



OKTEM CC LAB, TURKEY

**AN ALTERNATIVE APPROACH FOR ATTACK
POTENTIAL CALCULATIONS OF SMARTCARDS**

BETUL SOYSAL, CC EVALUATOR

betul.soysal@uekae.tubitak.gov.tr

➤ INTRODUCTION

- ❖ THE CURRENT ATTACK CALCULATION METHOD FOR SMARTCARDS
- ❖ THE MOTIVATION OF NEW PROPOSAL

➤ POINTS THAT WE PROPOSE REVISION & PROPOSALS

- ❖ COMBINING THE IDENTIFICATION & EXPLOITATION PHASES
- ❖ RESCALING & REGRADING THE FACTORS
- ❖ FINAL ATTACK & VULNERABILITY DEGREE CALCULATION TABLES AND EXAMPLES

➤ CONCLUSION

GENERAL ATTACK POTENTIAL CALCULATION APPROACH

- ✓ ATTACK SCENARIOS ARE DEFINED
- ✓ ATTACK POTENTIALS ARE CALCULATED
- ✓ ATTACKS ARE PERFORMED IF NOT MEANINGLESS
- ✓ FOR EACH SUCCESSFUL ATTACK SCENARIO, AVA_VAN
DEGREE IS DETERMINED

MAIN FEATURES OF THE CURRENT SMARTCARD ATTACK POTENTIAL CALCULATION



- THE MANDATORY DOCUMENT “APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS” IS USED (CEM IS NOT USED)
- THE ATTACK POTENTIAL IS CALCULATED IN TWO PHASES:
 - THE IDENTIFICATION PHASE
 - THE EXPLOITATION PHASE(CEM3.1 COMBINES THE TWO PHASES)
- THE ATTACK POTENTIAL IS CALCULATED USING THE FOLLOWING FACTORS:
 - ELAPSED TIME
 - ACCESS TO TOE
 - EXPERTISE
 - TOE KNOWLEDGE
 - EQUIPMENT
 - OPEN SAMPLE USAGE (ONLY FOR SMARTCARDS)

CURRENT SMARTCARD ATTACK POTENTIAL CALCULATION



	Time	Expertise	Toe knowledge	Number	Equipment	Open smpl
IDENTIFICATION	<1 hour /0	Layman /0	Public /0	< 10 /0	None /0	Public /0
	<1 day /1	Proficient/2	Restricted /2	< 100 /2	Standard /1	Restricted /2
	<1week /2	Expert /5	Sensitive /4	> 100 /3	Specialized /3	Sensitive /4
	<1month /3	Multiple Expert /7	Critical /6	Not Practical	Bespoke /5	Critical /6
	>1month /5		Very Critical HW Design /9		Mult. Bespoke /7	
EXPLOITATION	<1 hour /0	Layman /0	Public /0	< 10 /0	None /0	NA
	<1 day /3	Proficient/2	Restricted /2	< 100 /4	Standard /2	NA
	<1week /4	Expert /4	Sensitive /3	> 100 /6	Specialized /4	NA
	<1month /6	Multiple Expert /6	Critical /5	Not Practical	Bespoke /6	NA
	>1month /8		NA		Mult. Bespoke /8	NA

CURRENT SMARTCARD ATTACK POTENTIAL CALCULATION

	Time	Expertise	Toe knowledge	Number	Equipment	Open smpl
IDENTIFICATION	<1 hour /0	Layman /0	Public /0	< 10 /0	None /0	Public /0
	<1 day /1	Proficient/2	Restricted /2	< 100 /2	Standard /1	Restricted /2
	<1week /2	Expert /5	Sensitive /4	> 100 /3	Specialized /3	Sensitive /4
	<1month /3	Multiple Expert /7	Critical /6	Not Practical	Bespoke /5	Critical /6
	>1month /5		Very Critical HW Design /9		Mult. Bespoke /7	
EXPLOITATION	<1 hour /0	Layman /0	Public /0	< 10 /0	None /0	NA
	<1 day /3	Proficient/2	Restricted /2	< 100 /4	Standard /2	NA
	<1week /4	Expert /4	Sensitive /3	> 100 /6	Specialized /4	NA
	<1month /6	Multiple Expert /6	Critical /5	Not Practical	Bespoke /6	NA
	>1month /8		NA		Mult. Bespoke /8	NA

SUM : 9 + 10 = 19

CURRENT VULNERABILITY ASSESSMENT RATING IN THE CURRENT METHOD

Values Resulting from the current method	Attack potential required to exploit scenario:	Meets assurance components:	Failure of components:
0-15	BASIC	-	AVA_VAN.2,3,4,5
16-24	ENHANCED-BASIC	AVA_VAN.1, 2	AVA_VAN.3,4,5
21-24	MODERATE	AVA_VAN.1,2,3	AVA_VAN.4,5
24-30	HIGH	AVA_VAN.1,2,3,4	AVA_VAN.5
=>31	BEYOND HIGH	AVA_VAN.1,2,3,4,5	-

CURRENT VULNERABILITY ASSESSMENT RATING IN THE CURRENT METHOD



UEKAE

Values Resulting from the current method	Attack potential required to exploit scenario:	Meets assurance components:	Failure of components:
0-15	BASIC	-	AVA_VAN.2,3,4,5
16-24	ENHANCED-BASIC	AVA_VAN.1, 2	AVA_VAN.3,4,5
21-24	MODERATE	AVA_VAN.1,2,3	AVA_VAN.4,5
24-30	HIGH	AVA_VAN.1,2,3,4	AVA_VAN.5
=>31	BEYOND HIGH	AVA_VAN.1,2,3,4,5	-

➤ INTRODUCTION

- ❖ THE CURRENT ATTACK CALCULATION METHOD FOR SMARTCARDS
- ❖ THE MOTIVATION OF NEW PROPOSAL

➤ POINTS THAT WE PROPOSE REVISION & PROPOSALS

- ❖ COMBINING THE IDENTIFICATION & EXPLOITATION PHASES
- ❖ RESCALING & REGRADING THE FACTORS
- ❖ FINAL ATTACK & VULNERABILITY DEGREE CALCULATION

TABLES AND EXAMPLES

➤ CONCLUSION

❖ DISADVANTAGES OF THE CURRENT METHOD ARE:

- ❑ THE DIFFICULTY & SUBJECTIVITY IN DECIDING ON THE BOUNDARY OF THE IDENTIFICATION & THE EXPLOITATION PHASES
- ❑ THE DEFFICIENCY IN THE SCALING OF “ELAPSED TIME” AND “ACCESS TO TOE”

❖ THE MOTIVATION OF THE PROPOSED METHOD IS :

- ❑ TO EASE THE ATTACK CALCULATION,
- ❑ TO DECREASE THE SUBJECTIVITY
- ❑ TO INCREASE RESOLUTION IN GRADING
- ❑ TO KEEP THE VULNERABILITY DEGREES THE SAME

➤ INTRODUCTION

- ❖ THE CURRENT ATTACK CALCULATION METHOD FOR SMARTCARDS
- ❖ THE REASON OF NEW PROPOSAL

➤ POINTS THAT WE PROPOSE REVISION & PROPOSALS

- ❖ COMBINING THE IDENTIFICATION&EXPLOITATION PHASES
- ❖ RESCALING & REGRADING THE FACTORS
- ❖ FINAL ATTACK & VULNERABILITY DEGREE CALCULATION TABLES AND EXAMPLES

➤ CONCLUSION

❖ ATTACK CALCULATION GUIDE FOR SMARTCARDS OFFER TWO PHASES:

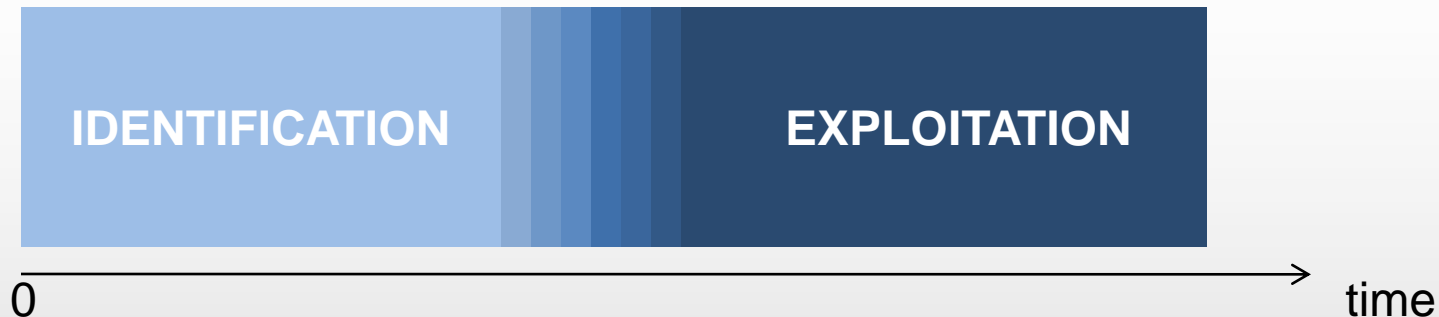
1. THE IDENTIFICATION OF THE ATTACK :

- ATTACK IS DEFINED,
- SCRIPTS ARE PREPARED,
- LAYOUT COORDINATES ARE RECORDED,
-

2. THE EXPLOITATION OF THE ATTACK :

- DEFINED ATTACK IS PERFORMED ON A DIFFERENT TOE,
- SCRIPTS ARE READY,
- NO TOE KNOWLEDGE IS USED
-

DIFFICULTY IN DECIDING THE IDENTIFICATION & THE EXPLOITATION PHASES



- ✓ THE ATTACK IS PERFORMED ONLY ONES,
DISTINCTION IS NOT BASED ON THE WAY THE ATTACK IS PERFORMED
- ✓ WHEN THE IDENTIFICATION ENDS ? &
WHEN THE EXPLOITATION STARTS ?
- ✓ SUBJECTIVITY INTRODUCED



ATTACK SCENARIO:

- ✓ AUTOMATED MEASUREMENT SW IS PREPARED
- ✓ POWER TRACES ARE OBTAINED & SAVED
- ✓ SCRIPTS FOR PROCESSING THE POWER TRACES ARE PREPARED
- ✓ PRE-PROCESSING IS DONE ON THE TRACES
- ✓ THE KEY BYTES ARE OBTAINED BY THE DPA METHOD

ATTACK CALCULATION:

IDENTIFICATION

- ✓ A
- ✓ P
- ✓ S
- ✓ P
- ✓ T
- ✓ T
- R

- IDENTIFICATION SCOPE IS EXACTLY THE SAME AS THE ATTACK SCENARIO

- EXPLOITATION SCOPE IS ONLY A REPETATION OF SOME STEPS

=> NO NEED FOR EXPLOITATION PHASE TO JUDGE ON THE POTENTIAL OF THIS ATTACK

EXPLOITATION

- ✓ P
 - ✓ P
 - ✓ TH
- USING RECORDED LOGS

ARE

OE

HOD

ATTACK CALCULATION:

IDENTIFICATION

- ✓ A
- ✓ PC
- ✓ SC
- A

- THE ATTACKER GENERALLY CAN NOT BE SURE ABOUT WHERE TO END THE IDENTIFICATION PHASE

BYTES

EXPLOITATION

- ✓ PC
- ✓ PE
- ✓ ALL

- SUBJECTIVE

OE

A PROPOSAL AGAINST THE SEPARATION OF THE PHASES

- ✓ COMBINE THE TWO ATTACK CALCULATION PHASES INTO ONE PHASE JUST AS IT IS IN THE ATTACK SCENARIO ITSELF



- ✓ OBTAIN AN ATTACK CALCULATION SCOPE, THE SAME AS THE ATTACK SCENARIO 😊

➤ INTRODUCTION

- ❖ THE CURRENT ATTACK CALCULATION METHOD FOR SMARTCARDS
- ❖ THE REASON OF NEW PROPOSAL

➤ POINTS THAT WE PROPOSE REVISION & PROPOSALS

- ❖ COMBINING THE IDENTIFICATION&EXPLOITATION PHASES
- ❖ RESCALING & REGRADING THE FACTORS
- ❖ FINAL ATTACK & VULNERABILITY DEGREE CALCULATION TABLES AND EXAMPLES

➤ CONCLUSION

- ELAPSED TIME IS RESCALED
- ACCESS TO TOE IS RESCALED
- EXPERTISE, TOE KNOWLEDGE, EQUIPMENT AND OPEN SAMPLE ARE REGRADED

CURRENT SCALING OF “ELAPSED TIME”

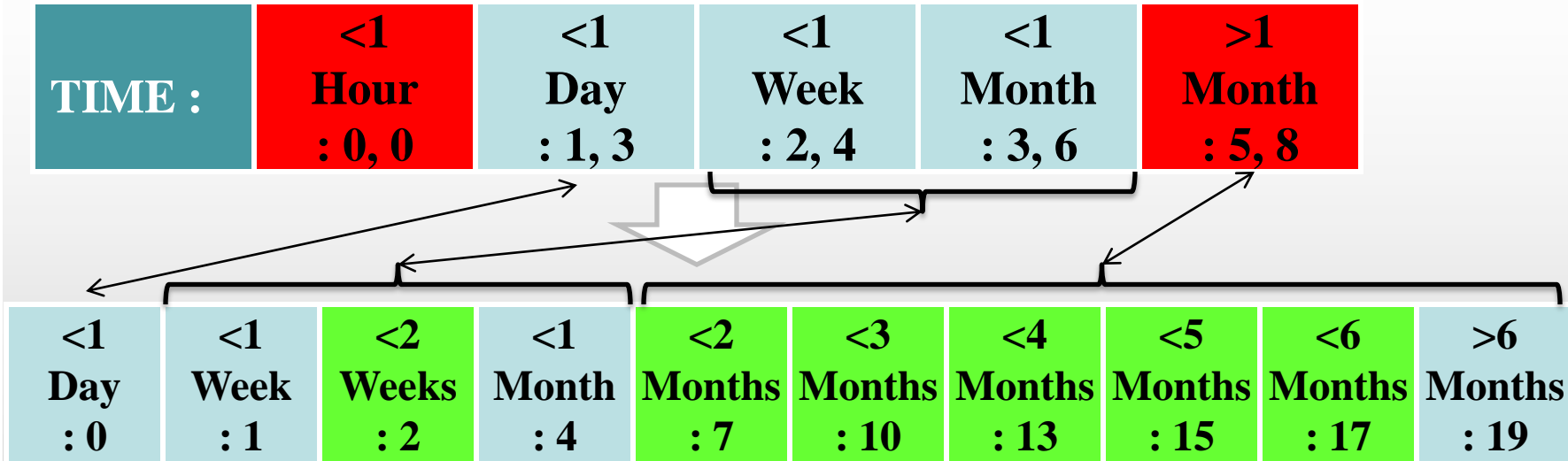
TIME :	<1 Hour : 0, 0	<1 Day : 1, 3	<1 Week : 2, 4	<1 Month : 3, 6	>1 Month : 5, 8
---------------	----------------------------------	---------------------------------	----------------------------------	-----------------------------------	-----------------------------------

- ❖ THERE SHOULD BE A DISTINCTION BETWEEN 1 WEEK & 4 WEEKS,
 - MOST OF THE ATTACKS LAST “<1 MONTH”

- ❖ THERE SHOULD BE MUCH MORE SCALINGS FOR TIME “>1 MONTH”,
 - EVEN A 1-YEAR–LASTING ATTACK MAY BE PRACTICAL FOR SMARTCARDS

- ❖ THE EFFECT OF THE TIME FACTOR ON TOTAL RATING SHOULD REMAIN THE SAME

REVISING THE SCALING OF “ELAPSED TIME”



- ✓ THE SAME AS CURRENT ELAPSED TIME SCALING FOR OTHER PRODUCTS
- ✓ <1 HOUR IS REMOVED AS NOT PRACTICAL WHEN PHASES ARE COMBINED
- ✓ <2 WEEKS IS ADDED TO DISTINCT 1 WEEK & 4 WEEKS
- ✓ >1 MONTH IS SCALED MORE, INCREASING THE RESOLUTION & ACCURACY

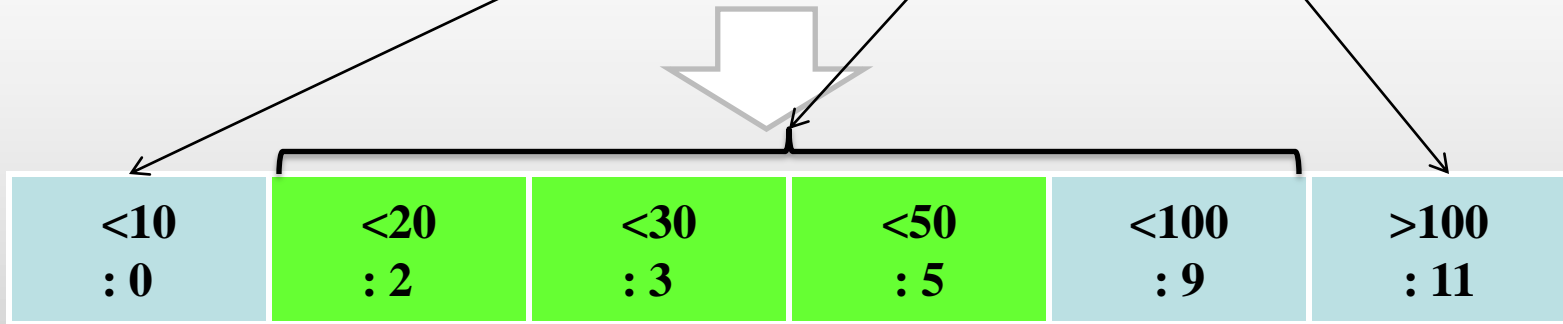
CURRENT SCALING OF “ACCESS TO TOE”

ACCESS TO TOE:	<10 : 0, 0	<100 : 2, 3	>100 : 4, 6
----------------	---------------	----------------	----------------

- ✓ SMALL# (LIKE 10) AND BIG# (LIKE 90) HAS THE SAME GRADING BUT THE DIFFERENCE IS CONSIDERABLE
- ✓ POINTS GIVEN FOR <100 & >100 ARE NOT ADEQUITE

REVISING THE SCALING OF “TOE NUMBER”

ACCESS TO TOE:	<10 : 0, 0	<100 : 2, 3	>100 : 4, 6
---------------------------	--------------------------	---------------------------	---------------------------



- ✓ <10 IS LEAVED THE SAME BECAUSE NUMBER IS NOT SUMMED UP WHEN PHASES ARE COMBINED
- ✓ <100 IS RESCALED TO SEPERATE USE OF SMALL AND BIG NOF SAMPLES
- ✓ HIGHER GRADES ARE GIVEN FOR <100 & >100
- ✓ NEW GRADES ARE GIVEN EVENLY

REVISING THE GRADING OF EXPERTISE, TOE KNOWLEDGE, EQUIPMENT AND OPEN SAMPLE



EXPERTISE		TOE KNOWLEDGE	
Layman	0, 0 ⇒ 0	Public	0, 0 ⇒ 0
Proficient	2, 2 ⇒ 2	Restricted	2, 2 ⇒ 2
Expert	4, 3 ⇒ 4		4, 3 ⇒ 4
Multiple Expert	6, 5 ⇒ 6		6, 5 ⇒ 6
			9, 0 ⇒ 9

✓ NO TOE KNOWLEDGE TO MAINTAIN
 H OTAI
 R ✓ NO OPEN SAMPLE IS USED IN RALLY
 E THE EXPLOITATION PHASE, SO SES
 THE GRADES IN THE
 ✓ IDENTIFICATION PHASE ARE AINED
 G NOT CHANGED ADES
 IC

EQUIPMENT		OPEN SAMPLE	
None	0, 0 ⇒ 0	Public	2 ⇒ 2
Standart	1, 2 ⇒ 3	Restricted	4 ⇒ 4
Specialized	3, 4 ⇒ 7	Sensitive	6 ⇒ 6
Bespoke	5, 6 ⇒ 11	Critical	9 ⇒ 9
Multiple Bespoke	7, 8 ⇒ 15		

➤ INTRODUCTION

- ❖ THE CURRENT ATTACK CALCULATION METHOD FOR SMARTCARDS
- ❖ THE REASON OF NEW PROPOSAL

➤ POINTS THAT WE PROPOSE REVISION & PROPOSALS

- ❖ COMBINING THE IDENTIFICATION & EXPLOITATION PHASES
- ❖ RESCALING & REGRADING THE FACTORS
- ❖ FINAL ATTACK POTENTIAL & VULNERABILITY DEGREE

CALCULATION TABLES AND EXAMPLES

➤ CONCLUSION

PROPOSED ATTACK POTENTIAL CALCULATION METHOD SUMMARY



Time	Expertise	TOE Knowledge	Access to TOE	Equipment	Open Sample
<1 day / 0	Layman / 0	Public / 0	< 10 / 0	None / 0	Public / 0
<1 week / 1	Proficient / 3	Restricted / 2	< 20 / 2	Standard / 3	Restricted / 2
<2 weeks / 2	Expert / 6	Sensitive / 4	< 40 / 3	Specialized / 7	Sensitive / 4
<1 month / 4	Multiple Expert / 8	Critical / 6	< 50 / 5	Bespoke / 11	Critical / 6
<2 months / 7		Very Critical HW Design / 9	< 100 / 9	Multiple Bespoke / 15	
<3 months / 10			> 100 / 11		
<4 months / 13					
<5 months / 15					
<6 months / 17					
>6 months / 19					

EFFECT OF THE PROPOSED METHOD ON THE VULNERABILITY ASSESSMENT RATING

Values Resulting from the current method	Values Resulting from the proposed method	Attack potential required to exploit scenario:	Meets assurance components:	Failure of components:
0-15	0-9	BASIC	-	AVA_VAN.2,3,4,5
16-20	10-13	ENHANCED-BASIC	AVA_VAN.1, 2	AVA_VAN.3,4,5
21-24	14-19	MODERATE	AVA_VAN.1,2,3	AVA_VAN.4,5
24-30	20-24	HIGH	AVA_VAN.1,2,3,4	AVA_VAN.5
=>31	=>25	BEYOND HIGH	AVA_VAN.1,2,3,4,5	-

✓THE SAME AS THE CEM3.1

EXAMPLES COMPARING THE TWO METHODS: PROBING A BUS



FACTOR	IDENTIFICATION		EXPLOITATION		ALTERNATIVE	
Elapsed Time	<1 month	/ 3	<1 week	/ 4	<1 month	/ 4
Expertise	Expert	/ 5	Proficient	/ 2	Expert	/ 6
Knowledge of TOE	Restricted	/ 2	Public	/ 0	Restricted	/ 2
O. S./ K. K	NA	/ 0	NA	/ 0	NA	/ 0
Access to TOE	<10 samples	/ 0	<10samples	/ 0	<10 samples	/ 0
Equipment	Specialized	/ 3	Specialized	/ 4	Specialized	/ 7
Points Sub Total		13		10		19
Total	23 MODERATE(21-24)			19 MODERATE(13-19)		

EXAMPLES COMPARING THE TWO METHODS: HIGHER ORDER DPA



FACTOR	IDENTIFICATION		EXPLOITATION		ALTERNATIVE	
Elapsed Time	< 1 month	/3	< 1 month	/6	< 1 month	/4
Expertise	Expert	/5	Proficient	/2	Expert	/6
Knowledge of TOE	Sensitive	/4	Public	/0	Sensitive	/4
Access to TOE	< 10 Samples	/0	<10Samples	/0	<10 Samples	/0
Open Sample / Known Key	Sensitive	/4	NA		Sensitive	/4
Equipment	Specialized	/3	Specialized	/4	Specialized	/7
Points Sub Total		19		12		25
Total	31 BEYOND HIGH(>=31)			25 BEYOND HIGH(>=25)		

➤ INTRODUCTION

- ❖ THE CURRENT ATTACK CALCULATION METHOD FOR SMARTCARDS
- ❖ THE REASON OF NEW PROPOSAL

➤ POINTS THAT WE PROPOSE REVISION & PROPOSALS

- ❖ COMBINING THE IDENTIFICATION & EXPLOITATION PHASES
- ❖ RESCALING & REGRADING THE FACTORS
- ❖ FINAL ATTACK & VULNERABILITY DEGREE CALCULATION TABLES
AND EXAMPLES

➤ CONCLUSION

- PROBLEMS OF THE CURRENT ATTACK POTENTIAL CALCULATION FOR SMARTCARDS ARE INTRODUCED AS:
 - DIFFICULTY AND SUBJECTIVITY OF ATTACK CALCULATION WHEN TWO DISTINCT PHASES “**IDENTIFICATION**” & “**EXPLOITATION**” ARE PRESENT
 - DEFFICIENCY IN THE SCALING OF “**ELAPSED TIME**” AND “**TOE NUMBER**”

- PROPOSED METHOD AGAINST THESE PROBLEMS
 - **COMBINING** THE IDENTIFICATION & EXPLOITATION PHASES
 - **RESCALING & REGRADING** FACTORS

✓ DECREASED COMPLEXITY &
DIFFICULTY

✓ DECREASED SUBJECTIVITY

✓ INCREASED RESOLUTION IN GRADING

✓ THE SAME VULNERABILITY RATINGS

THANK YOU FOR ATTENTION!

QUESTIONS ?