ATTRIBUTE REPAIR FOR THREAT PREVENTION

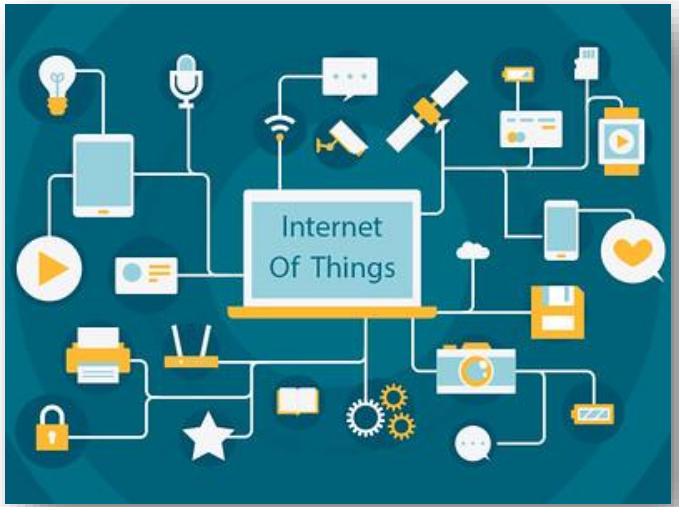
SAFECOMP 2023

Dejan Ničković

AIT Austrian Institute of Technology

Joint work with Thorsten Tarrach, Masoud Ebrahimi, Sandra König, Christoph Schmittner and Roderick Bloem

MOTIVATION



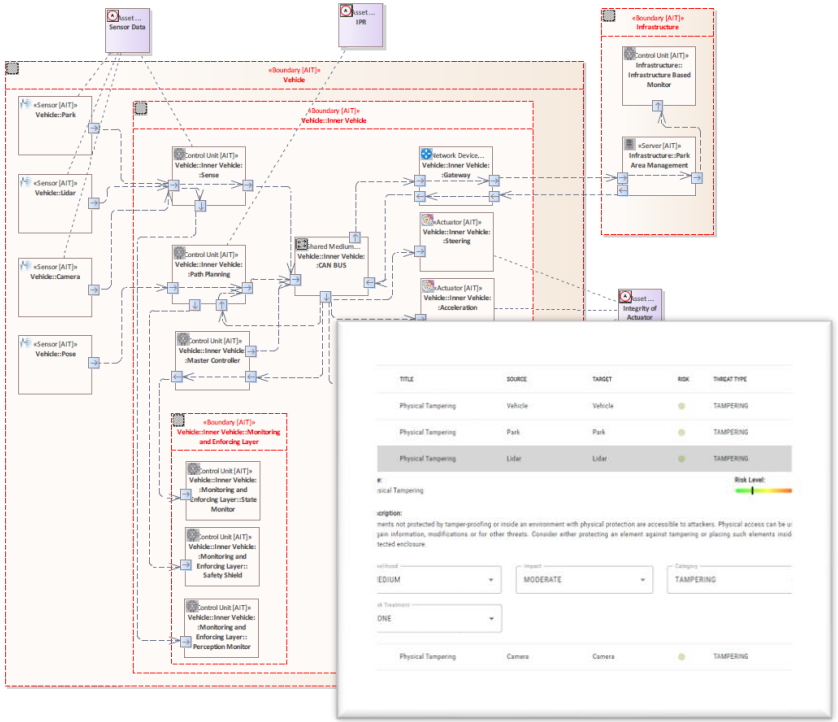
Larger attack surfaces

New security standards
ISO/SAE 21434

→ Security as first-class citizen from early stages of design

THREATGET

- THREATGET - tool for threat management and analysis
- Reusable analysis results
- Traceable mitigations and design decisions
- Up-to-date threat catalogue

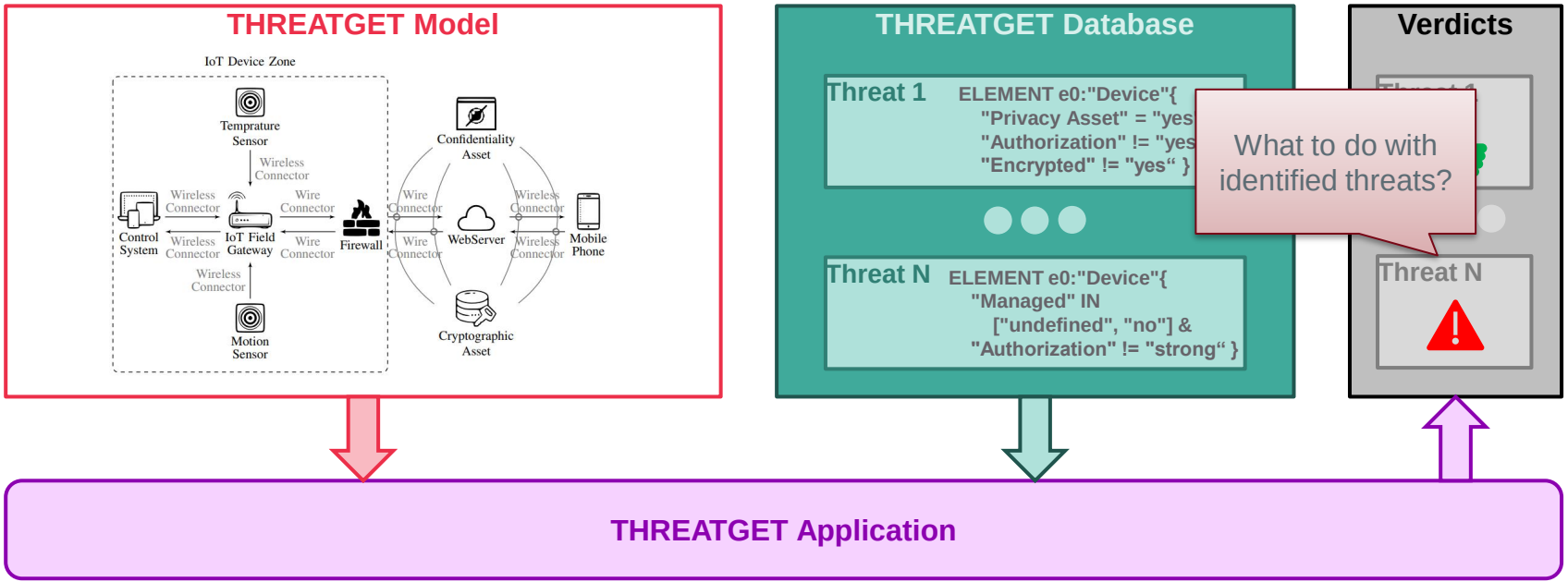


https://www.threatget.com/

Commercial tool, free academic license

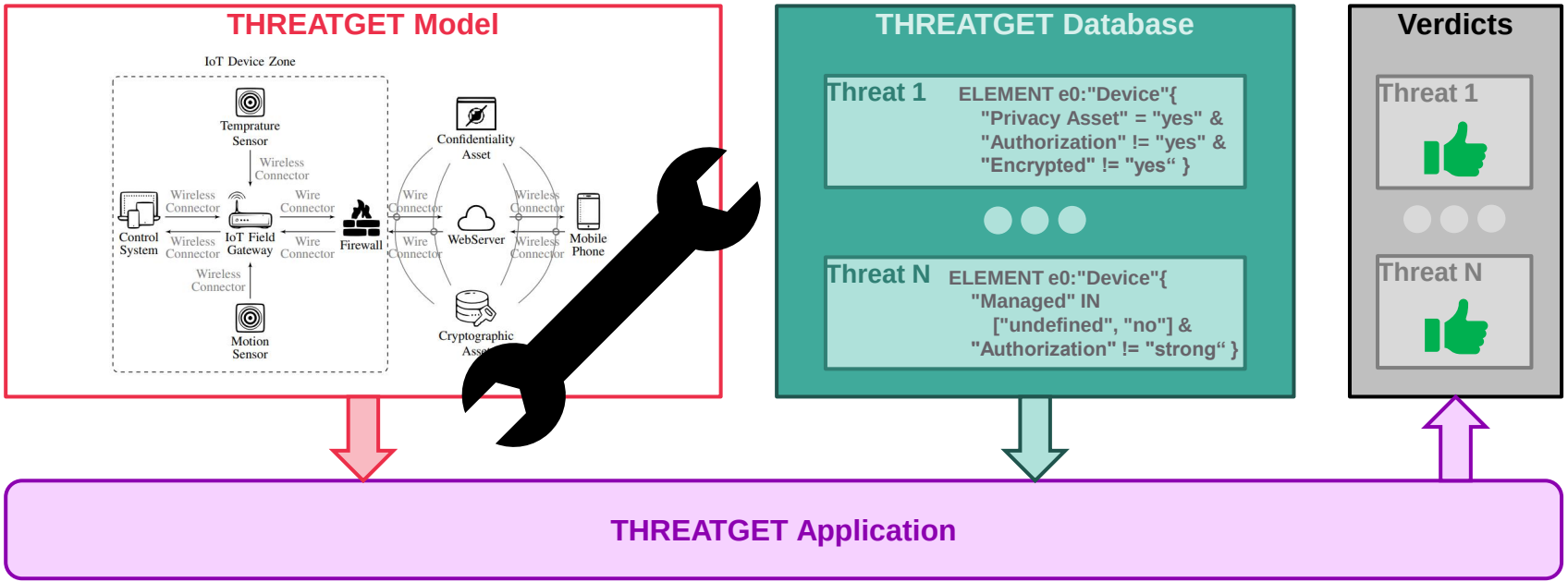
THREAT MODELING WITH THREATGET

https://www.threatget.com/



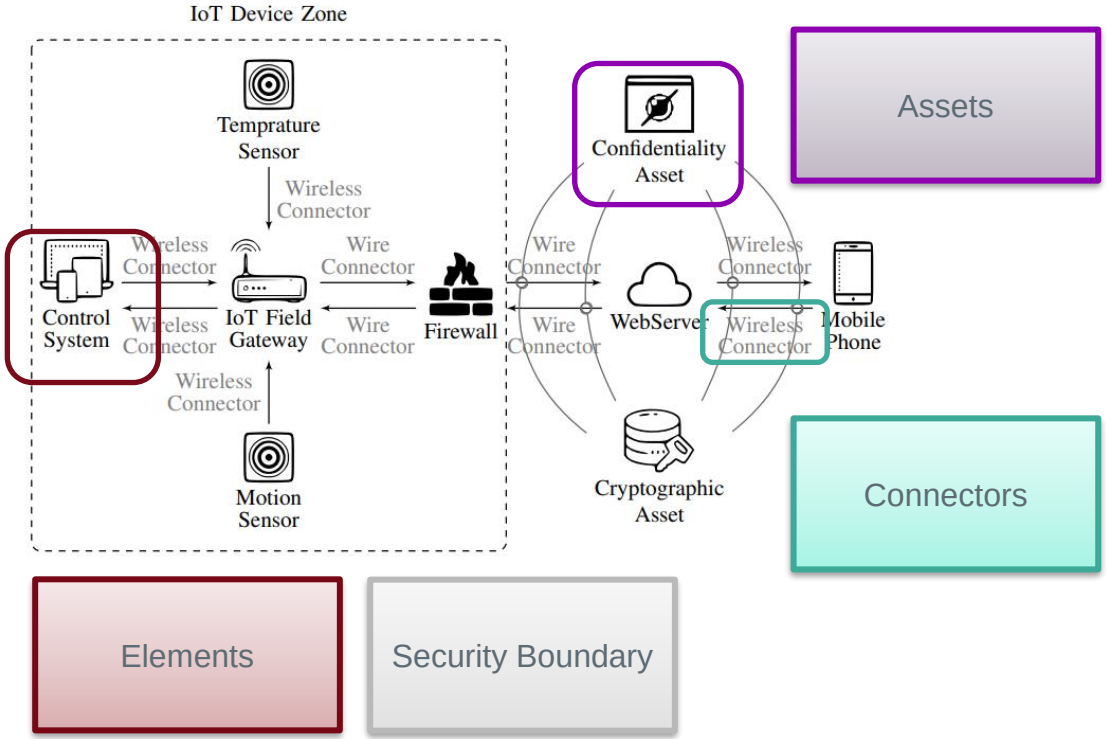
MODEL REPAIR

https://www.threatget.com/



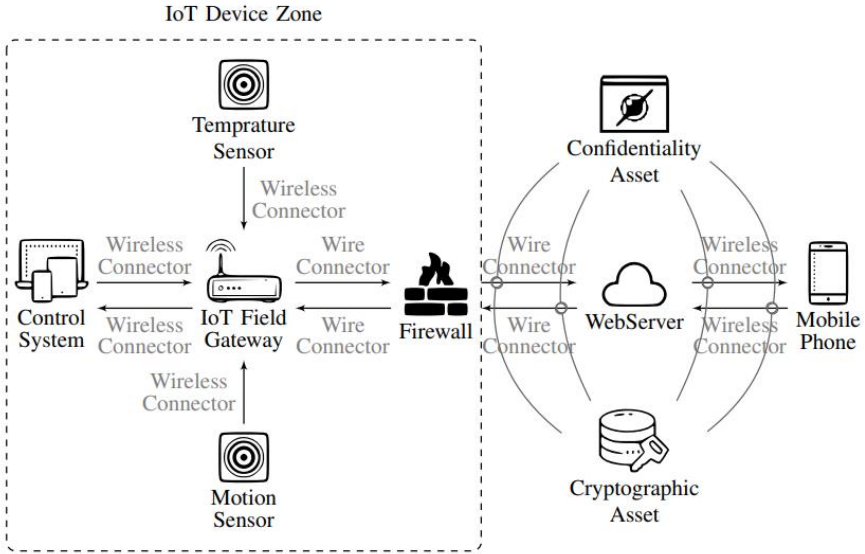
MODEL REPAIR

SYSTEM MODEL



Attribute	Value	Weight
Authentication	No	100
Encryption	Yes	10
…	…	

ATTRIBUTE REPAIR

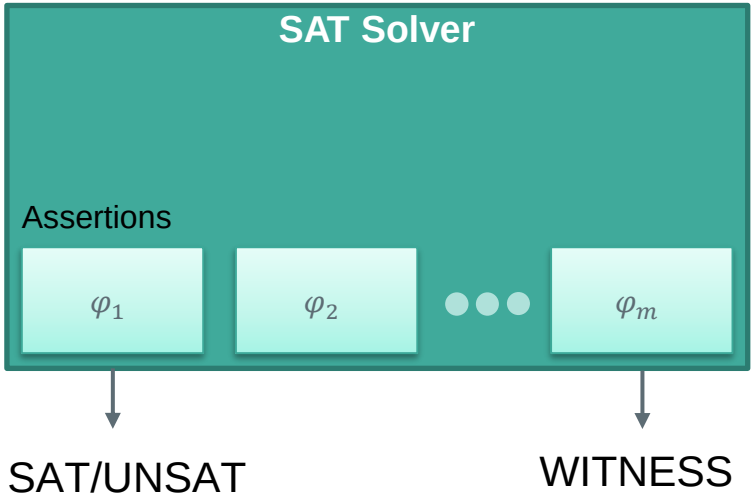


Attribute	Value	Weight
Authentication	No	100
Encryption	Yes	10
…	…	

- We repair **security attributes** of elements and connectors
- We are not allowed to changed the structure of the model

SAT

- Problem of determining if there exists an interpretation that satisfies a given Boolean formula

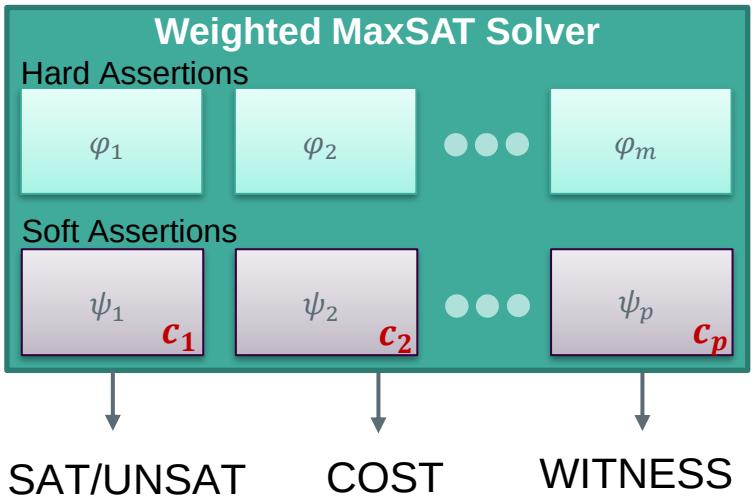


Example

$$\varphi_1 = p \wedge (q \vee r)$$
$$\varphi_2 = p \wedge (q \wedge r) \wedge (q \wedge \neg r)$$
$$solve(\varphi_1) = SAT$$
$$solve(\varphi_2) = UNSAT$$
$$witness(\varphi_1) = (p \rightarrow 1, q \rightarrow 1, r \rightarrow 0)$$

WEIGHTED MAXSAT

- Problem of determining the subset of clauses of a Boolean formula that can be made true by an interpretation and that minimizes the cost.



Weighted MaxSAT

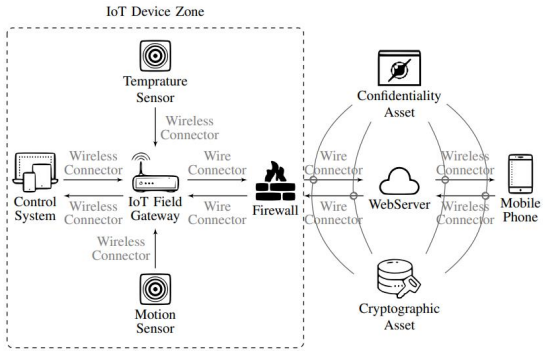
Given a set of formulas $\{\varphi_1, \dots, \varphi_m\}$ and $\{\psi_1, \dots, \psi_p\}$ and a set of real-valued costs $\{c_1, \dots, c_p\}$, weighted MaxSAT consists in finding $K \subseteq \{1, \dots, p\}$ such that:
(1) $\wedge_{i \in \{1,\dots,m\}} \varphi_i \ \wedge \ \wedge_{i \in K} \psi_i$ is SAT
(2) $\Sigma_{i \in \{1,\dots,p\}-K} \ c_i$ is minimized

$$\varphi_1 = (p \wedge q) \vee \neg r$$
$$\psi_1 = r, c_1 = 5$$
$$\psi_2 = p \wedge \neg q, c_2 = 2$$
$$solve(\varphi_1 \wedge \psi_1 \wedge \psi_2) = UNSAT$$
$$\text{max}sat\_solve(\varphi_1 \wedge \psi_1 \wedge \psi_2) = SAT$$
$$K = \{1\}$$
$$cost(\varphi_1 \wedge \psi_1 \wedge \psi_2) = 2$$
$$witness(\varphi_1 \wedge \psi_1 \wedge \psi_2) = (p \rightarrow 1, q \rightarrow 1, r \rightarrow 1)$$

ATTRIBUTE REPAIR AS WEIGHTED MAXSAT

System Model

Model Structure



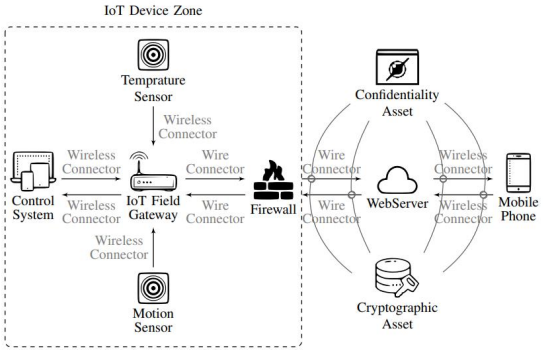
ATTRIBUTE REPAIR AS WEIGHTED MAXSAT

System Model

Model Structure

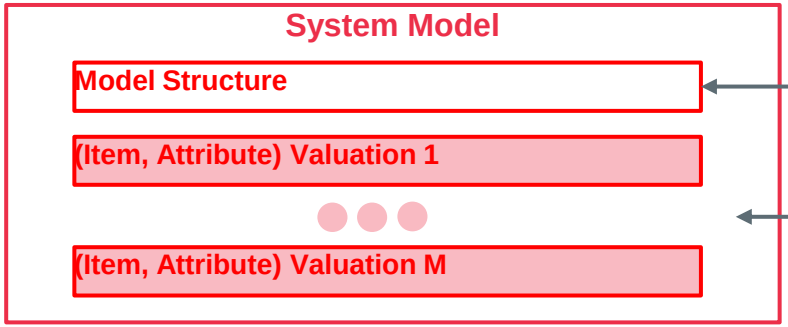
(Item, Attribute) Valuation 1

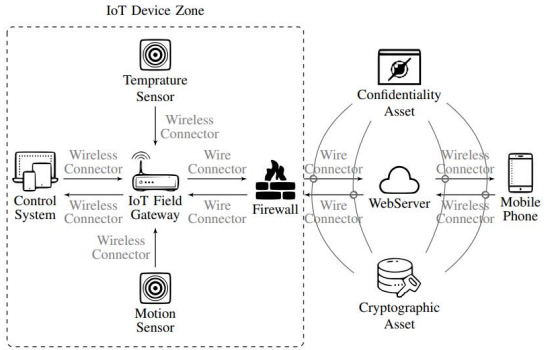
(Item, Attribute) Valuation M



Attribute	Value	Weight
Authentication	No	100
Encryption	Yes	10
…	…	

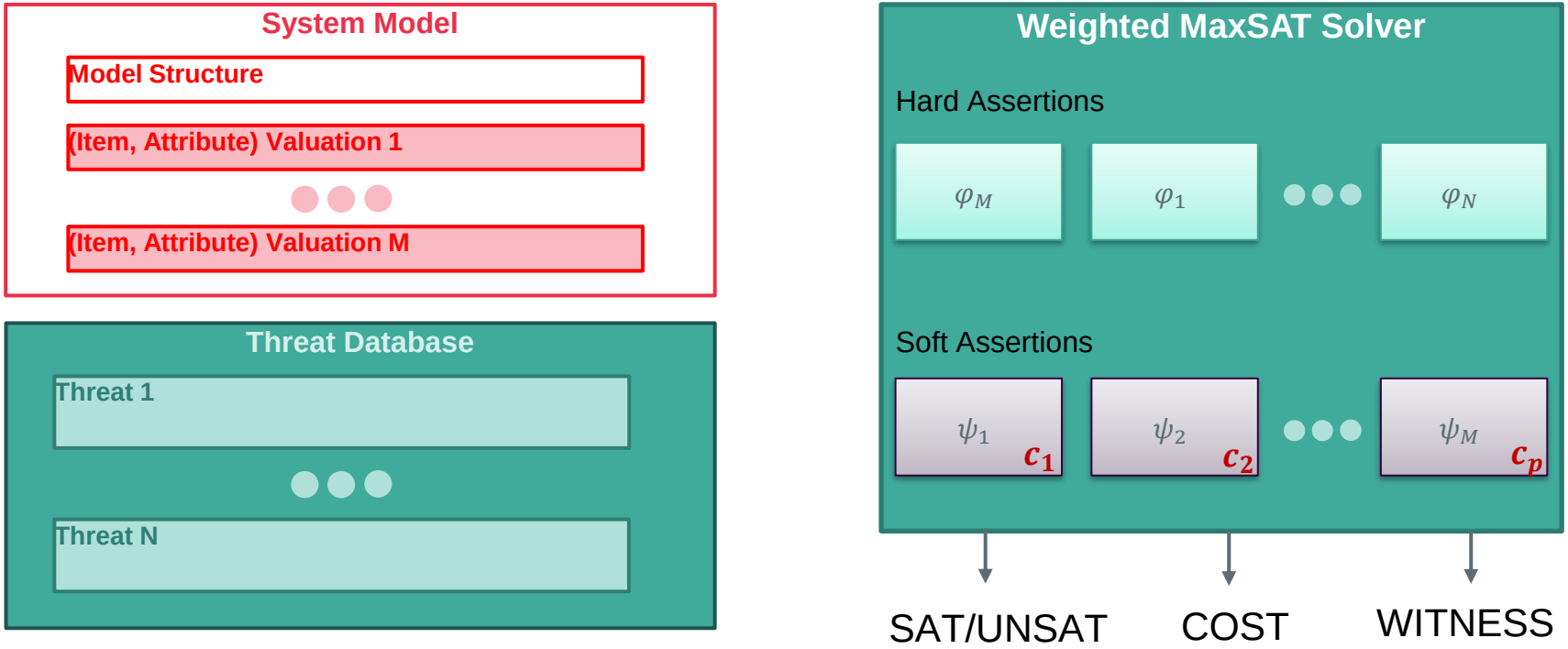
ATTRIBUTE REPAIR AS WEIGHTED MAXSAT



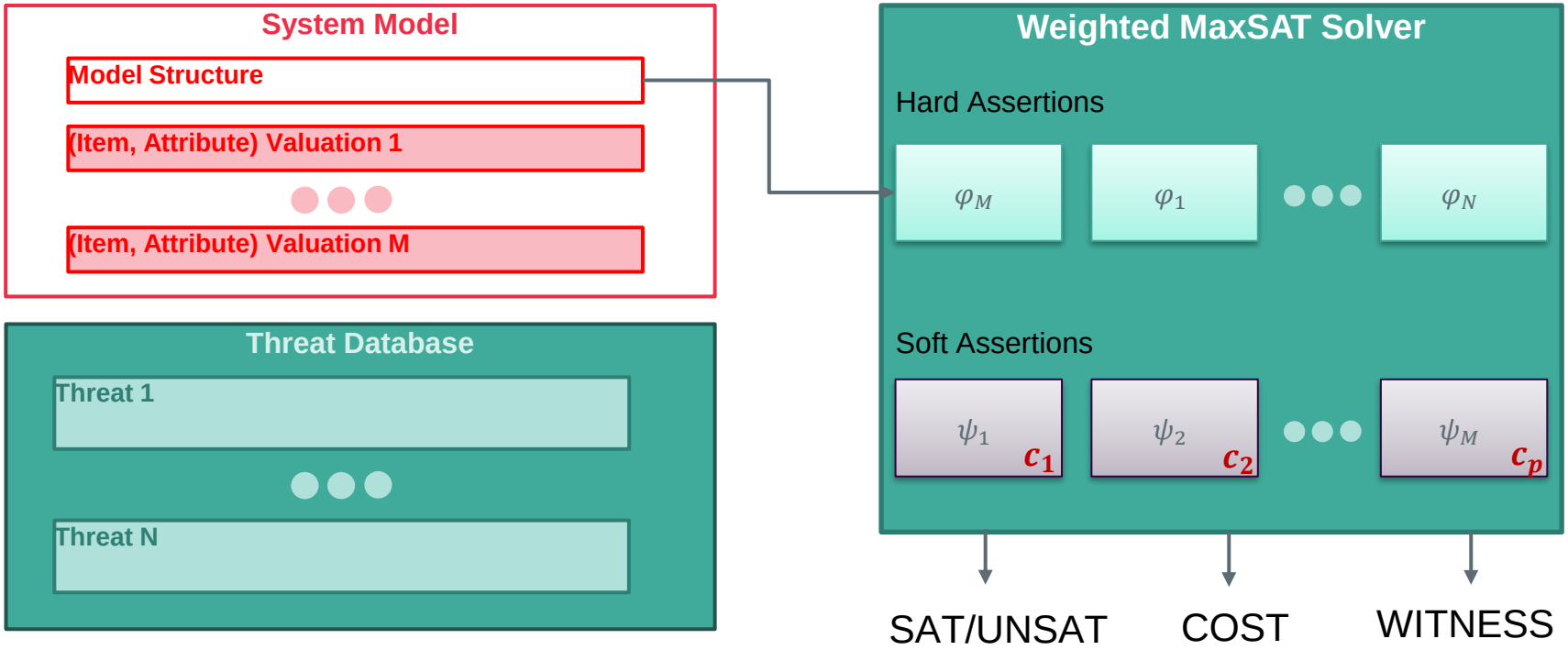


Attribute	Value	Weight
Authentication	No	100
Encryption	Yes	10
…	…	

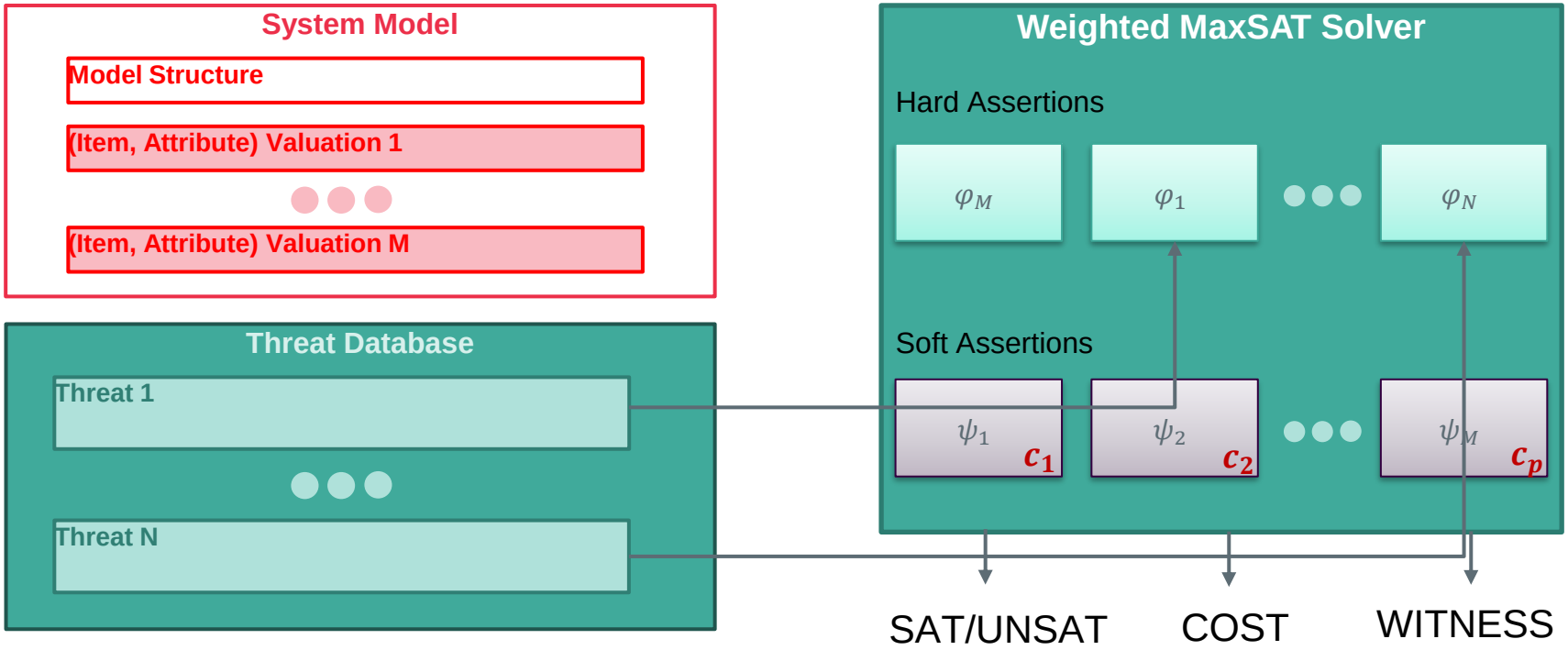
ATTRIBUTE REPAIR AS WEIGHTED MAXSAT



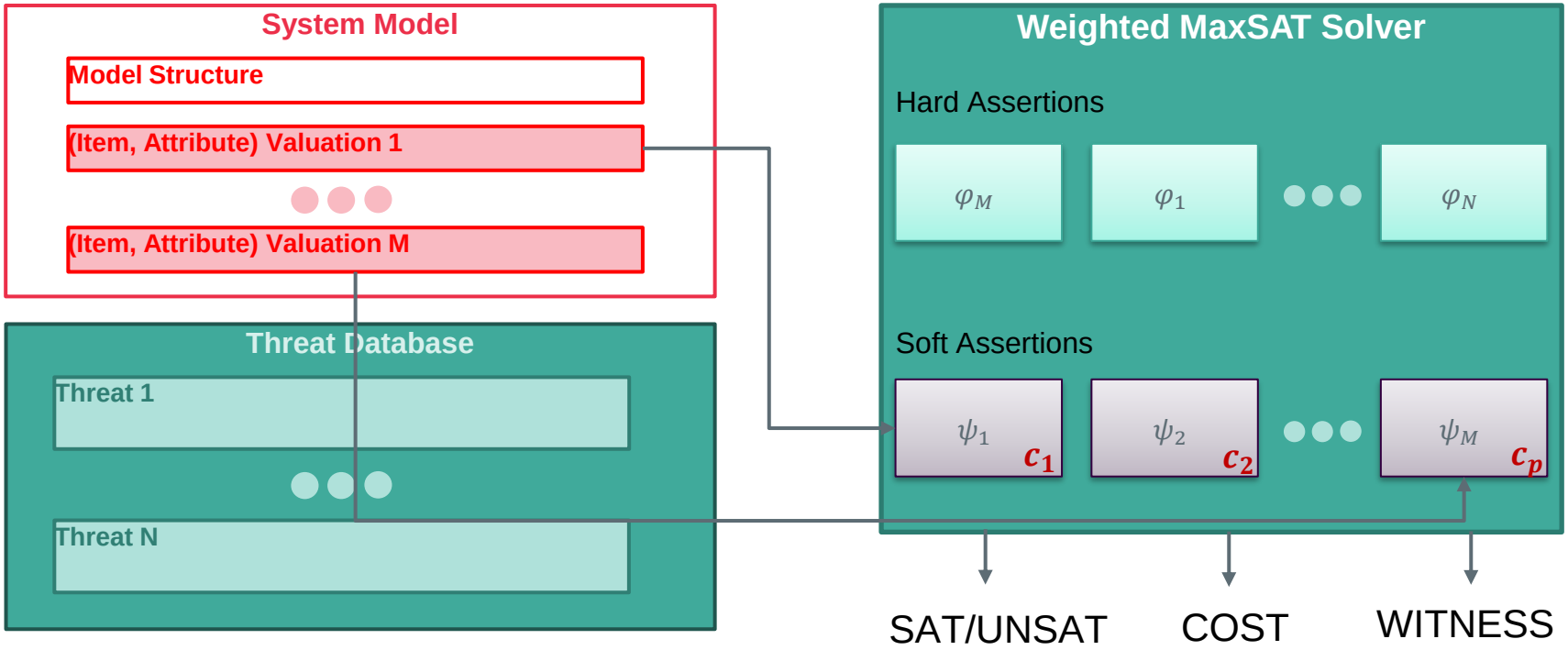
ATTRIBUTE REPAIR AS WEIGHTED MAXSAT

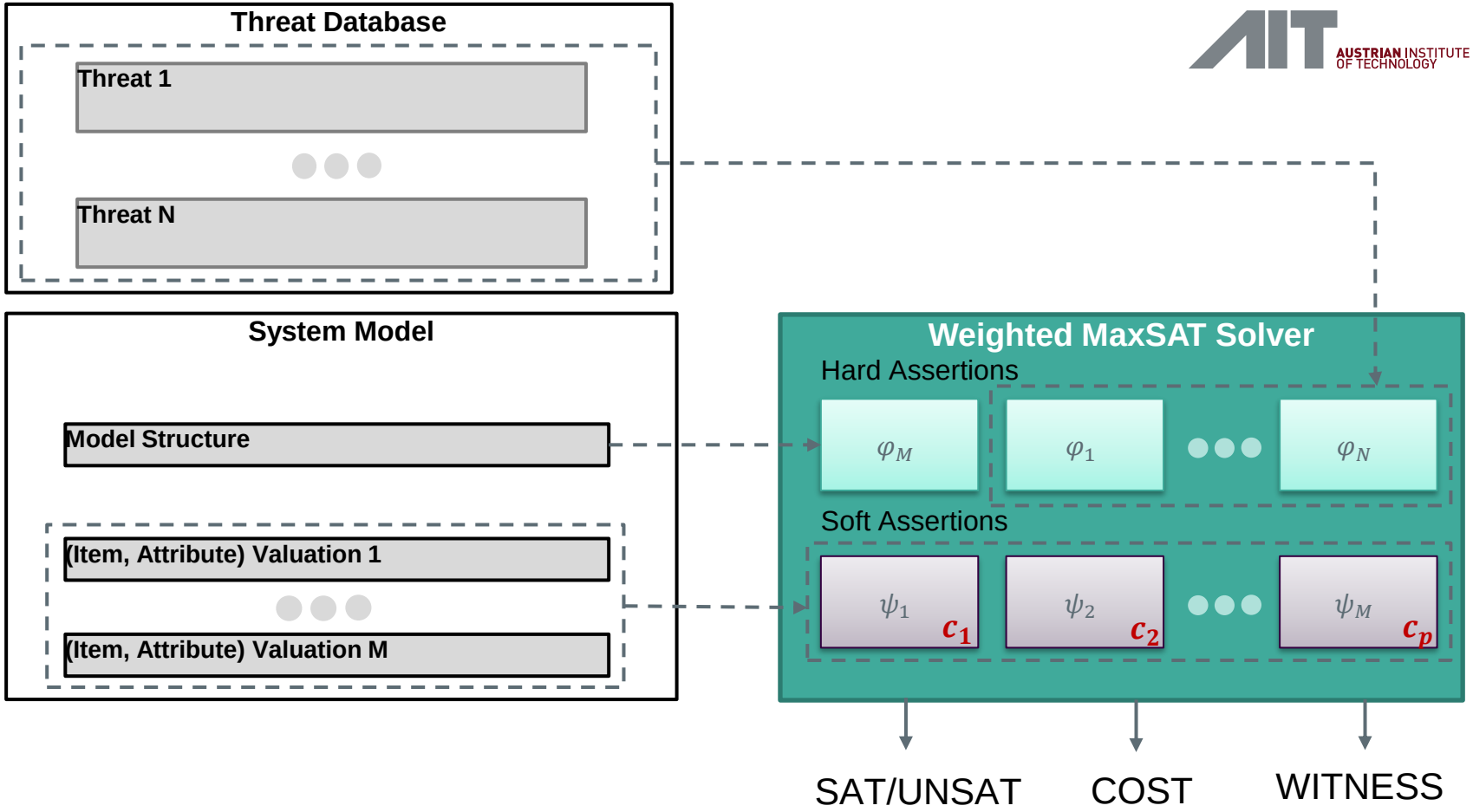


ATTRIBUTE REPAIR AS WEIGHTED MAXSAT

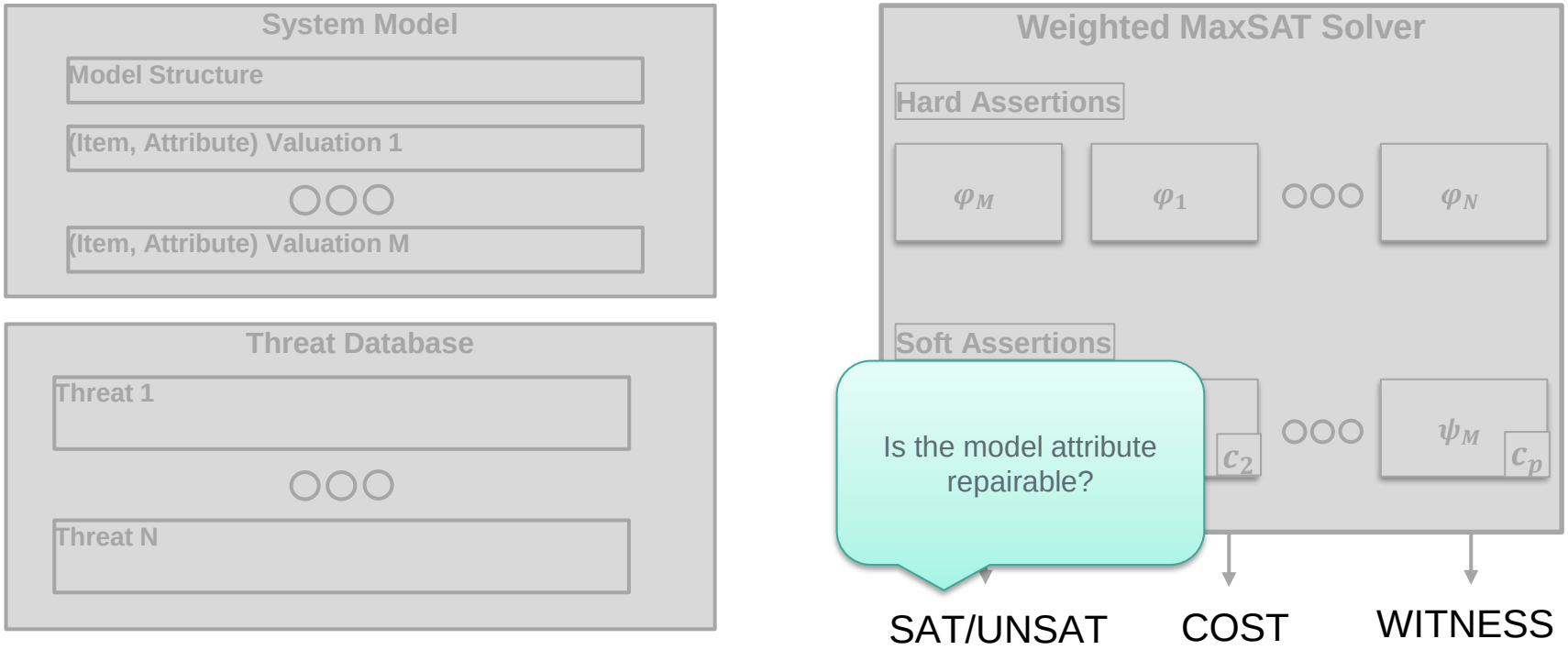


ATTRIBUTE REPAIR AS WEIGHTED MAXSAT

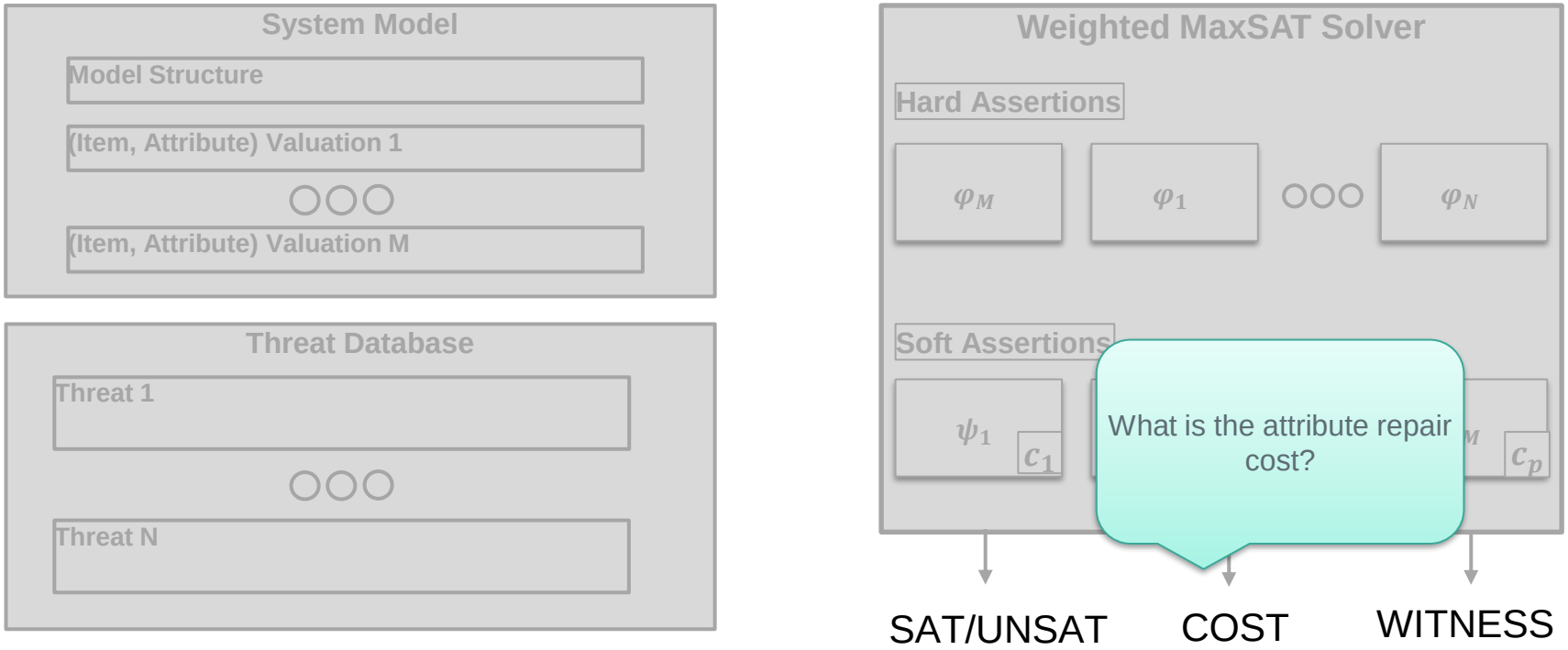



Threat Database
Threat 1
Threat N
System Model
Model Structure
(Item, Attribute) Valuation 1
(Item, Attribute) Valuation M
Weighted MaxSAT Solver
Hard Assertions
φ_M
φ_1
φ_N
Soft Assertions
ψ_1 c_1
ψ_2 c_2
ψ_M c_p
SAT/UNSAT
COST
WITNESS

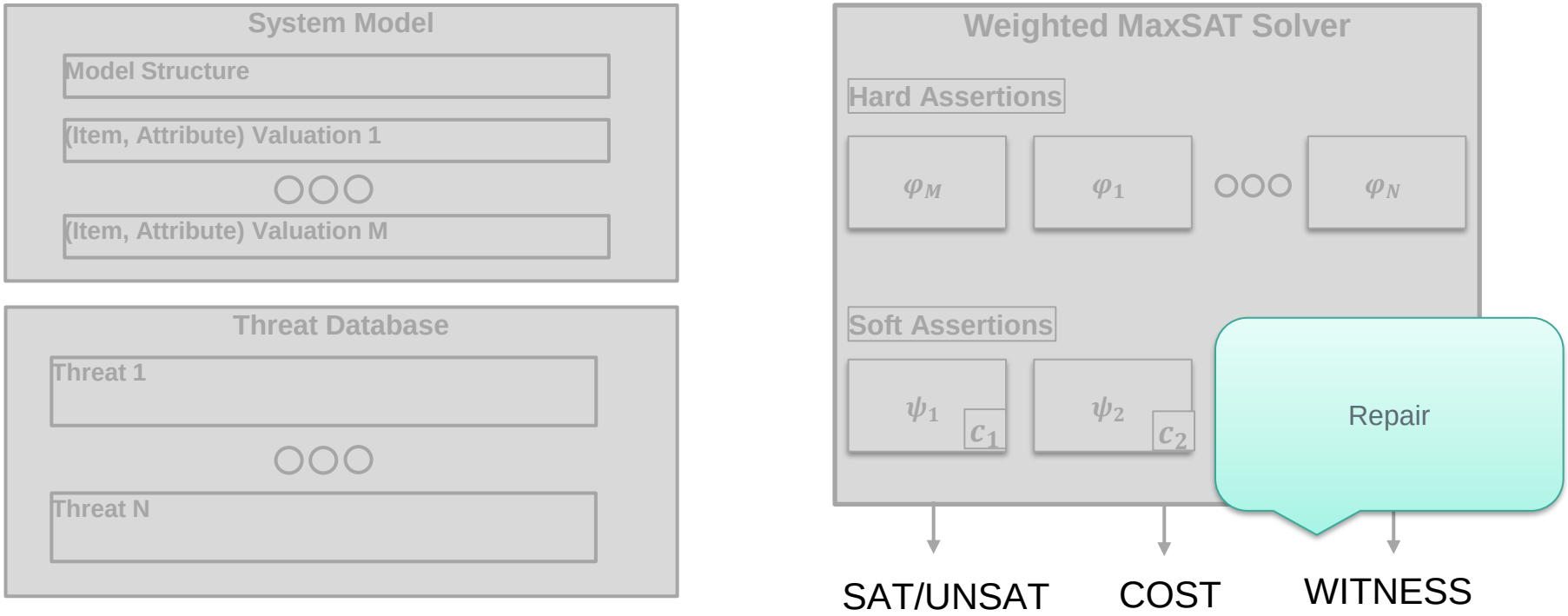
ATTRIBUTE REPAIR AS WEIGHTED MAXSAT



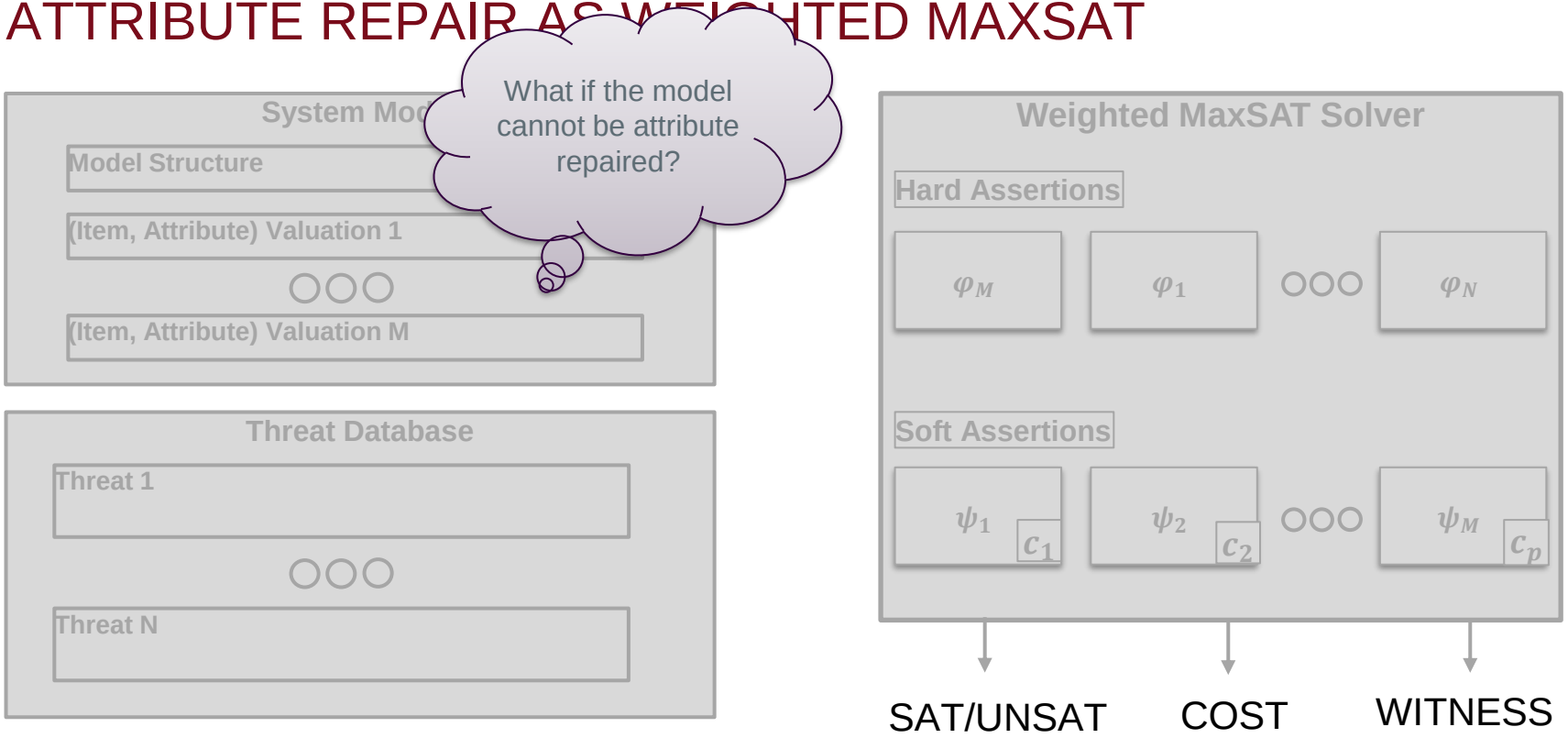
ATTRIBUTE REPAIR AS WEIGHTED MAXSAT



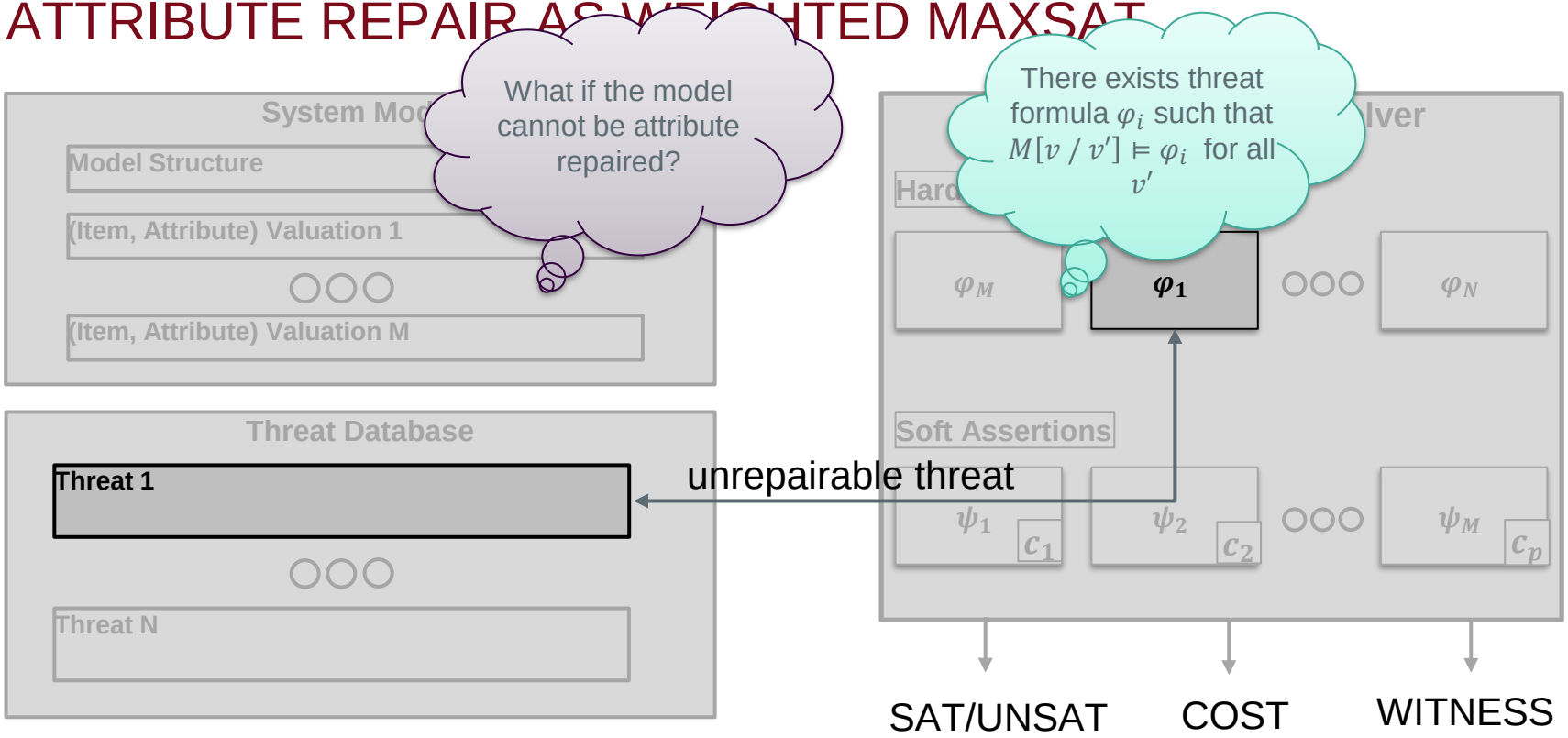
ATTRIBUTE REPAIR AS WEIGHTED MAXSAT



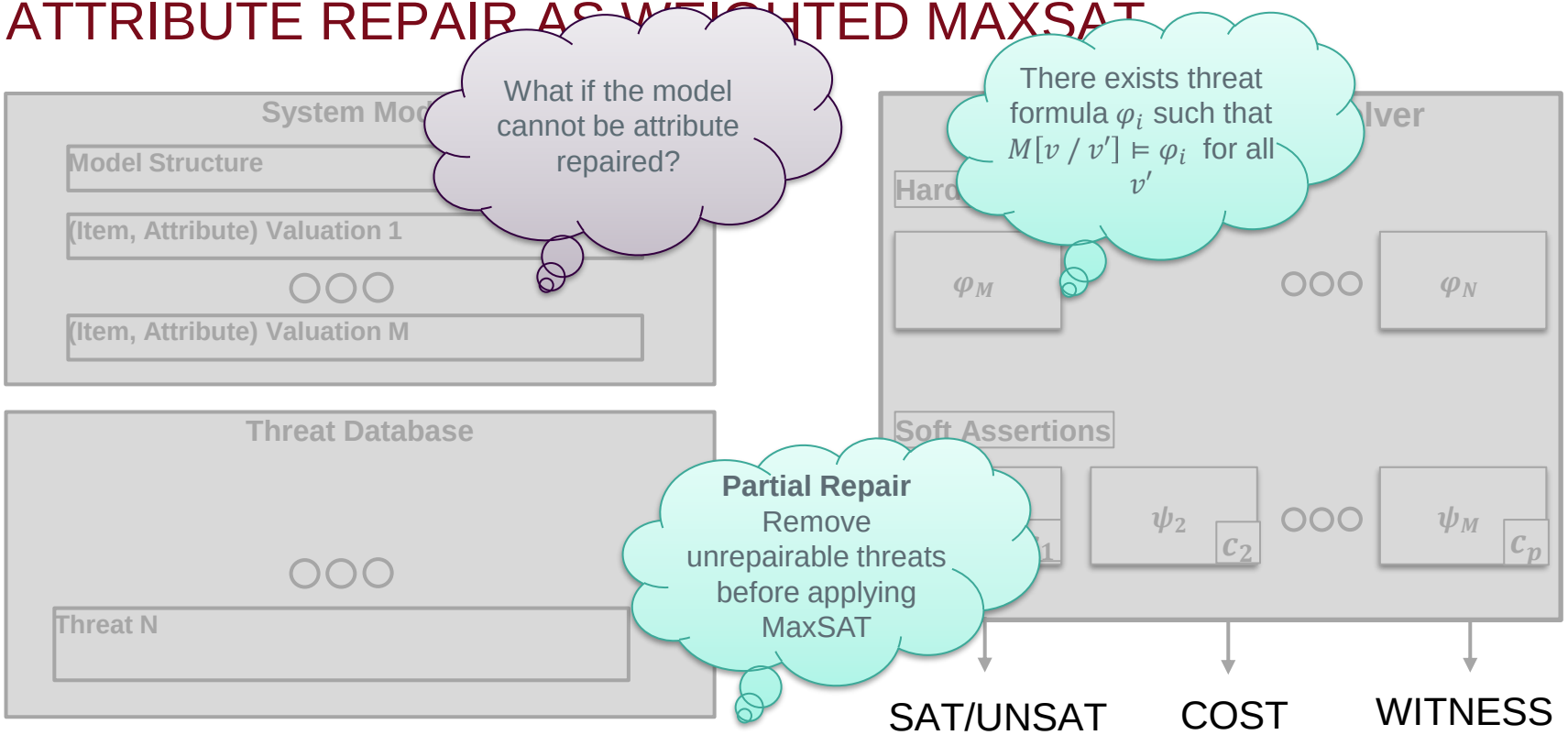
ATTRIBUTE REPAIR AS WEIGHTED MAXSAT



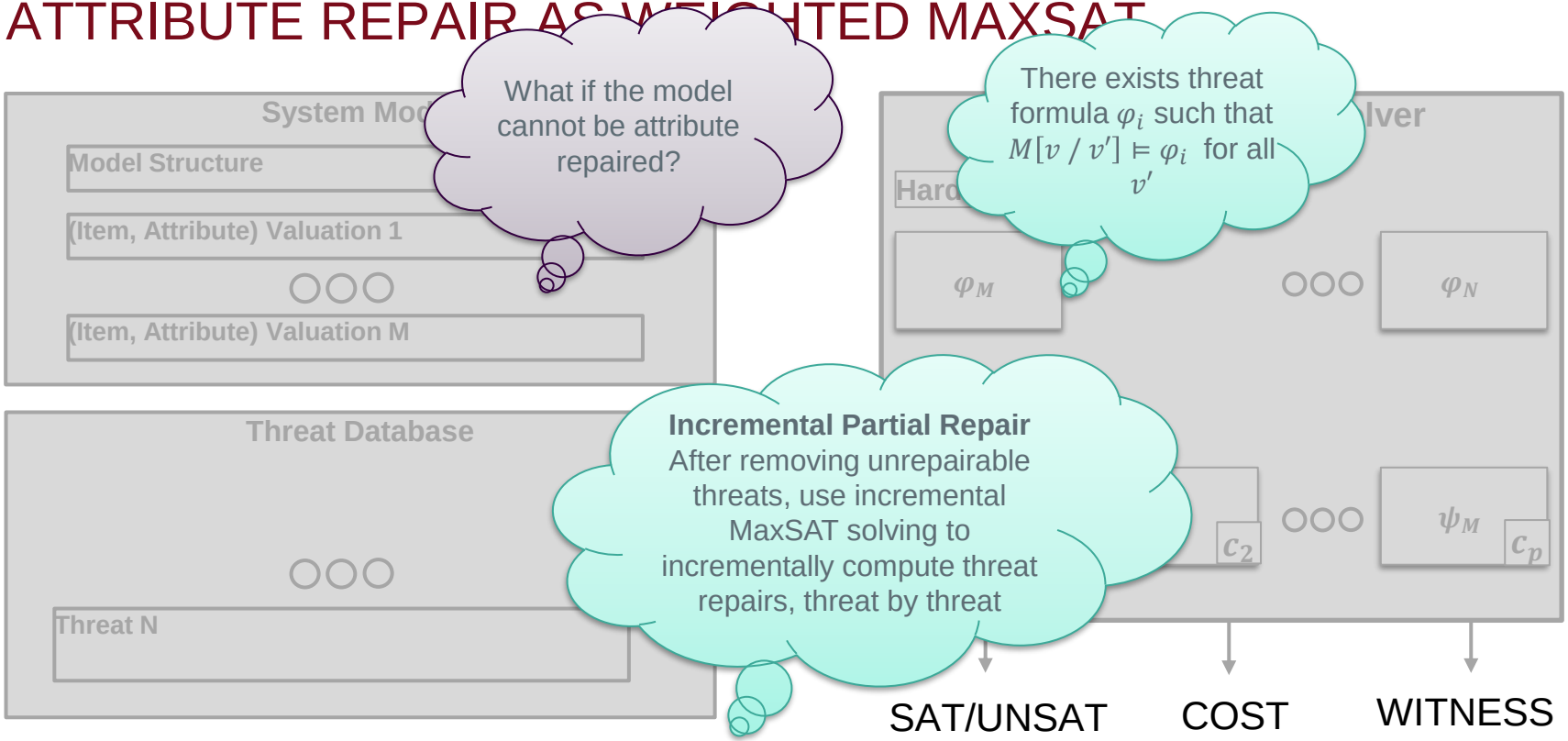
ATTRIBUTE REPAIR AS WEIGHTED MAXSAT



ATTRIBUTE REPAIR AS WEIGHTED MAXSAT



ATTRIBUTE REPAIR AS WEIGHTED MAXSAT

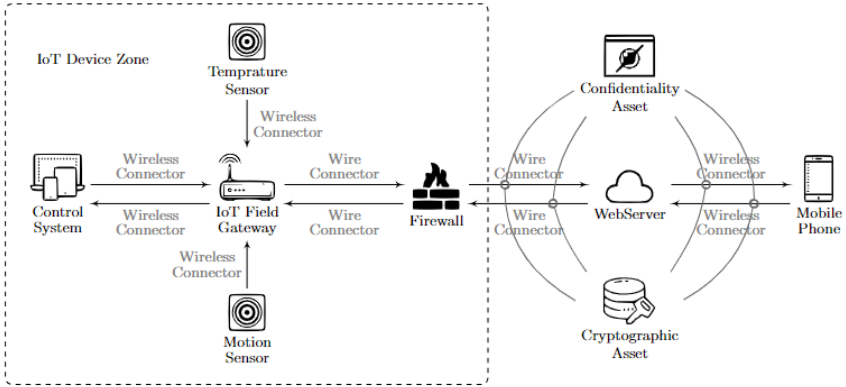


IMPLEMENTATION AND CASE STUDIES

IMPLEMENTATION

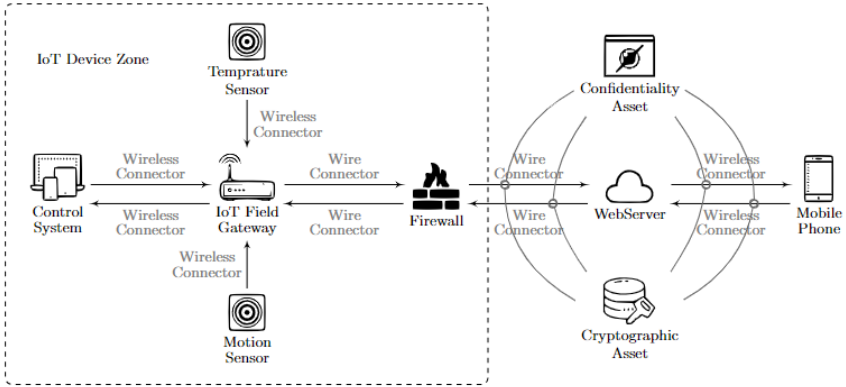
- Java implementation as an external module to THREATGET
- Z3 SMT solver used for MaxSAT

SMART HOME IOT



Verdict	SAT
# formulas (F)	169
# rep Fs	27
# unrep Fs	9
# Fs wo threat	133
Total cost	77
Time	47

SMART HOME IOT



Verdict	SAT
# formulas (F)	169
# rep Fs	27
# unrep Fs	9
# Fs wo threat	133
Total cost	77
Time	47

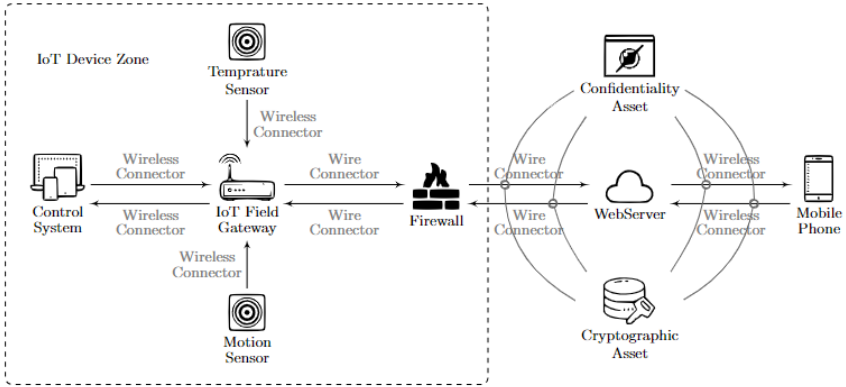
Example of repairable threat:

"Attacker can deny the malicious act and remove the attack footprints leading to repudiation issues"

$$\exists e.\, type(e) = Firewall \wedge v(e, Activity\ Logging) \in \{Missing, Undefined\}$$

Repair: set Activity Logging to Yes

SMART HOME IOT



Verdict	SAT
# formulas (F)	169
# rep Fs	27
# unrep Fs	9
# Fs wo threat	133
Total cost	77
Time	47

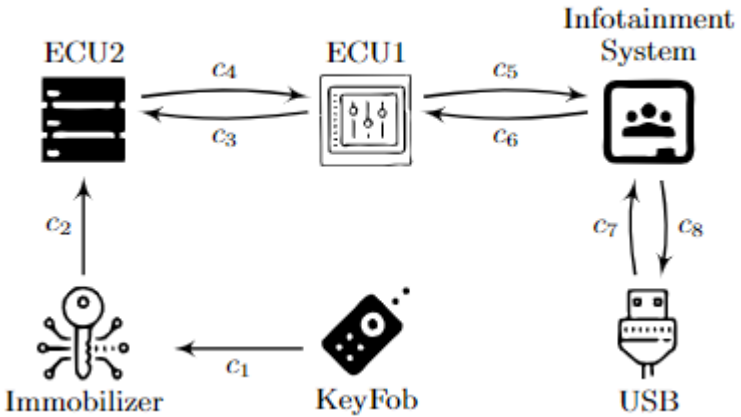
Example of unrepairable threat:

"Spoof IP"

$$\exists e_1, e_2, c.\, type(c) = Internet\ Connection \wedge src(c) = e_1 \wedge tgt(c) = e_2$$

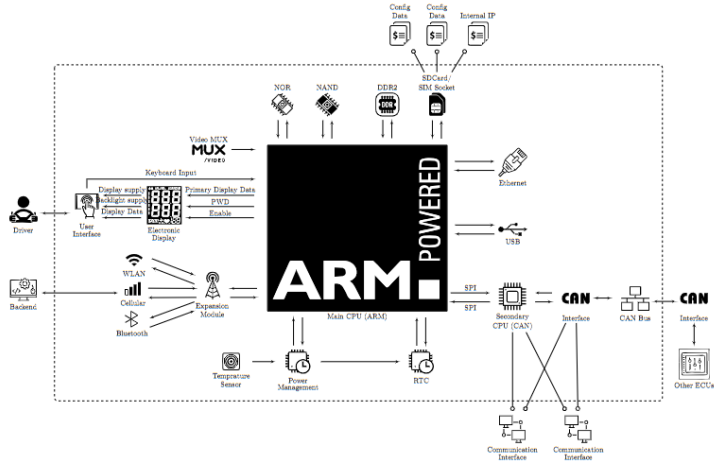
Cannot remove the internet connection with attributes

KEYFOB



	All threats		Subset	
	Full	**Heur**	**Full**	**Heur**
Verdict	UNSAT	SAT	SAT	SAT
Total # Fs	165	165	21	21
# rep Fs	n/a	25	4	4
# unrep Fs	n/a	7	0	0
# Fs wo threat	n/a	133	17	17
Cost	n/a	33	9	11
Time (s)	4	103	10	26

VEHICULAR TELEMATIC GATEWAY



Threat rule with flow (path) property

	With flow	WO flow
Verdict	SAT	SAT
Total # Fs	95	82
# rep Fs	19	18
# unrep Fs	23	21
# Fs wo threats	53	43
Cost	57	57
Time (s)	497	118

CONCLUSIONS

- Automated threat prevention
  - Repairing security-related system attributes
- Widely applicable
- SAT formulation of flows not optimal

- Model repair
  - Address limitation of attribute repair
  - Define a set of meaningful repair patterns

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Lecturer, Date