GARUDA 2.0

Sage Sefton
ss557415@ohio.edu
Ohio University

Avinash Karanth
karanth@ohio.edu
Ohio University

2020
Fall

1 Background

GARUDA was a system that operated on a two stream model of the "user" or program, and that which executed the instructions. GARUDA 2.0, we extend, or refine based on the point of view, this model to operate between the Execution (EXE) and Memory (MEM) stages of the pipeline. We assume a monitor theory shown by the graphic Fig **??**. The monitor appears to operate on a single stream, but the two hanging connections can be considered the two streams of the former model.

The most obvious change we need to make is to enable encryption and decryption of the EffAddr. Our attack vector focuses on a trojan targeting the state register between the EXE and MEM stages. They could cache these addresses and try to access that memory later, or they may try to use them as a side channel. Either way, allowing an adversary to track our memory accesses is clearly problematic. However, when we refer to "encryption", we really mean some reversible obfuscation function. We employ the proof assistant, Coq, to prove the EN and DE blocks are exact inverses. GARUDA is written in Coq for exactly this reason, so requiring a proof that $\forall P, DE(ENP) = P$ should be sufficient.

2 The Implementation of GARUDA 2.0

2.1 Syntax

2.1.1 Definitions

EXE Input Fields	f_{Ei}	::=	$f_{Ei_1} \mid \cdots \mid f_{Ei_k}$
State Reg Fields	f_{SR}	::=	$f_{SR_1} \mid \cdots \mid f_{SR_k}$
MEM Input Fields	f_{Mi}	::=	$f_{Mi_1} \mid \cdots \mid f_{Mi_k}$
Fields	f	::=	$f_{Ei} \mid f_{SR} \mid f_{Mi}$
Obfuscated Field	$f^{\mathbf{o}}$	::=	f
Inputs	i	::=	$\{f_{i_1} = v_{i_1}, \ \ldots \ , \ f_{i_k} = v_{i_k}\}$
Outputs	o	::=	$\{f_{o_1} = v_{o_1}, \ \ldots \ , \ f_{o_k} = v_{o_k}\}$
Obfuscation Fxn	Φ	::=	$f \to f^{\mathbf{o}} \mid f^{\mathbf{o}} \to f$

2.1.2 Syntax of Predicates

Predicates	a, b	$::=$	0	*False*
		$\mid$	1	*Identity*
		$\mid$	$f = n$	*Test*
		$\mid$	$a + b$	*Sum*
		$\mid$	$a \cdot b$	*Product*
		$\mid$	$\neg\ a$	*Negation*
Policies	p, q	$::=$	$\mathbf{test}(a)$	*Test*
		$\mid$	$(\Phi_{Encrypt}, \Phi_{Decrypt})$	*Obfuscation*
		$\mid$	inj_{SR}	*Injection to State Register*
		$\mid$	inj_{Mi}	*Injection to Memory Unit*
		$\mid$	$f \leftarrow n$	*Update*
		$\mid$	$p + q$	*Choice*
		$\mid$	$p \cdot q$	*Sequential Concatenation*

2.2 Semantics

2.2.1 Semantics of Predicates

$$
\begin{aligned}
[\![\cdot]\!] \ : \ & \mathbf{Stream}(E) \times \mathbf{Stream}(M) \to \\
& P(\mathbf{Stream}(E)) \times P(\mathbf{Stream}(M)) \\
[\![0]\!](-,-) &\triangleq (\varnothing, \varnothing) \\
[\![1]\!](es, ms) &\triangleq (\{es\}, \{ms\}) \\
[\![f = n]\!](es, ms) &\triangleq (\mathsf{filter}\ (f = n)\ \{es\},\ \mathsf{filter}\ (f = n)\ \{ms\}) \\
[\![a + b]\!](es, ms) &\triangleq [\![a]\!](es, ms) \cup [\![b]\!](es, ms) \\
& \quad \mathsf{where}\ (S_e^1, S_m^1) \cup (S_e^2, S_m^2) \triangleq (S_e^1 \cup S_e^2, S_m^1 \cup S_m^2) \\
[\![a \cdot b]\!](es, ms) &\triangleq [\![a]\!](es, ms) \cap [\![b]\!](es, ms) \\
& \quad \mathsf{where}\ (S_e^1, S_m^1) \cap (S_e^2, S_m^2) \triangleq (S_e^1 \cap S_e^2, S_m^1 \cap S_m^2) \\
[\![\neg a]\!](es, ms) &\triangleq \mathsf{let}\ (S_e, S_m) = [\![a]\!](es, ms) \\
& \quad \mathsf{in}\ (\{es\} - S_e, \{ms\} - S_m)
\end{aligned}
$$

2.2.2 Semantics of Policies

$$
\begin{aligned}
[\![\cdot]\!] \;:\; & \mathbf{Stream}(E) \times \mathbf{Stream}(M) \to \\
& P(\mathbf{Stream}(E)) \times P(\mathbf{Stream}(M)) \\
[\![(\Phi_{Encrypt}, \Phi_{Decrypt})]\!](es, ms) \triangleq\; & \mathsf{let}\ (e \to e^{\mathbf{o}} = \Phi_{Encrypt}),\ (m^{\mathbf{o}} \to m = \Phi_{Decrypt}) \\
& \mathsf{in}\ (\{e^{\mathbf{o}}\}, \{m\}) \\
[\![inj_{SR}(e)]\!](es, ms) \triangleq\; & (\{e : es\}, \{ms\}) \\
[\![inj_{Mi}(m)]\!](es, ms) \triangleq\; & (\{es\}, \{m : ms\}) \\
[\![f \leftarrow n]\!](es, ms) \triangleq\; & (\mathsf{map}\ (f \leftarrow n)\ \{e\},\ \mathsf{map}\ (f \leftarrow n)\ \{m\}) \\
[\![p + q]\!](es, ms) \triangleq\; & [\![p]\!](e, m) \cup [\![q]\!](e, m) \\
& \mathsf{where}\ (S_e^1, S_m^1) \cup (S_e^2, S_m^2) \triangleq (S_e^1 \cup S_e^2, S_m^1 \cup S_m^2) \\
[\![p \cdot q]\!](es, ms) \triangleq\; & \mathsf{let}\ (S_e, S_m) = [\![p]\!](e, m) \\
& \mathsf{in}\ \bigcup \{[\![q]\!](e', m') \mid e' \in S_e, m' \in S_m\}
\end{aligned}
$$

$$
\begin{aligned}
[\![\mathsf{filter}\ f]\!](S) &\triangleq \{l \in S \mid f(l) = \mathsf{true}\} \\
[\![\mathsf{map}\ g]\!](S) &\triangleq \{g(l) \mid l \in S\}
\end{aligned}
$$

3 Compilation to Verilog

3.1 The Intermediate Language

Values	v	::=	INSTR | RES	
Registers	b	::=	reg	
Expressions	e	::=	$read(b)$	*Read Reg*
		|	$write(b, v)$	*Write Value to Reg*
		|	$let\ x = e_1\ in\ e_2$	*Assignment*
		|	$e_1 \mid\mid e_2$	*Parallel*
		|	$f(e_1)$	*Apply Function*
		|	$if\ v = n\ then\ e_1\ else\ e_2$	*Conditional*
		|	e_1 && e_2	*Product (AND)*
		|	$e_1; e_2$	*Concatenation*
		|	$forever\ e$	*Hardwire*

3.2 Compiling GARUDA 2.0 to the Intermediate

We define a function **C** to be the compilation of some predicate or policy in GARUDA 2.0 to the intermediate language. **C** operates on the four ports of the GARUDA 2.0 monitor. These consist of the processing done after the Execution stage, before the Memory stage, and their respective altered streams. Table **??** summarizes each port. Assume all **C** are short for $\mathbf{C}_{(EXE,EXE^{\mathbf{o}},MEM^{\mathbf{o}},MEM)}$ if unspecified.

PORT	DESCRIPTION
EXE	Direct output of the execution stage.
$EXE^{\mathbf{o}}$	Altered state register input.
$MEM^{\mathbf{o}}$	Direct output of the state register.
MEM	Altered memory access input.

3.2.1 Compiling Predicates

$$
\begin{aligned}
\mathbf{C}[0] &= let\ E\_bog = \text{new buf} \\
&\quad\ M\_bog = \text{new buf} \\
&\quad in\ write(EXE^{\mathbf{o}}, E\_bog) \\
&\quad\ write(MEM, M\_bog) \\
\mathbf{C}[1] &= write(EXE^{\mathbf{o}}, read(EXE)) \\
&\quad write(MEM, read(MEM^{\mathbf{o}})) \\
\mathbf{C}[f = n] &= if\ EXE = n\ then \\
&\quad\ write(EXE^{\mathbf{o}}, read(EXE)) \\
&\quad\ else\ \mathbf{C}_{(EXE, EXE^{\mathbf{o}}, -, -)}[0] \\
&\quad if\ MEM^{\mathbf{o}} = n\ then \\
&\quad\ write(MEM, read(MEM^{\mathbf{o}})) \\
&\quad\ else\ \mathbf{C}_{(-, -, MEM^{\mathbf{o}}, MEM)}[0] \\
\mathbf{C}[\mathsf{test}(a + b)] &= (*Intermediate\ Execution\ Ports*) \\
&\quad let\ E_{ai}, E^{\mathbf{o}}_{ai}, E_{bi}, E^{\mathbf{o}}_{bi} = \text{new buf}\ in \\
&\quad (*Intermediate\ Memory\ Ports*) \\
&\quad let\ M^{\mathbf{o}}_{ai}, M_{ai}, M^{\mathbf{o}}_{bi}, M_{bi} = \text{new buf}\ in \\
&\quad\ \ DeMux(EXE, E_{ai}, E_{bi})\ || \\
&\quad\ \ DeMux(MEM^{\mathbf{o}}, M^{\mathbf{o}}_{ai}, M^{\mathbf{o}}_{bi}) \\
&\quad let\ i_a = \mathbf{C}_{(E_{ai}, E^{\mathbf{o}}_{ai}, M^{\mathbf{o}}_{ai}, M_{ai})}[a] \\
&\quad\ \ i_b = \mathbf{C}_{(E_{bi}, E^{\mathbf{o}}_{bi}, M^{\mathbf{o}}_{bi}, M_{bi})}[b] \\
&\quad in\ Mux(i_a\ \ i_b, (EXE^{\mathbf{o}}, MEM)) \\
\mathbf{C}[\mathsf{test}(a \cdot b)] &= \mathbf{C}[\mathsf{test}(a) \cdot \mathsf{test}(b)] \\
\mathbf{C}[\neg a] &= if\ \neg a\ then \\
&\quad\ write(EXE^{\mathbf{o}}, read(EXE)) \\
&\quad\ write(MEM, read(MEM^{\mathbf{o}})) \\
&\quad else\ \mathbf{C}[0]
\end{aligned}
$$

3.2.2 Compiling Policies

$$
\begin{aligned}
\mathbf{C}[inj_{SR}V] &= write(EXE^{\mathbf{o}}, V) \\
\mathbf{C}[inj_{Mi}V] &= write(MEM, V) \\
\mathbf{C}[f \leftarrow n] &= let\ e' = f(read(EXE)) \\
&\qquad m' = f(read(MEM^{\mathbf{o}})) \\
&\quad in\ write(EXE^{\mathbf{o}}, e') \\
&\qquad write(MEM, m') \\
\mathbf{C}[p + q] &= let\ e_p = \mathbf{C}[p] \\
&\qquad e_q = \mathbf{C}[q] \\
&\quad in\ Mux(e_p, e_q, (EXE^{\mathbf{o}}, MEM)) \\
\mathbf{C}[p \cdot q] &= let\ EXE_{mid} = \text{new buf} \\
&\qquad MEM_{mid} = \text{new buf} \\
&\qquad e_p = \mathbf{C}_{(EXE, EXE_{mid}, MEM^{\mathbf{o}}, MEM_{mid})}[p] \\
&\qquad e_q = \mathbf{C}_{(EXE_{mid}, EXE^{\mathbf{o}}, MEM_{mid}, MEM)}[q] \\
&\quad in\ e_p\ ;\ e_q
\end{aligned}
$$

4 Applications of GARUDA 2.0

4.1 Standard Taint

In the previous version of GARUDA, taint was implemented by tagging the most significant bit of a register. This caused no hardware overhead to maintain in the pipeline, but imposed an obvious bit-resolution hindrance. In GARUDA 2.0, the definition of such a policy is identical, but the compilation is different.

We assume a MIPS-like architecture for this example. The op codes of any given instruction are no more than 3; IN_1, IN_2, and OUT We denote these as RS, RT, and RD.

Let's suppose you want your taint to propogate on the inputs of any arithmetic instructions. Additionally, you prohibit any tainted instructions or addresses from accessing memory. In GARUDA 2.0, we can define this as follows. Please note that ALU can further be expanded to specific types of ALU instructions

$$
\begin{array}{rcl}
\textit{Instruction Fields } f_i & ::= & \mathsf{Taint_{RS}}, \mathsf{Taint_{RT}}, \mathsf{Taint_{RD}}, \mathsf{OP} \\
\mathsf{OP} & ::= & \mathsf{MEM_{READ}} \mid \mathsf{MEM_{WRITE}} \mid \mathsf{ALU} \mid \cdots \\
\textit{Result Fields } f_r & ::= & (*\mathsf{empty}*) \\
 & & \\
\mathsf{Arith} & \triangleq & \mathsf{OP} = \mathsf{ALU} \\
\mathsf{Read} & \triangleq & \mathsf{OP} = \mathsf{MEM_{READ}} \\
\mathsf{Write} & \triangleq & \mathsf{OP} = \mathsf{MEM_{WRITE}} \\
\mathsf{AnyMem} & \triangleq & \mathsf{Read} + \mathsf{Write} \\
 & & \\
\mathsf{TaintedInstr} & \triangleq & (\mathsf{Taint_{RS}} = \mathsf{TRUE}) + (\mathsf{Taint_{RT}} = \mathsf{TRUE}) \\
\mathsf{TaintRes} & \triangleq & \mathsf{Taint_{RD}} \leftarrow \mathsf{TRUE} \\
 & & \\
\mathsf{PropTaintALU} & \triangleq & act(\mathsf{Arith} \cdot \mathsf{TaintedInstr} \cdot \mathsf{TaintRes}) \\
 & & +act(\mathsf{Arith} \cdot \neg\mathsf{TaintedInstr}) \\
\mathsf{NoTaintMem} & \triangleq & act(\mathsf{AnyMem} \cdot \neg\mathsf{TaintedInstr}) \\
\mathsf{SecureMem} & \triangleq & \mathsf{PropTaintALU} + \mathsf{NoTaintMem} \\
 & & +act(\neg(\mathsf{Arith} + \mathsf{AnyMem}))
\end{array}
$$

4.2 Speculative Taint

[1]

$$
\begin{array}{rcl}
\textit{Instruction Fields } f_i & ::= & \mathsf{Taint_{RS}}, \mathsf{Taint_{RT}}, \mathsf{Taint_{RD}}, \mathsf{OP} \\
\mathsf{OP} & ::= & \mathsf{MEM_{READ}} \mid \mathsf{MEM_{WRITE}} \mid \mathsf{ALU} \mid \cdots \\
\textit{Result Fields } f_r & ::= & (*\mathsf{empty}*) \\
 & & \\
\mathsf{Arith} & \triangleq & \mathsf{OP} = \mathsf{ALU} \\
\mathsf{Read} & \triangleq & \mathsf{OP} = \mathsf{MEM_{READ}} \\
\mathsf{Write} & \triangleq & \mathsf{OP} = \mathsf{MEM_{WRITE}} \\
\mathsf{AnyMem} & \triangleq & \mathsf{Read} + \mathsf{Write} \\
 & & \\
\mathsf{TaintedInstr} & \triangleq & (\mathsf{Taint_{RS}} = \mathsf{TRUE}) + (\mathsf{Taint_{RT}} = \mathsf{TRUE}) \\
\mathsf{TaintRes} & \triangleq & \mathsf{Taint_{RD}} \leftarrow \mathsf{TRUE} \\
 & & \\
\mathsf{PropTaintALU} & \triangleq & act(\mathsf{Arith} \cdot \mathsf{TaintedInstr} \cdot \mathsf{TaintRes}) \\
 & & +act(\mathsf{Arith} \cdot \neg\mathsf{TaintedInstr}) \\
\mathsf{NoTaintMem} & \triangleq & act(\mathsf{AnyMem} \cdot \neg\mathsf{TaintedInstr}) \\
\mathsf{SecureMem} & \triangleq & \mathsf{PropTaintALU} + \mathsf{NoTaintMem} \\
 & & +act(\neg(\mathsf{Arith} + \mathsf{AnyMem}))
\end{array}
$$

References

[1] Jiyong Yu, Mengjia Yan, Artem Khyzha, Adam Morrison, Josep Torrellas, and Christopher W Fletcher. Speculative taint tracking (stt) a comprehensive protection for speculatively accessed data. In *Proceedings of the 52nd Annual IEEE/ACM International Symposium on Microarchitecture*, pages 954–968, 2019.