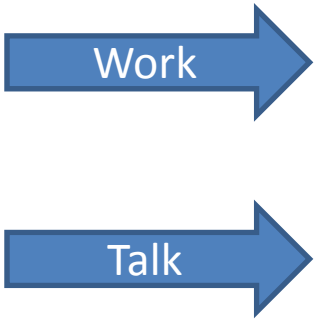
Argumentation-Based Security Requirements Elicitation: the next round

Dan Ionita
Jan-Willem Bullee
Roel Wieringa
University of Twente

Argumentation-Based Security Requirements Elicitation: the next round



Dan Ionita
Jan-Willem Bullee
Roel Wieringa
University of Twente

Research context

- FP7 Integrated Project TREsPASS
- Aims to develop quantitative support for security risk assessment of systems consisting of software, physical entities, people.
- Cases provided by companies in the project:
  - Home payment system
  - Cloud infrastructure
  - Telco fraud

Minority goal in the project

- No quantification of probabilities
- No quantification of impact
- Limited resources (time, money) to do the risk assessment and to do mitigations
- Incomplete information about target of assessment

Core idea

The structure of design arguments:

- Context & Artifact → Effects
- Effects contribute to stakeholder goals

Applied to a system:

- Some system in context & threat mitigations → Security goal

We would like to develop a method that delivers arguments like this.

Applied to a risk assessment method:

- System development & Argumentation-based risk assessment method → Suitably justified mitigations

Related work

Toulmin 1958	Against formalism in logic; informal argumentation structures modelled on legal argumentation .	Philosophical analysis
Haley et al 2005 (Open University)	Security arguments	Cannot deal with incomplete and uncertain information, nor with limited resources for risk assessment
Franqueira et al. 2011 (OU and us)	Security arguments plus public vulnerability catalogs	Complex to use, not scalable
Yu et al (OU)	OpenArgue tool for manipulation of argument graphs	Must write pseudo-code. Overhead
Prakken, Ionita, Wieringa 2013	Argumentation game formalized in defeasible logic called ASPIC	Complex to use, not scalale

Proposed RA method (so far)

- Security experts alternate between playing role of attacker and defender
- Architecture model of Target of Assessment
- Defenders can decide to change the architecture
- Spreadsheet stores and manipulates arguments. Each row contains
  - Claim,
  - Assumptions,
  - Facts,
  - Inference rule A&F -> C,
  - arguments defeated by this (if any),
  - architecture components referred to,
  - status of the argument (defeated or not, so far in the game)

At the end of the game

- Attacker's arguments that are not defeated represent accepted risks
- Attacker's argument that are defeated are risks that are reduced, eliminated or transferred.

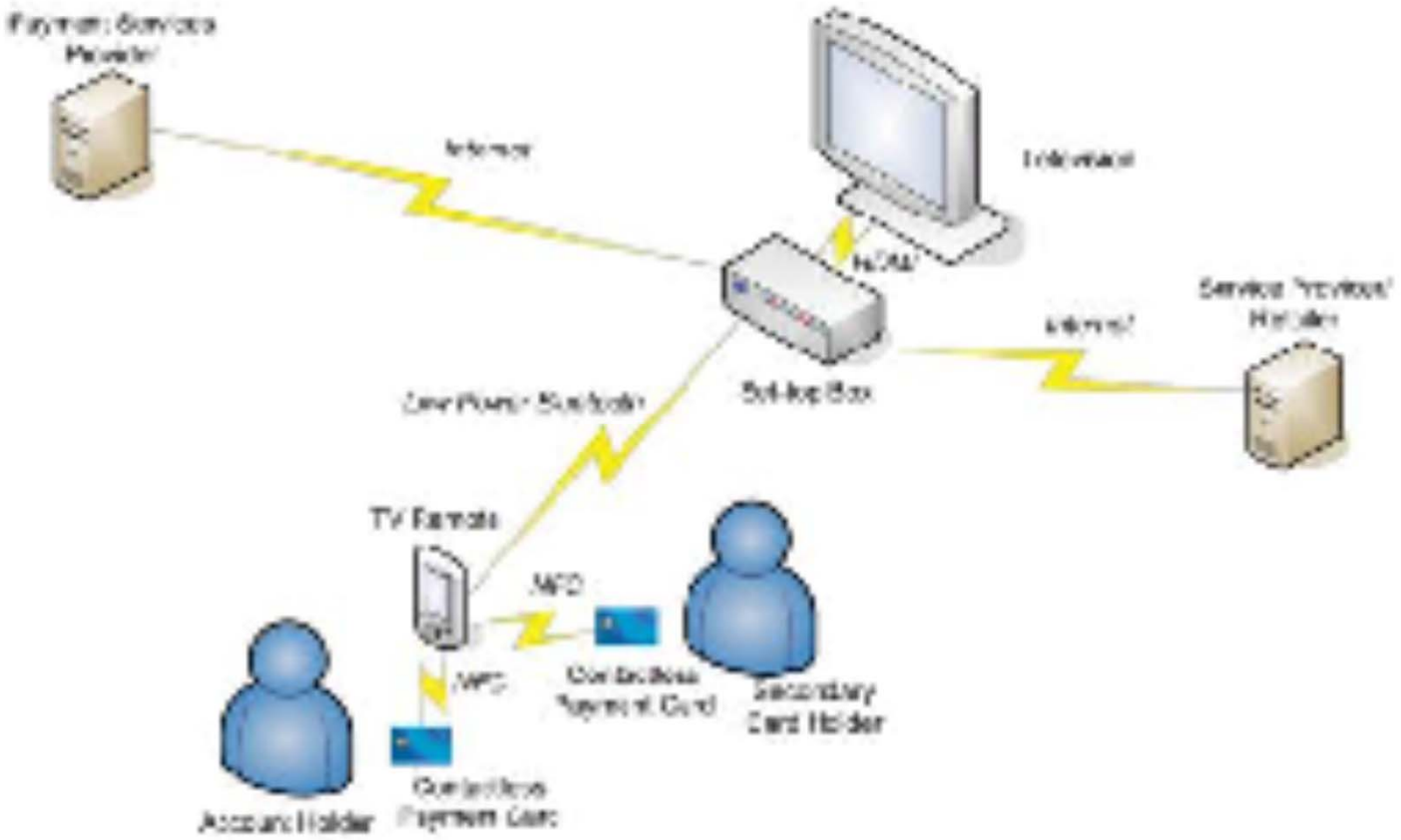
Research method to develop and validate the RA method

- Version 0: Use ASPIC to formalize argumentation game, illustrate with tiny example
- Version 1: Simplify the method
- Version 2: Test on Home payment system with students as experts; simplify the method further & develop tool
- Version 3: Test on HPS with experts; improve method
- Version 4: Use on cloud infrastructure with experts; improve method

Minority goals revisited

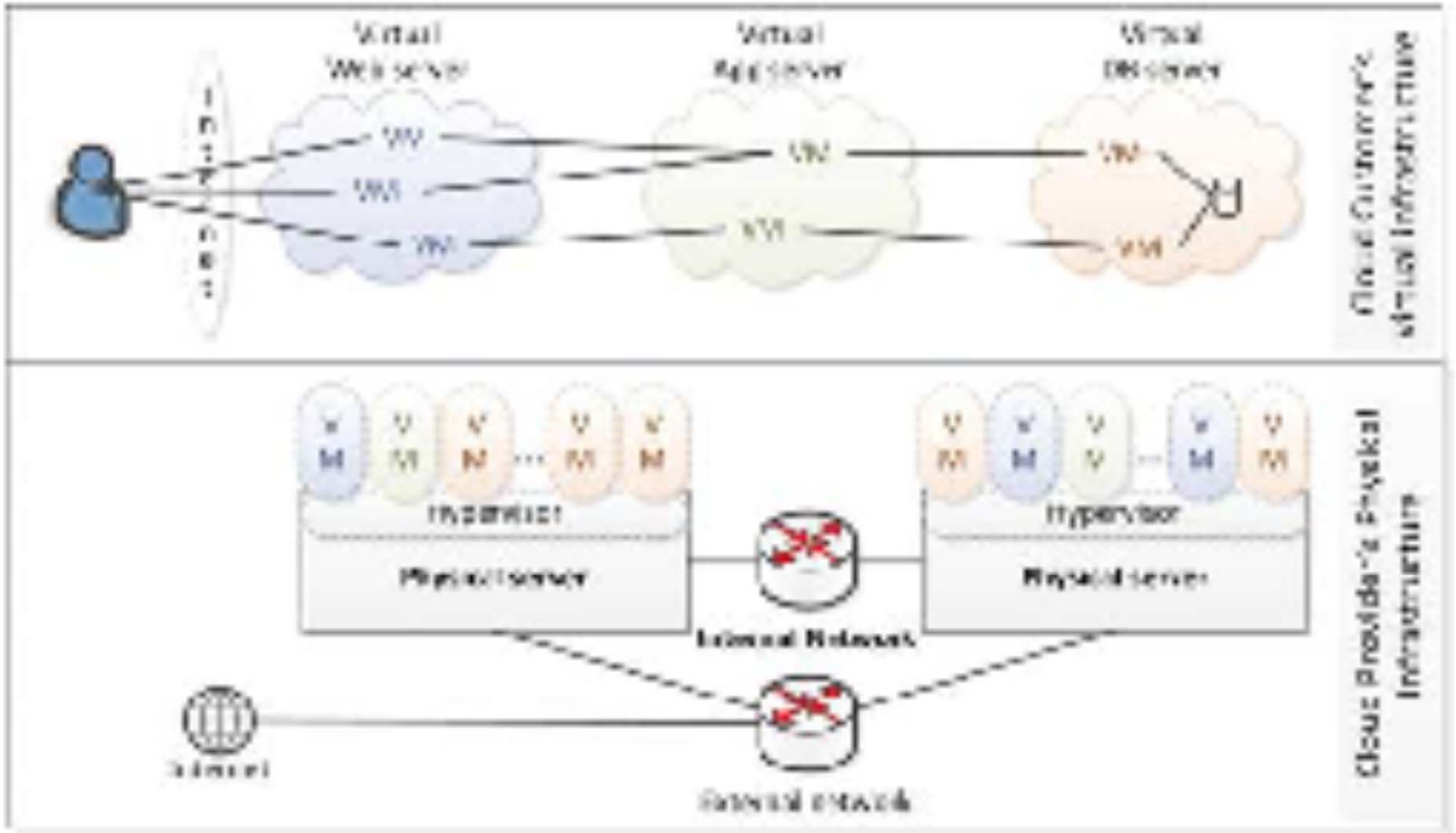
- No quantification of probabilities
- No quantification of impact
- Limited resources (time, money) to do the risk assessment and to do mitigations
- Incomplete information about target of assessment

Case 1
Used in case studies 1 and 2



Player	CLAIM		Inference Rule		Assumptions		Facts		Rebuts	Status	Flags
A/D	#	txt	#	txt	#	txt	#	txt	#	IN/OUT	T/R
A	C0	Listen in to Bluetooth: gather authentication/user data	R0	⇒	A0	Bluetooth signal can be received outside	F0	Range of Bluetooth is 10m		OUT	
D	C1	Authentication data is encrypted	R1	⇒	A1	AES encryption is good enough	F1	Bluetooth with 2.1 (AES) encryption	C0	IN	R
A	C2	User can be socially engineered to wire money	R2	⇒	A2	Attacker can gain user's trust;	F2	-		OUT	
D	C3	Social Engineering is user risk	R3	⇒	A3	-	F3	End-user agreement transferring liability for SocEng attacks	C2	IN	T
A	C4	User credentials can be stolen by peeking through the window	R4	⇒	A4	Apartment located on bottom floor(s); Curtains open	F4	-		IN	

Case 2
Used in case study 3



Observations

- Inference rules are obvious: need not be stated. What remains are traceability links. Improves justifiability and reusability of mitigations.
- There are infinitely many asssumptions. Argumentation is a way to make relevant assumptions explicit.
- Each argument round is only 2 steps. Unlike legal arguments.
- Defeat is complete or partial (eliminated or reduced risk)
- Consequences of “undefeat” are accepted or transferred.
- When formulating an attack, experts already think of mitigation against it. to get more results: Partition experts in attackers and defenders.
- If there is no application architecture, then architecture-based arguments cannot be given.
  - In the cloud infrastructure checklists of risks are given
  - Mitigation by SLA between customer and provider.

Future work

- Improve tool support
- Do more case studies (i-voting, more cloud, e-banking)
- Investigate relation among
  - Kind of system
  - What is known about the system
  - Security goals
  - Kind of risk assessment technique

- Questions