'Unified Side-Channel Attack - Model' (USCA-M): An Extension with Biometrics Side-Channel Type

Andrew Johnson
Faculty of Computing, Engineering, and Mathematics.
University of South Wales
Pontypridd, Wales
andrew.johnson@southwales.ac.uk

Dr. Richard Ward
Faculty of Computing, Engineering, and Mathematics.
University of South Wales
Pontypridd, Wales
richard.ward@southwales.ac.uk

***Abstract*— This paper presents the 'Unified Side-Channel Attack Model' (USCA-M) with an additional side-channel type of 'Biometrics.' The original published paper 'Introducing the Unified Side-Channel Attack – Model (USCA-M)' was presented and published through the International Symposium on Digital Forensics and Security (ISDFS) conference in 2020** [1]**. The USCA-M model was initially compiled by research on side-channel attacks (SCAs) from published journal articles and conference papers between 2015 and 2020. The study found that SCAs can be categorized into three main areas: SCA types, SCA methods, and SCA techniques. The USCA-M provides a unified model to categorize present and future SCA vulnerabilities and exploit techniques found. Its future use would provide a reference point for organizations to identify and place a found SCA within a standard or unified categorization. It can also be used to granulate SCA techniques into identifiable components to assist in defending SCAs, such as code pattern recognition and intrusion detection systems (IDS).**

Keywords — Side-channel attacks, model, Spectre, Meltdown, biometrics, Remote In-Flight Data Mode (RIDL), speculative execution, branch prediction side-channel type, side-channel attack method, side-channel attack technique.

I. INTRODUCTION

The previous publication described how exploiting vulnerabilities to extract data via a side-channel is known as side-channel attacks (SCAs), and how a SCA type can be further categorized into SCA methods and subsequent techniques used to carry out an attack. The scope of SCA methods and techniques used to exfiltrate data is broad, as are the hardware targets used to demonstrate the data extraction. Published works over the last five years have targeted a variety of hardware, including CPUs [2][3][4], Field Programmable Gate Arrays (FPGAs) [5][6][7], and Dynamic Random Access Memory (DRAM) [8][9] [10].

SCAs have been extensively studied, with many papers published since its inception in 1996 by Kocher [11], who demonstrated data extraction via cache timings, the earliest demonstration of a timing side-channel exploitation. Surveys of papers have also been published [12][13][14][15]. Hence the research in this field has provided an innovative and expanding science into how data can be extracted from computer systems by various side channels.

A further side channel not included in the original work – 'Biometrics' is now included as an additional 'physical' side-channel type alongside relevant placement within the original USCA-M. The new biometric SCA has a physical side-channel type described in Section II with the other eleven SCA types. Two new biometric SCA methods with associated biometric SCA techniques are described in Section III.

II. USCA-M: SCA TYPES

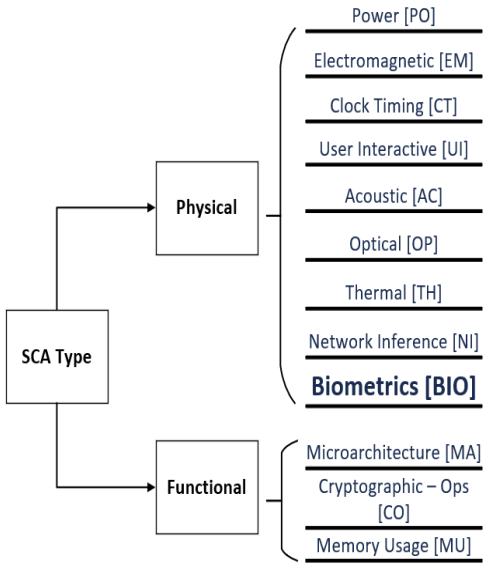

Fig. 1. Showing the grouping of the physical SCA types with the biometric inclusion

Fig. 1., a SCA type can either be physical or functional, and research identified twelve SCA types – nine physical types and three functional types. Physical SCA types are components of a computer system that can have a measurable by-product produced by its implementation. For example, the power side-channel type (PO) has a measurable component (voltage), and the electromagnetic (EM) type emissions can be measured via their frequency in hertz. Spreitzer *et al.* concur with the physical classification of SCAs, and they also describe the functional SCA types as 'logical' in their work [13]. A high-level description of physical and functional SCAs is next described.

A. Physical SCA Type

All physical SCA types have measurable by-products. The following sections describe the SCA types briefly for clarity, and all of the types have been exploited in previously published works. In the context of biometrics, the by-product is the human features such as the face, iris, fingerprint, and voice that can be imitated. In the case of biometric

cryptography, the templates of human features used to generate crypto-keys can be extracted.

1) Power [PO]

Electronic circuits consist of voltage (V), current (I), and resistance (R). The term 'power' relates to voltage. Voltage levels in any computer circuit can be measured as V = IR. When a CPU operates, the instructions that carry out the operation use a different voltage and current levels. Hence, there is a measurable differentiation in the levels of power used between instructions.

2) Electromagnets [EM]

Electromagnetic (EM) energy is a form of energy that is produced when current is propagated through a circuit. Specifically, a magnetic field is produced by a current flowing through a wire. The levels of EM energy produced are synonymous with the voltage levels as discussed in the power usage section above. Therefore, the frequency and amplitude of EM traces are also evident in the EM wavelengths produced in a circuit depending on which instructions are being processed by a computer.

3) Clock Timing [CT]

The internal clock of modern CPUs is itself a small processor that controls processing speed. Intel multi-core processors can carry out three of four instructions per clock cycle. In terms of memory timing, there is a vast difference (in computation) between the processing speeds of instructions and data that is held in primary memory (RAM), as opposed to the 'on chip' memory - cache (L1, L2, L3 or LLC). There is a point of contention regarding clock timing side channels. That is whether the type should be classified as functional micro-architectural (MA) types. However, this work will classify it as a physical SCA type.

4) User Interactive [UI]

At a very high level, the simplest example of a SCA is reading data from a user's display. Attacks such as 'shoulder surfing,' 'keystroke inference,' and 'gesture inference' are all examples of UI cyber attacks.

5) Acoustic [AC]

One of the earliest SCAs was conducted to decipher the 'clicks' of a cipher machine. Similarly, SCAs have been carried out on the audible acoustic clicks of printers and (older) PCs. A computer can also emit noise at a level not audible to humans that can be analyzed. In addition, noise can be induced into a computer system to corrupt data.

6) Optical [OP]

A Light Emitting Diode (LED) display at the front of desktop computers is becoming obsolete. The shift from desktops to laptops to tablets is ever-increasing, and the portability of computing has become more dominant and less spacious than a traditional desktop PC. However, as desktops are still used heavily in industry and education, some of their 'light emitting' side channels can be exploited. In particular, the LED display that flickers while a computer is processing has a wide variation in illumination levels unseen to the human eye that are measurable via highly sensitive cameras.

7) Thermal [TH]

Another side-channel by-product, perhaps less researched, is that of thermal dissipation or heat. It is noticeable that older computers with far less processing power and larger components generate more heat when the device becomes 'busy'. This temperature variation depends on the workloads of resource contention in the CPU, which again has measurable side effects.

8) Network Inference [NI]

Physically connected networks have properties that can be exploited, such as clamping onto the physical wires to extract data. Wireless networks are far more vulnerable targets to SCAs due to the 'openness' of packet switching techniques and network packet transfers that provide a side-channel for an adversary.

9) Biometrics [BIO]

In biometrics, it is the physical features of a human that forms part of the authentication process of a computer system. Attacks on biometric authentication are known as 'presentation attacks' (PSA) [16]. These attacks imitate human features, including fingerprints, facial recognition, iris recognition, speech, and even heartbeat signature recognition [17]. In addition, more recently, the unique features of the veins in a human finger are emerging as a new field in biometric security [18]. Galbally further identifies four parts that are the targets of biometric security in the context of SCAs [19]:-

1. Biometric characteristics.
2. The side channel measured.
3. The hardware components of the target system.
4. The type of system under attack.

The hardware components and systems are combined in this work to group them as 'hardware targets.'

III. USCA-M: SCA METHODS AND TECHNIQUES – BIOMETRIC

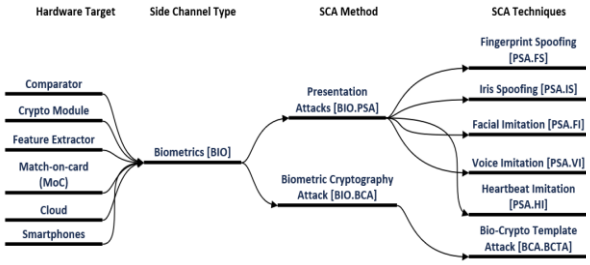

Fig. 2. The biometric USCA-M showing the hardware targets, side-channel type, SCA methods, and techniques

Fig. 2 shows the USCA-M methods and consequent techniques of biometric-based SCAs. The previous work on the USCA-M [1] describes the SCA techniques for the other 11 SCA types.

A. Presentation Attack [BIO.PSA] techniques

There are SCA techniques relating to how biometrics security can be exploited for the identification of the biometric presentation attack method.

1) Fingerprint Spoofing [PSA.FS]

This technique involves imitating the fingerprint of a human in the authentication process. The most common example is smartphone authentication. It is possible to create

a latex or wax material from a fingerprint that can be used to spoof a genuine fingerprint [20].

2) Iris Spoofing [PSA.IS]

Iris biometrics form a new age of human authentication as each human has a unique signature similar to a fingerprint that resides in the iris. However, research has shown that it is possible to duplicate the characteristics of an iris using contact lenses or even simple prints of an iris. Early work in iris spoofing is seen in work by Rathgeb and Uhl, who use a 'hill-climbing technique' to obtain access to iris biometric authentication [21].

3) Facial Imitation [PSA.FI]

Already used in airports to authenticate the human face to the passport photo [22], deep face recognition has become the most prevalent biometric authentication. However, facial imitation has been highly researched, and with the advent of biometric 'liveness' verification of facial biometrics, facial imitation is now extremely difficult. That is not to say that a simple photograph cannot be used to spoof an individual's identity on systems that do not utilize 'liveness' verification.

4) Voice Imitation [PSA.VI]

Voice identification is now used as an 'optional' biometric authentication mechanism for Her Majesties Revenue and Customs (HMRC) in the UK [23]. The security of voice identification is questionable as researchers have created voice imitation attacks through 'replay, voice conversion and speech synthesis' [24], which degrade the security of Automatic Speaker Verification (ASV) systems.

5) Heartbeat Imitation [PSA.HI]

For medical authentication of mobile-health solutions, the cardiac recordings of a human can be used. Medical authentication is a novel field of research. A recent paper by Seepers *et al.* shows how cardiac recordings were undertaken using technology such as remote 'photoplethysmography' (rPPG) as part of the authentication process is vulnerable to attackers pretending to be trusted devices that duplicate the cardiac signatures [17].

B. Biometric Cryptography Attack [BIO.BCA]

The use of biometrics as an additional security feature in cryptography has led to the evolution of biometric cryptosystems [19]. Even with this added complexity meant to thwart an adversary, they are still vulnerable to SCAs.

1) Bio-crypto Template Attack [BCA.BCTA]

Human feature recognition can be used to create a template to add an enhanced security feature of cryptographic key generation. However, in the same way, conventional templates are used, they are prone to SCAs. An early example provided by Delivasilis and Katsikas showed how templates from speech synthesis could be exposed [25].

IV. The USCA-M Design

The author used the research from papers published in the field of SCAs to create the USCA-M. The design of the USCA-M involved a testing methodology of existing exploit proof-of-concept (POC) code from authors of published journal articles such as Spectre [2], Meltdown [3], and, more recently, Remote In-Flight Data Load (RIDL) [26]. The testing methodology involved a four-phase testing process.

A. Phase 1 – USCA-M Exploit Placement

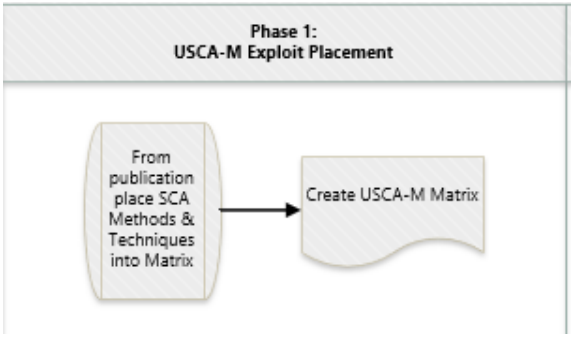

Fig.3. Phase 1: USCA-M Exploit Placement

In Fig.3, the first phase of the USCA-M design was to place an existing exploit into a USCA-M matrix, based on the research undertaken on the categorization of SCAs. An example matrix is shown below using the Specter v.1 exploit and the technique of Flush & Reload [2].

TABLE I. USCA-M Matrix example – Spectre Flush and Reload technique

USCA-M	
SCA Type	**CT**
SCA Method	**TA**
SCA Techniques	**FR**
Spectre v.1 Exploit	**x**

The above table represents the placement of the flush & reload technique used in the Spectre variant 1 exploit POC. From the above table, the abbreviations are:- CT=Clock Timing, TA=Timing Analysis, FR-Flush & Reload. Here, the flush & reload technique, part of the POC exploit, would categorize as **CT.TA.FR** within the USCA-M matrix.

B. Phase 2 – USCA-M Exploit Testing

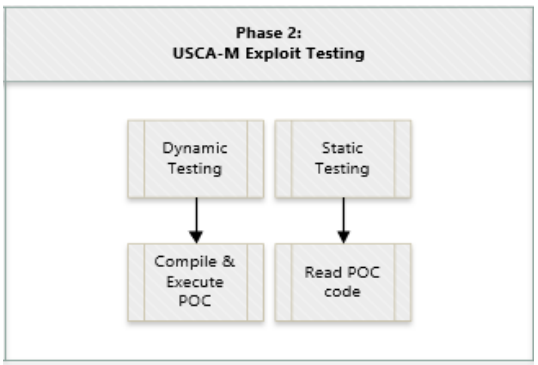

Fig.4. Phase 2:USCA-M Exploit Testing

In Fig.4, the next phase tests an existing exploit using static and dynamic testing of the exploit POC. The purpose of this

phase is to identify the critical components of code. For example, the Flush & Reload technique of the Spectre exploit [2], also used in RIDL [26], used assembly-level functions called CLFLUSH (cache line flush) and RDTSC (time stamp counter) to measure cache line eviction timings in clock cycles. The flush and reload technique is the critical component of the POC code that leaks sensitive information and is described by Kocher *et al.* as "*measuring the access time, the attacker learns whether the victim accessed the monitored cache"* [2].

C. Phase 3 – USCA-M Exploit Verification

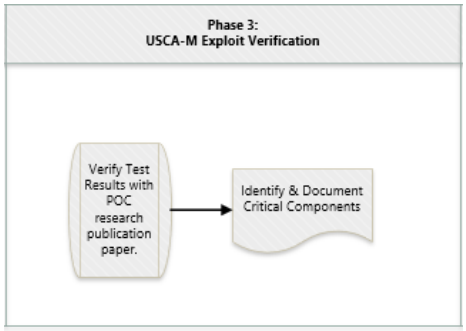

Fig.6. Phase 3: Exploit Verification

In phase 3, the test results are verified with the original published article work and check that the POC placement within a USCA-M matrix is correct.

D. Phase 4 – USCA-M Exploit Validation

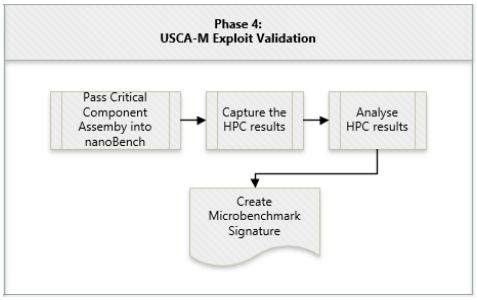

Fig.7. Phase 4:USCA-M Exploit Validation

In Fig.7., phase 4 of the USCA-M is the validation of the USCA-M design. The validation phase is essentially evaluating the usefulness of the USCA-M. The critical components identified in phase 2 were passed into a tool called 'nanoBench' [27]. The nanoBench tool by Abel and Reineke is a tool that can process single lines of assembly code or even single assembly instructions on the Intel x86 architecture to produce hardware performance counter (HPC) events of the micro-ops generated by specific instructions. These micro-ops events are then used to create a microbenchmark' signature' of low-level assembly instruction.

TABLE II. DISTRIBUTION OF MICRO-OPS ACROSS EXECUTION PORTS

	PORT_0	PORT_1	PORT_2	PORT_3	PORT_4	PORT_5	PORT_6	PORT_7
RDTSC	**4.00**	**6.00**	**0.00**	**0.00**	**0.00**	**2.00**	**8.00**	**0.00**
CLFLUSH	**0.00**	**1.00**	**1.00**	**0.00**	**1.00**	**0.00**	**1.00**	**0.00**

The singular instruction RDTSC and CLFLUSH have been passed through the nanoBench tool in the table above. The resulting distribution of the micro-ops distributed across the CPU execution ports for each instruction is shown. A microbenchmark signature can now be generated using the data collected.

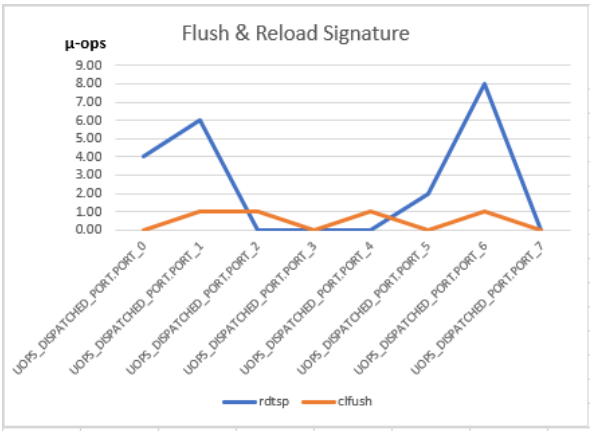

Fig.5. Flush & Reload Microbenchmark Signature

Fig.5. above shows a graph of the distribution of micro-ops across the eight execution ports within an Intel core i7 CPU. This Flush & Reload signature is helpful in that IDS could use it to identify code patterns evident in exploits during an attack.

V. SIMILAR AND FUTURE WORK

The Mitre Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework [28] is similar to the USCA-M. However, the ATT&CK framework does not include any techniques relating to the SCAs. The author of this work intends to make the USCA-M freely available to the public in the near future through resources such as GitHub as part of continuing research in the SCA field.

VI. CONCLUSION

This work extends the previously published work entitled 'Introducing the Unified Side-Channel Attack – Model' (USCA-M)' [1]. The extension provides an additional SCA type - Biometrics, and some of the security vulnerabilities that the human-centric side-channel can expose. The work here also highlights how the USCA-M has been developed into a 4-phase exploit testing process and can be further developed and expanded and utilized as a security categorization and benchmark for future discovered SCAs.

VII. References

[1] A. Johnson and R. Ward, "Introducing The 'Unified Side-Channel Attack - Model' (USCA-M)," in *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, 2020, pp. 1–9.

[2] P. Kocher *et al.*, "Spectre Attacks: Exploiting Speculative Execution," *40th IEEE Symp. Secur. Priv.*, 2018.

[3] M. Lipp *et al.*, "Meltdown: Reading Kernel Memory from User Space," *27th USENIX Secur. Symp. (USENIX Secur. 18)*, 2018.

[4] J. Van Bulck *et al.*, "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution," *Proc. 27th USENIX Secur. Symp.*, 2018.

[5] M. Zhao and G. E. Suh, "FPGA-Based Remote Power Side-Channel Attacks," in *Proceedings - IEEE Symposium on Security and Privacy*, 2018, doi: 10.1109/SP.2018.00049.

[6] C. Ramesh *et al.*, "FPGA Side Channel Attacks without Physical Access," in *Proceedings - 26th IEEE International Symposium on Field-Programmable Custom Computing Machines, FCCM 2018*, 2018, pp. 45–52, doi: 10.1109/FCCM.2018.00016.

[7] M. Tang *et al.*, "Side-Channel Attacks in a Real Scenario," *Tsinghua Sci. Technol.*, vol. 23, no. 5, pp. 586–598, 2018, doi: 10.26599/tst.2018.9010047.

[8] D. Gruss *et al.*, "Another Flip in the Wall of Rowhammer Defenses," in *Proceedings - IEEE Symposium on Security and Privacy*, 2018, doi: 10.1109/SP.2018.00031.

[9] R. Qiao and M. Seaborn, "A new approach for rowhammer attacks," in *Proceedings of the 2016 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2016*, 2016, doi: 10.1109/HST.2016.7495576.

[10] Y. Xiao, X. Zhang, Y. Zhang, and R. Teodorescu, "One Bit Flips, One Cloud Flops: Cross-VM Row Hammer Attacks and Privilege Escalation," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, 2016.

[11] P. C. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," *Crypto*, pp. 104--113, 1996, doi: https://doi.org/10.1007/3-540-68697-5_9.

[12] Y. Zhou and D. Feng, "Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing," *Inf. Secur. Semin. WS 0607*, no. 60503014, pp. 1–34, 2005.

[13] R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard, "Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices," *IEEE Commun. Surv. Tutorials 20(1)*, vol. 20, no. 1, pp. 465–488, 2018, doi: 10.1109/COMST.2017.2779824.

[14] J. Szefer, "Survey of Microarchitectural Side and Covert Channels , Attacks , and Defenses," *J. Hardw. Syst. Secur. 3(3)*, pp. 219–234, 2019, doi: 10.1007/s41635-018-0046-1.

[15] Y. Lyu and P. Mishra, "A Survey of Side-Channel Attacks on Caches and Countermeasures," *J. Hardw. Syst. Secur.*, pp. 33–50, 2017, doi: 10.1007/s41635-017-0025-y.

[16] R. Tolosana, M. Gomez-Barrero, C. Busch, and J. Ortega-Garcia, "Biometric Presentation Attack Detection: Beyond the Visible Spectrum," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1261–1275, 2020, doi: 10.1109/TIFS.2019.2934867.

[17] R. M. Seepers, W. Wang, G. De Haan, I. Sourdis, and C. Strydis, "Attacks on heartbeat-based security using remote photoplethysmography," *IEEE J. Biomed. Heal. Informatics*, vol. 22, no. 3, pp. 714–721, 2018, doi: 10.1109/JBHI.2017.2691282.

[18] K. Shaheed, A. Mao, I. Qureshi, M. Kumar, S. Hussain, and X. Zhang, "Recent advancements in finger vein recognition technology: Methodology, challenges and opportunities," *Information Fusion*, vol. 79. pp. 84–109, 2022, doi: 10.1016/j.inffus.2021.10.004.

[19] J. Galbally, "A new Foe in biometrics: A narrative review of side-channel attacks," *Computers and Security*, vol. 96. 2020, doi: 10.1016/j.cose.2020.101902.

[20] O. Kanich, M. Drahanský, and M. Mézl, "Use of creative materials for fingerprint spoofs," in *IWBF 2018 - Proceedings: 2018 6th International Workshop on Biometrics and Forensics*, 2018, pp. 1–8, doi: 10.1109/IWBF.2018.8401565.

[21] C. Rathgeb and A. Uhl, "Attacking iris recognition: An efficient hill-climbing technique," in *Proceedings - International Conference on Pattern Recognition*, 2010, pp. 1217–1220, doi: 10.1109/ICPR.2010.303.

[22] Gatwick Airport Ltd, "Biometric ID," 2022. [Online]. Available: https://www.gatwickairport.com/at-the-airport/flying-out/security/biometric-id/. [Accessed: 26-Apr-2022].

[23] HM Revenue & Customs, "Voice Identification Privacy Notice," 2018. [Online]. Available: https://www.gov.uk/government/publications/voice-identification-privacy-notice/voice-identification-privacy-notice. [Accessed: 26-Apr-2022].

[24] S. K. Ergünay, E. Khoury, A. Lazaridis, and S. Marcel, "On the vulnerability of speaker verification to realistic voice spoofing," in *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems, BTAS 2015*, 2015, doi: 10.1109/BTAS.2015.7358783.

[25] D. L. Delivasilis and S. K. Katsikas, "Side channel analysis on biometric-based key generation algorithms on resource constrained devices," *Int. J. Netw. Secur.*, vol. 3, no. 1, pp. 44–50, 2006.

[26] S. Van Schaik *et al.*, "RIDL: Rogue in-flight data load," in *Proceedings - IEEE Symposium on Security and Privacy*, 2019, doi: 10.1109/SP.2019.00087.

[27] A. Abel and J. Reineke, "nanoBench: A Low-Overhead Tool for Running Microbenchmarks on x86 Systems." 2020.

[28] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "MITRE ATT&CK - Design and Philosophy," 2018. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf.