Noname manuscript No.
(will be inserted by the editor)

Security Beyond Cybersecurity: Side-Channel Attacks Against Non-Cyber Systems and their Countermeasures

Aaron Spence · Shaun Bangay

the date of receipt and acceptance should be inserted later

Abstract Side-channels are unintended pathways within target systems that leak internal information, exploitable via *side-channel attack* techniques that extract the target information, compromising the system's security and privacy. Side-channel attacks are well established within the cybersecurity domain, and thus their cyber-physical systems are actively defended with countermeasures. Non-cyber systems are equally as vulnerable to side-channel attacks, however this is largely unrecognised and therefore countermeasures to defend them are limited. This paper surveys side-channel attacks against non-cyber systems and investigates the consequent security and privacy ramifications. Side-channel attack techniques rely on respective side-channel properties in order to succeed, therefore countermeasures that disrupt each side-channel property are identified, effectively thwarting the side-channel attack. This principle is captured within a countermeasure algorithm: a systematic and extensible approach to identifying candidate countermeasures for non-cyber systems. We validate the output of this process by showing how the candidate countermeasures could be applied in the context of each non-cyber system and in the real-world. This work provides an extensible platform for translating cybersecurity-derived side-channel attack research into defending systems from non-cyber domains.

Keywords side-channel attack · countermeasure · cybersecurity · side-channel sensing

Aaron Spence
aaron.spence@deakin.edu.au
Deakin University, Geelong, 3216, Australia

Shaun Bangay
shaun.bangay@deakin.edu.au
Deakin University, Geelong, 3216, Australia

1 Introduction

Side-channels are unexpected physically observable information leakages from target systems, such as computing systems, that can be exploited to reveal target information contained or generated within these systems. Active countermeasures are required to address the security and privacy risks due to the loss of control of such target information. The domain of cybersecurity (**CYB**) has formal underpinnings with respect to side-channel usage with its *side-channel attack* (**SCA**) frameworks [1,2,3,4], providing definitions and taxonomy, systematic methodologies and techniques that one can apply to attack a target system for the purpose of obtaining target information. Incorporated within the SCA frameworks is the development of countermeasures against SCA, a cat-and-mouse game between attackers and defenders. For example, a SCA might recover cryptographic keys by sensing modalities such as power consumption [5] during the encryption process. SCAs are traditionally focused on the characteristics of the systems within the CYB domain: electronic-based target systems, and a mindset that target systems are to be attacked or outmanoeuvred to bypass active countermeasures (e.g. encryption, leakage countermeasures), often through unexpected modifications or covert means.

Side-channels are not limited to CYB-related target systems. Systems from other domains have also been shown to have discoverable and exploitable side-channels [4], with such domains herein denoted as **non-CYB**[1]. While CYB-related systems assess the threat

[1] In this paper, the acronym CYB refers to cybersecurity and side-channel attacks on computing systems. The term non-CYB still focuses on security and side-channel attacks but where the systems are non-computational (or non-cyber) in nature.

and actively defend with countermeasures, non-CYB domains typically are vulnerable. This paper investigates the consequent security and privacy ramifications of SCAs deployed against target systems *beyond those traditionally associated with the CYB domain* (i.e. against non-CYB systems), and identifies candidate countermeasures. For example, SCAs against the human body can be used to covertly extract health-related target information such as heart rate, compromising one's privacy, and providing potential leverage during a negotiation.

The goals of this paper are to:

1. Survey the existence of non-CYB SCAs, by identifying SCAs (that meet criteria validated against the frameworks) in non-CYB systems.
2. Demonstrate how the security and privacy of non-CYB systems are vulnerable to SCAs.
3. Devise a method for the systematic identification of candidate countermeasures to defend non-CYB systems from SCAs.
4. Apply this algorithm to the non-CYB case studies to identify candidate countermeasures.

Through this work, we present the following contributions:

1. Demonstrates the applicability of SCAs against non-CYB systems, with details of the consequent security and privacy risks.
2. A novel dissection of side-channels that identifies the fundamental properties that they are comprised of.
3. A methodology for mapping SCA techniques to the respective side-channel properties they exploit to succeed.
4. A methodology for mapping CYB-derived countermeasures to the respective side-channel properties that they disrupt.
5. A countermeasure algorithm to systematically identify candidate countermeasures that are applicable to a given target system. This algorithm can be extended as fresh SCA strategies are developed.

This paper begins with an introduction of side-channels and the key properties that they consist of (section 2), followed by a forward introduction to a non-CYB target system shown to be vulnerable to SCAs (section 3). Section 4 collates SCA techniques and maps them to the respective side-channel properties that they exploit to succeed. Following is an investigation of how SCA techniques were utilised against non-CYB target systems, and the consequent security and privacy ramifications (section 5). Then, candidate countermeasures derived from the CYB literature are collated to form the basis for the development of a countermeasure algorithm: a systematic and reproducible approach for identifying candidate countermeasures for a given target system (section 6). To conclude, we validate the output of the countermeasure algorithm process by showing how the candidate countermeasures could be applied in the context of each non-CYB system and in the real-world.

2 Side-Channels

Side-channels are the *unexpected physical leakage* of target information from a target system via hidden or unknown channels. Side-channels deterministically correlate the internal operations of the system (e.g. execution of algorithms) to leaked signals (e.g. power consumption): the key property that SCAs exploit to succeed. They allow information to be obtained *indirectly* through pathways and/or modality transformations to outmanoeuvre implemented countermeasures, or access target information through novel means. For example, data on a PC may be protected by encryption. During execution of the encryption algorithm power consumption signatures are output that reliably correlate with the internal operations being perform, thus revealing enough information to recover the encryption key perhaps via differential power analysis [5]: an unintended side-channel. Analysis in the following sections demonstrate that SCAs against target systems from any domain depend on one or more of the following properties that make up a side-channel:

- **Modality Transformations**: target information is transformed between different sensory modalities during its traversal along its side-channel from its source to the sensing location.
- **Multi-stage Pathways**: a side-channel consists of an indirect pathway comprised of multiple nodes, and may branch into additional side-channels. The pathway is likely to traverse between multiple internal system components making discovery of all paths non-trivial.
- **Determinism**: the correlation between internal operations and the output signals must be reproducible.
- **Signal Mixing**: side-channels are subject to mixing with other channels. Target information that is not directly accessible may instead be detected when it is mixed in with another signal.
- **Varying Amplitude**: the target information within a side-channel may be difficult to detect due to its low amplitude when mixed with other signals.
- **Multivariate**: a single target information source can have multiple side-channels associated with it, increasing the number of attack vectors available.

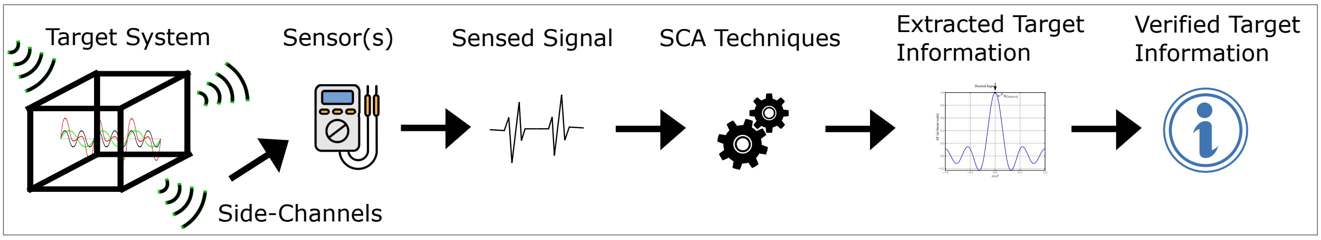

Figure 1 The SCA process. Target systems from any domain contain side-channels, highlighting the applicability of the SCA process to beyond CYB-related systems.

The breadth of examples present in both CYB and non-CYB literature demonstrate that even an individual system contains many side-channels, even for the same source of target information [4]. A key contribution of this paper is that side-channels exist within *any* target system, not just those traditionally associated with CYB, and thus the consequent security and privacy risks are also relevant to non-CYB systems. The following section expands on this with a detailed example as a prelude to categorizing the application of SCAs against target systems beyond those traditional to the CYB domain. Section 4 then classifies the analysis techniques employed to perform SCAs, and their dependence on the side-channel properties listed above.

3 SCAs in Non-CYB Target Systems - Prologue

3.1 Inferring Human Thoughts via EEG Readings of the Brain

Typically, literature outside the CYB domain does not recognise or consider the presence and potential of side-channels within their respective target systems [4]. Martinovic et al. [6] and Lange et al. [7] represent a handful of works that counter this trend, recognising explicitly the transferability of SCA techniques and mindsets to biological systems. The SCA category of *profiled attacks* was employed (section 4.1), in combination with the SCA techniques of *machine learning* (section 4.2) and *information theoretical approaches* (section 4.2).

As an example (see section 5 for the remaining case studies): reading thoughts by analysing electroencephalograms (EEG) signals is an example of side-channel sensing whereby information in a ‘closed’ system can be inferred from the complex mix of signals acquired by an external sensor [6,7]. At its foundation, the brain can be viewed as a bounded system with inputs and outputs of various modalities, akin to the power consumption of a PC, with a plausible correlation existing between the internal operations (thought processes) and the acquired signals (EEG): an unexpected side-channel. The authors exploit a neurophysiological actuality known as the Event-Related Potential (ERP): signatures within EEG readings that correspond with certain visual and auditory stimuli (the side-channel). EEG readings are collected from participants who are shown sets of visual information such as pictures of people they may know. Collected EEG readings are analysed via a series of statistical and regression analysis for classification and dimensionality reduction to extract the ERP that indicates a positive reaction to the currently presented visual information shown.

Potential privacy risks include collecting EEG data from an individual to act as a fingerprint of a person for identification purposes, or to inadvertently reveal private information such as their bank PIN or home address. While this case study is only at a prototyping stage and thus does not yet pose any immediate security and privacy risks, future iterations which improve on its robustness would require a reassessment. To address risks, countermeasures are suggested alongside the introduction of the developed countermeasure algorithm in section 7.

4 SCA Techniques within CYB

SCA techniques are designed to exploit side-channels to acquire target information not accessible directly, with an emphasis on exploiting weaknesses within systems, outmanoeuvring implemented defences, and performing covert sensing. Despite their CYB domain origin these techniques are just as applicable for non-CYB target systems [4]. Established SCA frameworks [1,2,3, 4] unify the field through formalisation and taxonomy to advance and share techniques within the CYB community.

4.1 SCA Categories

The SCA framework literature identifies the following SCA categories. The categories detail the *methodology* by which side-channel signals are acquired. These are

		SCA Techniques												
		DPA (or DEMA)	SPA (or SEMA)	CPA	Template attack	Signature matching	Maximum likelihood	Cryptanalysis	Transformation	Timing attacks	Fault injection	Deep learning	Supervised machine learning	Unsupervised machine learning
SCA Categories	Invasive Attacks										✓			
	Non-Invasive Attacks	✓	✓	✓										
	Active Attacks	✓	✓								✓			
	Passive Attacks	✓	✓	✓			✓			✓				
	Remote Attacks	✓	✓	✓				✓	✓					
	Local Attacks	✓	✓	✓		✓		✓		✓	✓			
	Profiled Attacks	✓	✓		✓				✓			✓	✓	
	Non-Profiled Attacks	✓		✓			✓	✓						✓
	Utilising Existing Third-Party Data					✓								
	Multivariate Attacks	✓	✓	✓			✓			✓				

Table 1 The SCA techniques can be grouped under the SCA categories, describing the methodology of the attack.

then paired with a SCA technique to extract the embedded target information from the acquired side-channel signal(s) (see Table 1).

- **Invasive vs Non-Invasive Attacks:** invasive approaches modify the components of the target system, for example removing component shielding, to acquire information leakages by exposing additional side-channels [8,9,2]. Non-invasive attacks only exploit externally available leakages.
- **Active vs Passive Attacks:** active attacks modify the operation of the target system so as to invoke measurable leaked signals via the side-channel, to learn about the internal operations, or to entice the primary internal operation to execute in more obvious measurable ways [2]. Tactics include the purposeful execution of operations that trigger measurable side-channels [10,2], feeding in particular input [11], or fault injection attacks (introducing errors) [12]. Passive attacks leave the system's operations undisturbed.
- **Remote vs Local Attacks:** some modalities can be measured from a distance by remote sensing, for example electromagnetic radiation emitted from a laptop [2]. Being closer to the source of the emitting modality typically achieves a clearer extraction of the desired signal. Remote sensing is fitting when there is a desire to attack covertly.
- **Profiled vs Non-Profiled Attacks:** profiled attacks, such as template attacks and stochastic model attacks, consist of (i) a profiling phase, and (ii) a side-channel extraction (or attack) phase [13,2]. During (i), with control over the target system (or a replica) a large number of signals are acquired and analysed to build a profile of the operations and behaviour of the system, at times with the utilisation of a supervised machine learning classifier [14,2]. During (ii), the side-channel can be sensed or acquired, and the previously built profiles assist with extraction of the target information. When a profiled attack is not possible, non-profiled attacks use signal processing techniques (e.g. a differential power analysis (DPA) [13]). More recent developments utilise deep learning techniques for non-profiled attacks where limited signals are available [15].
- **Utilising Existing Third-party Data:** existing data from a third-party may contain the target information, where it is possible that the data was not originally perceived to contain any embedded security or privacy comprising information. For example, identifying the media consumed on a TV can be obtained via the publicly available data from the home's smart power meter, an unexpected source [16].
- **Multivariate Attacks:** a single target information source can have multiple side-channels associated with it, providing the opportunity for a multivariate attack [17]. One approach to collate the different streams of signals is to identify the mutual and principal information between them through mutual information analysis and principal component analysis [17]. Recent works have utilised deep learning

algorithms such as deep neural networks which are trained to combine related information [18].

The applicability of SCA categories and subsequent SCA techniques is dependent on numerous factors such as the level of access and control of the target system obtained, whether being covert is an objective, and the properties of the modalities being sensed (e.g. do they propagate over distances or through materials). For example, attacks with a covert objective may be limited to *remote attacks* without the option for a *profiled attack*. Or conversely, where direct access to a target system is permitted, an *invasive* and *active attack* may yield stronger results by being able to manipulate the system, perhaps employing a *fault injection attack* to observe consequent output.

4.2 SCA Techniques

In combination with the SCA categories employed, SCA techniques analyse the acquired side-channel signal(s) to extract the embedded target information. While the set of signal processing, information theoretical, machine learning, and statistical analysis techniques applicable for SCAs is considerable, the high-level groupings below cover the most common techniques described in SCA frameworks and classifications:

- **Power Analysis Attacks:** exploiting the power consumption of target systems is the most established SCA technique, born from the seminal works of Kocher et al. [5]. Many variations exist, with differential power analysis (DPA), simple power analysis (SPA), and correlation power analysis (CPA) considered the primary set [19]. There is a strong correlation between the sensed power consumption signals and the internal operations of the target system. Differential electromagnetic analysis (DEMA) and simple electromagnetic analysis (SEMA) involve similar techniques as DPA and SPA respectively but have been adapted for side-channels with an electromagnetic radiation modality [19].
- **Information Theoretical Analysis:** encompasses SCA techniques with algorithmic processes steeped in information theory (e.g. Shannon's entropy, Hamming weights). This category tackles SCA by viewing the task of extracting target information from a mixed signal where all the other information sources can be temporarily regarded as noise. Included are established SCA techniques such as template attacks [13], cryptanalysis [20], timing attacks [21], and template attacks (such as stochastic or signal detection and estimation theory approaches [13]). Other techniques derive from statistical analysis, such as maximum likelihood [22, 14], signature matching techniques [16], correlation or simple regressions, and transformations (e.g. FFTs).
- **Fault Injection Attacks:** injection of a signal into the target system invokes malfunctions or unintended behaviour with observable and reproducible output signals to reveal insights into the inner workings of the system [19]. Such attacks require direct and unimpeded access to the original target system or a duplicated model. Examples include optical fault injection and electromagnetic fault injection to manipulate transistor states, and manipulations of system components such as cycle clock speeds or to under volt the CPU [2].
- **Machine Learning:** the supervised and non-supervised variants are akin to *profiled* and *non-profiled attacks* respectively [23]. Deep learning techniques such as convolutional neural networks offer the ability to automate the feature extraction stage when given a dataset of sensed side-channels. This provides opportunities to identify new side-channels [24]. Furthermore, deep learning provides opportunities for automated target information extraction, and perhaps identification of novel side-channels through previously unknown correlations with target information, given a sufficient and sizeable training collection of sensed signals [25, 18].

SCA techniques exploit the key characteristic of side-channels: the correlation between the internal operations of the system and a leaked signal. Deeper analysis can map which *key side-channel properties* (see section 2) each SCA technique depends on to succeed, as summarised in Table 2. Mapping for each SCA technique is achieved by individually assessing each of the six side-channel properties within the context of how each SCA technique operates (see Figure 2 for a graphical representation of side-channel properties). For example, considering for a DPA attack the target information's flow from its source (e.g. a passkey in memory) to sensor (e.g. power consumption meter), there is firstly a dependence on a *modality transformation* of the target information from virtual (e.g. a passkey represented virtually in memory) to electrical (e.g. CPU's power consumption during encryption). Secondly, there is a reliance on the deterministic nature of side-channels such that repeated measurements give the same target information. And thirdly, the target information may be of a *varying amplitude* which supports the need for a DPA attack where a statistical analysis of many readings of the side-channel is required rather than a single or few readings such as with a SPA attack.

Notable is that modality transformation is an exploited property relied on by all SCA techniques, as

	Side-Channel Properties					
SCA Techniques	Modality Transformation	Multi-stage Pathways	Determinism	Signal Mixing	Varying Amplitude	Multivariate
DPA	✓		✓		✓	
SPA	✓		✓			
CPA	✓		✓			
Template Attack	✓		✓			
Signature Matching	✓		✓			
Maximum Likelihood	✓	✓	✓			
Cryptanalysis	✓	✓	✓	✓	✓	
Transformation	✓	✓	✓			
Timing Attacks	✓	✓	✓			
Image Processing	✓	✓	✓		✓	
Correlation or Simple Regression	✓	✓	✓			
Source Separation	✓	✓	✓	✓		
Radio Detection Finding	✓		✓		✓	
Estimation and Decision Theory	✓		✓		✓	
Fault Injection Attack	✓	✓	✓		✓	
Deep learning	✓	✓				
Unsupervised learning	✓					
Supervised learning	✓					

Table 2 SCA Techniques to Side-Channel Properties (SCAT-SCP): Each SCA technique exploits particular side-channel properties to succeed.

may be expected by the very nature of *side*-channels: indirect leakage of target information. Determinism and providing a reproducible connection to the target information is also noted as a critical component of SCA techniques. Worth noting is that none of the SCA techniques listed relied on multivariate sensing to succeed. This mapping forms the basis for the developed countermeasure algorithm presented in section 7.

5 SCAs Against non-CYB Target Systems

This section enumerates SCA techniques that have been applied to target systems beyond those traditional to the CYB domain (i.e. non-CYB systems). Each case study has been matched with its corresponding SCA categories (see section 4.1) and SCA techniques (see section 4.2), and summarised in Table 3. The non-CYB target systems are sourced from a range of domains such as civil infrastructure, biological, and environmental. In common with CYB systems, each is a bounded system that contains or generates target information that is accessible indirectly (and sometimes covertly) through unintended information leakage (i.e. side-channels) of various modalities. Any side-channels discovered can be quantified using SCA techniques to extract embedded target information. The consequent security and privacy ramifications are identified, with further contributions made through the systematic proposal of candidate countermeasures in section 7.

5.1 Literature Methodology

The below case studies are sourced from a variety of literature. Case studies included are those that have used side-channels (section 2), albeit implicitly, to extract potentially *sensitive or private* target information. ‘Side-channel’ as a search keyword yields limited success as the term is seldom recognised outside of the CYB domain. Therefore, case studies are seeded from popular press articles reporting on unexpected or non-trivial sensing opportunities. The papers and research groups behind these articles are identified and linked through references and areas of research to identify additional case studies. Solutions where a direct measurement is made are excluded, for example a solution that uses a camera combined with machine learning to detect the movement of humans, as this lacks the *indirect* and *unexpected* characteristics associated with *side*-channels.

5.2 Geo-location Tracking via Frequency Variance on Electrical Grids

Garg et al. [26] demonstrate that the light source within a room present in a video recording can be used to approximate the geolocation of where the video recording originated. Electrical grids of the eastern United States have variance in their frequency on the order of ~50-100Mhz, denoted as an Electrical Network Frequency (ENF) signal. ENF signals are a result of load balancing across the grid and are unique to the geolocation of the grid. The light source from within a video recording can be analysed to derive a signature of the power frequency, and when compared to an ENF database of grids (utilising existing third-party data, 4.1) an inference can be made of the geolocation of where the video recording took place. The case study employs various filtering and *correlation or simple regression* techniques which are akin to a signature matching technique (4.2) from CYB. This solution shares commonality with CYB solutions: it essentially utilises power consumption as

Case Study	Security/Privacy Risks	SCA Techniques	Technique class
Inferring Human Thoughts via EEG Readings of the Brain [7, 6]	Inferring internal thoughts	Linear discriminant analysis (LDA)	Correlation or Simple Regression
Geo-location Tracking via Frequency Variance on Electrical Grids [26]	Geo-location inferred	Correlation coefficient	Correlation or Simple Regression
Automated Pothole Detection via Accelerometer Vibration on Road Networks [27]	Location/Route tracking	Custom filters influenced by machine learning	Custom filters
Heart Rate Detection via Photoplethysmography of the Face [28]	Inferring medical health, stress levels, psychological state	Pearson's correlation test	Correlation or Simple Regression
Heart/Breathing Rate via WiFi on the Chest [29]	Inferring medical health, stress levels, psychological state	Frequency modulated carrier waves (FMCW), FFT	Transformations
Inferring Psychological State by Reading Pupillary Response [30]	Infer psychological state such as cognitive load, reaction to visual stimuli, and stress levels	Convolutional neural network (CNN)	Deep learning
Movement Tracking via WiFi in the Open Environment[31]	Covert detection and tracking of people	Flash nulling, Inverse synthetic aperture radar (ISAR), radio detection finding (using the MUSIC algorithm)	Radio detection finding (RDF)
Surreptitious Audio-Recovery from Video Footage of Objects [32]	Covert, at distance, listening of audio and conversations	Complex steerable pyramid, Transfer coefficients	Source separation
Non-Line-Of-Sight Viewing of Objects with Reflected Light [33]	Covert ability to see without need of line-of-sight	Frequency wave-number migration (also known as f-k migration)	Imaging, Transformations

Table 3 Non-CYB target systems identified as targets of SCA techniques, with consequent security and privacy risks.

its attack vector, much like *DPA* attacks against PCs (4.2), however on an entirely different target system. The security significance of such an attack is due to its applicability to any video, thus raising privacy concerns for anyone who uploads videos online (perhaps to YouTube) as their location could be compromised.

5.3 Automated Pothole Detection via Accelerometer Vibration on Road Networks

The accelerometer and GPS within a smartphone can together automatically detect the presence of road potholes [27]. Data is collected while the smartphone is sitting on the dashboard of participating taxi drivers during their routine workday and routes. The authors developed a series of *custom filters* (4.2) for the 3-axis accelerometer data of the vibrations felt whilst driving to identify the vibration changes introduced by potholes. A pairing via timestamps between the GPS data and an aggregate of accelerometer signals over long time frames (weeks to months) reveals the locations of the potholes identified; an example of a *multivariate attack* (4.1). The location of identified potholes itself does not qualify as sensitive information, therefore the security concerns there are negligible. However, a signature match between the known number of potholes along every road, and the number of potholes detected via an accelerometer during a trip, could be used to infer the route a passenger has taken without the need to resort to GPS tracking.

5.4 Heart Rate Detection via Photoplethysmography of the Face

Video recordings of a person's face (*remote attack*, 4.1) via a smartphone can be processed to derive their heart rate [28]. This replicates the diagnostic technique of photoplethysmography (PPG), where light that reflects off the skin is influenced by the volume of blood present in the blood vessels beneath the skin, returning a periodic signal in accordance to oxygen being pumped and then depleted on each pulse (*profiled attacks*, 4.1). Video recordings can be processed via face detection techniques to isolate the region of interest, and filtering and correlation tests (Bland-Altman plots, Pearson's correlation test) (*correlation or simple regression*, 4.2) are applied to extract the target information. Consumer webcams have also been shown to be sufficient for acquiring PPG [34], thus performing such an attack covertly in the real-world is plausible, for example during an online video call. Knowing a person's heart rate can be used to infer medical health (e.g. presence of an arrhythmia), stress levels [35], or even psychological state such as whether they are lying [36]. Such knowledge could also be used for social engineering purposes, where an attacker could better gauge the victim's responses to the attacker's probing queries, perhaps during a job interview or when bidding during an auction. The current state of this technology requires recordings ~20 seconds in length of a completely stationary participant, therefore does lack robustness in real-world deployments, somewhat mitigating their security and privacy risks for the time being.

5.5 Heart/Breathing Rate via WiFi on the Chest

WiFi signals broadcast into a room from consumer grade routers and reflected off a participant reveals the oscillations of their chest rising and falling in enough detail that an inference of their heart and breathing rate can be made [29]. The purposeful emission of a signal (i.e. the WiFi signal) to conjure a side-channel is an example of an *active attack* (4.1). As the signals are reflected back and received by the router (*remote attack*, 4.1), frequency modulated carrier wave (FMCW) techniques are applied to isolate and differentiate between all objects present and their distances from the router. Extracting the signals associated with moving objects (e.g. humans) and the known properties of the signal (e.g. wavelength, distance travelled) reveal whether the person's chest is rising or falling (including the minute vibrations associated with a heart beat) by employing *transformation* techniques (i.e. FFT, linear regressions, iFFT) (4.2). Similar to the previously described case study above, knowing a person's heart and breathing rate can be used to infer medical health (e.g. presence of an arrhythmia), stress levels [35], or even psychological state [36]. This solution can be deployed without participant's consent, at remote distances, and exhibits a certain level of robustness, therefore is plausible for conducting covert attacks.

5.6 Inferring Psychological State by Reading Pupillary Response

Wangwiwattana et al. [30] exploit the known correlations between pupillary response (i.e. measuring the size and variance in pupil dilation), and cognitive and emotional states such as cognitive load, reaction to visual stimuli, level of alertness, and stress levels. Automated detection of pupillary response is achieved by filtering frames from video recordings of a participant's eyes to find the region of interest (the pupil) (*local attack*, 4.1), and then applying a convolutional neural network (*deep learning*, 4.2). While this kind of solution certainly has benevolent applications (e.g. monitoring alertness levels of pilots), the information inferred has similar security and privacy risks to knowing one's heart and breathing rates, such as revealing medical health or history, or gaining an advantage for social engineering purposes during interactions, perhaps within a job interview. Current implementations lack robustness as participants must be stationary, however more robust iterations could be achieved with inconspicuous and well-placed cameras (e.g. during an online video chat even).

5.7 Movement Tracking via WiFi in the Open Environment

Adib et al. [31] track the presence and movement of humans by broadcasting and receiving WiFi that has echoed off the surrounding objects (even *through walls*). WiFi from a consumer-grade router is emitted which reflects off inanimate and animate objects (*active attack*, 4.1), and returns back to the router (*remote attack*, 4.1). A 'flash nulling' technique cancels the impact of direct reflections and leaves remaining any signal that penetrated through the wall and reflected off objects on the other side. This case study uses an inverse synthetic aperture radar (ISAR) approach that allows a single antenna from the router to act as if it were an array of antennas for the tracking of objects moving through space. Received signals are distinguished as individual reflections via the MUSIC algorithm (4.2). This is a security risk relative to the detection or tracking of humans using traditional means such as cameras as it provides the opportunity for attacks to be performed covertly. Further works have investigated its effectiveness in the real-world and aim to improve its robustness [37] by deploying multiple coordinated routers, as well as expanding the target information that can be gleaned from such an attack to include activity recognition [38].

5.8 Surreptitious Audio-Recovery from Video Footage of Objects

Davis et al. [32] demonstrate that audio can be recovered from video footage of a nearby object that would not otherwise have been heard directly (such as when separated by distance or by glass). As audio propagates in its surroundings it interacts with nearby objects, causing them to vibrate upon impact in accordance with the sound waves. High frequency video recordings capture the vibration of objects that are in the vicinity of the audio source (e.g. an empty chip packet). Applying complex steerable pyramid filters, and other averaging, filtering and *source separation* techniques (4.2) to the video recordings allow for the reconstruction of the audio frequencies experienced by the object, translating them back into an audio signal. Given a powerful enough camera it is plausible for the solution to work at distance even when separated by glass (*remote attack*, 4.1) thus raising the possibility for covert eavesdropping. The current implementation of this case study is in the proof-of-concept stage, therefore its level of robustness is limited although should be reassessed to account for future advancements.

5.9 Non-Line-Of-Sight Viewing of Objects with Reflected Light

Lindell et al. [33] reconstruct the image of objects that are outside the line-of-sight of a camera, including objects that are around a corner or behind a wall. Picosecond pulses of light are directed at a wall that then reflect off the wall and onto the objects. These in turn reflect the light back onto the wall and then into a camera (*active attack*, 4.1, *remote attack*, 4.1). The light received by the camera on its return journey is analysed via frequency wave-number migration theory (*imaging*, *transformation*, 4.2) to reconstruct the shape and dimensions of the objects that the light reflected off. Through reflecting off the wall, the camera was able to covertly 'see' around corners and obstructions. The solution is currently in a proof-of-concept stage, thus lacks robustness when in a real-world application, albeit the security and privacy risks remain.

6 SCA Countermeasures for non-CYB Target Systems

This section focuses on the identification of candidate countermeasures for the non-CYB systems identified in the previous section. A key finding highlighted in section 4 is how SCA techniques depend on particular side-channel properties in order to succeed (see Table 2). As a consequence, countermeasures implemented to disrupt exploited side-channel properties within a system will effectively thwart the SCA technique and thus foil the attack.

We first devise a map of the countermeasures that disrupt each side-channel property, so that the correct countermeasure can be paired against its respective SCA techniques. The methodology behind this mapping stems from analysis of:

- each side-channel properties' role and impact on the flow of target information, and its relation in regards to the boundary of the target system.
- how each countermeasure impacts a side-channel and its path, and where in relation to the boundary of the target system.

A side-channel's path starts from the source of the target information within a target system (e.g. password stored in memory, heart beats, audio source) and ends at a sensor. At least one but possibly multiple of the side-channel properties are present (refer to section 2 for the role that each side-channel property plays). Each countermeasure acts on components within a side-channel, which by extension disrupts the side-channel properties associated with these components. For example, the isolation countermeasure applies to the boundary between the target system and the sensor, as illustrated in Figure 2. Isolation does not impact the internal operation of the target system and thus has no influence on the side-channel properties of modality transformation, determinism, signal mixing, or varying modality. It does however impact multi-stage pathway and multivariate sensing (section 6.3). This example demonstrates a systematic process for mapping countermeasures to respective side-channel properties, as summarised in Table 4.

Notable is the absence of a countermeasure for signal mixing. This can partially explain why SCAs are still effective at outmanoeuvring even actively defended target systems within the CYB domain, as the target information still has its chance to leak through adjacent signals within the system, forming additional side-channels.

The known countermeasures to SCAs, and the respective side-channel properties that they directly impact, are described below.

6.1 Hiding

Hiding adds variability to the sensed output signals to decouple its relationship with internal processes. This disrupts the side-channel properties of:

- Determinism: removes the correlation between the internal operations and the sensed signals by modifying the target system, or the internal operations, such that any respective leaked signals of the target information is randomised or uniform, therefore hinders the reproducibility of sensor readings.
- Varying Amplitude: hiding results in the target information existing at a lower amplitude in relation to other introduced variability such as randomised signals mixing with the side-channel.

Hiding has been used in CYB systems to counter power analysis attacks against AES encryption. Modifications

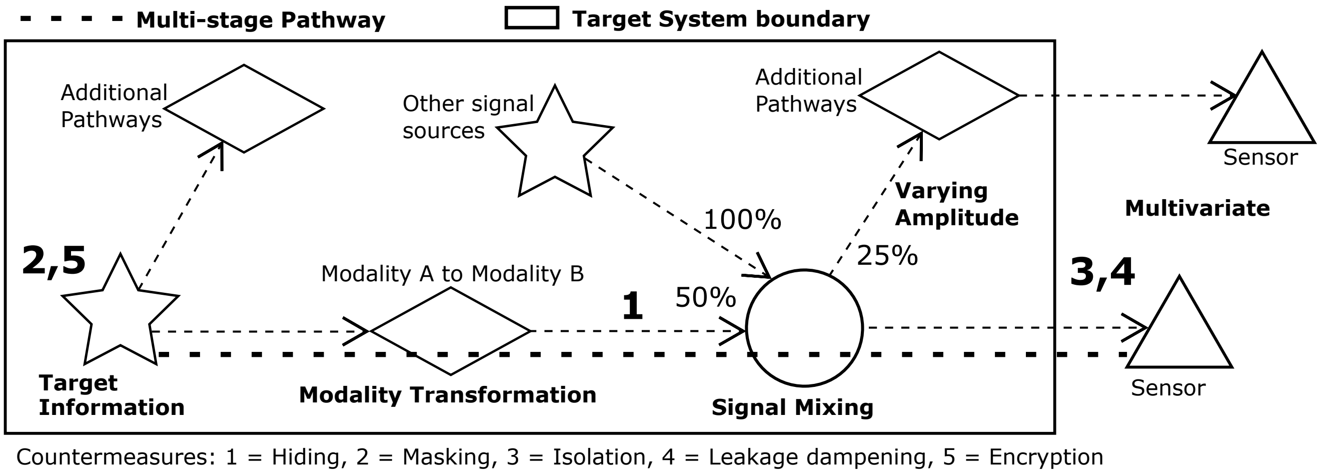

Figure 2 An illustration of an example side-channel, depicting the flow of the target information from its source to a sensor. Depicted are the side-channel properties (minus determinism), and the locations in which countermeasures impact a side-channel.

are made to the system, or to the internal operations through the addition of extraneous random calculations, such that the output power consumption is uniform or randomised independently to the internal operations [8].

6.2 Masking

Masking decouples the dependency between the internal operations related to the target information and the sensed output signals by masking the key variables associated with the target information with decoy data. This disrupts the side-channel properties of:

- Modality transformation: masking acts at the beginning of a side-channel on the target information source, before a modality transformation may have occurred (Figure 2). Any modality transformations that do occur will impact the masked (decoy) data and not the key variables associated with the target information.
- Determinism: decouples the SCA correlation as emitted sensed signals will contain information related to the internal processing of masked (decoy) variables and not the sensitive variables associated with the target information. With this decoupling, the reproducibility of sensing for the side-channel for embedded target information is hindered.

For CYB systems masking has been implemented by creating slightly varying copies of sensitive variables (e.g. characters of an encryption hash), and performing operations on the masked variables rather than the original sensitive variables, thus decoupling the SCA correlation required [39].

6.3 Isolation

Isolation blocks sensors from quantifying side-channels. The modalities of the side-channel involved must be taken into account to devise appropriate isolation mechanisms, for example the use of electromagnetic shielding to block the leakage of electromagnetic radiation. This disrupts the side-channel properties of:

- Multi-stage pathway: blocks the target information's path between its leakage from the target system and a sensor used to measure the leaked signal, therefore breaking the side-channel pathway from source to sensor.
- Multivariate: isolation can be adopted for an array of modality types and thus is able to block multiple side-channels simultaneously, disrupting multivariate sensing.

The concept of 'air-gapped' computers follows this technique by banning the use of external communication media (e.g. USBs) and keeping them in an isolated room [40]. Isolation implementations vary within CYB, from non-invasive approaches such as the placement of Faraday cages, to more invasive approaches such as making the hardware (e.g. PCB) read-proof via a protective coating [41].

6.4 Leakage dampening

Leakage dampening implements respective steps or materials for the modalities in play to reduce the amount of signal leaked [3]. It is a similar approach to isolation, and may be an alternative where isolation is not possible or ideal. For leakage dampening the internal operations and side-channels remain as-is, but there is a disruption of the side-channel between the boundaries of the target system and the sensor(s). This disrupts the side-channel properties of:

- Multi-stage pathway: dampens the strength of the output signal emitted from the target system to the sensor, thus disrupts the target information's path.
- Varying amplitude: dampening reduces the amplitude of target information making it harder to extract the target information embedded within the leaked signal.
- Multivariate: taking the modalities of the leaked signals into account, leakage dampening measures block one or more of the required side-channels, thus disrupting multivariate sensing.

The modalities of the side-channels must be considered, and then paired with appropriate leakage dampening steps or materials. For example, leaked audio signals could be dampened for nearby sensors by moving the target system further away, or sound absorption material can be installed.

6.5 Encryption

Encryption obfuscates target information such that it is not directly readable. This disrupts the side-channel property of:

- Determinism: the target information is still leaked via the side-channel, however direct readability of the target information is no longer available and thus the reproducible correlation of a deterministic side-channel is disrupted. Note that even when the deterministic relationship between target information and encrypted signal still remains, this countermeasure prevents this relationship being exploited.

Encryption as a countermeasure is traditional to the CYB domain thus far due to their bespoke design for electronic-based systems with virtual target information, and currently has limited applicability to non-CYB systems.

6.6 Countermeasure Algorithm

		SC Properties					
		Modality Transformation	Multi-stage Pathway	Determinism	Signal Mixing	Varying Amplitude	Multivariate
Counters	Hiding			✓		✓	
	Masking	✓		✓			
	Isolation		✓				✓
	Leakage Dampening		✓			✓	✓
	Encryption			✓			

Table 4 Side-Channel Properties to Countermeasures (SCP-C): Countermeasures are effective at impeding respective side-channel properties, which in turn impedes the SCA techniques that rely on each side-channel property.

The key contributions presented thus far are: (i) side-channels are composed of fundamental properties (section 2), (ii) SCA techniques depend on respective side-channel properties in order to succeed (section 4), and (iii) each side-channel property can be disrupted by respective candidate countermeasures, which in turn thwarts the associated SCA techniques (section 6). This principle is applied in the derivation of the Countermeasures Algorithm (see Algorithm 1, or Figure 3 for a graphical illustration), providing a reproducible and extensible process for proposing candidate countermeasures for any given target system. The algorithm is comprised of the following process:

1. Classify the SCA technique(s) that a non-CYB system is vulnerable to, akin to the example case studies summarised in Table 3. Identifying potential SCA techniques that apply to a novel target system is a separate research problem under investigation.
2. Identify the side-channel properties that each respective SCA technique depends on via a lookup in the *SCA Techniques to Side-Channel Properties* table (see Table 2).
3. A lookup in the *Side-Channel Properties to Countermeasures* table (see Table 4) identifies countermeasures that disrupt each relied on side-channel property.
4. For a given target system the algorithm outputs the associated SCA technique(s), its relied on side-channel properties, a set of candidate countermeasures, and the frequency in which each countermeasure was mapped to. The candidate countermeasures then need to be adapted to the context of the target system, as demonstrated in the following section.

The countermeasure algorithm is a representation of knowledge manipulation rather than one of algorithmic computation, and is guided by the data captured within the respective lookup tables. The efficiency and robustness of the algorithm is tied to the accuracy and breath of data within these lookup tables, which future works can further contribute to. The countermeasure algorithm directly addresses one of the research objectives of this paper by providing a method for the systematic iden-

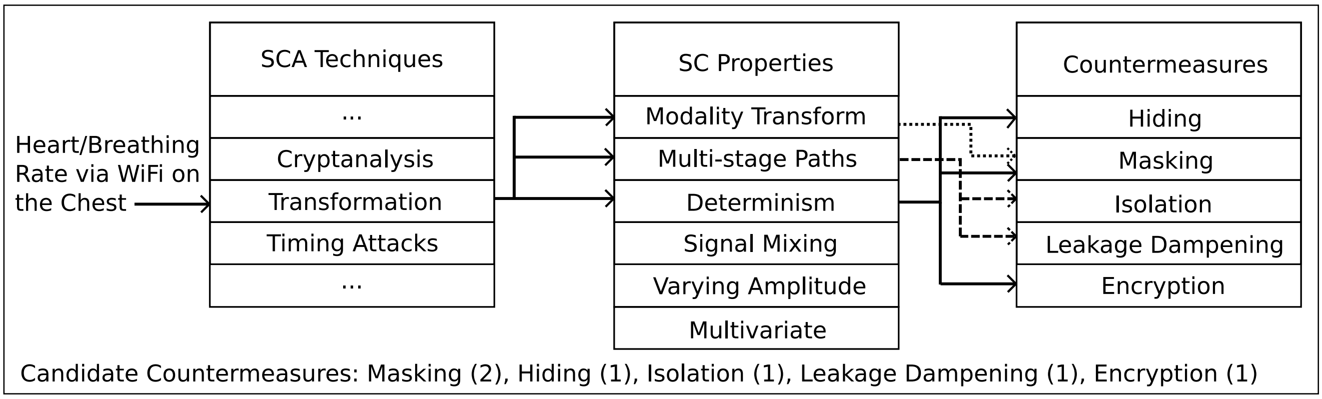

Figure 3 Depicts the process for deriving candidate countermeasures for a given case study, in addition to the frequency in which each candidate was mapped to (e.g. Masking (2)). The process performs lookups of the *SCA Techniques to Side-Channel Properties* table (Table 2), and the *Side-Channel Properties to Countermeasures* table (Table 4). In this example, candidate countermeasures are derived for the case study 'Heart/Breathing Rate via WiFi on the Chest [29]'.

tification of candidate countermeasures to defend non-CYB systems from SCAs. In the following section the countermeasure algorithm is applied to each of the non-CYB target systems from section 5.

Algorithm 1 The countermeasures algorithm is a representation of the systematic approach to identifying candidate countermeasures for a given target system derived from a synthesis of the SCA countermeasures surveyed. The algorithm performs a lookup of the respective tables that detail the relationship between SCA techniques, side-channel properties, and countermeasures. **SCAT-SCP** = SCA Techniques to Side-Channel Properties table (Table 2). **SCP-C** = Side-Channel Properties to Countermeasures table (Table 4).

```
function identifyCountermeasures(targetSystem)
  techniques = ∅, properties = ∅, countermeasures = ∅

  for each scaTechnique in GetSCATechniques(targetSystem)
    add scaTechniques to techniques

    for each scProperty in SCAT-SCP[scaTechnique]
      add scProperty to properties

      for each countermeasure in SCP-C[scProperty]
        add countermeasure to countermeasures
      end for

    end for
  end for

  # Obtain a count of how many times each
  # countermeasure is mapped to
  occurrenceCount = CountOccurences(countermeasures)

  return techniques, properties, countermeasures, occurenceCount
```

7 Countermeasures for non-CYB Target Systems

This section presents the results of the countermeasures algorithm (see Algorithm 1) when applied to each of the vulnerable non-CYB target systems identified in section 5. An example of the process is also illustrated graphically in Figure 3. A summary of the output of the countermeasure algorithm for each case study is presented in Table 5, detailing its respective SCA technique, relied on side-channel properties, and candidate countermeasures. Additional output includes a count of how many times each countermeasure is mapped to, as shown in the Countermeasures column (e.g. Masking (2)). A higher count suggests that the candidate countermeasure disrupts multiple relied on side-channel properties, while a lower or uniform count suggests that each countermeasure is equally important, and that relying on just one or two would not achieve resistance to the range of potential SCA pathways.

All proposed candidate countermeasures are well established within the CYB literature, thus already have evidence to indicate that they work, albeit within the context of the CYB domain and its related target systems. We assume that they are transferable to non-CYB domains, and are plausible as countermeasures for the identified non-CYB target systems. This assumption is based on the mapping process performed in Algorithm 1 which relates dependencies in the countermeasures to side-channel properties relied on by the SCA technique.

Each case study is revisited below with an explanation of how their respective candidate countermeasures can be implemented in the context of the non-CYB system and the real-world. Worth noting is that the countermeasure of encryption was not translated as it currently has no analogue in the context of a non-CYB system.

7.1 Inferring Human Thoughts via EEG Readings of the Brain

Side-channel recovery from EEG readings is a fragile process and relies on the cooperation of the participant. While disrupting the modality transformation stages internal to the brain required by *masking* is not feasible, *hiding* only involves a participant (or victim) to control their thoughts or move their limbs to introduce noise. This also disrupts the deterministic correlation between target information and the signal leakage. Multi-stage pathways are countered by *isolation* and *leakage dampening* measures achieved by restricting physical access to the participant. Future advances of the technology would require more active isolation and leakage dampening measures, for example the ability to take EEG readings from a distance may require the wearing of hats with embedded materials to block remote readings.

7.2 Geo-location Tracking via Frequency Variance on Electrical Grids

Modality transformations can be countered by *masking*, which in a real-world scenario could include the use of light sources with controlled or randomised frequency variances. The determinism property can be countered by masking and *hiding*, perhaps through the use of an inverter to decouple the correlation. Multi-stage pathways are countered by going off-the-grid or by recording video away from artificial light sources (*isolation*), or the dimming or obstruction of the light source (*leakage dampening*). Additional *leakage dampening* opportunities involve manipulation of the video recording itself, such as by randomly dropping frames, variating the frame rates, or with blur or video filtering techniques.

7.3 Automated Pothole Detection via Accelerometer Vibration on Road Networks

Masking to counter modality transformation can be achieved by placing the smartphone on an actively moving surface such that accelerometer readings detect the ‘decoy’ movements instead. *Hiding* is achieved through purposeful movement of the phone such that it produces random or uniform accelerometer readings. The multi-stage pathway can be disrupted through *leakage dampening* and *isolation* techniques: moving the smartphone or placing it on a malleable surface such as within a pocket to dampen the detected accelerometer readings from the road, and turning off the smartphone, respectively.

7.4 Heart Rate Detection via Photoplethysmography of the Face

Determinism can be countered through *masking*: purposely manipulating one’s heart rate by lowering it through relaxation techniques or raising it through physical exertion in order to control the output leaked. Masking to counter modality transformation is not practical without being able to decouple the heart rate from the periodic colour changes of the skin. For multi-stage pathway, one can obscure their face (particularly the forehead) for *isolation*, or the introduction of obscurities to the captured image for *leakage dampening* perhaps by applying a reflective medium such as make-up. Where PPG is attempted to be derived from online video calls, *leakage dampening* may be achieved through manipulation of the video feed, perhaps with blur or video filtering techniques, or via variable frame rates or dropping random frames.

7.5 Heart/Breathing Rate via WiFi on the Chest

Masking techniques could involve generating additional interference through a wearable vibration device on the chest to disrupt the modality transformation. The level of robustness of this solution is of course limited however, whereby substantial movement from a participant or baggy clothing would introduce sufficient *leakage dampening* (countering the multi-stage pathway). Lastly, as routers are stationary with a limited broadcast range, sensing can be countered if at a sufficient distance as a form of *isolation* (countering the determinism side-channel property).

7.6 Inferring Psychological State by Reading Pupillary Response

To counter the modality transformation a *masking* countermeasure should be used, however that does not quite translate into the real-world. Multi-stage pathways can be countered by closing one’s eyes or wearing sunglasses, or avoiding looking at cameras directly as a form of *isolation. Leakage dampening* is achievable by wearing contact lenses or with low-light level environments.

Non-CYB Target Systems	SCA Technique	Side-Channel Properties	Countermeasures
Inferring Human Thoughts via EEG Readings of the Brain	Correlation or Simple Regression	Modality Transformation, Multi-stage Pathways, Determinism	Masking (2), Isolation (1), Leakage dampening (1), Hiding (1), Encryption (1)
Geo-location Tracking via Frequency Variance on Electrical Grids	Correlation or Simple Regression	Modality Transformation, Multi-stage Pathways, Determinism	Masking (2), Isolation (1), Leakage dampening (1), Hiding (1), Encryption (1)
Automated Pothole Detection via Accelerometer Vibration on Road Networks	Custom filters	Modality Transformation, Multi-stage Pathways, Determinism	Masking (2), Isolation (1), Leakage dampening (1), Hiding (1), Encryption (1)
Heart Rate Detection via Photoplethysmography of the Face	Correlation or Simple Regression	Modality Transformation, Multi-stage Pathways, Determinism	Masking (2), Isolation (1), Leakage dampening (1), Hiding (1), Encryption (1)
Heart/Breathing Rate via WiFi on the Chest	Transformation	Modality Transformation, Multi-stage Pathways, Determinism	Masking (2), Isolation (1), Leakage dampening (1), Hiding (1), Encryption (1)
Inferring Psychological State by Reading Pupillary Response	Deep learning	Modality Transformation, Multi-stage Pathways	Masking (1), Isolation (1), Leakage dampening (1)
Movement Tracking via WiFi in the Open Environment	Radio detection finding	Modality Transformation, Multi-stage Pathways, Determinism, Varying Amplitude	Masking (2), Leakage dampening (2), Hiding (2), Isolation (1), Encryption (1)
Surreptitious Audio-Recovery from Video Footage of Objects	Radio detection finding	Modality Transformation, Determinism, Varying Amplitude	Masking (2), Hiding (2), Leakage dampening (1), Encryption (1)
Non-Line-Of-Sight Viewing of Objects with Reflected Light	Transformation	Modality Transformation, Multi-stage Pathways, Determinism	Masking (2), Isolation (1), Leakage dampening (1), Hiding (1), Encryption (1)

Table 5 The candidate countermeasures that disrupt side-channels techniques in the non-CYB target systems identified, as per the results of Algorithm 1. The numbers (e.g. Masking (2)) indicate how many times each countermeasure was mapped to given the SCA techniques and respective side-channel properties that they rely on.

7.7 Movement Tracking via WiFi in the Open Environment

Modality transformation can be addressed through *masking*, applicable through the emittance of a signal of a similar frequency in vicinity of the person(s) to mask your own movements. Determinism and varying amplitude can be countered though *hiding*, such as having a backpack swinging off your shoulder such that your own movements are obscured. Multi-stage pathways can be disrupted through *isolation* by taking advantage of WiFi's inability to propagate through certain materials, or moving outside of its range (if the location of the router is known). *Leakage dampening* is not as practical, as it would involve carrying on your person the appropriate materials to absorb the EM radiation, perhaps covering the majority of your height.

7.8 Surreptitious Audio-Recovery from Video Footage of Nearby Objects

To implement a *masking* countermeasure to disrupt the modality transformation and varying amplitude properties, the input of additional sound sources will force the object in focus (e.g. a chip packet) to vibrate irrespective of the target information sound source. The removal of malleable objects from the vicinity provides a *leakage dampening* countermeasure, as the solution is ineffective with rigid objects such as bricks as the vibrations are too minute for cameras to detect, thus countering the determinism side-channel property. *Hiding* involves impacting after the modality transformation stage (from audio into visual) through the introduction of excess light on the object.

7.9 Non-Line-Of-Sight Viewing of Objects with Reflected Light

The addition of bright lights directed at the target object is a form of *hiding* to counter the modality transformation and determinism side-channel properties, as the received light by the camera will return at a constant illuminance level (e.g. always reflect the same amount). A *leakage dampening* approach includes the use of wall paints that diffuse light, reducing the clarity of the reflected light of the target object, and the introduction of obstacles such as indoor plants can act as *isolation* to counter the multi-stage pathway side-channel property. *Masking* however does not quite translate in this case study.

7.10 Insights and Limitations

The development of mappings between side-channel properties, SCA techniques, and countermeasures provides a systematic approach to defend non-CYB systems against SCAs. This process is demonstrated in this section with specific proposals made to defeat SCAs for each of the case studies identified. SCAs are usually fragile and only demonstrated under controlled conditions, making it possible to achieve practical countermeasures provided the risk is identified. It is expected that future developments in this area will produce more subtle and robust attacks providing opportunities to extend the range of SCA techniques, side-channel properties, and countermeasures. However, while the candidate countermeasures identified are well established within the CYB domain, their applicability to the non-CYB case studies are only theoretical at this stage and will still need to be experimentally verified within each of these contexts.

8 Conclusion

Side-channels exist within target systems of *any* domain and thus are equally as vulnerable to SCAs as those traditional to the CYB domain. In contrast to CYB related systems that actively consider countermeasures, non-CYB domains do not recognise the presence and hazards of side-channels and thus their systems remain undefended. Section 5 surveys the existence of a broad range of non-CYB target systems at risk to SCAs, and demonstrates the consequent security and privacy risks. To defend such systems, it is demonstrated that each SCA technique relies on certain side-channel properties in order to succeed, and that each side-channel property can be disrupted by respective countermeasures derived from the CYB domain. SCAs can thus be prevented by deploying countermeasures that defeat the respective side-channel properties that a particular SCA technique relies on. A key contribution of this work is in identifying candidate countermeasures, through categorizing side-channel properties in non-CYB systems, and being able to apply this across a range of diverse systems. This principle is captured within the countermeasure algorithm (Algorithm 1): a systematic and extensible approach to identifying candidate countermeasures for non-CYB systems. We validate the output of this process by showing how the candidate countermeasures could be applied to each scenario (section 7).

8.1 Future Works

This work spurs on future research of applying SCAs to non-CYB systems [4], and defending them with countermeasures. Both SCA techniques and countermeasures stem from the CYB domain, therefore future research could investigate how much more effective ones that are specifically designed for non-CYB systems may be when their respective characteristics are taken into account (e.g. the ‘interconnectedness’ within the human body). Furthermore, opportunities exist to develop further the robustness of both SCAs and their proposed countermeasures within real-world settings. Our current research direction is how to better identify side-channels that may exist in any target system, and standardising their use between domains.

Acknowledgements The authors thank the anonymous reviewers for their invaluable feedback on this work.

Compliance with Ethical Standards

Conflict of interest All authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

1. F.-X. Standaert, T. G. Malkin, and M. Yung, “A unified framework for the analysis of side-channel key recovery attacks,” in *Advances in Cryptology - EUROCRYPT 2009*. Springer Berlin Heidelberg, 2009, pp. 443–461.
2. R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard, “Systematic classification of side-channel attacks: A case study for mobile devices,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 465–488, 2018.
3. I. Giechaskiel and K. Rasmussen, “Taxonomy and challenges of out-of-band signal injection attacks and defenses,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 645–670, 2020.
4. A. Spence and S. Bangay, “Side-channel sensing: Exploiting side-channels to extract information for medical diagnostics and monitoring,” *IEEE Journal of Translational Engineering in Health and Medicine*, vol. 8, pp. 1–13, 2020.
5. P. Kocher, J. Jaffe, and B. Jun, *Differential Power Analysis*. Berlin: Springer, 1999.
6. I. Martinovic, D. Davies, M. Frank, D. Perito, T. Ros, and D. Song, “On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces,” in *USENIX security symposium*, 2012, pp. 143–158.
7. J. Lange, C. Massart, A. Mouraux, and F.-X. Standaert, “Side-channel attacks against the human brain: The pin code case study,” in *Constructive Side-Channel Analysis and Secure Design*, S. Guilley, Ed. Cham: Springer International Publishing, 2017, pp. 171–189.

8. S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secrets of smart cards.* Springer Science & Business Media, 2008, vol. 31.
9. F.-X. Standaert, *Introduction to Side-Channel Attacks*, I. M. R. Verbauwhede, Ed. Boston, MA: Springer-Verlag GmbH, 2010.
10. D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, "ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs," in *Cryptographers' Track at the RSA Conference.* Springer, 2016, pp. 219–235.
11. B. Yang, K. Wu, and R. Karri, "Scan based side channel attack on dedicated hardware implementations of data encryption standard," in *2004 International Test Conference.* Washington, DC, USA: IEEE Computer Society, Oct 2004, pp. 339–344.
12. A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proceedings of the IEEE*, vol. 100, no. 11, pp. 3056–3076, 2012.
13. S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Cryptographic Hardware and Embedded Systems - CHES 2002*, Springer. Springer Berlin Heidelberg, 2003, pp. 13–28.
14. T.-H. Le, C. Canovas, and J. Clédiere, "An overview of side channel analysis attacks," in *Proceedings of the 2008 ACM symposium on Information, computer and communications security.* ACM, 2008, pp. 33–43.
15. B. Timon, "Non-profiled deep learning-based side-channel attacks with sensitivity analysis," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 107–131, 2019.
16. U. Greveler, B. Justus, and D. Loehr, "Multimedia content identification through smart meter power usage profiles," in *Proceedings of the International Conference on Information and Knowledge Engineering (IKE)*, 2012, p. 1.
17. S. R. Chhetri and M. A. A. Faruque, "Side-Channels of Cyber-Physical Systems: Case Study in Additive Manufacturing," *IEEE Design & Test*, vol. 34, no. 4, pp. 18–25, Aug. 2017.
18. R. Benadjila, E. Prouff, R. Strullu, E. Cagli, and C. Dumas, "Study of deep learning techniques for side-channel analysis and introduction to ascad database," *ANSSI, France & CEA, LETI, MINATEC Campus, France*, vol. 22, p. 2018, 2018.
19. J. Fan, X. Guo, E. D. Mulder, P. Schaumont, B. Preneel, and I. Verbauwhede, "State-of-the-art of secure ECC implementations: a survey on known side-channel attacks and countermeasures," in *2010 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST).* IEEE, jun 2010, pp. 76 – 87.
20. D. Genkin, A. Shamir, and E. Tromer, "Rsa key extraction via low-bandwidth acoustic cryptanalysis," in *Advances in Cryptology – CRYPTO 2014*, J. A. Garay and R. Gennaro, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 444–461.
21. A. K. Biswas, D. Ghosal, and S. Nagaraja, "A survey of timing channels and countermeasures," *ACM Computing Surveys*, vol. 50, no. 1, pp. 1–39, Apr. 2017.
22. C. Wang, X. Wang, Z. Long, J. Yuan, Y. Qian, and J. Li, "Estimation of temporal gait parameters using a wearable microphone-sensor-based system," *Sensors*, vol. 16, no. 12, p. 2167, 2016.
23. B. Hettwer, S. Gehrer, and T. Güneysu, "Applications of machine learning techniques in side-channel attacks: a survey," *Journal of Cryptographic Engineering*, pp. 1–28, 2019.
24. X. Ding, D. Nassehi, and E. C. Larson, "Measuring oxygen saturation with smartphone cameras using convolutional neural networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 23, no. 6, pp. 2603–2610, nov 2019.
25. T. Giallanza, T. Siems, E. Smith, E. Gabrielsen, I. Johnson, M. A. Thornton, and E. C. Larson, "Keyboard snooping from mobile phone arrays with mixed convolutional and recurrent neural networks," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 3, no. 2, pp. 1–22, Jun. 2019.
26. R. Garg, A. Hajj-Ahmad, and M. Wu, "Geo-location estimation from electrical network frequency signals," in *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*, May 2013, pp. 2862–2866.
27. J. Eriksson, L. Girod, B. Hull, R. Newton, S. Madden, and H. Balakrishnan, "The pothole patrol: using a mobile sensor network for road surface monitoring," in *Proceedings of the 6th international conference on Mobile systems, applications, and services.* ACM, 2008, pp. 29–39.
28. S. Sanyal and K. K. Nundy, "Algorithms for monitoring heart rate and respiratory rate from the video of a user's face," *IEEE Journal of Translational Engineering in Health and Medicine*, vol. 6, pp. 1–11, 2018.
29. F. Adib, H. Mao, Z. Kabelac, D. Katabi, and R. C. Miller, "Smart homes that monitor breathing and heart rate," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15.* Seoul, Republic of Korea: ACM Press, 2015, pp. 837–846.
30. C. Wangwiwattana, X. Ding, and E. C. Larson, "PupilNet, measuring task evoked pupillary response using commodity RGB tablet cameras," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 4, pp. 1–26, jan 2018.
31. F. Adib and D. Katabi, "See through walls with WiFi!" *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 75–86, sep 2013.
32. A. Davis, M. Rubinstein, N. Wadhwa, G. J. Mysore, F. Durand, and W. T. Freeman, "The visual microphone: Passive recovery of sound from video," *ACM Trans. Graph.*, vol. 33, no. 4, pp. 79:1–79:10, Jul. 2014. [Online]. Available: http://doi.acm.org/10.1145/2601097.2601119
33. D. B. Lindell, G. Wetzstein, and M. O'Toole, "Wave-based non-line-of-sight imaging using fast fk migration," *ACM Transactions on Graphics (TOG)*, vol. 38, no. 4, pp. 1–13, 2019.
34. P. Ming-Zher, D. J. McDuff, and R. W. Picard, "Advancements in Noncontact, Multiparameter Physiological Measurements Using a Webcam," *Biomedical Engineering, IEEE Transactions on*, vol. 58, no. 1, pp. 7–11, 2011.
35. H.-G. Kim, E.-J. Cheon, D.-S. Bai, Y. H. Lee, and B.-H. Koo, "Stress and heart rate variability: a meta-analysis and review of the literature," *Psychiatry investigation*, vol. 15, no. 3, p. 235, 2018.
36. G. Duran, I. Tapiero, and G. A. Michael, "Resting heart rate: A physiological predicator of lie detection ability," *Physiology and Behavior*, vol. 186, pp. 10 – 15, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0031938418300027
37. Y. Zhu, Z. Xiao, Y. Chen, Z. Li, M. Liu, B. Y. Zhao, and H. Zheng, "Adversarial wifi sensing," *CoRR*, vol. abs/1810.10109, 2018. [Online]. Available: http://arxiv.org/abs/1810.10109
38. J. Yang, H. Zou, H. Jiang, and L. Xie, "Device-free occupant activity sensing using wifi-enabled iot devices for smart homes," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3991–4002, Oct 2018.
39. H. Eldib and C. Wang, "Synthesis of masking countermeasures against side channel attacks," in *Computer Aided Verification*, A. Biere and R. Bloem, Eds. Cham: Springer International Publishing, 2014, pp. 114–130.

40. M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Acoustic data exfiltration from speakerless air-gapped computers via covert hard-drive noise ('diskfiltration')," in *European Symposium on Research in Computer Security.* Springer, 2017, pp. 98–115.
41. P. Tuyls, G.-J. Schrijen, B. Škorić, J. van Geloven, N. Verhaegh, and R. Wolters, "Read-proof hardware from protective coatings," in *Cryptographic Hardware and Embedded Systems - CHES 2006*, L. Goubin and M. Matsui, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 369–383.