Karlsruhe Institute of Technology

Through Fabric: A Cross-world Thermal Covert Channel on TEE-enhanced FPGA-MPSoC Systems

Hassan Nassar, Jeferson Gonzalez-Gomez, Varun Manjunath, Lars Bauer, and Jörg Henkel

ASP-DAC 2025

Agenda

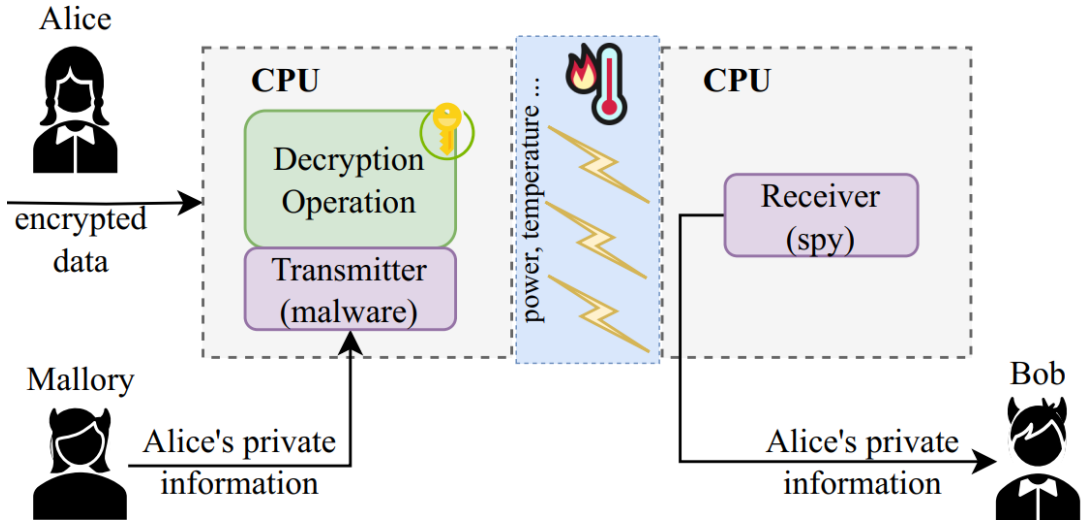
- Background
- Covert Channels
- State of the Art
- Assumptions and Limitations
- Through Fabric
- Design and Implementation
- Evaluation
- Channel Performance
- Conclusion

Background: Covert-Channel Attacks

Emerging security threats

"Hidden" communication channel

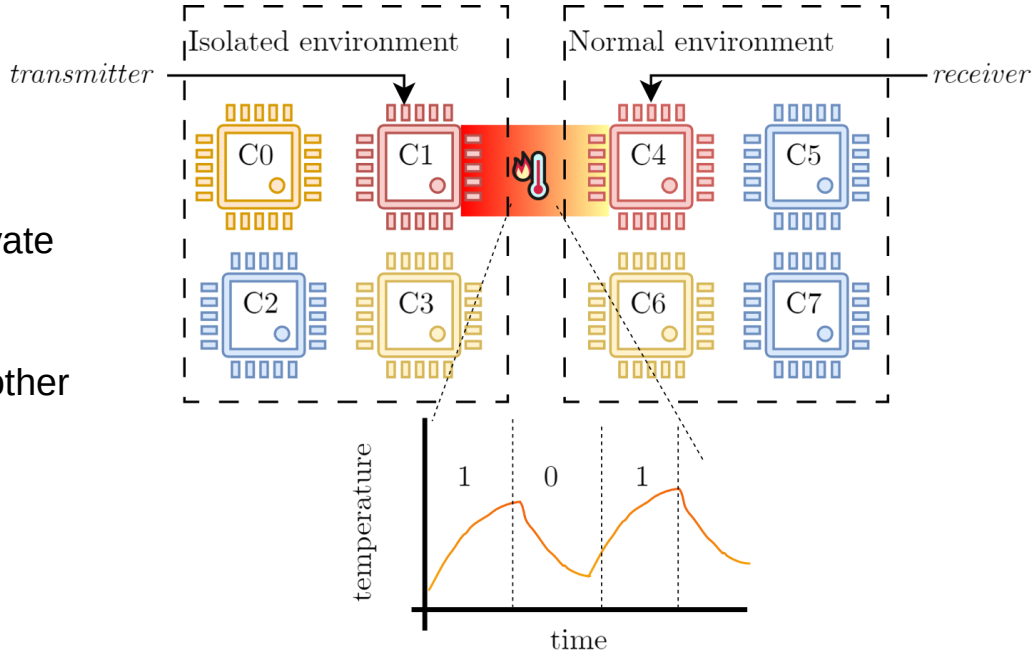
Goal: Extract information out of the (trusted) system



Thermal-based Covert Channel Attacks

Communication between two malicious applications through temperature.

- Power intensive, controlled CPU activity
- *Malware*: (isolated env) has access to private information.
  - ***Transmitter***
- *Spy*: (normal env) has access to I/O and other apps.
  - ***Receiver***



State of the Art

Trusted Execution Environments

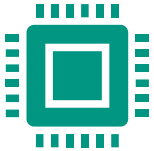
Assumption: TEEs ensure isolation between secure and normal worlds

Limitation: Vulnerable to covert and side-channel attacks

Thermal Covert Channels

Assumption: Temperature variations can enable covert communication

Limitation: Several state-of-the-art works are limited to simulation only



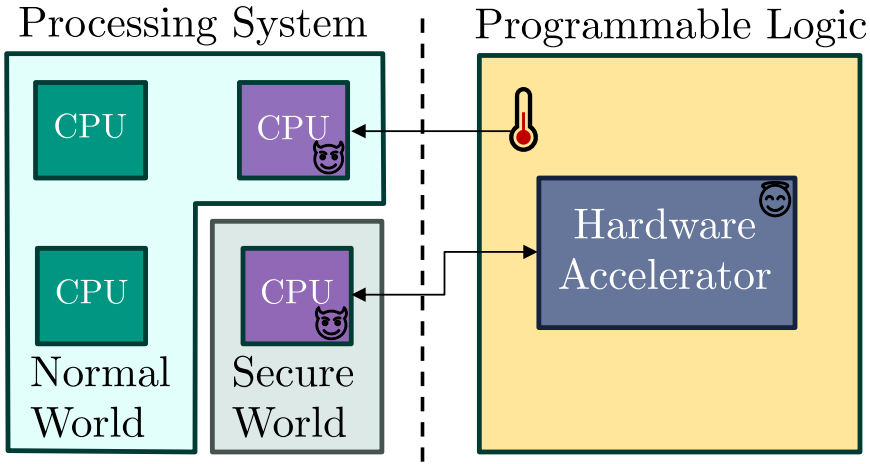
FPGA-based Covert Channels

Assumption: FPGAs enable covert channels via shared resources

Limitation: Detectable malicious hardware limits stealth

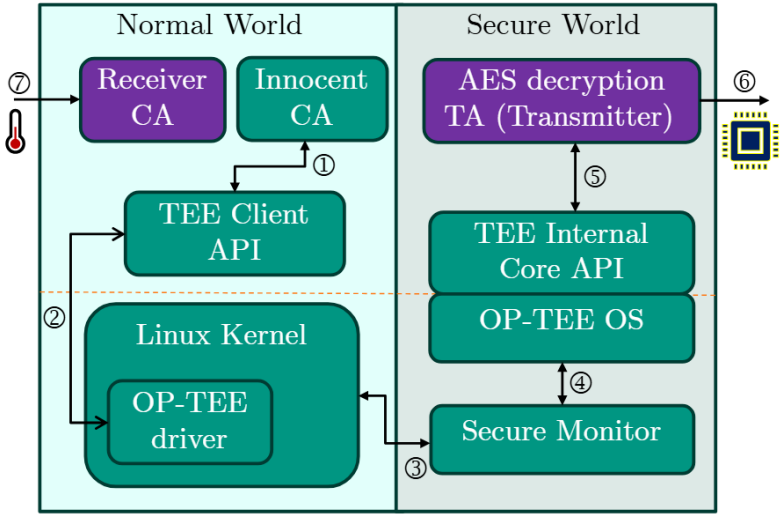
Through Fabric Hardware Design

- Thermal-based covert channel
- Targets FPGA-MPSoCs
- Breaks trusted execution environment
- Uses FPGA as a shared medium to transmit data and break isolation
- Open-source AES accelerator used as heating mechanism



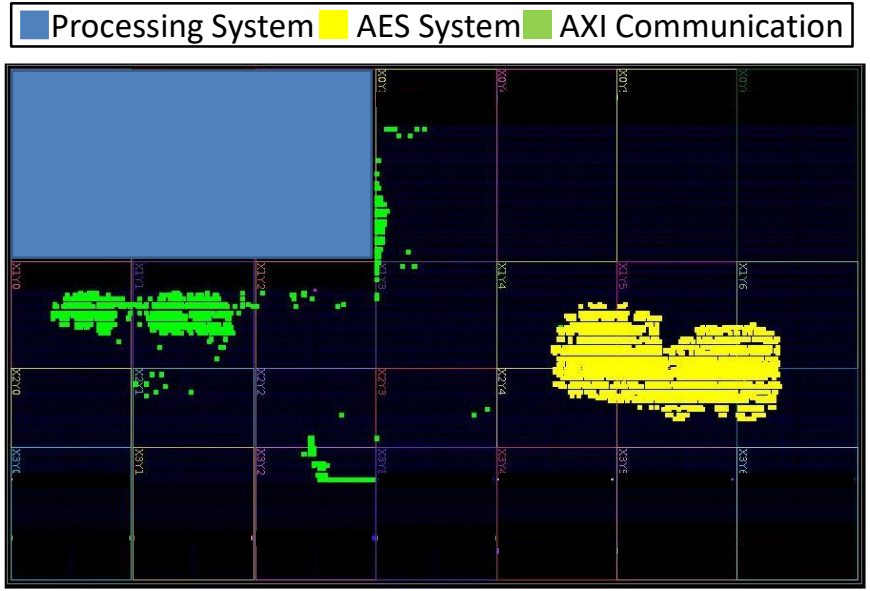
Through Fabric Software Components

- Innocent CA Request
  - OP-TEE API routes the request to the malicious TA
- Malicious TA Behavior
  - Performs decryption and leaks sensitive data via temperature modulation
- Receiver CA Action
  - Malicious CA reads FPGA temperature



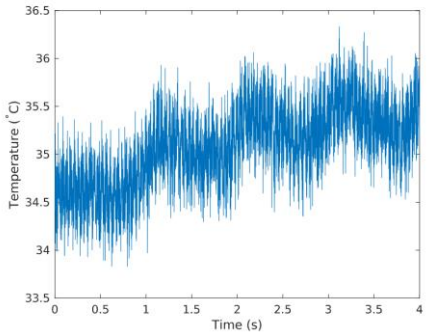
Through Fabric Implementation

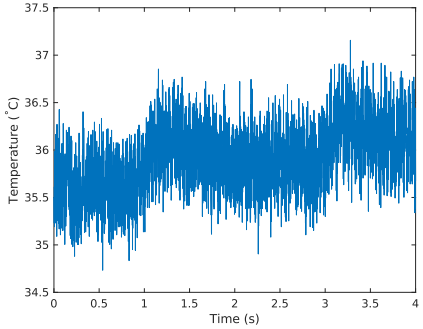
- Transmitter Hardware
  - Uses AES decryption accelerator on ZCU102 as a heating engine
  - ‘1’ bits raise temperature ‘0’ bit cools down
- Receiver Software
  - Monitors FPGA temperature in normal world
  - Uses FFT to filter signals
  - Threshold-based detection of received data

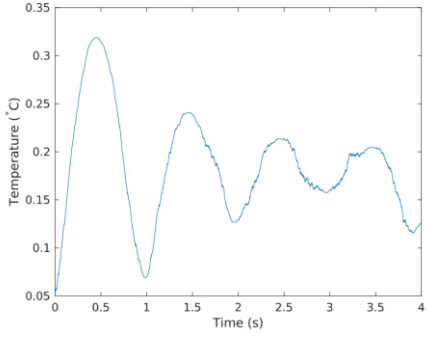


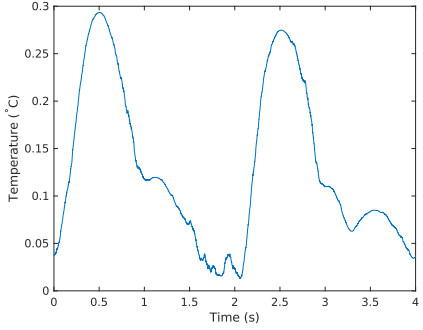
Data Transmission

- Receiver continuously monitor the temperature sensor
- Raw readings show no useful information
- After filtering at the desired frequency
  - Patterns immerge
  - Data can be identified as 0s and 1s







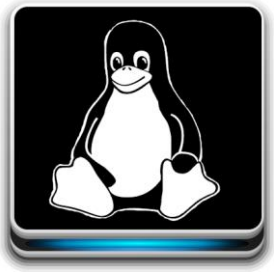


Evaluation Framework

- Board: AMD/Xilinx ZCU102
  - CPU: Quad-core Arm® Cortex®-A53
  - PL:

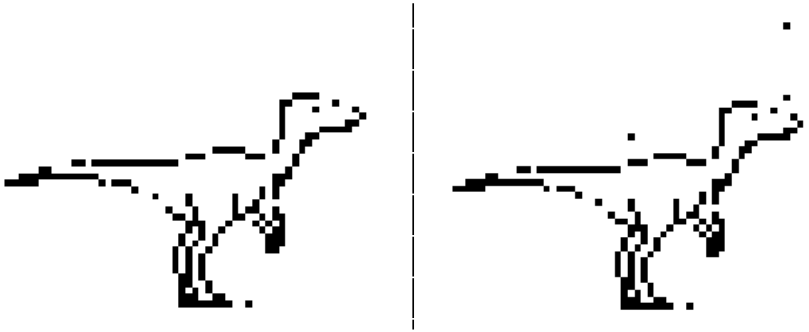
System Logic Cells (K)	600
Memory (Mb)	32.1
DSP Slices	2,520

  - Operating Systems:
    - Secure World: OPTEE
    - Normal World: Custom Linux (Petalinux SDK)



Results: Channel Metrics

- 1000 packets each one byte
- Low error rate per bit and packet
- Successful transmission of images



Metric	Value
Bits	8000
Packets	1000
Transmission Rate (bps)	2
BER (%)	1.9
PER (%)	4.3

Results: Resource Utilization

- 2 out of 4 Processors
  - One running normal world
  - One running isolated TA
- 14K LUT out of 200K LUT
- PL runs at 100 MHz
  - Enough for modulating the temperature
- PS runs at 1.2 GHz

Component	LUT
AES	11000
AXI	3100

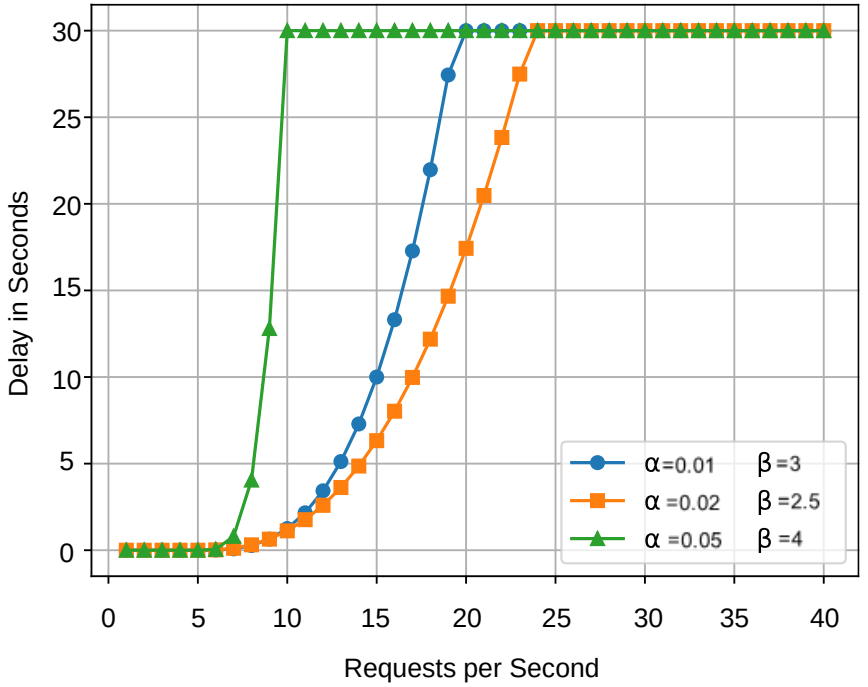
Comparison to Related Works

Our work is the only one not requiring any malicious hardware for transmitter or receiver

Work	Requires malicious transmitter	Requires malicious receiver	Covert channel type	Breaks TEE
Ours	X	X	Temperature	√
TODAES'21	√	√	Voltage	X
HOST'23	√	√	Frequency	X
Crypto'23	X	√	Voltage	X
ICCD'19	√	√	Voltage	X
Euro S&P'23	X	√	Frequency	X
TRETS'22	X	X	PCIe	X
TRETS'19	√	√	Inter. Wiring	X

Possible Countermeasure

- Software based delay
  - Increasing delay with usage of accelerator
  - Disturbs the transmission in time domain
- Based on α and β
  - Faster disruption of transmission
  - Lower overhead for normal applications



Conclusion

Proposed a Thermal Covert Channel	Utilizes a benign hardware accelerator in FPGA-MPSoC to enable covert communication
Effective Communication	Achieved 2 bps transmission rate with minimal bit and packet error rates
Broke TEE Security	Demonstrated how the attack compromises TEE isolation and data confidentiality within the OP-TEE framework
Proposed Countermeasures	Discussed potential solutions to mitigate accelerator-based covert channels

Karlsruhe Institute of Technology

Thank you for your attention!

More information about our research: Scan the QR!