MUHAMMAD AZWAN IBRAHIM

Proving attack tree for software risk analysis in legal metrology

Enhancing the analysis of attack tree via formal method

Software Risk Assessment in Legal Metrology

The main purpose of the risk analysis is to identify threats to the legally relevant assets provided and to determine their associated risk, i.e. assign a score to each threat based on its impact and probability of occurrence.

- Previously PTB has developed a software risk assessment procedure tailored for the needs in legal metrology
- manufacturers of measuring instruments shall perform and document a risk assessment of their instruments before submitting a prototype to a NB for conformity assessment
- The procedure closely follows the vulnerability analysis of ISO/IEC 18045

Sum of points	TOE resistance	Probability score
0-9	No rating	5
10-13	Basic	4
14-19	Enhanced Basic	3
20-24	Moderate	2
≥ 24	High	1

Target of Evaluation Resistance Rating

ISO/IEC 27005 defines the term risk as a combination of the consequences (impact), which follows from an unwanted event (threat), and the probability of occurrence of the threat.

Thus, the risk associated with a threat can be modelled by the following equation:

$$\text{risk} = \text{impact} \times \text{probability of occurrence}$$

In the context of legal metrology, the term impact refers to a breach of the essential requirements.

Three components are required to calculate risk:

- List of unwanted events
- Consequences resulting from such events
- Likelihood of occurrence

APEC Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Risk Identification

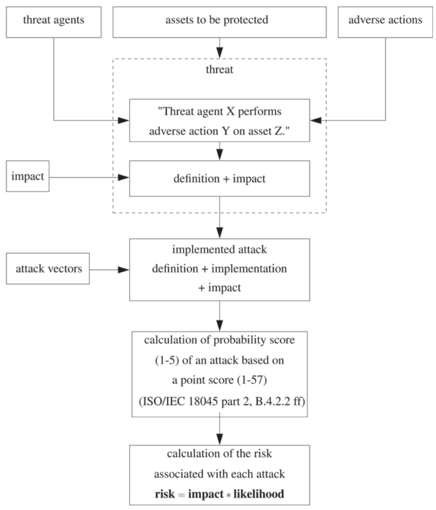
- During risk identification, unwanted events (so-called threats to assets) are defined based on ”legal and regulatory requirements, and contractual obligations“
- In Europe, assets is derived from the essential requirements given in Annex I of MID.

APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Flowchart of the basic risk assessment procedure



APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Calculation of Attack Probability
(ISO 18045 Part 2)

Vulnerability Analysis

1) Elapsed Time (1-19 points)
2) Expertise (0-8 points)
3) Knowledge of the TOE (0-11 points)
4) Window of Opportunity (0-10 points)
5) Equipment (0-9 points)

Σ

TOE resistance

Value	Resistance	Probability Score
0-9	No rating	5
10-13	Basic	4
14-19	Enhanced Basic	3
20-24	Moderate	2
>24	High	1

Risk Evaluation

Calculation of the Risk associated with an attack

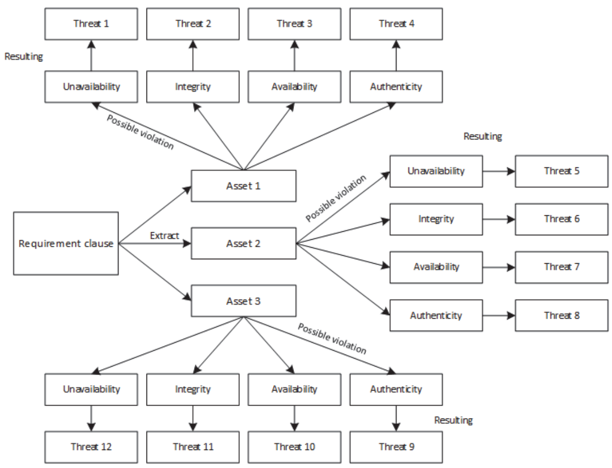
risk = impact*likelihood

Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Deriving threats to assets



- Threats consist of at least one asset to be protected and a statement, which security property is invalidated by the threat.
- At least one threat for each asset need to be formulated.
- A threat does not include any reference to its implementation w.r.t the instrument to be assessed.
- Example of threat: An attacker invalidates the integrity of one legally relevant parameter.

Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

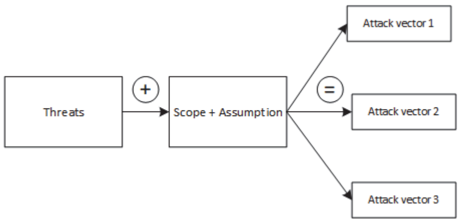
APEC

Example: Deriving of Assets from OIML R76 requirement

OIML R76	Requirements	Asset	Security Property
5.5.2.2 (a)	The **legally relevant software** shall be adequately **protected** against accidental or intentional changes. **Evidence of an intervention** such as changing, uploading or circumventing the legally relevant software shall be **available** until the next verification or comparable official inspection.	A1: Legally Relevant Software A2: Evidence of Intervention	Integrity (A1) Availabillity (A2) Integrity(A2)
5.5.2.2 (b)	When there is associated software which provides other functions besides the measuring function(s), the **legally relevant software** shall be **identifiable** and shall **not be inadmissibly influenced** by the associated software.	A3: Software identification A4: Inadmissible influence on the software	Availability (A3) Unavailability* (A4)
5.5.2.2 (c)	**Legally relevant software** shall be **identified** as such and shall be **secured**. Its **identification** shall be easily **provided** by the device for metrological controls or inspections.	A3: Software identification A1: Legally Relevant Software	Availability (A3) Integrity (A1) Authenticity (A1)

**Term "Unavailability" should be interpreted as: "There shall be no inadmissible influence on the legally relevant software."*

Deriving Attack Vectors



- Attack vector is the reference of method of implementations to realize a threat.

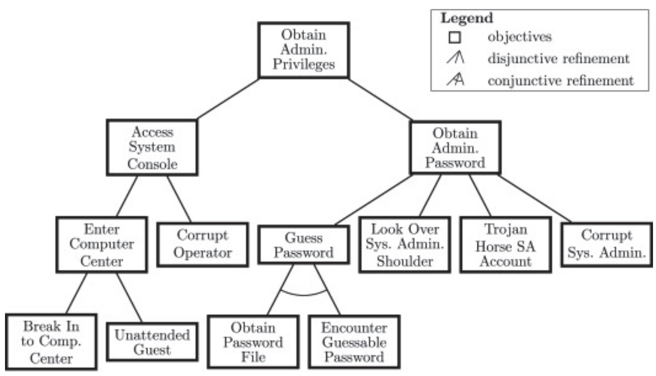
Attack vector	Time	Exper-tise	Knowl-edge	Window of opport.	Equip-ment	Justification
Attacker constructs fake results from datasets protected by a CRC32 with a secret start vector.	0	3	3	0	0	Assumed attacker: customer. CRC is a linear operation on binary vectors, an XOR-connection of two datasets automatically produces a third dataset with correct CRC. This can be calculated with standard software by a proficient user. No window of opportunity needed. The CRC is described in the manual.

**The scope is only for all threats that can be realized without leaving a trace.*

APEC Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

Introduction: Attack Tree

Attack trees are conceptual diagrams showing how an asset, or target, might be attacked. Attack trees have been used in a variety of applications. In the field of information technology, they have been used to describe threats on computer systems and possible attacks to realize those threats.



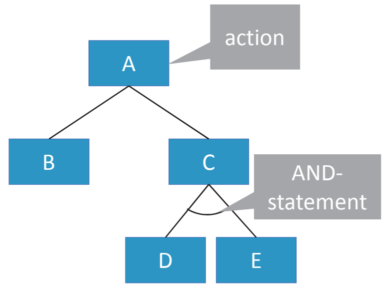
APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Introduction: Attack Probability Tree (AtPT)

- Graphical way to express the whole risk assessment procedure.
- Nodes in a tree represent actions or goals.
- Child nodes correspond to intermediate or sub-goals.
- Nodes may be linked by OR- and by AND-statements

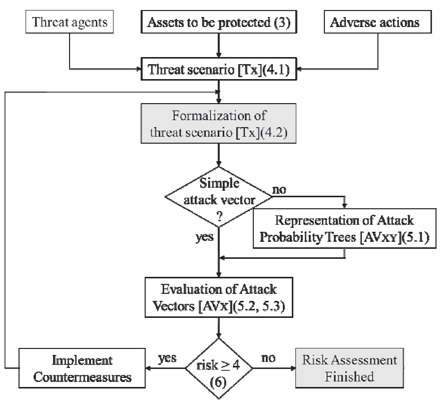


APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

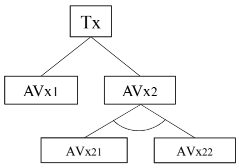
Workflow of the risk assessment



Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC



Attack Vector ID	Description	T	Ex	K	W	Eq
AVx1						
AVx2						
AVx21						
AVx22						

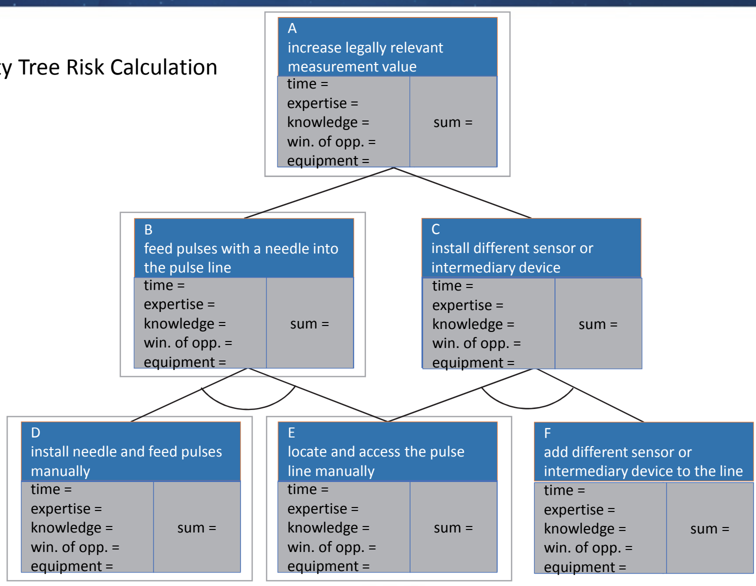
Exemplary Attack Probability Tree diagram with AND- and OR-connected nodes, for threat Tx, with attack vectors AVx1 and AVx2 and elementary attack vectors AVx21 and AVx22

Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Example of Attack Probability Tree Risk Calculation

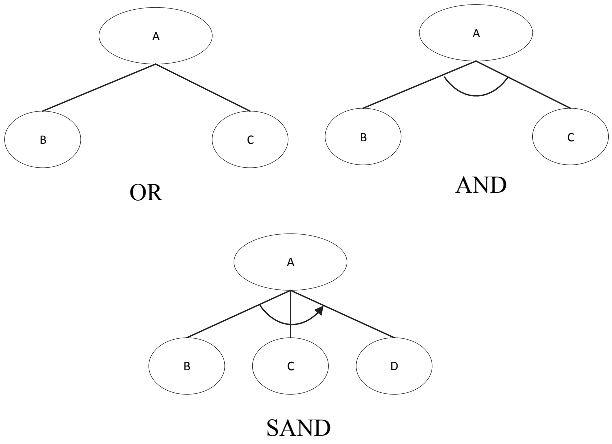


Attack Tree

OR nodes representing alternative choices – to achieve the goal of the node, the attacker needs to achieve the goal of at least one child;

AND nodes representing conjunctive decomposition – to achieve the goal of the node, the attacker needs to achieve all of the goals represented by its children (the children of an AND node are connected with an arc);

SAND nodes representing sequential decomposition – to achieve the goal of the node, the attacker needs to achieve all of the goals represented by its children in the given order (the children of a SAND node are connected with an arrow)



Correctness properties

Admissible property *if* : $[\![\langle \iota , \gamma \rangle]\!]^{S} \neq \emptyset$

Under-Match property *if* $[\![OP (\langle \iota_1 , \gamma_1 \rangle , \langle \iota_2 , \gamma_2 \rangle , \ldots \langle \iota_n , \gamma_n \rangle)]\!]^{S} \subseteq [\![\langle \iota , \gamma \rangle]\!]^{S}$

Over-Match property *if* $[\![OP (\langle \iota_1 , \gamma_1 \rangle , \langle \iota_2 , \gamma_2 \rangle , \ldots \langle \iota_n , \gamma_n \rangle)]\!]^{S} \supseteq [\![\langle \iota , \gamma \rangle]\!]^{S}$

Match property *if* $[\![OP (\langle \iota_1 , \gamma_1 \rangle , \langle \iota_2 , \gamma_2 \rangle , \ldots \langle \iota_n , \gamma_n \rangle)]\!]^{S} = [\![\langle \iota , \gamma \rangle]\!]^{S}$

Relevance of the correctness properties

- Meet property: The lowest level of property. At least one path in the system satisfying both parent goal and its refinement
- Under-Match property: Stronger level of property. From attackers perspective, bottom-up analysis need this. Enough to find vulnerability on the system.
- Over-Match property: The strongest property. From defender point of view. All the paths satisfying the parent goal also satisfy the its decomposition into sub-goals. For the purpose to find countermeasure.

M. Audinot et al. 2017

APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Description	AtPT	Audinot
Tree Model	Generic	Formal
Refinement	OR, AND	OR, AND, SAND
Node names	Informal, normal text-based	Formal notation$\langle \iota, \gamma \rangle$
Node description	Action-based (Motivation)	State-based
Design validation	None	Based on finite state transition

$\langle \iota, \gamma \rangle$: Leaf / Goal

$\langle \iota_i, \gamma_i \rangle$: Sub-goal

$[\![\langle \iota, \gamma \rangle]\!]^{\mathcal{S}}$: Set of paths in $\mathcal{S}$

M. Audinot et al. 2017

APEC Asia-Pacific Economic Cooperation

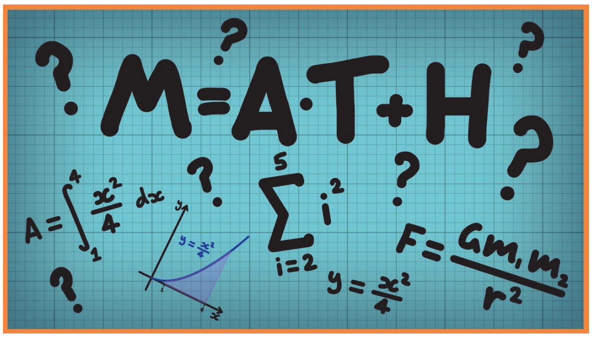
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Introduction

What is formal methods?

formal methods are a particular kind of mathematically rigorous techniques for the specification, development and verification of software and hardware systems.



Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Transition System

- A transition system consists of a set of configurations and a collection of transitions.
- Transition systems are used to describe dynamic processes with configurations representing states and transitions saying how to go from state to state.
- The main purpose of describing processes formally is that this allows us to subject the processes to formal analysis, ie. it allows us to talk about their properties in a precise way.

Set the Prop of propositions use to formalize possible configurations of the real system.
Prop contains propositions of the form ι, γ, to denote preconditions (ι) and postconditions (γ) of the goals.

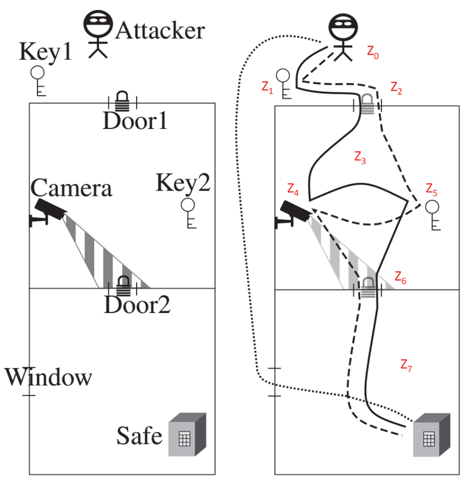
Definition (Transition system). *A transition system over* Prop *is a tuple* $\mathcal{S} = (S, \rightarrow, \lambda)$, *where* S *is a finite set of* states *(elements of* S *are denoted by* s, s_i *for* $i \in \mathbb{N}$*),* $\rightarrow \subseteq S \times S$ *is the* transition relation *of the system (which is assumed left-total), and* $\lambda : \text{Prop} \rightarrow 2^S$ *is the* labeling *function. We say that a state* s is labeled by p *when* $s \in \lambda(p)$*. The* size *of* $\mathcal{S}$ *is* $|\mathcal{S}| = |S| + |\rightarrow|$.

M. Audinot et al. 2017

Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC



(a) Floor plan (b) Attack scenarios

z_0 : Position = Outside; WOpen = ff; Locked1 = Locked2 = tt; Key1 = Key2 = ff; CamOn = tt; Detected = ff

consider 7 additional states z_i such that for every $1 \le i \le 7$, the specification of z_{i-1} is equal to z_i except one variable changed

z_1 : Same as z_0 except Key1 = tt

z_2 : Same as z_1 except Locked1 = ff

z_3 : Same as z_2 except Position = Room1

z_4 : Same as z_3 except CamOn = ff

z_5 : Same as z_4 except Key2 = tt

z_6 : Same as z_5 except Locked2 = ff

z_7 : Same as z_6 except Position = Room2

M. Audinot et al. 2017

Modeled using state variables whose values determine possible configurations of the system.

Position – variable describing the attacker's position, ranging over {Outside, Room1, Room2};
WOpen – Boolean variable describing whether the window is open (tt) or not (ff);
Locked1 and **Locked2** – Boolean variables to describe whether the respective doors are locked or not;
Key1 and **Key2** – Boolean variables to describe whether the attacker possesses the respective key;
CamOn – Boolean variable describing if the camera is on;
Detected – Boolean variable to describe if the camera detected the attacker

Initial configuration

ι := (Position = Outside) ∧ (Key1 = ff) ∧ (Key2 = ff) ∧ (Locked1 = tt) ∧ (Locked2 = tt) ∧ (CamOn = tt)

Final configuration

ι := (Position = Room2) ∧ (Detected = ff)

M. Audinot et al. 2017

APEC
Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC

State_variable	state: z0	z1	z2	z3	z4	z5	z6	z7
Wopen	✗	✗	✗	✗	✗	✗	✗	✗
Key1	✗	✓	✓	✓	✓	✓	✓	✓
Key2	✗	✗	✗	✗	✗	✓	✓	✓
Locked1	✓	✓	✗	✗	✗	✗	✗	✗
Locked2	✓	✓	✓	✓	✓	✓	✗	✗
CamOn	✓	✓	✓	✓	✗	✗	✗	✗
Detected	✗	✗	✗	✗	✗	✗	✗	✗
Position	O	O	O	R1	R1	R1	R1	R2

Table: Propositions

Red color indicate state changed.

O = Outside

R1, R2 = Room1, Room2

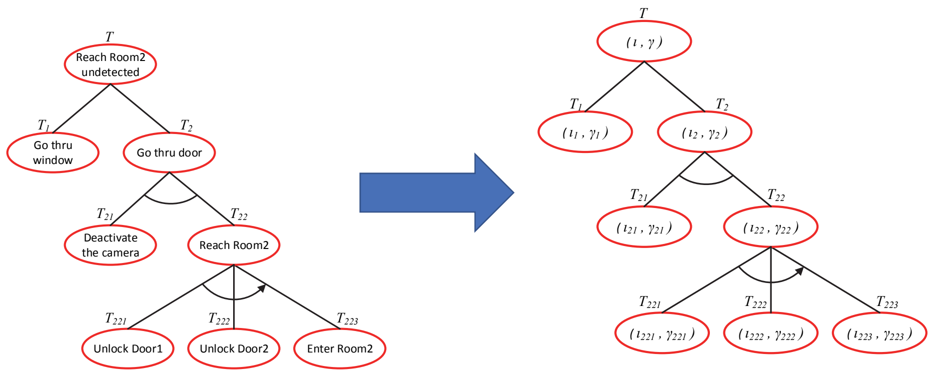
The path $p = z_0z_1z_2z_3z_4z_5z_6z_7$ is depicted using solid line in Fig.1 (b)

The set { $z_0z_1z_2z_3z_4$, $z_3z_4z_5z_6z_7$ } is an example of parallel decomposition of p.

M. Audinot et al. 2017

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

Formal notation of attach tree



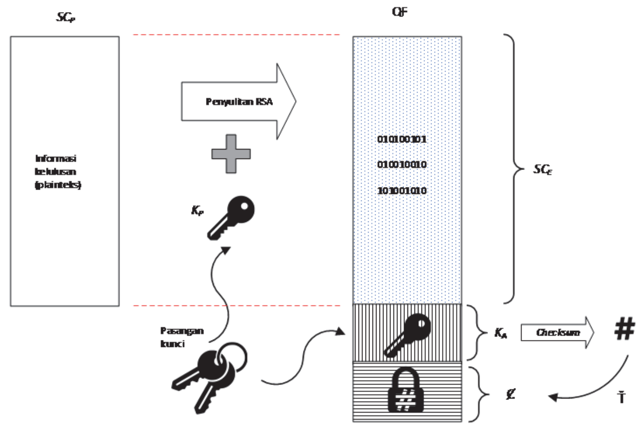
Definition (Attack tree). *An attack tree* T *over the set of propositions* Prop *is either a leaf* $\langle \iota, \gamma \rangle$, *where* $\iota, \gamma \in$ Prop, *or a composed tree of the form* $(\langle \iota, \gamma \rangle, \mathit{OP})(T_1, T_2, \ldots, T_n)$, *where* $\iota, \gamma \in$ Prop, $\mathit{OP} \in \{\mathit{OR}, \mathit{AND}, \mathit{SAND}\}$ *has arity* $n \geq 2$, *and* $T_1, T_2, \ldots, T_n$ *are attack trees. The main goal of an attack tree* $T = (\langle \iota, \gamma \rangle, \mathit{OP})(T_1, T_2, \ldots, T_n)$ *is* $\langle \iota, \gamma \rangle$ *and its* operator *is* OP.

$$[\![\langle \iota , \gamma \rangle]\!]^S = \{ z_0 z_1 z_2 (z_3 z_4)^k z_5 z_6 z_7 \mid k \geq 1 \}$$

M. Audinot et al. 2017

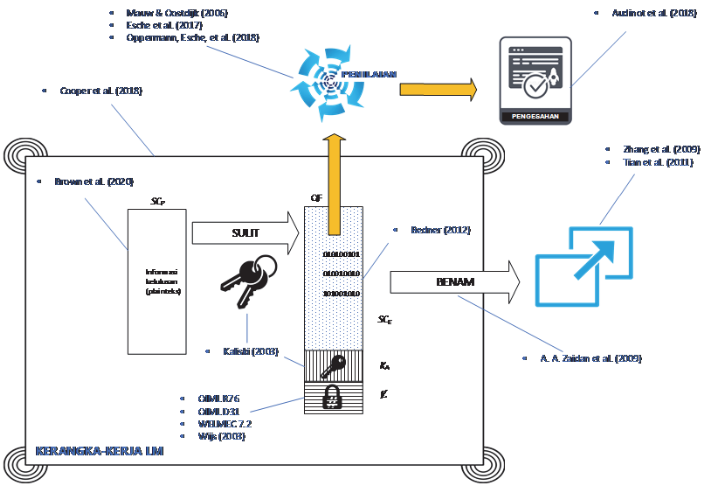
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

Security Object

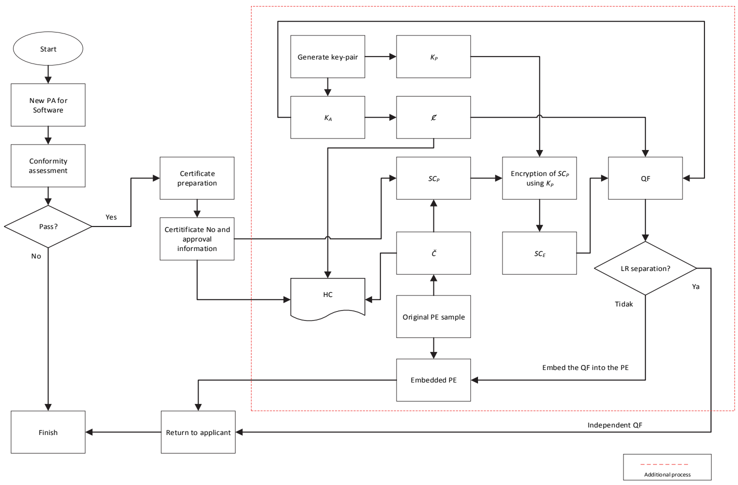


$$SC_P = decr(SC_E , K_A) = decr(encr(SC_P , K_P) , K_A)$$

Theoretical framework



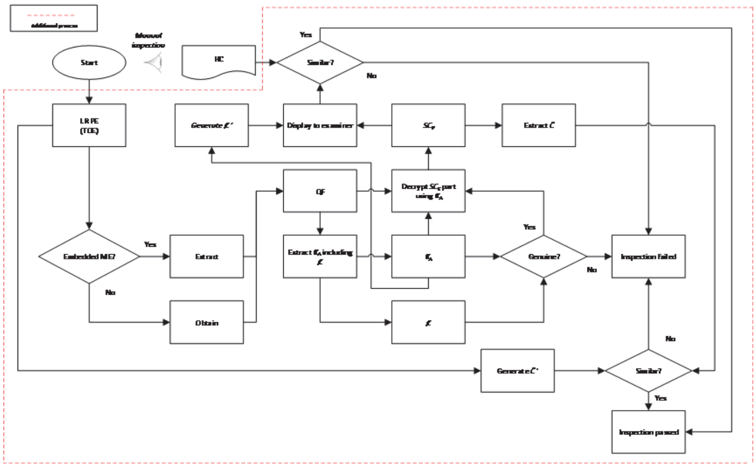
APEC
Asia-Pacific
Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC



APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC



APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

A set of questions which mimic the situation of each leaf has been constructed. This is to assign marks to each of the attributes in risk analysis.

This is possible due to the nature of state-based attack tree

Expert	Organisation	Expertise	Experience (Tahun)
A	CyberSecurity Malaysia	Protective Security Management	10
B	BIT Software Sdn. Bhd.	Programming, Cyber Security, Blockchain Technology	9
C	SIRIM Berhad	IT Infrastructure	20
D	Serba Dinamik IT Solutions	Customized software solution expert for top leading industries using advanced technologies	15
E	CIAST	Network & IT Management	20

PART B2: ATTRIBUTES ASSIGNMENT

1. Assuming a person is locating for a suspicious file (unidentified) inside a folder and the person is very familiar with the file contents inside the target folder. What are the attributes required to perform the task?

a. Elapsed Time. Time required to perform the task:

a. ☐ Less than one (1) day	f. ☐ Less than three months
b. ☐ Less than one (1) week	g. ☐ Less than four months
c. ☐ Less than two (2) weeks	h. ☐ Less than five months
d. ☐ Less than one month	i. ☐ Less than six months
e. ☐ Less than 2 months	j. ☐ More than six months

b. Expertise. Level of expertise required to perform the task:

a. ☐ Layman	c. ☐ Expert
b. ☐ Proficient	d. ☐ Multiple experts

c. Knowledge. Knowledge required to perform the task

a. ☐ Public	c. ☐ Sensitive
b. ☐ Restricted	d. ☐ Critical

d. Equipment. Tools required to perform the task

a. ☐ Standard	c. ☐ Bespoke
b. ☐ Specialized	d. ☐ Multiple bespoke

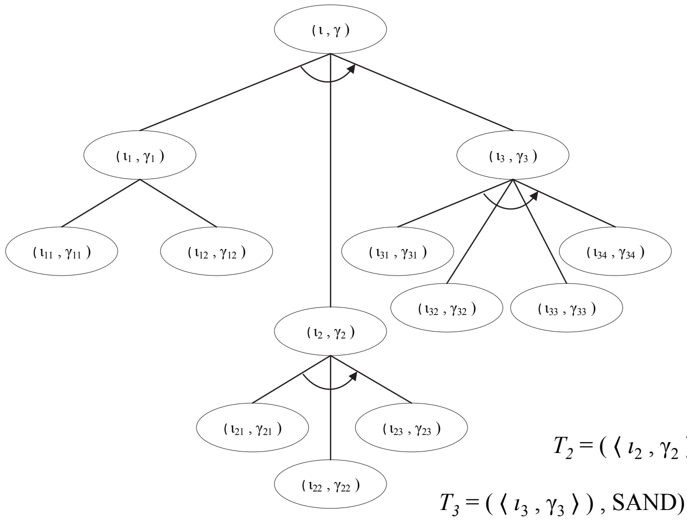
Additional remark (optional) : ....

- The score of attack vector attributes were taken from experts in IT

APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC



$T_1 = (\langle \iota_1 , \gamma_1 \rangle) , \mathrm{OR}) (\langle \iota_{11} , \gamma_{11} \rangle , \langle \iota_{12} , \gamma_{12} \rangle)$

$T_2 = (\langle \iota_2 , \gamma_2 \rangle) , \mathrm{SAND}) (\langle \iota_{21} , \gamma_{21} \rangle , \langle \iota_{22} , \gamma_{22} \rangle , \langle \iota_{23} , \gamma_{23} \rangle)$

$T_3 = (\langle \iota_3 , \gamma_3 \rangle) , \mathrm{SAND}) (\langle \iota_{31} , \gamma_{31} \rangle , \langle \iota_{32} , \gamma_{32} \rangle , \langle \iota_{33} , \gamma_{33} \rangle , \langle \iota_{34} , \gamma_{34} \rangle)$

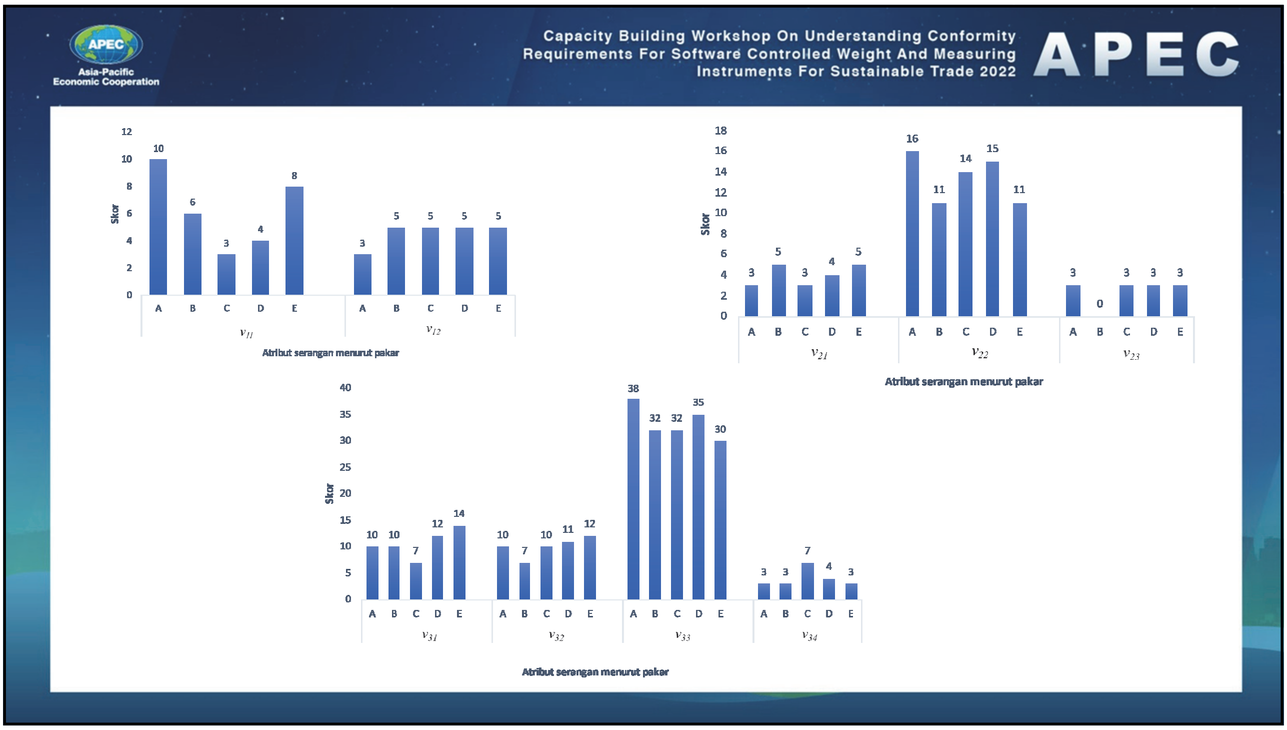
APEC Asia-Pacific Economic Cooperation

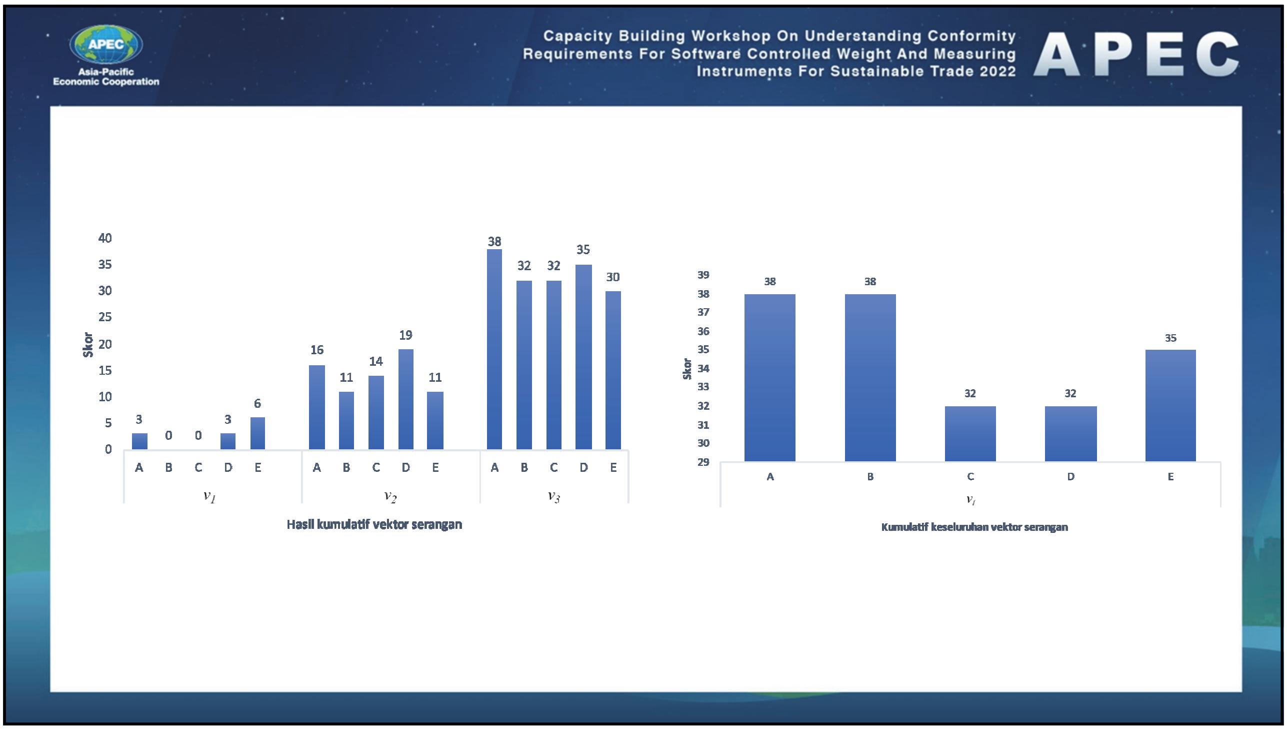
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

Variable	z_0	z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9
Q	Q-	Q+	Qg	Qg	Qg	Qg	Qg	Qg	Qg	Qt
PKey	NaC	NaC	NaC	AcG	AcG	AcG	AcF	AcF	AcF	AcF
ScP	Uo	Uo	Uo	Uo	Op	Oe	Oe	Oc	Oc	Oc
TpRev	ff	ff	ff	ff	Ff	ff	ff	ff	tt	tt

Tree	Admissible	Meet	Match
T	✓	✓	✓
T_1	✓	✓	✓*
T_2	✓	✓	✓
T_3	✓	✓	✓

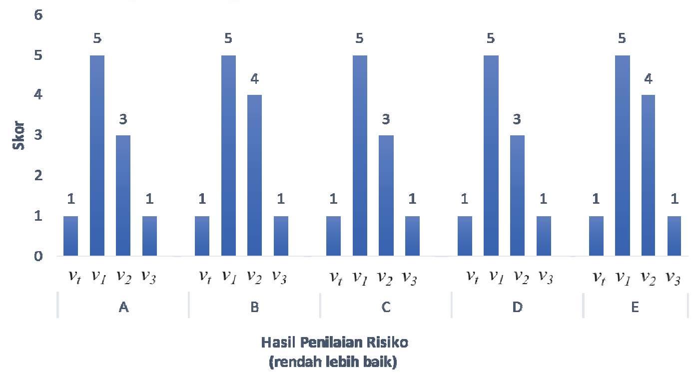

APEC
Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC
Skor
Atribut serangan menurut pakar
Skor
Atribut serangan menurut pakar
Skor
Atribut serangan menurut pakar


APEC
Asia-Pacific Economic Cooperation
Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022
APEC
Skor
Hasil kumulatif vektor serangan
Skor
Kumulatif keseluruhan vektor serangan

APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC



Risk Ri < 3 shows the minimum acceptable. Total risk of vt from overall experts show 1 (lowest). Thus, it can be concluded that the security object is very secure.

APEC Asia-Pacific Economic Cooperation

Capacity Building Workshop On Understanding Conformity Requirements For Software Controlled Weight And Measuring Instruments For Sustainable Trade 2022

APEC

SIRIM

NMIM NATIONAL METROLOGY INSTITUTE OF MALAYSIA

National Metrology Institute of Malaysia
Lot PT 4803, Bandar Baru Salak Tinggi
43900 Sepang, Selangor Malaysia

Dr. Muhammad Azwan Ibrahim
Telephone: 603 8778 1658
E-Mail: mdazwan@sirim.my
www.nmim.gov.my