CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Information Technology

Proceedings of the 8th Prague Embedded Systems Workshop

November 6-7, 2020

Virtual event organized from Prague

Czech Republic

ISBN 978-80-01-06772-7

Editors:

doc. Ing. Hana Kubátová, CSc.

doc. Ing. Petr Fišer, Ph.D.

Ing. Jaroslav Borecký, Ph.D.

Message from the Program Chairs

The Prague Embedded Systems Workshop is a research meeting intended for the presentation of Ph.D. students' results and partial progress in their research in the field of all aspects of embedded systems design, including their testing, reliability, secure, safe, and low-power applications and communications. The workshop is organized annually by members of the Department of Digital Design of the Faculty of Information Technology of the Czech Technical University in Prague, for the eighth time this year. The main aim of PESW is to boost mutual discussions and establishing possible future cooperation between young researches not only inside EU. Therefore, the PESW workshop will be based on oral presentations and discussions.

This year, due to the Covid crisis, PESW has been shifted from June to November and organized only virtually with on-line live presentations.

There are three types of students' submissions and presentations at PESW 2020:

- Full papers describing the student's original research. These papers were submitted to a standard reviewing process
- Abstracts of authors' earlier published and successfully presented papers (at conferences, journals, etc.). These contributions were not reviewed; emphasis was put on the presentation and discussion
- Student posters - abstracts of defended Bc. and MSc. Theses with subsequent poster presentation

Eight papers were accepted for PESW 2020 presentation, from which there were 3 full papers and 5 abstracts. Contributions from Czech, French, and Italian university research teams were accepted this year.

The technical program is also highlighted by three keynote speakers in the areas of security, network monitoring, and approximate computing:

- Security in internet of (safety-critical) things.
  Speaker: Tomáš Martinec, SYSGO, Czech Rep.
- Graph-Based Models in Prediction and Projection of Cyber Attacks.
  Speaker: Martin Husák, Masaryk University, Brno, Czech Rep.
- Approximate Computing: Test and Reliability issues and opportunities.
  Speaker: Alberto Bosio, INL – Ecole Centrale de Lyon, France.

Four technical sessions were formed, with the following topics:

- Network traffic processing & Datasets
- Design and test it all
- Network traffic detection and classification
- To approximate or not to approximate?

Last but not least we would like to thank to our sponsors (CTU in Prague, EATON, SYSGO, CZ.NIC, ASICentrum, CESNET).
Special thanks go to IEEE: IEEE Student Branch at Czech Technical University in Prague and IEEE Young Professionals, organizing student contest, and Czechoslovakia Section of IEEE.

Hana Kubátová and Petr Fišer

Committees

Workshop Chairs

Hana Kubátová, CTU in Prague (CZ)

Petr Fišer, CTU in Prague (CZ)

Programme Committee

P. Bernardi, Politecnico di Torino (IT)

A. Bosio, École Centrale de Lyon (FR)

T. Čejka, CTU in Prague (CZ)

G. DiNatale, TIMA, Grenoble (FR)

P. Fišer, CTU in Prague (CZ)

J.L. Gaudiot, University of California, Irvine (USA)

K. Jelemenská, STU Bratislava (SK)

M. Jenihhin, Tallinn Univ. of Technology (EE)

L. Kekely, BUT, Brno (CZ)

P. Kitsos, TEI West. Greece (GR)

H. Kubátová, CTU in Prague (CZ)

I. Levin, Tel-Aviv University (IL)

A. McEwan, University of Leicester (UK)

N. Mentens, KU Leuven (BE)

M. Novotný, CTU in Prague (CZ)

A. Orailoglu, UC San Diego (USA)

Z. Plíva, TU Liberec (CZ)

E. Sanchez, Politecnico di Torino (IT)

J. Schmidt, CTU in Prague (CZ)

M. Skrbek, CTU in Prague (CZ)

B. Steinbach, TU Chemnitz (DE)

R. Stojanovic, Univ. of Podgorica Montenegro (ME)

R. Ubar, Tallinn Univ. of Technology (EE)

Z. Vašíček, BUT, Brno (CZ)

I. Vatajelu, TIMA - CNRS / Université Grenoble Alpes (FR)

P. Velan, ICS MUNI (CZ)

H.T. Vierhaus, Brandenburg University of Technology (DE)

M. Zachariášová, ASICentrum (CZ)

W. Zając, Jacob of Paradies University (PL)

Special Session on Network Security Chair

Tomáš Čejka, CTU in Prague (CZ)

Student Poster Session Co-Chairs

Tomáš Kolárik, CTU in Prague (CZ)

Jan Bělohoubek, CTU in Prague (CZ)

Organizing Committee

H. Kubátová, CTU in Prague (CZ)

P. Fišer, CTU in Prague (CZ)

M. Novotný, CTU in Prague (CZ)

R. Kinc, AMCA (CZ)

E. Uhrová, AMCA (CZ)

Contents

Technical Lectures

Turris:Sentinel - scalable collecting network (big) data in practice

Speaker: **Martin Prudek & Miroslav Hanák**, *CZ.NIC, Czech Rep.*

Turris:Sentinel is a data collecting and processing system deployed on thousands of Turris network devices. It gathers gigabytes of data about cyberattacks detected by minipots also running on Turris devices. Minipot stands for the minimal honeypot, which detects only connection and login attempts made by attackers. Sentinel represents the innovative state-of-the-art solution for centralized data collection from a high number of devices assembled around the globe and connected to the Internet. Collected data are processed in real-time while flowing through various interconnected Sentinel components called a pipeline. Sentinel is highly modular, extensible, and scalable thanks to the right combination of the right technologies and microservice architecture. The data serve as an input to Dynamic firewall, which automatically blocks detected attackers on all Turris devices. They are also analyzed with various clustering algorithms and are statistically inspected because they provide a unique and exclusive source of information about cyberattacks.

Martin Prudek

Martin Prudek graduated from cybernetics and robotics at the Department of Control Engineering, FEE CTU and now works at CZ.NIC as the guarantor of Turris:Sentinel. He is a Linux/GNU and open source enthusiast and occasional teacher at CTU.

Miroslav Hanák

Miroslav Hanák studied Computer Engineering at CTU FEE. Currently, he works at Laboratories of CZ.NIC as a software developer. He actively participates in the development of Turris:Sentinel data-collecting system, especially on its minimal honeypots component.

Keynotes

Security in internet of (safety-critical) things

Speaker: **Tomáš Martinec**, *SYSGO, Czech Rep.*

The presentation summarizes the outcome of an investigation of how the cyberattacks on safety-critical infrastructure are nowadays possible. The investigation was informally done based on internet research, interviews with various shareholders - admins, penetration testers and other security experts, owners of companies that manufacture IoT devices, and a few on-site visits in Czech Republic. Then, from high-level perspective some approaches and views on offensive and defensive tactics are presented. The presentation concludes with an explanation of a cyberattack on jeep Cherokee (2015) to demonstrate an example of hacking practices in IoT.

Tomáš Martinec

Tomáš Martinec graduated at MFF UK from Computer Science and he works in Sysgo where he is responsible for testing and certification of software with safety aspects. He mentors less experienced colleagues and has among other fields interest in securing safety-related devices.

Graph-Based Models in Prediction and Projection of Cyber Attacks

Speaker: **Martin Husák**, *Masaryk University, Brno, Czech Rep.*

Predictive analysis allows next-generation cyber defense that is more proactive than current approaches based solely on intrusion detection. In this talk, we will discuss various approaches to predicting and projecting cyber attacks. Graph-based models are dominating the field since the foundation of this research area. Attack graphs were used to traverse through the attacker's actions and project the continuation of an ongoing attack. Later, attack graphs were combined with Bayesian networks and Markov models to reflect the probabilistic nature of predictions and overcome uncertainties in observation of attack steps. However, there are still open issues, such as how to create such models and evaluate the predictions. The talk will shed light on using graphs in this research area and summarize resolved and open issues.

Martin Husák

Martin Husák is a researcher at the Institute of Computer Science at Masaryk University, a member of the university's security team (CSIRT-MU), and a contributor to The Honeynet Project. His Ph.D. thesis addressed the problem of early detection and prediction of network attacks using information sharing. His research interests are related to cyber situational awareness and threat intelligence with a special focus on the effective sharing of data from honeypots and network monitoring.

Approximate Computing: Test and Reliability issues and opportunities

Speaker: **Alberto Bosio**, *INL – Ecole Centrale de Lyon, France*

Approximate Computing (AxC) is today one of the hottest topics related to system design and optimization. Thanks to this computing paradigm, designers are able to reduce area, power consumption, and even production costs in the case the target application can accept a given degree of inaccuracy in the final computations. This presentation discusses the impact of Approximate Computing on the test and reliability. More in particular, it aims at showing that it is possible to use Approximate Computing to implement low cost but still efficient test mechanisms and fault tolerant architectures.

Alberto Bosio

I have carried out all my studies in Italy, after a PhD in Computer Engineering in the area of digital systems dependability at the Politecnico di Torino (Italy) in 2006, I had the opportunity to obtain a permanent position as Maître de Conférences in the Université de Montpellier in 2007. From 2018 I'm a Full Professor at INL - Ecole Centrale de Lyon. The works carried out over 13 years of career let me be the co-author of 1 book, 38 international journal papers, 5 patents, 7 invited papers, 3 embedded tutorials and more than 120 papers in international conferences. I had supervised 13 Ph.D. students. I actively participated to 19 european- and national-funded projects and research contracts with industrial partners. I served as committee and organizing member in several international conferences as well as reviewers for many international journals. I'm a member of the IEEE and the Chair of the European Test Technical Technology Council (eTTTC).

The next step of P4 FPGA architectures: External Memories

Tomáš Beneš, Tomáš Čejka, Hana Kubatová
FIT Czech Technical University in Prague CESNET a.l.e.
Thákurova 9, Prague 6 Zikova 4, Prague 6

benesto3@fit.cvut.cz,
cejkat@cesnet.cz, kubatova@fit.cvut.cz

Keywords. Network, Monitoring, Analysis, Encryption, Security, Hardware

Abstract

P4 is a recent feasible technology that helps to make a modern infrastructure flexible and ready for changes. Software solutions are available, but not efficient enough for high throughput and low latency applications. Therefore, hardware acceleration is used commonly. This paper discusses caveats of currently existing approaches, mainly focused on FPGAs, which are flexible but resource-limited. Our aim is to propose an extension of standard P4 architecture to support external memory and explain a possible approach to overcome the issues.

2 Introduction

Modern network infrastructures require high flexibility and adaptability. Therefore, software-defined networking has become a very popular approach in recent years. The evolution of the network technology brought a P4 language as a standard to describe the functionality of flexible network devices.

For high-speed networks, pure software solutions are usually insufficient. Therefore, proprietary devices with ASICs or specialized network processors were dominating for many years due to high performance and cost reasons because the programmable ASICs (e.g., FPGAs) were even more expensive. However, due to limits of the fixed set of supported features with minimal options for configuration, programmable platforms are needed. Nowadays, the solutions based on specialized chips are evolving into more flexible ones, and FPGA technology is feasible because it is flexible enough and becomes a commodity.

The P4 language, which addresses the current requirements on network devices, has been designed with respect to three goals [10]:

Protocol independence The language is designed as protocol independent. That means, it is possible to describe any protocol, e.g., IP, VXLAN, or TCP. The language supports descriptions of any header formats and field names of the processed protocols.

Reconfigurability The P4 target devices should be able to change the packet processing behavior multiple times after deployment.

Portability P4 programs are target-independent, and the mapping to specific architectures, e.g., general-purpose CPU, ASIC, or FPGA is performed by the compiler [1, 9, 2, 7], which translates P4 to the target.

The P4 community established a standardized architecture called Programmable Switching Architecture (PSA) [3]. The architecture ensures high-level features that should be supported on any P4-compatible target platform. P4 specification describes three types of memory blocks:

Register Simple register for loading and storing values by the P4 program.

Counter Mechanism for keeping statistics, which can only be incremented by the P4 program.

Meter More complex mechanism for keeping statistics about packets called 3-color meters [3].

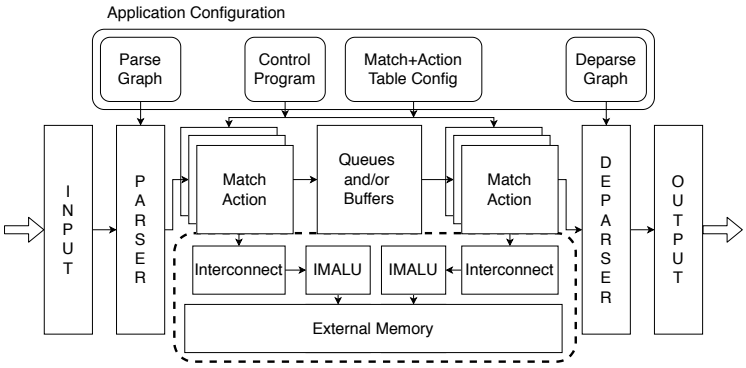


Figure 1: Augmented P4 architecture with *In-Memory ALU* to solve external memory latency issues.

3 Challenges and Our Approach

There are many applications already described in P4 that cover a wide variety of use cases, such as Network Monitoring, Virtual Switching, DDoS detection, Routers, Quality of Service [5, 8, 6]. Most of them are implemented as software architecture created by [1]. The main disadvantage of software targets is a performance penalty, which is unfeasible for high-speed networks; therefore, the applicability in a production environment is minimal.

FPGA platform overcomes the performance disadvantages by hardware accelerating P4 applications. The latest existing architectures are capable of processing 100 Gb/s packet streams [9]. However, the use of FPGA also brings new challenges. The difficulty of a hardware implementation of some essential mathematical functions and limited internal memory (usually < 30 Mb) of FPGA leads to the limitation of existing P4 accelerator architectures for FPGA. P4 $\rightarrow$ NetFPGA project [11], which uses Xilinx P4-SDNet architecture and others [9] currently do not provide any support for external memories (usually > 2 Gb) and solely depend on the internal resources of the FPGA. Most of the implementations of virtual switching and network monitoring are not usable due to this memory limitation.

An architecture with external memory is non-trivial. Therefore, it is not supported in current FPGA designs. The large and inconsistent latency [4] leads to an advanced pipeline principle that consumes a high amount of resources, even in a simple design. Also, sharing one memory resource between multiple P4 actions leads to memory hazards like *Read after Write* (RAW) and *Write after Read* (WAR) due to the parallel nature of the P4 program, especially when the counters are used. Finally, the P4 compiler needs to apply advanced optimization to split a P4 application into latency-critical (high-utilized) blocks and other parts. Both must be correctly mapped onto fast internal FPGA resources or external slower memory to preserve overall high throughput.

We addressed some of these challenges by extending an FPGA architecture (Fig. 1) to *In-Memory ALU* (IMALU), that performs in-memory computing and caching. The combination of these principles highly reduces the inconsistent latency by offloading operations like addition directly into the memory system. Also, dealing with RAW and WAR hazards is much easier, because the memory operation tasks are implicitly ordered. This promising solution with external memory support is going to have a significant impact, especially in the network monitoring and virtual switching areas.

4 Conclusion

The P4 language allows for description of high-speed network processing devices. Since it is platform-independent, there are several technologies that are currently supported by P4 compiler. We focused on one of them, FPGA, which is flexible and re-programmable. Currently used architectures did not support external memory, which is an essential issue for many real-world applications. This paper proposed an extended architecture with In-Memory ALU to solve latency issues in cases where higher memory capacity is needed as well as low latency.

Acknowledgment

This research has been supported by the CTU grant project SGS20/210/OHK3/3T/18 "Research and development of tools for security analysis of computer network traffic."

References

[1] `https://github.com/p4lang/p4c`.

[2] `https://www.xilinx.com/support/documentation/sw_manuals/xilinx2018_2/ug1252-p4-sdnet.pdf`.

[3] `https://p4.org/p4-spec/docs/PSA.html`.

[4] `https://www.xilinx.com/support/documentation/ip_documentation/ug586_7Series_MIS.pdf`.

[5] D. Ding et al. Estimating Logarithmic and Exponential Functions to Track Network Traffic Entropy in P4. In *NOMS2019*.

[6] D. Ding et al. An incrementally-deployable P4-enabled architecture for network-wide heavy-hitter detection. *IEEE Transactions on Network and Service Management*, 2020.

[7] R. Miao and et al. Silkroad: Making stateful layer-4 load balancing fast and cheap using switching asics. SIGCOMM '17, 2017.

[8] P. Benáček et al. Flexible OVS acceleration with P4 and low profile FPGA card. TNC18, 2018.

[9] P. Benáček et al. P4-to-VHDL: Automatic generation of high-speed input and output network blocks. *Microprocessors and Microsystems*, Feb. 2018.

[10] P. Bosshart et al. P4: Programming protocol-independent packet processors. *SIGCOMM Comput. Commun. Rev.*, 44(3):87–95, July 2014.

[11] S. Ibanez et al. The P4 $\rightarrow$ $NetFPGAWorkflowforLine - RatePacketProcessing.FPGA'19$, 2019.

QoD: Ideas about Evaluating Quality of Datasets

Dominik Soukup, Karel Hynek, Tomas Cejka
FIT Czech Technical University in Prague CESNET a.l.e.
Thákurova 9, Prague 6 Zikova 4, Prague 6

soukudom@cesnet.cz, hynekkar@fit.cvut.cz, tomas.cejka@fit.cvut.cz

Keywords. Datasets, Machine Learning, Metrics

Abstract

Importance of computer networks is raising every year. The reason is that we are connecting more and more devices, applications and our daily routines depends on connectivity. On the other hand, this is a great potential for attackers. They can hide their activities in complex network environment and steal valuable data. Therefore, network traffic monitoring is a mandatory component of any computer network.

It's amazing to see the progress in monitoring computer networks. The journey from deep packet inspection (DPI) detection modules to modules based on machine learning (ML). ML detection modules have a great potential in the future because they can leverage huge amount of data to detect even complex behavioral patterns. However, the key prerequisite for stable and reliable ML module is a dataset with relevant data composed by feature sets. Without solid dataset, our evaluation score is misinterpreting the real score in production environment, and, therefore, proper datasets have essential role in research&development of any ML-based classifier or detector.

The main motivation for this paper is to find a way how to evaluate quality of any dataset to estimate if it is good enough for ML experiments. In practice, we create annotated datasets iteratively and continuously using generated or captured real traffic. ML detection modules training and evaluation are very time and resource consuming, especially for large datasets and complicated problems. Therefore, it can be very valuable to predict whether a provided dataset has already enough information and sufficient quality. With this assumption we will be able to decrease number of prototypes of ML detection modules, and decide whether dataset X will have similar results as dataset Y.

To our best knowledge, there are only a few studies focused on quality evaluation of datasets with network traffic. The paper (2) studied performance of different ML models based on effect of dataset size, metrics set, and the feature selection techniques. Brabec et al. (1) has in mind the importance of test dataset and real-world dataset. However, their evaluation metrics are done at ML model level.

In this paper, we propose initial ideas and experiments about datasets quality evaluation. For experiments, we selected datasets (3) about DNS over HTTP (DoH) detection and URL classification problems that are already being elaborated, e.g., in (4). All metrics are calculated from dataset level. Impact of these metrics is evaluated on Random Forest (RF) model. We show results we have discovered in our datasets and ML detection modules. Eventually, we discuss possible next steps in this research.

Acknowledgment

This research has been supported by the CTU grant project SGS20/210/OHK3/3T/18 "Research and development of tools for security analysis of computer network traffic."

References

[1] Brabec, J., Komárek, T., Franc, V., Machlica, L.: On model evaluation under non-constant class imbalance (2020)

[2] Catal, C., Diri, B.: Investigating the effect of dataset size, metrics sets, and feature selection techniques on software fault prediction problem. Information Sciences (2009). https://doi.org/https://doi.org/10.1016/j.ins.2008.12.001, http://www.sciencedirect.com/science/article/pii/S0020025508005173

[3] Vekshin, D., Hynek, K., Cejka, T.: Dataset used for detecting dns over https by machine learning. (May 2020). https://doi.org/10.5281/zenodo.3906526

[4] Vekshin, D., Hynek, K., Cejka, T.: Doh insight: Detecting dns over https by machine learning. In: Proceedings of the 15th International Conference on Availability, Reliability and Security. ARES '20, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3407023.3409192

EA-based Optimization of Digital Circuits

Jitka Kocnova
Brno University of Technology, Faculty of information Technology
IT4Innovations Centre of Excellence,
Brno, Czech Republic

ikocnova@fit.vutbr.cz

Keywords. CGP, evolution, resynthesis, combinational circuit, optimization

The increasing complexity of the designs and problematic scalability of original representations led to a shift in internal representations used in logic synthesis and optimization. Heterogeneous representations were replaced with homogeneous intermediate representations. And-inverter graph (AIG) has been identified as the most promising intermediate structure for scalable logic optimization and many efficient algorithms were implemented on top of it. However, the inability of AIG to efficiently represent XOR gates together with heuristic nature of logic optimization algorithms leads to some inefficiency causing that the logic can be further minimized even after it has been mapped. The ability to capture XOR gates is, however, essential for efficient representation of arithmetic and XOR-intensive circuits.

To address this issue, we proposed to employ the evolutionary algorithms for circuit optimization. This decision is based on our positive based on our positive experience with the application of evolutionary algorithms in [4, 3], where various evolutionary approaches working directly at the level of gates were successfully applied to address the problem of the logic optimization on the AIG level. In [4, 3], it was demonstrated that the evolutionary synthesis using Cartesian Genetic Programming (CGP) conducted directly at the level of common gates is able to provide significantly better results compared to the state-of-the-art synthesis operating on AIGs. In average, the method enabled a 34% reduction in gate count on an extensive set of IWLS benchmark circuits when executed for 15 minutes.

However, the efficiency of the evolutionary approach deteriorates with the increasing number of gates because of various scalability issues inevitably connected with the usage of GP, hence we propose to combine this approach with various sub-circuit selection strategies to maintain the scalability and achieve reasonable reduction in the circuit size.

This abstract summarizes the key ideas and results related to our work. In particular, two papers are covered and discussed. The first paper Towards a Scalable EA-based Optimization of Digital Circuits [1] describes the preliminary results of the EA-based optimization combined with sub-circuit selection. This paper was presented at EuroGP conference in 2019 and was nominated for best paper award. The second paper EA-based Resynthesis: An Efficient Tool for Optimization of Digital Circuits [2] includes a more detailed comparision between the two different techniques to the sub-circuit extraction, the evolutionary method working on whole circuits, and the state-of-the-art logic synthesis algorithm.

Two complementary approaches to the extraction of the sub-circuits have been presented and evaluated so far in our research. The proposed approaches are inspired by the refactoring which iteratively selects large cones of logic, optimizes them and returns them back to the original structure provided that there is an improvement in some metric. The experimental results show that the evolutionary resynthesis provides better results compared to globally operating evolutionary optimization (further denoted as global) as proposed in [3]. In more than 85% cases, a substantially higher number of redundant gates was removed while keeping the computational effort at the same level.

Our optimization procedure is based on the CGP and the crucial steps can be seen in the Algorithm 1. Several calls of this procedure are executed in the proposed methods that use a simple divide-and-conquer strategy. The proposed methods are allowed to create n_{cuts} sub-selections depending on the sub-selection strategy implemented in the GetSubcircuit function. For each sub-selection, the OptimizeNetworkUsingEA is allowed to perform n_{iters}/n_{cuts} iterations. In total, n_{iters} evolutionary iterations are evaluated in both cases. This naive strategy supposes that the computation effort does not depend on the window size but it helps to fairly evaluate the impact of the proposed method. In the paper [1], the sub-selection strategy is based on the cut-selection inspired by the BFS algorithm. In the paper [2], the sub-selection approach is modified and inspired by so called windowing, and it iteratively selects all the nodes connected to the nodes already present in the cut in order to make the cut selection wider.

The only criterion in the fitness function considered in this paper is the area on a chip expressed as the number of gates. The proposed method was implemented in C++ and integrated in Yosys open synthesis suite.

Algorithm 1: OPTIMIZATION OF DIGITAL CIRCUITS USING EA-BASED RESYNTHESIS

Input: A Boolean network N
Output: Optimized network N', $cost(N') \leq cost(N)$

```
1 N' ← N
2 while terminated condition not satisfied do
3     m ← identify the best candidate root node m ∈ N'
4     W ← GetSubcircuit(m)
5     if W is a suitable candidate then
6         W' ← OptimizeNetworkUsingEA(W)
7         if cost((N' \ W) ∪ W') < cost(N') then
8             N' ← (N' \ W) ∪ W'
9 return N'
```

In [1], the GetSubcircuit method was cut-based. The proposed method performed substantially better than the global one considering the average as well as the best results. It won in 22 out of 28 cases. There were even cases, when the global method provided none or nearly none improvement. Compared to the conventional logic synthesis, state-of-the-art EA-based optimization was able to produce substantially better results but at the cost of a higher run time. Unfortunately, the run time increased with the increasing complexity of the Boolean networks. The proposed method is able to outperform the original EA-based optimization applied to the whole Boolean networks. The number of nodes w.r.t the original method was improved by 9.2% on average. Even though only area was analyzed in this study, the depth of the optimized circuits is comparable with the original circuits.

However, the cut-based sub-selection method based on the BFS algorithm (denoted further as GS1) leads to simple cuts where the presence of reconvergence driven paths or don't care nodes is poor. The problem is the actual size and number of PIs and POs of the subgraph and so the choose of the selecting algorithm is a non-trivial issue. To adress this problem, in the [2] we changed the cut-selection algorithm to iteratively select all the nodes connected to the nodes already present in the cut in order to make the cut selection wider, with more nodes, PIs and POs. This new techique (denoted as GS2) was slightly inspired by a conventional windowing technique.

Even though we used a simple setting which may degrade the capabilities of the resynthesis (e.g. the fixed number of evaluations of EA or random root node selec- tion), both the proposed approaches were able to outperform the EA-based optimization applied to the whole Boolean networks. The proposed sub-circuit extraction inspired by windowing was significantly better than the cut-based alternative.

All the evolutionary approaches were able to further reduce the size of the benchmark circuits despite

that the fact that they were highly optimized by the ABC synthesis tool.

On average, the evolutionary resynthesis achieved 8.9% circuit size improvement on controllers and 21.4% improvement on arithmetic circuits. The globally applied evolution was able to improve the circuits belonging to the mentioned groups by 7.5% and 1.8%, respectively. Example of the achieved reduction can be seen in the Table 1.

Table 1: Evaluation of the proposed method on a sub-set of industrial benchmarks optimized by the state-of-the-art synthesis (column best ABC). The performance is given as the best as well as average achieved reduction, i.e. the number of removed gates, for the proposed method and two methods available in the literature.

			input (best ABC)		resynthesis – GS1 [1]		resynthesis – GS2 [2]		global method [3]	
Benchmark	inputs	outputs	gates	depth	average	best	average	best	average	best
aes_core	789	532	21128	20	2.9%	2.9%	**4.7%**	**5.5%**	0.6%	1.7%
ethernet	10672	10452	60413	23	0.5%	0.5%	**0.9%**	**1.1%**	0.0%	0.0%
i2c	147	127	1161	12	9.2%	9.2%	**16.9%**	**17.8%**	10.0%	10.7%
systemcdes	314	126	2601	25	4.8%	5.0%	**9.2%**	**10.7%**	9.1%	9.9%
usb_phy	113	73	452	9	13.9%	14.0%	**16.7%**	**17.6%**	12.2%	12.2%
average (logic benchmarks)			15620	20	6.3%	6.4%	**9.7%**	**10.6%**	6.3%	6.5%
sqrt32	32	16	1462	307	**22.3%**	**24.3%**	12.6%	15.4%	3.0%	3.0%
diffeq1	354	193	20719	218	11.5%	11.5%	**13.1%**	**15.7%**	0.0%	0.0%
div16	32	32	5847	152	15.7%	15.8%	**20.5%**	**27.9%**	0.0%	0.0%
hamming	200	7	2724	80	28.6%	30.1%	**40.1%**	**40.9%**	14.6%	14.6%
revx	20	25	8131	171	14.5%	14.5%	**16%**	**17.8%**	0.0%	0.1%
average (aritmetic benchmarks)			8956	148	18.2%	19.2%	**20.5%**	**23.5%**	3.5%	3.5%

The best results obtained by a particular method are relatively close to the average ones which suggests that the evolutionary methods are quite stable although they are in principle non-deterministic.

A significant improvement was recorded for the arithmetic circuits. The number of gates was reduced by 27.4% using GS2 (15.3% for GS1) on average. The detailed analysis revealed that this was possible due to better handling of XORs/XNORs compared to the conventional synthesis. The relative number of AND/OR/NAND/NOR gates remained nearly the same (around 74%) but the absolute number of XORs/XNORs increased from 10% to 15% for GS1 and 18% for GS2.

It can be concluded, in general, that the global method works well especially for small instances that are compact (do not contain many independent sub-circuits) and that have a reasonable depth (10 to 25 levels). On the other hand, the optimization of circuits having a large depth, many gates or many independent sub-parts performs unsatisfactory when the global method is applied.

In addition to the optimization capabilities, we also evaluated the computational effort of the evolutionary methods. The global method converges faster than the locally working ones, but it has a strong tendency to get stuck at a local optima, especially when working with the complex and XOR-intensive arithmetic circuits. The slow convergence is caused by the fact that each sub-circuit produced by the proposed windowing algorithm is optimized for a fixed number of generations independently on its parameters such as the size or the number of PIs. This simplifies the problem but it may lead to a potential inefficiency. Many generations can be wasted to optimize small circuits. Depending on the circuits structure, it may be impossible to create such a large working window because there may be independent parts that consist of the smaller number of gates. However, the number of inputs and outputs positively correlates with the size of W for both sub-cirtuit extraciton methods. The larger the number of gates in the window, the higher number of inputs and outputs.

The number of inputs of the sub-circuits optimized by the evolution is substantially higher compared

to the numbers used by the rewriting algorithm which is applied in the conventional synthesis. Compared to the rewriting and other techniques, a relatively complex portions of the original circuits are chosen for subsequent optimization. This could explain the reason, why the proposed EA-based method is able to achieve such reduction compared to the conventional state-of-the-art synthesis.

In our future work, we would like to implement an adaptive strategy that modifies the maximum number of evaluations according to the size of the optimized logic circuit. We suppose that this mechanism helps us to improve the convergence. In addition to that, we would like to focus on improvement of root node selection strategy. The question here is whether the result would be better if the cut is built from a node near to the previously chosen one.

References

[1] Kocnova, J., Vasicek, Z.: Towards a Scalable EA-based Optimization of Digital Circuits, Sekanina L., Hu T., Lourenco N., Richter H., Garcia-Sanchez P. (eds) Genetic Programming. EuroGP 2019. Lecture Notes in Computer Science, vol 11451. Springer, Cham.

[2] Kocnova, J., Vasicek, Z.: EA-based resynthesis: an efficient tool for optimization of digital circuits, Genet Program Evolvable Mach 21, 287–319.

[3] Vasicek, Z.: Cartesian GP in Optimization of Combinational Circuits with Hundreds of Inputs and Thousands of Gates, Proceedings of the 18th European Conference on Genetic Programming – EuroGP, 2015, 139–150.

[4] Sekanina, L., Ptak, O., Vasicek, Z.: Cartesian Genetic Programming as Local Optimizer of Logic Networks, 2014 IEEE Congress on Evolutionary Computation, 2014, 2901–2908.

DoH detection: Discovering hidden DNS

Karel Hynek, Tomas Cejka, Dmitrii Vekshin
FIT Czech Technical University in Prague CESNET a.l.e.
Thákurova 9, Prague 6 Zikova 4, Prague 6

hynekkar@fit.cvut.cz, tomas.cejka@fit.cvut.cz, vekshdmi@fit.cvut.cz

Keywords. DNS over HTTPS, DoH, Detection, Classification, Machine Learning, Datasets

Abstract

The necessity of securing users' privacy on the internet has given the rise of a new protocol called DNS over HTTPS (DoH). It aims to replace traditional DNS for domain name translation with encryption as a benefit. Unfortunately, the laudable attempt to increase the privacy of users also brings some security threats as well. Readable information from DNS is one of the most essential data-source in computer security, especially for security forensic analysis. The DNS queries in the network can reveal malicious activity in the network like the presence of malware, botnet communication, and also data ex-filtration. Thus network administrators might want to block encrypted DoH in their network, however, the currently available approaches are based on lists of IP adresses of well-known DoH providers/resolvers. This way of detection can be easily surpassed by its own private or not generally known DoH resolver. Since the presence of DoH communication might also indicate some malicious activity or at least a policy violation, we decided to find a possible way to detect DoH based on the traffic behavior. This research aims to recognize DoH from extended IP flow data by Machine Learning regardless IP addresses.

1 Introduction

Translation of human-readable domain names into machine-usable IP addresses and vice versa is an essential feature in the network services. Traditionally, this mechanism is performed by Domain Name System (DNS) (3) protocol, which is based on transferring unencrypted queries and answers.

The unencrypted nature of DNS protocol makes it essential for many existing security systems. Since an application must always translate a domain name before establishing a connection, DNS traffic can identify many security threats. However, the monitoring of the DNS traffic (even with autonomous systems) might disrupt users' privacy because it discloses services (e.g., web sites) that were visited. Therefore, a new protocol DNS over HTTPS (DoH) has been developed by engineers from IETF. DoH encapsulates traditional DNS into encrypted HTTPS channel (2).

The encryption of the traffic effectively provides better privacy, however, it also decreases visibility into network traffic for various security tools. As a result, it can affect the level of network security. There are already the first known malware families (such as (1)), that take advantage of encryption and hide their DNS activity in the DoH channel. The decreased network visibility motivates administrators to block DoH in their network, which is usually achieved by blocking particular IP addresses of well-known DoH resolvers. This solution is not perfect because any malicious software or unruly user, who wants to hide, can easily create own DoH resolver on non-standard address and port. Therefore, we focused on

the detection of DoH using Machine Learning in combination with particular statistical features obtained from IP flow data, and we have originally published this research in (5).

2 Detector design

For the DoH detection, we created a large dataset (4), that contained traffic from main DoH-enabled browsers (Firefox and Chrome). The traffic was generated by the autonomous browsing of websites from Alexas top 10,000 dataset. The manual analysis of the data revealed 18 features suitable for DoH detection.

For example, both browsers create a single connection to DoH resolver at their startup and use this connection for a long time, usually, until the user turns it off. Therefore the flow duration is much longer than in regular web browsing. The DoH communication can also be distinguished from regular HTTP by the size of transmitted packets. Since DoH is only encapsulated DNS packets in HTTP, their maximum size usually does not exceeds 600 KB. DoH communication also follows the burst-like scheme like in classical web browsing. When the user enters the web site, the browser generates multiple DNS (DoH) queries to services like javascript library providers and content delivery networks. The burstiness of the traffic is also one of the most fundamental indicators of DoH.

The feature vector extracted from the dataset was then used as the input for the Machine-Learning classifier. We experimented with multiple ML-based algorithms such as 5-NN, C4.5 decision tree, but the AdaBoosted decision tree performed the best with 99.6 % accuracy. The classification performance was measured with 5-fold cross-validation and the results are presented in form of a confusion matrix in Tab 1.

3 Usage in practice

In practice, we need an IP flow exporter that is capable of exporting additional information about packets within an HTTPS connection. Therefore, we have improved an existing IPFIX[1] flow exporter called *ipfixprobe*[2]. This flow exporter can extract timestamps and sizes of the first N packets of each connection. It is worth noting that ipfixprobe aggregates both directions of a connection into the bi-directional flow records (*biflows*).

In order to collect IP flow records, we use a flow collector called IPFIXcol[3] that is able to receive several data formats like NetFlow or IPFIX. IPFIXcol2 can be used to store the data and to translate them into easily processable binary format UniRec, which is used in the stream-wise modular NEMEA system for detection and analysis.

Finally, the flow data can be analyzed by the modules of the open source NEMEA system[4]. For the experiments, we used Jupyter notebooks written in Python, however, for the production deployment, it is straightforward to transcript the experimental code into a NEMEA module, which can subsequently analyze an online stream of flow data.

4 Conclusion

This paper presented a brief overview of the already published research progress in the scope of the identification of DNS over HTTPS network traffic. Our presented detector based on Machine Learning

[1] IPFIX is a standard format for IP flow representation and transfer

[2] `https://github.com/CESNET/IPFIXprobe`

[3] `https://github.com/CESNET/IPFIXcol2`

[4] `https://github.com/CESNET/NEMEA`

Table 1: Confusion matrix of DoH classification from a regular HTTPS traffic. The table contains class accuracy and class recall for both classified classes: DoH and regular HTTPS.

		Ground truth		**Class Accuracy**
		DoH	HTTPS	
Result	DoH	32,668	81	99.7 %
	HTTPS	1,511	411,791	99.6 %
Class Recall		95.5 %	99.9 %	

achieved excellent results using IP flow data with statistical features. We plan to extend our research focused on DoH for inferring the encrypted content and also for threat detection based on DoH.

Acknowledgment

This research has been supported by the CTU grant project SGS20/210/OHK3/3T/18 "Research and development of tools for security analysis of computer network traffic."

References

[1] Cimpanu, C.: First-ever malware strain spotted abusing new DoH (DNS over HTTPS) protocol (2019)

[2] Hoffman, P.E., McManus, P.: DNS Queries over HTTPS (DoH). Tech. Rep. 8484 (Oct 2018). https://doi.org/10.17487/RFC8484, https://rfc-editor.org/rfc/rfc8484.txt

[3] Mockapetris, P.: Domain names - concepts and facilities. RFC 1034 (Internet Standard) (Nov 1987). https://doi.org/10.17487/RFC1034, https://www.rfc-editor.org/rfc/rfc1034.txt

[4] Vekshin, D., Hynek, K., Cejka, T.: Dataset used for detecting dns over https by machine learning. (May 2020). https://doi.org/10.5281/zenodo.3906526

[5] Vekshin, D., Hynek, K., Cejka, T.: Doh insight: Detecting dns over https by machine learning. In: Proceedings of the 15th International Conference on Availability, Reliability and Security. ARES '20, Association for Computing Machinery, New York, NY, USA (2020). https://doi.org/10.1145/3407023.3409192, https://doi.org/10.1145/3407023.3409192

Classification of Network Traffic using Traffic Features

Matej Hulak, Tomas Cejka
FIT Czech Technical University in Prague
Thákurova 9, Prague 6

hulakmat@fit.cvut.cz, tomas.cejka@fit.cvut.cz

Keywords. Classification, Network Traffic, Machine Learning, Datasets

Abstract

Computer networks are gradually becoming essential people's needs. The amount of network traffic and network devices is increasing every day due to improvements and expansion of network infrastructure. The new trend of smartphones, watches, fridges and, in general, smart homes connect a high number of new devices into a network infrastructure. Therefore, the overall volume of network traffic grows, and also networks are getting more complex, which means they are harder to monitor.

The main focus of our presentation is the monitoring technology for high speed networks that is able to analyze and classify network traffic automatically. Traffic classification is an essential functionality for various purposes, such as network security. Identification of types of network traffic is a part of the process of, e.g., forensic analysis. Therefore, the accurate and fast classification algorithm provides valuable information for network operators and security analysts.

In practice, network traffic monitoring is usually based on IP Flow data (as it is explained in (5)), which are being created in network monitoring probes and collected in a network flow collector. Each IP Flow record represents one communication between two hosts, and we aim to insert a label with the meaning/purpose of the communication.

Among existing related works, there are various approaches (1; 2; 4; 7) that are based, e.g., on pattern matching/deep packet inspection, support vector machine (SVM) or other machine learning methods, statistics, or simply based on well-known port numbers. This work builds on the bachelor thesis (6), which shows the feasibility of the pre-computed statistical characteristics based on statistical percentiles of the IP Flow metrics. However, our goal is to evaluate the expected increase in accuracy of the classifier based on the used machine learning algorithm and available level of detail obtained from IP Flow data. More specifically, we compare a) basic NetFlow data, b) IP Flow data extended with unencrypted L7 headers, c) IP Flow data with "per-packet-information."

As a software prototype for our experiments, we use NEMEA system (3). We have developed NEMEA modules that contain the classification algorithms. These prototypes allow us to compare different algorithms in an experimental environment with offline data, and the same software module (with the best performance) can also be deployed in production for online analysis.

Using this classification module, we were able to achieve some promising results of the experiments. They showed us that it is possible to classify network flows with high accuracy even with the simple NetFlow data and the method based on percentiles proposed in (6). The proposed classifier is fast enough to process millions of IP flow records per second; therefore, it is deployable even on large network infrastructure. The accuracy of this method is about 85 %. Besides, we have evaluated some machine learning models that reached slightly higher accuracy (approximately 88 %) using a classifier based on

Decision Trees. However, those results are only preliminary and we expect a more considerable precision increase in the future.

Acknowledgment

This research has been supported by the CTU grant project SGS20/210/OHK3/3T/18 “Research and development of tools for security analysis of computer network traffic.”

References

[1] libprotoident [online], `https://research.wand.net.nz/software/libprotoident.php`, wAND Network Research Group. [vid. 2020-05-19]

[2] Alcock, S., Nelson, R.: Libprotoident: traffic classification using lightweight packet inspection. WAND Network Research Group, Tech. Rep. (2012)

[3] Cejka, T., et al.: NEMEA: A framework for network traffic analysis. In: 12th International Conference on Network and Service Management (CNSM) (2016)

[4] Cisco Systems, Inc.: Classifying network traffic using nbar (2006), `ftp://ns.nobatel.com/pub/manuales/cisco/pdfs/qsnbar1.pdf`

[5] Hofstede, R., Čeleda, P., Trammell, B., Drago, I., Sadre, R., Sperotto, A., Pras, A.: Flow monitoring explained: From packet capture to data analysis with netflow and ipfix. IEEE Communications Surveys Tutorials **16**(4), 2037–2064 (2014)

[6] Hulák, M.: Klasifikace provozu a zařízení v počítačových sítích na základě toků. B.S. thesis, České vysoké učení technické v Praze. Vypočetní a informační centrum. (2020)

[7] Kasner, Z.: Klasifikace zařízení na základě tok v počítačovỳch sítích. B.S. thesis, České vysoké učení technické v Praze. Vypočetní a informační centrum. (2016)

Deadline Verification Using Model Checking

Jan Onderka
Faculty of Informatics, Czech Technical University in Prague
Thákurova 9, 160 00 Prague 6, Czech Republic

onderjan@fit.cvut.cz

Keywords. Model checking, deadline checking, microcontroller formal verification, machine code level, cycle-accuracy, hybrid technique, nondeterminism, control flow generation, simple cycle path reduction

Abstract

In this thesis, a new utility is presented for performing formal deadline checking of simple microcontroller programs at machine code level.

The existing formal verification approaches and tools are studied and their weaknesses identified. Namely, source level techniques cannot guarantee cycle-count precise execution times, while machine code verification tools are few, not generally available, and usually heavily tailored to a specific processor, significantly reducing their usefulness.

To counteract the weaknesses of current microcontroller verification tools, a novel hybrid approach is proposed and implemented. Machine code level model checking techniques are used for state space representation and verification of adherence to specification. Microcontroller memory and step behaviour is specified using a simple imperative language that can be manipulated using standard source code level techniques. This allows cycle-count based deadline checking, simple extension to other microcontrollers in addition to the implemented ATmega328P, and implementation of advanced techniques without dependence on the actual processor used.

In addition to the core functionality, advanced techniques for handling nondeterminism, control flow generation, and simple cycle path reduction are implemented. The utility is tested, showing its usefulness for simple program deadline verification. The impact of various techniques used is discussed and promising future improvements are identified.

Acknowledgment

I would like to thank doc. Dipl.-Ing. Dr. techn. Stefan Ratschan for supervising the thesis, providing guidance and helpful feedback.

Programmable Generator of Synchronous Pulse Sequences

Vojtěch Nevřela
FIT CTU, Department of Digital Design
Thákurova 9, 160 00 Prague 6 Czech Republic

nevrevoj@fit.cvut.cz

Keywords. pulse sequencer, pulse generator, FPGA, high-speed, programmable

Abstract

The need for precise scientific equipment is rising as the research becomes more focused on the minuscule features of our universe with every following day. One example of such a device, and also the subject of this thesis, is the pulse train generator, also called the pulse sequencer, pulse sequence generator, or many other takes on the same name. Pulse train generators are used to generate stimuli for a variety of exper- iments that require pulses of precise widths to be administered to inputs at correct times. The precision required can even reach the magnitudes of pi- coseconds. This makes the task vitally unattainable by microprocessor-based systems. The objective of this thesis is the design of a FPGA-based solution which would be capable of reaching 1 ns precision while keeping the cost and electronic complexity minimal.

Acknowledgment

I wish to express my thanks to the opponent of the correcponding thesis, Michal Dudka, who has provided me with the necessary facilities and knowledge to complete the electronics part of the work. I would also like to thank my supervisor, Ing. Jaroslav Borecký, Ph.D., for sharing his expertise in digital design and much appreciated guidance.

Detection of HTTPS brute-force attacks in high-speed computer networks

Jan Luxemburk
Faculty of Information Technology, Czech Technical University in Prague
Thákurova 9, 160 00 Praha 6

luxemjan@fit.cvut.cz

Keywords. Network monitoring, brute-force attacks, HTTPS, IPFIX.

Abstract

This thesis presents a review of flow-based network threat detection, with the focus on brute-force attacks against popular web applications, such as WordPress and Joomla. A new dataset was created that consists of benign backbone network traffic and brute-force attacks generated with open-source attack tools. A new method is proposed for brute-force attack detection that is based on packet-level characteristics and uses modern machine-learning models. It is designed to work with encrypted HTTPS traffic, even without decrypting the payload, which is important because more network traffic is being encrypted, and it is crucial to update our intrusion detection methods to maintain a sufficient level of network visibility. The method could be especially useful for web hosting and internet providers, which would like to monitor their customers' network traffic and protect them from brute-force attacks. We evaluated the method with leave-out cross-validation and achieved a recall of 84% attacks generated by 3 brute-force tools towards 7 different web applications with a false positive rate of 1:10 000.

Acknowledgment

I would like to thank my supervisor Ing. Karel Hynek for his guidance and helpful approach.

Influence of Synthesis Parameters on Vulnerability to Side-Channel Attacks

Tomáš Balihar
Faculty of Information Technology, Czech Technical University in Prague
Thákurova 9, 160 00 Praha 6

balihto1@fit.cvut.cz

Keywords. Side-Channel Attacks, Cryptography, Synthesis Parameters, FPGA, Welch's t-test

Abstract

Every cryptographic design has to be secure to fulfil its function properly. As side-channel attacks are becoming easier and easier to perform, designers of secure circuits must pay attention to implementing various countermeasures against these attacks. However, in some cases, their hard work can be thwarted if automatic optimizations invalidate the defences.

During work on implementing different countermeasures in FPGA, colleague Jan Brejník [1] has found out that the vulnerability to side-channel attacks is not affected solely by the countermeasures used, but also significantly by the configuration of synthesis parameters. Synthesis is a batch of processes that translate RTL description of a design to a configuration of the FPGA. This complex flow uses many different tools, which can be customized using various parameters, to implement the desired design on board. Changes in these parameters settings can have various consequences on the designs implementation properties, which includes its security. This work expands on Brejník's work and explores the effect of synthesis parameters settings on the vulnerability of the cryptographic designs implemented in FPGAs to side-channel attacks.

To evaluate how vulnerable the implemented design is, we utilize Test Vector Leakage Assessment based on Welch's t-test [2], in which the power consumption of implemented design is measured during encryption of chosen constant or random data. From these power traces, two sets are created, one containing power traces when constant data were encrypted and the other containing power traces when random data were encrypted. These two sets are then compared using Welch's t-test, and its output is used to conclude how vulnerable is the measured design to side-channel attack.

The design used for these tests is implementation of AES by Jan Brejník [1], which utilizes three countermeasures against side-channel attacks: S-Box Decomposition, Boolean Masking and Register Precharge [3]. For the purpose of this work, four parameters were chosen for testing. These are Keep Hierarchy, Register Balancing, Allow Logical Optimizations Across Hierarchy and Starting Placer Cost Table. These parameters are all from ISE Design Suite by Xilinx, which is a software tool for working with Xilinx programmable devices. The tool allows to synthesise, implement, analyse and simulate designs for FPGAs by Xilinx.

Measuring the impact of the parameters on security is done in two experiment groups. In the first group, the influence of Keep Hierarchy, Register Balancing and Allow Logical Optimizations Across Hierarchy is measured, as these parameters can affect each other. In the second group of experiments we solely test the influence of the Starting Placer Cost Table parameter by varying its value. We execute the

measurement for every combination of parameters and save the results, which are then processed with Welch's t-test. From these results, we get readings of maximal t-value during encryption, which should not go over 4.5 in a secure circuit, and getting higher values means the implementation tested could be vulnerable to side-channel attacks. [2]

We have found out that the Keep Hierarchy parameter had significant effect on security and Register Balancing had minor effect in some cases. The Allow Logical Optimizations parameter seemed to have very little to no effect on the vulnerability. We also evaluated the impact of a parameter Starting Placer Cost Table, which also proved to have no significant impact on the vulnerability.

In the measurements, we discovered an anomaly of high leakage of information at the end of some measurements. We attributed this to the way the chosen implementation of AES works with non-masked ciphertext after the encryption is done.

This work shows the significance of choosing the right synthesis parameters in security critical designs, that use some kind of countermeasures against side-channel attacks. To make it that the hard work done by designers on these countermeasures will not be wasted, cautious decisions about the parameter settings should be made in places where security is of most importance.

Acknowledgment

I would like to thank my supervisor Dr.-Ing. Martin Novotný for all his advice and guidance through this research, which was extremely helpful.

References

[1] BREJNÍK, J. *Dynamic logic reconfiguration based side-channel attack countermeasures in FPGA*. Master's thesis, Czech Technical University in Prague, 2019.

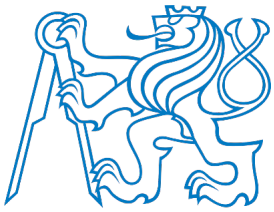
[2] Schneider, T.; Moradi, A. Leakage assessment methodology. *Journal of Cryptographic Engineering*, volume 6, no. 2, 2016: pp. 85–99.

[3] Sasdrich, P.; Moradi, A.; et al. Achieving side-channel protection with dynamic logic reconfiguration on modern FPGAs. In *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, IEEE, 2015, pp. 130–136.

Author Index

Sponsors

Czech Technical University in Prague



The conference has been sponsored by the CTU grant SVK 55/20/F8.

EATON

Eaton's mission is to improve the quality of life and the environment through the use of power management technologies and services. We provide sustainable solutions that help our customers effectively manage electrical, hydraulic and mechanical power – more safely, more efficiently and more reliably. Eaton's 2019 revenues were $21.4 billion, and we sell products to customers in more than 175 countries. We have approximately 95,000 employees.

SYSGO

SYSGO is the leading European provider of real-time operating systems for critical embedded applications. Our products have been designed to meet the highest requirements when it comes to Safety and Security. Our customers are leading players in the Avionics & Defense, Space, Railway, Automotive and Industrial Automation and Medical industries, who use our PikeOS product as a platform for critical systems that need to be certified against industry-specific Safety and Security standards.

CZ.NIC

CZ.NIC, interest association of legal entities, was founded by leading providers of Internet services in 1998. The association currently has 114 members. The key activities of the association include operation of the domain name registry for the .CZ domain, operation of the CZ top-level domain and public education in the area of domain names. The association is now intensively working on development of the DNSSEC technology and mojeID service, extension and improvements of the domain administration system and support of new technologies and projects beneficial to the Internet infrastructure in the Czech Republic. CZ.NIC is a member of the EURid association, managing the European domain – EU, and other similarly oriented organizations (CENTR, ccNSO etc.).

CESNET

CESNET is an association of universities of the Czech Republic and the Czech Academy of Sciences. It operates and develops the national e-infrastructure for science, research and education which encompasses a computer network, computational grids, data storage and collaborative environment. It offers a rich set of services to connected organizations.

ASICentrum

ASICentrum, established in 1992 in Prague is a design center of EM Microelectronic and a competence center of ETA, belonging to the Swatch Group. EM Microelectronic is one of the most innovative IC providers. It developed and manufactured the smallest and the lowest power consuming Bluetooth chip on the market, the top performing optical sensors for optical office as well as gaming mice and it was the first to release the award-winning world-first dual-frequency NFC + RAIN RFID emlecho.

Partners

IEEE Student Branch at Czech Technical University in Prague

IEEE Young Professionals

Computer (C) Society Chapter of the Czechoslovakia Section of IEEE

ASICentrum®
A COMPANY OF THE SWATCH GROUP

em microelectronic
A COMPANY OF THE SWATCH GROUP

★

DO YOU LOVE CHIPS?

NO, NOT THESE...

★

SUPER HOT CHIPS?

WE LOVE TO **DESIGN** THEM.

★ ★ ★ **JOIN US!** ★ ★ ★

ASICENTRUM PRAHA / BRNO