Graphical Modeling of Security Arguments

Current State and Future Directions

Dan Ionita, Margaret Ford, Alexandr Vasenev, and Roel Wieringa

Problem context

- Socio-technical systems:
  - Large
  - Complex
  - Multi-layered
- Socio-technical risk assessment:
  - Often qualitative, informal
  - 100% security is un-achievable
  - Involves opportunity costs
  - Has to be frequently revisited
  - Is a collaborative process
  - Formal proofs are impossible

Why argumentation modelling?

- Traceability
- Defensibility
- Understandability
- Reusability

Methodology

1. Review **argumentation** theory
2. Review **security argumentation** frameworks
3. Review **graphical security argumentation** tools
4. Compare **graphical models of security arguments**
5. Draw conclusions w.r.t. **usability, utility, scalability** of the representations

Argumentation

- Legal, e.g. Toulmin
- Design rationale, e.g. QOC
- Decision support, e.g. CAE and GSN

Argumentation in security

- Arguing satisfaction of security requirements
- Supporting the elicitation of security requirements
- Argumentation-based risk assessment

Graphical security argumentation tools

- OpenArgue / OpenRISA
  - Graph-based, semi-formal
- Argumentation spreadsheets
  - Table-based, semi-formal
- ArgueSecure
  - Tree-based, informal

OpenArgue / OpenRISA

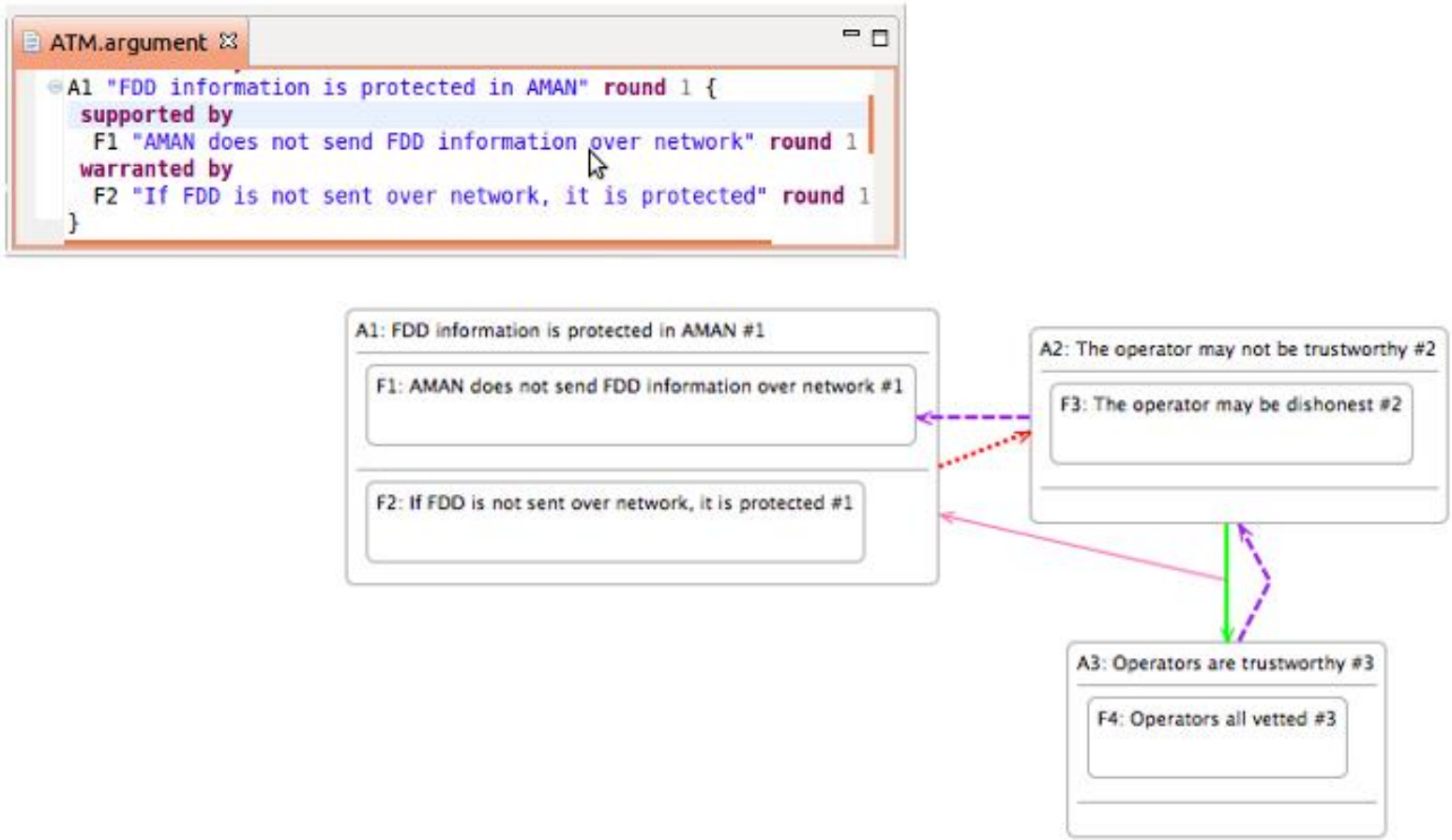
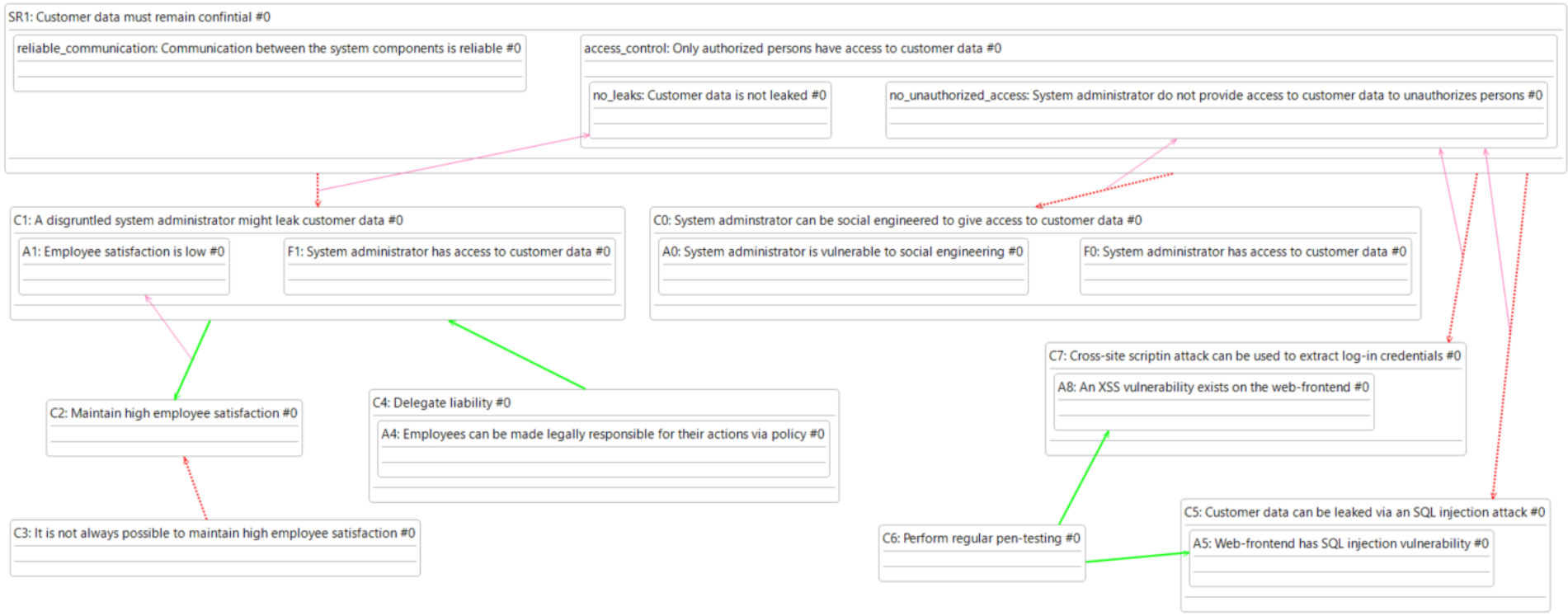


Figure from:
Yu, Yijun, et al. "OpenArgue: Supporting argumentation to evolve secure software systems." *Requirements Engineering Conference (RE), 2011 19th IEEE International*. IEEE, 2011.

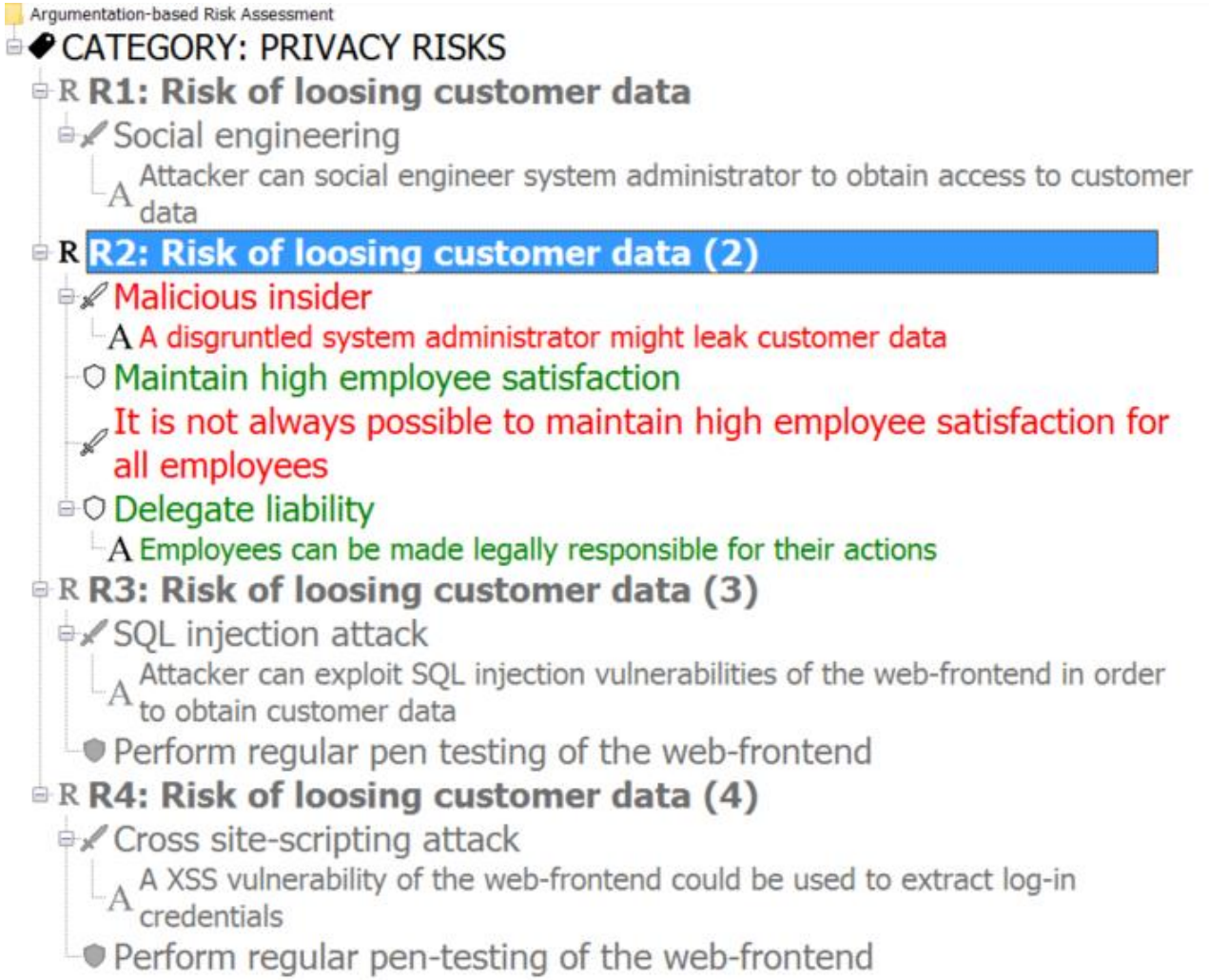
OpenArgue / OpenRISA



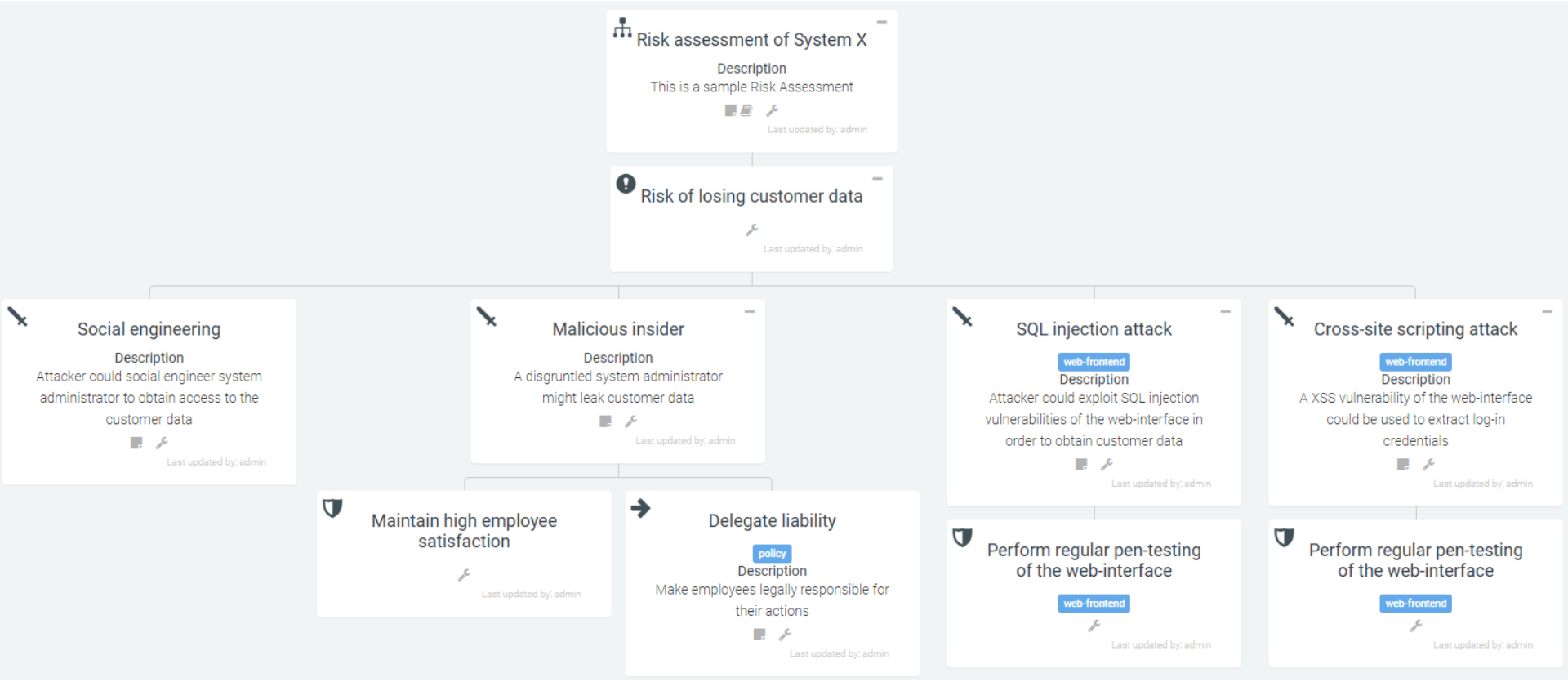
Argumentation spreadsheets

ARGUMENTS										TAGS	
Claim		Assumptions		Facts		Re-	Asset(s)	Status	Notes	Assets	
#	txt	#	txt	#	txt	buts	ID(s)	IN / OUT	Transf./ Red.	ID	NAME
C0	System adminstrator can be social engineered to give access to customer data	A0	System administrator is vulnerable to social engineering	F0	System administrator has access to customer data			IN		T!	policy
C1	A disgruntled system administratot might leak customer data	A1	Employee satisfaction is low	F1	System administrator has access to customer data			OUT		T2	web-frontend
C2	Maintain high employee satisfaction	A2	-	F2	-	A1		IN			
C3	It is not always possible to maintain high employee satisfaction	A3	-	F3	-	C2		OUT			
C4	Delegate liability	A4	Employees can be made legally responsible for their actions via policy	F4	-	C3	T!,	IN	Transf.		
C5	Customer data can be leaked via an SQL injection attack	A5	web-frontend has SQL injection vulnerability	F5	-		T2,	OUT			
C6	Perform regular pen-testing of the web-frontend	A6	-	F6	-	A5	T2,	IN	Red.		
C7	Cross-site scripting attack can be used to extract log-in credentials	A8	An XSS vulnerablity exists on the web-frontend	F8	-		T2,	OUT			
C8	Perform regular pen-testing of the web-frontend	A9	-	F9	-	A8	T2,	IN	Red.		

ArgueSecure-offline



ArgueSecure-online



Comparison

	Open Argue	Arg. Sheets	AS-offline	AS-online
Intra-argument granularity	3	3	2	2
Inter-argument granularity	4	2	1	1
Relate to security requirements	Y	N	N	N
Relate to assets	N	Y	N	Y
>1 attack vector per risk	Y	N	N	Y
>1 mitigatation per attack	Y	N	N	Y
Supports risk transfer	N	Y	Y	Y
Collaborative	N	N	N	Y
Planned vs. implemented	N	N	Y	N
Search and filters	N	N	N	Y
Export and reports	N	N	Y	Y

Observations

- **Graphs** are a suitable representation for security arguments
- Security arguments consist of at least: a **risk,** one or more **vulnerabilities**, and one or more **mitigations**
- Relationships other than **rebuttals** are a threat to scalability and usability.
- **Features to help navigate** the argumentation graph are critical to making it human-writable and human-readable

Conclusions

- Security arguments help mitigate uncertainty
  - Important for certification, compliance, awareness, assurance
- Graphical modelling of security arguments is still an academic pursuit
- To be usable in practice, graphical argumentation models need to be
  - conceptually simpler,
  - functionally more intuitive,
  - a lot more scalable;
  - at lest partially automated;
- Trees are a good start!