





# HUMAN FACTORS IN HRE An Interdisciplinary Approach to Hardware Security

René Walendy, Steffen Becker



Gefördert durch DFG Deutsche Forschungsgemeinschaf

#### HARRIS 2023, 25.01.2023





# **INTERDISCIPLINARY RESEARCH TEAM**

#### **Psychology Squad**



#### Security Squad







Institut für Erziehungswissenschaft Ruhr-Universität Bochum















High-Level

Description

### **HUMANS DRIVE HRE**

**Research Gap:** Human factors influencing HRE success remain poorly understood





#### HUMAN FACTORS RESEARCH IN RE



Votipka et al. "An Observational Investigation of Reverse Engineers' Processes." USENIX Security Symposium (2019).





Mantovani et al. "RE-Mind: a First Look Inside the Mind of a Reverse Engineer." USENIX Security Symposium (2022).



"Reverse engineering of Boolean functions = a special kind of problem solving"

Lee & Johnson-Laird "A theory of reverse engineering and its application to Boolean systems" Journal of Cognitive Psychology (2013).

## **PROBLEM SOLVING IN HRE**



Problem solving = essential cognitive ability and key competence that enables persons to solve (complex) situations

Funke et al., 2018





### **INITIAL WORK: A "COGNITIVE VIEW" OF HRE**





### **RESEARCH ENVIRONMENT: HAL**





3-month HRE course Practical HRE task in the open hardware analyzer "HAL"

Table 1. Excerpt from the Pre-processed Log File of Participant 8 Showing 6 of 153 Total Events

Timestamp	Type	Attribute	Component ID or File Name
3,822 s	Script	Working	003822_Participant8.py
3,856 s	Manual	Gate	514
4,240 s	Script	Erroneous	004240_Participant8.py
4,268 s	Script	Working	004268_Participant8.py
4,334 s	Manual	Gate	531
4,341 s	Manual	Net	2,437

Behavioral log files and executed scripts

# **SELECTED RESULTS (COGNITIVE FACTORS)**



Disclaimer: only descriptive analysis; further research needed!

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



# FROM QUALITATIVE TO QUANTITATIVE





#### HRE SIMULATION: REVERSING GAME





# HRE SIMULATION: COGNITIVE FACTORS



Performance in HRE Simulation Task

- Observations corroborate findings from the prior study
- Test bed for future cognitive factors research



# **Challenges and Opportunities** for practical applications and further research



#### **"OFFENSIVE" SECURITY**





# **DEFENSIVE SECURITY**

- Current obfuscation: based on algorithmic complexity
- What if we add a **cognitive complexity** component?
- **Cognitive obfuscation:** protecting intellectual property by impeding human sensemaking



Thanks @ Max Hoffmann



Source: www.constructionknowledge.net



# **WE WANT YOUR INPUT!**

We're interested in ...

- ... exchange of ideas with experts
- ... volunteers for our studies
- ... the relevance of hardware obfuscation (and, on the other side of the same coin, hardware Trojans) for the industry
- ... real-world **netlists & problem settings**

P	ractical						-	-	
I. How would us	inter rele	vance o	of hard	Non-					
relevant) to 5 (very rel	e the practical re	ol.	- All	ware re	everse	engine			
Eail	(vani);	caesance o	f the folio	wine		8-46	ering		
Patture analysis				-8 (CI)	rrse eng	incering o	nde e		
Detecting IP violations	Gunni		-	_		0.0	saly from	ton) I	
Extension France Transmission	is an entronal blog	cks, count	web to a				1 2	3.	
Dotal a Dotal	OM Supply d	ain verifi	cation ICs	9			0 0	0 0	5
Idantia Idantia	or Flash m	emory co	ninom ninom				0 0	0 0	0
High L	al un'	ces (trans	intents			(	00	200	
Account of understanding	of in the of areas	of interes	sours, cor	stacts, etc	)	0	0 0	0 0	
Red to:	individual cir	cuit block				0	0 0	0 0	
Circuit	ou) a netlist fro	an an Asi	or the e	ntire desi	1771	0	0 0	0 0	
Obrol.			or FPC	A		0	0 0	0 0	
Collegence management						0	0 0	0 0	
Other (please specific-						0 0	0 0	0 0	
2. How we have						0 0	0	0	
I (not relevant) to a rate the process	had a					0 0	0 0	0	
	cal relevance of	Protect				0 0	- 0	0	
Unauthorized own			g ICs agai	nst the fe	n		0 0	0	
Netlist recovery 1	the for				Sound	attack som			
The second se	and the second se						arios 6		
Competitive analysis	r purposes of					1 .	larios fros	n	
Competitive analysis Invasive attacks apol-	r purposes of pl	agiarism		_	_	1 2	arios fron	n 5	
Competitive analysis Invasive attacks seeking to compro Other (please at	r purposes of planise securi	agiarism				1 2	arios fron	n 5	
Competitive analysis Invasive attacks seeking to comprov Other (please specify):	r purposes of plantice security	agiarism			0	1 2	arios fron	5	
Competitive analysis Invasive attacks seeking to comprod Other (please specify): 3. How common do specify	r purposes of plantice security	agiarism			0	1 2 0 0 0 0 0 0 0	arios fron	n 5	
Competitive analysis Invasive attacks seeking to comprov Other (please specify): 3. How <b>common</b> do you think the follo from 1 (very rare) to 5 freez.	r purposes of pla nise security	agiarism			000		arios fron	5	
Competitive analysis Invasive attacks seeking to comprov Other (please specify): 3. How common do you think the follo from 1 (very rare) to 5 (very common)? Analysis et	r purposes of pla nise security wing starting po	agiarism xints are in	n a har'		0		arios front 3 4 0 0 0 0 0 0 0 0 0 0	n 5	
Competitive analysis Invasive attacks seeking to compro- Other (please specify: 3. How common do you think the follo from 1 (very rare) to 5 (very common)? Analysis of an unknown As(r	r purposes of pl nise security wing starting pe	agiarism Dints are in	n a hardw	are reven			arios fron 3 4 0 0 0 0 0 0 0 0 0 0 0 0	n 5	
Competitive analysis Competitive analysis Invasive attacks seeking to compro- Uner (please specify): 3. How common do you think the follo from 1 (very seel) to 5 (very common)? Analysis of an unknown ASIC Analysis of an ASIC with available sci Information with a science with available sci	r purposes of pl nise security wing starting pc	agiarism Dints are in	n a hardu	ate reven	0 0 0 ee engin	1 2 0 0 0 0 0 0 0 0 0 0 0 0 0	arios front 3 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n 5	
Competitive analysis Competitive analysis Invasive attacks reeking to compro- Other (please specify: 3. How compared do you think the fold from 1 (very rare) to 5 (very composi- field of the standard of the standard from 1 (very rare) to 5 (very composi- tion 1 (very rare) to 5 (very composi- tion 1 (very rare) to 5 (very composi- tion 1 (very rare) to 5 (very rare) from 2 (very rare) to 5 (very rare) from 2 (very rare) to 5 (very rare) formation about the standard for the standard information about the standard for the standard for the standard information about the standard for the standard for the standard for the standard information about the standard for	is purposes of plu mise security wing starting pc	agiarism xints are is	n a hardu	ate reven	O O O ie engin i	1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	arios front 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n 5	
Compression analysis Compression analysis Compression and the second second second Compression and the second second second second Compression and the second second second second from a rever rese to second second second second compression and the second second second second compression and second	is purposes of plu mise security wing starting po loper) document is built into	agiarism pints are is station, an	n a hardw d/or	ste teven		1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	arrises from 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n 5	$\left  \right $
Competitive analysis Imative analysis Imative analysis and the second second Other pieces specify. A there commends and the second second factors report to device second second Analysis of an unknown ASIC Analysis of a analysis of a analysis and Analysis of a analysis of a analysis and Analysis of a analysis of a analysis and Analysis of a analysis and Analysis of a analysis and Analysis of a analysis of a analysis and Analysis of a analysis of a analysis and Analysis of a analysis and Analysis of a analysis of a analysis of a analysis and Analysis of a analysis of a analysis of a analysis of a analysis and Analysis of a analysis of a analysi	nine soundry r purposes of pl nise security wing starting pc doper) document is built into orm an ASIC or	agiarism pints are is station, an	n ə hərdu d/or	ste reven		1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	arios fros 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n 5	$\left  \right $
Competitive analysis Competitive analysis Invaries exacts seeking to compose Other (please previd): 1. Other (please previd): 1	nise security nise security wing starting po doper) documen is built into om an ASIC or om an ASIC or	agiarism xints are is station, an FPGA	n a hardn d/or	ale reven		1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	arlies free 3 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n 5	$\left  \right $
Competitive analysis Competitive analysis Transfer and the seeking to compose the problem of the seeking to the seeking of the problem of the seeking the seeking the Analysis of an unknown AGC Analysis of an unknown AGC Analysis of an unknown and acc Analysis of a seeking account of Analysis of a seeking account	in numbers in purposes of plu- mise security wring starting po- loper) document is built into orm an ASIC or orm an ASIC or orm an design files	agiarism xints are is station, an FPGA	n æ hærdn d/or	ate reven		1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	arrises from 3 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n 5	$\left  \right $
Comparison with a stude part of a finded part of a Comparison of the stude of the	in soundry r purposes of pl mise security wing starting pc loper) documen is built into is built into onn an ASIC or an design files bin	agiarism xints are is station, an FPGA	n æ hærdø d/or	are reven		1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	arlies free 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n 5	
Comparing on the Atom Resolution Comparing on the Atom Resolution of the Instance and the atom Resolution of the Other Determined on the Atom Resolution Determined on the Atom Resolution of the Atom Resolution of the Atom Resolution of the Atom Resolutio	Animatry in purposes of pla mise security wring starting pe wring starting pe wring starting pe wring starting pe shoper) document is built into orm an ASIC or orm an ASIC or or or orm an ASIC or or orm an ASIC or o	agiarism xints are is station, an FPGA	n æ hardø d/or			1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 eering proj 2 3 4 0 0 0 0 0 0 0 0 0 0 0 0	arrises free 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n 5	
Comparing with the second seco	anindry it purposes of pl mise security wring starting pc wring starting pc wring starting pc security of per decument is built into orm an ASIC or an ASIC or an an a	agiarism aints are in station, an FPGA non	n a hardn d/or	ste teven		1 2 0	arrises free 3 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n 5	
Comparing on the state of the s	* namety * purposes of pl mise security wing starting po wing starting po to be pl to be p	agiarism pints are is station, an FPGA non O	n a hardn d/or	are reven	( 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	1 2 0	arrises free 3 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n 5	
Comparing and the state of the	in valindry it purposes of pla raise security wring starting pe wring starting pe is koult into orn an ASIC or orn an ASIC or or orn an ASIC or orn an ASIC orn	agiarism pints are is plation, an plation, an plation, an o o o	n a hardn d/or e ≤3	21c reven		1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	arrises free 3 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	71	
Comparing on the stand of the stand Comparing on the stand of the stan	- vandaty - purposes of pla - purposes of pla	agiarism sints are is station, an FPGA non O O	e s3	are reven		1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	3     4     0     c       0     0     0     0     0       0     0     0     0     0       0     0     0     0     0       0     0     0     0     0       0     0     0     0     0       0     0     0     0     0       0     0     0     0     0       0     0     0     0     0	n 5	
Compared with the sector of the stand and the sector of th	Anadry anadry i purposes of plat purposes of plat proposes of plat purposes of plat plat plat plat plat plat plat plat	agiarism pints are in station, an FPGA 0 0 0	n a hardu d/or 0 0	are reven	0 0 0 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0	1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	and a second sec	n 5	
Comparing on the stand and one of the stand and one of the stand and and and and and and and and and	- validaty in purposes of pla purposes of pla purposes of pla mise security wring starting pc wring starting pc wring starting pc starting pc starting pc starting pc starting pc start	aggiarism nints are is station, an FPGA 0 0 0	c ±33 O O O	ate reven		1 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	3 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n 5	
Comparison of the analysis of	n namdry promoses of ph promoses of ph nnise security wing starting pe depend accurate the bault into the bault into t	agisrism and agisrism and a set in an and a set in an an a	e = 33 0 0 0	ate reven		1     2       0     0	3 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n 5	
	- nondry in purposes of pl purposes of pl prime security wing starting pc wing starting pc wing starting pc is built into orn an ASIC orn an ASIC o	Agéiarisan aints are in suints	e ±3 0 0 0 0 0 0 0 0 0 0	are reven	1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	2 2 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	arlos frod 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n 5	
Comparison of the state of the	Vandry Purposes of ph Purposes of ph wing starting ph wing sta	Agéisrisan Jointes are is Agéisrisan Attation, an Antation, an Antatio	e s3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		( ( 0	1     2       0     0     0	starlos frod     for     for <t< td=""><td>n 5</td><td></td></t<>	n 5	



RUHR

**UNIVERSITÄT** BOCHUM



CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

# **THANK YOU** For your attention!

RUB

Please contact us: Steffen.Becker@rub.de and Rene.Walendy@rub.de

Gefördert durch DFG Deutsche Forschungsgemeinscha



HG HORST INSTITUT