## avatar<sup>2</sup>

Marius Muench

34c3 - December 29, 2017



- 1. Binary firmware analysis
- 2. Tooling landscape
- 3. The  $avatar^2$  framework
- 4. Examples
- 5. Conclusion

#### **Binary Firmware Analysis**

- Amount of embedded devices steadily increasing
- Misconfigurations, bugs, and vulnerabilities are common
- A lot of reported vulnerabilities are "low-hanging fruits"
- Discovery of more complex bugs benefits from sophisticated tooling

- Variety of platforms
  - Memory layout
  - Peripherals
- Often no OS-level abstractions
- Many devices use monolithic firmware
- Hardware interactions are embedded in firmware code
  - Memory Mapped I/O
  - Interrupts
- Variety of architectures

(approximate ) of	and an index of the second	444.000	Pastar	Cade 1 ID. 1991	Trated NP3 6 NP3	Anhorson
March 1	0040	1000	Passer Passer	Last and Me	1000.0010.000	
	0004		International Activity Control	No.	120.1177	
and the second					5.11 (MR) (MV)	
	ANRALI	44610	Trapient NK (MA), protect and the name Antheorem Destroyed to the Antheorem	No. 101614	1.000 (0.100)	
AREAS .	ANRALI	14.00	And a stage and a stage and a	100.000	12165.025.000	
		1583	APAR to but support 10 bits in memory plate the guardy must be 10 bits. Memory and an apart and a support	Net	121005 (312100	
	10000	AAMEE	6/6983 obtained opcomed buckle MUE fasthagenet unit	105.056	10.001.0.01.002	
		ARREST	A MIRE of a second to r	(Bude	11101.01100	
		44.07.110		liteda	0.00	-
4		AARTIN	AL APPROX PROX PROV PROV PROV PROV PROV PROV PROV PROV	10.000	41184	
AREA.	10580				41004	
4		1897314	6x(001)	118 celos	DALOWUP/	
		0.00 334 10	End aparticities Toronto, URDed First Endowing to URD End and include	lare .	11 MPL 0 18 8 MA	
	45541	1007317		11210104.000	14107-0-0190	
		10001017	ALANE 1984 (1984)	# ER united, Weisels With the Carlos Sales and Sales	10 MPL 0 10 4 Mp.	
		1000.017	0.000 TM (stre			
-	10100.00	and the second s		Bala		
and the local division of the local division	107584	10000	5-dayspace additional prototo, textman and to any constraints of the second	113 Fai, 891	11/05/07 U MO	801
		000.000	5 starssifte Note	No.	11104104	
	44847	1000211	A 1659-158, 029	14 KE/14 KE/MC/AD /CLE PAL Color Table Extension	2001001.00.0000	
Tangan	100411 -	1008117	As LEASTING (set or	112/128.004		
		1000101	Au 1.000 Yest, autors	4.100/14.108,00FU		
			Turne, whereast third residues, other	Variable, Eg/El/cougreet memorie, MPE		
	UPINA W		Runs, advantations	Read of Kills		
-			0.009488.4	Brial A TA		
	10004-01		Tack path 10%, while and 10% of a set o	Veralle Vill, MA	111/00/01/02/00	
			Calabacy instant as Addition 1 E deparation 5 with an and 00 PPA addition (7/6)	No. 647 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)		
4000.00	10040.3	448.000	transporter	10.00/10.000		
	citizen bu	4440.010004	Konte balance (Bandrood and Calendrood and Calendro	Victor March 199		
	0044	AAMUTHEESS	E dispersive INE, New Address INE, New Address INF, Addre	Velation	141-0-112-445 (Mil-1-0023 Tel), 410-123 (Mil-	-
	10103-0			Value MV		
				Caluate Wei + Publishe	HIS SHEEP IN THE READ AND SHEEP AND ANY PROPERTY.	
	LOBAL C	0001000a4	A CONTRACT OF A	Vellex.MU		
beaution -	14841				1.1.100.000	
Reariage .	1004.01	903399			10.08546	
	0.000 8	Laboration .	Received and to the Party State APP and an end of the second well as the analysis of the second second	Inclusion of Without With	14100000	
	10004	Caladevid	Response profiles and france in provide the second and the provided and a second approximately and the second approximately and the second approximately app	Operation of Distance Plant English	131049340	
two at			Bernah dar profile met Tanda Landa Landa (2014) and write spinodowill, it give anti-117 danage datapartie spinodowill, it give anti-117 danage datapartie spinodowill, it give anti-117 danage datapartie spinodowill, it give anti-117 datapartie spinodowill, it give anti-117 datapartie spinodowill, it give anti-117 dataparties spinodowill, it give anti-117 datapartie	Charlow and a chorage of the Charles	110 1001 0 111 00.01 114 1001.00 001.00 001.00 001	
Factors III	ARX8.7 11		Microart sets profile, Yurnik (Yurnik ), Aaksemmul pily and alsemmul pily and alsemmul values, spheral ki kanding memory	Optional California (California) (Physical and Physical & Oppions)	121005050	
	-		Worksenholder prefek Tecnel / Storie J / Storie J / Storie president PRU hasheem in Starkeem in	Optimization of TOC get and PECkill & regions	1.11-04PUPG (1.17 MPG)	
				n de la construction de la construction de la construction de la construcción de	111/08/1984	
			Participation for the second s	D 46 KR II 46 KR D 4 KR D 4 KR D 4 KR RA 100 KR 10		
Carbon R	100.70		Relationship the Second 2004 approximation (Second and Advances) and a photo and and a second according to a photo and a second according to a photo and a second according to a photo according to accor	THE REPORT OF THE DRIVE THE THE THE ADDRESS OF THE ADDRESS OF THE		
		(a) = 10				
		Callenge of the	NAMES AND ADDRESS OF ADDRESS OF ADDRESS AND ADDRESS ADDR	C REAL PROPERTY AND A DESCRIPTION OF THE	LAT DEPARTMENT OF	
		Carlon La Pill	Autor of the Physic Pure 2 (10) (10) (10) (10) (10) (10) (10) (10)	IF THE REPORT OF CONTRACT OF A MADE IN THE PARTY OF THE PARTY	LA CARGING LA CAR	
			Application profile APR/Tecnel (Tecnel / APPL/TECNED Depth (Tecnel APPL))	14-32 09/14-32 0931.0-13832 oct.022/MU+TedDox	Tal 143300 (3.8 SWID/Work good Fan ADD MoCragond a That 3 SHD	
Continue de	ARMAY A.		Application profile AMP Particle CPUM Particle CPUM Provide CPUM Provide CPUM Provide CPUM Participan (CPUM	THE R.R. MILLION CO., N. MILLION, M. MILLION, MI	A REMARK SHOW AND ADDRESS OF A DAMAGE AND ADDRESS AND ADDRESS ADDR	
(10.0.000)			Applicate profile (RMV Technik DEDPVTML RD NB Dechestrament updates, und element seculations accupations, 1-4 DM and, Expert pola Mathematication accupation, 2003, analy antimized in 100, approximation accupation (RD), and accupation accupati		12 OMSING pricer	
			Applicate profile MR Flower Flowed (2004) REV MRW INSTANCE CONFIDENCE AND ADDRESS ADDR	12 KK spectry 12 KK selection, 5 of WE (3, 0) have 12, MM in Twelfare At 18 kL (20, 18 of 18 kL (20, 18 kL))	Ar lead 1.5 CMPURS per centry for 0.1 CMPURS depending at implementation (14	
	10044		Explana park AN Turk (Turk (TURY We We Web) to park (Turk park (Turk to park to park (Turk to park (Turk to park (Turk to park (Turk to park	A FEEL AND REAL AND R	1.0 1005,000	
	LADIA A.		Exploring units Aut / 41.1 - 1.4 Winners, Verball will be advanced 1018, VMA. An external relation for the profession Agenting units function and advanced 1.4 Winners, Verball and WMA Languagement (advance), relating units and are profession	8.44 KK reptond party (F44 KK reprint at CCL) preserved 20 KB - 1 Mich reptond FCC-band B-44 KK repetitive R-44 KK repton preserved at 100 KK - 1 Mich diamet, 40 Mich physical at income.	1.11.1985.054	
			Application profile statistic part Application in the Control	E-64 KE AGARTU S AN	111040346	
	ARMA A.		Approach priority access to a constraint of the second second access to the second access to the second second access to the second access to the second second access to the second acces	The second	11.11.000.000	
Contract A			Application prefix devices and a devices of a second se	18 18 w/01 party 11 18 w/17 11 par one 111 18 4 18 14 shared w/17, 11 bit physical anti-mos	A 7 1987-184 a	
100.000			Application profile double 22 and Accelerat, 1 all Differente, Ecclarera Michaelmannia (UM), VPAC, A and and Acceleration double, 2 may spectrate	10.10, 10 YO MILLING ON AND AND A MILLING AND A VALUE AND A	6.8 2005,00 gml	
			Applications and in Control 20 and Advanded 2.5 of COMParing Transformed 1000, VPM-2, and some introductions, in polymology in advanced 1	64 / M L M LD, T M LM LD per select CML D dramer		
			Application profile and AA-VALL ( II THE WAVE AVAILABLE	Bit (Marsheld, Bit Brite), Bit Brite of part serve, Britley at an an		
Announds a	multiplications PPI	464 8578	Pashar	Cashe (110), NMU	Typical rank girling	Antonnan

https://en.wikipedia.org/wiki/List\_of\_ARM\_microarchitectures#Designed\_by\_ARM

- Instrumentation
- Emulation
- Fault detection
- Interrupt handling
- Microarchitecture dependent instructions

**Tool**ing Landscape

- A lot of binary analysis tools for desktop software
- Way less for embedded devices software
  - Especially when considering open source tools
- Often, challenges for embedded devices exceed capabilities of static analysis tools
  - Assumuption about environment may not hold true
  - Difficult to infer peripheral behaviour and interrupts

- Based on KLEE
- Targets MSP430 firmware
- Symbolic Execution
- Uses explicit analysis, memory and interrupt specifications

Davidson, Drew, et al. "FIE on Firmware: Finding Vulnerabilities in Embedded Systems Using Symbolic Execution." USENIX Security Symposium 2013.

- Based on KLEE
- Targets MSP430 firmware
- Symbolic Execution
- Uses explicit analysis, memory and interrupt specifications
- Requires source code of firmware

Davidson, Drew, et al. "FIE on Firmware: Finding Vulnerabilities in Embedded Systems Using Symbolic Execution." USENIX Security Symposium 2013.

- Based on Qemu
- Targets ARM & MIPS firmware
- Instrumented Linux kernel
- Automated analysis of web pages and SNMP implementations
- Automated testing with known exploits

Chen, Daming D., et al. "Towards Automated Dynamic Analysis for Linux-based Embedded Firmware." NDSS 2016.

- Based on Qemu
- Targets ARM & MIPS firmware
- Instrumented Linux kernel
- Automated analysis of web pages and SNMP implementations
- Automated testing with known exploits
- Works only for Linux based firmware with no too specific kernel modules

Chen, Daming D., et al. "Towards Automated Dynamic Analysis for Linux-based Embedded Firmware." NDSS 2016.

- Based on instrumented QEMU
- Work in progress
- Example targets BCM4358 firmware
- Prototyping of Boards with LUA
- Instrumentation capabilities

https://github.com/Comsecuris/luaqemu

- Based on instrumented QEMU
- Work in progress
- Example targets BCM4358 firmware
- Prototyping of Boards with LUA
- Instrumentation capabilities
- Requires a significant amount of modeling and trial & error

https://github.com/Comsecuris/luaqemu

#### Avatar

- Based on S<sup>2</sup>E (QEMU+KLEE) and OpenOCD/GDB
- Targets ARM firmware
- Partial emulation together with real hardware
- I/O forwarding
- Orchestration
- Symbolic Execution

Zaddach, Jonas, et al. "AVATAR: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares." NDSS 2014.

#### Avatar

- Based on S<sup>2</sup>E (QEMU+KLEE) and OpenOCD/GDB
- Targets ARM firmware
- Partial emulation together with real hardware
- I/O forwarding
- Orchestration
- Symbolic Execution
- Heavily tied to the S<sup>2</sup>E infrastructure
- Requires the presence of the physical device

Zaddach, Jonas, et al. "AVATAR: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares." NDSS 2014.

- A lot of focus on ARM
- QEMU's emulation capabilities are a common building block
- Frameworks are heavily bound to underlying components

### The avatar<sup>2</sup> framework

- Dynamic Multi-Target Orchestration and Instrumentation Framework
- Focus on firmware analysis
- Python based framework
- Re-designed and re-implemented from scratch
- Open source: https://github.com/avatartwo
  - Research project
  - Released in June 2017

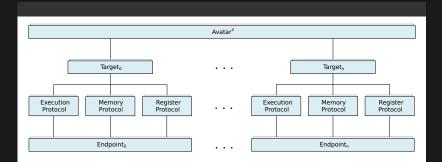
- Developed by the Software and System Security Group at Eurecom
- Specifically:
  - Marius Muench
  - Dario Nisi
  - Aurélien Francillon
  - Davide Balzarotti

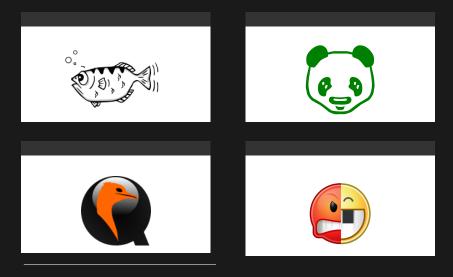
- Target orchestration
  - Abstraction of debuggers, emulators and other frameworks
  - Easy addition of new targets
- Separation of execution and memory
  - Enables I/O forwarding/remote memory
- State transfer and synchronization
  - Don't keep the state of analysed software local to single targets

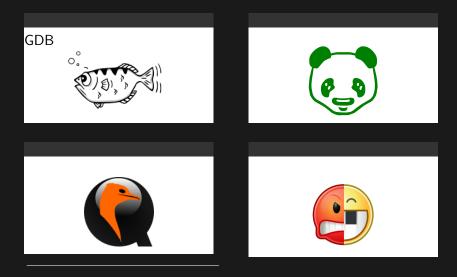
#### avatar<sup>2</sup>- components

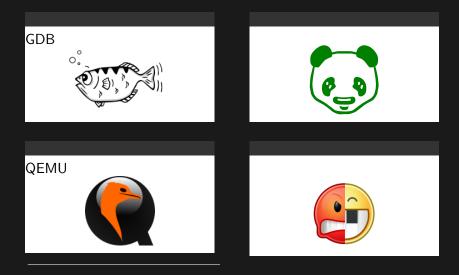
- avatar<sup>2</sup> core
- Targets
- Endpoints
- Protocols

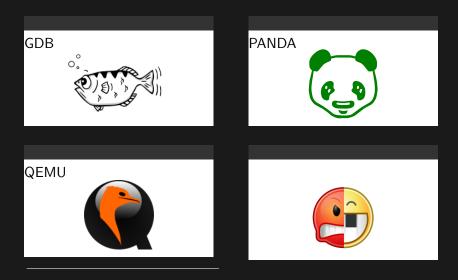
#### avatar<sup>2</sup>- architecture overview

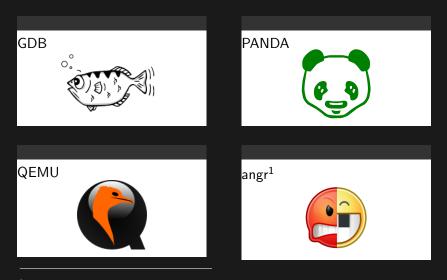












<sup>1</sup>Still under development

Avatar<sup>2</sup> provides a costomized QEMU

- All located in a single subfolder: hw/avatar
- New board: Configurable Machine
  - Already present in the first avatar
  - Allows flexible configuration of emulated hardware
- New peripheral: avatar-peripheral
  - Communicates with avatar<sup>2</sup> via posix message queues
  - Utilizes custom remote-memory protocol

- Architecture independent design
- Internal memory layout representation
- Legacy python support
- Peripheral modeling
- Plugin System
  - Assembler/Disassembler
  - Orchestrator
  - Instruction Forwarder

## Examples

An avatar<sup>2</sup> scripts needs to:

- 1. Create the Avatar-object
- 2. Define a set of targets
- 3. Optionally define memory layout
- 4. Specify an execution plan

## Demo

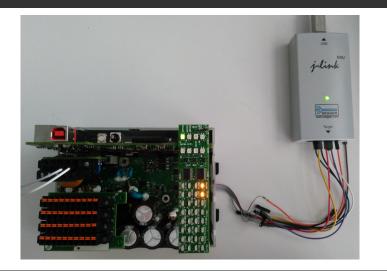
- Let's move on to a real target!
- Proof of concept implementation of HARVEY<sup>2</sup>
  - Malware for a COTS PLC
  - The plc utilizes multiple boards
  - Code injection via JTAG

<sup>&</sup>lt;sup>2</sup>Garcia, Luis, et al. "Hey, My Malware Knows Physics Attacking PLCs with Physical Model Aware Rootkit." NDSS 2016.

#### **Binary Instrumentation**

# (Fragile) Demo

### Demo backup ;)



- Part of WYCINWYC<sup>3</sup>
  - Joint work with SIEMENS
- Investigates challenges specific to fuzz testing embedded devices
  - Fault detection
  - Instrumentation
  - Scalability
- Evaluates different strategies to aid fuzz-testing
  - $\bullet\,$  Uses avatar^2 for partial and full emulation of the firmware

<sup>&</sup>lt;sup>3</sup>Muench, Marius, et.al. "What you corrupt is not what you crash: Challenges in Fuzzing Embedded Devices" To be presented at NDSS 2018

#### The setup

- Two Targets
  - STM32I152re
  - PANDA
- Target Software
  - expat, a popular XML-parser
  - Artificially inserted vulnerabilities
- Orchestration
  - Board initilization on physical device
  - Emulation of main-loop inside PANDA
- Analysis
  - 5 PANDA plugins to detect different types of vulnerabilities
  - Mimicry of existing techniques for desktop software
  - Doesn't require modification of the firmware

### **Evaluation**

- 100 Fuzzing sessions in different setups
  - Native
  - Partial emulation with I/O forwarding
  - Partial emulation with avatar<sup>2</sup>-peripherals
  - Full emulation
- Plugins could detect previously undetected faults
- Full emulation provided better performance than native fuzzing
- More details in the paper: http://s3.eurecom.fr/docs/ndss18\_muench.pdf

- Dynamic binary analysis of firmware requires often the device
- PANDA allows to record and replay execution
- Allows exchange of executions fur further analysis without the device

# Demo

- Firefox with inserted bug
  - Executed concretely inside gdb until function of interest
  - Analysis of only one thread
- Automated memory layout extraction from gdb
- Transfer of layout into angr
- Copy-On-Read
- Symbolic function arguments

Preliminary Results:

- Approximatly 10 minutes of runtime
- 36 executed basic blocks
- 21 uniquely accessed pages
- Found the bug

- 5 Examples:
  - Dynamic Instrumentation of GDB
  - Dynamic Instrumentation of a plc
  - Fault Detection with an development board and PANDA
  - Record and Replay with an development board and PANDA
  - Symbolic Execution with firefox and gdb

## Conclusion

- Dynamic firmware analysis is still a challenging topic
- Avatar<sup>2</sup> aims to tackle some of the challenges
- Multi-target orchestration is not limited to firmware

- Move main development to github
- Introduce proper versioning
- More, exciting targets

Get in touch with us:

- #avatar2@freenode
- avatar2@lists.eurecom.fr
- Talk to me

We may be looking for people to join our group in the near future

- S3@Eurecom
- jzaddach
- Subwire & domenukk
- Zardus & ccm
- Tasteless

### Thank you!