REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
08-05-2016	Final Report	5-Jan-2015 - 4-Jan-2016

4. TITLE AND SUBTITLE
Final Report: Embedded Mobile Tactical Systems -- Reverse Engineering and Countermeasures

5a. CONTRACT NUMBER
W911NF-15-1-0044

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
106012

6. AUTHORS
Kevin T. Kornegay

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Morgan State University
1700 East Cold Spring Lane

Baltimore, MD 21251 -0001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
66315-CS-REP.1

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
The acquired instrumentation was used to assess a device's resistance to side-channel attacks (e.g. SPA, EMA, DEMA, DPA, and FI). The EM module provides electromagnetic SCA capabilities. It enables non-contact measurements for side-channel testing of complex systems and embedded system designs. Additional equipment includes an integrated receiver, a hardware down sampling module, EM probes, and software. Data capture, signal and visualization tools are included to support side-channel analysis, enabling rapid identification and isolation of side-channel signals from noise and interference.

15. SUBJECT TERMS
Side channel analysis, fault injection.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Kevin Kornegay
UU	UU	UU	UU		19b. TELEPHONE NUMBER 443-885-4869

Report Title

Final Report: Embedded Mobile Tactical Systems -- Reverse Engineering and Countermeasures

ABSTRACT

The acquired instrumentation was used to assess a device's resistance to side-channel attacks (e.g. SPA, EMA, DEMA, DPA, and FI). The EM module provides electromagnetic SCA capabilities. It enables non-contact measurements for side-channel testing of complex systems and embedded system designs. Additional equipment includes an integrated receiver, a hardware down sampling module, EM probes, and software. Data capture, signal and visualization tools are included to support side-channel analysis, enabling rapid identification and isolation of side-channel signals from noise and interference.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received Paper

TOTAL:

Number of Manuscripts:

Books

Received Book

TOTAL:

Received	Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

Internet of Things Security Endowed Professorship

Graduate Students

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Names of Post Doctorates

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Names of Faculty Supported

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period:	0.00
The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:.....	0.00
The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:.....	0.00
Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):.....	0.00
Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:.....	0.00
The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense	0.00
The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:	0.00

Names of Personnel receiving masters degrees

NAME

Total Number:

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

"See Attachment"

Technology Transfer

4. Statement of the Problem

In 2011, and later in 2013, the Cyber Priorities Steering Council presented a science and technology roadmap and initiatives that address a critical DOD problem which states, "the DOD lacks agile cyber operations and resilient infrastructure to assure military missions" [1,2]. There are many factors that contribute to this problem however one of particular interest and one that we will address in this research proposal, is that cyber systems are becoming increasingly more complex thus making them more susceptible to cyber attacks and difficult to defend. These systems utilize globalized commercial hardware that compromises the underlying cyber infrastructure. They have fundamental flaws in that they lack resiliency in their inability to stop attack spread and trustworthiness in that you can't trust the global supply chain for mission critical components. Malicious hardware insertions such as Trojan circuits that act as kill switches, sensitive IP extraction via hardware-based side-channels, and system disruption and diversion using backdoors in hardware all pose serious threats to the DOD cyber infrastructure. Embedded, mobile, tactical (EMT) systems comprise the physical layer of the cyber infrastructure in the battlefield. At the core of these systems is a cryptographic device in the form of a field-programmable-gate array (FPGA), which is an integrated circuit that can be configured for a particular application by the user using a program written in a hardware description language. The program used to configure the FPGA is usually stored as an encrypted bitstream, which is loaded from external memory and exposed during power up. FPGAs, like most hardware such as custom logic in application specific integrated circuits and standard CPU chips executing cryptographic software or firmware, leak information through side-channels. These unintended side-channels include the instantaneous power consumption of the hardware, radiated electromagnetic fields, or timing information. Side-channel analysis (SCA) is a passive reverse engineering (RE) technique used to reveal the encryption key via noninvasive side-channel monitoring. SCA attacks can only be effective while the hardware is performing cryptographic operations. SCA attacks have been used successfully to uncover the encryption key of several commercial FPGAs [3]. Countermeasures are necessary to secure the EMT system's ability to withstand SCA attacks, and sustain or recover critical functions. The U.S. DOD's anti-tamper security policies and other security requirements mandate that devices include countermeasures against SCA. Therefore, our research objective is twofold: 1) to assess the vulnerabilities of a state-of-the-art FPGA system using SCA; and 2) to develop countermeasures to mitigate SCA attacks. More importantly, the instrumentation acquired with this award has helped us establish side-channel analysis and fault injection capability. Additionally, the instrumentation was augmented by education and outreach activities that allow Morgan State University (MSU) meet DOD's workforce demand for US engineers with the requisite skill set to work in cyberspac.

5. Summary of the Most Important Results

The instrumentation purchased with this award includes the following.

- **Agilent N9030A PXA Signal Analyzer --** to provide real-time SDR spectrum measurements for countermeasure analysis.
- **Tektronix DPO 7104 Oscilloscope** – for data capture and display.
- **Zynq SDR II Evaluation Kit** -- this kit enables a broad range of transceiver applications for wireless communications. Tuned to a narrower RF range in the 2400 – 2500 MHz region, the kit is ideal for the RF engineer seeking optimized system performance meeting datasheet specifications in a defined range of RF spectrum.

The acquired instrumentation was used to support a wide variety of reverse engineering research activities. Several typical configurations are illustrated below.

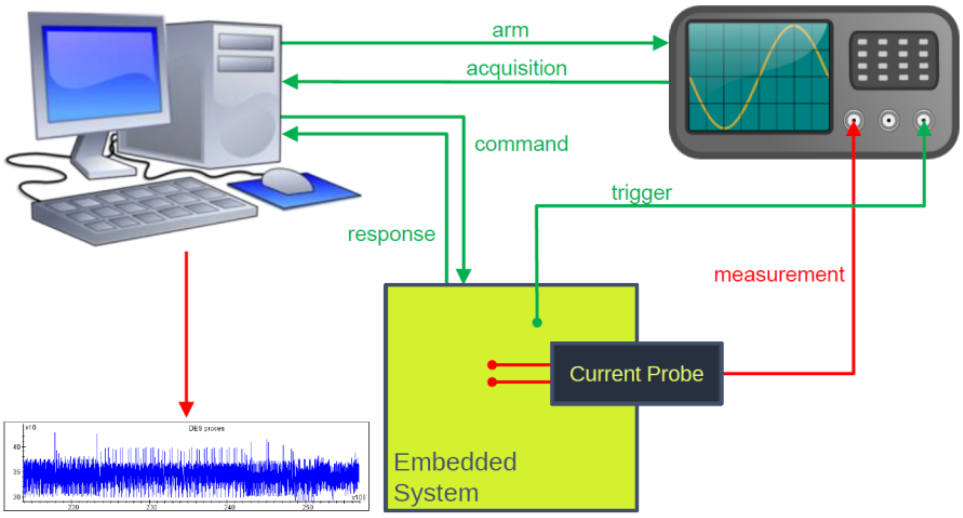


Fig. 1: Embedded system SCA configuration.

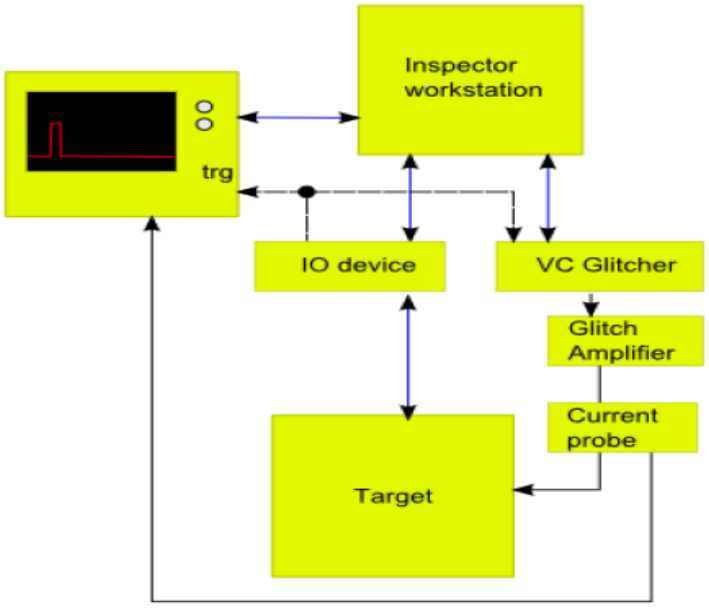


Fig. 2: Embedded system FI configuration.

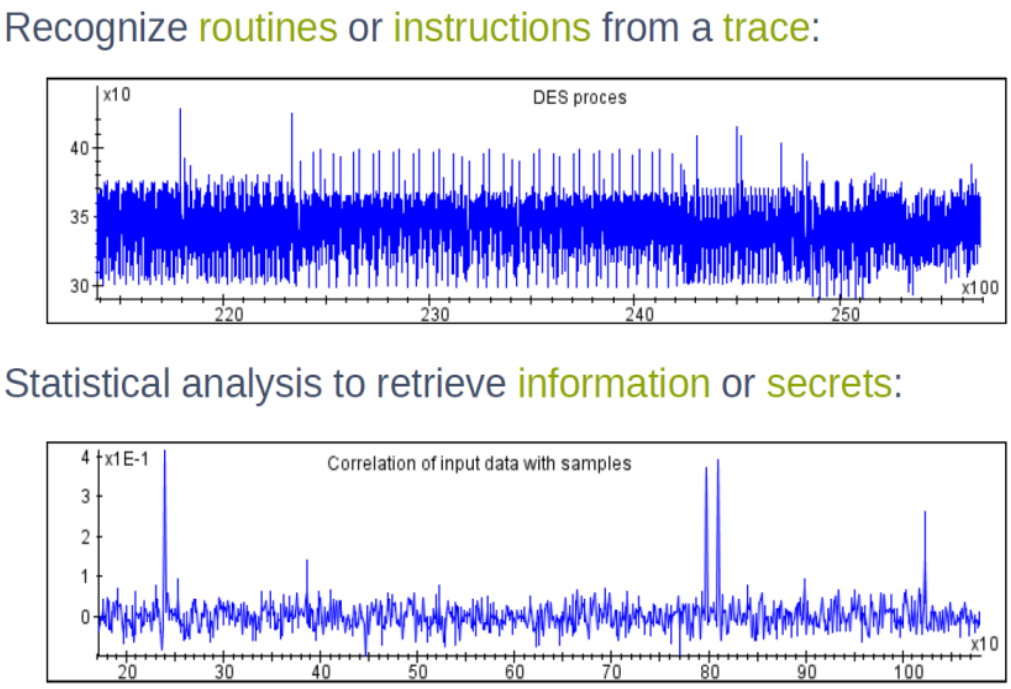


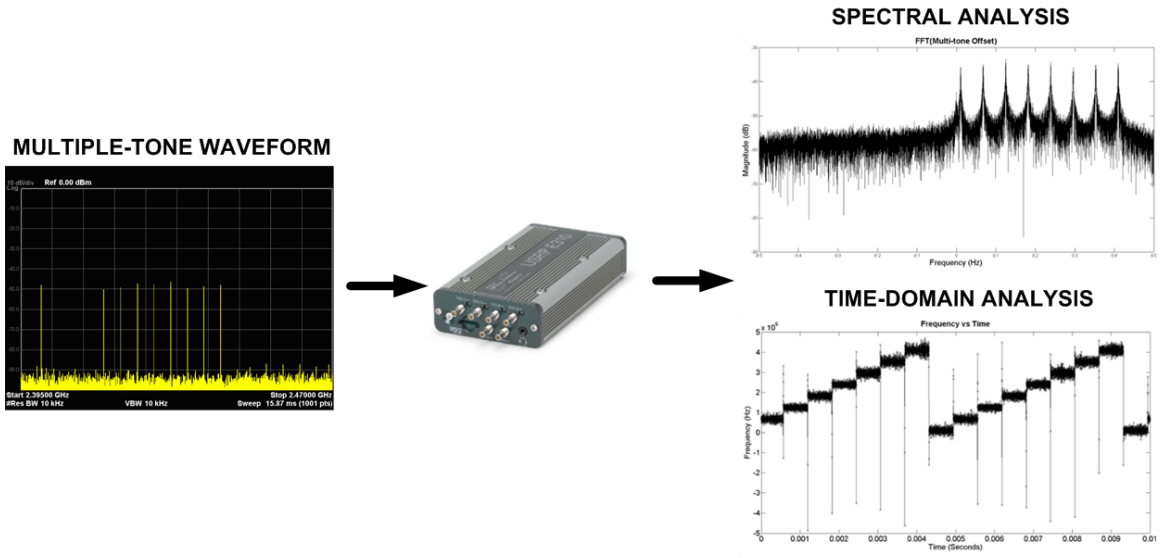
Fig. 3: 16-Bit DES SCA attack example.

New capabilities established with instrumentation.

- Side channel analysis
  - Simple power analysis
  - Differential power analysis
  - Correlation power analysis
  - Differential electromagnetic analysis
- Fault injection
  - Power and clock glitching
  - Electromagnetic pulse
  - Laser

Agilent N9030A PXA Signal Analyzer

The instrumentation has been fully integrated into CETACT and Embedded Systems Cybersecurity Research laboratories to support the design and evaluation of embedded systems. During the performance period, the instrumentation was leveraged to support the design and evaluation of a frequency-hopping receiver for a funded project. The following spectral and time-domain verifications were performed as illustrated in the below figure.



Research Impact: Without the instrumentation, we would not have been able to perform the verification of the frequency-hopping capabilities and develop the technical expertise in designing with industry-leading, low-cost software-defined radio platform. As directed result of this work, we are in position to securing additional funding from industry and government sources. Lastly, we envision this instrumentation will impact our new activities in the area of embedded hardware security.

Student Impact: Graduate and undergraduate students have been trained on the using the instrumentation to support their research projects. Community access to the instrumentation for faculty and students as a part of the Center for Reverse Engineering and Assured Microelectronics. (CREAM)

Bibliography

[1] Cyber S&T Priority Steering Council Research Roadmap. (2011, November 8). Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a554675.pdf.

[2] Defense Cyber S&T Strategies and Initiatives. (2013, July 23). Retrieved from http://www.dhs.gov/sites/default/files/publications/csd-sbir-2013-drsteven-king.pdf.

[3] Paul Kocher, Joshua Jaffe and Benjamin Jun, "Differential Power Analysis", *Advances in Cryptology CRYPTO'99, Lecture Notes in Computer Science (LNCS)*, vol.1666, Springer Verlag, Berlin, pp. 388-397, Aug, 1999.