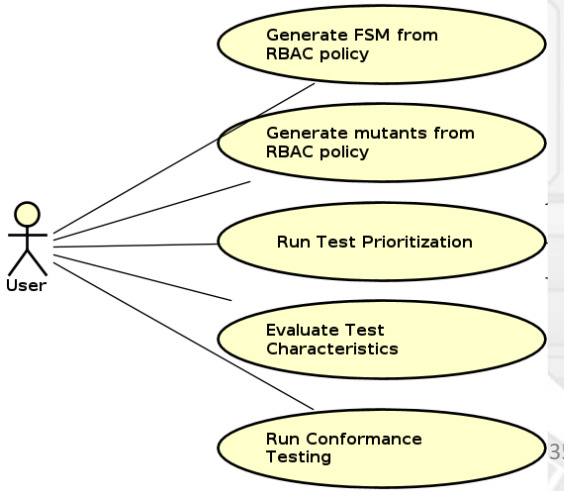
Limitations

- Other test generation methods
  - *Test prioritization effectiveness depends on the test cases*
- Role hierarchies (*Hierarchical RBAC*)
- Large number of users and roles → **State explosion**

Results

- Lab package for further replications
  - **Test artifacts:** *RBAC policies, protocols, test suites...*
  - **RBAC-BT tool:** https://github.com/damascenodiego/rbac-bt





Results

One **published** work → Workshop on Systematic and Automated Software Testing (**SAST 2014**)

- **Authors: DAMASCENO, C. D. N.**; DELAMARO, M. E.; SIMÃO, A. S.
- **Title:** Uma revisão sistemática em teste de segurança baseado em modelos. [2]
- **In:** Congresso Brasileiro de Software: Teoria e Prática (CBSoft) Porto Alegre,
- **Year:** 2014
- Source: http://www.ic.ufal.br/evento/cbsoft2014/anais/sast_v1_p.pdf

Uma Revisão Sistemática em Teste de Segurança Baseado em Modelos 31

Carlos Diego Nascimento Damasceno , Márcio Eduardo Delamaro, Adenilso da Silva Simão

[2] DAMASCENO, C. D. N.; DELAMARO, M. E.; SIMÃO, A. d. S. Uma revisão sistemática em teste de segurança baseado em modelos. In: Anais do Workshop Brasileiro de Testes de Software Automatizados e Sistemático - CBSoft - Congresso Brasileiro de Software: Teoria e Prática. Porto Alegre: SBC, 2014. p. 31–40.

Results

One **submitted** work → XXX Simpósio Brasileiro de Engenharia de Software 2016 (**SBES 2016**)

- **Authors: DAMASCENO, C. D. N.**; MASIERO, P. C.; SIMÃO, A. S.
- **Title:** Evaluating test characteristics and effectiveness of FSM-based testing methods on RBAC systems.
- Year: **2016**.

Evaluating test characteristics and effectiveness of FSM-based testing methods on RBAC systems

Carlos Diego Nascimento Damasceno
University of São Paulo – USP
São Carlos, SP, Brazil
damascenodiego@usp.br

Paulo Cesar Masiero
University of São Paulo – USP
São Carlos, SP, Brazil
masiero@icmc.usp.br

Adenilso Simao
University of São Paulo – USP
São Carlos, SP, Brazil
adenilso@icmc.usp.br

Future work

Under development

- Title: Similarity Testing for Role Based Access Control Systems
- Research Topics
  - **Test prioritization for Role Based Access Control**
  - Compare **RBAC similarity** vs. **Simple similarity** vs. **Random prioritization**

Future work

- Further replications
  - Other policies and/or test generation methods
- Extending RBAC-BT with *Hierarchical RBAC*
- RBAC similarity as test criteria
  - Deterministic generation
  - Random generation
  - Search-Based Software Testing

References

[1] FELDERER, M.; ZECH, P.; BREU, R.; BÜCHLER, M.; PRETSCHNER, A. Model-based security testing: a taxonomy and systematic classification. Software Testing, Verification and Reliability, p. n/a–n/a, 2015.

[2] DAMASCENO, C. D. N.; DELAMARO, M. E.; SIMÃO, A. d. S. Uma revisão sistemática em teste de segurança baseado em modelos. In: Anais do Workshop Brasileiro de Testes de Software Automatizados e Sistemático - CBSoft - Congresso Brasileiro de Software: Teoria e Prática. Porto Alegre: SBC, 2014. p. 31–40.

[3] MASOOD, A.; BHATTI, R.; GHAFOOR, A.; MATHUR, A. P. Scalable and effective test generation for role-based access control systems. IEEE Transactions on Software Engineering, IEEE Press, Piscataway, NJ, USA, v. 35, n. 5, p. 654–668, Sep. 2009.

[4] ENDO, A. T.; SIMAO, A. Evaluating test suite characteristics, cost, and effectiveness of fsm based testing methods. Information and Software Technology, v. 55, n. 6, p. 1045 – 1062, 2013.

[5] CARTAXO, E. G.; MACHADO, P. D. L.; NETO, F. G. O. On the use of a similarity function for test case selection in the context of model-based testing. Software Testing, Verification and Reliability, John Wiley & Sons, Ltd., v. 21, n. 2, p. 75–100, 2011.

[6] BERTOLINO, A.; DAOUDAGH, S.; KATEB, D. E.; HENARD, C.; TRAON, Y. L.; LONETTI, F.; MARCHETTI, E.; MOUELHI, T.; PAPADAKIS, M. Similarity testing for access control. Information and Software Technology, v. 58, p. 355 – 372, 2015.

[7] BROY, M.; JONSSON, B.; KATOEN, J.-P.; LEUCKER, M.; PRETSCHNER, A. Model-Based Testing of Reactive Systems: Advanced Lectures (Lecture Notes in Computer Science). Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2005.

[8] FADHEL, A. B.; BIANCULLI, D.; BRIAND, L. A comprehensive modeling framework for role-based access control policies. J. Syst. Softw., Elsevier Science Inc., New York, NY, USA, v. 107, n. C, p. 110–126, Sep. 2015.

[9] SIMÃO, A.; PETRENKO, A.; YEVTUSHENKO, N. Generating reduced tests for fsms with extra states. In: NUNEZ, M.; BAKER, P.; MERAYO, M. (Ed.). Testing of Software and Communication Systems. Springer Berlin Heidelberg, 2009, (Lecture Notes in Computer Science, v. 5826). p. 129–145.

[10] ELBAUM, S.; MALISHEVSKY, A. G.; ROTHERMEL, G. Prioritizing test cases for regression testing. SIGSOFT Softw. Eng. Notes, ACM, New York, NY, USA, v. 25, n. 5, p. 102–112, Aug. 2000.

Thank you!

Carlos Diego Nascimento Damasceno – damascenodiego@usp.br

Advisor: Prof. Dr. Adenilso da Silva Simão

Laboratory of Software Engineering – LabES

Institute of Mathematics and Computer Science – ICMC

University of Sao Paulo – USP

Sao Carlos – SP – Brazil