Cryo-Mechanical Memory Extraction Against Modern Embedded Systems

Yuanzhe Wu, Dr. Grant Skipper, Dr. Ang Cui
IEEE Symposium on Security and Privacy Workshop
WOOT'23

This material is based in part upon work supported by the United States Air Force and DARPA under Contract No. FA8750-18-C-0127. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Air Force and DARPA. Distribution Statement "A" (Approved for Public Release, Distribution Unlimited).

Traditional Cold Boot Attack

- A method to extract sensitive data from a device's volatile memory (RAM) after a power cycle or system reboot
- Exploiting the Memory Remanence Effect: data in volatile memory (RAM) remains accessible for a short period after power is lost: Rapidly cool down the memory modules to slow down data decay
- Common targets: Devices with removable memory modules, such as desktop computers and laptops

Limitations of traditional cold boot attacks

Limited applicability to embedded systems or devices with non-removable memory modules

Dependence on standardized connectors or custom kernel/bootloader for successful memory extraction

Tradition Cold Boot Attack with DIMM slot and cooling spray[1]

[1] Halderman, J. Alex, et al. "Lest we remember: cold-boot attacks on encryption keys." Communications of the ACM 52.5 (2009): 91-98.

Re-imagine Cold-Boot

Objectives: Develop a generalized and automated system for reliable RAM content extraction against modern embedded devices

Challenges:

- Memory modules soldered onto PCBs
- Memory Readout methodology
- Physical Memory Reconstruction
- Virtual to Physical Memory Correlation
- Mechanical Challenges

Cryo-Mechanical Apparatus

A generalized, automated system designed for reliable RAM content extraction on modern embedded devices

Built using low-cost, widely available COTS hardware

Supports target devices with single or multiple DDR memory chips

Custom memory socket for devices with soldered memory modules:

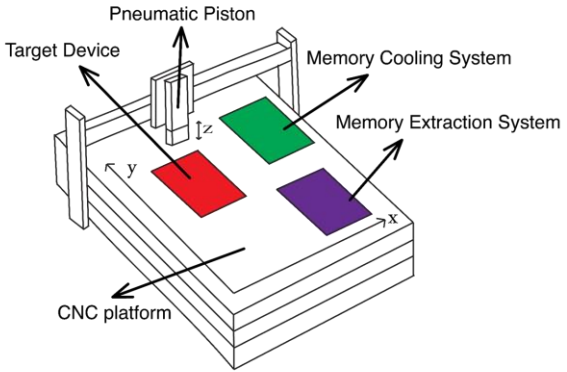
- Enables memory extraction on devices without standardized connectors

Cryogenic cooling mechanism:

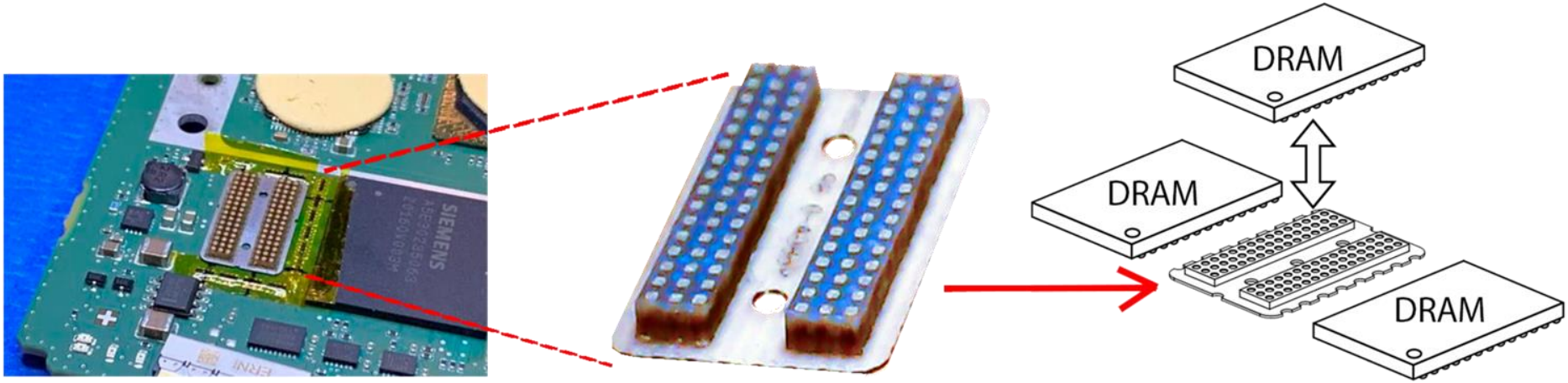
- Ensures memory content preservation during the extraction process

Enhanced spatial and temporal precision

- Enhanced spatial and temporal precision



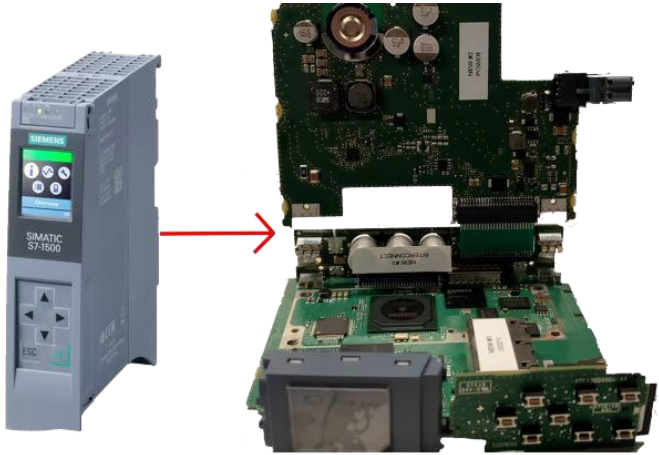
Integrated Circuit Test Sockets



New method for transferring embedded memory chips, such as BGA DRAM chips that are soldered on the embedded device printed circuit board (PCB) board. Our designed conductive rubber can make all the memory removable at runtime without affecting the function of the target device.

Target Device: Siemens S7-1500 PLCs

- Adoption in critical infrastructures (Critical Systems!)
  - Energy, Water, Transportation, Oil and gas: Nuclear facility
  - Manufactory and Building automation
- Stuxnet Target (early models) [2]
- Objective:
  - Determine how the S7-1500 PLC is protecting itself from adversarial activity.
- Challenges:
  - Encrypted Firmware!
  - No Debug Access (JTAG, Serial, etc)
  - Opaque Boot Process

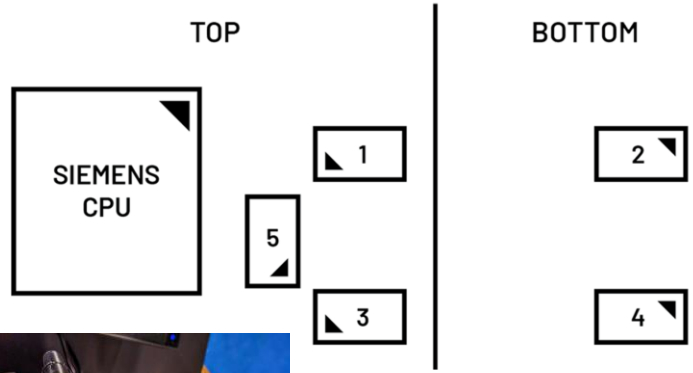


[2] N. Falliere, L. O. Murchu, and E. Chien, “W32. stuxnet dossier,” White paper, symantec corp., security response, vol. 5, no. 6, p. 29, 2011.

Timing Analysis for Memory Extraction

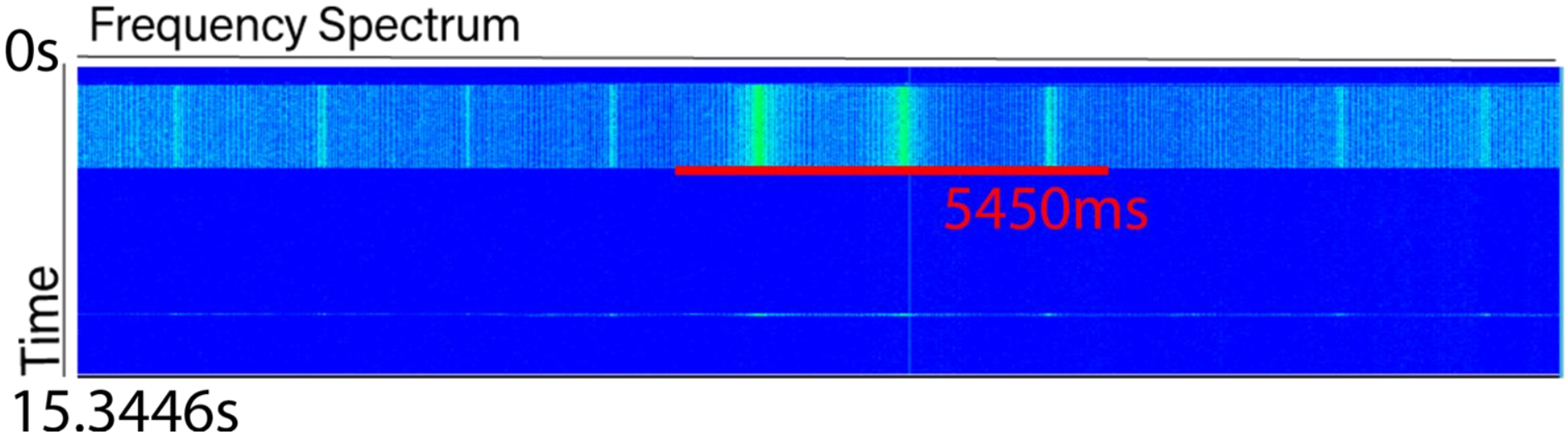
Challenge: 5 dedicated DDR2 DRAM chips soldered on PCB

Solution:
- Noninvasive side-channel based technique for determining optimal timing
- Electromagnetic analysis during boot process
- Observing intensity of electromagnetic emanations with near-field probes, RF amplifier, and spectrum analyzer



Electromagnetic Probing for Timing Extraction

Electromagnetic emission spectrum of DDR2 chip

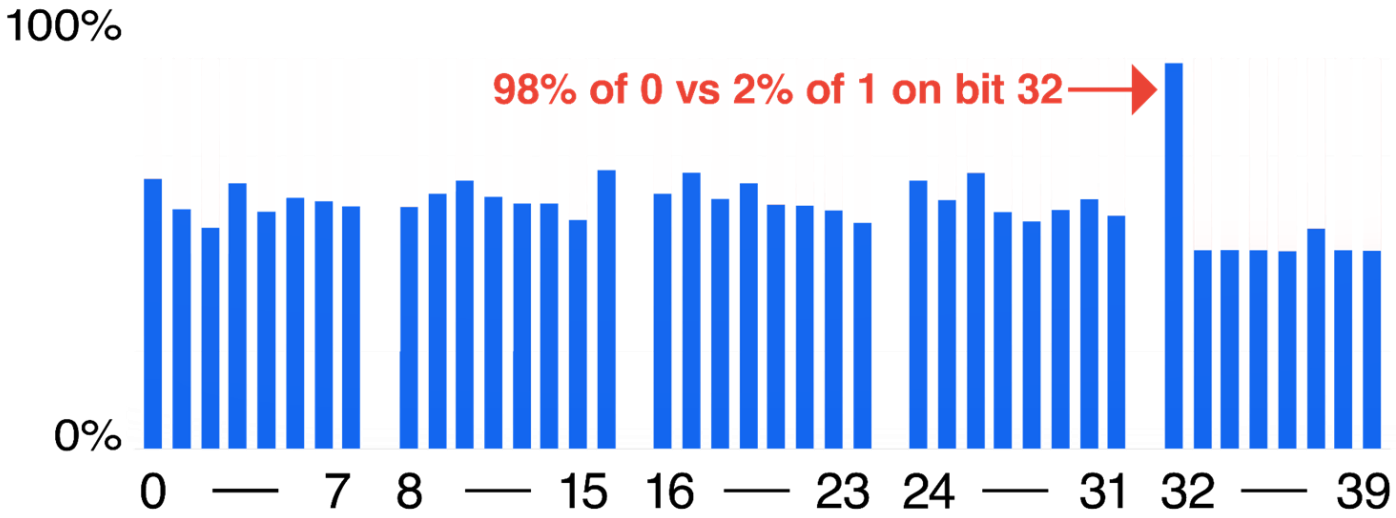


Reconstructing Memory Contents

Challenges:
- making sense of 40-bit word and its correlations with virtual memory

Hypothesis:
- MIPS instructions size is 32-bit word and the 8-bit could be used to as ECC correction.

Observation: Hamming ECC have 7 bits of ECC data for 32-bit data words.



Total 32+7=39 bits data line is needed as opposed to total 40 bits present. The 1 unused bit can be seen from this statistical distribution graph, which indicate the Hamming ECC is used in this Embedded system and the 5th DRAM chip contains the ECC data.

Unshuffling Memory with Known Plaintext

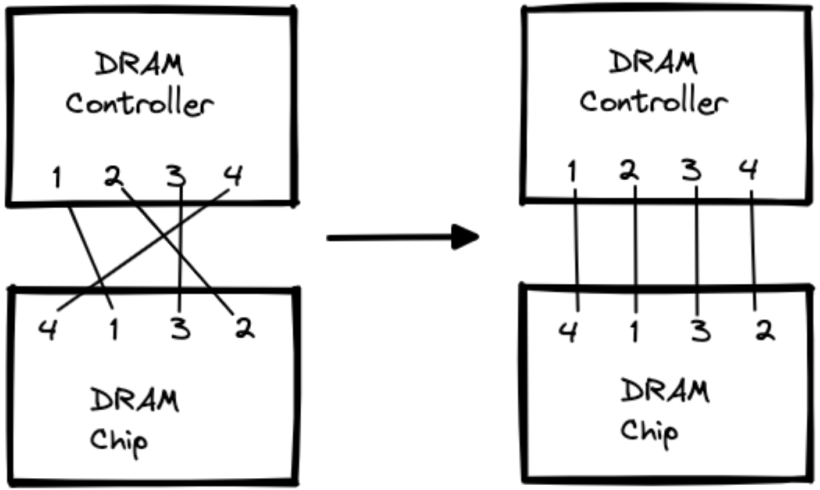
Identifying plaintext information from memory dumps

Searching permutations to find the closest match against plaintext

Using cryptographic constants for unshuffling strategy: AES S-Box

Using Hamming weight as an invariant

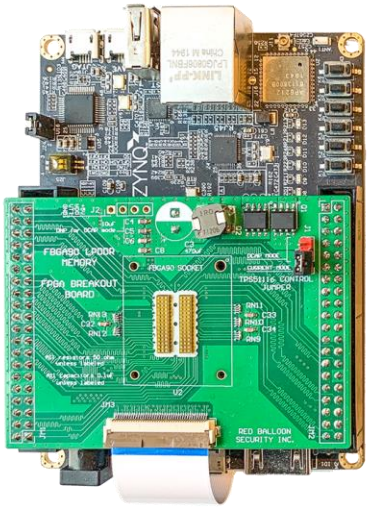
Identifying byte ordering and specific bit shuffling used by SIMATIC S7-1500

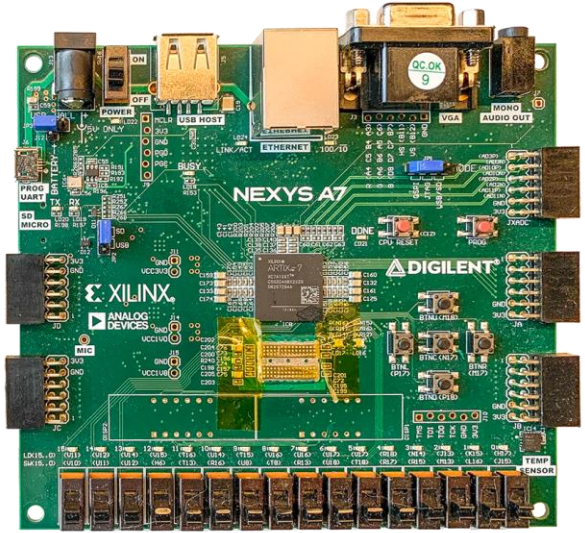


PCB routing pin swapping optimizations are used in Escape Interface Routing, such as memory controller with multiple data lines, which can be interchangeable for routing.

FPGA-based Memory Extraction Platform

- FPGA as a flexible and cost-effective solution
- AXI4 protocol for system-on-chip designs
- Digilent Nexys A7 board with conductive elastomer for DDR2 memory



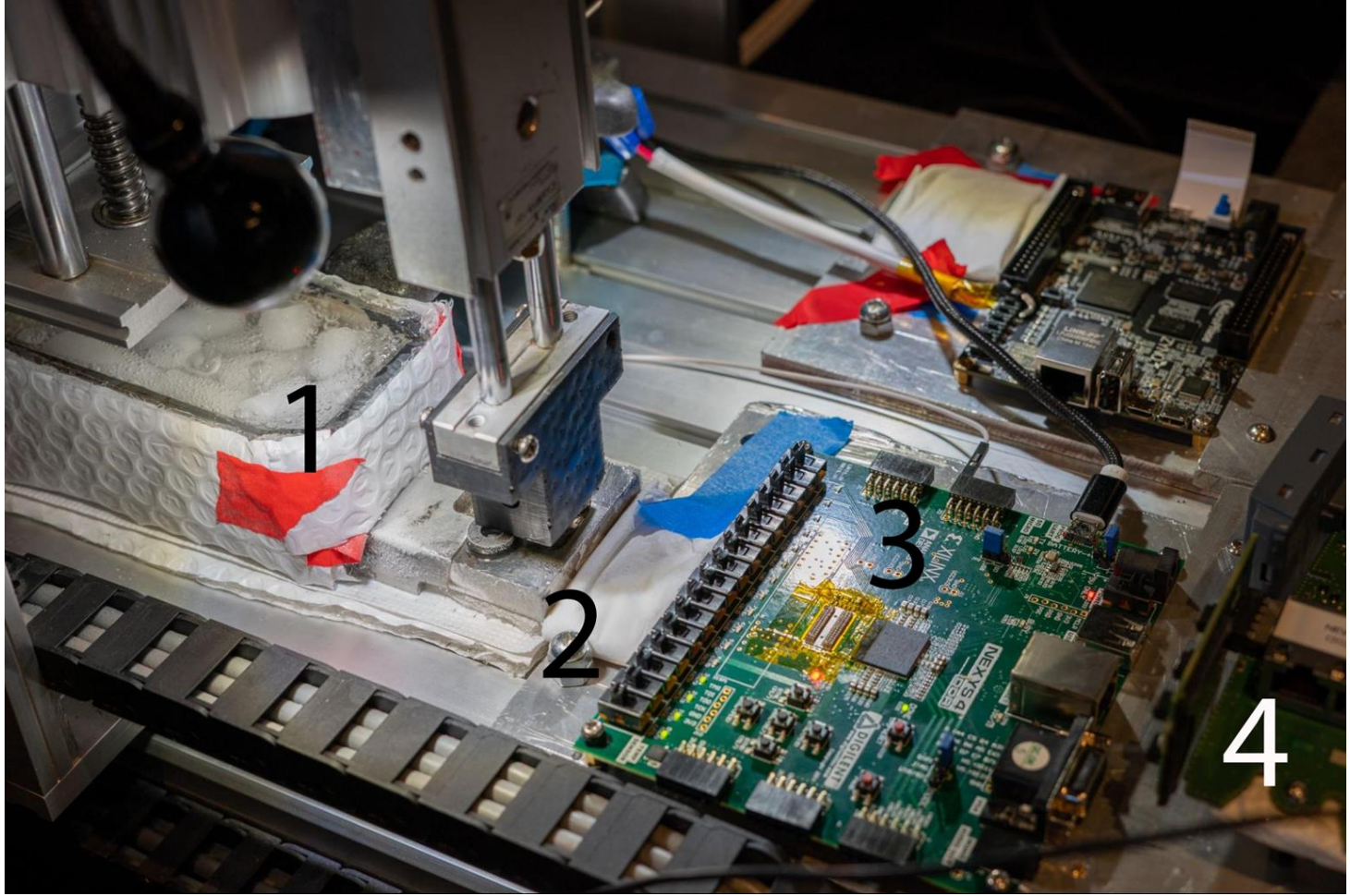


CNC Machine Modifications

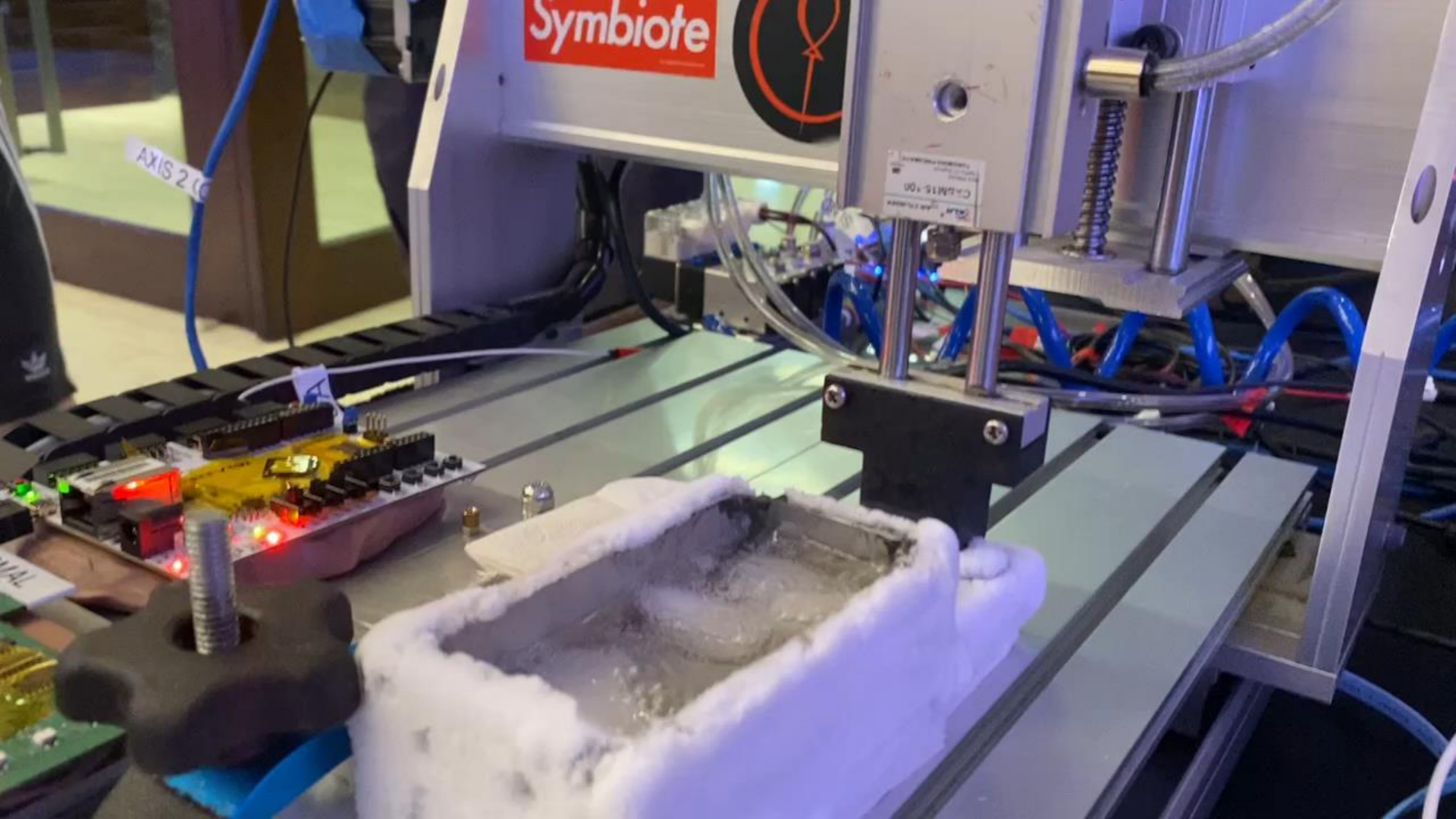
- Generic type 3040 CNC
- Replaced stock stepper motors with ClearPath MCPV stepper motors
- Replaced Z-axis drive system with SMC CXSM15-100 pneumatic linear actuator
  Controlled through ESP32 microcontroller board

Programmed sequence of motions:

- Submerging chip into the dry ice cooling bath
- Pressing chip against tissue paper to wipe excess isopropyl alcohol
- Positioning chip onto the target device
- Transferring chip to the FPGA readout platform

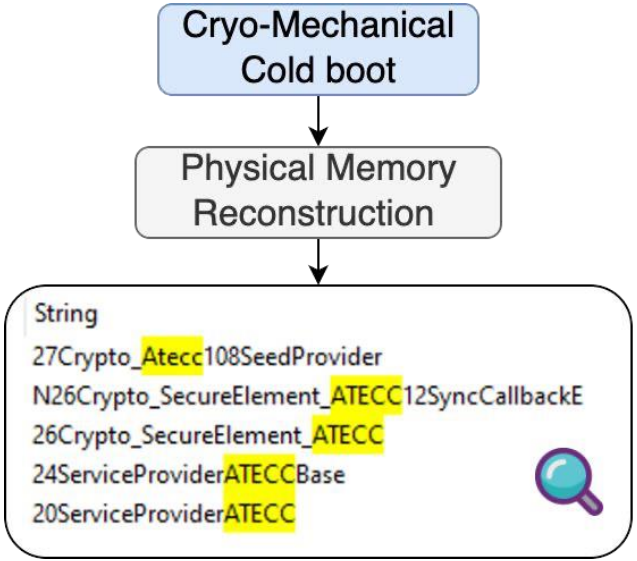


The apparatus setup for the new cold attack. (1) Memory cooling system (2) Tissue paper to wipe liquid (3) FPGA-based Memory extraction system (4) Target device


Symbiote

Revealing Trust

One single S7-1500 PLC can be used as an oracle to decrypt, re-encrypt, re-authenticate, tampered firmware for an entire generation of devices (Over 100 models affected). [3]



[07/22/2022] Privately disclosed to Siemens and interested partners.
[10/25/2022] Siemens assigns CVE-2022-38773.
[01/10/2023] Public release by Siemens: Siemens Security Advisory (SSA-482757: Missing Immutable Root of Trust in S7-1500 CPU devices)

Affected Product and Versions	Remediation
SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

[3] Y. Wu, G. Skipper, and A. Cui, “Uprooting trust: Learnings from an unpatchable hardware root-of-trust vulnerability in Siemens S7-1500 PLCs,” in 2023 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2023

Conclusion

Cryo-mechanical methodology extended cold boot attacks on embedded systems

Overcomes limitations of removable memory or code execution with debugging

Physically transfers discrete memory chips, reads data with FPGA, and reconstructs memory image

Demonstrated on Siemens SIMATIC S7-1500 PLC to recover encrypted firmware binaries

Adapting the procedure for DDR3 chips in Cisco IP phones, DDR4, and DDR5 (with higher costs for FPGA boards)

Acknowledgement

The authors would like to thank Jack Zheng and Aleksey Nogin from Red Balloon Security and WOOT anonymous reviewers for their feedback on the early versions of the paper.

Contact Me: yuanzhewu@gmail.com | hans@redballoonsecurity.com