Project Information

Project Title

TC: Large: Collaborative Research: 3Dsec: Trustworthy System Security through 3-D Integrated Hardware

Total Period

1 March 2010 through 28 February 2015 (CNS-0910734)
1 March 2010 through 28 February 2013 (CNS-0910389)
1 March 2010 through 28 February 2014 (CNS-0910581)

Current Period

1 March 2013 through 28 February 2014

Agreement Numbers

Agreement Number CNS-0910734 (Naval Postgraduate School)
  • Principal Investigator: Ted Huffmire
  • Co-Principal Investigator: Cynthia Irvine

Agreement Number CNS-0910389 (University of California, Santa Barbara)
  • Principal Investigator: Timothy Sherwood

Agreement Number CNS-0910581 (University of California, San Diego)
  • Principal Investigator: Ryan Kastner

Activities

Research and Education Activities

3-D circuit-level integration is a chip fabrication technique in which two or more dies are stacked and combined into a single circuit through the use of vertical electro-conductive posts. Since the dies may be manufactured separately, 3-D circuit integration offers the option of enhancing a commodity processor with a variety of security and reliability functions. A wide range of enhancements are possible, including a secure alternate service, passive monitoring, and isolation & protection.

During the current funded term of this grant, we have made significant progress in achieving our research objectives. Specifically, we have refined a framework with which
the function, economics, and complexity of security features can be isolated from the underlying computing hardware, and can be managed as customer-selectable fabrication options. Similar to co-processors, the lineage (e.g., venue of manufacture) of the additional layers is also separated from the commodity layer, enabling customized enhancement of the developmental assurance and reliability of add-on features.

Towards this goal, we have continued the development of a set of circuit-level primitives (described in our proposal in Research Objective 2: 3-D Configurable Base Layer Circuits and Optimization) that allow one layer to disable, tap, reroute, and override another layer. These efforts were recently published in the premier journal *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)* [5, 6]. To evaluate our approach to securing the supply chain through 3-D split manufacturing, we have developed application-level security solutions (described in our proposal in Research Objective 4: End-to-End Evaluation of the Control Plane for Security), and we developed functional FPGA prototypes (described in our proposal in Research Objective 1: Cost and Performance Analysis of 3-D Integration of Security Layers) [5, 6].

Regarding our ambitious and long-term goal to evaluate the effectiveness of our circuit-level primitives in silicon through tape-out of a 3D IC, we have made a course correction because no MOSIS 3D IC multi-project wafer (MPW) run was scheduled in 2012 or 2013, and no 3D IC MPW run is scheduled for 2014 either. Therefore, NPS has requested and received from NSF another one-year no-cost extension to continue conducting 3-D security research. In particular, we will explore applications such as 3-D extensible Instruction Set Architectures (ISAs), which allow a general-purpose CPU’s ISA to be extended with new security-related instructions by adding a control plane that contains the circuitry to implement the new instructions [1, 4]. We also plan to investigate the use of 3-D integration for efficient and secure network-on-chip (NoC) interconnect designs [2, 3].

While NPS has received another automatic one-year no-cost extension and is on schedule for the subsequent term, the current funded term is the final term for UC San Diego, and the previous funded term was the final term for UC Santa Barbara. Despite this, all three institutions have continued their weekly discussions. PI Huffmire attended an in-person project meeting at UC San Diego in January 2014 with PI Kastner, Kastner’s PhD candidate Jason Oberg, and Kastner’s postdoc, Dr. Jonathan Valamehr. In May 2013, PI Huffmire attended Valamehr’s dissertation defense at UC Santa Barbara [4]. Valamehr’s dissertation supervisor was PI Sherwood, and his committee also included Fred Chong, Peter Michael Melliar-Smith, and PI Huffmire.

**Findings**

We have found that our circuit-level primitives enable passive and active monitoring by one 3-D layer of another layer by adding a minimal amount of interface mechanisms to the layer that is monitored. These circuit-level primitives can be employed as part of a number of strategies to enhance the security of a computation plane (i.e., the plane that is
monitored) with a control plane (see Figure 1). This work provides a pathway for the high-assurance community to utilize high-performance hardware while shortening development cycles for trustworthy systems.

![Cross Section of 3D chip with two dies connected by vertical posts](image)

Figure 1: A 3-D chip consisting of two dies connected by vertical posts.

We have shown that a control plane, specifically dedicated to security, has the potential to implement a variety of security functions in a cost-effective and computationally efficient way. We are the first to develop a method of using 3-D integration for trustworthy system development. We have also shown how the 3-D control plane can be integrated in a purely optional and minimally intrusive manner with very minor modification to the commodity computation plane.

Training and Development

The 3Dsec project has provided training and development to many students, including at least one PhD student at each campus involved in this project. For example, Jason Oberg at UCSD designed a MIPS processor for the computation plane. Jonathan Valamehr developed the 3-D integrated cache monitor [29]. Oberg and Valamehr integrated the MIPS processor with a cryptographic coprocessor. Oberg is conducting research on detecting side channels in cryptographic hardware by using Gate-Level Information Flow Tracking (GLIFT) [14, 16, 21], and he is currently writing and preparing to defend his dissertation. Valamehr defended his UCSB ECE dissertation [4] in May 2013 and is currently a postdoc at UCSD CSE. CDR Michael Bilzor (U.S. Navy) at NPS developed a technique for detecting malicious inclusions [13, 25, 27]. Bilzor graduated in 2011 and is now a member of the faculty of the US Naval Academy [19]. In addition, this project has funded travel by those students to important conferences.

Outreach

To broaden the impact of our work, we have actively sought dissemination in a variety of venues. In addition to our publications, we describe other outreach activities below.
Research Experiences for Undergraduates (REU):

PI Kastner is working with several undergraduates as part of the REU supplements that UCSD has been awarded. Our current undergraduate researchers have provided much of our design testing infrastructure. For the 3Dsec project, we are required to use a wide range of design tools from Mentor Graphics’ ModelSim to Synopsys’ Design Compiler. Incorporating the outputs of each of these design tools in order to produce meaningful results requires a large amount of scripting. Our current undergraduates have greatly helped in this realm by building both Bash and Python scripts to better automate these design flows. By building a more ‘push button’ testing infrastructure, we have been able to more effectively test our designs and undergraduates have significantly aided us in this. In addition to helping develop the tools around testing our designs, our undergraduates have also greatly helped us automate data collection. We are often required to process many different designs to collect results such as area, delay, and power consumption. Rather than collect data for each of those components at a time, our undergraduates have done a tremendous job in setting up the scripts necessary for automatic data collection. They have helped us build the scripts that allow us to automatically collect large amounts of data with a very simple interface.

In 2013 and 2012, PI Huffmire continued to communicate regularly with David Marangoni-Simonsen, an undergraduate at Harvey Mudd College, who participated in a nine-week internship at NPS in the summer of 2011. Maraongoni-Simonsen’s accomplishments in the digital design and prototyping of 3-D applications have contributed to two of our recent publications [5, 6]. Maraongon-Simonsen is now a graduate student at Georgia Tech.

COSMOS:

PI Kastner teaches a California State Summer School for Mathematics and Science (COSMOS) cluster focused on the design and implementation of embedded computing systems. This is a four-week residential summer program for high school students. This past year saw a diverse set of students in the “Computers in Everyday Life” cluster [36]. In four short weeks, the students developed a variety of embedded computing systems including robots, vision and wireless controllers [26, 33]. We will incorporate the research within this proposal into one of the lectures discussing how computer are used in a variety of fields for image processing. It is especially important to provide these high school students, most of who will continue onto college majoring in computer science, computer engineering or electrical engineering, an accurate view of what they can do with these degrees. Unfortunately, the normal view of computing is sitting in front of a desktop programming, which couldn’t be farther from the truth for most college students graduating in these fields. Finally, this cluster is extremely hands-on, requiring more TA resources than made available by the program. We partially utilized graduate student summer support from this grant to fund additional teaching assistants for our COSMOS cluster.
Freshman Seminars:

Based upon the COSMOS experience, PI Kastner offers two freshman seminars quarterly, one focused on mobile phone programming and the other on robotics. Both of these provide an introduction to programming using frustration free languages (AppInventor and Python, respectively). It is known that these seminars are important for recruiting and retaining underrepresented minorities in engineering [31]. And with less than 20 students per class, and 3-4 TAs (volunteers students funded from NSF grants), it is an intimate environment for the students to not only learn basic CS concepts, but also do it in an interactive manner.

Contributions

Contributions within Discipline

The discipline of hardware-oriented security is growing in importance as attackers target the lowest level of system abstraction. Unlike traditional coprocessors, 3-D integration offers the ability to monitor and even override internal structures of a processor as well as the ability to offer a secure alternate service (e.g., cryptographic processing) at much higher bandwidth than a coprocessor. A 3-D integration approach also offers the ability to separate hardware resources by incorporating computational cores in physically distinct layers with separate lineage and developmental assurance. In summary, the key advantages of 3-D integration are (1) high bandwidth and low latency; (2) direct, granular access to chip features; and (3) controlled lineage (e.g., use of a trusted foundry). Additionally, we find the following general advantages: (4) the ability to change the economics of developing critical systems; (5) application-specific security enhancements to commodity hardware; (6) the ability to decouple security and non-security functionality, thus simplifying the design; (7) the ability to create "interfaces" to the commodity processor at chosen locations; (8) the ability to combine independently optimized dies into a single stack; and (9) the ability to reduce delay by locating electrical functions on the control plane close to their counterparts on the computation plane. In addition, all hardware security approaches share the advantages that, when they are designed to do so, they have the ability to operate below the lowest level of the software stack in terms of privilege and dependency; and they can impose strong spatial separation on the software components. Challenges specific to 3-D integration include (1) thermal cost, (2) design expense, (3) yield loss, (4) testing, and (5) the delivery of power and I/O.

Our contribution within the discipline of hardware-oriented security has been to (1) educate the community as to the security challenges and opportunities of 3-D system design; (2) develop novel techniques necessary to address an important subset of these problems; and (3) demonstrate the effectiveness of these techniques through the analysis of functional prototype designs. In the subsequent term of this project, we will develop additional 3-D systems that demonstrate the wide range of possible 3-D security applications. These systems will be physically realized as small functional prototypes on FPGAs (as described in our proposal Research Objective 1).
Towards our goal of developing primitives that can monitor, audit, track, and modify the flow of information on the computation plane (as described in our proposal in Research Objective 3: Novel Control Plane Architectures and Analysis Tools), we have developed a 3-D application for monitoring the execution of a general-purpose CPU to detect malicious behavior [13, 19, 25, 27]. This 3-D application has been physically realized as an FPGA prototype.

**Contributions to other Disciplines**

Outside of security, we have driven to demonstrate to the 3-D design community that our techniques are practical. We have demonstrated to the 3-D design community that it is possible to enhance a commodity integrated circuit with a separate layer that provides useful security functions without significantly impacting the performance or correctness of the commodity layer. Our design framework includes a set of circuit-level primitives that can be used by the 3-D design community. In the subsequent term of this project, our efforts to apply these circuit-level primitives to other 3-D systems and evaluate their feasibility in functional prototypes (e.g., FPGA and 3DIC) will provide valuable lessons for the practice of secure 3-D design.

**Contributions to Human Resource Development**

Here we have had outstanding successes. In particular, Jason Oberg at UC San Diego is writing and preparing to defend his dissertation on using Gate-Level Information Flow Tracking (GLIFT) [14, 16, 21] to detect side channel attacks on cryptographic hardware. Oberg also developed a MIPS processor for the computation plane. Jonathan Valamehr developed the 3-D integrated cache monitor [29]. Valamehr spent the summers of 2012 and 2010 as an intern at Intel Corporation and the summer of 2011 as an intern at Microsoft Research. Valamehr defended UCSB ECE dissertation [4] and is now a postdoc at UCSD CSE. Valamehr, Oberg, PI Sherwood, and PI Kastner, working with the NSF Innovation Corps (I-Corps) Program, have developed a commercial venture called Tortuga Logic that will allow their research contributions in the area of hardware-oriented security and trust to have impact in industry. CDR Michael Bilzor (U.S. Navy) developed a novel technique for detecting malicious inclusions at the Naval Postgraduate School [13, 25, 27]. Bilzor graduated in 2011 and is now a member of the faculty of the US Naval Academy, where we anticipate that he will have a significant impact far beyond the time frame of this grant as a professional researcher and educator of US Navy officers [19]. Lt. Dimitrios Megas (Hellenic Navy) and Lcdr. Kleber Pizolato (Brazilian Navy) completed their joint M.S. Thesis, Data Transformation in a Three Dimensional Integrated Circuit Implementation, in March 2012 [17]. LCDR Jay Elson (USN) completed his M.S. Thesis, Methods for Trustworthy Design of On-chip Bus Interconnect for General-purpose Processors, in March 2012 [18].

**Contributions to Resources for Research and Education**

Little of this grant was allocated for physical resources, with the exception of the cost of fabricating the 3-D integrated circuit as part of a Multi-Project Wafer. Most of the
resources required, including the CAD tools, FPGA boards, and workstations, were already available to the PIs. However, our 3-D design framework will serve as a building block for others who wish to continue exploring the research and educational aspects of this work.

**Contributions Beyond Science and Engineering**

The primary contribution beyond the research of science and engineering is to help establish security best practices within the 3-D design community and promote the adoption of 3-D integration as an efficient and effective method of enhancing the security of commodity integrated circuits. This has the potential to increase the security of trusted devices that depend on hardware to be inherently trustworthy.

**Publications**


