Out-of-Band Covert Channels—A Survey

BRENT CARRARA and CARLISLE ADAMS, University of Ottawa

A novel class of covert channel, out-of-band covert channels, is presented by extending Simmons' *prisoners' problem*. This new class of covert channel is established by surveying the existing covert channel, device-pairing, and side-channel research. Terminology as well as a taxonomy for out-of-band covert channels is also given. Additionally, a more comprehensive adversarial model based on a knowledgeable passive adversary and a capable active adversary is proposed in place of the current adversarial model, which relies on an oblivious passive adversary. Last, general protection mechanisms are presented, and an argument for a general measure of "covertness" to effectively compare covert channels is given.

Categories and Subject Descriptors: C.2.0 [**General**]: Security and Protection; C.2.1 [**Network Architecture and Design**]: Wireless Communication; D.4.6 [**Security and Protection**]: Invasive Software

General Terms: Security, design

Additional Key Words and Phrases: Information hiding, covert channels, solitary confinement problem, out-of-band covert channels, physical covert channels, single-host covert channels, network covert channels, steganography, subliminal channels, taxonomy, covertness

ACM Reference Format:
Brent Carrara and Carlisle Adams. 2016. Out-of-band covert channels—A survey. ACM Comput. Surv. 49, 2, Article 23 (June 2016), 36 pages.
DOI: http://dx.doi.org/10.1145/2938370

1. INTRODUCTION

In 1984, Simmons motivated his work on *subliminal channels* with the prisoners' problem [Simmons 1984]: two individuals incarcerated in a prison wish to communicate with one another in order to develop an escape plan. The warden of the prison permits his trustees, the guards, to pass messages between the prisoners in the hopes that he can deceive one of them into accepting a message modified or fraudulently created by the warden as genuine; however, since the warden suspects the prisoners will develop an escape plan, he will only allow messages to be passed between them if he can read the messages and they appear to be innocuous. The prisoners, on the other hand, are willing to communicate under these conditions so they can in fact develop a plan. The *prisoners' problem* is therefore to communicate in full view of the warden yet deceive him and communicate an escape plan in secrecy, that is, develop a *subliminal channel*. Furthermore, the prisoners, fully expecting the warden to try and deceive them, will only accept messages if they are able to authenticate the origin of the message.

Let us extend this scenario. The warden has become increasingly suspicious of the prisoners and has put both of them in solitary confinement. The two prisoners still wish to formulate an escape plan; however, neither the warden nor any agent of the prison will pass messages between them. As a result, the prisoners must find a new method

Authors' address: School of Electrical Engineering and Computer Science (EECS), University of Ottawa, 800 King Edward Avenue, P. O. Box 450, Station A, Ottawa, Ontario, Canada K1N 6N5.

DOI: http://dx.doi.org/10.1145/2938370

of communication. Furthermore, they must sufficiently hide their communication so as to not arouse the suspicion of the guards, since the warden has also decided that if any evidence of communication is found, one of the prisoners will be transferred to a different facility. We deem this problem the *solitary confinement problem*, which can be viewed from two different perspectives: the perspective of the prisoners, who wish to communicate covertly to establish an escape plan, and the perspective of the guards, who wish to find concrete evidence proving the prisoners are communicating.

The problem, in detail, for the prisoners is therefore to:

(1) find a channel to communicate over such that:
   (a) the transmitting prisoner can modulate data symbols by effecting changes in the channel, and
   (b) the receiving prisoner can observe changes in and demodulate the changes into data symbols;
(2) agree upon a modulation and demodulation scheme; and,
(3) secure the channel so the guards cannot detect that communication is taking place.

We make the following assumptions in the construction of the solitary confinement problem. We first assume that the prisoners have managed to pre-share a key or keys in secret from the warden prior to being put into solitary confinement, which can be used, as needed, to secure the communication channel between them. We also assume that the guards are able to monitor all possible channels accessible to the prisoners and are knowledgeable in modulation and demodulation schemes. The solitary confinement problem from the perspective of the guards is, therefore, to detect communication between the prisoners given knowledge of the medium and modulation scheme but not the secret keys that the prisoners have shared. In other words, let P_D be the probability that the guards detect covert communication. Stated mathematically, the problem from the perspective of the prisoners is to secure their communication channel such that $P_D \rightarrow 0$, and the problem from the perspective of the guards is to devise a scheme such that $P_D \rightarrow 1$. A diagram showing the model for out-of-band covert channels can be seen in Figure 1.

We present the *solitary confinement problem* to motivate our work on classifying *out-of-band covert channels,* a term we first coined in our work on covert acoustic channel communication in Carrara and Adams [2015a]. In this work, we define out-of-band covert channels as follows:

Definition 1.1. An *out-of-band covert channel* is a low-probability-of-intercept (LPI) communication channel established between isolated processes (i.e., processes not able to communicate through traditional links) by modulating and demodulating a shared medium using devices that are traditionally not used for communication.

In this work, we take the term *low probability of intercept* to mean a waveform whose *covert-key* is unknown (unexploitable) from the viewpoint of the guards, who thus are forced to use wideband detection techniques because they cannot perform normal correlation detection. Note that this definition is a modified version of the low-probability-of-intercept definition provided by Polydoros and Weber [1985] as used in the study of low-probability-of-intercept spread-spectrum communications by Peterson et al. [1995]. Our definition is also in line with the definition of *undetectability* of Pfitzmann and Hansen [2010], where the data being communicated over the out-of-band covert channel are the item-of-interest and the goal for the prisoners (i.e., the sender and receiver) is to construct messages such that the guards cannot sufficiently distinguish whether the messages exist. We construct the problem in such a way that the guards are not *involved* by virtue of the fact that they have no knowledge of the pre-shared key(s).

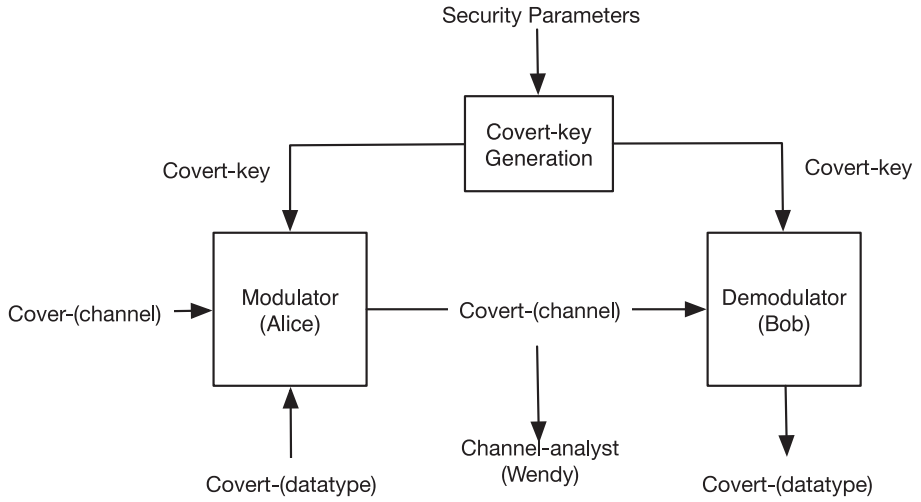

Fig. 1. The communications model for out-of-band covert channels. The *covert-key* is first generated based on the *security parameters* of the system and made available to the *modulator* and *demodulator*. The *modulator* (Alice) after receiving the *covert-key* modulates its *covert-(datatype)* onto a *cover-(channel)* to produce a *covert-(channel)* using a modulation scheme. Similarly, the *demodulator* (Bob) demodulates the *covert-(channel)* to reproduce the *covert-(datatype)* using an appropriate demodulation scheme and the *covert-key*. The *channel-analyst* has access to the *covert-(channel)* and is knowledgeable of the modulation and demodulation scheme used by the *modulator* and *demodulator*. The *channel-analyst*, however, does not have knowledge of the *covert-key*. We point out that this model is a derivative of the information hiding model initially proposed at the First International Workshop on Information Hiding [Pfitzmann 1996].

1.1. Overview

In this work, we classify out-of-band covert channels as a separate sub-category of covert channels alongside single-host covert channels [Lampson 1973], physical covert channels [Hanspach and Keller 2014], and network covert channels [Girling 1987]. Furthermore, we compare out-of-band covert channels to other related categories of information hiding [Petitcolas et al. 1999], namely steganography, anonymity, and subliminal channels. Additionally, we analyze the literature in related disciplines (e.g., side channels, Transient ElectroMagnetic Pulse Emanation STandard (TEMPEST), and device pairing) to present a comprehensive survey of techniques that could be used to establish out-of-band covert channels. Last, we classify each of these techniques and discuss their effectiveness (i.e., the bandwidth) and efficiency (i.e., covertness).

We undertake this study to show that, given the wide support set of sensors and devices now embedded in commodity hardware, there are a number of viable alternatives to create out-of-band covert channels without hardware modification. Furthermore, we aim to show that while these covert channels are not as high-bandwidth as conventional radio-frequency channels, they are, in general, capable of transferring information requiring low bit rates (e.g., text). Additionally, through our analysis of state-of-the-art out-of-band covert channels, we show that current covert channel solutions rely on an oblivious passive adversary and that, as a result, the security model currently used to evaluate covert channels needs to be enhanced. Last, in addition to showing that the current adversarial model for out-of-band covert channels is built on weak security assumptions, where applicable, we highlight various solutions from the literature on LPI communications, for example, spread spectrum, that possibly could be employed in order to improve the covertness of out-of-band covert channels.

As a result of this work, we make the following contributions:

(1) We present a novel class of covert channels, namely *out-of-band covert channels*.
(2) We demonstrate that covert channels, to date, have relied on "security through obscurity" and demonstrate, through example, that a more standard passive and active adversarial model should be adopted to evaluate all covert channels in order to determine their level of covertness.
(3) We present a comprehensive survey of the channels that could be used for out-of-band covert communication and document the effectiveness and the efficiency of each alternative. This is useful for:
    (a) Secure system developers building systems that require protection against out-of-band covert channels
    (b) Privacy-conscious users, that is, covert channel designers, developing covert communication systems in order to avoid detection by a third party.
(4) Last, we present the first taxonomy of out-of-band covert channels based on their physical channel as well as their modulator and demodulator hardware requirements.

1.2. Terminology

The following terminology is used throughout our survey and has been heavily influenced by the terminology already established in the study of steganography [Pfitzmann 1996]. In our communications model, covert communication takes place between a *modulator* (Alice) and a *demodulator* (Bob). The *modulator* takes as input a *covert-(datatype)* message as well as a *covert-key* to modulate data symbols onto a *cover-(channel)* to produce a *covert-(channel)*. The *(datatype)* of the message is specific to the type of data being modulated (e.g., text, image, audio, and so on, which results in covert-text, covert-image, covert-audio, etc.) and (*channel*) is specific to the type of physical channel used to transmit *(datatype)* data symbols (e.g., acoustic, vibration, light, and so on, which results in covert-acoustic, covert-vibration, covert-light, etc.). The *covert-key* used in the modulation process can either be the same as the key used during demodulation to create a *symmetric-key covert channel*, or the *covert-key* can be different resulting in an *asymmetric-key covert-channel*. Furthermore, the *covert-key(s)* generated is dependent on the security parameters of the system (e.g., type of covert channel, channel security).

In our adversarial model, we assume that the *channel-analyst* (the guards) has access to both the *covert-(channel)* as well as the modulation and demodulation scheme used by the *modulator* and *demodulator* to secure their communication. The *channel-analyst*, however, does not have access to the *covert-key(s)*. The security of the out-of-band covert channel, therefore, is derived from the strength of the *security parameters* used to generate the *covert-key* and not on the choice of *covert-(channel)* or the choice of modulation and demodulation scheme. This assumption is in line with Auguste Kerckhoffs principles of communications security [Kerckhoffs 1883], in which he cautioned that secure systems should not rely on the method used to protect (encrypt) data for security but rather should rely on the choice of key. Systems that base their security on hiding the details of the algorithm used to protect data are commonly referred to as systems that rely on "security through obscurity." History is littered with examples of secure systems that relied on this assumption and the ways in which they were broken [Petitcolas et al. 1999].

We note that our definition of covert channels is more rigorous than the informal definition that has been used in previous covert channel work, which deemed a channel covert if the signals used for communication were imperceptible to humans present in the environment. This is ultimately a form of "security through obscurity," since any

adversary aware of the medium and modulation scheme could detect that communication is taking place, that is, knowledge of the medium implies detection. In our survey, we show that the schemes proposed to date fail to meet our definition of covert channels and, therefore, more research is required to create truly undetectable out-of-band covert channels.

1.3. Intended Audience and Applications for Out-of-Band Covert Channels

The intended audience of this work is the secure system development community (i.e., the guards) who wish to secure their systems by reducing the risks posed by out-of-band covert channels. By understanding the various out-of-band covert channel techniques, secure system developers can implement countermeasures into their system designs based on the peripherals and sensors installed on their systems. Furthermore, this work benefits privacy-conscious users as well as users requiring a LPI communications channel (i.e., the prisoners). By understanding the various out-of-band covert channels, covert channel designers will be able to develop solutions to hide their communications based on the constraints imposed on their systems. Unfortunately, as is usually the case with security, there is a dual use for out-of-band covert channels. While out-of-band covert channels can be used by free-speech advocates and privacy-conscious users, these same channels can be used by criminal elements to support nefarious activity. While these ill-intended parties are not the target audience of this work, they could potentially benefit from it. Defences against the covert channels discussed in this work will be presented to counterbalance this risk. To summarize, our motivation for this work is therefore to help secure system developers better understand out-of-band covert channels and the threat that they pose as well as, conversely, to show covert channel designers that a passive adversary with knowledge of the covert communication method could detect their covert channels.

There are a number of potential applications for out-of-band covert channels. First, they can be used for malware communication between systems that are physically separated or isolated from one another, that is, air-gapped machines. Researchers have demonstrated that malware is capable of communicating cryptographic key material, documents, and recorded audio between air-gapped systems using out-of-band covert channels [Carrara and Adams 2015a]. Additionally, out-of-band covert channels have been used to provide policy-breaking inter-process communication between isolated processes on modern operating systems [Novak et al. 2015]. Similarly, out-of-band covert channels can be used for communication between entities not willing to or allowed to use traditional communication links. This is a common problem in applications supporting the expression of free speech in oppressive environments and during times of protest when traditional communication links are taken down, in whistleblower scenarios where sensitive information needs to be exfiltrated, and, in general, when the fact that communication is taking place needs to be kept hidden from detection by a third party (e.g., governments, criminals, etc.) [Carrara and Adams 2015b]. Furthermore, out-of-band covert channels can be used for authentication. Two parties that agree on both a medium and modulation scheme can use them to authenticate each other, which is similar to network covert channels that authenticate using "port knocking" [Zander et al. 2007]. This type of authentication, however, is based on "security through obscurity" and is generally not recommended in direct application without some reliance on secret information. Last, out-of-band covert channels could potentially be used to augment traditional communication links.

Our article is organized as follows. In Section 2, we review the literature in relevant fields of information hiding as well as covert channels and show where out-of-band covert channels fit into the information hiding hierarchy. In Section 3, we scope the study of our work and discuss how out-of-band covert channels relate to device-pairing

and side channels. In Section 4, we present a survey of the literature related to out-of-band covert channels and in Section 5 we present a novel taxonomy for the area. Finally, in Sections 6 and 7 we present future work and conclude, respectively.

2. BACKGROUND ON COVERT CHANNELS AND INFORMATION HIDING

In 1973, Lampson examined the problem of constraining a program to prevent it from leaking sensitive information and named the problem the *confinement problem* [Lampson 1973]. Lampson modelled the problem using *customers* and *services*, where services performed some function on behalf of their customers, and harmed a customer if they leaked (i.e., communicated to a third party) the customer's data without their consent. Lampson [1973] explored ways in which a service could leak a customer's data to another program without the customer's knowledge (e.g., via shared memory, files, message passing, and modulating shared resources not typically used for communication such as locks, system load, ratio of a process' computing time to idle time, page rate as well as encoding data in the customer's bill). In enumerating and categorizing the ways in which a process could leak data to another process, Lampson introduced *covert channels:*

Definition 2.1. A *covert channel* is a communication channel that is not intended for information transfer at all [Lampson 1973].

2.1. Single-Host Covert Channels

Lipner [1975] furthered Lampson's work and applied formal non-discretionary (i.e., mandatory) access control security models, such as the Bell-LaPadula (BLP) model [Bell and LaPadula 1973], to the confinement problem. Lipner argued that by applying formal security models as well as other techniques (e.g., virtual time), the confinement problem could be solved for known communication channels, but acknowledged that covert channels are difficult, if not impossible, to eliminate. Based on Lipner and Lampson's research, a number of formal methods have been developed to monitor, as well as search for, covert channels on a single host: namely, the shared-resource matrix methodology [Kemmerer 1983], covert flow trees [Kemmerer and Porras 1991], non-interference methods [Goguen and Meseguer 1982], and security kernels [Millen 1976]. While these methods can be used to formally demonstrate that no information is leaked through known communication channels, covert channels can still exist on systems that employ these methods as they do not take into account all possible abuses of system resources for communication purposes.

In acknowledgement that covert channels cannot always be eliminated, the Trusted Computer System Evaluation Criteria (TCSEC) [Latham 1986], developed by the United States Department of Defence (DoD) as criteria to certify secure systems, classified covert channels based on their bandwidth and laid out certification requirements for handling covert channels [Gligor 1994]. Additionally, the TCSEC presented a method for analyzing covert channels and clarified that single-host covert channels only exist on systems that employ mandatory access control policies since the owner of an object sets the access rules in discretionary systems. Millen [1999] separated the covert channel research into four general, not necessarily non-overlapping, areas: modelling, searching, measuring, and mitigating. Since the publication of TCSEC's certification criteria a number of articles have been written on the modelling [Kemmerer 1983; Meadows and Moskowitz 1996; Millen 1976; Trostle 1993; Goguen and Meseguer 1982], searching [Haigh et al. 1987; He and Gligor 1990; Tsai et al. 1990; Loepere 1985; Schaefer et al. 1977; Wray 1992; Melliar-Smith and Moser 1991; Kemmerer and Porras 1991], measuring [Millen 1989; Moskowitz and Kang 1994; Moskowitz and Miller 1994; Shieh and Chen 1999; Moskowitz and Miller 1992; Marforio et al. 2012],

and mitigating [Son et al. 2000; McDermott 1994; Hu 1992; Karger and Wray 1991; Gray III 1993; Kang and Moskowitz 1993] aspects of single-host covert channels.

Based on the work of previous researchers, single-host covert channels can be classified as follows:

(1) Single-host covert channels are established on a (single) system that implements a non-discretionary (i.e., mandatory) access control policy (e.g., Bell and LaPadula [1973], Biba [1977], and Clark and Wilson [1987]) [Gligor 1994].
(2) Single-host covert channels are established for the purposes of circumventing the security policy of the system (e.g., passing information from a high-security process to a low-security process, i.e., write-down) [Schaefer et al. 1977].
(3) Single-host covert channels exist between two processes that are not permitted to communicate but do so anyway, a few bits at a time, by modulating shared resources [Millen 1999].

Both single-host covert channels and out-of-band covert channels establish a communication link between processes that are not intended to communicate; however, single-host covert channels (ab)use a shared resource (e.g., file, lock, bus, etc.) or resources on a single host in order to establish a communication link, while out-of-band covert channels use a shared physical medium (e.g., air, light, radio waves, etc.) to establish a communication link. Furthermore, the modulators and demodulators of a single-host covert channel can rely on a shared operating system and shared hardware, whereas the communicating parties establishing an out-of-band covert channel cannot make the same assumptions, as out-of-band covert channels are established among isolated processes, typically running on physically separated machines, and share no common resources (aside from a shared medium). Additionally, single-host covert channels are designed to circumvent the security of mandatory access control systems, whereas out-of-band covert channels are established between processes regardless of the access control policy of the hosts they are running on. It is important to point out that out-of-band covert channels have been proposed to facilitate policy-breaking communication on a single host and in this specific application has been referred to as *physical covert channels* [Hanspach and Keller 2014].

2.2. Network Covert Channels

In 1987, Girling presented the first work on covert channels facilitating policy-breaking communication between processes running on separated, networked hosts [Girling 1987]. Girling defined network covert channels as additional network information transmitted between a sender and receiver that is communicated in a way that violates the network's security policy. The covert channels presented by Girling differ from traditional single-host covert channels in an important way: A network covert channel modifies a traditional communication protocol and thus the traditional communication protocol forms a cover for the covert channel. Building on the work of Girling, network covert channels have been used in many different, yet related, applications [Zander et al. 2007]:

—Communicating in secret between networked hosts (either directly or indirectly)
—Exfiltrating sensitive data
—Circumventing firewall policies
—As an alternative to the use of strong encryption on networks that have banned its use
—As a means to express free speech
—Malware communication

Thorough literature reviews on the topic of network covert channels can be found in Zander et al. [2007] and Wendzel et al. [2015]. In Wendzel et al. [2015], over 100 different network covert channel techniques were analyzed and classified into 11 different patterns. The research concluded that network covert channels create stealthy communication links by modifying either the structure or timing of existing network protocols (e.g., Internet Protocol, User Datagram Protocol, Transmission Control Protocol, etc.) in some way. This is consistent with the literature on single-host covert channels and, in general, all covert channels can be separated into storage or timing channels [Kemmerer 1983]. Although some researchers have demonstrated that they are one and the same [Wray 1992], covert channels are generally categorized as either storage channels, timing channels, or mixed. Wendzel et al., further classified covert storage channels into the sub-patterns "modification of non-payload data" (e.g., header and padding) and "modification of payload data" and furthermore categorized the discipline of steganography under the pattern of "modification of payload data."

Given the literature on the subject, network covert channels can be summarized as follows:

(1) Network covert channels are established between processes whose traditional communication channels are subject to a formal or an informal network security policy.
(2) Network covert channels are established for the purposes of circumventing the security policy of the network.
(3) Network covert channels are established by modifying the structure or timing of a traditional communication protocol (i.e., the cover) in order for policy-breaking processes to communicate either directly or indirectly.

Network covert channels and out-of-band covert channels are similar in that they establish a covert connection between processes executing on different hosts. The major difference between out-of-band covert communication and network covert communication is that network covert channels leverage an established link between the hosts to hide their communication. Covertly communicating processes using a network covert channel do not necessarily have to be executing on the endpoint hosts (i.e., as the sender or receiver) participating in the traditional communication protocol; however, they must be in the path of communication in order to transfer information. On the other hand, out-of-band covert channels are established in the absence of any traditional communication link between the communicating parties and are established to create a covert general-purpose communication link. Furthermore, where network covert channels are designed to hide data within traditional communication protocols, out-of-band covert channels are concerned with modulating a shared medium in covert fashion in order to exchange data and use the channel itself as cover.

Our survey differs from the works of Zander et al. [2007] and Wendzel et al. [2015] in three major ways. First, while their works are surveys of network covert channels, that is, channels that hide information within network protocols, our work is a survey of the novel ways that commodity hardware devices could be used to establish out-of-band covert channels. Second, while the works of Zander et al. and Wendzel et al. focused on network protocols and the fields within the protocols that information could be hidden in to allow connected hosts to covertly communicate, our study enumerates the various mediums, hardware devices, and modulation schemes that could be used to provide covert communication between isolated, disconnected processes. Third, the previous works either categorized network covert channels by the technique that they used to hide information (e.g., adding information to padding) [Zander et al. 2007] or by generic pattern classes that were used to group similar hiding techniques [Wendzel et al. 2015]. Conversely, as discussed in Section 5, we classify out-of-band covert channels by the modulator and demodulator hardware requirements as well as by the physical medium

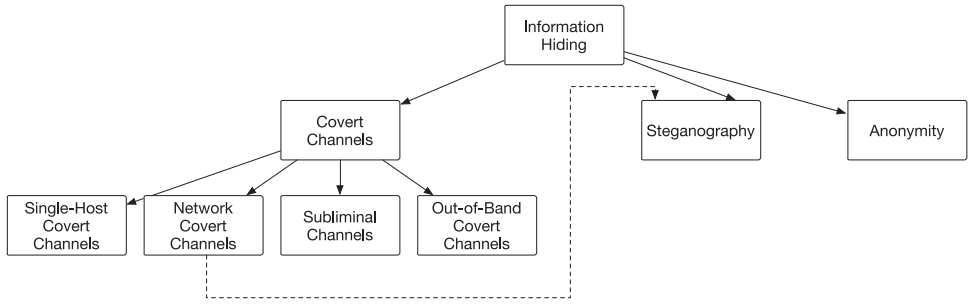

Fig. 2. The classification of information hiding techniques with a focus on covert channels. This is a modified version of Figure 1 from Petitcolas et al. [1999]. We have modified the original image by omitting the class of "Copyright Marking" as well as the sub-classes of "Steganography" because they are outside the scope of this work. We have also added the category of "Out-of-Band Covert Channels" to the "Covert Channels" branch. The relationship between steganography and network covert channels is also shown in this diagram to reflect the work of Wendzel et al. [2015].

used to communicate. To the best of our knowledge, this is the first study that examines out-of-band covert channels and while there is similarity in the applications for network covert channels and out-of-band covert channels, the two classes of channels establish communication in two fundamentally different ways, that is, by hiding information in network protocols and by communicating symbols over a shared physical medium, respectively.

2.3. Information Hiding

Information hiding [Petitcolas et al. 1999] is the discipline within communications security that deals with preventing the *detection* of communications by an adversary. This is in contrast to the discipline of cryptography, which looks at protecting the confidentiality and integrity of communications (as well as non-repudiation and origin authentication in certain applications). There are a number of categories of research within information hiding that are relevant to this work, namely, steganography, anonymity, and the sub-class of covert channels, subliminal channels [Petitcolas et al. 1999]. For completeness, we briefly compare and contrast each of these areas with out-of-band covert channels in this section. Furthermore, in Figure 2, we present an updated information hiding classification tree. The original tree was first presented by Petitcolas et al. [1999]. Our version of the tree shows the location of out-of-band covert channels amongst the existing categories of information hiding.

2.3.1. Subliminal Channels. As previously mentioned, Simmons motivated his work on subliminal channels with the prisoners' problem [Simmons 1984]. In his work, Simmons presented two example solutions to the problem and demonstrated that it is possible to use several ciphers that decrypt to the same message and that, by this fact, information can be communicated in secret not by modifying the message itself but rather by the choice of the cipher parameters used to encrypt or sign messages. Further research into subliminal channels showed that subliminal channels can be established in cryptographic algorithms such as El-Gamal and the Digital Signature Algorithm [Simmons 1985, 1994; Anderson et al. 1996]. Similarly to network covert channels, subliminal channels require the covertly communicating parties to be engaged in overt communication. This differs from out-of-band covert channels in that the goal of out-of-band covert channels is to establish an undetectable communication link between parties without any overt communication between them. Furthermore, subliminal channels can only be established when the communicating parties are

engaged in a cryptographic protocol. Out-of-band covert channels have no such requirement.

2.3.2. Steganography. Steganography is the discipline of embedding secret messages in a cover medium and literally means "covered writing" in Greek [Petitcolas et al. 1999]. In the literature, the *embedded* message is the secret message and the *cover* is referred to as *cover-text* [Singh et al. 2009; Bennett 2004], *cover-image* [Chandramouli et al. 2004], or *cover-audio* [Jayaram et al. 2011], depending on the type of cover that is used. The process of embedding a secret message into a cover is governed by the *stego-key* and successful execution of the process results in the creation of a *stego-object*. Much like the requirements for network covert channels, steganography requires a cover to embed the secret message into. One difference between steganography and network covert channels is that in steganography the cover is generally interpreted by humans (e.g., text, audio) and the goal of steganography is to hide information so humans cannot perceive the hidden data, whereas in network covert channels the cover channel is interpreted by machines, and data are hidden in redundant parts of network protocols [Wendzel et al. 2015]. Out-of-band covert channels differ from steganographic messages in that they do not hide their information in the digital encoding of human-perceivable cover media but rather utilize physical channels in novel ways in order to achieve covertness. Additionally, for steganographic techniques to be applied, overt communication is required between the covertly communicating parties, whether it be direct or indirect. As previously stated, overt communication is not a requirement of out-of-band covert channels. For an overview on the field of steganography and steganalysis, see Anderson and Petitcolas [1998], Provos and Honeyman [2003], and Johnson and Katzenbeisser [2000].

2.3.3. Anonymity. Protecting the identity of endpoints participating in a conversation as well as when they are communicating is referred to as the *traffic analysis problem* [Chaum 1981]. Solutions to the problem are broadly broken down into three categories: preserving the anonymity of the receiver, preserving the anonymity of the sender, and providing unlinkability, the strongest sense of anonymous communication [Pfitzmann and Waidner 1987]. A number of solutions, both practical and theoretical, have been presented to solve the traffic analysis problem including mix-nets [Chaum 1981], crowds [Reiter and Rubin 1998], and Tor [Dingledine et al. 2004] (this is an extremely small subset of the works in this area; see Danezis and Diaz 2008] for a vast number of proposed solutions to this problem). While anonymous communication solutions provide some identity protection for endpoints, the fact that entities are communicating is not hidden, simply the fact of who they are communicating with and when. Furthermore, anonymous communication systems rely on an external party or parties to provide anonymity. In out-of-band covert channels, no such party is required. Last, out-of-band covert channels are designed to make communication undetectable and not to hide the identity of the endpoints.

3. SCOPE

We return to the solitary confinement problem to scope our work as well as to place bounds on our survey. Let us assume that in addition to being prevented from exchanging messages over traditional channels, the prisoners are further constrained to establishing a covert channel given the current configuration of their environment. That is to say, the prisoners are limited in that they cannot add anything to the their environment, nor can they remove anything. Analogously, in this work, we study the ability for a modulator and demodulator to communicate without making physical changes to their systems. This restriction on out-of-band covert channels is in line with the constraints placed on systems that support single-host, physical, and network covert

channels. In general, covertly communicating parties must leverage existing system resources, networks, or cryptographic protocols to communicate their message. Out-of-band channels, similarly, must be established through the use of existing hardware (e.g., components, sensors, peripherals) found on commodity systems. Given this restriction, we bound our survey to non-traditional communication channels that can be established using commodity hardware (e.g., display, speaker, microphone, CPU, light emitting diodes (LEDs), ambient light sensor (ALS), magnetometer, etc.). We scope our study in this fashion to distinguish our work from the body of research in the area of LPI radar communications [Proakis 2008; Peterson et al. 1995], where there is no such hardware restriction. We do, however, pull from the LPI communications literature to provide recommendations on securing existing covert channel proposals.

In the next section, Section 4, we survey the covert channel, side-channel, and device-pairing literature to summarize existing techniques and channels that could be used as out-of-band covert channels. We survey the literature on side-channel attacks (see Zhou and Feng [2005] for an overview of the subject) and device pairing (see Kobsa et al. [2009] and Kumar et al. [2009] for an overview of the subject) because of their similar requirements, that is, non-traditional forms of communication. The research in the area of side-channel attacks examines unintentional leakage of information (usually plain text or cryptographic keys) from secure systems, where the sender unintentionally leaks data, and only the receiver is interested in successful reception of the communication. We also review the relevant TEMPEST literature [Van Eck 1985] as part of our survey. Furthermore, given the vast number of side-channel attacks in the literature, we only review techniques that fit within the scope of this note, namely non-invasive side-channel attacks as defined in Anderson et al. [2006], which leak sensitivity information from machines without hardware modification. Additionally, we survey the literature on covert channels that fall within our definition of out-of-band covert channels but, to date, have not been categorized as such. We also examine the literature on device pairing, which covers out-of-band channels as well as side channels (e.g., light, audio, vibration). These alternative communication channels are used in bootstrapping other protocols (e.g., Secure Sockets Layer (SSL), network joining, etc.) as well as providing alternatives (e.g., audio communication) to traditional forms of communication (e.g., Bluetooth, near-field communication (NFC), etc.). We specifically cover the channels in this area that we feel could be adapted and used as out-of-band covert channels, that is, transmission can be controlled by a sender and the signals can be made imperceptible.

There is a subtle yet clear distinction to be made between device pairing and out-of-band covert channels. Work in the device-pairing literature examines communication alternatives that are resistant to eavesdropping and man-in-the-middle attacks by creating authenticated out-of-band channels (A-OOB). Device-pairing solutions rely on the fact that a human is a participant in the pairing process in order to ensure it is authentic, either actively, by participating in the protocol (e.g., clicking buttons, shaking devices, etc.), or passively, by simply pointing their device at another device and letting the pairing protocol run. Furthermore, by utilizing out-of-band channels that are configured to communicate over short distances, the device-pairing channel is assumed to also be secret, that is, an eavesdropper cannot listen in on the exchange because of the attacker's distance from the exchange [Halevi and Saxena 2010]. However, researchers have shown that in addition to humans being able to perceive these out-of-band device-pairing channels, technical solutions can also be developed to eavesdrop on secret and authenticated out-of-band device-pairing channels (AS-OOB) [Halevi and Saxena 2010]. Out-of-band covert channels as defined here, on the other hand, are established specifically to avoid both human perception as well as detection by a third party who has access to technical tools.

Although outside the scope of this note, hardware Trojans deliberately added to integrated circuits for the purpose of leaking sensitive information are relevant to the discussion on out-of-band covert channels [NSA 2013; Lin et al. 2009; Kiamilev et al. 2008]. Hardware Trojans are hardware modifications, either through circuit manipulation [Kiamilev et al. 2008; Lin et al. 2009] or added special-purpose hardware [NSA 2013], specifically designed to leak information. Typically, hardware Trojans are added to special-purpose cryptographic processing hardware to purposefully leak either the plaintext being encrypted, the secret key used for encryption, or intermediate values used in the encryption process. Information can be leaked in a number different ways: via modulated power fluctuations, temperature fluctuations, or radio-frequency signals. These leaked side-channel signals are typically picked up by specialized hardware at the demodulator, for example, simple power analysis [Kocher et al. 1999], differential power analysis [Kocher et al. 1999], thermal cameras [Kiamilev et al. 2008], or radio-frequency (RF) receivers [Kiamilev et al. 2008; NSA 2013]. We consider this work outside the scope of our survey, however, as these techniques require hardware modification at the modulator as well as specialized hardware at the demodulator, and are more relevant to both the area of LPI communications in general as well as hardware tamper protection and detection.

4. SURVEY

In this section, we analyze the different channels that we feel could possibly be built on to establish an out-of-band covert channel by reviewing the related literature. We summarize the channel's effectiveness, that is, bandwidth, and further discuss the limitations of each channel as well as determine the hardware required for the modulator and demodulator to facilitate communication. Last, we summarize relevant protection mechanisms that can be put in place to limit or eliminate the proposed covert channel and discuss the efficiency, that is, covertness, of each alternative. We organize our survey into six sub-sections, each covering a specific channel:

(1) Acoustic
(2) Light
(3) Vibration
(4) Magnetic
(5) Temperature
(6) Radio-frequency

4.1. Out-of-Band Covert-Acoustic Channels

Utilizing covert audio signals for the purposes of leaking information from air-gapped systems has previously been discussed in Carrara and Adams [2015a], Deshotels [2014], OMalley and Choo [2014], and Hanspach and Goetz [2013, 2014]. Hanspach and Goetz [2013] built a proof-of-concept covert network with five identical Lenovo laptops and demonstrated that audio communication can be achieved in the near-ultrasonic range from 17kHz to 20kHz. Their research demonstrated that frequency-hopping spread spectrum (FHSS) with 48 sub-channels can be used to effectively establish a covert channel capable of transmitting data at a rate of 20 bits per second (bps) up to a distance of 19.7m. Hanspach and Goetz [2014] documented the ability to communicate using two Lenovo T400 model laptops over the ultrasonic range from 20.5kHz to 21.5kHz at a speed of 20bps up to a range of 8.2m. OMalley and Choo [2014] established a covert channel between a MacBook Pro and a Lenovo tablet using Frequency Shift Keying (FSK) in the ultrasonic range between 20kHz and 23kHz; however, the authors used an external speaker at the transmitter to achieve their results. Additionally, Deshotels [2014] demonstrated the ability to communicate information between mobile

Android devices using audio signals between units separated by 100 feet. Deshotels was able to achieve over 300bps using FSK in the 18-kHz to 19-kHz bandwidth. Last, Carrara and Adams [2015a] demonstrated the ability to communicate in the ultrasonic range from 20kHz to 20.5kHz at a rate of 140bps using orthogonal frequency-division multiplexing (OFDM) signals. Furthermore, the authors defined the concept of the *overnight attack*, that is, leaking information via audio signals when no humans are present in the environment, and demonstrated that, by using the audible spectrum, bit rates over 6.7 kilobits per second (kbps) could be achieved.

The use of audio has also been researched as an alternative to traditional wireless communication (e.g., infrared (IR), Bluetooth, RF, Wi-Fi, and NFC); however, due to the relatively low bandwidth available in the channel when compared to IR and RF as well as the negative impacts of audio on humans and animals, this alternative solution has been primarily only studied in academic circles [Gerasimov and Bender 2000; Landström 1990]. Gerasimov and Bender [2000] studied the use of audio communication over-the-air for the purpose of device-to-device communication and were able to achieve a bit rate of 3.4kbps using spread-spectrum techniques in the 0-Hz to 20-kHz bandwidth. In Lopes and Aguiar [2001, 2003, 2010], researchers examined the ability to communicate using pleasant-sounding audio signals in order to exchange pre-authorization information required for wireless networks as well as uniform resource locators (URLs). The researchers synthesized audio signals using frequencies from musical scales, chords, and lullabies as well as from fictional characters (e.g., R2D2 from Star Wars) and insects. Similarly, Domingues et al. [2002] studied the ability to communicate using audio signals that sound like musical instruments (e.g., piano, clarinet, and bells). Madhavapeddy et al. [2003, 2005] examined audio communication as an alternative to Bluetooth wireless communication through the use of dual-tone multi-frequency (DTMF) signalling, on-off keying (OOK), and melodic sounds. Madhavapeddy et al. also studied ultrasonic communication between two laptops with third-party speakers. Last, Nandakumar et al. [2013] experimented with audio communication as an alternative to NFC. In their work, the authors also presented *Jam Secure*, a self-interfering technique to provide information-theoretically secure communication. *Jam Secure*, however, uses audible signals to secure the communication that can easily be detected by both humans and technical equipment.

Side channel attacks that recover information from leaked acoustic signals have also been presented. Tromer [2004, 2007] demonstrated that CPUs in modern machines leak a specific acoustic signal related to the operation being performed. Using an external microphone, the researchers were able to pick up specific acoustic signatures during common CPU operations (e.g., HLT, MUL, FMUL, ADD, etc.) as well as common cryptographic operations (e.g., RSA decryption). The researchers found that the leaked audio signals emanated from the capacitors on the motherboards that they studied. The work of Tromer was extended by LeMay and Tan in LeMay and Tan [2006] in which they demonstrated that covert data could be leaked using acoustic signals by varying the algorithms executed on the CPU of the modulator. The acoustic signature generated by each algorithm could then be detected by a demodulator to recover the transmitted data. Recent work in Genkin et al. [2013] has demonstrated that not only specific algorithms executed on remote machines but also the contents of RSA private keys can be identified. Genkin et al. [2013] demonstrated that by performing a chosen plain-text attack against a target, the target's RSA private key can be recovered. In their research, they were able to recover key material by analyzing acoustic signals captured by the built-in microphone of a mobile device that was placed 30cm from the target. Performing the same attack using specialized equipment (e.g., a parabolic microphone) allowed the researchers to recover the target's private key at a distance of over 4m.

4.1.1. Limitations. Interference in the context of acoustic communication can be caused by background ambient noise; however, as discussed in Carrara and Adams [2015a], the background noise in office environments is larger for frequencies below 5kHz and tapers off as frequency increases. Given that sound is a slow-moving signal (about 300m/s in air), the modulator and demodulator must account for delays as well as changes in the channel impulse response in time as well. Furthermore, Doppler effect must be accounted for if either the modulator, demodulator, or both are moving while communication is taking place. Last, reflections of audio signals off of objects in the environment can also cause significant echo, which can result in inter-symbol interference.

4.1.2. Device Requirements and Bandwidth. Given the research in the area, acoustic signals can be generated by a modulator either by sending audio signals to a speaker or by executing specific algorithms on its CPU. Producing audio signals by executing specific algorithms is a particularly insidious method for generating covert signals as all machines must have at least one CPU to operate and thus no additional hardware is required. On the other hand, speakers are either optional or can be physically removed. Audio signals can be produced using commodity speakers in at least the 0-Hz-to-22-kHz range; some add-on speakers demonstrate frequency responses much higher than 22kHz. Furthermore, the electronic components on motherboards (e.g., capacitors, coils) can produce signals at frequencies at least as high as 40kHz. More research is required to determine the true low-pass frequency of CPU acoustic emanations and if all frequencies under 40kHz are accessible to the modulator. On the demodulator end, commodity microphones installed in most laptops, mobiles, and USB headsets can detect audio signals upwards of 22kHz with various degrees of fidelity, and therefore acoustic communication between unmodified systems is possible over the 0-Hz-to-22-kHz bandwidth.

4.1.3. Covertness. We examine the covertness of audio signals by qualitatively analyzing the ability of an adversary to detect covert communication given knowledge of the medium and modulation scheme. In the works that we studied, the authors' claims of creating a covert channel were based on their adversary's naïvety regarding the use of audio signals for communication. Techniques such as communicating via ultrasonic signals or audible signals using the overnight attack rely on the fact that humans are not able to perceive the signals using their natural ability to hear. Furthermore, the covertness of audio signals generated by CPUs rests on the signals being of very low power and therefore only faintly audible to humans present in the environment. In other words, the reviewed covert channels relied on "security through obscurity." In all the cases we studied, knowledge of the medium implied detection. Adversaries (e.g., guards in the solitary confinement problem) concerned with protecting themselves against this type attack could easily detect the covert communication by tuning their equipment to the correct frequency(ies). A number of the modulation schemes that we studied were based on spread-spectrum techniques (e.g., FHSS, direct sequence spread spectrum (DSSS)); however, none of the authors presented results showing the use of spread-spectrum techniques in low-signal-to-noise-ratio (SNR) configurations, where the signal power is constrained to be lower than the noise power in order to hide the signal. The use of spread-spectrum techniques combined with low-SNR signals is a known method for hiding communication from adversarial detection [Proakis 2008] and has previously been applied to audio signals in the area of underwater covert audio communication, see Ling et al. [2010], Leus and van Walree [2008], and van Walree et al. [2009].

4.1.4. Defence Mechanisms. A number of defence mechanisms have been presented by various authors to either prevent or detect covert audio communication. Hanspach and Goetz [2013, 2014] proposed the use of a low-pass filter to remove all ultrasonic signals from audio tracks before they are played by the system's speakers. The same authors also proposed the use of a host-based audio intrusion detection system (HIDS) tuned to detect the leakage of information via audio signals. While potentially effective, a HIDS suffers from the fact that all parameters of the attack must be known before a signature can be generated. This might be difficult, if not impossible, where spread-spectrum techniques are used and the pseudonoise (PN) sequence is generated in a sufficiently random fashion. Furthermore, Carrara and Adams pointed out in Carrara and Adams [2015b] that wideband techniques can be employed by a passive device to easily detect "covert" signals by checking the spectrum for abnormally high peaks of energy in areas of the spectrum where the energy is typically lower (e.g., in the ultrasonic spectrum). All authors also proposed the obvious protection mechanism of physically removing the speakers and microphones from machines that do not require them or disabling them in software. As pointed out by Carrara and Adams [2015a], however, malware can easily enable the devices if they are simply disabled in software. Other defence mechanisms that should be further explored include wideband and narrowband jamming, depending on the modulation scheme used by the covertly communicating partners [Proakis 2008]. To protect against acoustic signals produced by devices on CPU motherboards, the authors of Tromer [2004, 2007] proposed placing the leaky devices in sound-proof chambers as well as covering the devices in acoustic shielding; however, the authors pointed out that the source of the acoustic signals was typically vent holes, which cannot be covered, as they are required to prevent the machine from overheating. The introduction of random operations by the CPU is also a potential defence mechanism worth exploring.

4.2. Out-of-Band Covert-Light Channels

Light communication for the purposes of malware command and control was examined in Hasan et al. [2013]. In Hasan et al. [2013], two light-based communication experiments were performed: First, a modulator was implemented to modify the intensity of a light source in a room such that a demodulator could detect the intensity changes using a mobile phone's ALS. Second, the authors displayed a "trigger" image on a liquid crystal diode (LCD) monitor, laptop display, and 47-inch LCD TV and used an ALS to pick up the trigger. The authors performed range and angle tests to determine the maximum bit rate they could achieve and determined that light-based signals can be used to establish a very low bit-rate covert channel. To date, the use of light signals to pair devices has also been explored by many researchers. Balfanz et al. [2002] used IR signals, a privileged side channel, between two devices to exchange pre-authentication information, that is, commitments on public keys, to bootstrap key exchange in ad hoc wireless networks. The initial exchange of commitments was done over the IR channel since it was assumed that the channel provided "demonstrative identification," that is, channel authentication given IR's limited range and line of sight requirements. Additionally, McCune et al. used barcodes, both printed and displayed on a screen, to communicate pre-authentication information, that is, hashes [McCune et al. 2005]. In their *Seeing-is-Believing* protocol, the modulator displayed a barcode (or a series of barcodes) and the demodulator took a photo of the barcode to extract the hash from the captured image. Mutual entity authentication is supported but requires both devices to have a display and a camera. Saxena et al. [2008] created a device-pairing scheme based on blinking LEDs. The modulator required two LEDs (or a display), one for data exchange and one for synchronization, while the demodulator required a camera. Their scheme exchanged short authenticated strings (SAS) [Vaudenay 2005] to authenticate

the communicating parties' public keys. Data are communicated by having one device modulate data by blinking its LEDs and the other capture and process images of the blinking LEDs. As a follow-up to this work, Sexena, et al. created a protocol to attain mutual entity authentication with only one use of the out-of-band channel in Saxena et al. [2011]. Their algorithm, however, required a human to interact with one of the devices to complete the protocol. Similar LED-based approaches are discussed in Gauger et al. [2009], Perković et al. [2009], and Roman and Lopez [2008] to perform key assignment in ad hoc wireless sensors networks.

Side channel attacks based on optical emissions, "Optical TEMPEST," has also received attention in the research community. Kuhn [2002] showed that the contents of cathode ray tube (CRT) monitors could be reconstructed by analyzing the light intensity of the display's diffuse reflection off a wall. Reconstruction of the screen's contents was possible because the light intensity of the last few thousand pixels drawn by a CRT leaked a low-pass-filtered version of the video signal. Using signal processing techniques and specialized hardware (e.g., photomultiplier and photosensor), a reading chart displayed on the screen could be reconstructed by processing the screen's reflections. According to Kuhn, however, LCD monitors are not susceptible to the same light intensity attack [Kuhn 2005]. Backes et al. showed that the contents of LCD screens could also be reconstructed by analyzing diffuse reflections off objects in the environment (e.g., teapots, eyeglasses, bottles, spoons, and a wine glass) [Backes et al. 2008]. The authors showed that 18-pt font displayed on a screen and reflected off a teapot could be reconstructed from up to 10m away. Furthermore, by using telescopic lenses, their attack could be extended to 30m—a realistic distance between two buildings. Backes et al. followed up their compromising reflections work in Backes et al. [2009] by improving their attack through the use of a deconvolution algorithm and showed that reflections off more objects in the environment (e.g., human eye, shirt) could be used to reconstruct the screen's contents. Similarly, Raguram et al. [2011] were able to reconstruct characters typed on the LCD screen of an iPhone by analyzing reflections of the screen off objects in the environment. Their work demonstrated that using a commodity camera, captured images of both the screen directly as well as its reflection could be analyzed to extract typed key sequences by looking for the "pop-out" keys displayed by the iPhone's virtual keyboard. Their attack was effective over distances up to 14 feet away. This work is significant because it represents a method of communication (or leakage) that is based on the normal function of the device, that is, displaying an image on the screen, and not an unintended leakage produced by using the device. Last, Loughry and Umphress [2002] demonstrated that certain devices, namely network gear, leaked their internal state through the LEDs on their interfaces. Given the speed at which LEDs can turn on and off, and the fact that a number of device manufactures tied their status LEDs to their devices' serial lines, the LEDs can be monitored by a simple photodiode, that is, ALS, to read the data being processed.

4.2.1. Limitations. Communicating via light intensity works best in low-light conditions where there is little to no ambient light in the room (e.g., overhead light, sun, television, etc.). Furthermore, a number of the results that we outlined in this section required the help of specialized hardware (astronomic telescopes in the works of Backes et al. and a photomultiplier in the work of Kuhn) that are not found in commodity laptops, desktops, or mobiles. Additionally, while IR transceivers were once typical in commodity hardware, they are no longer as widely deployed as they used to be. Light communication also generally requires the receiving sensor to be unobstructed and therefore light communication will not work if the receiving device (e.g., camera and ALS) is stowed. Further research is required to determine if the cameras that are prevalent in today's mobile phones, laptops, and monitors are capable of capturing images that will

allow reflections or off-angle views of the modulator's screen to be processed in order to facilitate communication.

4.2.2. Device Requirements and Bandwidth. In order for light signals to be used, a light-emitting device is required at the modulator, whether it be a screen (e.g., CRT, LCD, or LED) or status LEDs. On the other hand, the demodulator either requires an ALS or a camera to pick up the transmitted signal. In the work of Hasan et al. [2013], the authors were able to achieve a maximum bit rate of 0.5 bits per second with no bit errors using LEDs and an ALS. In McCune et al. [2005], the researchers were able to achieve bit rates of around 580 bps using a screen and camera. The bandwidth of their channel is highly governed by the choice of barcode displayed, that is, the amount of data encoded in the barcode, and how long the barcode needs to be displayed in order for the demodulator to decode the message. The researchers in Saxena et al. [2008] required the LEDs to be lit for 250ms in order for a bit to be communicated and therefore they were able to achieve a bit rate of approximately 4bps using LEDs and a camera. The goal of device pairing, however, is not necessarily to achieve the highest possible bit rate and it is often desirable for the communication to be slowed down so the humans involved in the pairing process can visually validate what is going on. In Gauger et al. [2009], the researchers were able to achieve bit rates of up to 71bps using the *sensor node lamp*, a specialized LED modulator, and 8bps using the display of a personal digital assistant (PDA). Furthermore, Roman and Lopez [2008] achieved bit rates of 500bps using their KeyLED scheme. In general, the bit rate of light communication will be governed by the maximum rate that the modulator can update its display and the sampling rate of the demodulator. Further research is required to determine the maximum rate at which data can be communicated between commodity hardware using light communication in typical usage environments (e.g., office and home).

4.2.3. Covertness and Defence Mechanisms. The goal of Hasan et al. [2013] was to create a covert command and control network based on light signals. Communication was facilitated through small fluctuations in the overhead light to modulate data, which presumably were unnoticeable to any humans in the environment. This, too, is a form of "security through obscurity," as any entity monitoring the light intensity in the room would be able to detect that "covert" communication is taking place. Additionally, in Gauger et al. [2009] and Perković et al. [2009], the researchers made the assumption that no adversary had access to the light-based communication channel. This assumption is not valid in our model, but one that is perhaps valid in the context of initial key assignment and shows that more research is required to determine ways in which light communication can be used to meet the security requirements of out-of-band covert communications. The main defence against information transfer via light is to either reduce the brightness of the modulator, that is, display, or shield it. Filters can also be added to displays to reduce their viewing angle and polarized filters that are 90° offset from each other can be placed on screens in the room as well as the room's windows to prevent signals from leaking outside the room. Jamming, by ensuring high levels of ambient light, can also be used to reduce the risk of diffuse reflections. Additionally, to limit the channel's bandwidth, operating systems can either prevent access to the status LEDs on devices or limit the rate at which status LEDs can be turned on and off.

4.3. Out-of-Band Covert-Vibration Channels

Hasan et al. [2013] also explored covert malware communication through vibration signals by describing two methods that a modulator could use to create vibrations: playing an audio track with low-frequency content or activating the vibrator in a device. Creating vibrations using audio equipment is especially effective if the machine under the control of the modulator has a sub-woofer or speakers with an ideal frequency response

in the low-frequency range. Hasan et al. hypothesized that low-frequency audio signals could be imperceptible to humans but detectable using commodity microphones at a distance of a few feet. The authors also described a method to transmit communication signals through enabling and disabling a mobile phone's vibrator; however, the vibration signals were shown to have a high latency and were only detectable from a few centimeters away. Subramanian et al. [2013] similarly demonstrated that malware communication could also be accomplished through vibrations. Furthermore, researchers have shown that by utilizing the vibrator and accelerometer on the same device, a physical covert channel can also be established [Deshotels 2014; Al-Haiqi et al. 2014]. Deshotels [2014] demonstrated that Android devices, in contact with one another, could communicate using vibration signals lasting as little as 1ms. Interestingly, the vibration signals used in Deshotels' work were imperceptible to humans.

Vibration-based communication has also been used in device-pairing applications. Saxena et al. [2009] devised PIN-Vibra, a protocol between a vibrator-equipped mobile device and an accelerometer-equipped radio-frequency identification (RFID) tag. The authors used OOK and a 200-ms symbol time, that is, vibration time, to transmit information. Their scheme was built on the assumption that the vibration channel was authenticated (user pressed the vibrating mobile phone against a specific RFID tag) and secret (user could verify that no eavesdropper was also simultaneously in contact with the mobile phone); however, Halevi and Saxena [2010] demonstrated that the mobile phone's vibrations produced an acoustic signal that could be picked up by a commodity microphone from up to 3 feet away. Additionally, Studer et al. [2011] proposed an alternative to the widely popular Bump protocol [Wikipedia 2014]. Bump is a protocol that allows users, having no pre-shared keys, to exchange information in a more secure manner by incorporating accelerometer readings taken while bumping their phones together. Studer et al. were able to show that a man-in-the-middle attack could be launched against the protocol and proposed an alternative protocol, Shake on it. Their protocol used the vibrator in one phone to send a pre-authenticator hash to another phone in contact with it. The pre-authenticator hash was then subsequently used to verify the transmitter's public key, which was exchanged over a traditional wireless link. Last, Marquardt et al. [2011] were able to demonstrate a side-channel attack to reconstruct the keystrokes typed on a keyboard located in close proximity to an accelerometer-equipped cell phone. The authors remarked that the mobile phone could only determine the keystrokes pressed if the mobile was within a couple of inches from the keyboard.

4.3.1. Limitations. The biggest current limitation of the vibration channel, in the context of out-of-band covert channels, is that over-the-air communication has not been demonstrated to be possible. Additionally, as demonstrated by Marquardt et al. [2011], the vibration signal can only be detected over a short distance; however, more exhaustive testing is required to determine the maximum distance vibrations can travel given common mediums (e.g., desk and table). Path loss in the vibration channel has been shown to be dependent on the distance between the communicating devices, the velocity of the vibrations, and the medium the vibrations are travelling through. Furthermore, the authors in Deshotels [2014] argued that vibrations induced by a speaker could be detected up to a few feet away; however, the authors did not test their hypothesis. Last, as is the case with acoustic channels, vibration signals suffer from a high degree of latency, which must be taken into account at the demodulator.

4.3.2. Device Requirements and Bandwidth. Vibration-based channels are transmitted by a modulator with commodity hardware through controlled vibrations using a speaker or vibrator and are received by a demodulator through readings from an accelerometer. Subramanian et al. [2013] demonstrated bit rates up to 65bps using a vibrator and

accelerometer; however, the vibrations were not meant to be undetectable to users in the environment but rather were made to be covert by mimicking the same vibrations generated when an incoming call is received. In Studer et al. [2011], the researchers were able to achieve 17bps using the same devices. In both cases, however, the vibrator and the accelerometer were in mobile devices that were placed in contact with one another. Therefore, a bit rate of tens of bits per second most likely represents an upper bound on the amount of data that can be exchanged using the vibration channel established when commodity hardware is used.

4.3.3. Covertness. As previously mentioned, Deshotels generated vibrations in such a way that the signals were not perceptible to humans because short signal periods were used, that is, 1ms. Similarly, the low-frequency audio signals hypothesized by Hasan et al. were presumably of low-enough amplitude and frequency that the amplitude of the signals fell below the human auditory threshold for a given frequency. Both of these solutions generated signals that were imperceptible to humans but perceptible to correctly-tuned commodity hardware devices without reliance on a secret key. Further research is required to determine if vibration-based channels can even be established in a manner that meets the requirements of out-of-band covert channels, that is, undetectable communication. Mimicking environmental vibrations is an alternative that should be further explored to meet these requirements [Subramanian et al. 2013].

4.3.4. Protection Mechanisms. To protect against covert vibrations generated through low-frequency sound, a high-pass filter could be applied to all audio tracks before they are amplified by the speaker. Furthermore, access to the vibrator and accelerometer could be monitored to ensure the device is not being abused. Additionally, systems that do not attach explicit user-controlled permissions to the vibrator and accelerometer should add mandatory access control policies that would limit liberal use of these components. Last, the sensitivity of the accelerometer should be reduced to the point where it still provides utility to generic application developers but limits the covert communication bandwidth possible.

4.4. Out-of-Band Covert-Magnetic Channels

Hasan et al. [2013] also explored malware command and control through magnetic signals. The authors described a malware triggering method detectable by a demodulator equipped with a magnetometer (i.e., e-compass), which is a component that can be found in most modern-day mobile phones to provide compass functionality. The authors modulated signals by using a programmatically controlled electro-magnet to induce changes in the detected magnetic field of the magnetometer and noticed that a 60-microtesla signal could be observed at a distance of 5 inches away from the demodulator device, and error-free communication was possible over a distance of 3.5 inches. Their experiments also showed that triggering via magnetic field was not negatively impacted when the electro-magnet (modulator) was covered by clothing. Given this property, the authors concluded that a magnetic trigger could be covertly installed at a choke point where multiple magnetometer-equipped devices pass through (e.g., elevator, doorway). Additionally, a number of patents have been filed documenting the ability to pair devices using magnetic signals. Libes [2002] proposed the use of add-on peripherals, capable of sending and receiving magnetic signals, in order to create an alternative wireless communication link between devices in close proximity to each other. The authors also proposed using the magnetic wireless link for bootstrapping traditional wireless communication. Similarly, Hanna et al. [2009] described a method for bootstrapping wireless communication by exchanging credentials over a magnetic wireless link. The pairing protocol was designed to replace the traditional simple pairing protocol used to allow Bluetooth-enabled devices to communicate. Last, researchers

have proposed the use of magnets to induce faults in cryptoprocessors in order to mount side-channel attacks [Giraud and Thiebeauld 2004; Samyde et al. 2002].

4.4.1. Limitations, Device Requirements, Bandwidth, Covertness, and Protection Mechanisms. There are a number of limitations to the magnetic channel. First, a transmitting device (i.e., (electro-)magnet) is not typically found in commodity devices, and therefore external hardware would be required to realize this channel. Second, magnetic field strength dissipates quickly as distance is increased because the field's strength is inversely proportional to the distance cubed. Third, all the works covered in this section only describe communication over a distance of at most 6 inches (the distance achievable is proportional to the strength of the electro-magnet used for modulation). Magnetometers are also designed to monitor the Earth's natural magnetic field (i.e., noise), and therefore any received magnetic signals from the channel must be stronger than those coming from the Earth, which were measured at between 30 and 50microtesla in Hasan et al. [2013]. Additionally, while magnetic fields can travel through non-metallic objects, the presence of metal will cause interference. Finally, in order for magnetic signals to be used, a large amount of current, 500A, is required to induce a magnetic field even over a distance of just 1m (note that 1A is enough to cause electrocution) [Griffiths and College 1999].

From a demodulator's perspective, magnetometers are prevalent in today's modern mobile phones and have a sampling rate of anywhere from 100kHz to 400kHz; however, further research is required to determine realistic achievable bit rates using the magnetic channel. From a protection point of view, the most obvious physical safeguard would be to place the device in metal shielding; however, confining devices to a shielded room is most likely impractical in areas other than high-security zones as users want to be mobile. Furthermore, generally applying metal shielding would cause interference to traditional RF signals. Last, none of the works studied explicitly took undetectability into account and it is presumed that a covert analyst that has knowledge of the algorithms used in these works would be able to detect the channel using technical tools. Going forward, schemes such as spread-spectrum modulation [Peterson et al. 1995] at power levels below that of the Earth's magnetic field should be explored as a possible solution to hide covert-magnetic channels from a passive adversary.

4.5. Out-of-Band Covert-Temperature Channels

While examining the problem of deanonymizing Tor hidden services, Murdoch first introduced the concept of temperature-based covert channels in Murdoch [2006]. In his work, Murdoch demonstrated that a process (modulator) could increase the CPU load on a machine in order to cause a rise in the machine's internal temperature and, causally, an increase in the machine's clock skew (i.e., a delay in the clock signal). Furthermore, Murdoch showed that a machine's clock skew could be monitored by a remote process (demodulator) by observing the machine's transmission control protocol (TCP) timestamps. Given the causal relationship between increased CPU load and clock skew, a covert channel could be created between two remote processes. Additionally, Murdoch showed that a server's CPU load could also be increased remotely by initiating additional network traffic to the server. By combining the abilities to remotely increase CPU load and observe timestamps, Murdoch was able to demonstrate a novel network covert channel. Murdoch finally demonstrated that hidden services on the Tor network could be exposed through the use of this covert channel. Murdoch's proposal for creating an out-of-band covert channel between two adjacent servers placed in contact with one another in a server rack is of particular relevance to this survey. Murdoch hypothesized that two processes, running on two different machines, Servers A and B, could covertly communicate: A modulator on Server A would increase its server's CPU load that would

in turn increase the temperature of Server A and Server B; a demodulator on Server B would then measure Server B's clock skew. Although Murdoch presented this idea for an out-of-band covert channel, no bit rates were provided. Last, while the work was not necessarily presented in a covert channel context, researchers have proposed the use of temperature-based proximity sensors to facility device pairing [Cohen et al. 2011; Rinaldo et al. 2005] and the induction of temperature-based faults into crypto-processors to make side-channel attacks possible [Li et al. 2012].

4.5.1. Limitations, Device Requirements, Bandwidth, and Protection Mechanisms. Murdoch's temperature-based communication channel was measured in Murdoch [2006] and Zander et al. [2011] and was shown to be of extremely low bandwidth, on the order of about 10^{-4} Hz [Zander et al. 2011]. Therefore, the bit rates achieved by Murdoch and Zander et al. range in the tens of bits *per hour*; however, low-bandwidth information, that is, passwords, could still be leaked using a temperature-based channel over a long period of time (see the small message criterion [Moskowitz and Kang 1994]). In conclusion, however, known temperature-based covert channels do not form a viable general-purpose communication channel, and more research would be required to determine if temperature-based channels are a viable solution to the solitary confinement problem. On the other hand, temperature-based channels do have one major advantage in that they do not require any additional hardware at the modulator or demodulator, and thus there are no additional hardware requirements in order for the covert channel to be established. Furthermore, modern devices contain an internal thermometer, and therefore research should be performed to determine if the bandwidth of temperature-based covert channels could be increased through utilizing this component. Finally, Zander et al. [2011] outlined a number of possible protection mechanisms for temperature-based covert channels. They proposed the use of a clock crystal producing a regular clock signal that is not influenced by temperature. Additionally, they proposed throttling network traffic or CPU load to further reduce the bandwidth of the channel, removing all timestamps from network protocols (e.g., TCP timestamps), as well as introducing noise by either running the CPU at 100% utilization at all times or spiking the CPU to 100% utilization at random intervals.

4.6. Out-of-Band Covert RF Channels

According to Highland [1988], government agencies have known about the possibilities of compromising electromagnetic emanations from electronic equipment since the 1980s and have focused their study of these possibilities under the program name TEMPEST. Electronic equipment (e.g., power supplies, microprocessor chips, cables, monitors, video display units, printers, keyboards, etc.), in general, generates high levels of radio-frequency radiation when left unshielded. CRTs, specifically, have been shown to leak a significant amount of radio-frequency radiation to the extent that the displayed contents of a CRT monitor can be reconstructed by an eavesdropper from 1km away [Van Eck 1985]. In 1985, van Eck realized, through his research, that CRTs leaked their contents at harmonic frequencies of the CRT's clock and pixel rate (time between illuminating adjacent pixels) in a manner that resembled television broadcasting. By tuning his eavesdropping equipment to the specific frequencies of the leaked signals, van Eck was able to reconstruct images displayed by an unshielded (plastic) CRT from 1km away as well as images displayed on a shielded (metal) CRT from up to 200m away. In his attack, van Eck used no special signal processing techniques to enhance the signal and instead relied on readily available RF communication equipment (e.g., antenna, variable oscillator, television set). Since van Eck's work, many researchers have continued to exploit leaked-CRT electromagnetic emanations and have studied signal processing algorithms to improve their reception as well as focused

their attack on different sources of CRT electromagnetic emanations [Hongxin et al. 2009; Köksaldi et al. 1998; Ling et al. 1997; Sekiguchi 2009; Dong et al. 2002]. In 2005, Kuhn demonstrated that LCD displays were also vulnerable to TEMPEST-style attacks [Kuhn 2005, 2006]. Kuhn was able to demonstrate that, despite increased shielding becoming a requirement, pixel frequencies and video bandwidths increasing, and analog signals between computers and monitors approaching gigabit per second speeds, compromising emanations were still detectable at a distance of up to 10m away using a wideband antenna. Furthermore, Kuhn was able to show that, by controlling a display's foreground (text) and background color, remote reconstruction of leaked images displayed on a monitor could be improved. Other researchers have also examined leakage from LCD monitors in an effort to quantitatively assess the amount of information leaked [Tanaka 2007] and reduce the cost and space of the eavesdropping equipment [Elibol et al. 2012]. Last, side-channel attacks exploiting compromising RF emanations from cryptographic processing devices have been demonstrated in Chari et al. [2003], Gandolfi et al. [2001], and Agrawal et al. [2003].

Controlling electromagnetic emanations through software, specifically for the purposes of leaking sensitive information, has been the focus of "Soft TEMPEST" research [Kuhn and Anderson 1998; Anderson and Kuhn 1999]. Kuhn and Anderson [1998] examined a scenario where a virus installed on a secure "red" machine could egress data to an insecure "black" machine by controlling the contents of the secure machine's display. Armed with knowledge of the display's pixel rate and horizontal and vertical frequencies, the authors were able to demonstrate two techniques, FSK and Amplitude Modulation (AM), to leak information from a secure system to an insecure system. In their first experiment, the authors demonstrated the ability to generate signals that could be picked up by a commodity AM radio by displaying a periodic pattern of solid black and white vertical bars on the screen. By controlling the width of the bars, specific frequencies could be detected by the AM radio, thus allowing a virus to leak signals using FSK. The screen displayed a very distinct visible pattern, but the researchers were able to achieve a data rate of 50bps using this technique. Kuhn and Anderson improved their attack by using dithering techniques to embed recoverable images and text in the images that were displayed to the user, thus hiding the source of the leaked emanations. By hiding high-frequency colours behind low-frequency colours (the human eye is more sensitive to low-frequency colors) a virus could leak AM signals using this technique. As a countermeasure, the authors presented *TEMPEST Fonts* that consisted of filtered fonts whose high-frequency components had been removed. Tanaka et al. [2005], however, showed that even the use of *TEMPEST Fonts* could not prevent the leaking of compromising emanations and proposed the use of additional filtering techniques using Gaussian filters to reduce the leakage. Similarly, Guri et al. [2014] demonstrated that by modulating the video signals being sent to a display through different types of cables (e.g., video graphics array (VGA), digital video interface (DVI), and high-definition multimedia interface (HDMI)), FSK and DTMF data symbols could be communicated to the commodity frequency-modulation (FM) radios that are found in popular mobile phone models.

4.6.1. Limitations and Device Requirements. Electromagnetic emanations are able to travel long distances through non-metallic mediums with little interference. However, the biggest limitation to covert RF channels is the lack of commodity hardware at the receiver capable of detecting or receiving covert RF signals over long distances. The research of Kuhn and Anderson [1998] and Guri et al. [2014] is of particular relevance to our work because of the ability to receive signals using commodity AM and FM radios, which can be found in a number of modern mobile devices. The other side-channel attacks listed in this section, however, require a number of highly specialized probes,

antennae, synchronization equipment, and filters, not all of which can be replicated in software. Furthermore, for a number of the side-channel attacks discussed in the literature, there is a requirement for the probes to be placed either in contact or in close proximity to the leaky components embedded in crypto-processors in order to isolate the required signals. From a modulator device requirement perspective, the main system component studied in the literature capable of transmitting covert RF signals has been monitors (e.g., CRTs and LCDs) and video display units; however, research has also shown that it is possible to recover signals from the cables used to connect a machine to other peripherals as well [Smulders 1990].

4.6.2. Bandwidth and Covertness. Research into the capacity of signals leaked by LCDs has been analyzed from an information-theory perspective in Tanaka [2007]. Tanaka calculated that the information capacity of signals emanating from an LCD could be upwards of 100 megabits per second (Mbps) due the large SNR that the author measured using a near-field magnetic probe. There is potential for a large amount of data to be leaked by a video display unit, simply from the fact that a large amount of information is processed by the device. A 24-bit color display at a pixel resolution of 1024×768 processes 18 megabits of information per frame. At a frame rate of 60Hz the display will process about one gigabit of data per second. It remains to be seen, however, if all of the pixels and their color values displayed to the user can be recovered by analyzing leaked electromagnetic radiation. Furthermore, the amount of information deliberately leaked through display emanations would presumably be much less once the covert RF signals are hidden from both human perception as well as detection by a motivated passive adversary. Kuhn and Anderson [1998] were able to leak data at a rate of 50bps; however, the frequencies that they needed to generate required a specific image to be displayed on the screen that was clearly visible to the user. Kuhn and Anderson were able to hide their leaked signals using a dithering technique; however, the leaked signals were only hidden from human perception and could be reconstructed by any party with knowledge of their algorithm. Guri et al. [2014] were able to leak data at a rate of up to 60 bytes per second and demonstrated that signals could be leaked even when the monitor was turned off. Spread spectrum at low SNR should also be explored going forward as a possible technique to hide covert RF communication.

4.6.3. Protection Mechanisms. In general, the countermeasures that can be put in place to protect against leaky devices are broken down into hardware protections and software protections. Shielding, both at the device and in rooms where sensitive material is processed, is an effective way to prevent electromagnetic signals from being leaked. Similarly, filters can be added to all cables as well as external devices to prevent them from amplifying signals. Jamming can also be used to increase the noise in the environment. Additionally, government organizations worried about compromising emanations have designated special zones, which have been specifically retrofitted to prevent leaks [Kuhn 2006]. Using this scheme, both devices and locations in a building are assigned a zone. Each location's zone indicates at what minimum distance an eavesdropper could have access to emanations leaked from this zone. Similarly, a device is assigned to a zone based on how far its electromagnetic signals travel. A device is therefore restricted to a zone or zones to prevent its electromagnetic emanations from being accessed by an eavesdropper.

A number of software-based countermeasures have also been proposed. The use of *TEMPEST Fonts* was proposed to prevent Kuhn and Anderson's dithering attack. Similarly, the use of filters, in general, has also been proposed by researchers [Tanaka 2007; Tanaka et al. 2005] in order to reduce the possibility of leaking high-frequency signals. Additionally, randomized displays, where pixels are not drawn in sequential

order, have also been proposed. Kuhn also proposed using two DVI standards to thwart eavesdropping in Kuhn [2005]. By using *selective refresh* or *digital content protection*, the intelligible leaked signals can be reduced or completely eliminated.

4.7. Summary

We provide a summary of our survey in Tables I and II. We see from the results that, in general, the channels that we studied are of relatively low bandwidth (kilobits per second and below) when compared to traditional communication links (e.g., Wi-Fi, mobile communication standards). This is not surprising, given that the channels that we examined are established by abusing sensors and devices that were never designed for communication. Additionally, while the use of the devices can be tailored for optimum reception, the bandwidth of the channels is still constrained by the limited power that can be vectored towards achieving covert communication. In saying that, general purpose text-based communication is possible using the limited-bandwidth channels that we have presented in this work. As an example, an individual typing 7-bit ASCII text at 80 words per minute at an average word length of 5.1 characters would produce data at an average rate of 47.6bps, which could be communicated in real-time through covert acoustic, covert light, or covert RF channels and nearly in real-time using the covert vibration channel. Furthermore, using a low-bit-rate codec (e.g., LPC-10 [Lee and Cox 2001]), voice data could be communicated using covert acoustic signals and, realistically, documents could also be transmitted using covert acoustic, covert RF, and covert light channels. A summary of popular document formats and their average page sizes is presented in Table III.

We also note from the results of our study that, aside from some covert RF configurations, the out-of-band signals that we studied have limited transmission range and are furthermore typically constrained by common environmental obstacles (e.g., walls, doors, and ceilings). This is due to the the physical properties of the signals and the fact that out-of-band covert channels are exploiting non-traditional modes of communication that have not been engineered for communication purposes. Additionally, the signals that we studied have limited transmit power available for communication and attenuate very quickly with increased distance. Last, for some channels (e.g., covert-magnetic, some covert-RF configurations), there is limited hardware support for out-of-band communication and, therefore, these channels are less likely to provide a good medium for general-use out-of-band covert communication. On the other hand, there are a number of viable existing physical channels available for out-of-band covert channels. Both covert-light and covert-acoustic channels as well as covert-RF channels that allow demodulation using an AM/FM receiver benefit from widespread hardware support, increased distance when compared to the other alternatives, and the possibility of achieving higher-bandwidth channels (hundreds of bits per second and above). While a study to determine the highest-achievable bandwidth using covert-acoustic and covert-RF channels in common environments has been performed in Carrara and Adams [2015a] and Guri et al. [2014], respectively, a similar study is required for covert-light channels.

All the out-of-band covert channels that we studied achieved covertness by hiding their signals in the signal space above the sensitivity of on-board sensors and below human perception, thus relying on the fact that on-board sensors are *more sensitive* than our natural senses. The current adversarial model that researchers have been using assumes a passive adversary that is both unaware and unassuming of the covert communication, and therefore the covertness of the channels has only been measured by a human's natural ability to perceive the signals. This adversarial model needs to be expanded to include a passive adversary that is aware of both the channel and modulation scheme and is armed with technical tools developed to detect covert communication. Furthermore, the ability of an active adversary (e.g., ability to jam signals

Table I. Out-of-Band Covert Channel Summary (Table 1 of 2)

Covert -*(channel)*	Acoustic		Light				
Modulator Requirements	Speaker	CPU	Screen	Screen	LEDs	LEDs	Infrared transceiver
Demodulator Requirements	Microphone	Microphone	ALS	Camera	ALS	Camera	Infrared transceiver
Order of Data Rate	Kilobits per second	Data rates not provided in LeMay and Tan [2006]	Bits per second	Hundreds of bits per second	Hundreds of bits per second	Hundreds of bits per second	Megabits per second
Order of Distance	Tens of meters	Tenths of a meter	Meters	Meters	Meters	Meters	Meters
Channel Limitations	–Relatively large ambient noise –Relatively large signal delay –Relatively large Doppler effect –Reverberations –Limited range (CPU modulator) –Limited transmission power (CPU modulator)		–Relatively large ambient noise (e.g., sun, room lighting) –Signal doesn't travel through opaque objects –Limited deployment of hardware in some cases (e.g., Infrared)				

Covert -*(channel)*	Vibration		Magnetic	Temperature
Modulator Requirements	Speaker	Vibrator	(Electro-)magnet	CPU load-inducing process
Demodulator Requirements	Accelerometer	Accelerometer	Magnetometer	Clock monitoring process
Order of Data Rate	Data rates were not provided in Hasan et al. [2013]	Tens of bits per second	Data rates were not provided in Hasan et al. [2013]	Tens of bits per hour
Order of Distance	Tens of meters	Tenths of a meter	Tenths of a meter	Contact is required
Channel Limitations	–Cannot travel over the air –Relatively large signal delay –Path loss is dependent on the medium –Limited range (vibrator)		–Controllable electro-magnets (modulator) are not typically found in commodity devices –Limited range –Path loss is inversely proportional to the distance cubed –Background noise from the earth's natural magnetic field	–Extremely low bandwidth –Contact (or extremely close proximity) of modulator and demodulator required –100% CPU utilization required to increase temperature

Table II. Out-of-Band Covert Channel Summary (Table 2 of 2)

Covert *-(channel)*	Radio-Frequency					
Modulator Requirements	CRT	CRT	LCD	Screen	Peripheral Cables	CPU
Demodulator Requirements	AM receiver	Specialized hardware	Specialized hardware	FM receiver	Specialized hardware	Specialized hardware
Order of Data Rate	Tens of bits per second	Data rates not provided	Data rates not provided	Hundreds of bits per second	Data rates not provided	Data rates not provided
Order of Distance	Tens of meters	Kilometers	Meters	Meters	Meters	Tenths of a meter
Channel Limitations	–Lack of hardware support at the demodulator in commodity devices (aside from AM/FM demodulator) –Device-specific parameters (e.g., pixel rate, horizontal and vertical frequencies) affect modulated signals					

Table III. Average Sizes (kb) of Popular Document Types

Document Type	Average Size (kb) per Page [NetDocuments 2014]
Microsoft Word	15
Microsoft Excel	6
Microsoft PowerPoint	57
Portable Document Format	100
Text	1.5
Email	10
Tagged Image File Format	65

and inject messages) should be examined more closely. Going forward, out-of-band covert communication protocols should not rely on "security through obscurity" to obtain covertness if truly covert channels capable of undetectable communication are to be realized. Hiding strategies (e.g., hiding information in background noise, utilizing diverse channels for communication) [Che et al. 2014] could be employed to increase the covertness of current out-of-band covert channels and should be considered by covert channel designers going forward.

The protection mechanisms that have been documented in each of the sections above can be broken down into a number of general strategies. First, signals below the threshold of human perception should be filtered out so they cannot be used for covert communication. Similarly, devices should be physically shielded whenever possible. If filtering or shielding is not possible, then the covert signals should be deliberately jammed, that is, increase the ambient noise in the environment. Additionally, if the device sensors are superfluous, then they can either be physically removed from the device or disabled in software. Furthermore, all sensors should be monitored for abuse (in terms of frequency of access), perhaps with the use of an intrusion detection system, and, whenever possible, the sensitivity of the sensor's readings should be reduced such that their legitimate use can continue but not their abuse. From a secure system development perspective, mandatory access control policies should be enforced to limit access to sensors, and application-specific manifests should be used to document all required sensor accesses. Last, as a general rule, all sensor accesses should be logged and periodically audited to help determine if a sensor is being used for covert communication.

5. TAXONOMY

In Figure 3, we present a hierarchy showing the classification of out-of-band covert channels. Our research shows that modulation schemes, channel limitations, and protection mechanisms, at this point in the study of out-of-band covert channels, are directly related to the hardware used to realize each covert channel, and, therefore, grouping by channel and hardware is the most representative view of the research at this point in time. As a result, we propose first grouping out-of-band covert channels along the general category of hardware required by each modulator and demodulator, which can be seen in *Tier 1* and *Tier 2*, respectively, in Figure 3. Furthermore, in *Tier 3*, we group modulator and demodulator hardware requirements based on the channel that they communicate over. Last, in *Tier 4*, we place the modulator and demodulator hardware devices as the leaf nodes in our taxonomy tree.

Our taxonomy classifies hardware devices into three general categories: *commodity-pervasive*, *commodity-limited*, and *specialized*. We place hardware in the *commodity-pervasive* category if the hardware can be found in most commodity systems (e.g., mobile phones, laptops, and desktops). Furthermore, we place hardware in the *commodity-limited* category if the hardware can only be found in a limited number of systems or only in a general category of systems (e.g., only mobile phones). Finally, we place hardware in the *specialized* category if the hardware is not found in commodity systems but instead is specialized hardware constructed for a specific purpose (e.g., telescope, parabolic microphone, and wideband antenna). We group the hardware that we studied as follows:

—**Commodity-Pervasive:** CPU, screen (including LCD, CRT), speaker, microphone
—**Commodity-Limited:** Ambient light sensor, camera, light-emitting diodes, infrared transceiver, vibrator, accelerometer, magnetometer, AM receiver, FM receiver, cables
—**Specialized:** Electro-magnet, specialized RF equipment

In general, we group the hardware required at the modulator and demodulator based on their availability for a couple of reasons. First, for secure system developers, the prevalence of the required hardware maps to the risk posed by the covert channel. Grouping based on prevalence provides a qualitative measure that secure system developers can use to prioritize the risk of the covert channel and thus the priority of the requirement to build appropriate countermeasures into their systems. Second, for low-probability of intercept system developers, the prevalence of the covert channel's hardware provides a qualitative measure that allows developers to determine the general applicability of the covert channel to deployment scenarios, that is, as the covert channel can be established using more *commodity-pervasive* hardware the utility of the covert channel increases.

Given the infancy of the study of out-of-band covert channels, we provide our taxonomy as one such possible grouping. An alternative taxonomy would see out-of-band covert channels categorized based on their effectiveness, that is, bandwidth, and efficiency, that is, covertness; however, at this point in the research, the achievable bandwidth of each covert channel is still an open question. Furthermore, classifying channels based on their bandwidth would be a moving target, since, presumably, as out-of-band covert channels become more well studied, their achievable bandwidth would also increase. Last, while a general measure for the capacity of a channel exists there is no general measure for covertness (see Section 6).

6. FUTURE WORK

Going forward, there is work required on four general fronts. First, while covert-acoustic and covert-RF channels have been the most widely studied of the covert

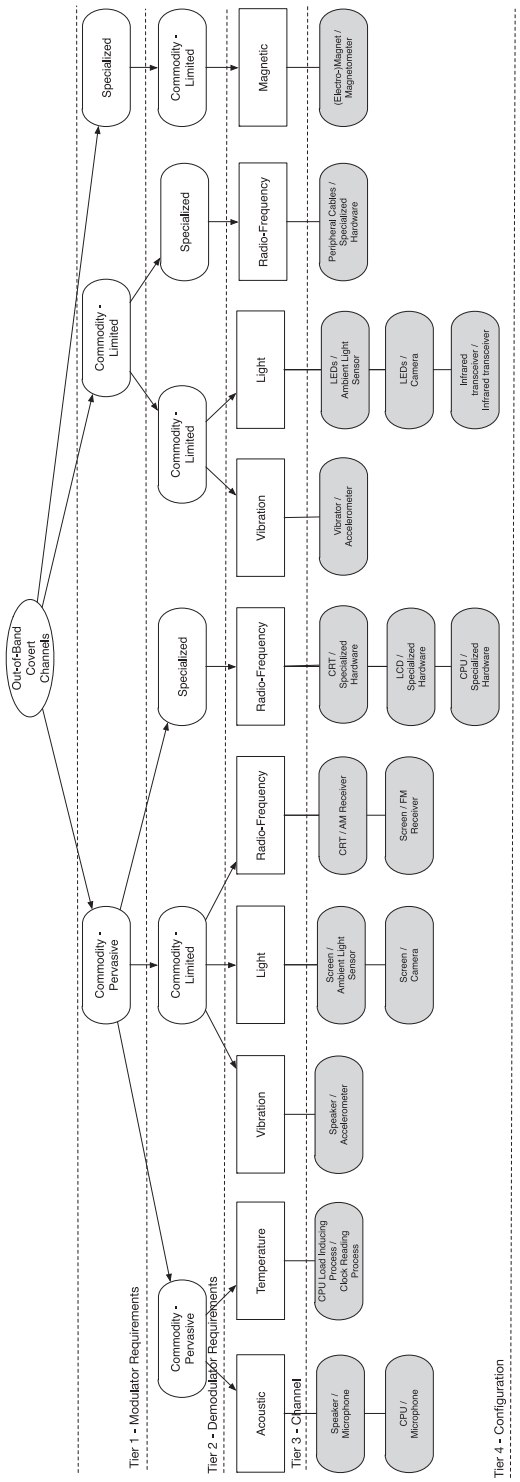

Fig. 3. Out-of-band covert channel hierarchy.

channels we analyzed, the other covert-*(channels)* that is, light, vibration, magnetic, and temperature, should similarly be extensively examined to determine the maximum bit rates that the channels can support. This involves studying the effects imposed on the channels from typical environments, that is, home, office, outdoors, as well as performing tests on a broad range of commodity equipment to assess general support for the channel. Additionally, a model governing the bit error rates (BER) of the channels should be established and the sources of all errors should be closely examined in order to determine the proper error-correcting codes to apply given the observed channel perturbations. Furthermore, new, innovative covert-*(channels)* should also be investigated.

Second, a generally agreed-on adversarial model needs to be established to assess the covertness of out-of-band covert channels going forward. At a minimum, we would recommend the following: First, the passive adversary considered should be aware of the channel and modulation scheme used for communication while the active adversary considered should be capable of injecting data into the channel as a means to disrupt communication, that is, jam. In the LPI literature, these adversaries are referred to as interceptors and their objective, in both the active and passive cases, is to increase the probability of detecting covert communication, while reducing the probability of false alarms, that is, a false positive that detection has occurred. Furthermore, given an active adversary's capabilities, out-of-band covert channels should also be analyzed to determine the jammer's effect on bit error rate, which is the typical analysis carried out when assessing LPI radar systems [Glenn 1983].

Third, given an updated adversarial model, researchers should explore solutions to limit the detectability of out-of-band covert channels by applying techniques from the body of literature on LPI and low probability of detection communication systems [Glenn 1983; Proakis 2008; Schoolcraft 1991]. General techniques, such as DSSS and FHSS, should be applied to the covert-*(channels)* outlined in this work. While some of these techniques have been used in previous work, they have not been used in a manner that would deter detection from a knowledgeable passive or active adversary. By applying low probability of detection solutions to out-of-band covert channels, tradeoffs between parameters (e.g., interceptor bandwidth, spread-spectrum bandwidth, and range) and probability of detection can be more closely examined to determine appropriate system thresholds.

Last, and most importantly, a general measure of "covertness" should be studied and established. Currently, there is no general measure that allows the covertness of two arbitrary covert channels to be compared. A measure, similar to channel capacity, that allows the upperbound of two arbitrary channels' rates to be compared, should be established going forward to better classify and compare covert channels. While some researchers have discussed ideas for measuring covertness [Giani et al. 2006], no definitive measure has been established.

7. CONCLUSION

In this work, we present the solitary confinement problem, an extension of Simmons' classical subliminal channel problem, to motivate our classification of out-of-band covert channels. The solitary confinement problem is stated as follows: Two prisoners are placed in solitary confinement and are unable to communicate with one another by traditional means, that is, message passing. Their goal, however, is to establish a covert, out-of-band communication channel that is undetectable by the guards who are watching them. The goal of the guards, on the other hand, is to devise a scheme to detect the covert communication channel. We present this model in order to motivate our classification of out-of-band covert channels, which are LPI communication channels established between isolated processes by modulating and demodulating a shared medium using devices that are not traditionally used for communication.

We compare the existing sub-categories of covert channels, namely single-host, physical, and network covert channels, to out-of-band covert channels and demonstrate that out-of-band covert channels are a new category on their own that, to date, has not been studied in depth. In our survey, we further categorize the existing techniques in the covert channel, device-pairing, and side-channel literature that share similar requirements to out-of-band covert channels, that is, non-traditional forms of communication, and focus on covert channels that do not require hardware modification but instead leverage the set of sensors now standard in commodity hardware. We further provide terminology for out-of-band covert channels as well as a taxonomy based on the physical channels, that is, acoustic, light, vibration, magnetic, temperature, and radio-frequency, and the hardware requirements of the modulator (transmitter) and demodulator (receiver).

Our survey shows that out-of-band covert channels, in general, are not as high bandwidth as conventional radio-frequency channels; however, they are, in general, capable of transferring up to hundreds and, in some cases, for example, covert-acoustic, thousands of bits per second. We also note that, in general, out-of-band covert signals have limited transmission range and are, furthermore, typically constrained by common environmental obstacles (e.g., walls, doors, and ceilings). Additionally, in some cases (e.g., covert-magnetic and some covert-RF configurations), there is limited hardware support for out-of-band communication at the demodulator and therefore these channels are less likely to provide good general-use out-of-band covert communication. We show, however, that there are viable covert channels available for system developers to incorporate into privacy-preserving applications. Both covert-light and covert-acoustic channels as well as covert-RF channels provide benefits in the form of widespread hardware support, increased sender-receiver distance when compared to other alternatives, and the possibility for higher-bandwidth channels (hundreds of bits per second and above).

Additionally, through our analysis of state-of-the-art out-of-band covert channels, we show that current covert channel schemes rely on an unaware and unassuming passive adversary. As a result, we propose a more comprehensive adversarial model where a passive adversary is aware of both the communication channel and modulation scheme used for covert communication. We additionally propose that the capabilities of an active adversary be considered when determining the effectiveness of covert channels going forward. Furthermore, we show that, to date, none of the existing covert channels that we studied meet the requirements for out-of-band covert channels. Last, in addition to enhancing the adversarial model, we generalize the protection mechanisms that can be put in place by secure system developers to either eliminate or limit the efficiency, that is, bandwidth, of out-of-band covert channels and point out that a general measure of "covertness" is required.

REFERENCES

Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, and Pankaj Rohatgi. 2003. The EM sidechannel (s). In *Cryptographic Hardware and Embedded Systems-CHES 2002*. Springer, Berlin, 29–45.

Ahmed Al-Haiqi, Mahamod Ismail, and Rosdiadee Nordin. 2014. A new sensors-based covert channel on android. *The Scientific World Journal* 2014, Article ID 969628, 14 pages.

Ross Anderson, Mike Bond, Jolyon Clulow, and Sergei Skorobogatov. 2006. Cryptographic processors-a survey. *Proc. IEEE* 94, 2 (2006), 357–369.

Ross Anderson, Serge Vaudenay, Bart Preneel, and Kaisa Nyberg. 1996. The Newton channel. In *Information Hiding (Lecture Notes in Computer Science)*, Ross Anderson (Ed.), Vol. 1174. Springer, Berlin, 151–156.

Ross J. Anderson and Markus G. Kuhn. 1999. Soft tempest–An opportunity for NATO. *Protecting NATO Information Systems in the 21st Century* (1999).

Ross J. Anderson and Fabien A. P. Petitcolas. 1998. On the limits of steganography. *IEEE J. Select. Areas Commun.* 16, 4 (1998), 474–481.

Micahel Backes, Tongbo Chen, Markus Duermuth, Hendrik Lensch, and Martin Welk. 2009. Tempest in a teapot: Compromising reflections revisited. In *2009 30th IEEE Symposium on Security and Privacy*. IEEE Los Alamitos, CA, 315–327.

Michael Backes, Markus Durmuth, and Dominique Unruh. 2008. Compromising reflections-or-how to read LCD monitors around the corner. In *IEEE Symposium on Security and Privacy, 2008 (SP 2008)*. IEEE, Los Alamitos, CA, 158–169.

Dirk Balfanz, Diana K. Smetters, Paul Stewart, and H. Chi Wong. 2002. Talking to strangers: Authentication in ad-hoc wireless networks. In *Network and Distributed System Security Symposium*.

D. Elliott Bell and Leonard J. LaPadula. 1973. *Secure Computer Systems: Mathematical Foundations*. Technical Report. Defense Technical Information Center Document.

Krista Bennett. 2004. *Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text*. Technical Report. Purdue University. CERIAS TR 2004-13.

Kenneth J. Biba. 1977. *Integrity Considerations for Secure Computer Systems*. Technical Report. Defense Technical Information Center Document.

Brent Carrara and Carlisle Adams. 2015a. On acoustic covert channels between air-gapped systems. In *Foundations and Practice of Security*, Frdric Cuppens, Joaquin Garcia-Alfaro, Nur Zincir Heywood, and Philip W. L. Fong (Eds.). Lecture Notes in Computer Science, Vol. 8930. Springer International Publishing, Berlin, 3–16.

Brent C. Carrara and Carlisle Adams. 2015b. On characterizing and measuring out-of-band covert channels. In *Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec'15)*. ACM, New York, NY, 43–54.

Rajarathnam Chandramouli, Mehdi Kharrazi, and Nasir Memon. 2004. Image steganography and steganalysis: Concepts and practice. In *Digital Watermarking*. Springer, Berlin, 35–49.

Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi. 2003. Template attacks. In *Cryptographic Hardware and Embedded Systems-CHES 2002*. Springer, Berlin, 13–28.

David L. Chaum. 1981. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM* 24, 2 (1981), 84–90.

Pak Hou Che, S. Kadhe, M. Bakshi, Chung Chan, S. Jaggi, and A. Sprintson. 2014. Reliable, deniable and hidable communication: A quick survey. In *Information Theory Workshop (ITW), 2014 IEEE*. 227–231.

David D. Clark and David R. Wilson. 1987. A comparison of commercial and military computer security policies. In *2012 IEEE Symposium on Security and Privacy*. IEEE Computer Society, 184–184.

Alexander J. Cohen, Edward K. Y. Jung, Royce A. Levien, Robert W. Lord, Mark A. Malamud, and John D. Rinaldo Jr. 2011. Device pairing via device to device contact. (April 12 2011). US Patent 7,925,022.

George Danezis and Claudia Diaz. 2008. *A Survey of Anonymous Communication Channels*. Technical Report. Technical Report MSR-TR-2008-35, Microsoft Research.

Luke Deshotels. 2014. Inaudible sound as a covert channel in mobile devices. In *Proceedings of the 8th USENIX Conference on Offensive Technologies (WOOT'14)*. USENIX Association, Berkeley, CA, USA, 16–16. http://dl.acm.org/citation.cfm?id=2671293.2671309.

Roger Dingledine, Nick Mathewson, and Paul Syverson. 2004. *Tor: The Second-Generation Onion Router*. Technical Report. Defense Technical Information Center Document.

Natacha Domingues, Joao Lacerda, Pedro M. Q. Aguiar, and Cristina V. Lopes. 2002. Aerial communications using piano, clarinet, and bells. In *2002 IEEE Workshop on Multimedia Signal Processing*. IEEE, 460–463.

Shiwei Dong, Xu Jiadong, Haobin Zhang, and Wu Changying. 2002. On compromising emanations from computer VDU and its interception. In *Electromagnetic Compatibility, 2002 3rd International Symposium on*. IEEE, Los Alamitos, CA, 692–695.

Fürkan Elibol, Uğur Sarac, and Işin Erer. 2012. Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system. In *Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European*. IEEE, Los Alamitos, CA, 1767–1771.

Karine Gandolfi, Christophe Mourtel, and Francis Olivier. 2001. Electromagnetic analysis: Concrete results. In *Cryptographic Hardware and Embedded Systems CHES 2001 (Lecture Notes in Computer Science)*, Vol. 2162. Springer, Berlin, 251–261.

Matthias Gauger, Olga Saukh, and Pedro J. Marron. 2009. Enlighten me! Secure key assignment in wireless sensor networks. In *Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on*. IEEE, Los Alamitos, Ca, 246–255.

Daniel Genkin, Adi Shamir, and Eran Tromer. 2013. RSA key extraction via low-bandwidth acoustic cryptanalysis. *IACR Cryptology ePrint Archive* 2013 (2013), 857.

Vadim Gerasimov and Walter Bender. 2000. Things that talk: Using sound for device-to-device and device-to-human communication. *IBM Syst. J.* 39, 3.4 (2000), 530–546.

Annarita Giani, Vincent H. Berk, and George V. Cybenko. 2006. Data exfiltration and covert channels. *Proc. SPIE* 6201 (2006), 620103–620103–11.

Christophe Giraud and Hugues Thiebeauld. 2004. A survey on fault attacks. In *Smart Card Research and Advanced Applications VI*. Springer, Berlin, 159–176.

C. Gray Girling. 1987. Covert channels in LAN's. *IEEE Trans. Softw. Eng.* 2 (1987), 292–296.

Alvin Glenn. 1983. Low probability of intercept. *IEEE Commun. Mag.* 21, 4 (1983), 26–33.

Virgil D. Gligor. 1994. *A Guide to Understanding Covert Channel Analysis of Trusted Systems*. National Computer Security Center.

Joseph A. Goguen and José Meseguer. 1982. Security policies and security models. In *2012 IEEE Symposium on Security and Privacy*. IEEE Computer Society, 11–11.

David Jeffrey Griffiths and Reed College. 1999. *Introduction to Electrodynamics*. Vol. 3. Prentice Hall, Upper Saddle River, NJ.

Mordechai Guri, Gabi Kedma, Assaf Kachlon, and Yuval Elovici. 2014. AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. In *2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE)*. 58–67.

J. Thomas Haigh, Richard A. Kemmerer, John McHugh, and William D. Young. 1987. An experience using two covert channel analysis techniques on a real system design. *IEEE Trans. Softw. Eng.* 2 (1987), 157–168.

Tzipora Halevi and Nitesh Saxena. 2010. On pairing constrained wireless devices based on secrecy of auxiliary channels: The case of acoustic eavesdropping. In *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS'10)*. ACM, New York, NY, 97–108.

George S. Hanna, Robert J. Higgins, John B. Preston, and Daniel A. Tealdi. 2009. Method and system for near-field wireless device pairing. (Aug. 3 2009). US Patent App. 12/534,246.

Michael Hanspach and Michael Goetz. 2013. On covert acoustical mesh networks in air. *J. Commun.* 8, 11 (2013).

Michael Hanspach and Michael Goetz. 2014. Recent developments in covert acoustical communications. In *Sicherheit (Safety) 2014 (Lecture Notes in Informatics)*. 243–254.

Michael Hanspach and Jörg Keller. 2014. A taxonomy for attack patterns on information flows in component-based operating systems. *Computing Research Repository* abs/1403.1165 (2014). http://arxiv.org/abs/1403.1165.

Ragib Hasan, Nitesh Saxena, Tzipora Haleviz, Shams Zawoad, and Dustin Rinehart. 2013. Sensing-enabled channels for hard-to-detect command and control of mobile devices. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (ASIA CCS'13)*. ACM, New York, NY, 469–480.

Jingsha He and Virgil D. Gligor. 1990. Information-flow analysis for covert-channel identification in multilevel secure operating systems. In *Computer Security Foundations Workshop III, 1990. Proceedings*. IEEE, 139–148.

Harold Joseph Highland. 1988. The tempest over leaking computers. *Abacus* 5, 2 (1988), 10–18.

Zhang Hongxin, Huang Yuewang, Wang Jianxin, Lu Yinghua, and Zhang Jinling. 2009. Recognition of electro-magnetic leakage information from computer radiation with SVM. *Comput. Security* 28, 1 (2009), 72–76.

Wei-Ming Hu. 1992. Reducing timing channels with fuzzy time. *J. Comput. Security* 1, 3 (1992), 233–254.

P. Jayaram, H. R. Ranganatha, and H. S. Anupama. 2011. Information hiding using audio steganography–A survey. *Int. J. Multimed. Appl.* 3 (2011), 86–96.

Neil F. Johnson and Stefan Katzenbeisser. 2000. A survey of steganographic techniques. In *Information Hiding*. Artech House, Norwood, MA, 43–78.

Myong H. Kang and Ira S. Moskowitz. 1993. A pump for rapid, reliable, secure communication. In *Proceedings of the 1st ACM Conference on Computer and Communications Security (CCS'93)*. ACM, New York, NY 119–129.

Paul A. Karger and John C. Wray. 1991. Storage channels in disk arm optimization. In *1991 IEEE Computer Society Symposium on Research in Security and Privacy, 1991, Proceedings.*. IEEE Computer Society, 52–61.

Richard A. Kemmerer. 1983. Shared resource matrix methodology: An approach to identifying storage and timing channels. *ACM Trans. Comput. Syst.* 1, 3 (1983), 256–277.

Richard A. Kemmerer and Phillip A. Porras. 1991. Covert flow trees: A visual approach to analyzing covert storage channels. *IEEE Trans. Softw. Eng.* 17, 11 (1991), 1166–1185.

Auguste Kerckhoffs. 1883. *La Cryptographie Militaire*. Vol. 9. 5–38 pages.

Fouad Kiamilev, Ryan Hoover, Ray Delvecchio, Nicholas Waite, Stephen Janansky, Rodney McGee, Corey Lange, and Michael Stamat. 2008. Demonstration of hardware Trojans. *DEFCON* 16 (2008).

Alfred Kobsa, Rahim Sonawalla, Gene Tsudik, Ersin Uzun, and Yang Wang. 2009. Serial hook-ups: A comparative usability study of secure device pairing methods. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS'09)*. ACM, New York, NY, Article 10, 12 pages.

Paul Kocher, Joshua Jaffe, and Benjamin Jun. 1999. Differential power analysis. In *Advances in Cryptology CRYPTO 99 (Lecture Notes in Computer Science)*, Michael Wiener (Ed.), Vol. 1666. Springer, Berlin, 388–397.

N. E. Köksaldi, S. S. Şeker, and B. Sankur. 1998. Information extraction from the radiation of VDUs by pattern recognition methods. In *EMC'98: Electromagnetic Compatibility Conference*. 678–683.

Markus G. Kuhn. 2002. Optical time-domain eavesdropping risks of CRT displays. In *Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on*. IEEE, Los Alamitos, CA, 3–18.

Markus G. Kuhn. 2005. Electromagnetic eavesdropping risks of flat-panel displays. In *Privacy Enhancing Technologies (Lecture Notes in Computer Science)*, David Martin and Andrei Serjantov (Eds.), Vol. 3424. Springer, Berlin, 88–107.

Markus G. Kuhn. 2006. Eavesdropping attacks on computer displays. *Information Security Summit* (2006).

Markus G. Kuhn and Ross J. Anderson. 1998. Soft tempest: Hidden data transmission using electromagnetic emanations. In *Information Hiding (Lecture Notes in Computer Science)*, Vol. 1525. Springer, Berlin, 124–142.

Arun Kumar, Nitesh Saxena, Gene Tsudik, and Ersin Uzun. 2009. Caveat eptor: A comparative study of secure device pairing methods. In *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*. IEEE, Los Alamitos, CA, 1–10.

Butler W. Lampson. 1973. A note on the confinement problem. *Commun. ACM* 16, 10 (1973), 613–615.

Ulf Landström. 1990. Noise and fatigue in working environments. *Environ. Int.* 16, 4 (1990), 471–476.

Donald C. Latham. 1986. *Department of Defense Trusted Computer System Evaluation Criteria*. National Computer Security Center.

Ki-Seung Lee and Richard V. Cox. 2001. A very low bit rate speech coder based on a recognition/synthesis paradigm. *IEEE Trans. Speech Audio Process.* 9, 5 (2001), 482–491.

Michael LeMay and Jack Tan. 2006. Acoustic surveillance of physically unmodified PCs. In *Security and Management*. Citeseer, 328–334.

Geert Leus and Paul A. van Walree. 2008. Multiband OFDM for covert acoustic communications. *IEEE J. Select. Areas Commun.* 26, 9 (2008), 1662–1673.

Yang Li, Kazuo Ohta, and Kazuo Sakiyama. 2012. New fault-based side-channel attack using fault sensitivity. *IEEE Trans. Forens. Security* 7, 1 (2012), 88–97.

Michael Libes. 2002. Method and system for communication between two wireless-enabled devices. (February 2002). US Patent App. 10/087,536.

Lang Lin, Markus Kasper, Tim Güneysu, Christof Paar, and Wayne Burleson. 2009. Trojan side-channels: Lightweight hardware Trojans through side-channel engineering. In *Cryptographic Hardware and Embedded Systems-CHES 2009*. Springer, Berlin, 382–395.

Jun Ling, Hao He, Jian Li, William Roberts, and Petre Stoica. 2010. Covert underwater acoustic communications. *J. Acoust. Soc. Am.* 128, 5 (2010), 2898–2909.

Lu Ling, Nie Yan, and Zhang Hongjin. 1997. The electromagnetic leakage and protection for computer. In *Electromagnetic Compatibility Proceedings, 1997 International Symposium on*. IEEE, Los Alamitos, CA, 378–382.

Steven B. Lipner. 1975. A comment on the confinement problem. *SIGOPS Oper. Syst. Rev.* 9, 5 (Nov. 1975), 192–196.

Keith Loepere. 1985. Resolving covert channels within a B2 class secure system. *ACM SIGOPS Operat. Syst. Rev.* 19, 3 (1985), 9–28.

Cristina V. Lopes and Pedro M. Q. Aguiar. 2001. Aerial acoustic communications. In *Applications of Signal Processing to Audio and Acoustics, 2001 IEEE Workshop on the*. IEEE, Los Alamitos, CA, 219–222.

Cristina Videira Lopes and Pedro M. Q. Aguiar. 2003. Acoustic modems for ubiquitous computing. *IEEE Perv. Comput.* 2, 3 (2003), 62–71.

Cristina Videira Lopes and Pedro M. Q. Aguiar. 2010. Alternatives to speech in low bit rate communication systems. *Computing Research Repository* abs/1010.3951 (2010). http://arxiv.org/abs/1010.3951.

Joe Loughry and David A. Umphress. 2002. Information leakage from optical emanations. *ACM Trans. Inform. Syst. Security* 5, 3 (2002), 262–289.

Anil Madhavapeddy, David Scott, and Richard Sharp. 2003. Context-aware computing with sound. In *UbiComp 2003: Ubiquitous Computing (Lecture Notes in Computer Science)*, AnindK. Dey, Albrecht Schmidt, and JosephF. McCarthy (Eds.), Vol. 2864. Springer, Berlin, 315–332.

A. Madhavapeddy, R. Sharp, D. Scott, and A. Tse. 2005. Audio networking: The forgotten wireless technology. *IEEE Perv. Comput.* 4, 3 (July 2005), 55–60.

Claudio Marforio, Hubert Ritzdorf, Aurélien Francillon, and Srdjan Capkun. 2012. Analysis of the communication between colluding applications on modern smartphones. In *Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC'12)*. ACM, New York, NY, 51–60.

Philip Marquardt, Arunabh Verma, Henry Carter, and Patrick Traynor. 2011. (Sp)iPhone: Decoding vibrations from nearby keyboards using mobile phone accelerometers. In *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11)*. ACM, New York, NY, 551–562.

Jonathan M. McCune, Adrian Perrig, and Michael K. Reiter. 2005. Seeing-is-believing: Using camera phones for human-verifiable authentication. In *Security and Privacy, 2005 IEEE Symposium on*. IEEE, Los Alamitos, CA, 110–124.

John McDermott. 1994. *The B2/C3 Problem: How Big Buffers Overcome Covert Channel Cynicism in Trusted Database Systems*. Technical Report. Defense Technical Information Center Document.

Catherine Meadows and Ira S. Moskowitz. 1996. Covert channels - A context-based view. In *Information Hiding (Lecture Notes in Computer Science)*, Ross Anderson (Ed.), Vol. 1174. Springer, Berlin, 73–93.

Peter M. Melliar-Smith and Louise E. Moser. 1991. Protection against covert storage and timing channels. In *Computer Security Foundations Workshop IV, 1991. Proceedings*. IEEE, Los Alamitos, 209–214.

Jonathan K. Millen. 1976. Security kernel validation in practice. *Commun. ACM* 19, 5 (1976), 243–250.

Jonathan K. Millen. 1989. Finite-state noiseless covert channels. In *Computer Security Foundations Workshop II, 1989., Proceedings of the*. IEEE, Los Alamitos, CA, 81–86.

Jonathan K. Millen. 1999. 20 years of covert channel modeling and analysis. In *Security and Privacy, 1999. Proceedings of the 1999 IEEE Symposium on*. IEEE, Los Alamitos, CA, 113–114.

I. S. Moskowitz and A. R. Miller. 1994. Simple timing channels. In *Research in Security and Privacy, 1994. Proceedings., 1994 IEEE Computer Society Symposium on*. IEEE, Los Alamitos, CA, 56–64.

Ira S. Moskowitz and Myong H. Kang. 1994. Covert channels-here to stay? In *Computer Assurance, 1994. COMPASS'94 Safety, Reliability, Fault Tolerance, Concurrency and Real Time, Security. Proceedings of the Ninth Annual Conference on*. IEEE, Los Alamitos, CA, 235–243.

Ira S. Moskowitz and Allen R. Miller. 1992. The channel capacity of a certain noisy timing channel. *IEEE Trans. Inform. Theor.* 38, 4 (1992), 1339–1344.

Steven J. Murdoch. 2006. Hot or not: Revealing hidden services by their clock skew. In *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'06)*. ACM, New York, NY, 27–36.

Rajalakshmi Nandakumar, Krishna Kant Chintalapudi, Venkat Padmanabhan, and Ramarathnam Venkatesan. 2013. Dhwani: Secure peer-to-peer acoustic NFC. *SIGCOMM Comput. Commun. Rev.* 43, 4 (Aug. 2013), 63–74.

NetDocuments. 2014. File Sizes and Types. (2014). http://help.netdocuments.com/file-sizes/.

Ed Novak, Yutao Tang, Zijiang Hao, Qun Li, and Yifan Zhang. 2015. Physical media covert channels on smart mobile devices. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp'15)*. ACM, New York, NY, 367–378.

NSA. 2013. NSA's ANT Division Catalog of Exploits for Nearly Every Major Software/Hardware/Firmware. (2013). http://leaksource.info/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/

Samuel Joseph OMalley and Kim-Kwang Raymond Choo. 2014. Bridging the air gap: Inaudible data exfiltration by insiders. In *20th Americas Conference on Information Systems (AMCIS 2014)*. To appear.

Toni Perković, Ivo Stančić, Luka Mališa, and Mario Čagalj. 2009. Multichannel protocols for user-friendly and scalable initialization of sensor networks. In *Security and Privacy in Communication Networks*. Springer, Berlin, 228–247.

Roger L. Peterson, Rodger E. Ziemer, and David E. Borth. 1995. *Introduction to Spread-Spectrum Communications*. Vol. 995. Prentice Hall, Upper Saddle River, NJ.

Fabien A. P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn. 1999. Information hiding-a survey. *Proc. IEEE* 87, 7 (1999), 1062–1078.

Andreas Pfitzmann and Marit Hansen. 2010. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf. (Aug. 2010). v0.34.

Andreas Pfitzmann and Michael Waidner. 1987. Networks without user observability. *Comput. Security* 6, 2 (1987), 158–166.

Birgit Pfitzmann. 1996. Information hiding terminology - results of an informal plenary meeting and additional proposals. In *Proceedings of the First International Workshop on Information Hiding*. Springer-Verlag, London, 347–350. http://dl.acm.org/citation.cfm?id=647594.731530.

Andreas Polydoros and Charles L. Weber. 1985. Detection performance considerations for direct-sequence and time-hopping LPI waveforms. *IEEE J. Select. Areas Commun.* 3, 5 (1985), 727–744.

John G. Proakis. 2008. *Digital Communications*. McGraw-Hill, New York.

Niels Provos and Peter Honeyman. 2003. Hide and seek: An introduction to steganography. *IEEE Security Priv.* 1, 3 (2003), 32–44.

Rahul Raguram, Andrew M. White, Dibyendusekhar Goswami, Fabian Monrose, and Jan-Michael Frahm. 2011. iSpy: Automatic reconstruction of typed input from compromising reflections. In *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11)*. ACM, New York, NY, 527–536.

Michael K. Reiter and Aviel D. Rubin. 1998. Crowds: Anonymity for web transactions. *ACM Trans. Inform. Syst. Security* 1, 1 (1998), 66–92.

James W. Gray III. 1993. On introducing noise into the bus-contention channel. In *Research in Security and Privacy, 1993. Proceedings. 1993 IEEE Computer Society Symposium on*. IEEE, Los Alamitos, CA, 90–98.

John Rinaldo, Royce Levien, Robert Lord, Alexander Cohen, Mark Malamud, Edward Jung, and others. 2005. Device pairing via human initiated contact. (May 24 2005). US Patent App. 11/137,859.

Rodrigo Roman and Javier Lopez. 2008. KeyLED - transmitting sensitive data over out-of-band channels in wireless sensor networks. In *Mobile Ad Hoc and Sensor Systems, 2008. MASS 2008. 5th IEEE International Conference on*. IEEE, Los Alamitos, CA, 796–801.

David Samyde, Sergei Skorobogatov, Ross Anderson, and Jean-Jacques Quisquater. 2002. On a new way to read data from memory. In *Security in Storage Workshop, 2002. Proceedings. First International IEEE*. IEEE, Los Alamitos, CA, 65–69.

Nitesh Saxena, J.-E. Ekberg, Kari Kostiainen, and N. Asokan. 2011. Secure device pairing based on a visual channel: Design and usability study. *IEEE Trans. Inform. Forens. Security* 6, 1 (2011), 28–38.

Nitesh Saxena, Md. Borhan Uddin, and Jonathan Voris. 2008. Universal device pairing using an auxiliary device. In *Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS'08)*. ACM, New York, NY, 56–67.

Nitesh Saxena, Md Borhan Uddin, and Jonathan Voris. 2009. Treat'em like other devices: User authentication of multiple personal RFID tags. In *SOUPS*, Vol. 9. Citeseer, 1–1.

Marvin Schaefer, Barry Gold, Richard Linde, and John Scheid. 1977. Program confinement in KVM/370. In *Proceedings of the 1977 Annual Conference (ACM'77)*. ACM, New York, NY, 404–410.

Ralph Schoolcraft. 1991. Low probability of detection communications-LPD waveform design and detection techniques. In *Military Communications Conference, 1991. MILCOM'91, Conference Record, Military Communications in a Changing World*. IEEE, Los Alamitos, CA, 832–840 vol.2.

Hidenori Sekiguchi. 2009. Measurement of radiated computer RGB signals. *Progr. Electromagn. Res. C* 7 (2009), 1–12.

Shiuh-Pyng Shieh and Arbee L. P. Chen. 1999. Estimating and measuring covert channel bandwidth in multilevel secure operating systems. *J. Inf. Sci. Eng.* 15, 1 (1999), 91–106.

Gustavus J. Simmons. 1984. The prisoners problem and the subliminal channel. In *Advances in Cryptology*, David Chaum (Ed.). Springer, Berlin, 51–67.

Gustavus J. Simmons. 1985. The subliminal channel and digital signatures. In *Advances in Cryptology (Lecture Notes in Computer Science)*, Thomas Beth, Norbert Cot, and Ingemar Ingemarsson (Eds.), Vol. 209. Springer, Berlin, 364–378.

Gustavus J. Simmons. 1994. Subliminal communication is easy using the DSA. In *Advances in Cryptology EUROCRYPT 93 (Lecture Notes in Computer Science)*, Tor Helleseth (Ed.), Vol. 765. Springer, Berlin, 218–232.

Hitesh Singh, Pradeep Kumar Singh, and Kriti Saroha. 2009. A survey on text based steganography. In *Proceedings of the 3rd National Conference*. 3–9.

Peter Smulders. 1990. The threat of information theft by reception of electromagnetic radiation from RS-232 cables. *Comput. Security* 9, 1 (1990), 53–58.

Sang Hyuk Son, Ravi Mukkamala, and Rasikan David. 2000. Integrating security and real-time requirements using covert channel capacity. *IEEE Knowl. Data Eng.* 12, 6 (2000), 865–879.

Ahren Studer, Timothy Passaro, and Lujo Bauer. 2011. Don't bump, shake on it: The exploitation of a popular accelerometer-based smart phone exchange and its secure replacement. In *Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC'11)*. ACM, New York, NY, 333–342.

Venkatachalam Subramanian, Selcuk Uluagac, Hasan Cam, and Raheem Beyah. 2013. Examining the characteristics and implications of sensor side channels. In *2013 IEEE International Conference on Communications (ICC)*. IEEE, Los Alamitos, CA, 2205–2210.

Hidema Tanaka. 2007. Information leakage via electromagnetic emanations and evaluation of tempest countermeasures. In *Information Systems Security*. Springer, Berlin, 167–179.

Hidema Tanaka, Osamu Takizawa, and Akihiro Yamamura. 2005. Evaluation and improvement of the tempest fonts. In *Information Security Applications*. Springer, 457–469.

Eran Tromer. 2004. Acoustic cryptanalysis: On nosy people and noisy machines. *Eurocrypt2004 Rump Session, May* (2004).

Eran Tromer. 2007. *Hardware-based Cryptanalysis*. Ph. D. Dissertation. Weizmann Institute of Science, Tese de Doutorado. http://www.tau.ac.il/ tromer/papers/tromer-phd.pdf (Date last accessed: October 20, 2015).

Jonathan T. Trostle. 1993. Modelling a fuzzy time system. *J. Comput. Security* 2, 4 (1993), 291–309.

C.-R. Tsai, Virgil D. Gligor, and C. Sekar Chandersekaran. 1990. On the identification of covert storage channels in secure systems. *IEEE Trans. Softw. Eng.* 16, 6 (1990), 569–580.

Wim Van Eck. 1985. Electromagnetic radiation from video display units: An eavesdropping risk? *Comput. Security* 4, 4 (1985), 269–286.

Paul A. van Walree, Thorsten Ludwig, Connie Solberg, Erland Sangfelt, Arto Laine, Giacomo Bertolotto, and Anders Ishøy. 2009. UUV covert acoustic communications. In *Proceedings of the 3rd Conference on Underwater Acoustic Measurements: Technologies and Results*.

Serge Vaudenay. 2005. Secure communications over insecure channels based on short authenticated strings. In *Advances in Cryptology CRYPTO 2005 (Lecture Notes in Computer Science)*, Victor Shoup (Ed.), Vol. 3621. Springer, Berlin, 309–326.

Steffen Wendzel, Sebastian Zander, Bernhard Fechner, and Christian Herdin. 2015. Pattern-based survey and categorization of network covert channel techniques. *ACM Comput. Surv.* 47, 3, Article 50 (April 2015), 26 pages.

Wikipedia. 2014. Bump (application). (2014). https://en.wikipedia.org/wiki/Bump_(application)

John C. Wray. 1992. An analysis of covert timing channels. *J. Comput. Security* 1, 3 (1992), 219–232.

Sebastian Zander, Grenville J. Armitage, and Philip Branch. 2007. A survey of covert channels and countermeasures in computer network protocols. *IEEE Commun. Surv. Tutorials* 9, 1-4 (2007), 44–57.

Sebastian Zander, Philip Branch, and Grenville Armitage. 2011. Capacity of temperature-based covert channels. *IEEE Commun. Lett.* 15, 1 (2011), 82–84.

Yong Bin Zhou and Deng Guo Feng. 2005. Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing. *IACR Cryptology ePrint Archive* (2005), 388.

Received November 2014; revised November 2015; accepted April 2016