HoliSec

Holistic Approach to Improve Data Security

Evolving Threat analysis Techniques to Catch What Matters

Presenters: Katja Tuma, Mathias Widman

March 26, 2019

VINNOVA FFI VOLVO VOLVO ARC CORE CHALMERS ASSURED SECURITY CONSULTANTS RI. SE Research Institutes of Sweden

Why analyze threats?

Security threats are costly

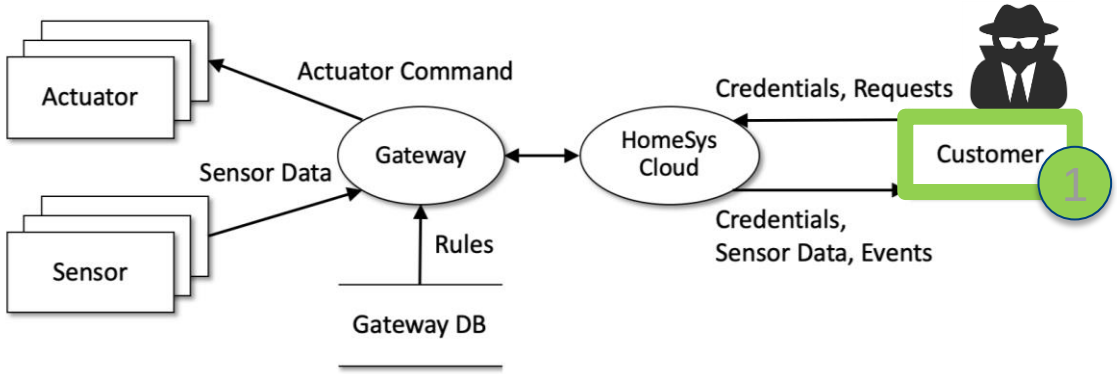
- bug fixing, code refactoring, re-deployment, loss of reputation,...

Avoid security design flaws at level of architecture

- by analyzing design, attacker's profile vis-a-vis assets

STRIDE-per-element

Model-based technique



Data Flow Diagram (DFD)

Table 3-9: STRIDE-per-Element

	S	T	R	I	D	E
2 External Entity	x		x			
Process	x	x	x	x	x	x
Data Flow		x		x	x	
Data Store		x	?	x	x	

Table 3-2: Spoofing Threats

THREAT EXAMPLES	WHAT THE ATTACKER DOES	NOTES
Spoofing a process on the same machine	Creates a file before the real process	
	Renaming/linking	Creating a Trojan "su" and altering the path
	Renaming	Naming your process "sshd"
Spoofing a file	Creates a file in the local directory	This can be a library, executable, or config file.
	Creates a link and changes it	From the attacker's perspective, the change should happen between the link being checked and the link being accessed.
	Creates many files in the expected directory	Automation makes it easy to create 10,000 files in /tmp, to fill the space of files called /tmp /"pid.NNNN, or similar.
Spoofing a machine	ARP spoofing	
	IP spoofing	
	DNS spoofing	Forward or reverse
	DNS Compromise	Compromise TLD, registrar or DNS operator
	IP redirection	At the switch or router level
Spoofing a person	Sets e-mail display name	
	Takes over a real account	
Spoofing a role	Declares themselves to be that role	Sometimes opening a special account with a relevant name

3

What's the problem?

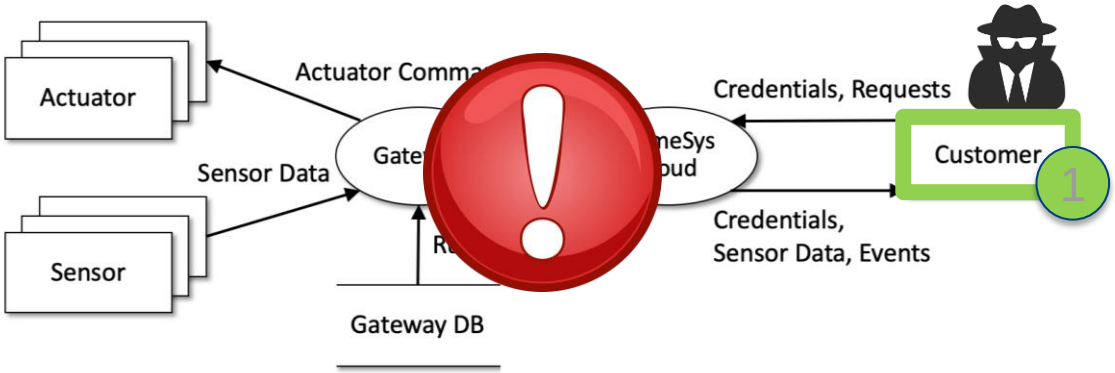


Table 3-9: STRIDE-per-Element

	S	T	R	I	D	E
2 External Entity	x		x			
Process	x	x	x	x	x	x
Data Flow		x		x	x	
Data Store		x	?	x	x	

Manual effort is high

Recall $\left(\frac{correctly\ identified\ threats}{existing\ threats}\right)$ is low

Table 3-2: Spoofing Threats

THREAT EXAMPLES	WHAT THE ATTACKER DOES	NOTES
Spoofing a process on the same machine	Creates a file before the real process	
	Renaming/linking	Creating a Trojan "su" and altering the path
	Renaming	Naming your process "sshd"
Spoofing a file	Creates a file in the local directory	This can be a library, executable, or config file.
	Creates a link and changes it	From the attacker's perspective, the change should happen between the link being checked and the link being accessed.
	Creates many files in the expected directory	Automation makes it easy to create 10,000 files in /tmp, to fill the space of files called /tmp /"pid.NNNN, or similar.
Spoofing a machine	ARP spoofing	
	IP spoofing	
	DNS spoofing	Forward or reverse
	DNS Compromise	Compromise TLD, registrar or DNS operator
	IP redirection	At the switch or router level
Spoofing a person	Sets e-mail display name	
	Takes over a real account	
Spoofing a role	Declares themselves to be that role	Sometimes opening a special account with a relevant name

3

Agenda

High effort

Low recall

SLR @ JSS 2018

STRIDE vs. STRIDE (ECSA 2018)

eSTRIDE & eDFD (CyberICPS 2017)

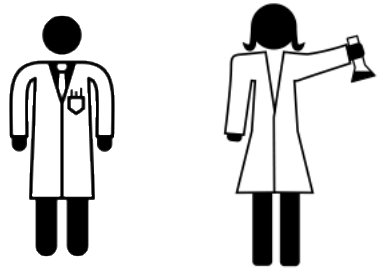
Bang for the Buck (ESEM 2019?)

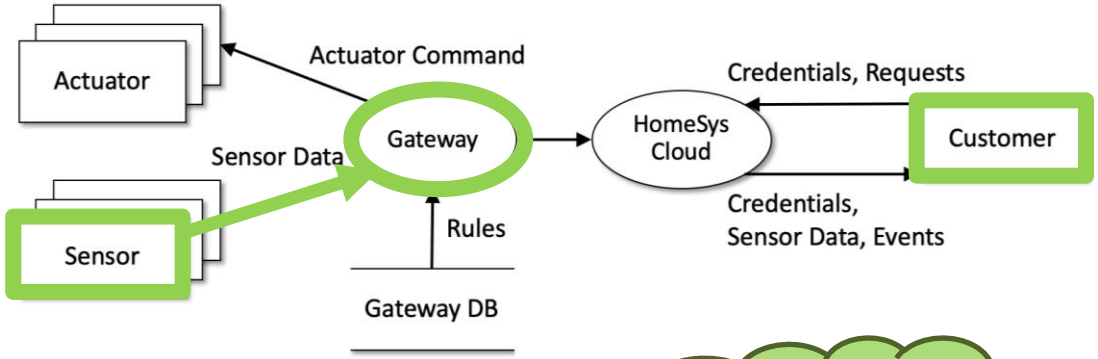
SecDFD & Analysis (ICSA 2019)

Completed

On-going

STRIDE vs STRIDE



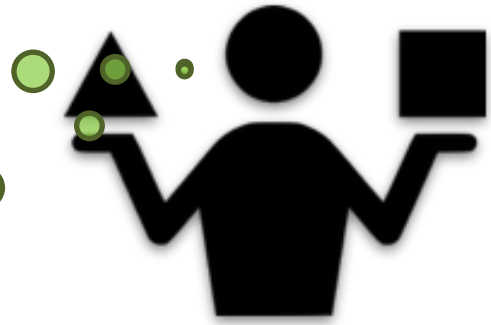


Analysis scope = **1 element**, e.g., STRIDE per element

Analysis scope = **3 elements**, e.g., STRIDE per interaction

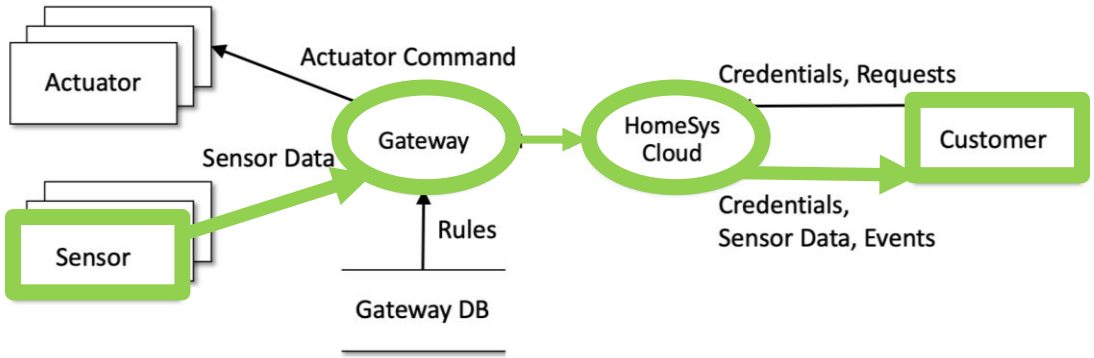
Different performance? No.

What about end-to-end?



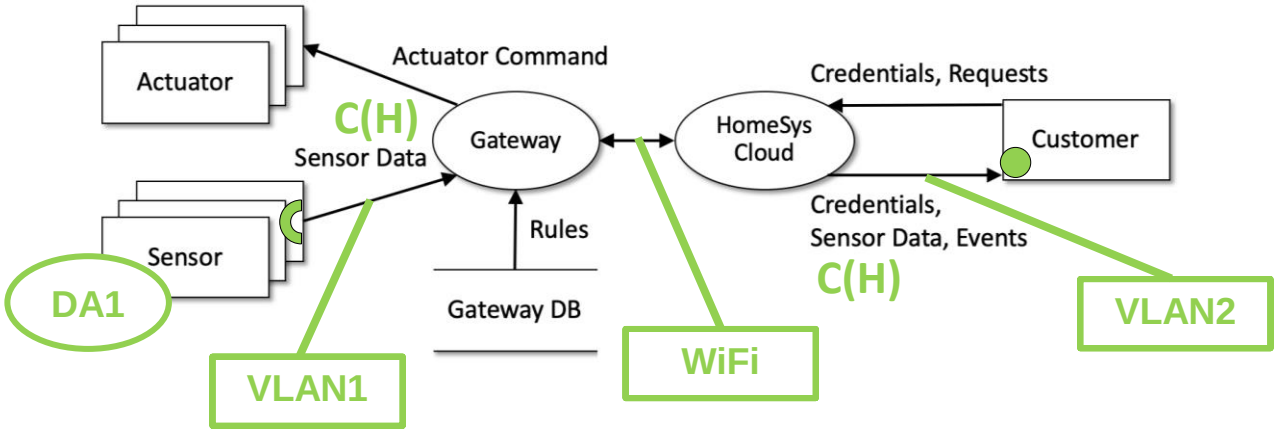
Extended DFD (eDFD)

- Enlarge the analysis scope **and** frontload with security information
  - e.g., follow `Sensor data' end-to-end



The `e' in eDFD

- Assets, assumptions, channels



DA1 = The sensor is working securely and the Sensor Data it outputs is trusted.

End-to-end STRIDE (eSTRIDE)

- Reduction in the procedure

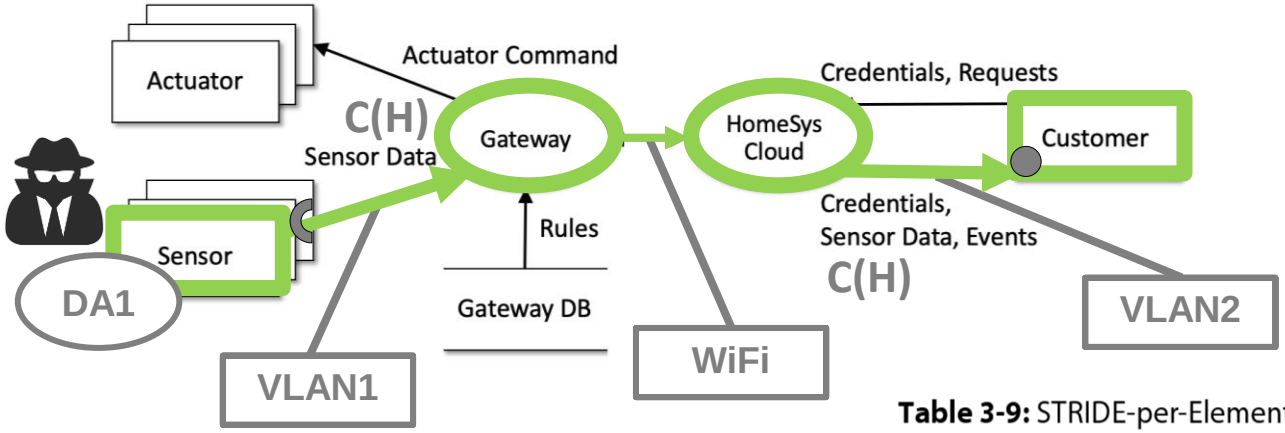
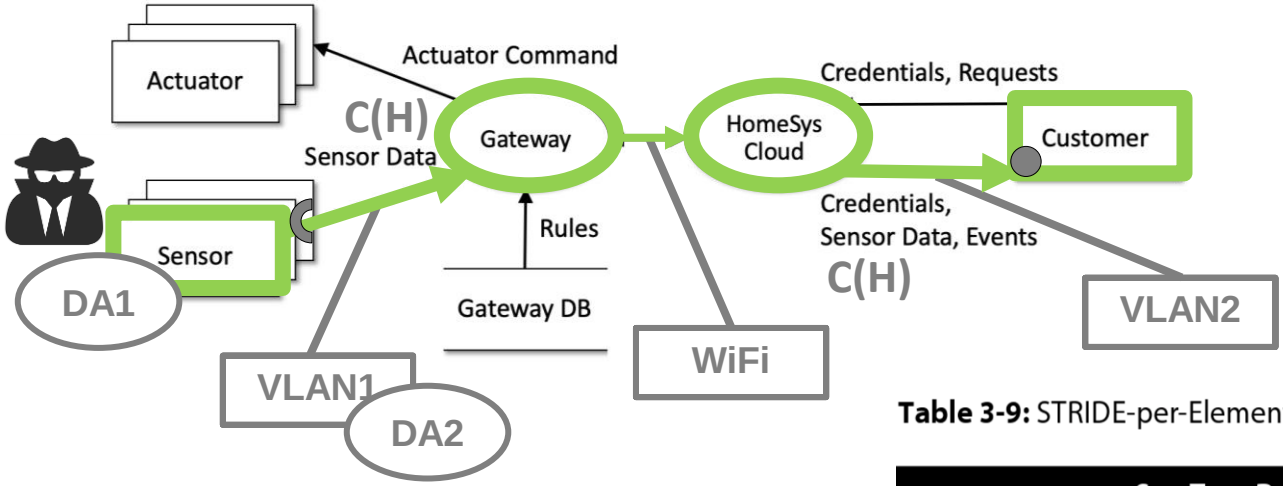


Table 3-9: STRIDE-per-Element

	S	T	R	I	D	E
External Entity	X		X			
Process	x	x	x	x	x	x
Data Flow		x		x	x	
Data Store		x	?	x	x	

End-to-end STRIDE (eSTRIDE)

- Reduction in the procedure



DA2 = The VLAN1 network has sufficient security mechanisms in place to mitigate I threats.

Table 3-9: STRIDE-per-Element

	S	T	R	I	D	E
External Entity	x		x			
Process	x	x	x	x	x	x
Data Flow		✗		✗	✗	
Data Store		x	?	x	x	

End-to-end STRIDE (eSTRIDE)

- Reduction in the procedure

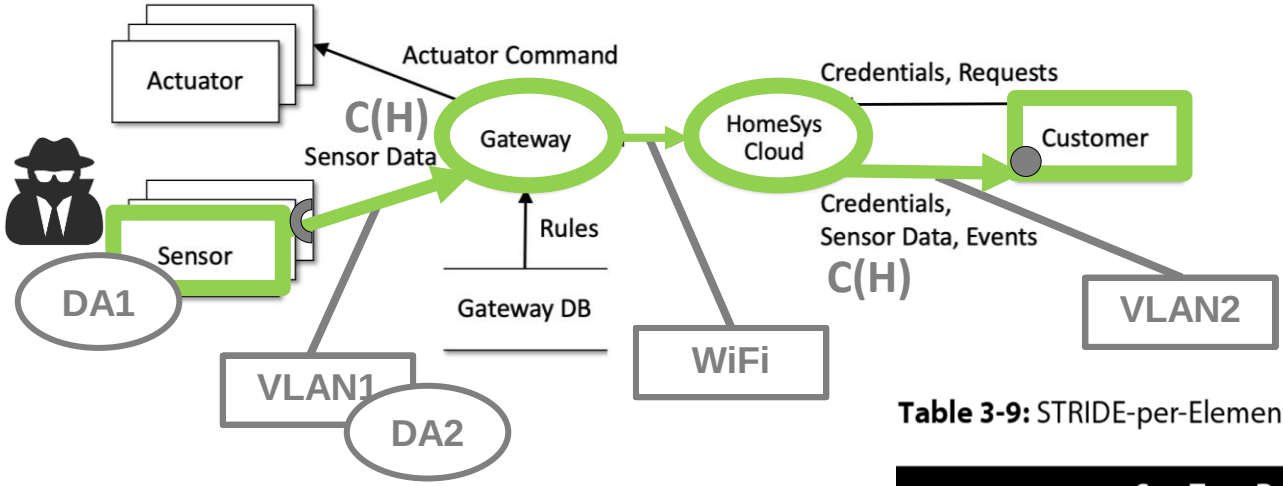


Table 3-9: STRIDE-per-Element

	S	T	R	I	D	E
External Entity	x		x			
Process	X	X	X	x	X	X
Data Flow		x		x	x	
Data Store		x	?	x	x	

What's next?

High effort

Low recall

SLR @ JSS 2018

STRIDE vs. STRIDE (ECSA 2018)

eSTRIDE & eDFD (CyberICPS 2017)

Bang for the Buck (ESEM 2019?)

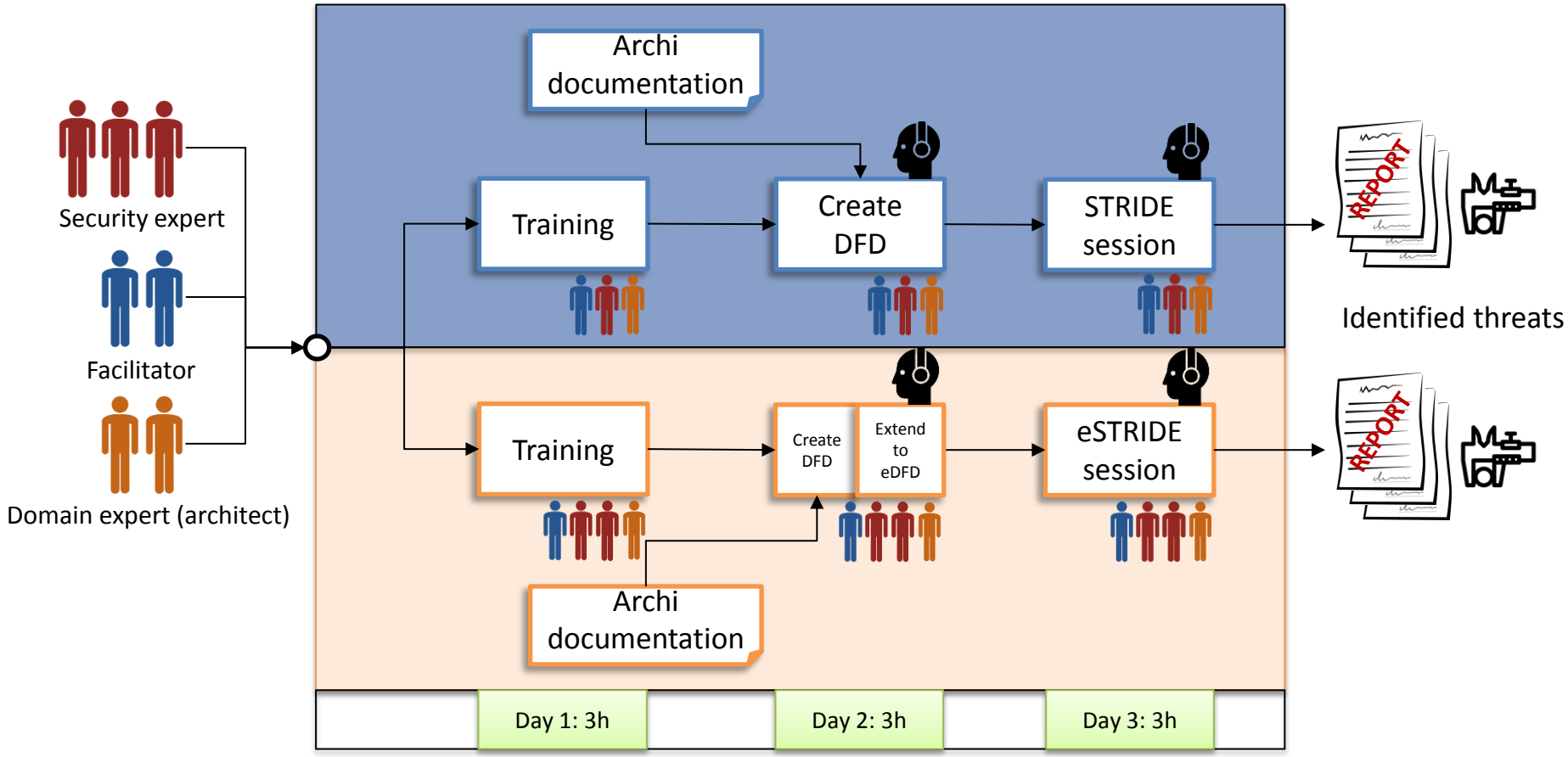
SecDFD & Analysis (ICSA 2019)

eSTRIDE vs. STRIDE

Completed

On-going

Comparative case study



Research questions

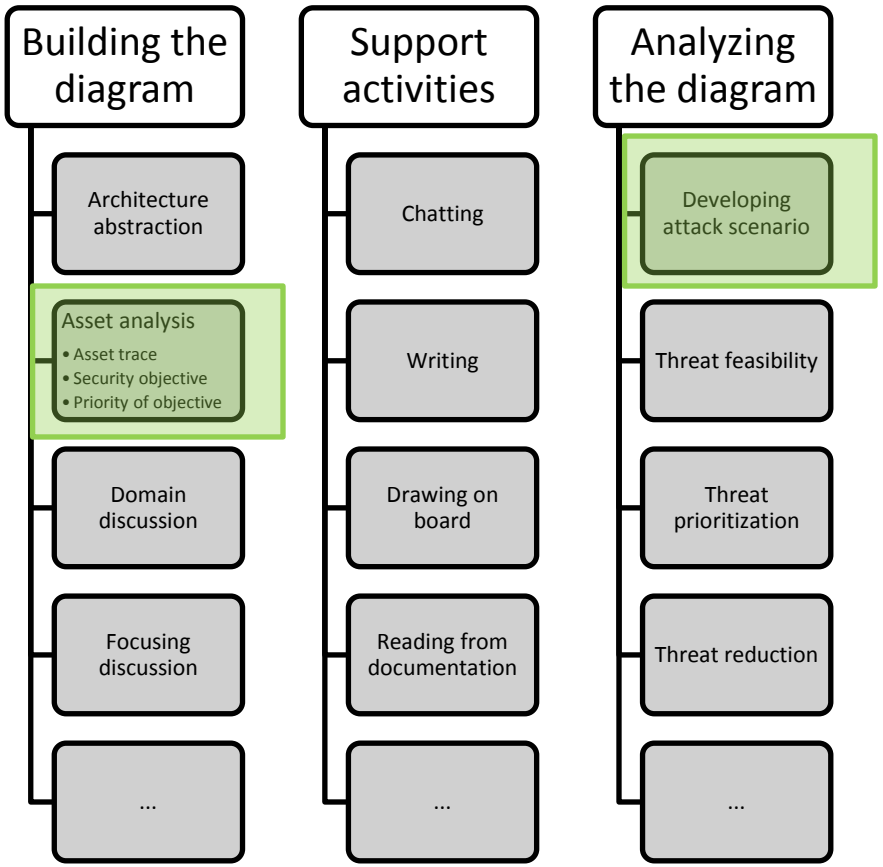
- What are the performance differences?
  - precision, false discovery rate, priority of TP, productivity

- What are the procedure execution differences?
  - activity patterns,
  - when are TP found,
  - When are high TP found.

> F: So, we are going to start with the EEs.
> S1: We should draw the people as EE.
> F: Yeah, like we did yesterday. I haven't worked with this type of systems before, but that's good. Let's start with the Driver and Fleet Technician - or do we want them as two separates?
> S2: That was my question too.
> S1: I think it's separate because they have different actions and credentials.

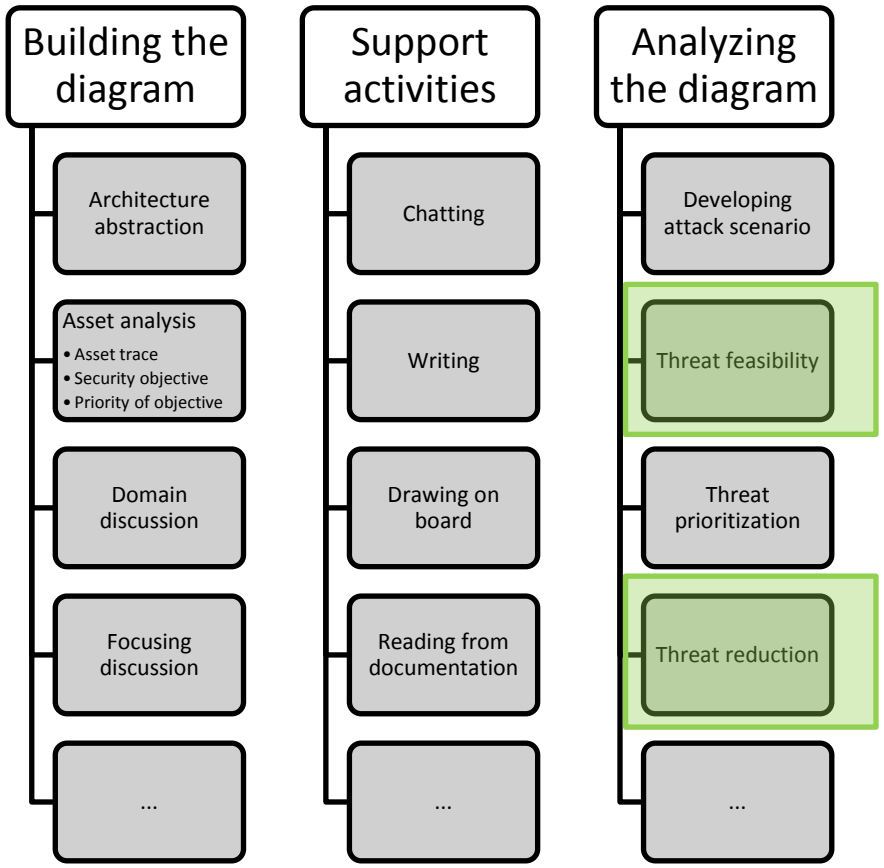
Architecture abstraction

Quantitative analysis



Is early asset analysis quickly followed by attack scenario development?

Quantitative analysis



Is threat feasibility followed by threat reduction?

Performance differences

- Similar amount of **true positives** ($11_{eSTRIDE}$ vs 12_{STRIDE})
- Similar **productivity** (3_{STRIDE} vs $2.2_{eSTRIDE}$ threats/h)

- eSTRIDE found **more high priority threats** ($9_{eSTRIDE}$ vs 6_{STRIDE})

Qualitative analysis

Making domain assumptions early-on spurs attack scenario development.

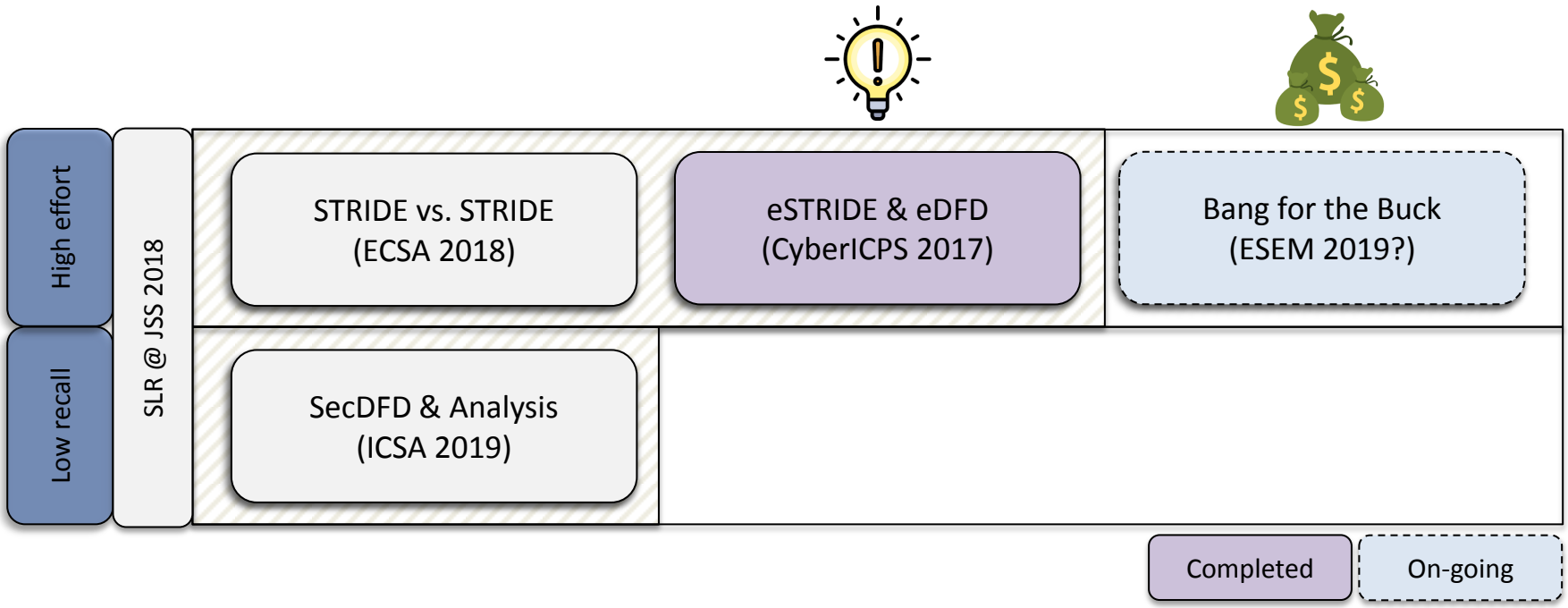
Making an assumption

S1: ... We can say OK, the link is encrypted here, so the password is protected in that way. But it's still a high priority that it should be confidential, right?
F: Yeah. We will probably **make an assumption here** that it's encrypted and then we don't need to...**so that is solved**.

S1: Yeah. Or **we can think of an attack scenario** to break the encryption then. We are using TLS 1.1.
F: Exactly, maybe that's true. It's not the state of the art.
S1: Now I don't know if it's even possible to do this now, but **maybe you could find a scenario to downgrade**....

Developing attack scenario

Cooperation with industry



Threats and risk at Volvo

- Volvo is using TARA for in-vehicle and back office threat analysis and risk assessment
- Feels inefficient with high effort and low recall
- Connecting vehicles to back office -> threat explosion!
  - Domain expands
  - Long chains with attack surfaces
- How to spend time on what is relevant (risks)?

Volvo TARA efficiency improvements

- Theory: frontloading with the right knowledge could eliminate spending analysis time on less relevant areas
- We developed the idea further together in workshops
  - Detailing what would be optimal initial knowledge
  - Ways of modelling the frontloading, i.e. eDFD
  - Rules of “game of elimination”
- A new approach was proposed, eDFD/eSTRIDE

Case study and future

- A case study was eventually formed where we wanted to verify parts of our approach
- Case study was really small and we need more confidence in our hypothesis
  - Tryouts in our daily work
- Future: Improve our TARA process with the results from our work

Agenda

High effort

Low recall

SLR @ JSS 2018

STRIDE vs. STRIDE
(ECSA 2018)

eSTRIDE & eDFD
(CyberICPS 2017)

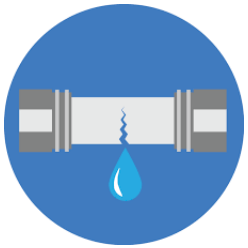
Bang for the Buck
(ESEM 2019?)

SecDFD & Analysis
(ICSA 2019)

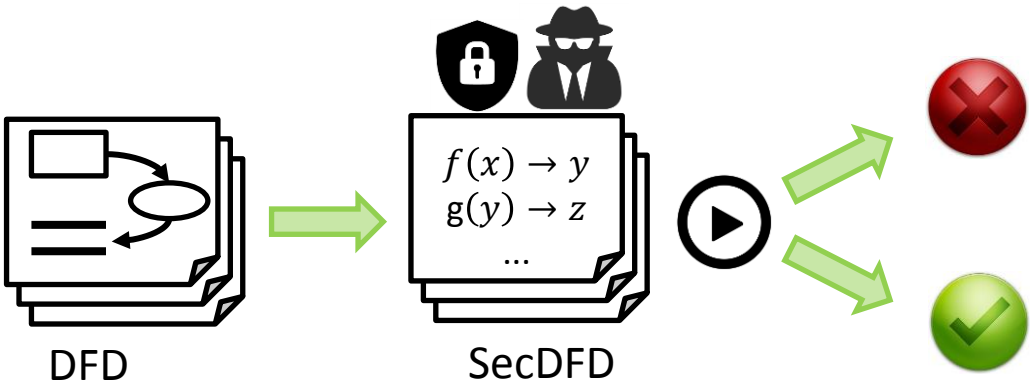
Completed

On-going

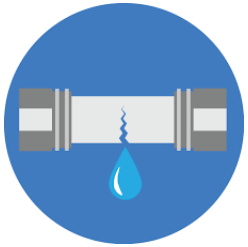
Flaws in Flows: SecDFD Analysis

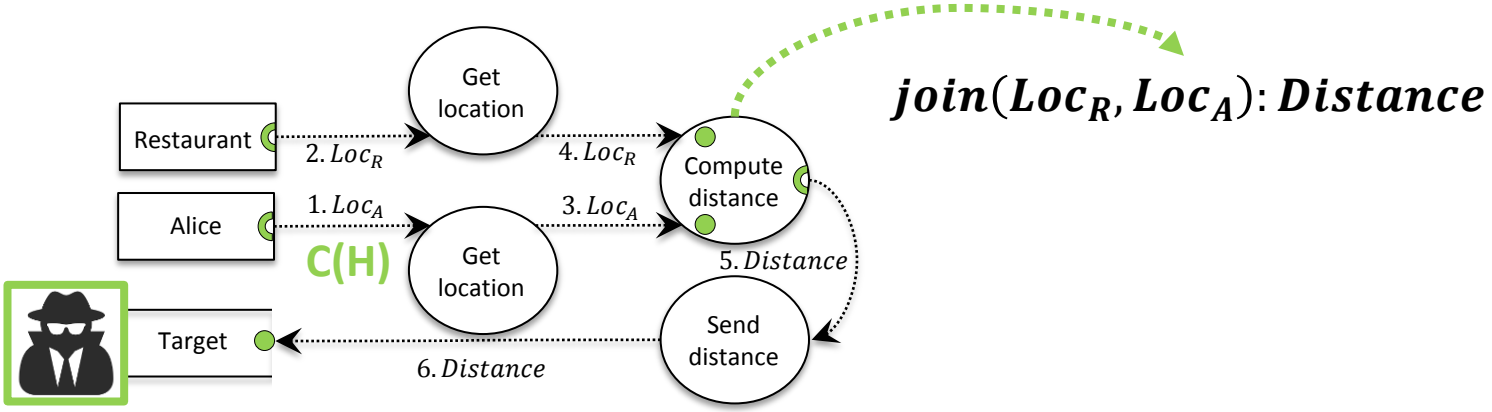


How to raise the recall, how to guarantee completeness of threat analysis on DFD-like models?



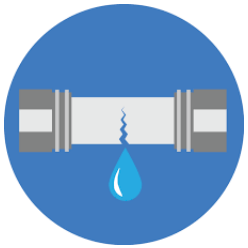
Building the SecDFD

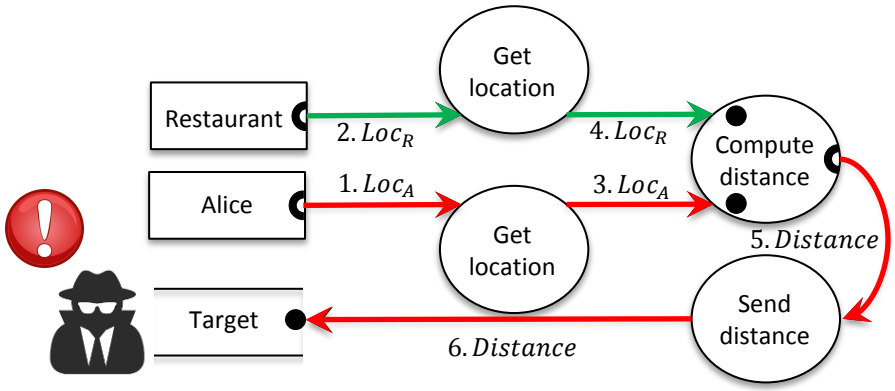




1. Security objectives and their priorities
2. Asset traces
3. Node types liked to operations over assets
4. Attacker model

Propagating labels

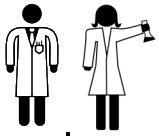




1. $fwd(Loc_A)$: Loc_A
2. $fwd(Loc_R)$: Loc_R
3. $join(Loc_R, Loc_A)$: $Distance$
4. $fwd(Distance)$: $Distance$

Wrap up

- Problems of high effort & low recall



- Empirical study of analysis scope

- Novel approach eDFD & eSTRIDE

- Empirical case study evaluating eDFD & eSTRIDE

- Cooperation with industry

- Novel approach SecDFD Analysis

Future directions

- Benefits of eSTRIDE longer sessions
- SecDFD analysis compare code-level analysis
- Automating with tool support

HoliSec

Holistic Approach to Improve Data Security

Thank you for your attention!