Intel Labs
University Research Office
University Collaborative Research

FAPESP-Intel Joint CFP on Side-channel Resistant Security for SoC Devices

São Paulo, Brazil
June 5, 2014

David Ott, University Research Office

Abstract

FAPESP-Intel Joint CFP on Side-channel Resistant Security for SoC Devices

Broadly, a *side-channel attack* refers to the use of physically observable characteristics of a system or device to deduce internal states and gain access to protected information (e.g., cryptographic keys). *Countermeasures* refer to hardware or software techniques that reduce or eliminate side channel information available to an attacker, thus protecting a system or device against side channel attacks. While previous work has explored side channel attacks and countermeasures in length, Intel believes there is much more to be done in the design and development of side-channel resistant security specifically for lightweight SoC devices. Such devices are characterized by their:

- Physical exposure to attackers who may have unlimited access to the device,
- Limited computation, memory, and storage resources,
- Limited power resources (following from battery constraints),
- Exposed data communications via wireless communication channels (which are inherently broadcast),
- Frequently sparse patterns of data transfer, and
- Narrowness of device functionality and close coupling with its operating environment.

FAPESP and Intel invite proposals from São Paulo province academics in Brazil on novel approaches to side-channel resistant security for lightweight IoT devices. Research should address an important class of side-channel attack and a security solution or countermeasure demonstrating how resistance to that attack can provably be achieved. Approaches that are widely applicable to a variety of SoC device types and usage contexts, those that look more deeply at quantifying the threat of side channel vulnerabilities, and those that result in a better theoretical understanding of what is possible given lightweight SoC device constraints are of particular interest. In this session, we will discuss the CFP in some detail, including basics of the research agenda, areas of interest, and various goals to be achieved by proposed approaches.

Our Future

The IoT Device Trend (Evans, D. *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything.* Cisco Systems. April 2011)

- 25 billion devices by 2015
- 50 billion by 2020

Areas of Rapid Proliferation:

- Consumer electronics (digital cameras, media players, GPS devices, gaming)
- Mobile communications (smart phones, feature phones, cellular base stations)
- Health and medicine (diagnostic equipment, patient monitoring devices, medical imaging)
- Transportation (vehicle control systems, traffic monitoring and regulation)
- Energy (smart meters, climate sensors, energy management systems)
- Security (surveillance and monitoring devices, home alarm systems)
- Industrial applications (control and monitoring, quality management)
- Commerce/Retail (supply and merchandise management, point-of-sales devices)

Lightweight SoC Devices

What makes securing lightweight SoC devices hard?

Design Constraints

- Size and cost constraints
- Integration of third party IP modules

Resource Constraints

- Limited hardware resources (processor, memory, storage)
- Limited power resources (follows from battery constraints)

Exposure

- Physical exposure of devices to attackers who have unlimited access to the device
- Exposed data communications via wireless communication channels (inherently broadcast)

Usage Context

- Lack of administrative configuration or management
- Frequently sparse patterns of data transfer
- Narrowness of device functionality and close coupling with its operating environment

Side Channel Attack

Side-channel attack: Use of physically observable characteristics of a system or device to deduce internal states and gain access to protected information (e.g., cryptographic keys).

Examples of *side-channel information*:

- Variations in execution time,
- Variations in power consumption,
- Variations in electro-magnetic emanation,
- Variations in acoustic behavior, and
- Unexpected behavior caused by induced faults on the device or system.

Canonical approach:

- Examine side-channel information in a fine-grained and/or statistical manner
- Study the behavior of a system as it executes a particular instruction, a sensitive operation, or an entire algorithm
- Correlations between system behavior and input data are explored to look for *information leaks*
- May reveal a targeted secret directly, supply intermediate data within the underlying computation, or provide clues about the underlying structure or format of computation
- Side-channel information often has the effect of reducing entropy within a cryptographic scheme

Examples of specific side-channel attacks:

Simple Power analysis (SPA), Simple Electromagnetic Analysis (SEMA), Timing Analysis (TA), Differential Power Analysis (DPA), Differential Electromagnetic Analysis (DEMA),Pro filing Analysis, Differential Collision Analysis (DCA), Higher Order Differential Side-Channel Analysis, e.g. second order DPA, Multivariate Analysis (Template Attacks), Simple Fault Analysis (SFA), Differential Fault Analysis (DFA), and Stochastic Approach.

SCA Countermeasures

Countermeasure: Hardware or software techniques that reduce or eliminate side channel information available to an attacker, thus protecting a system or device against side channel attacks.

Example SCA countermeasures:

- Structuring cryptographic algorithms to be isochronous across all inputs
- Use of random timing delays
- Power line shielding, conditioning, and filtering
- Randomizing data before execution (blinding)
- Adding random values to sensitive data (masking)
- Introducing noise into side channel information
- Reducing statistical correlations
- Insuring that an execution path does not depend on secret values (i.e., PC-secure)

Other Sources of Information Leakage

1. Data Communications

- Patterns in encrypted data communications (e.g., wireless communications) that reveal information about secrets either within the data stream itself or on the communicating device.
- Examples: packet number, packet sizes, transmission timing, or receiver response patterns
- Attacker looking to do cryptographic analysis of a secure communication protocol or to identify nature and format of a data exchange,
- Attacker may deduce information about device state and cryptographic operations

2. Software Execution Context

- Examples: CPU usage metrics, instruction analysis (e.g., branch prediction analysis), cache usage, register analysis, I/O patterns, and so on.
- Attacker reconstructs a full or partial instruction path of program execution and uses to deduce internal state
- Attacker reduces entropy protecting data from cryptographic attack

CFP: The Research Challenge

Side-channel resistant security for lightweight SoC devices

Summary: Develop countermeasure approaches that address the threat of side-channel attack in lightweight SoC devices

Driving motivations for Intel:

- Better understanding of the side channel threat in SoCs
- Better theoretical understanding of countermeasure approaches (and limitations) given device constraints
- How to design more secure SoC devices for the rapidly expanding IoT space?

Research Goals

CFP: Side-channel resistant security for lightweight SoC devices

Threat Model

- **Goal 1:** Demonstrate the side channel attack and quantify its requirements and complexity. Requirements are demonstrably feasible, making the threat of high importance.

Solution/Countermeasure Robustness

- **Goal 2:** Solution or countermeasure increases side-channel attack requirements by 10x-100x or makes it provably infeasible.

Resource Requirements

- **Goal 3:** Resources required to implement the solution or countermeasure do not exceed 10-15% of overall device resources, or do not add more than 10-15% resource overhead beyond an existing approach. Resource usage includes:
  - Power requirements
  - CPU, memory, storage
  - Wireless radio usage

Also desirable:

- Widely applicable to a variety of SoC device types and usage contexts,
- Approach looks more deeply at quantifying the threat of side channel vulnerabilities
- Better theoretical understanding of what is possible given lightweight SoC device constraints

Research Vectors

CFP: Side-channel resistant security for lightweight SoC devices

RV1: Cryptography. Algorithms and technologies that create, adapt, extend, or implement core cryptographic technologies in side-channel resistant manner for lightweight SoC devices.

- Block and stream ciphers
- Symmetric key cryptography
- Public key cryptography
- Hash algorithms
- Digital signatures and message authentication codes

RV2: Data Communications. Countermeasures that make SoC-based device communications secure against side-channel attack. Emphasis on wireless data transmissions which are broadcast in nature.

- Application of cryptography to communications protocols
- Approaches to key management
- Application-level communication protocols
- Communication within sensor networks
- Device-to-device communication
- Client/server communication

Research Vectors

CFP: Side-channel resistant security for lightweight SoC devices

RV3: Software. Countermeasures and techniques for making SoC software robust against side channel attacks. Solutions should consider the software execution context of the device and the manner in which attackers may use basic hardware state information to attack application-specific secrets.

- Cache management
- Execution time management
- Branch prediction logic
- Memory layout and access patterns
- Algorithmic masking
- Fault response and handling logic
- Operating system support
- Compiler-based countermeasures

Proposal Format

- **Cover page {1 page}**. Title of proposal, name(s) of author(s), contact information, name of university, funds requested, the amount of cost share (if any)
- **Executive summary {1 page}**. Define the problem/challenge that this research will address, the effort's technical objectives/success criteria, and the basic proposed approach.
- **Relevance and impact claims {1-2 pages**}. This section is the centerpiece of the proposal. It should succinctly describe the uniqueness and non-incremental benefits of the proposed objective and approach relative to the state-of-the-art and current approaches.
- **Detailed technical rationale, approach, and constructive plan {2-4 pages}**. Details of proposed research. Proposals should address key issues along one or more of the above research vectors (or another topic still addressing program objectives and goals), and the rationale should include a basis of confidence for meeting the program metrics.
- **Statement of work, schedule, milestones, success criteria and deliverables {2 pages}**. Outline the scope of the effort including tasks to be performed, schedule, milestones, deliverables, and success criteria. It is understood that this is an exploratory research effort and schedules/deliverables reflect intentions rather than a firm commitment.

Proposal Format

- **Proposal team {1-2 pages}**. Summarize the members of the program team, their qualifications, and their level of participation in the project.
- **Other support {1 page}**. List other contributions by the Host Institution to this project (cash, goods, or services), if any, but not including items such as the use of university facilities otherwise provided on an ongoing basis. Note that authors of selected proposals will be required to present an original letter on university letterhead signed by the director of the Host Institution certifying the commitment of any additional support.
- **Fellowships {unlimited}**: The proposed budget may include costs for Scientific Initiation, Masters or Post-Doctoral fellowships.
- **Citations {unlimited}.**
- **Requested budget description {unlimited}**. Proposals must include separate budget descriptions for the items requested to FAPESP and to Intel. It is desirable to keep the fraction of the total amount requested for each of the parties at around 50%.

A Note on Evaluation Criteria

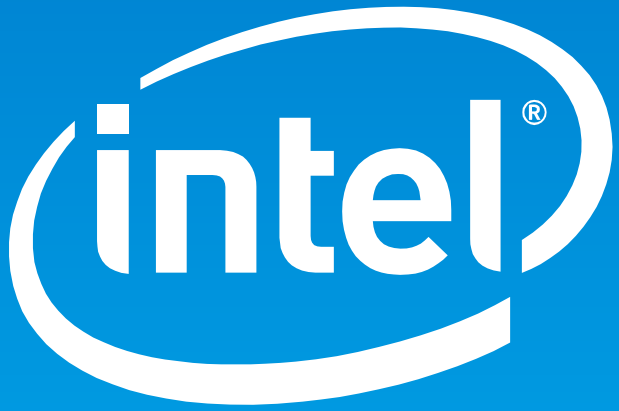
Two Key Points for Intel (within CFP):

Potential for technological innovation. The extent to which the proposal's problem formulation and key approaches are innovative, important, and relevant to the problem at hand. Novelty and ambition of the proposed academic research project, as it relates to the goals of this CFP. Potential for technological innovation as measured by comparisons with existing and competing technologies.

Potential contribution and relevance to Intel. The estimated degree to which proposals have a substantial potential for influencing the direction of Intel's long range technology plans.

Quick summary:

1. *Problem relevance*
2. *Innovation within SCA space*
3. *Potential for impact on Intel*


intel