Secured Integration of Non-Trusted IPs in SoCs

Festus Hategekimana, Taylor JL Whitaker,
Md Jubaer Pantho Hossain, Christophe Bobda
Smart Embedded Systems Lab, Computer Science Computer Engineering Dept.
University of Arkansas - Fayetteville, Arkansas
AsianHOST – Beijing, 19 October 2017

Agenda

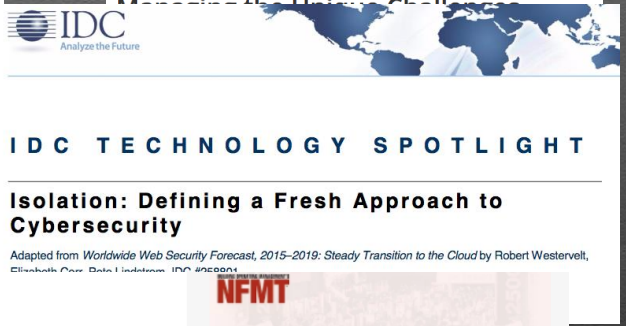
- Introduction
- Hardware Sandboxing
- CAPSL Design Flow
- Evaluation
- Roadmap

Isolation/Separation

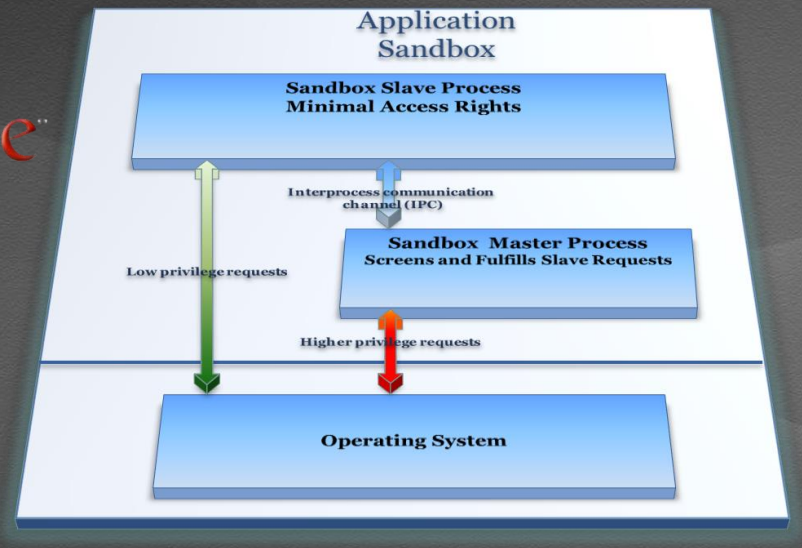
- Threat Model
  - Insertion/Activation of hardware Trojan in trusted system designs
  - Increasingly relevant with growing adoption rate of third-party IPs

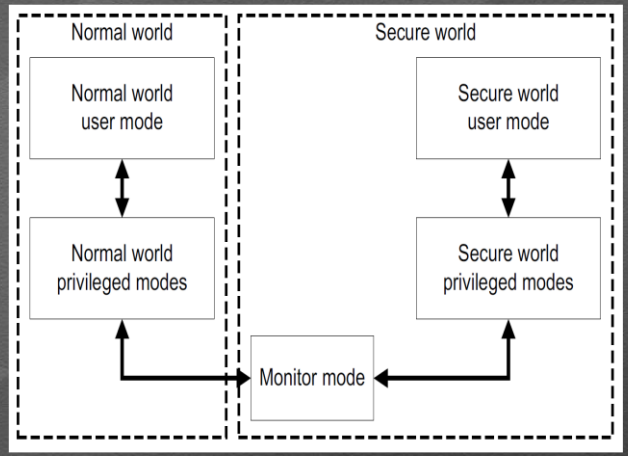
Introduction

- Deception
- Separation
- Diversity
- Consistency
- Depth
- Discretion
- Collection
- Correlation
- Awareness
- Response



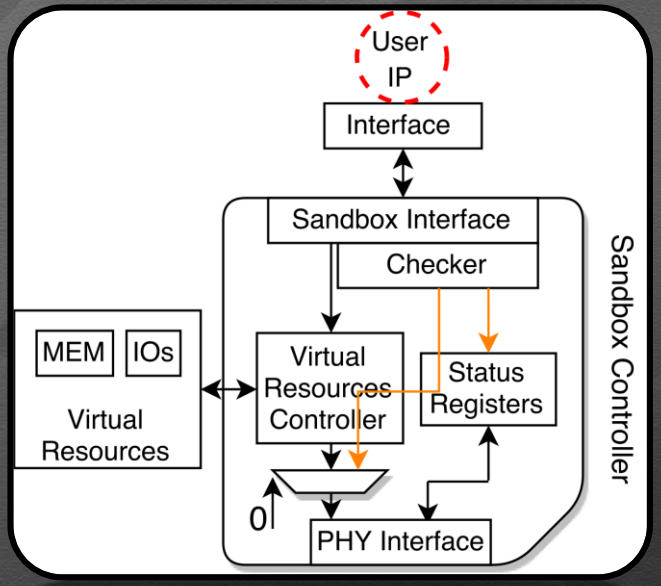
Isolation


Application Sandbox
Sandbox Slave Process
Minimal Access Rights
Interprocess communication channel (IPC)
Sandbox Master Process
Screens and Fulfills Slave Requests
Low privilege requests
Higher privilege requests
Operating System


Normal world
Secure world
Normal world user mode
Secure world user mode
Normal world privileged modes
Secure world privileged modes
Monitor mode

Hardware Sandboxing

- Isolation, Integrity, Containment
  - IP limited to specified interactions
    - Enforces data accessibility and modification
  - Potentially malicious interactions are contained
  - Critical system resources are protected



UNIVERSITY OF ARKANSAS

Hardware Sandboxing

- Controller
  - Routes connections between untrusted IP, the properties checker, virtual resources, and a host system
- Virtual Resources
  - Prevents physical resource damage
- Status/Control Registers
  - Accesses sandbox checker status and setting checker parameters
- Interfaces
  - System-Sandbox, IP-Sandbox
- Checker
  - Checks interactions against pre-determined specification

Hardware Sandboxing

- Feasibility
  - Verified with a UAV anti-jamming application
- Issues
  - Sandbox controller must be customized to an IP
  - No generalization

Automating Hardware Sandboxes

Component Authentication Process for Sandboxed Layouts

IP Specification

- IP Interface Specification
  - Interface Automata
  - Expected behavioral specification
  - Resource Requirements
- Extended Logic
  - PSL SERE
    - Explicit denial of interface behavior

IP Specification

```
<IP_name>.def{
  // Signal types: input, output
  <signal_name> : <signal_type>,  // Interface ports
  <vector_name> : <signal_type>(<length>),

  transitions{
    s0          : <signal_name>   : s<integer>, // s0 always initial state
    s<integer> : !<signal_name> : s<integer>,
  },

  resources{
    <resource_name> : { <option_name> : <option_setting> }
  }
}
```

IP Specification

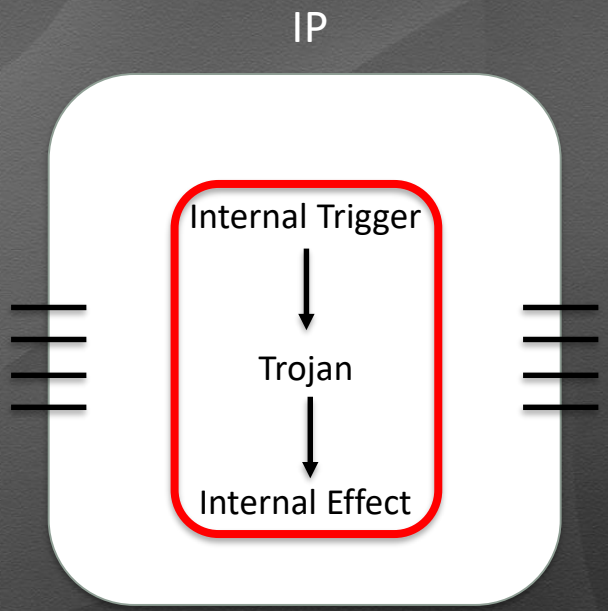
```
logic.def{
  // Logic operators: and, or, ==, !=
  <signal_name> : <signal_name> <logic_operator> <signal_name>,

  <signal_name> : counter {   // Counter example
    on:     <signal_name>,
    start:  <integer>,
    end:    <integer>
  },

  prohibited{
    { <signal_name> : <signal_name> },            // fusion
    { <signal_name> ; <signal_name> },            // concatenation
    { <signal_name>[ *<integer> ]   },            // kleene star
    { <signal_name>[ =<integer> .. <integer> ] }, // non-consecutive repeat
  }
}
```

Extended Logic

UNIVERSITY OF ARKANSAS

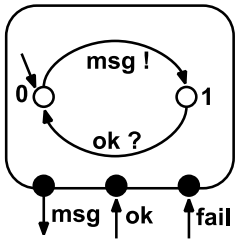
IP Specification

- Formal Model Limitations
  - Expresses only interface behaviors
  - Cannot monitor signals that do not propagate beyond IP interface
- Ex. Internally triggered Trojan activating power draw circuit



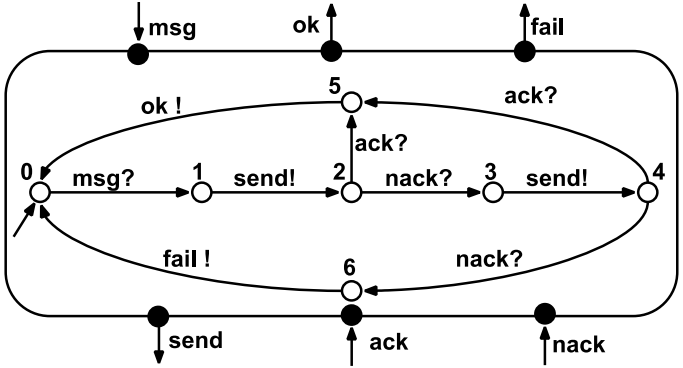
Model Optimization

- IA Operations
  - Composition, Refinement



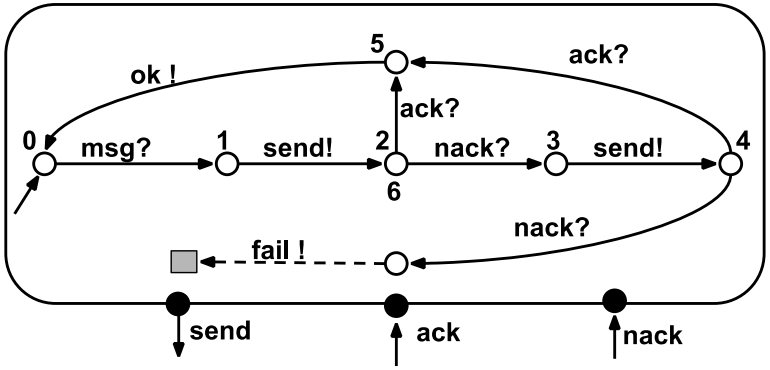
User

2 states, 2 transitions



Message

7 states, 9 transitions



User ⊗ Message

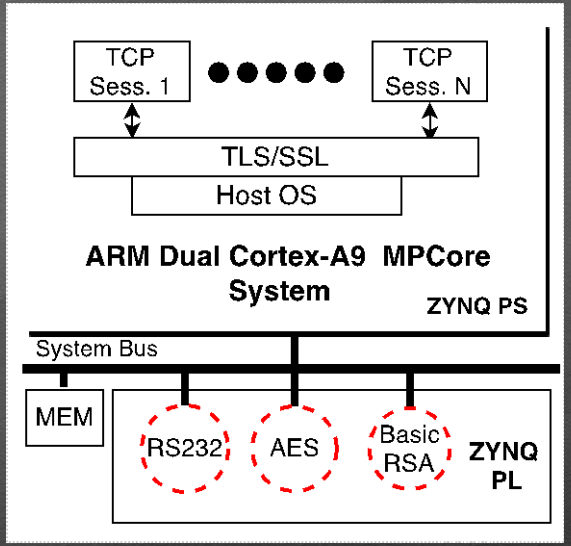
7 states, 8 transitions

Sandbox Generation

- Final set of IP models -> Properties Checker
- Currently generating Xilinx Vivado IP
  - Immediately available to integrate into design
- Adaptable output
  - VHDL, SystemC

Evaluation

- Echo Server
  - Uses infected hardware encryption core purposed for TLS/SSL
  - Performs TLS upon new connection
  - Encrypts the echo
- Client
  - Initiates TLS, sends/receives message



Evaluation

- Trojan Detection
  - AES-T300 never propagates to the IP interface

Design	Trojan Class	Activated?	Trigger	Effect
AES-T100	Info Leak	Always On	N/A	Key Leak via Side-Channel
AES-T300	Info Leak	Always On	N/A	Key Leak via Power Fluctuation
AES-T500	DoS	Yes	Input Sequence	Power Draw Increase
BasicRSA-T100	Info Leak	Yes	Input Value	Key Leak via Protocol
BasicRSA-T300	DoS	Yes	Internal Counter	Key Leak via Protocol
RS232-T100	DoS	Yes	Internal Comparator	Protocol Deviation
RS232-T300	DoS	Yes	Internal Counter	Protocol Deviation
RS232-T500	DoS	Yes	Internal Counter	Protocol Deviation

Evaluation

- Resource Reduction
  - Composing individual IP checkers to form global system checker
  - Size of the sandboxes is less when utilizing composition

Component	LUTs	LUTs W/ Composition	FFs	FFs W/ Composition
RS232 Checker	57 (0.026%)	-	60 (0.013%)	-
AES-128 Checker	213 (0.09%)	-	18 (0.004%)	-
BasicRSA Checker	22 (0.01%)	-	4 (< 0.001%)	-
Composed Checker	-	101 (0.05%)	-	28 (0.006%)
Sandbox (Checkers + Controller)	487 (0.22%)	294 (0.13%)	82 (0.02%)	28 (0.006%)

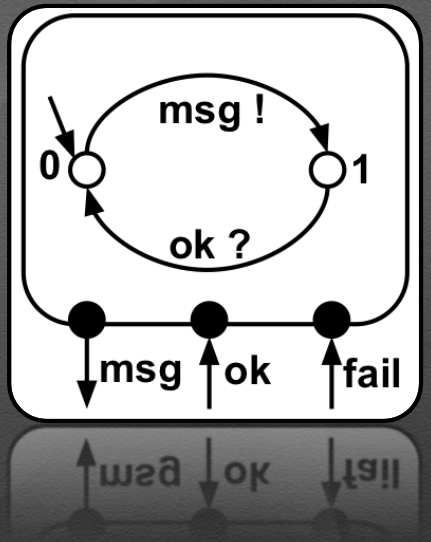
Acknowledgements

- Supported by the Air Force Research Laboratory, Cyber Assurance (SSFP 2016) and the Office of Naval Research (ONR) under grant number CCN 0402-17643-21-0000

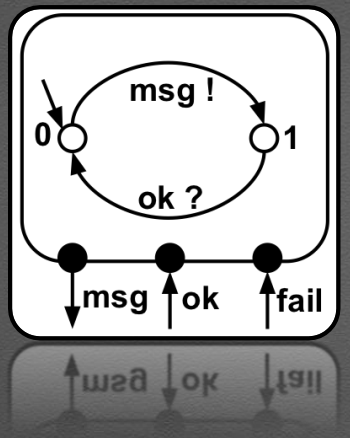
Thank You.

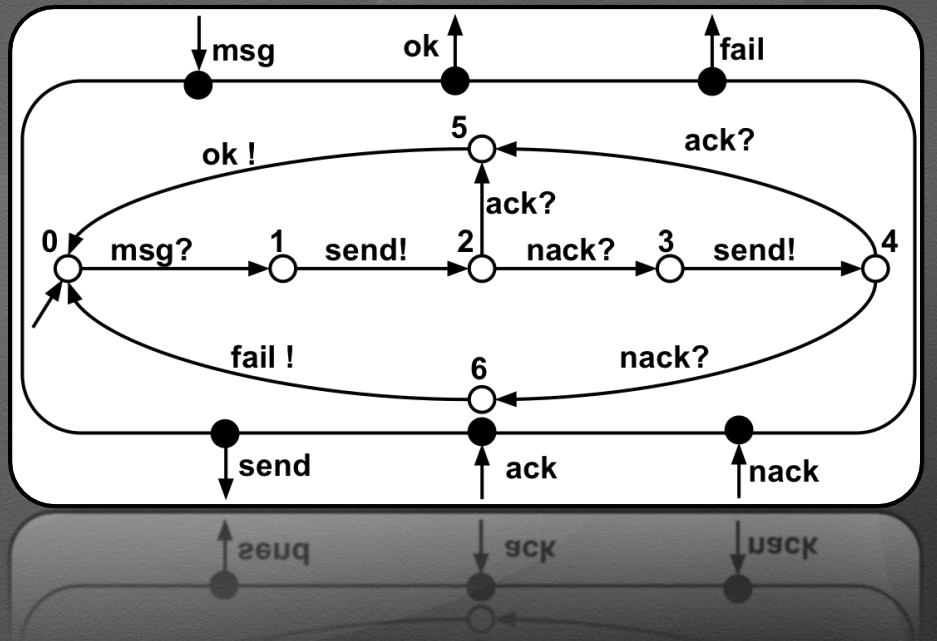
Hardware Sandboxing

- Properties Checker
  - Are the IP behaving as expected?
  - IP specification with Interface Automata and PSL Sequential Extended Regular Expressions
  - Set of property-defining automata are used to generate the sandbox checker

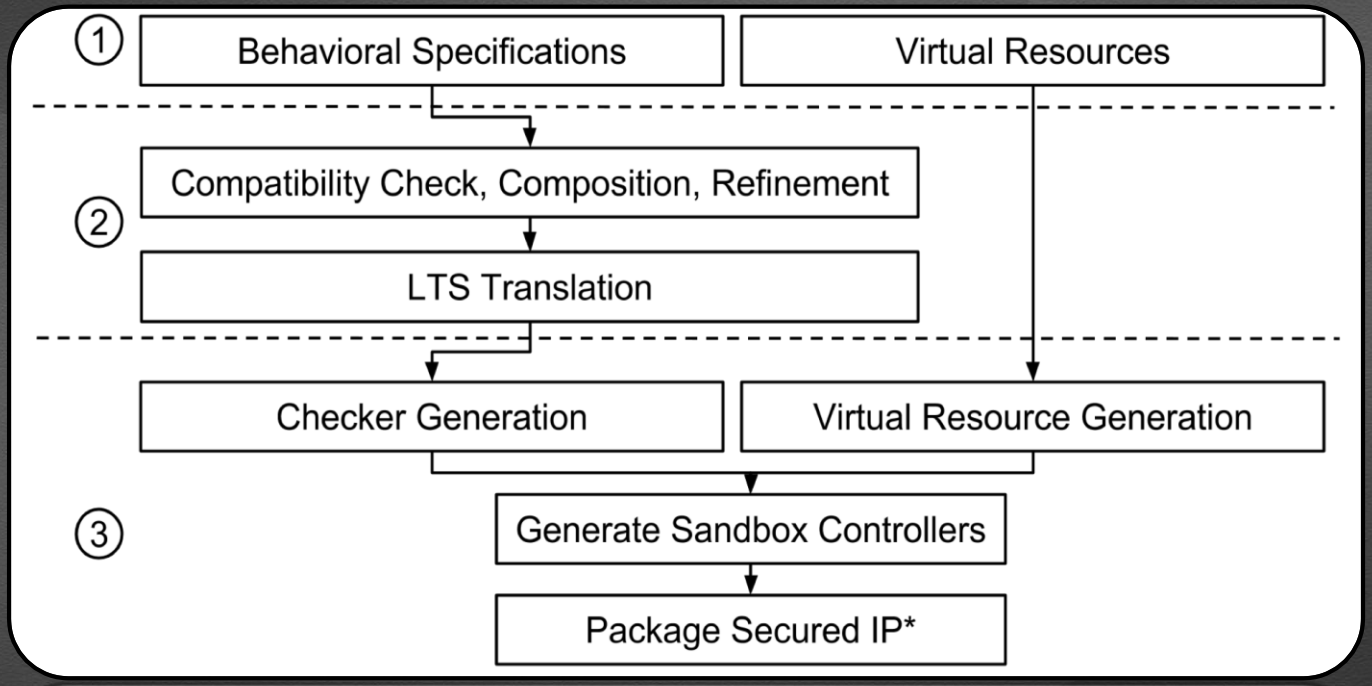


IA Composition





Design Flow


1
Behavioral Specifications
Virtual Resources
2
Compatibility Check, Composition, Refinement
LTS Translation
Checker Generation
Virtual Resource Generation
3
Generate Sandbox Controllers
Package Secured IP*

Evaluation

- Infected TLS/SSL Encryption Core
  - Trojan classes account for 63% of Trust-Hub.org RTL Trojans

Design	Trojan Class	Activated?	Trigger	Effect
AES-T100	Info Leak	Always On	N/A	Key Leak via Side-Channel
AES-T300	Info Leak	Always On	N/A	Key Leak via Power Fluctuation
AES-T500	DoS	Yes	Input Sequence	Power Draw Increase
BasicRSA-T100	Info Leak	Yes	Input Value	Key Leak via Protocol
BasicRSA-T300	DoS	Yes	Internal Counter	Key Leak via Protocol
RS232-T100	DoS	Yes	Internal Comparator	Protocol Deviation
RS232-T300	DoS	Yes	Internal Counter	Protocol Deviation
RS232-T500	DoS	Yes	Internal Counter	Protocol Deviation

Evaluation

- Trojan Detection
  - AES-T300 never propagates to the IP interface

Design	Trojan Class	Activated?	Trigger	Effect
AES-T100	Info Leak	Always On	N/A	Key Leak via Side-Channel
AES-T300	Info Leak	Always On	N/A	Key Leak via Power Fluctuation
AES-T500	DoS	Yes	Input Sequence	Power Draw Increase
BasicRSA-T100	Info Leak	Yes	Input Value	Key Leak via Protocol
BasicRSA-T300	DoS	Yes	Internal Counter	Key Leak via Protocol
RS232-T100	DoS	Yes	Internal Comparator	Protocol Deviation
RS232-T300	DoS	Yes	Internal Counter	Protocol Deviation
RS232-T500	DoS	Yes	Internal Counter	Protocol Deviation