

Graphical Modeling of Security Arguments

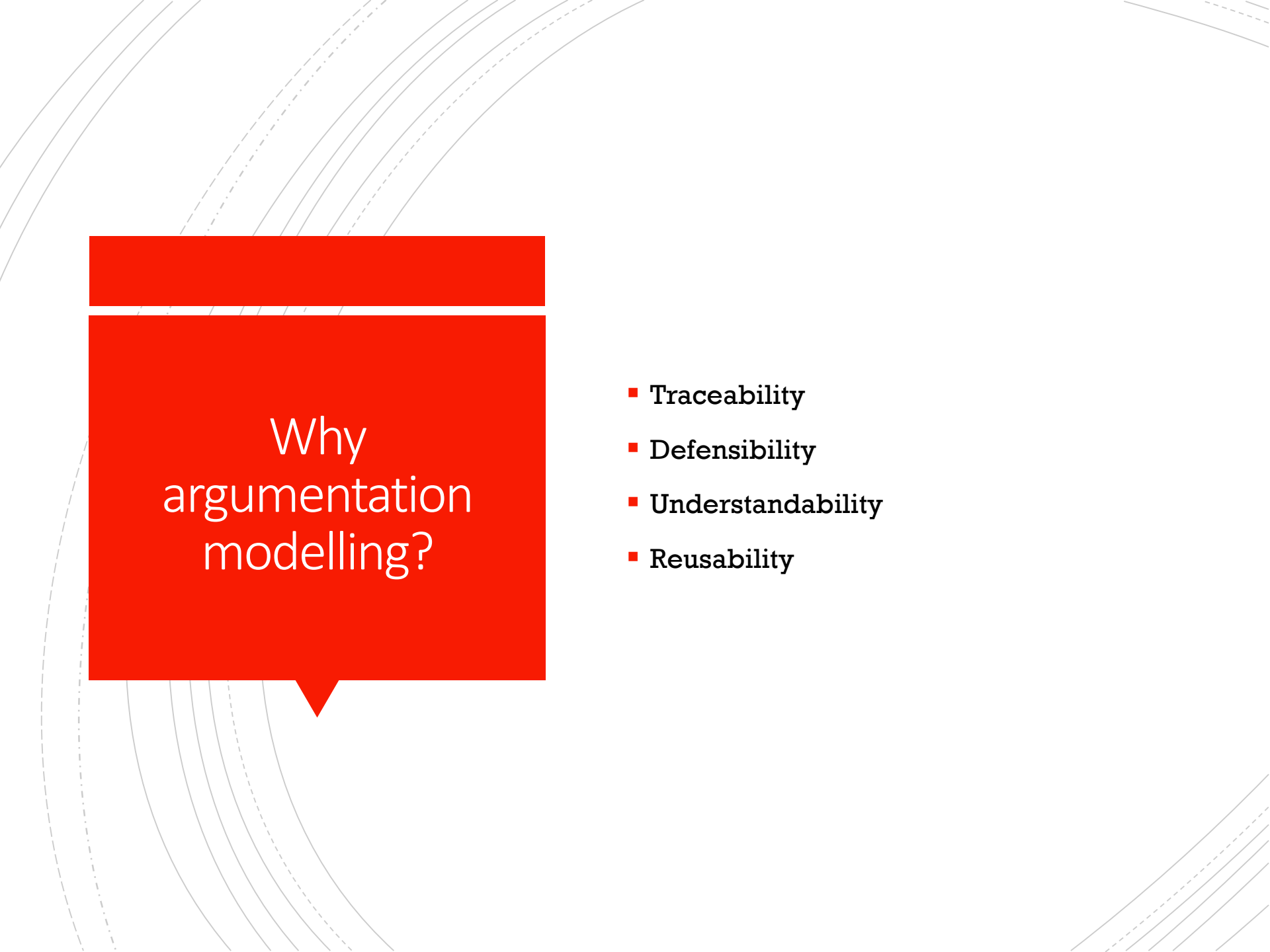
Current State and Future Directions

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

A large red speech bubble graphic with a white outline, containing the text 'Problem context'. The bubble has a tail pointing downwards and to the right. The background of the slide features several concentric, curved lines in shades of gray, some solid and some dashed, creating a sense of depth and movement.

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

The background features several sets of concentric, curved lines in light gray, some solid and some dashed, creating a sense of motion or flow. A large red speech bubble shape is positioned on the left side of the slide.

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

```
ATM.argument
├─ A1 "FDD information is protected in AMAN" round 1 {
│   └─ supported by
│       └─ F1 "AMAN does not send FDD information over network" round 1
│           └─ warranted by
│               └─ F2 "If FDD is not sent over network, it is protected" round 1
│                   }
│       }
└─ }
```

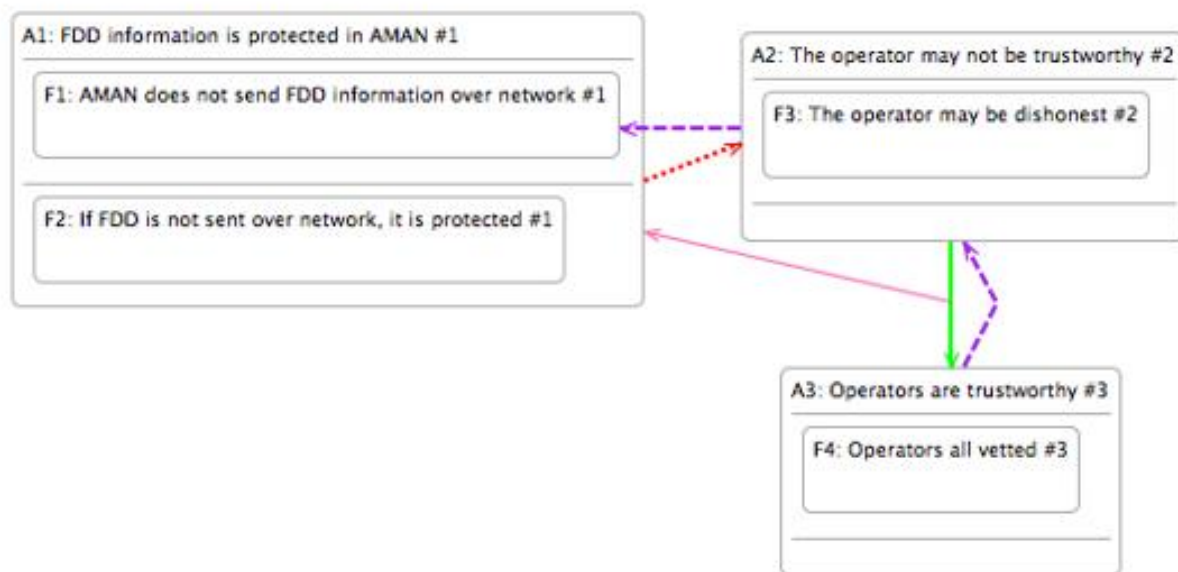


Figure from:

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

OpenArgue / OpenRISA

SR1: Customer data must remain confidential #0

reliable_communication: Communication between the system components is reliable #0

access_control: Only authorized persons have access to customer data #0

no_leaks: Customer data is not leaked #0

no_unauthorized_access: System administrator do not provide access to customer data to unauthorizes persons #0

C1: A disgruntled system administrator might leak customer data #0

A1: Employee satisfaction is low #0

F1: System administrator has access to customer data #0

C0: System administrator can be social engineered to give access to customer data #0

A0: System administrator is vulnerable to social engineering #0

F0: System administrator has access to customer data #0

C2: Maintain high employee satisfaction #0

C4: Delegate liability #0

A4: Employees can be made legally responsible for their actions via policy #0

C7: Cross-site scriptin attack can be used to extract log-in credentials #0

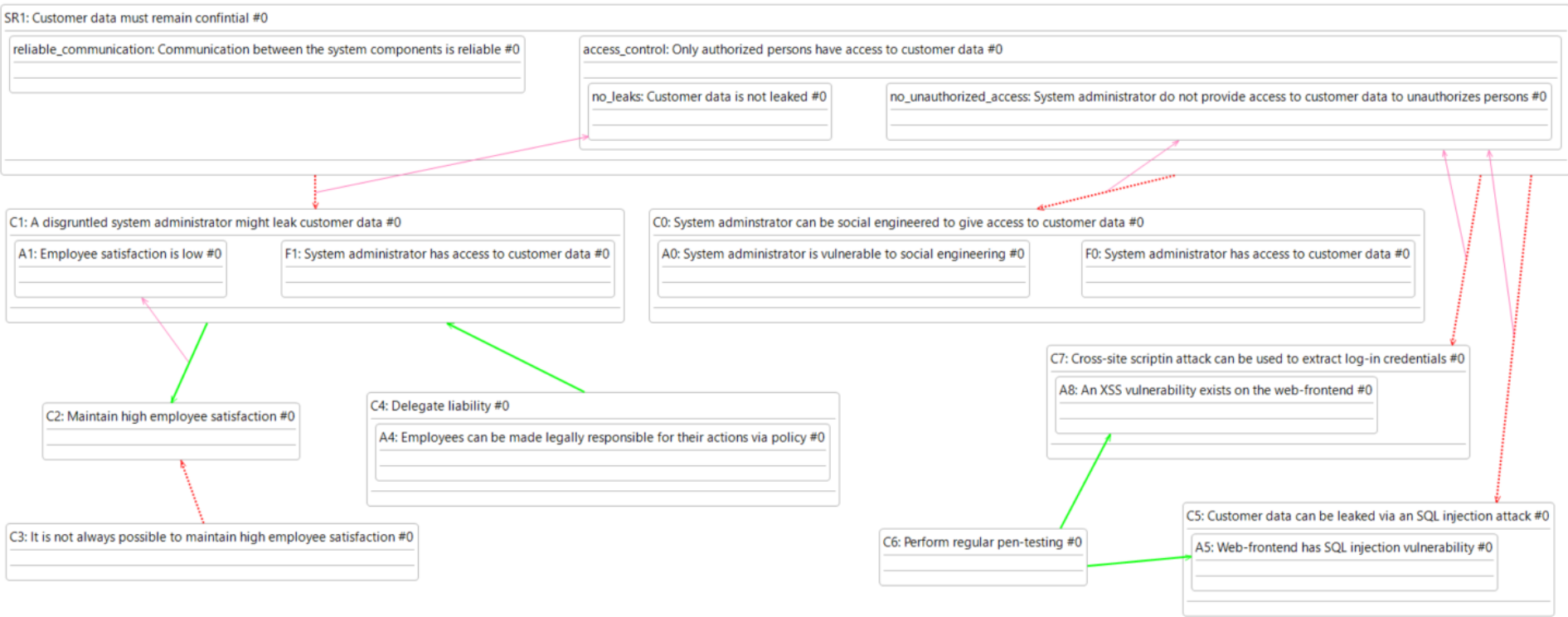
A8: An XSS vulnerability exists on the web-frontend #0

C3: It is not always possible to maintain high employee satisfaction #0

C6: Perform regular pen-testing #0

C5: Customer data can be leaked via an SQL injection attack #0

A5: Web-frontend has SQL injection vulnerability #0



Argumentation spreadsheets

ARGUMENTS								TAGS			
Claim		Assumptions		Facts		Re-buts	Asset(s)	Status	Notes	Assets	
#	txt	#	txt	#	txt		ID(s)	IN / OUT	Transf./ Red.	ID	NAME
C0	System administrator 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			T1 policy
C1	A disgruntled system administrator 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	T1,	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 vulnerability 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

Argumentation-based Risk Assessment

☛ CATEGORY: PRIVACY RISKS

☛ R R1: Risk of losing customer data

☛ Social engineering

☛ A Attacker can social engineer system administrator to obtain access to customer data

☛ R R2: Risk of losing customer data (2)

☛ Malicious insider

☛ A A disgruntled system administrator might leak customer data

○ Maintain high employee satisfaction

☛ It is not always possible to maintain high employee satisfaction for all employees

○ Delegate liability

☛ A Employees can be made legally responsible for their actions

☛ R R3: Risk of losing customer data (3)

☛ SQL injection attack

☛ A Attacker can exploit SQL injection vulnerabilities of the web-frontend in order to obtain customer data

● Perform regular pen testing of the web-frontend

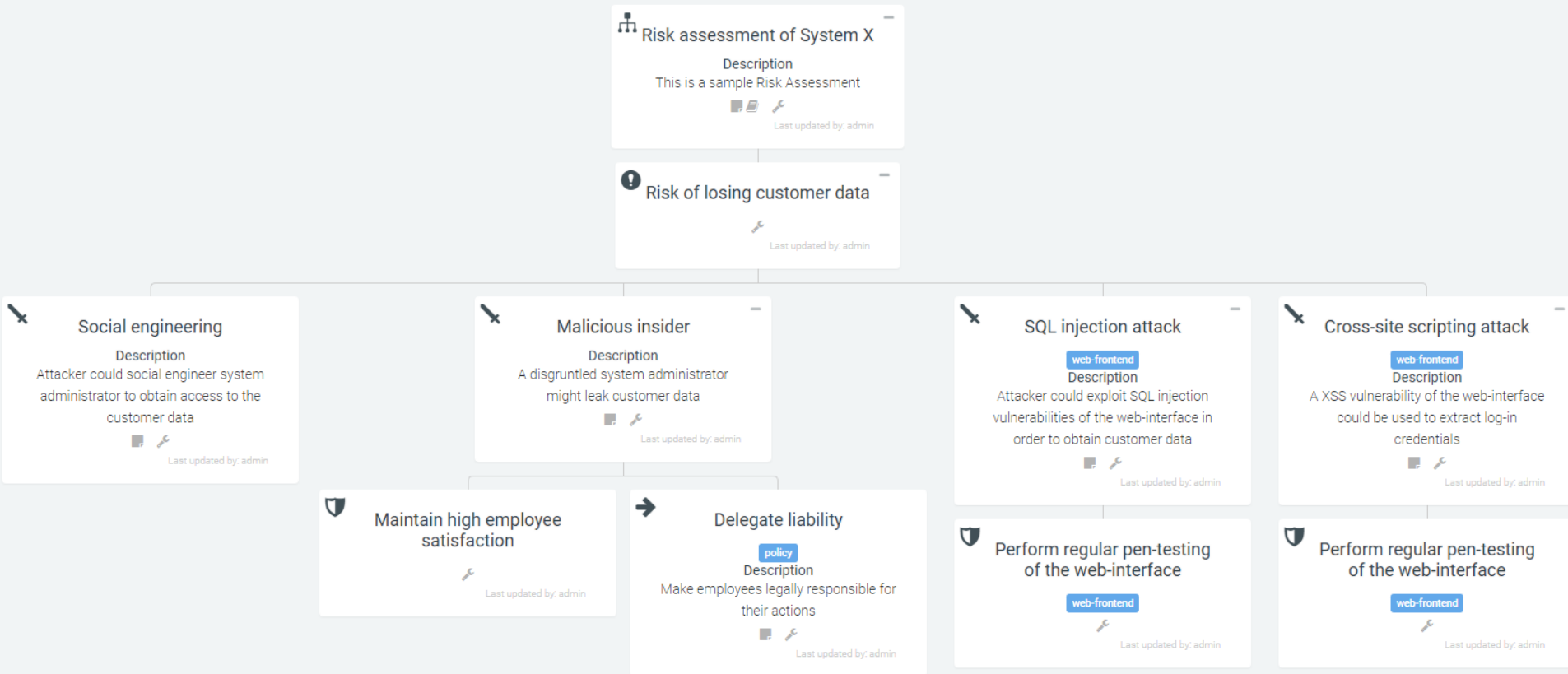
☛ R R4: Risk of losing customer data (4)

☛ Cross site-scripting attack

☛ A A XSS vulnerability of the web-frontend could be used to extract log-in credentials

● Perform regular pen-testing of the web-frontend

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 mitigation 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 least partially automated;
- **Trees are a good start!**