STARBLEED
A FULL BREAK OF THE BITSTREAM ENCRYPTION
OF XILINX 7-SERIES FPGAS

Maik Ender, Amir Moradi, and Christof Paar

Ruhr University Bochum & MPI for Privacy and Security

USENIX Security, August 14, 2020
STARBLEED
A FULL BREAK OF THE BITSTREAM ENCRYPTION OF XILINX 7-SERIES FPGAS

Maik Ender, Amir Moradi, and Christof Paar
Ruhr University Bochum & MPI for Privacy and Security
USENIX Security, August 14, 2020

https://www.reddit.com/r/ElectricalEngineering/comments/g6vaey/u/iguetesilva
FIELD PROGRAMMABLE GATE ARRAYS

Bitstream contains FPGA's design
Stored on external memory

Field **Programmable** Gate Array (FPGA)
Special IC
Reprogrammable logic
BITSTREAM SECURITY

Possible Consequences

- IP theft & design cloning
- Reverse engineering
- Design manipulation
- Hardware Trojans
Bitstream Encryption

Security Goals

- **Confidentiality**: bitstream is encrypted
- **Authenticity**: FPGA loads only designs from integrator
- **Integrity**: Bitstream is not changed

Key

FPGA

encrypted program

AES-256

HMAC
Security Goals

- **Confidentiality**: bitstream is encrypted
- **Authenticity**: FPGA loads only designs from integrator
- **Integrity**: Bitstream is not changed

**Starbleed Attack I**: Break Confidentiality

**Starbleed Attack II**: Break Authenticity
HOW TO PROGRAM AN FPGA?
CONFIGURATION ENGINE

FPGA

Configuration Engine

Configuration Registers
- FDRI
- FDRO
- Status
- Control 0
- WBSTAR
- ...

Fabric

JTAG

AES

Dec?

"Header"
"StartDec"

Encrypted

Bitstream
BITSTREAM PROGRAM

FPGA

Configuration Engine

Configuration Registers
- FDRI
- FDRO
- Status
- Control 0
- WBSTAR
- ...

Fabric

JTAG

Encrypted

"Header"

"StartDec"

Bitstream

Dec?

AES

0x03FE5

COFFEEEEE

HMAC tag
ATTACK 1
BREAKING CONFIDENTIALITY
ATTACK

FPGA resets

Authenticity Check

Config Engine

Configuration Registers

FDRI

FDRO

Status

WBSTAR

Fabric

Exploit CBC malleability

Cut bitstream

Bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Dec?

AES

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartEnc"

HMACHead

"WrCntr0"

02003FE5

"WrFDRI"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream

"Header"

"StartDec"

HMACHead

"WrCntr0"

02003FE5

"WrWBSTAR"

COFFEEEE

BADB0070

HMAC tag

Exploit CBC malleability

Cut bitstream
Reconfiguration and MultiBoot

This chapter focuses on full bitstream reconfiguration methods in 7 series FPGAs.

Fallback MultiBoot

Overview

The 7 series FPGAs MultiBoot and fallback features support updating systems in the field. Bitstream images can be upgraded dynamically in the field. The FPGA MultiBoot feature enables switching between images on the fly. When an error is detected during the MultiBoot configuration process, the FPGA can trigger a fallback feature that ensures a known good design can be loaded into the device.

When fallback happens, an internally generated pulse resets the entire configuration logic, except for the dedicated MultiBoot logic, the warm boot start address (WBSTAR), and the boot status (BOOTSTS) registers. This reset pulse pulls INIT_B and DONE Low, clears the configuration memory, and restarts the configuration process from address 0 with the revision select (RS) pins driven to 00. After the reset, the bitstream overwrites the WBSTAR starting address.
ATTACK – READOUT

FPGA

Bitstream

JTAG

Exploit CBC malleability

Cut bitstream

Authenticity Check

FPGA resets

Fabric

Configuration Registers

FDRI

FDRO

Status

C: 02003FE5

W: COFFEE

...
**ATTACK – OVERVIEW**

1) Manipulated Bitstream

- "Header"
- "StartDec"
- HMACHead
- "WrCntr0"
- 02003FE5
- COFFEEEE
- BADB0070
- HMAC tag

2) Readout Bitstream

- "Header"
- RdWBSTAR

→ Leaks one bitstream word (32 bits)

FPGA

1) Manipulate the bitstream

2) Configure the FPGA with the malicious bitstream

3) Resets the FPGA (automatically)

4) Read out the WBSTAR register

5) Reset the FPGA (manually)

Authenticity Check

FPGA resets

Configuration Registers

- FDRI
- FDRO
- Status
- Control 0
- WrWBSTAR
- ...
ATTACK II
BREAKING AUTHENTICITY
ATTACK II: BREAKING AUTHENTICITY

- HMAC key can be decrypted by attack I
  → Forge new valid HMAC tags
WHAT WENT WRONG?
WHAT WENT WRONG?

1. “Use before validate“ (Attack I)
2. Key dependency (Attack II)
COUNTERMEASURES AND DEFENSE TECHNIQUES
COUNTERMEASURES & DEFENSE TECHNIQUES

Countermeasures
Current 7-Series

Only raise-the-bare countermeasures exists

Countermeasures
New FPGA Series

- Validate the bitstream before use
- Needs new silicon
- Available in new FPGA Series

General defense techniques

- Avoid ad-hoc security designs
- Model checking, information flow analysis
- Community analysis

Reconfiguration and MultiBoot

This chapter focuses on full-system reconfiguration methods in 7-series FPGAs.

Fallback MultiBoot

Overview

The 7-series FPGA's MultiBoot and Fallback features support updating systems in the field. Bitstreams can be updated down-stream or in the field. The FPGA's MultiBoot feature enables switching between images on the fly. When an error is detected during the MultiBoot configuration process, the FPGA can trigger a fallback feature that re-issues a known good design to fix the device.

When fallback happens, an untrusted power-up prevents the entire configuration type, except for the selected MultiBoot image. After restoring the system, the MultiBoot image is loaded to the system. Otherwise, the MultiBoot image is restored to the system for a system-level partition image. If necessary, the restore system image is replaced in the MultiBoot image after restoring the system image. After restoring the system image, the restored system is returned to the system image for the system-level partition image.
CONCLUSION
CONCLUSION

Full break of Xilinx 7-Series Bitstream Encryption

Any questions?

@MaikEnderEU
Amir Moradi
@ChristofPaar