Security Extensions to JTAG

Linda Lieu
SecureHardware LLC
November 12, 2010

Outline

- Background
- Problem Definition
- Possible Attacks
- Proposed Solutions
- Ongoing Work

History of JTAG

- Testing of multi-layer boards became much more difficult
- Bed-of-nails testing
- Joint Test Action Group (JTAG)
- IEEE Standard 1149.1 Test Access Port and Boundary Scan Architecture

JTAG Standard

- Increased controllability, faster testing time, lower cost

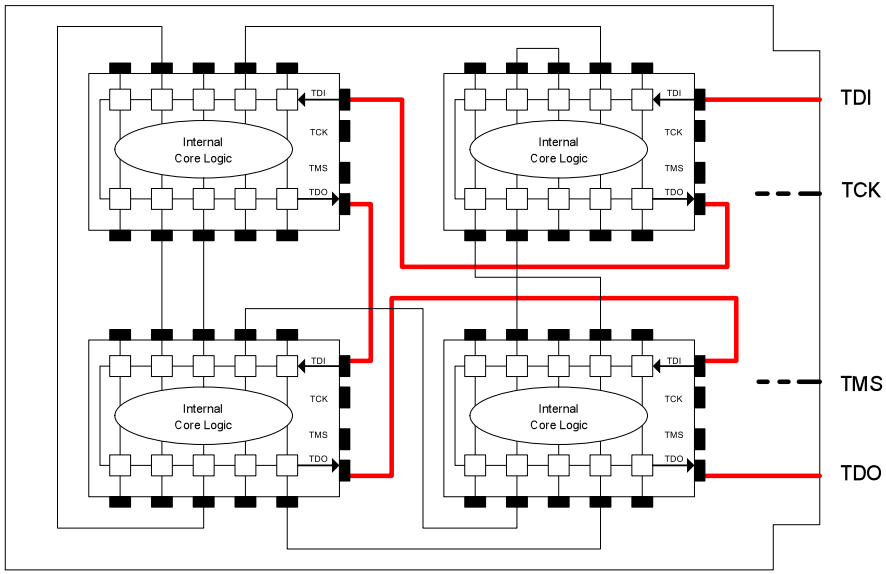


Fig. 1 Printed circuit board with four chips

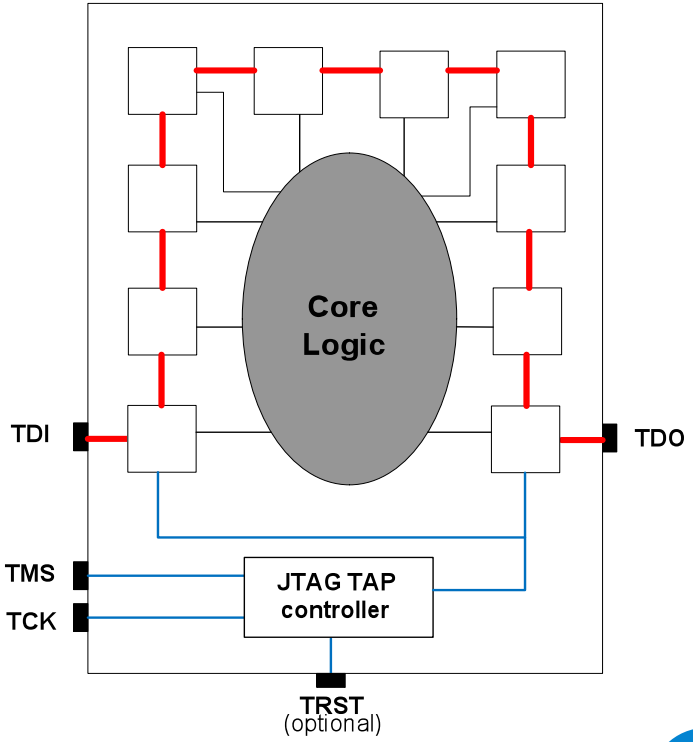


Fig. 2 Boundary Scan Testing on a Chip

JTAG Applications

- Debugging of software and programming of integrated circuits

- Widespread use in telecommunications, medical, government, financial industry etc.

- Enabled in most devices
  - Mobile phones, computers, microwaves

What is at Risk?

- Mission data
- Intellectual property
- Proper system functionality

JTAG Attacks

Source: Cisco Systems

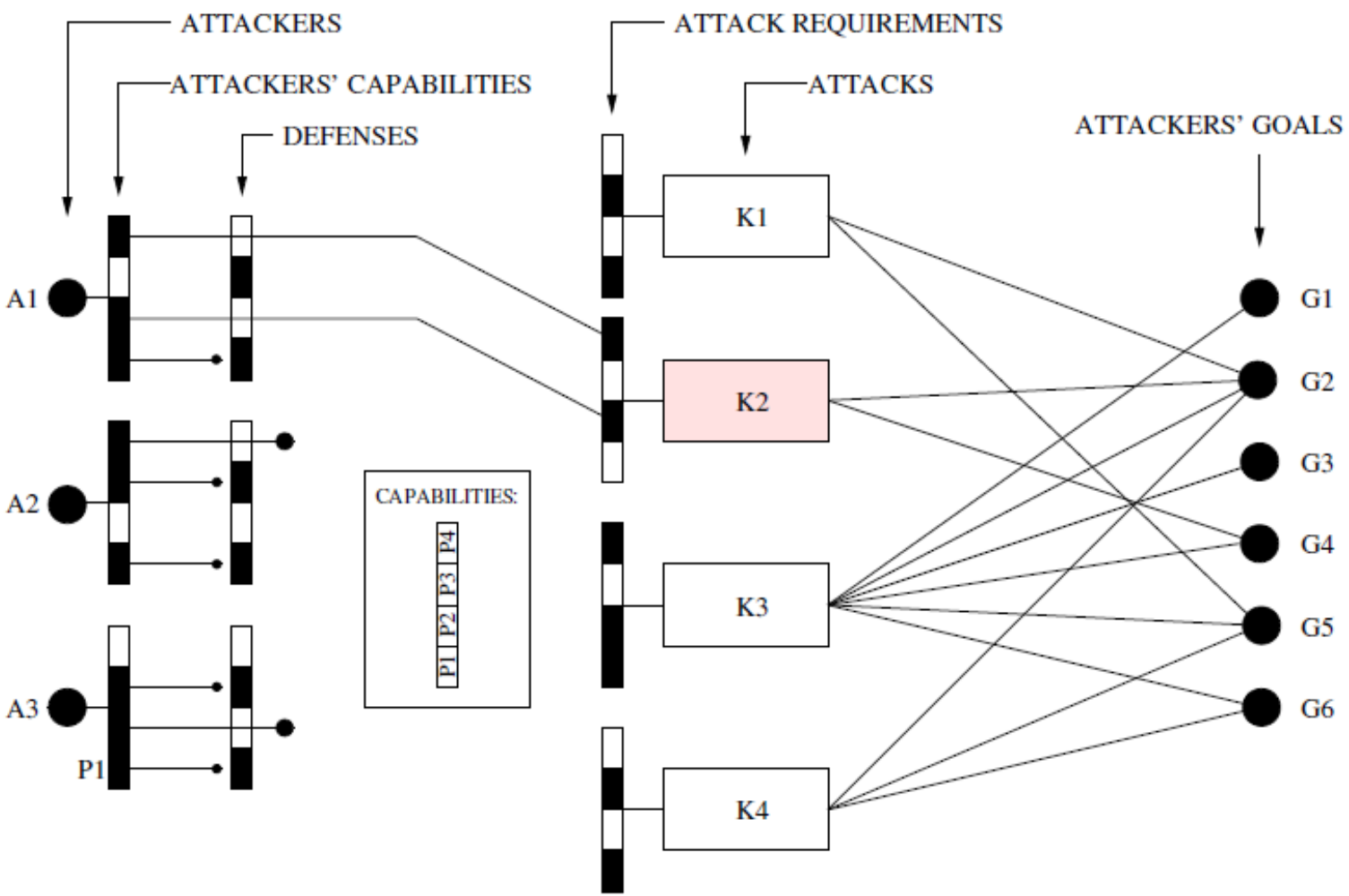
Potential Attackers

- Vendors of on-board components
- Producers of system components
- Users and/or consumers of the system

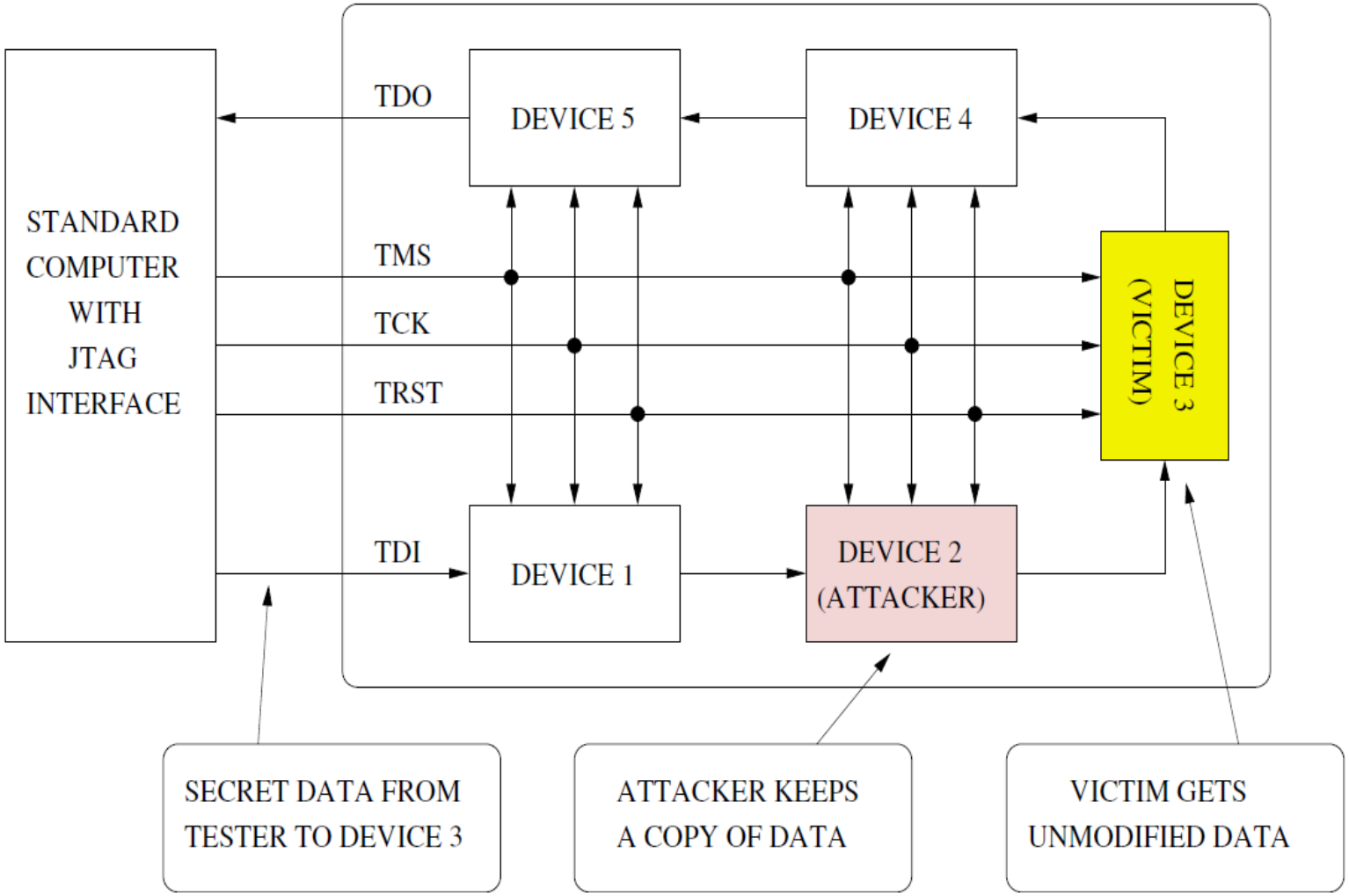
Goals of the Attacker

- Disable or corrupt the system
- Extract embedded code or crypto key
- Embed trojan functionality without detection
- Duplicate system design

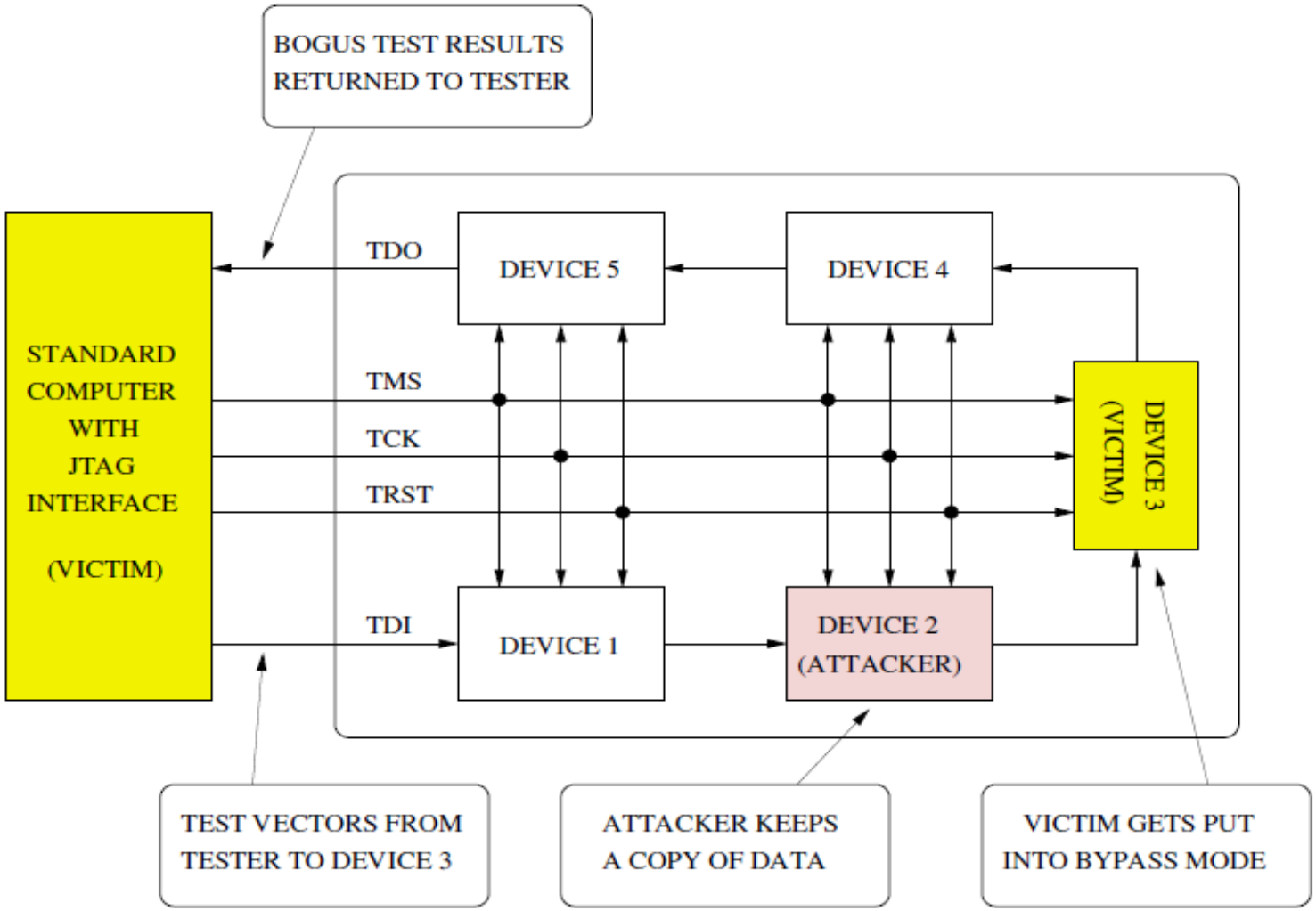
THREAT MODEL



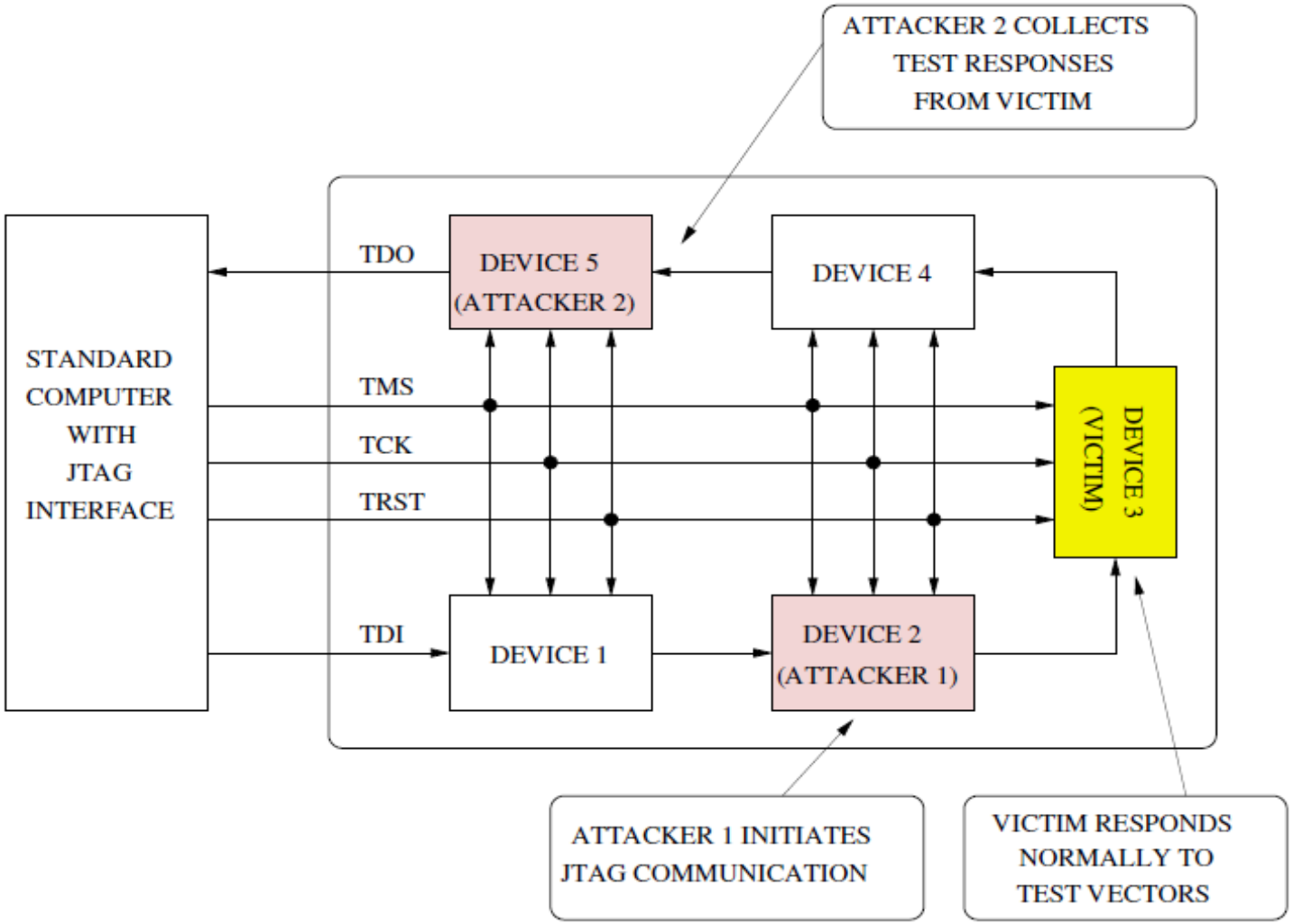
Attacker Obtains Test Data



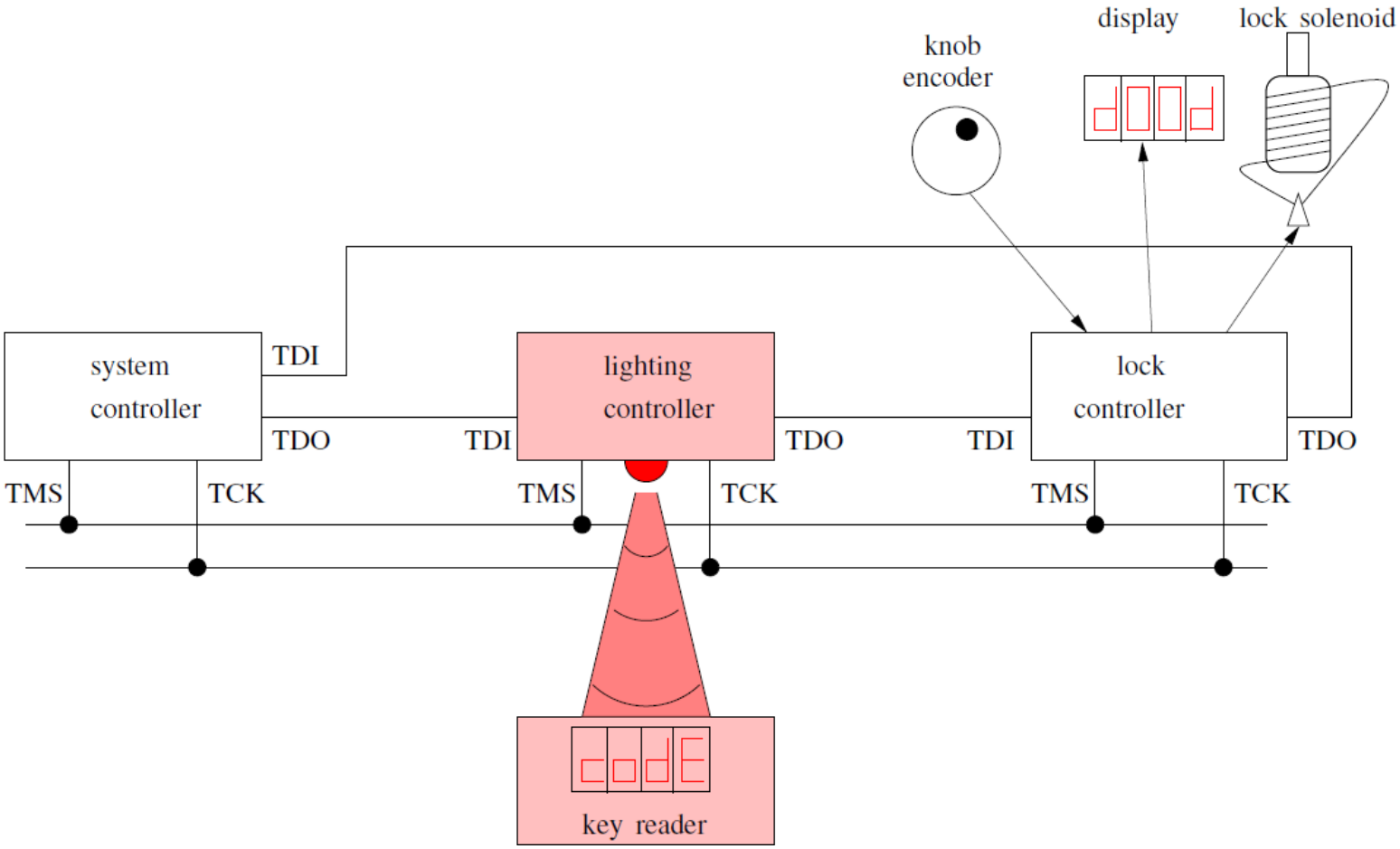
Tester Receives False Responses



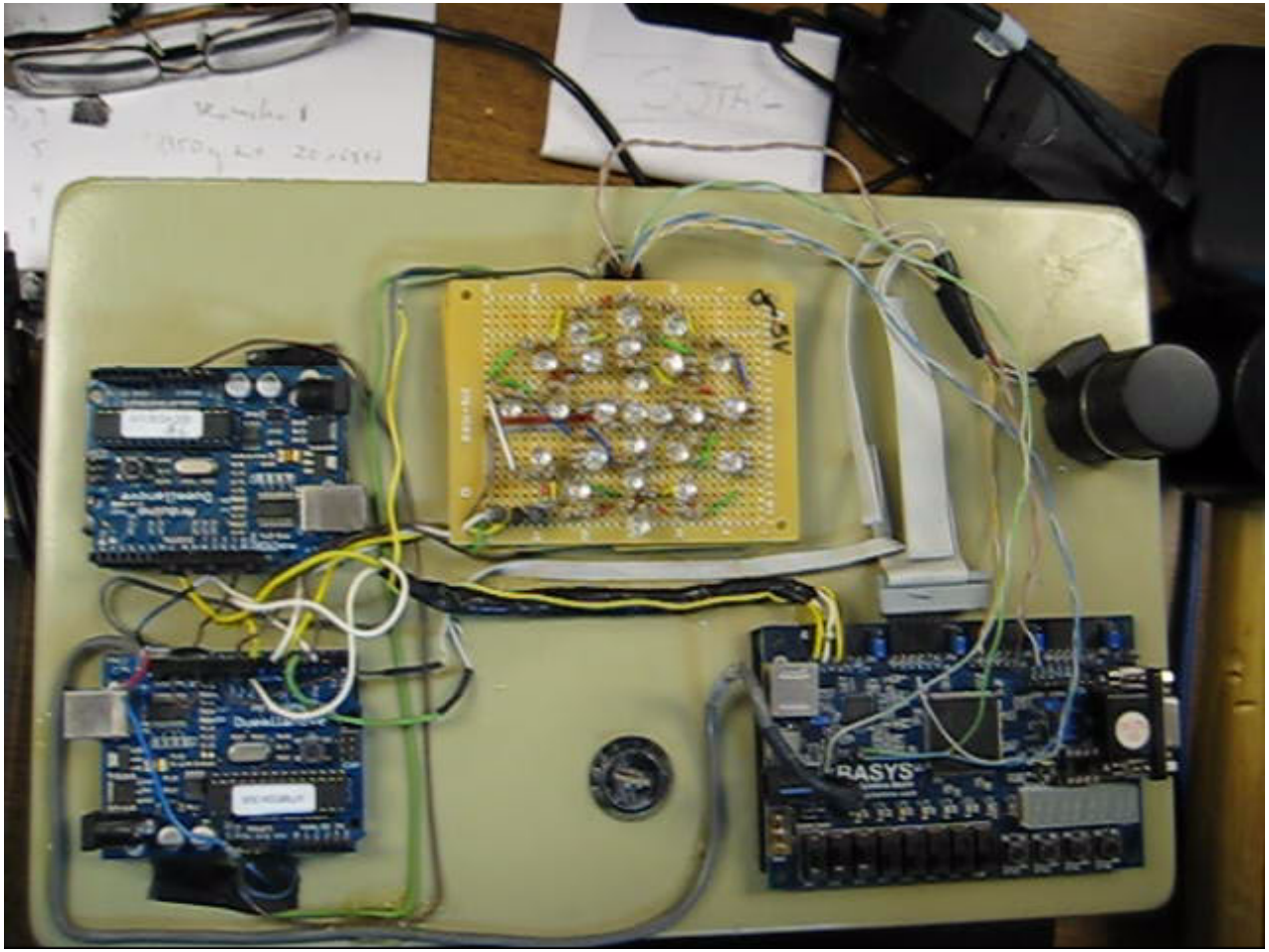
Attacker Reads Out Secret



Attack Demo


knob
encoder
display
lock solenoid
system
controller
TDI
TDO
TMS
TCK
lighting
controller
TDI
TDO
TMS
TCK
lock
controller
TDI
TDO
TMS
TCK
key reader

Attack Demo

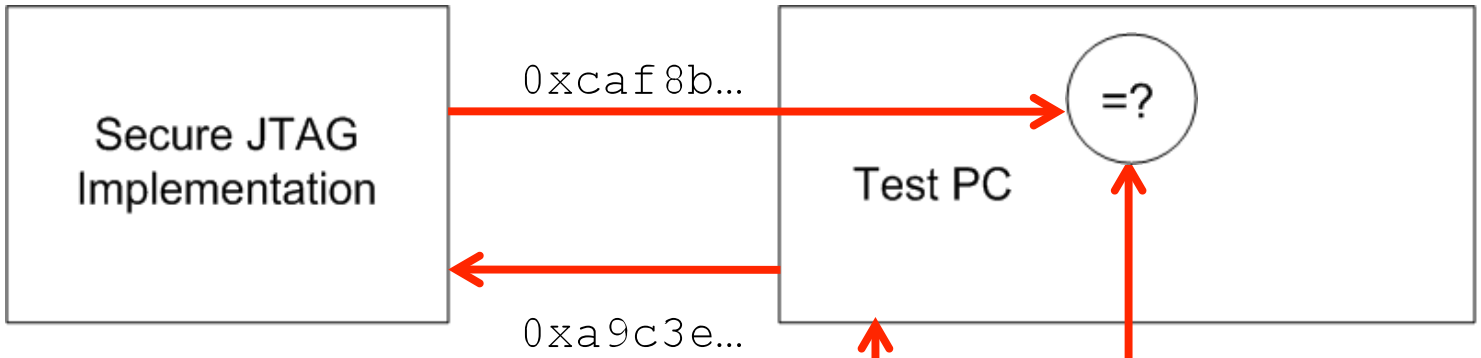


Our Solution

We propose the following security mechanisms:

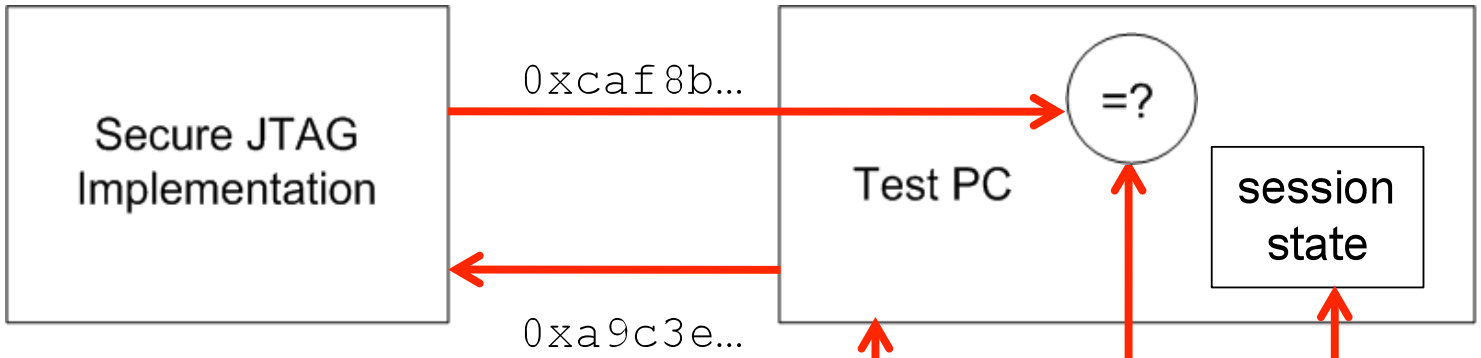
- Device/chip identification
- Test data encryption
- Communication integrity

Chip Authentication



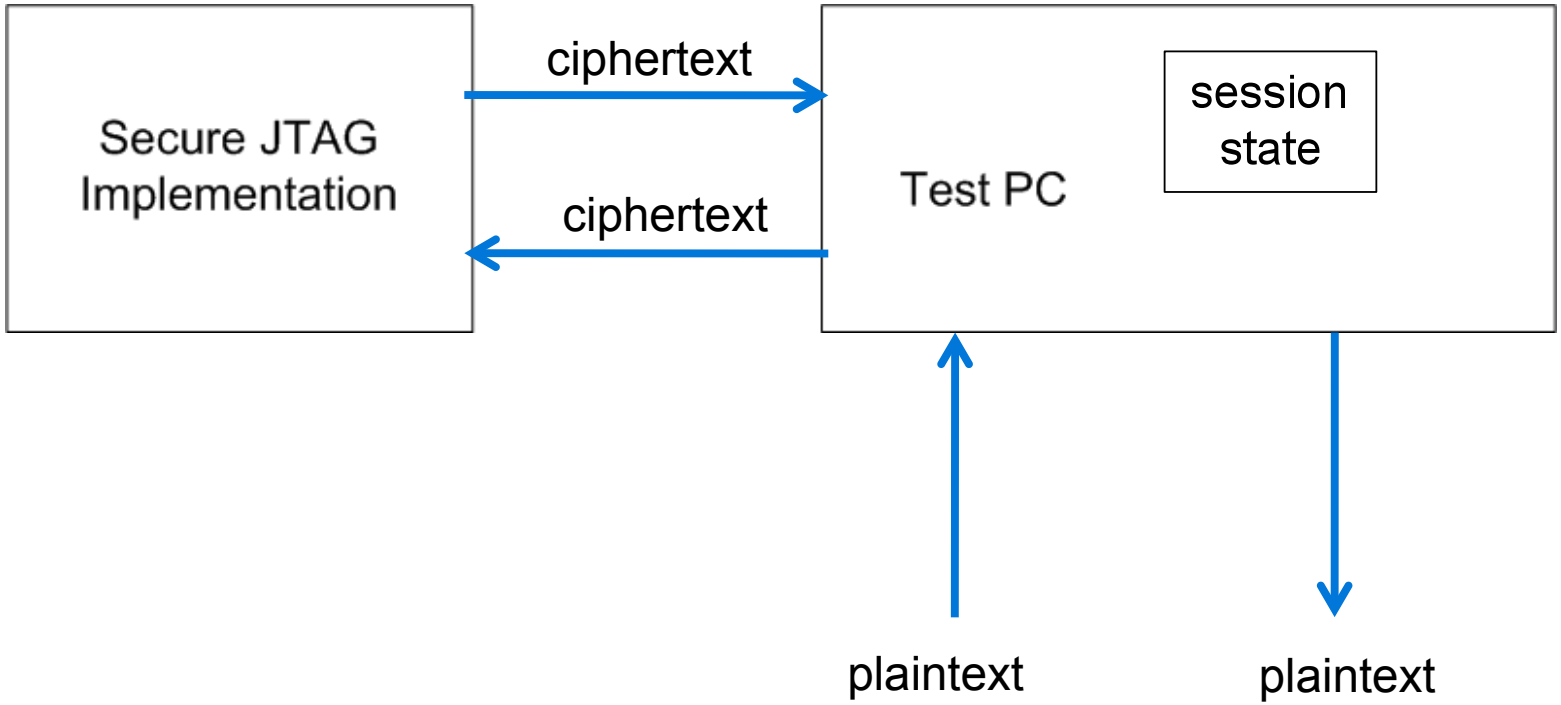
CHAL	RESP1	RESP2
0x23af4...	0xa938c...	0x32893...
0xeb4d8...	0x2459e...	0xf83bb...
0xa9c3e...	0xcaf8b...	0xb982c...
0x6d917...	0x9df44...	0xd1d8d...
0x0d0a3...	0x098a5...	0xfa083...
0x3b5c1...	0xda671...	0xc99b6...
0xd10c9...	0xe6333...	0x84d1a...

ENCRYPTION

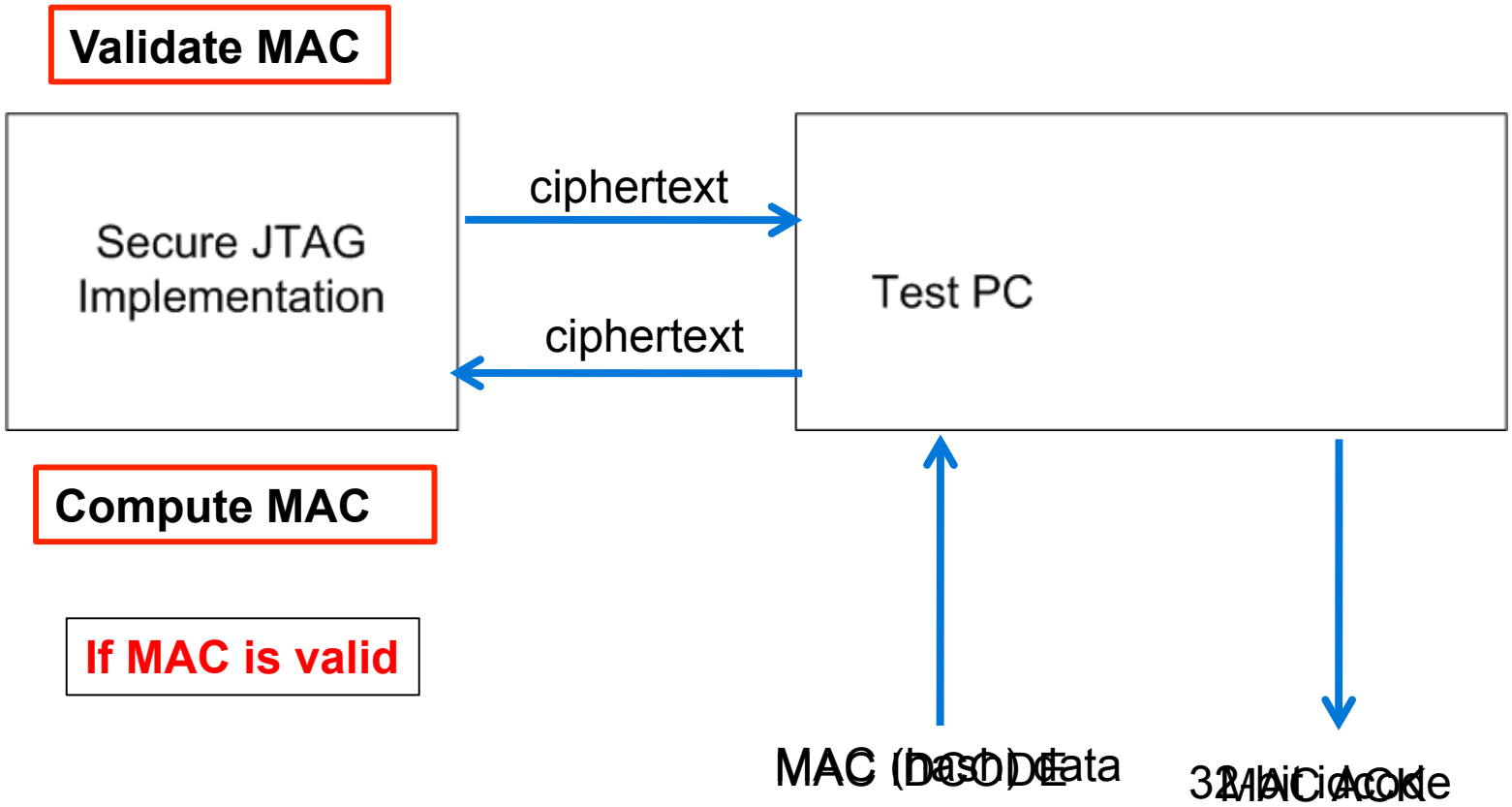


CHAL	RESP1	RESP2
0x23af4...	0xa938c...	0x32893...
0xeb4d8...	0x2459e...	0xf83bb...
~~0xa9c3e...~~	~~0xcaf8b...~~	~~0xb982c...~~
0x6d917...	0x9df44...	0xd1d8d...
0x0d0a3...	0x098a5...	0xfa083...
0x3b5c1...	0xda671...	0xc99b6...
0xd10c9...	0xe6333...	0x84d1a...

Encryption


Secure JTAG Implementation
ciphertext
ciphertext
Test PC
session state
plaintext
plaintext

Message Authentication Code



Continuing Work

- Identify other JTAG vulnerabilities
- Reduce impact on performance
- Explore different MACs and encryption algorithms
- Commercialize Secure JTAG design