Adaptive Information Security for the Cloud

Risk Assessment using Early Requirements Models

Dr. Yijun Yu

The Open University, UK

http://mcs.open.ac.uk/yy66

5 September 2017 @ Lisbon, Tutorial, RE 2017

Yijun YU

WeChat : xihuatech (嘻话Tech)

- 1988-1998 Fudan University, Shanghai, China
  - 1991-1995 Jadebird CASE Environment with Peking University
    Structured Analysis and Design CASE tools
- 1999-2002 Ghent University, Belgium
- 2003-2006 University of Toronto, Canada
- Since 2006: The Open University, UK
  Since 2007: Collaborating with NII, Japan
- Interests: High Trustworthy and Dependability
  - Parallelizing Compiler for High *Performance*
  - Software Maintenance for High *Productivity*
  - Requirements Engineering for High *Quality*
  - Self-Tuning and Self-Optimizations with High *Variability*
  - Software Engineering for *Aviation Safety*
  - Argumentation for *Security and Privacy* Risks

Yijun YU

WeChat : xihuatech (嘻话Tech)

- 1988-1998 Fudan University, Shanghai, China
  - 1991-1995 Jadebird CASE Environment with Peking University
    Structured Analysis and Design CASE tools
- 1999-2002 Ghent University, Belgium
- 2003-2006 University of Toronto, Canada
- Since 2006: The Open University, UK
  Since 2007: Collaborating with NII, Japan
- Interests: High Trustworthy and Dependability
  - Parallelizing Compiler for High *Performance*
  - Software Maintenance for High *Productivity*
  - Requirements Engineering for High *Quality*
  - Self-Tuning and Self-Optimizations with High *Variability*
  - Software Engineering for *Aviation Safety*
  - Argumentation for *Security and Privacy* Risks

Shall I take a flight ?

- My first flight from Shanghai to Beijing, 25 years ago.
- It is important for the *Jadebird* team to demonstrate a CASE tool (Structured Analysis) I programmed …
- However, there was a bug, a show stopper, one day before the demo to the Chinese Minister of Science and Technology …
- If I take a train instead, it will be slow, and the demo will be a failure ...
- I risked my life (rather young) to go to PKU …
- As a result, the project had won a number of awards in China and I joined the SE group as a MSc student.

- Today's talk is my personal reflection of 25 years

SEAD Software Engineering and Design

TEAM | RESEARCH | PUBLICATIONS | OUTREACH | NEWS | CONTACT

Team

ACADEMICS

RESEARCHERS

STUDENTS

VISITORS

ADMINISTRATORS

COLLABORATORS

FUNDERS

Bashar Nuseibeh

Professor

Andrea Zisman

Professor

Helen Sharp

Professor

Marian Petre

Professor

Arosha Bandara

Senior Lecturer

Blaine Price

Senior Lecturer

Yijun Yu

Senior Lecturer

Michel Wermelinger

Senior Lecturer

Amel Bennaceur

Lecturer

Recruiting...

SEAD Software Engineering and Design

The Open University

TEAM | RESEARCH | PUBLICATIONS | OUTREACH | NEWS | CONTACT

Team

- Academics
- Researchers
- Students
- Visitors
- Administrators
- Collaborators
- Funders

Michael Jackson
Visiting Professor

Cory Doctorow
Visiting Professor

David Bush
Visiting Senior Research Fellow
(NATS)

Advait Deshpande
Visiting Research Fellow
(Rand Europe)

Luke Hutton
Visiting Research Fellow
(BBC News)

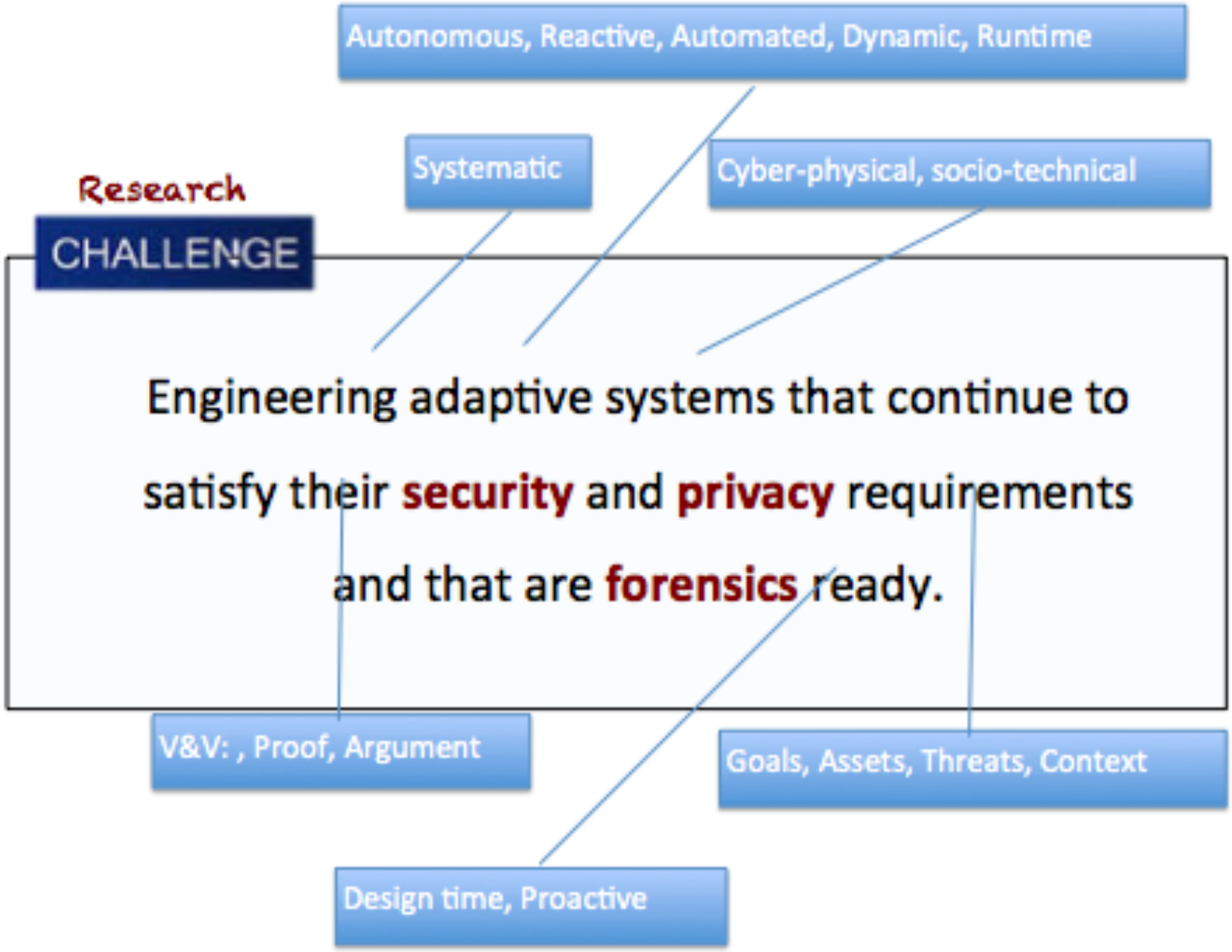
Angus Marshall
Visiting Research Fellow
(University of York)

Oliver Pearce
Visiting Professor
(Milton Keynes Hospital)

Mark Levine
Visiting Professor
(University of Exeter)

In Requirements We Trust

- Bashar Nuseibeh, Charles B. Haley, Craig Foster (2009). "*Securing the Skies: In Requirements We Trust*". *IEEE Computer* 42(9):64-72.
  - Toulmin Argumentation (a.k.a. dual diligence) (claim, rebuttal, mitigation) [TSE'08]
  - Risk and argumentation (RE'11 Distinguished Paper)
- SecureChange, an EU project with Deep Blue and Rome Airport
- Adaptive Security and Privacy, an ERC Adv. Grant
- Adaptive Information Security for the Cloud, an QNRF Grant


Autonomous, Reactive, Automated, Dynamic, Runtime
Systematic
Cyber-physical, socio-technical
Research
CHALLENGE
Engineering adaptive systems that continue to satisfy their security and privacy requirements and that are forensics ready.
V&V: , Proof, Argument
Goals, Assets, Threats, Context
Design time, Proactive

The Open University

الصندوق القطري لرعاية البحث العلمي
Qatar National Research Fund
Member of Qatar Foundation عضو في مؤسسة قطر

Adaptive Information Security for the Cloud

erc
European Research Council
Established by the European Commission

Risk Assessment using Early Requirements Models

Dr. Yijun Yu

The Open University, UK

http://mcs.open.ac.uk/yy66

5 September 2017 @ Lisbon, Tutorial, RE 2017

Life is full of risks

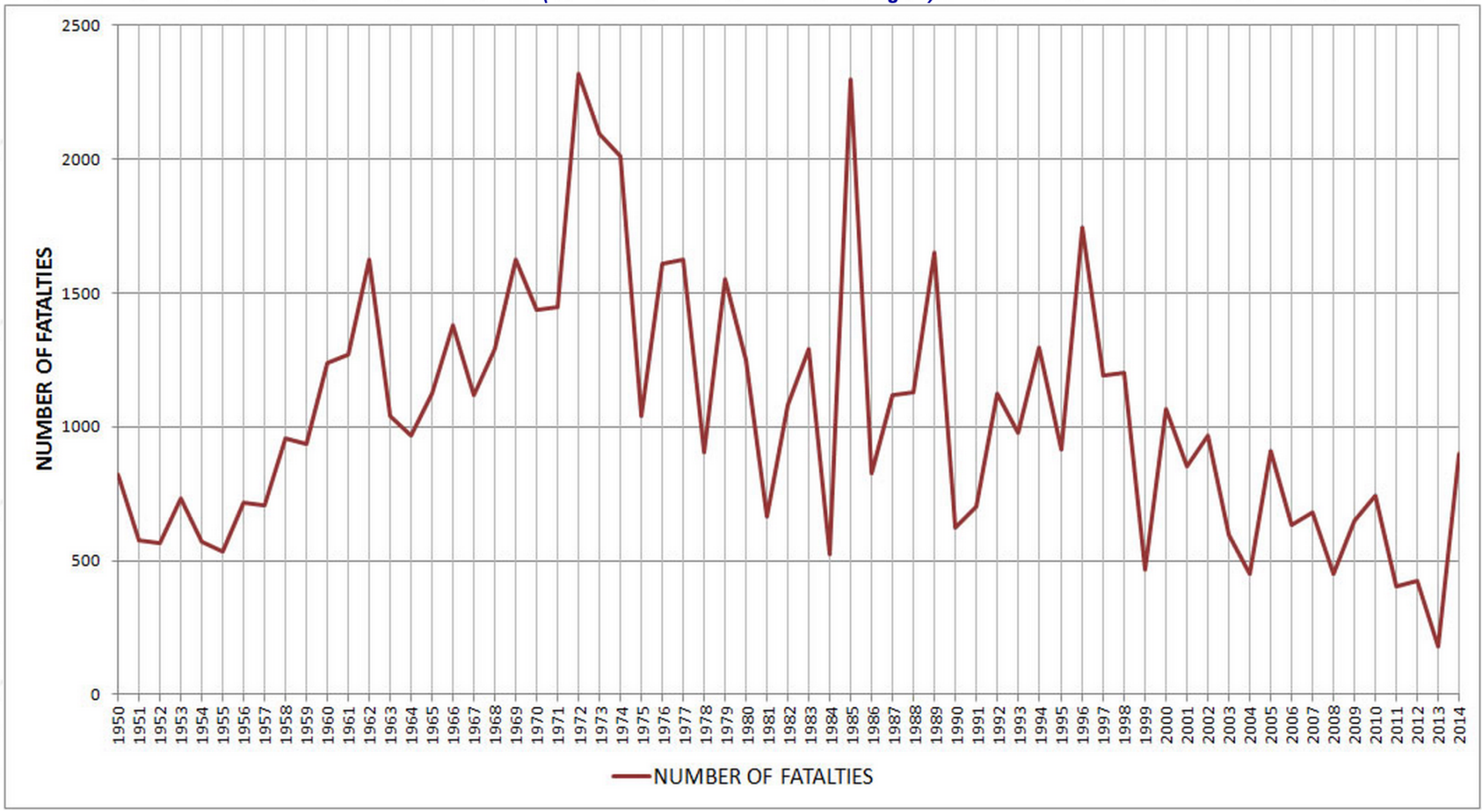
- FSE and RE are held in the same week
  - London => Dusseldorf => Paderborn => talk
  - Parderborn => Dusseldorf => London => Lisbon
- From Dusseldorf to Lisbon via London
  - I have one hour in flight connection
  - Flight BA943 was delayed by 30 minutes
  - Shuttle Bus from Terminal 5 to Terminal 3 was delayed by 22 minutes
  - …fortunately, BA504, the flight from London to Lisbon was also delayed by 10 minutes, so I am here ☺
- *Why are FSE/RE scheduled on the same week?*

Which one is more deadly?

Perceived Risks

According to "The Shark Trackers", you've got a better chance of dying from heating up your waffle than you do of being killed by a shark. In 2014, over 400 people were killed by malfunctioning or improperly working toasters as compared to less than a dozed by shark attacks.

Death tolls of flights



A Guided Tour

1. Risks in life
2. Qualitative Risk Assessment based on Requirements
3. Quantitative Risk Assessment based on Requirements
4. Abstract Goal Behaviors and the Right Hand Side Problems
5. Quantitative Risk Assessment based on Probabilistic Behavior Models and Requirements
6. Risk Assessment for Requirements-Driven Self-Adaptive Systems

Safer to take planes

- Driving cars is much more dangerous.
- Would self-driving cars be safer?
  - Yet to know.
  - It depends.
  - How much autonomy men shall give to machine?
    - NASA, Russia Space Agency, Chinese Space Agency
    - Shall Manned Space Vehicles be controlled by Ground Controls?
    - Shall Manned Space Vehicles be controlled by Robots?

Exercise 1

- What's your rationale when deciding to take flight for the first time in your life?
- Do you calculate the risk?
- What factors were used in your calculations?

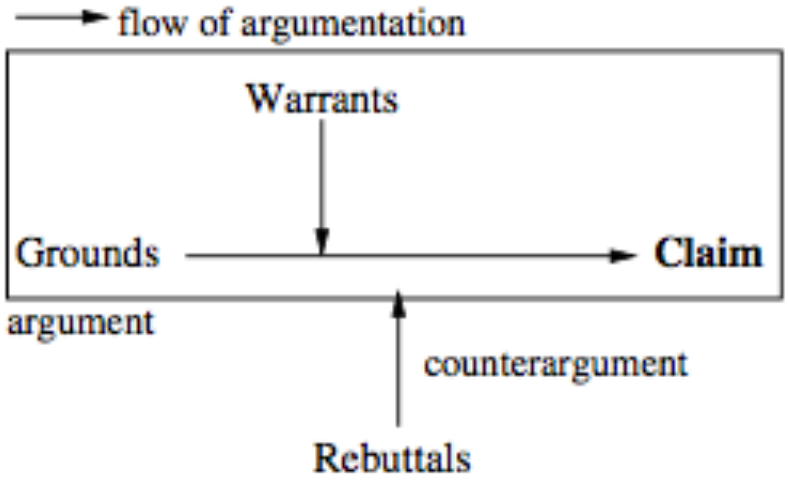
- Discuss in pairs (for 5 minutes)

A Guided Tour

1. Risks in life
2. Qualitative Risk Assessment based on Requirements
3. Quantitative Risk Assessment based on Requirements
4. Abstract Goal Behaviors and the Right Hand Side Problems
5. Quantitative Risk Assessment based on Probabilistic Behavior Models and Requirements
6. Risk Assessment for Requirements-Driven Self-Adaptive Systems

Risks and Arguments

- Security requirements: protecting assets from malicious attacks
- Risks are important to assess the satisfaction argument of security requirements



Using Argumentation to Explain Ambiguity in Requirements Elicitation Interviews by Yehia Elrakaiby, Alessio Ferrari, Paola Spoletini, Stefania Gnesi and Bashar Nuseibeh

How to Assess Risks from Requirements Satisfaction Arguments?

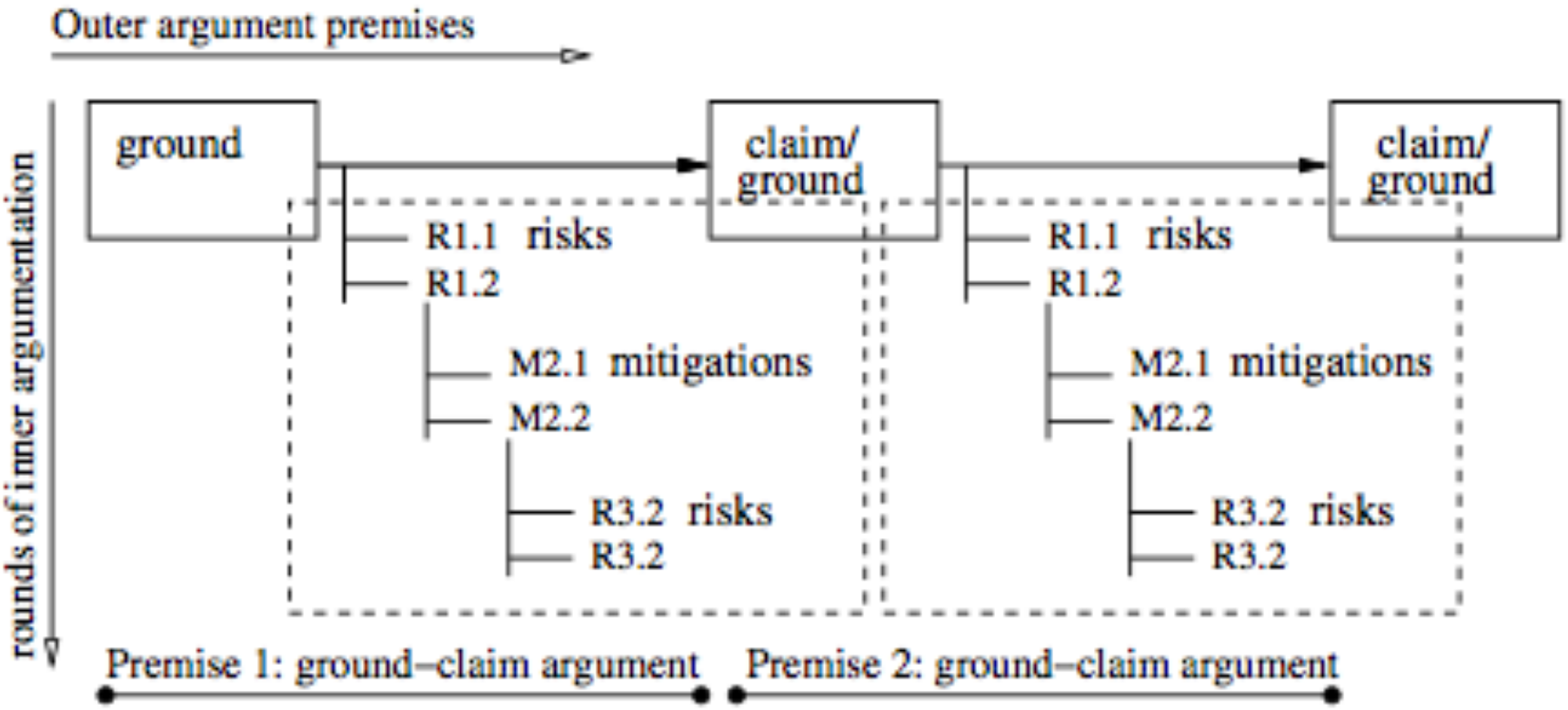
Charles B. Haley, Robin C. Laney, Jonathan D. Moffett, Bashar Nuseibeh: **Security Requirements Engineering: A Framework for Representation and Analysis.** IEEE Trans. Software Eng. 34(1): 133-153 (2008)

Yijun Yu, Thein Than Tun, Alessandra Tedeschi, Virginia N. L. Franqueira, Bashar Nuseibeh: **OpenArgue: Supporting argumentation to evolve secure software systems.** RE 2011: 351-352

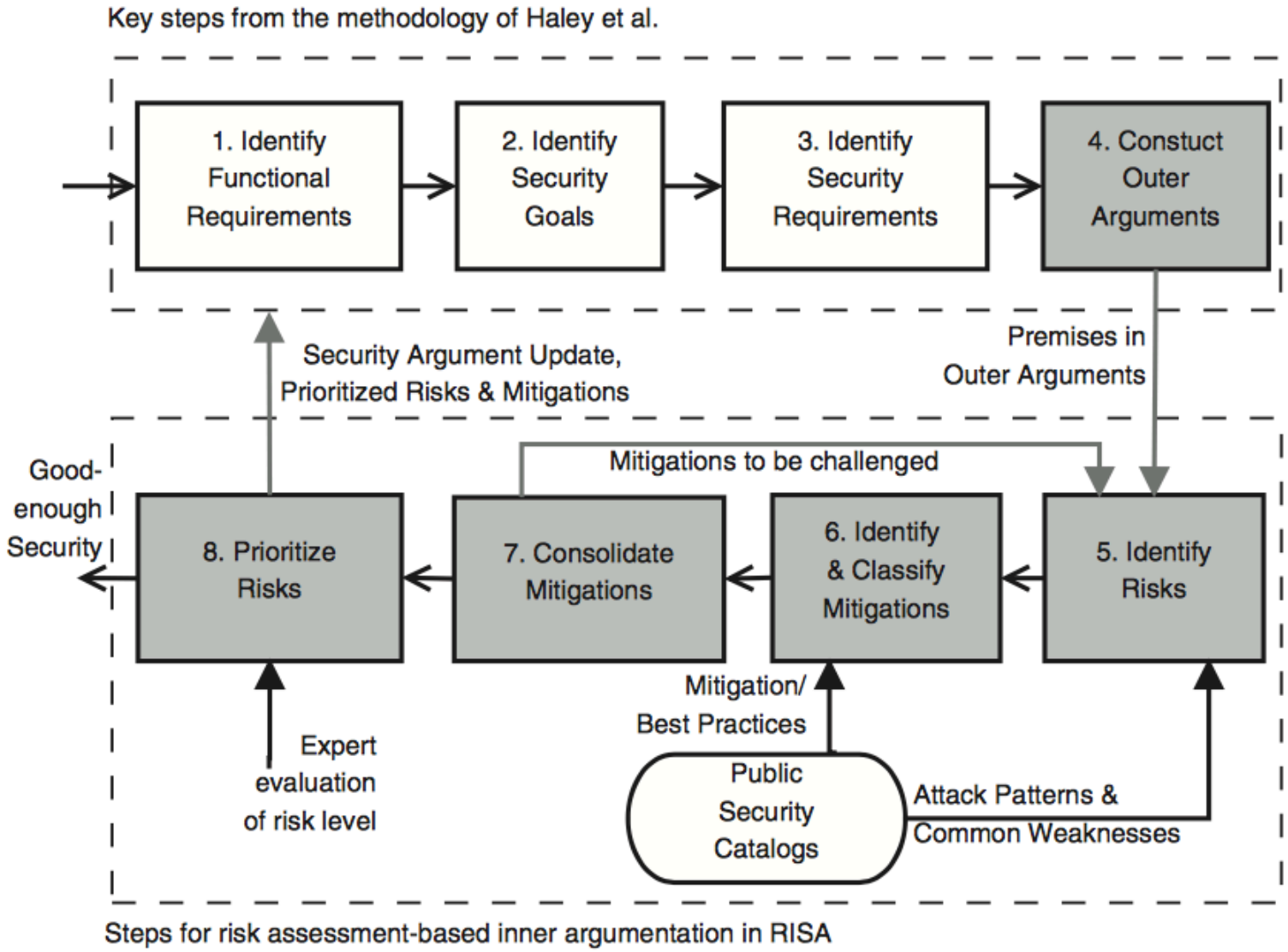
Virginia N. L. Franqueira, Thein Than Tun, Yijun Yu, Roel Wieringa, Bashar Nuseibeh: **Risk and argument: A risk-based argumentation method for practical security.** RE 2011: 239-248

Yijun Yu, Virginia N. L. Franqueira, Thein Than Tun, Roel Wieringa, Bashar Nuseibeh: **Automated analysis of security requirements through risk-based argumentation.** Journal of Systems and Software 106: 102-116 (2015)

Risks ~ Rebuttals



Risk and Argument (RISA)



DSL

```
1  argument: prop_example

3  boolean S1, S2, S3

5  S1 "User enters ID and passcode" with S1
6  S2 "User ID and passcode match a pair
7        of stored  ID and passcode" with S2
8  S3 "User is a valid user" with
9        S1 & S2 -> S3
```

PIN Entry Device (PED) example

1) Step 1—Identify Functional Requirements: The overall functional goal of the system in relation to PED users is the following:

[FG1]: Provide convenient payment option at Points-Of-Sale to consumers

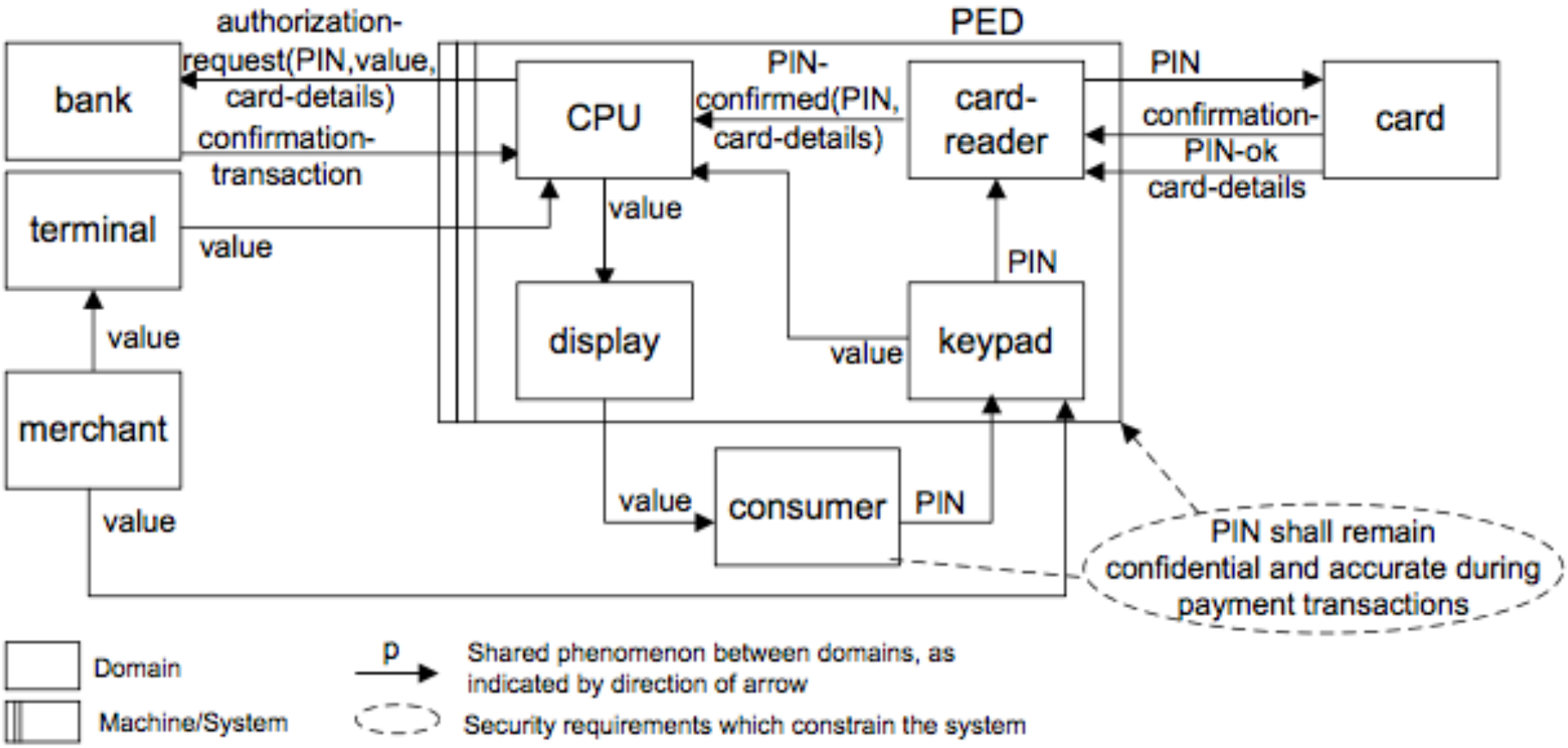
The following functional requirement can be derived from the functional goal above:

[FR1]: Allow consumers to pay at Points-Of-Sale with PIN

Identify Security Requirements and Security Functionality

[SR1]: PIN entered by consumers shall remain confidential during payment transactions at Points-Of-Sale
[SR2]: PIN entered by consumers shall remain accurate during payment transactions at Points-Of-Sale (i.e. integrity of the PIN shall be preserved)

[SF1]: Enclosure of PED components provides tamper detection and response mechanisms to resist physical attacks
[SF2]: Encryption/Decryption of PIN ensures that the PIN is encrypted within the PED immediately after the PIN entry is complete


PED
bank
terminal
merchant
CPU
card-reader
card
display
keypad
consumer
authorization-request(PIN,value, card-details)
confirmation-transaction
value
value
value
PIN-confirmed(PIN, card-details)
value
value
PIN
PIN
confirmation-PIN-ok
card-details
value
PIN
PIN shall remain confidential and accurate during payment transactions
Domain
Machine/System
p
Shared phenomenon between domains, as indicated by direction of arrow
Security requirements which constrain the system

Outer Argument

P1, P2, P3, P4, P5, P6, A7 ⊢ bank!confirmation-transaction

The premises are defined below using the propositional logic.

Premises:

P1. consumer!PIN → keypad!PIN

P2. keypad!PIN → card-reader!PIN

P3. card-reader!PIN → card!confirmation-PIN-ok

P4. card!confirmation-PIN-ok → card-reader!PIN-confirmed

P5. card-reader!PIN-confirmed → CPU!authorization-request

P6. CPU!authorization-request → bank!confirmation-transaction

Triggering assumption:

A7. consumer!PIN holds

Conclusions:

C8. keypad!PIN (Detach,P1,A7)

C9. card-reader!PIN (Detach,P2,C8)

C10. card!confirmation-PIN-ok (Detach,P3,C9)

C11. card-reader!PIN-confirmed (Detach,P4,C10)

C12. CPU!authorization-request (Detach,P5,C11)

C13. bank!confirmation-transaction (Detach,P6,C12)

IDENTIFICATION OF RISKS FOR PREMISES P1 AND P2

Challenged	Risk	Reference
Premise P1	R1.1: consumer is triggered to reveal PIN via social engineering attack	CAPEC-403⋆
Premise P1	R1.2: PIN is revealed by missing PIN field masking	CWE-549
Premise P1	R1.3: PIN is revealed by brute force attack	CAPEC-49, CAPEC-70 & CAPEC-112
Premise P1	R1.4: PIN is revealed due to lack of aging policy	CWE-262
Premise P1	R1.5: PIN is collected by fake PED set to allow pharming attack	CAPEC-89
Premise P2	R1.6: PIN is revealed if sent unencrypted within the PED and the PED enclosure can be tampered with	CWE-311 & CAPEC-436⋆
Premise P2	R1.7: PIN is revealed if sent encrypted within the PED but PED enclosure can be tampered with	CAPEC-20 & CWE-327 & CAPEC-436⋆
Premise P2	R1.8: PIN is revealed via sniffer installed by PED administrators	CAPEC-65
Premise P2	R1.9: Unauthorized access to PIN is concealed via log injection-tampering-forging by PED administrators	CAPEC-93

CLASSIFICATION OF RISKS FOR PREMISES P1 AND P2

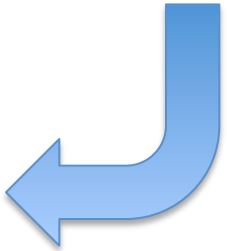
Risk	Risk treatment
R1.1	**Transfer risk**: assumed consumers take mitigations
R1.2	**Mitigate risk**: PED should obfuscate display of PIN as entered by consumers in keypad
R1.3	**Transfer risk**: assumed banks (e.g., require strong PIN policy) and consumers (e.g., avoid common, guessable PIN) take mitigations
R1.4	**Transfer risk**: assumed banks and card issuers take mitigations (e.g., by periodically requiring PIN change and card renewal)
R1.5	**Mitigate risk**: PED should use (i) authentication mechanisms, and (ii) audit mechanisms to log authorized replacements
R1.6	**Mitigate risk**: Any transmission of PIN should use well-vetted encryption algorithms
R1.7	**Mitigate risk**: (i) encryption of PIN should use accepted algorithms and recommended key sizes, (ii) cryptographic keys should be managed and protected (**Transfer risk**: assumed cards will also comply with this mitigation), (iii) PED design should allow upgrade of cryptographic algorithms
R1.8	**Mitigate risk**: Any transmission of PIN should be encrypted
R1.9	**Mitigate risk**: PED should provide access control to physical log files

Risk Mitigations

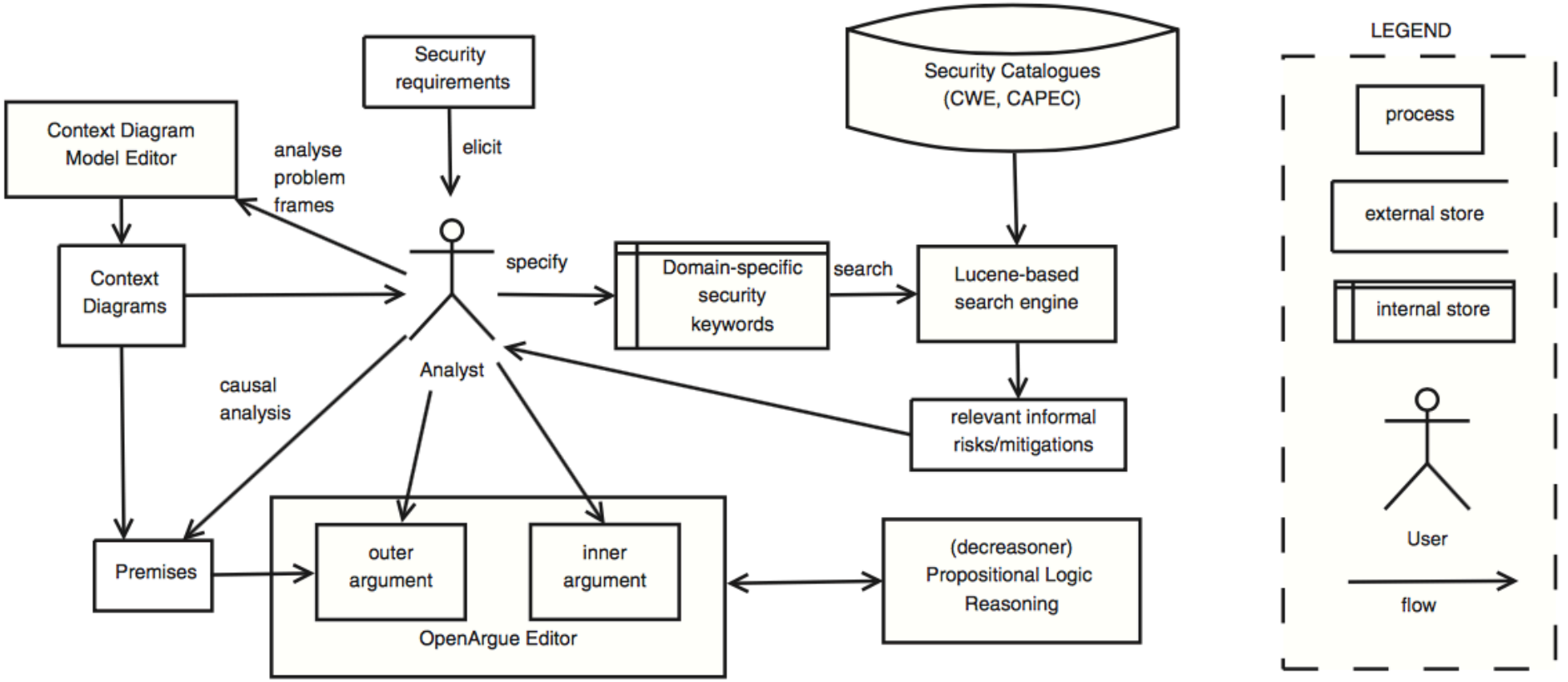
Risk	Mitigation
R1.2	M2.1: PED should obfuscate display of PIN as entered by consumers in keypad
R1.5	M2.2: PED should use authentication mechanisms
R1.5	M2.3: PED should have audit mechanisms to log authorized replacements
R1.6 & R1.7 & R1.8	M2.4: Any transmission of PIN should use well-vetted encryption algorithms and recommended key sizes
R1.7	M2.5: Cryptographic keys should be managed and protected
R1.7	M2.6: PED design should allow upgrade of cryptographic algorithms

Automated Reasoning

- Domain Specific Language (argument), supporting informal and formal specification of Toulmin arguments
- Translation from DSL to Decreasoner for event calculus-based reasoning
  - http://decreasoner.sourceforge.net



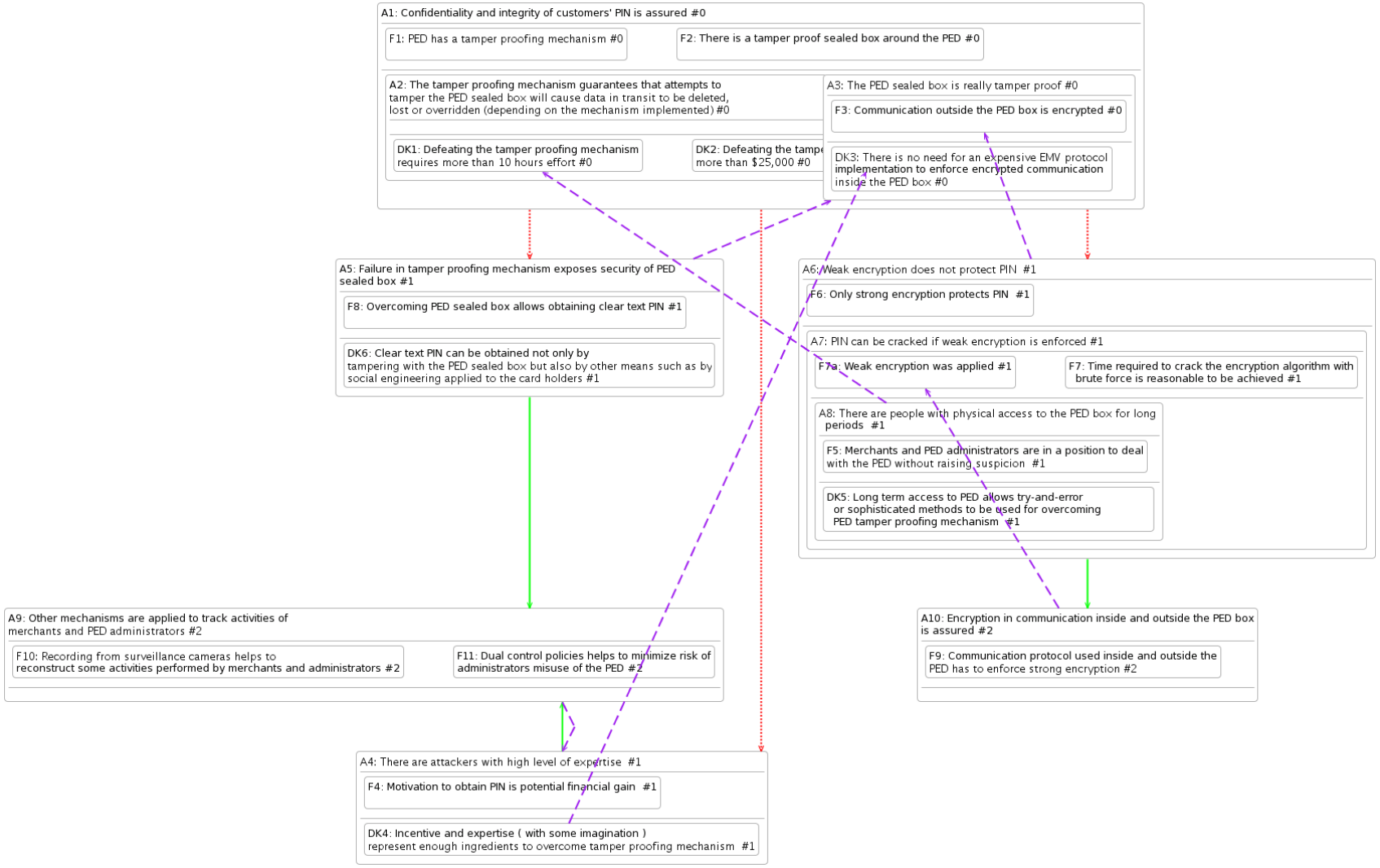
Overview of the RISA tools



Example Argument

```
1  argument: arg_rebuttal

3  boolean A1, A2, A3, F3, F4, W1, W2, W3

5  A1 rebutted by A3 on A2

7  A1 "Unauthorised access is prevented" round 1 {
8     supported by
9        A2 "Each user needs to provide
10             valid ID and passcode" round 1 {
11       supported by
12          F3 "Each legitimate user is given
13                an ID and passcode" round 2
14             warranted by
15             W2 "Users remember their IDs and
16                   passcodes" round 2
17       }
18       warranted by
19          W1 "Users without valid IDs and
20               passcodes are denied access" round 1
21 }

23 A3 "Users could divulge their IDs and
24     passcodes" round 3 priority 8 {
25    supported by
26       F4 "Some users might share their IDs and
27            passcodes"  round 3
28    warranted by
29       W3 "Shared IDs and passcodes may allow
30             unauthorised access" round 3
31 }
```

Visualizing the argument graph



Exercise 2 (offline)

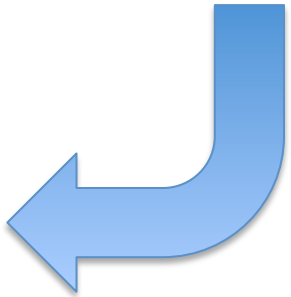
- Starting with your problem context, construct a qualitative list of risks to address your security requirements
- Without the reasoning tool, can you rank the list by precision/recall or other metrics?

Panel: Context-Dependent Evaluation of Tools for NL RE Tasks: Recall vs. Precision, and Beyond

Chair: Daniel M. Berry

Panelists: Jane Cleland-Huang, Alessio Ferrari, Walid Maalej, John Mylopoulos, Didar Zowghi

Room: Auditorio B, Building Reitoria



Tool support

- Eclipse-based tools
  - http://sead1.open.ac.uk/risa
  - http://computing-research.open.ac.uk/trac/openre
- Open Source code
  - https://github.com/problem-frames/openpf
- which depends on open-source event calculus reasoning tools (decreasoner)
  - http://decreasoner.sourceforge.net

A Guided Tour

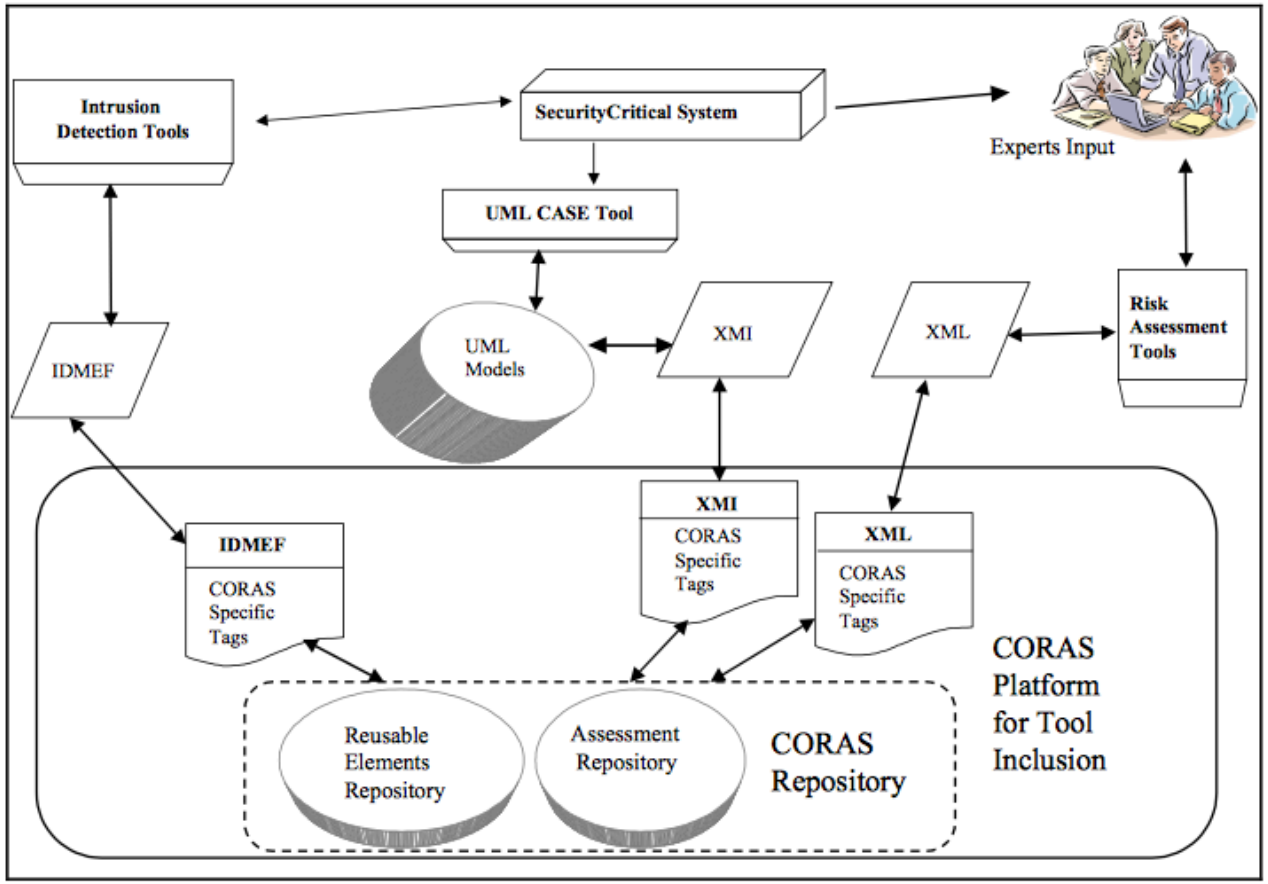
1. Risks in life
2. Qualitative Risk Assessment based on Requirements
3. Quantitative Risk Assessment based on Requirements
4. Abstract Goal Behaviors and the Right Hand Side Problems
5. Quantitative Risk Assessment based on Probabilistic Behavior Models and Requirements
6. Risk Assessment for Requirements-Driven Self-Adaptive Systems

Quantitative Reasoning of Risks

- Risk = Likelihood x Impact
- With a list of risk factors, give likelihood from [0,1] and impact arbitrary number, then the total risk of selected risk factors is the sum of risks
- Prioritisation, or the 80-20 Pareto rule:
  - Deal with the risk in the order of HH, (HL | LH), LL
  - Or simply deal with the higher risks first

Model-based Risk Assessment

- E.g., CORAS: http://coras.sourceforge.net

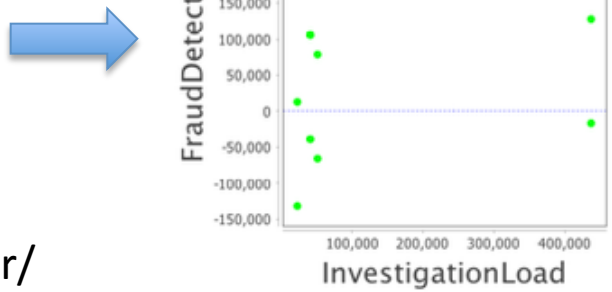


Elicitation of contribution labels of goal models using AHP approach

S. Liaskos, R. Jalman and J. Aranda, "On eliciting contribution measures in goal models," *2012 20th IEEE International Requirements Engineering Conference (RE)*, Chicago, IL, 2012, pp. 221-230.

RADAR Approach

```
NbrFraudPerAccountBeforeBlocked = decision("blocking policy"){
        "block first" : NbrFraudBeforeDetection;
        "investigate first" : NbrFraudBeforeDetection + NbrFraudDuringInvestigation;
}
NbrFraudBeforeDetection = decision("processing type"){
        "continuous" : 1 / ContinuousTrueAlertRate;
        "batch" : NbrFraudsPerCompromisedAccountPerDay / BatchTrueAlertRate ;
}
ContinuousTrueAlertRate = decision("fraud detection method"){
        "classifier" : ContinuousAlertThreshold;
        "rule-based" : deterministic(0,75)
}
BatchTrueAlertRate = decision("fraud detection method"){
        "classifier" : BatchAlertThreshold;
        "rule-based" : deterministic(0,80);
}
ContinuousAlertThreshold = decision("alert threshold"){
        "high" : deterministic(0.9);
        "medium" : deterministic(0,8);
        "low" : deterministic(0,7);
}
BatchAlertThreshold = decision("alert threshold"){
        "high" : deterministic(0.95);
        "medium" : deterministic(0,85);
        "low" : deterministic(0,75);
}
```



https://ucl-badass.github.io/radar/

- Using DSL to specify risks quantitatively on architectural choices (goal alternatives)
- Derive Pareto fronts by simulations

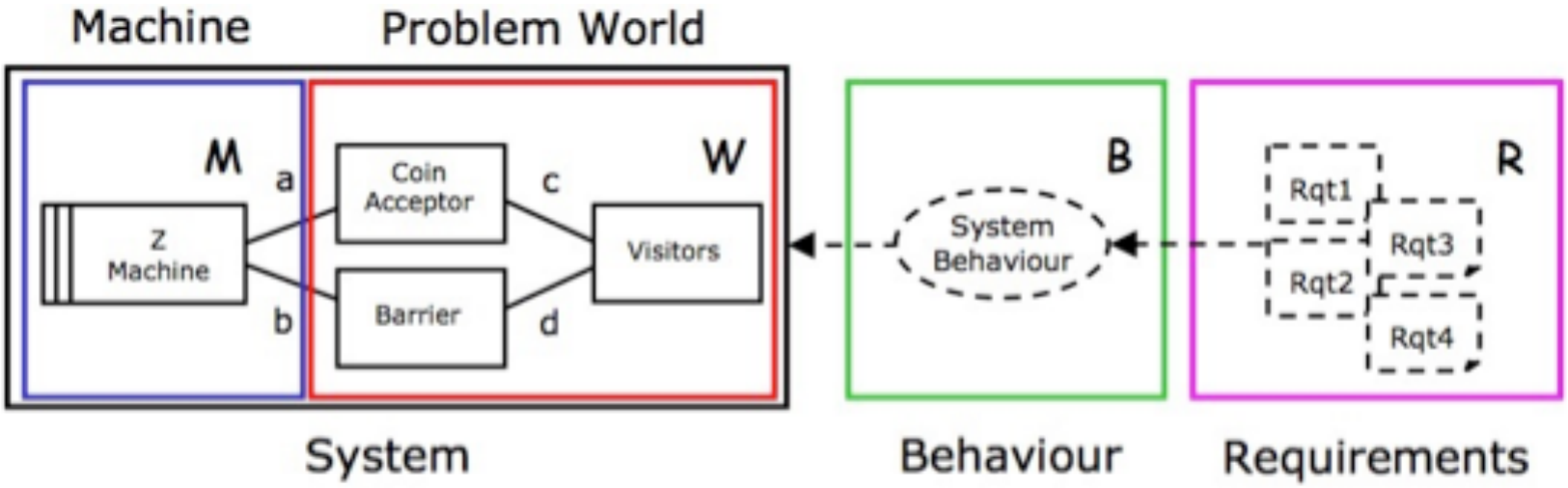
S. A. Busari, E. Letier, RADAR: A Lightweight Tool for Requirements and Architecture Decision Analysis, Proc. 39th International Conference on Software Engineering 2017 (ICSE 2017).

A Guided Tour

1. Risks in life
2. Qualitative Risk Assessment based on Requirements
3. Quantitative Risk Assessment based on Requirements
4. Abstract Goal Behaviors and the Right Hand Side Problems
5. Quantitative Risk Assessment based on Probabilistic Behavior Models and Requirements
6. Risk Assessment for Requirements-Driven Self-Adaptive Systems

Jackson's new thoughts

- Abstract goal behaviors



- Right hand side problem

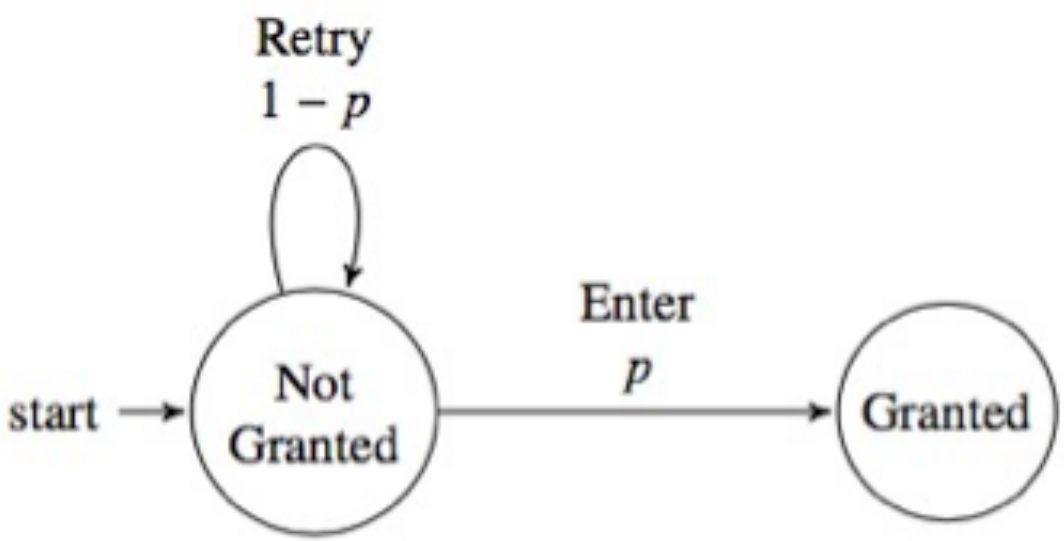
The Right-Hand Side Problem: Research Topics in RE by Michael Jackson [slides]

A Guided Tour

1. Risks in life
2. Qualitative Risk Assessment based on Requirements
3. Quantitative Risk Assessment based on Requirements
4. Abstract Goal Behaviors and the Right Hand Side Problems
5. Quantitative Risk Assessment based on Probabilistic Behavior Models and Requirements
6. Risk Assessment for Requirements-Driven Self-Adaptive Systems

Why consider probabilistic behavior model for risks?

- A security example (simplified from PED)
- Known unknowns: p the probability



Exercise 3

- What is the risk of exposing the bank account to an attacker?
  - Hint: consider the “traces”, or sequences of transitions in the behavioral model
- What are the strategies to reduce the risk? (offline)

Answer to the first question

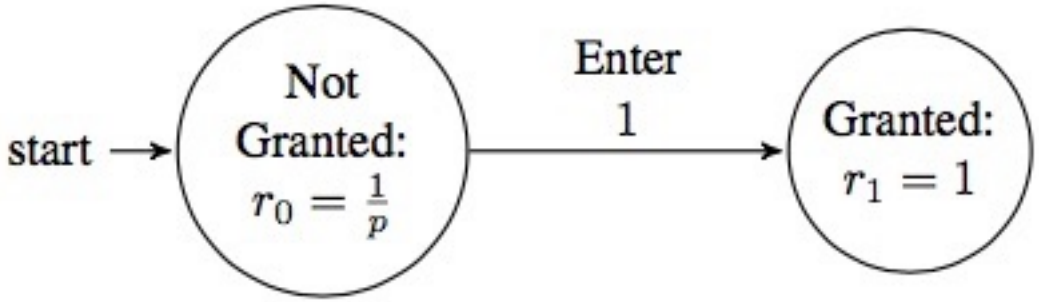
Definition 4 (Recurrence equations, probability matrix, likelihoods, and converging risks)**.** *Intuitively, when the simulation of an exploration machine converges, the overall likelihood on each state s is a constant:*

$$p(s) = \lim_{n \to \infty} p(s_n) \tag{5}$$

and so do the risks by Definition 3:

$$r^*(s) = \lim_{n \to \infty} r^n(s) \tag{6}$$

Enumerate all traces and sum

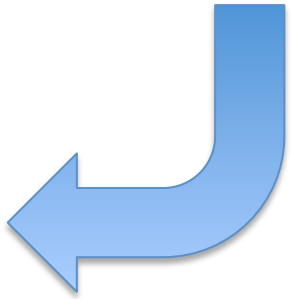


$$p > 0.$$

PRISM

Existing work has the following problems:

- Cyclic traces
- Symbolic solutions



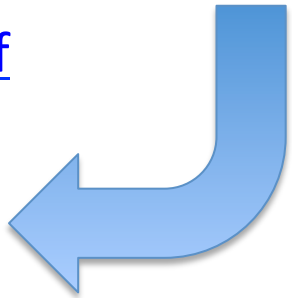
- M. Kwiatkowska, G. Norman, and D. Parker, "PRISM 4.0: Verification of probabilistic real-time systems," in *International Conference on Computer Aided Verification (CAV 2011)*. Springer Berlin Heidelberg, 2011, pp. 585–591.

Risk Explore tool

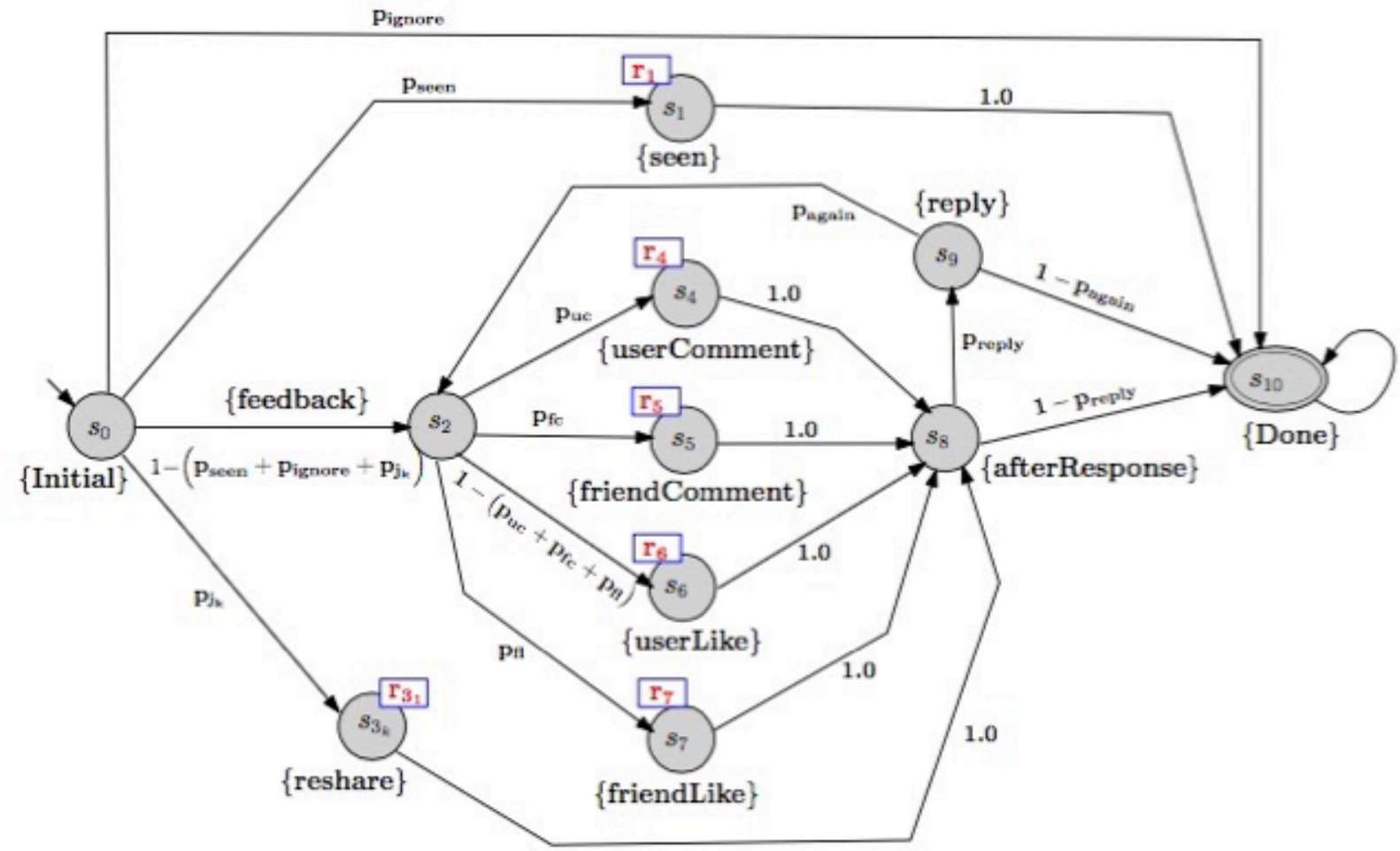
- Perform symbolic computation of risks
- Visualise impact
- Efficiently compute minimal risk under symbolic constraints using search-based optimisation algorithms

Armstrong Nhlabatsi, Yijun Yu, Thein Than Tun, Arosha K. Bandara, Niamul Khan, Khaled M. Khan, and Bashar Nuseibeh. "Beyond 'Access Denied': Risk-based Exploration of Adaptive Access Control Systems". Techical Report TR2016-04. The Open University, UK. http://computing-reports.open.ac.uk/2016/TR2016-04.pdf

- https://github.com/yijunyu/demo-riskexplore



A privacy example



Y. Rafiq, L. Dickens, A. Russo, A. K. Bandara, M. Yang, A. Stuart, M. Levine, G. Calikli, B. A. Price, and B. Nuseibeh, "Learning to share: Engineering adaptive decision-support for online social networks," in 32nd IEEE/ACM International Conference on Automated Software Engineering (ASE 2017), 30 October - 3 November 2017, University of Illinois at Urbana- Champaign, Illinois, USA., to appear.

Risk profile function

```
pseen*r1+pjk*r3-(r4*puc*(pjk-(1-pseen-pignore)
-pagain*preply*pjk))/(1-pagain*preply*pfl
+pagain*preply*(pfl-(1-puc-pfc))-pagain*preply*pfc
-pagain*preply*puc)-(r5*pfc*(pjk-(1-pseen-pignore)
-pagain*preply*pjk))/(1-pagain*preply*pfl
+pagain*preply*(pfl-(1-puc-pfc))-pagain*preply*pfc
-pagain*preply*puc)+(r6*(pfl-(1-puc-pfc))*(pjk-
(1-pseen-pignore)-pagain*preply*pjk))/(1
-pagain*preply*pfl+pagain*preply*(pfl-(1-puc-pfc))
-pagain*preply*pfc-pagain*preply*puc)-(r7*pfl*(pjk
-(1-pseen-pignore)-pagain*preply*pjk))/(1
-pagain*preply*pfl+pagain*preply*(pfl-(1-puc-pfc))
```

Singularity condition

$$0<1-pagain*preply*pfl+pagain*preply*(pfl-(1-puc-pfc))$$

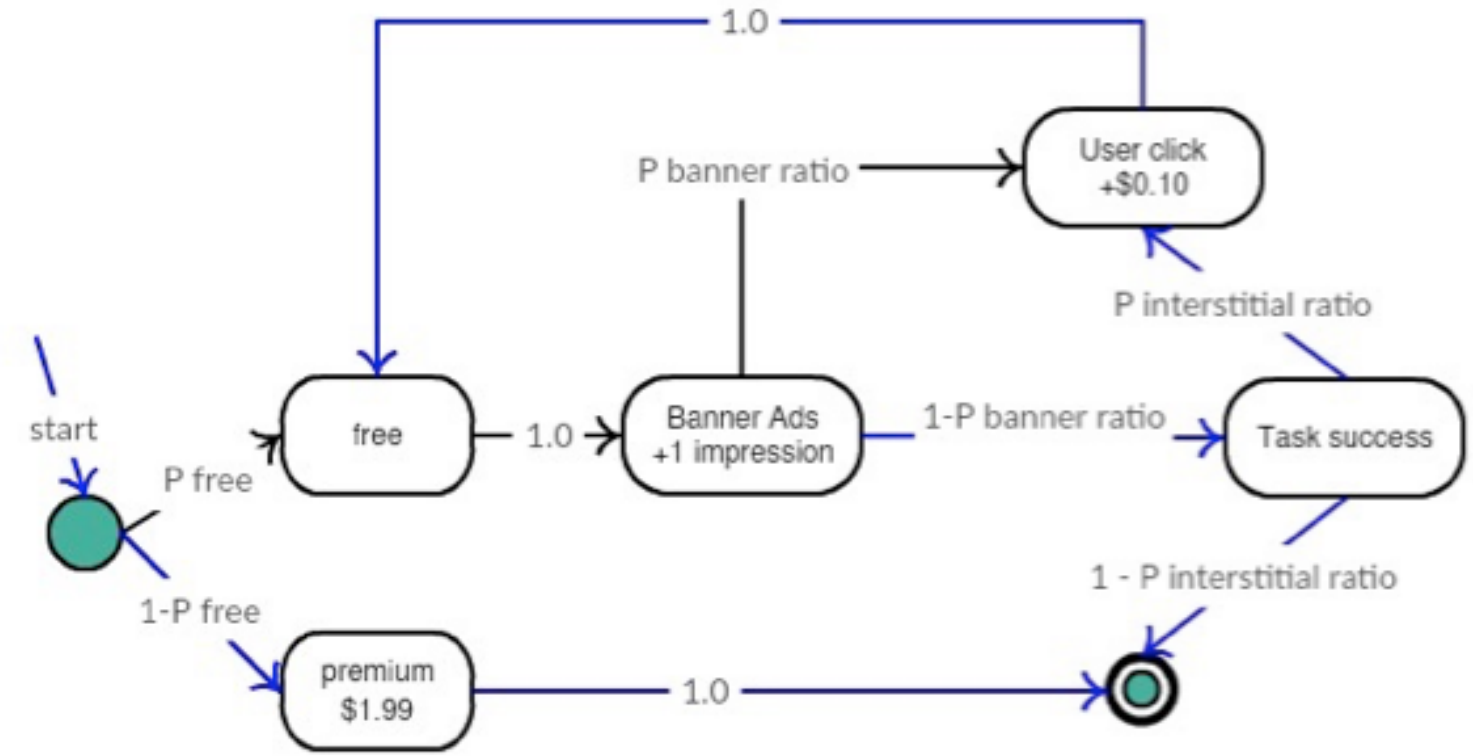
$$-pagain*preply*pfc-pagain*preply*puc$$

If r1=r2=r3=r4=r5=r6=r7=1, the minimal risk = 0.012. when

pseen = 0.006239582,
pignore = 0.987266657,
pjk = 0.003001324,
puc = 0.115949677,
pfc = 0.446085095,
pfl = 0.131866686,
preply = 0.003728548,
pagain = 0.048901284.

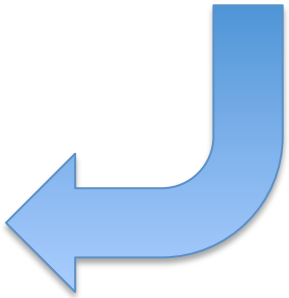
Business requirement example

- Android App Advertisement model



Computation results

- Risk profile function:
- (1-pfree)*Premium+(Impression*pfree)/(1-(pbanner-pinterstitial*(pbanner-1)))-(Click*(pinterstitial*(pbanner-1)-pbanner)*pfree)/(1-(pbanner-pinterstitial*(pbanner-1)))
- When Premium=$1.99, Impression=$0.01, Click=$0.10
  - pfree=1, pbanner=1, pinterstitial=1 // Freemium
  - If additionally pbanner=0.1, and pinterstitial=0.1, then pfree=0 // Premium

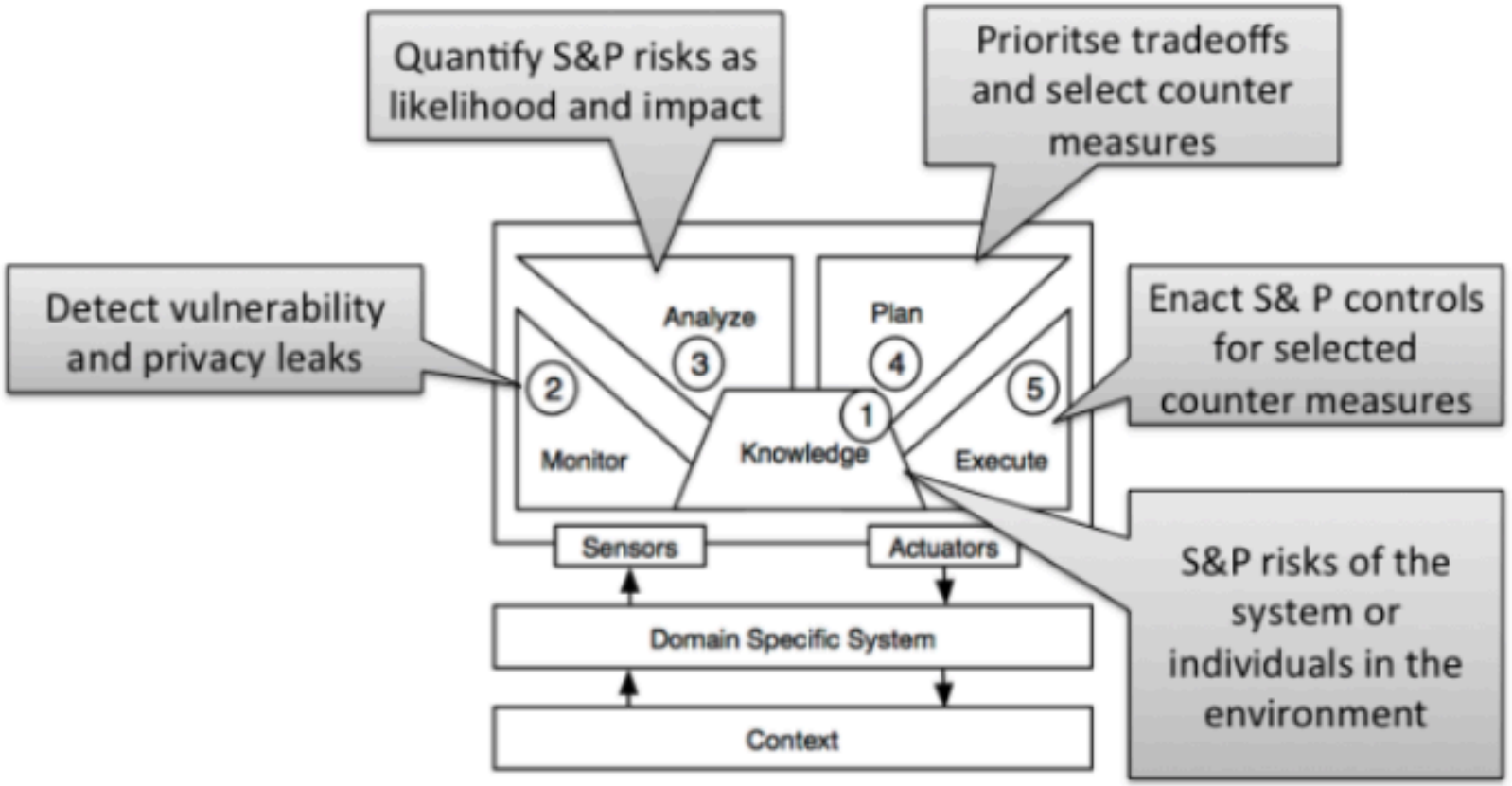


Yijun Yu, Chun Liu. “Little Model in Big Data: An Algebraic Approach to Analysing Abstract Software Behaviours,”. Ruan Jian Xue Bao/Journal of Software, 2016. [doi: 10.13328/j.cnki.jos.000000]

A Guided Tour

1. Risks in life
2. Qualitative Risk Assessment based on Requirements
3. Quantitative Risk Assessment based on Requirements
4. Abstract Goal Behaviors and the Right Hand Side Problems
5. Quantitative Risk Assessment based on Probabilistic Behavior Models and Requirements
6. Risk Assessment for Requirements-Driven Self-Protecting Systems

Risk-based Self-Protection architecture

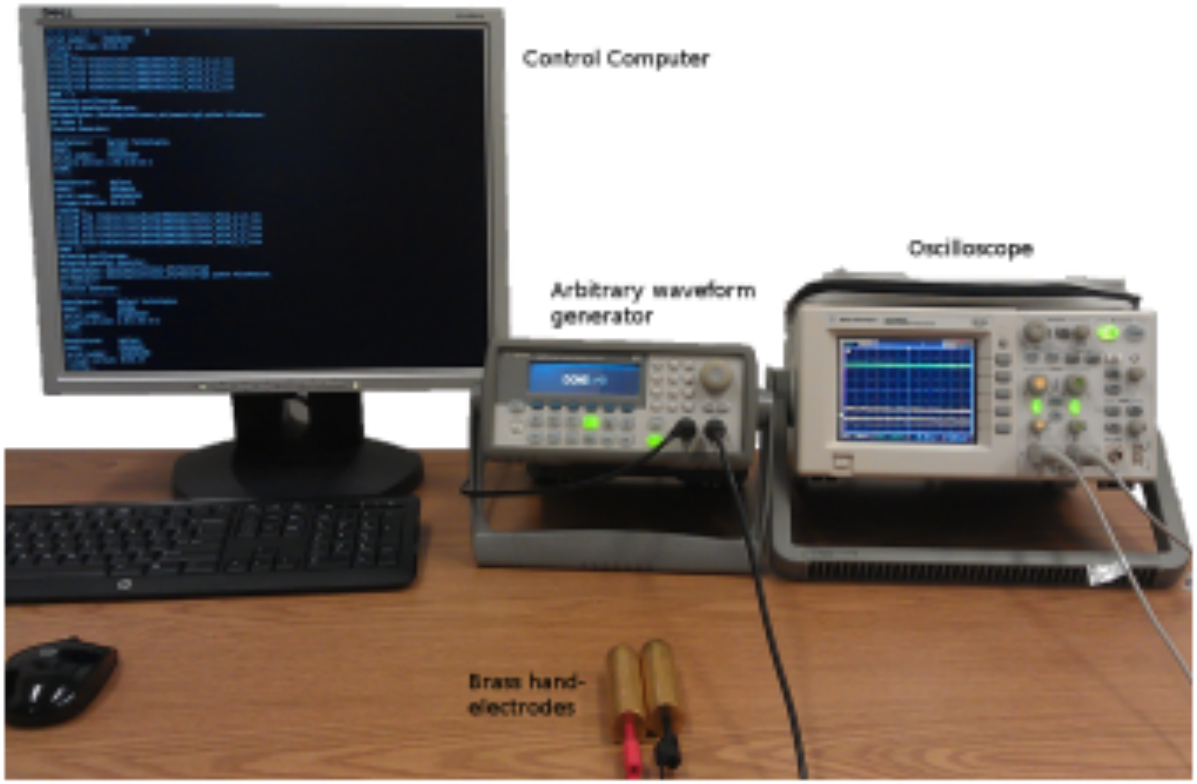


Yu, Yijun and Tun, Thein (2017). Snap Forensics: A Tradeoff between Ephemeral Intelligence and Persistent Evidence Collection. In: 1st International Workshop on Software Engineering and Digital Forensics, 4 September, 2017, Padeborn, Germany.

UK National Rail's plan

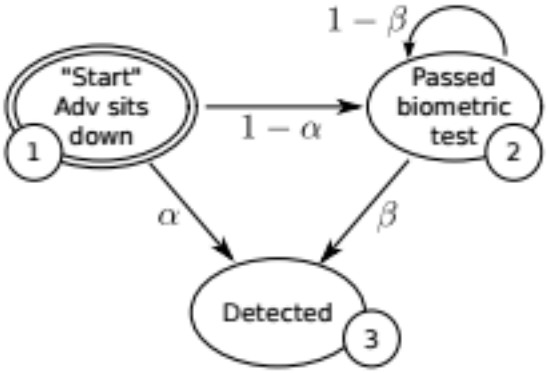
- *Andy Weir. "UK rail network considers using iris and fingerprint scans as part of digital transformation", **Evening Standard**, Feb 8, 2017.*

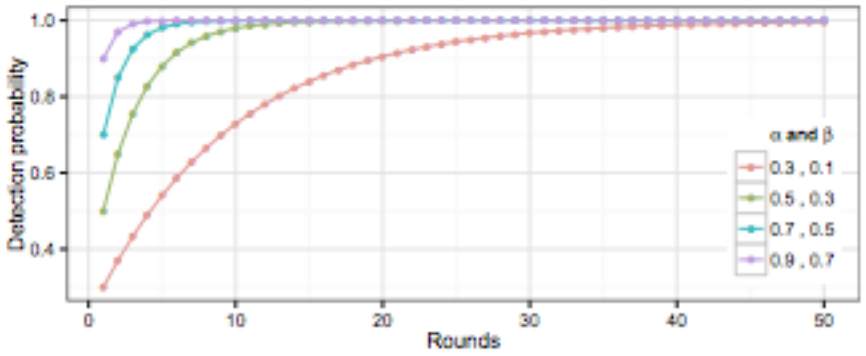
Biometric Authentication



Ivan Martinovic, Kasper Bonne Rasmussen, Marc Roeschlin, Gene Tsudik: Authentication using pulse-response biometrics. Commun. ACM 60(2): 108-115 (2017)

Markov model of continuous authentication and simulation of detection probability



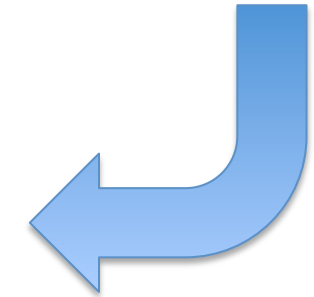


$$[1,0,0] \cdot P^i = [0, (1-\alpha)(1-\beta)^{i-1}, 1-(1-\alpha)(1-\beta)^{i-1}]$$

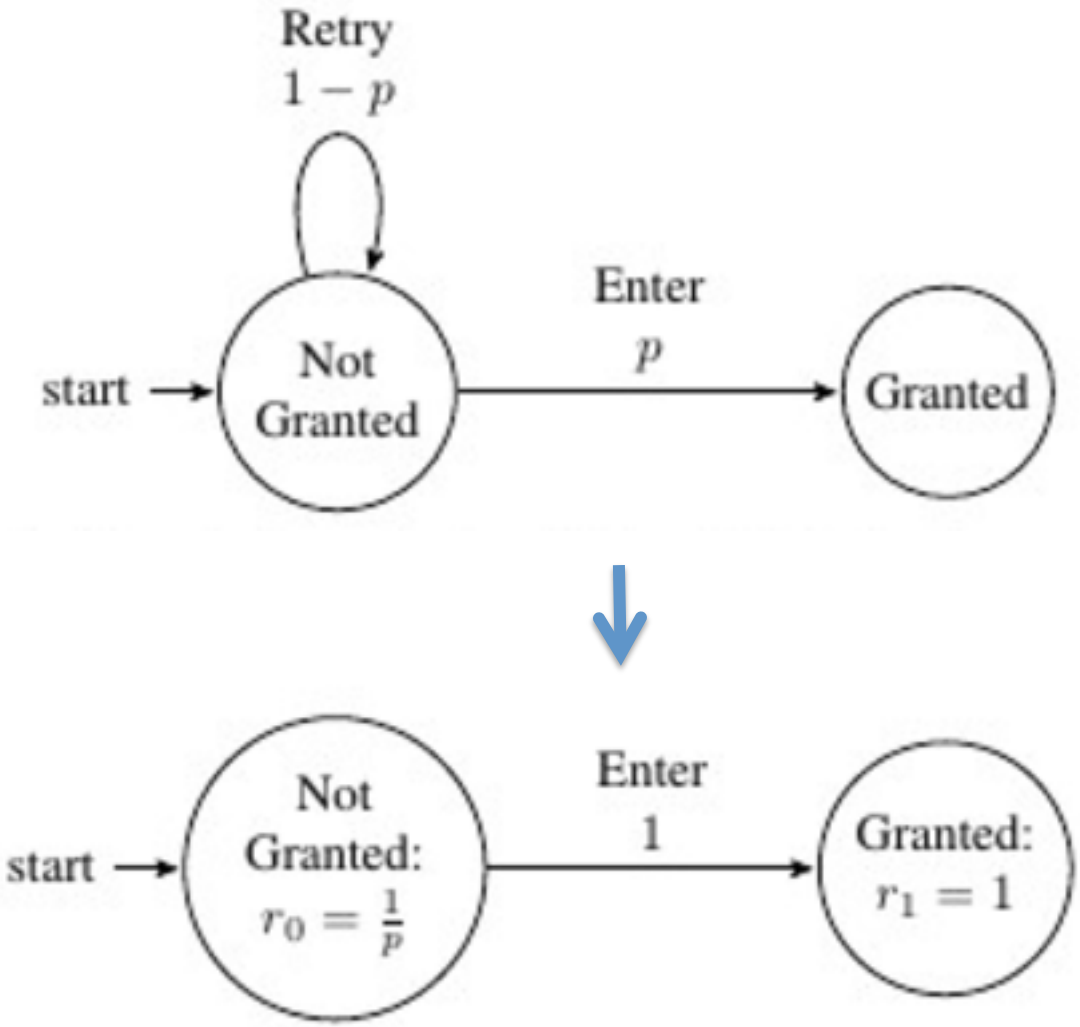
$$\begin{aligned} 1-(1-\alpha)(1-\beta)^{i-1} &= 1-(1-0.99)(1-0.3)^{10-1} \\ &= 1-0.01 \cdot 0.7^9 = 0.99959 \approx 99.96\% \end{aligned}$$

Challenges for Probabilistic Model Checkers

- Simulation requires convergence
  - However, when N approaches infinity, the probability may no longer be a constant
- Numeric computations are hard in system identification for self-adaptive systems
  - Antonio Filieri, Giordano Tamburrelli, Carlo Ghezzi: Supporting Self-adaptation via Quantitative Verification and Sensitivity Analysis at Run Time, TSE'16



Insight: to remove cycles



Solving Linear Recurrent Equations

$$\begin{bmatrix} p_0 \\ p_1 \end{bmatrix} = \begin{bmatrix} 1-p & 0 \\ p & 0 \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

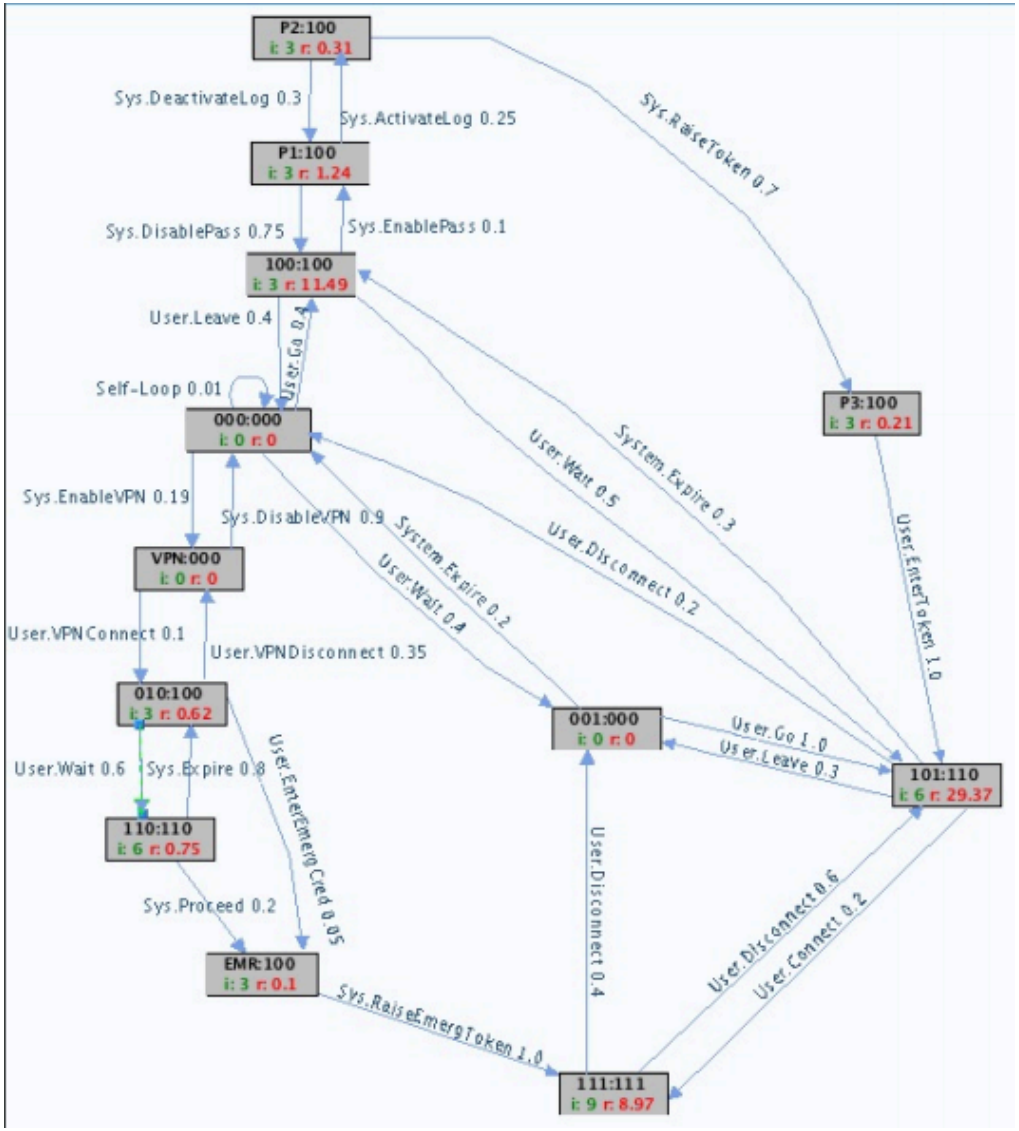
$$\begin{bmatrix} p_0 \\ p_1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ p & 0 \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \end{bmatrix} + \begin{bmatrix} \frac{1}{p} \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} p_0 \\ p_1 \end{bmatrix} = \begin{bmatrix} \frac{1}{p} \\ 1 \end{bmatrix}$$

Applied to Adaptive Access Control

Event/Action	Description
User.Wait	User is waiting for working hours.
User.Go	User goes to and reaches hospital premises.
User.Connect	User connects to hospital WiFi.
User.VPNConnect	User connects to hospital network using VPN.
User.EnterToken	User enters a security token.
User.EnterEmergCred	User enters emergency credentials.
Sys.EnableVPN	System enables the VPN features for secure connect.
Sys.RaiseEmergToken	A trusted hospital official raises an emergency token confirming that a patient is in a critical condition.
Sys.EnablePass	System enable the user's access card for access to the hospital outside office hours.
Sys.ActivateLog	System activate logging of user actions.
Sys.RaiseToken	System raises a security token to access outside office hours.

Simulate to Divergence!

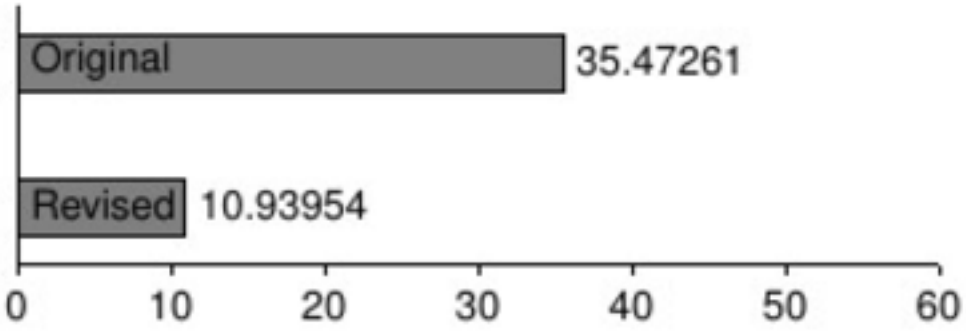


Turn transition probability into independent variables

- 15 free variables in range [0,1], and 12 reward variables in combination of {READ, WRITE, SHARING}
- A risk profile function is thus obtained symbolically, which can print to 5 pages

$$
\begin{aligned}
Risk = ((r + w) * (p02/(1 - (-p25 * (p56 - 1))/((p67 - 1)* \\
p56 + 1) - p32 * (p23 + (p25 * p73 * p67 * p56)/((p67 \\
- 1) * p56 + 1))) - (-p32 * p13 * (p01 + (p02 * p31* \\
\ldots \\
+ (p25 * p73 * p67 * p56)/((p67 - 1) * p56 + 1)))))
\end{aligned}
$$

Optimization results (minimal risks)

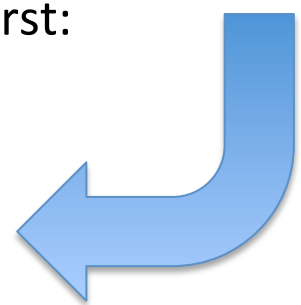


$\|S\|$	$\|\delta\|$	Simul.	Numer.	PRISM	Symb.	DEoptim
2	2	1.46	0.74	2.42	1.26	0.36
7	10	2.03	0.79	2.49	2.92	0.48
11	19	3.18	0.77	2.52	8.08	1.59
12	27	7.15	0.83	2.83	26.67	11.56

Parallel composition

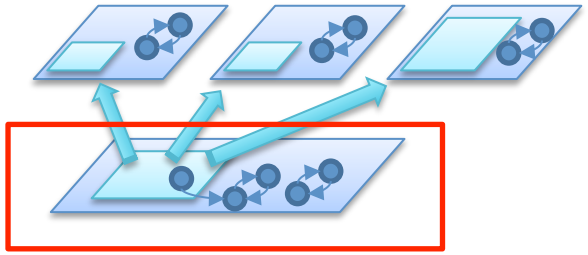
- $E \mid\mid x_I \mid = G$

  Nicholas D'Ippolito, Víctor Braberman, Jeff Kramer, Jeff Magee, Daniel Sykes, Sebastian Uchitel. Hope for the Best, Prepare for the Worst: Multi-tier Control for Adaptive Systems, ICSE'14.

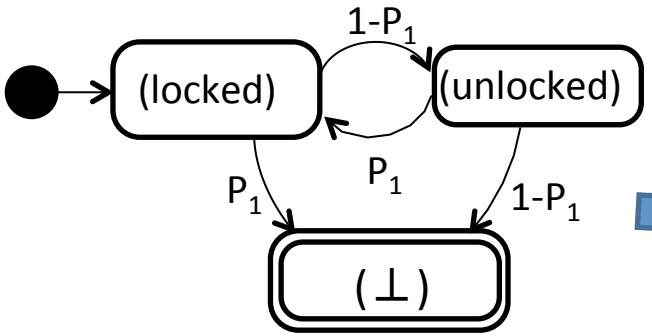


- Given multiple symbolic DTMC's, compose them in parallel
  - https://github.com/yijunyu/demo-riskexplore
- Compute "adaptive transparency"

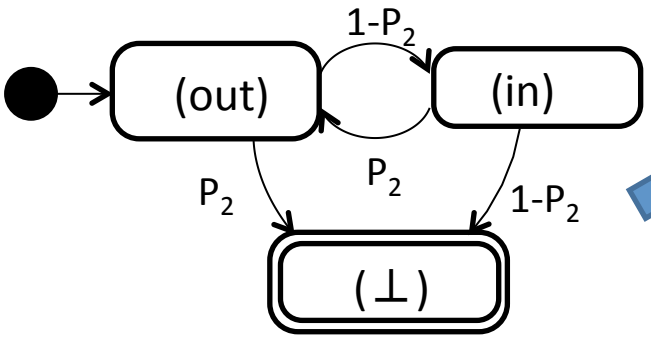
System Model



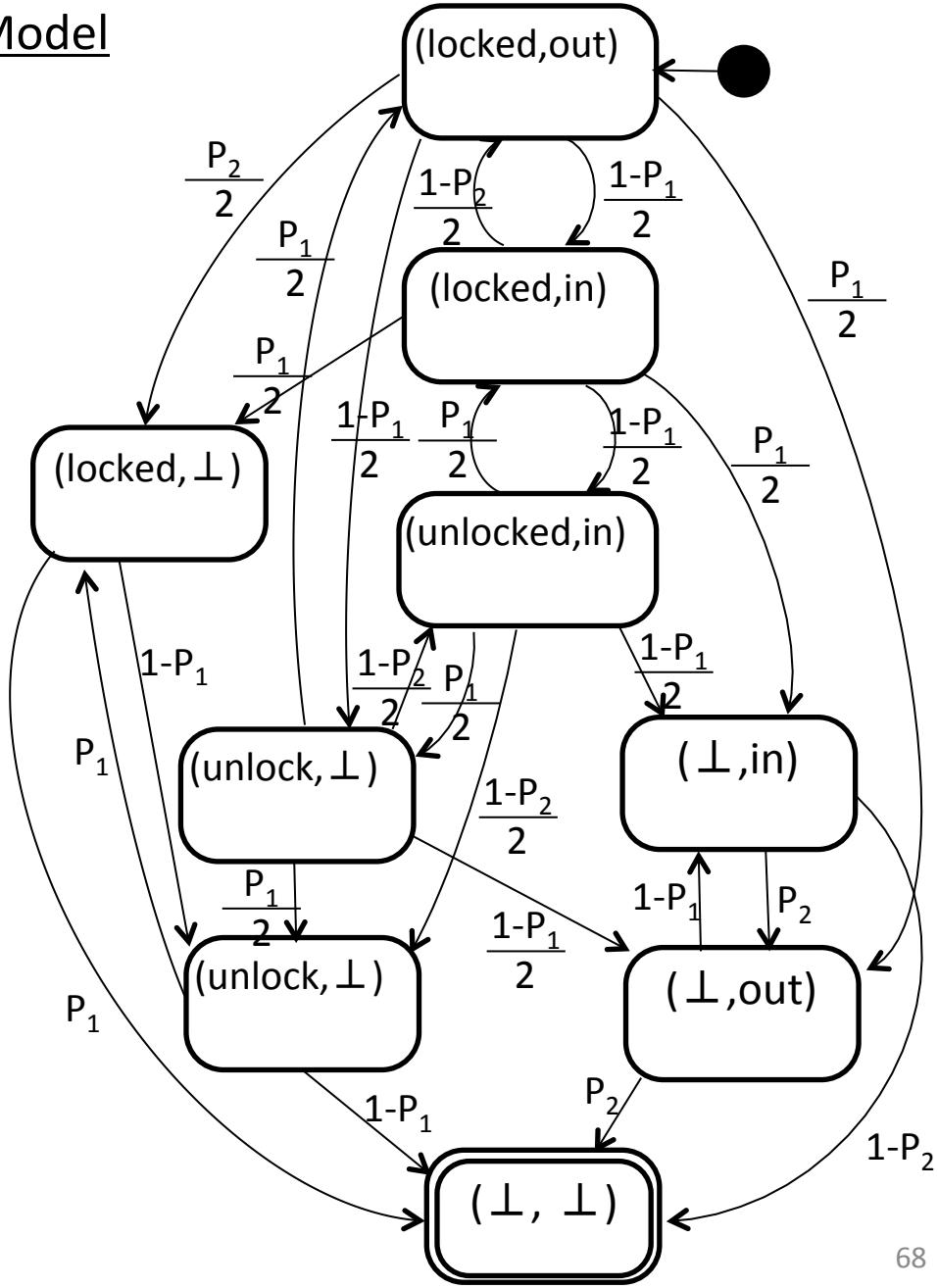
…



Door of Office



User



End of the Tour

1. Risks in life
2. Qualitative Risk Assessment based on Requirements
3. Quantitative Risk Assessment based on Requirements
4. Abstract Goal Behaviors and the Right Hand Side Problems
5. Quantitative Risk Assessment based on Probabilistic Behavior Models and Requirements
6. Risk Assessment for Requirements-Driven Self-Adaptive Systems
7. If you want to try the tool

Install Docker

https://docs.docker.com/machine/install-machine/#installing-machine-directly

* If you are using Mac OSX

brew install docker-machine
docker-machine **create** *--driver virtualbox default*
docker-machine ssh default

How to use our tool?

- docker run -it yijun/riskexplore
  cd /demo
  ./r examples/PIN

PRISM specification of PIN example

/demo # cat examples/PIN.pm

```
dtmc

const double p;
const double r1;
const double r2;

module PIN

s : [0..1] init 0;

[]s=0->p:(s'=0)+(1-p):(s'=1);

endmodule

rewards "impact"
  s=0: r1;
  s=1: r2;
endrewards
```

examples/composed

examples/PIN

/demo/prism/prism/bin/prism examples/PIN.pm -exportmodel examples/PIN.all -const p=0.1 -const r1=0.1 -const r2=0.1

examples/PIN-symbolic.pm

NormaliseMDP({{p,0},{(1-p),0}},{r1,r2})

r =

	0
0	r1/(1-p)
1	r2

p2 =

	0	
0	1	0
1	1	1

i2 =

	0
0	r1/(1-p)
1	r2

0<(1-p)

The total risks is 0 + (r1/(1-p)) + (r2)

P =

	0	1	
0	0	0	0
1	1	0	1

c =

	0
0	1/(1-p)
1	0

Summary and on-going work

- Risk based exploration of adaptive systems
  - Forensic analysis for continuous authentication [CACM'17] and adaptive access control [QNRF]
  - Proactive forensics [Pasquale et al. RE'13]
  - Adaptive transparency for security risk assessment [to submit with NII colleague]
  - Privacy risk and social benefit tradeoffs [TrustCom'14]
- Bottom line: self-adaptive systems cannot afford long simulation, hence model-based risk assessment is the most promising approach [Filieri et al, TSE'16]

End of the Tour

1. Risks in life
2. Qualitative Risk Assessment based on Requirements
3. Quantitative Risk Assessment based on Requirements
4. Abstract Goal Behaviors and the Right Hand Side Problems
5. Quantitative Risk Assessment based on Probabilistic Behavior Models and Requirements
6. Risk Assessment for Requirements-Driven Self-Adaptive Systems
7. Welcome to contact me at: y.yu@open.ac.uk