A Security Model for VoIP Steganography

Zhiwei Yu*, Clark Thomborson†, Chaokun Wang‡1, Junning Fu‡2 and Jianmin Wang‡3
*Department of Computer Science and Technology, Tsinghua University
‡School of Software, Tsinghua University
Key Laboratory for Information System Security, Ministry of Education
Tsinghua National Laboratory for Information Science and Technology(TNList), Beijing, China
Email: {yzw08*, fjn08[2]}@mails.tsinghua.edu.cn, {chaokun[1], jimwang[3]}@tsinghua.edu.cn
†Department of Computer Science, The University of Auckland, New Zealand
Email: cthombor@cs.auckland.ac.nz

***Abstract*—In 2005, an extensive taxonomy of threats for VoIP was published by a prominent industry group. Strangely, this taxonomy does not identify stegocommunication as a threat, even though many steganographic channels have been identified in VoIP protocols. To avoid such security gaps in the future, we argue that stegocommunication should be added to the traditional list of network threats: interruption, interception, modification, fabrication. The stegocommunication threat arises when the communication channel is purchased, provided, or supervised by anyone other than the communicating parties. We illustrate a stegocommunication threat to a business owner Charles. If Charles purchases a VoIP service for business-related communications by an employee Alice, then he faces the risk that Alice may undetectably communicate a business secret to an outside party Bob. In this insider-threat scenario, Charles can mitigate his security risk by installing a stegodetector.**

***Index Terms*—VoIP; Steganography; Security Model**

I. Introduction

Voice over Internet Protocol (VoIP) is the name given to any technology for voice communications over IP networks. VoIP's prominent advantage over traditional telephony is that the Internet provides a low-cost, highly-available, global IP service. This can greatly lower the total cost of voice, fax, video, and data services. VoIP has rapidly become a mainstream communications tool for many businesses, because of its cost and performance advantages. However, as with any new technology, the functional advantages and disadvantages of VoIP must be assessed in the light of its security advantages and disadvantages.

A few years ago, the Voice over Internet Protocol Security Alliance (VOIPSA) published an extensive taxonomy of threats for VoIP [1]. This taxonomy provides an excellent starting-point for a security assessment of a proposed or existing VoIP installation. According to its website (www.voipsa.org), VOIPSA is an open, vendor-neutral organization made up of VoIP and information security companies, organizations, and individuals with a desire to improve the security of VoIP. Its main activities include hosting discussion lists, writing white papers, supporting VoIP security research projects, and developing relevant tools and methods. It has three working groups, which focus respectively on best practices, security requirements, and a threat taxonomy for VoIP.

A threat taxonomy is useful in both retrospective and prospective security analyses. A retrospective analysis can categorise security events accurately, only if each security event is easily matched to exactly one category. In a prospective analysis, the completeness of a threat taxonomy is of paramount importance, because a security analyst may overlook important threats if they are not included in the taxonomy. We argue, in Section 2, that the VOIPSA taxonomy has a high-level category ("Service Abuse") within which a stegocommunication event could be clearly classified during a retrospective analysis. However the lack of any explicit mention of stegocommunication in the lower levels of the VOIPSA taxonomy seems a regrettable omission.

In Section 3, we discuss the influential taxonomy of network security described in Stallings' 1995 textbook [2], in which the fundamental threats are interruption, interception, modification, and fabrication. Stegocommunication threats are unclassifiable in this taxonomy. This seems a strange omission in a textbook which adopts the OSI definition of a security attack as "any action that compromises the security of information owned by an organisation." The taxonomic gap arises, we believe, because of a tacit assumption that the message-sending Alice always defines the security requirements for the communication system she is using. Another tacit assumption is that Alice's intended communication partner, Bob, is not adversarial. Stalling's 2007 edition [3] has some additional threats but still does not cover stegocommunication. We indicate how Stalling's taxonomies can be extended to cover the insider threat of stegocommunication.

In Section 4, we discuss insider threats in more detail, showing that an insider threat will arise whenever we analyse a communication system from the point of view of any actor other than Alice. Alice's security goals differ, in general, from those of her employer, her government, her economic peers, or her social peers. These four types of security-defining actors are derived from Lessig's control taxonomy [4] in the context of a general framework for security analysis [5]. We illustrate a relevant analysis in this analytic framework, by considering a business scenario where Alice is an employee of Charles. Charles provides Alice with VoIP so that she can communicate with trusted business clients. He also reveals a business secret to her. A confidentiality threat arises for Charles if Alice isn't trustworthy, for she may reveal the secret to her accomplice

Social Threats	Misrepresentation	Misrepresenting Identity
		Misrepresenting Authority
		Misrepresenting Rights
		Misrepresenting Content
	Theft of Services	
	Unwanted Contact	Harrassment
		Extortion
		Unwanted Lawful Content
Eavesdropping	Call Pattern Tracking	
	Traffic Capture	
	Number Harvesting	
	Conversation Reconstruction	
	Voicemail Reconstruction	
	Fax Reconstruction	
	Video Reconstruction	
	Text Reconstruction	
Interception and Modification	Call Black Holing	
	Call Rerouting	
	Fax Alteration	
	Conversation Alteration	
	Conversation Degrading	
	Conversation Impersonation and Hijacking	
	False Caller Identification	
Service Abuse	Call Conference Abuse	
	Premium Rate Service (PRS) Fraud	
	Improper Bypass or Adjustment to Billing	
	Stegocommunication	
	Other Improper Access to Services	
Interruption	Denial of Service	VoIP Specific DoS
		Network Services DoS
		Underlying Operating System/Firmware DoS
		Distributed Denial of Service
	Physical Intrusion	
	Loss of Power	
	Resource Exhaustion	
	Performance Latency	

TABLE I
VOIPSA THREAT TAXONOMY [1], WITH STEGOCOMMUNICATION.

Bob. If Charles is aware of the stegocommunication threat, he might periodically inspect Alice's PC for steganographic software, and he might install a stegodetector on his intranet. However these mitigations would be considered only if Charles is aware of his exposure to a stegocommunication threat. Existing taxonomies from VOIPSA and Stallings would not help Charles identify this threat, unless they are extended as suggested in Sections 2 and 3 of this paper.

We summarise our three-fold contributions in Section 5. In this paper we propose an extension to the VOIPSA taxonomy, so that it clearly covers the stegocommunication threat. We also extend Stallings' threat taxonomies. Finally, we derive a stegocommunication threat in a specific business scenario, using a framework in which the security analyst is encouraged to consider how an employee Alice's functional and security goals may differ from the goals of her employer Charles.

II. EXTENSION OF THE THREAT TAXONOMY OF VOIPSA

As indicated in Table I, there are six primary categories in VOIPSA's threat taxonomy [1]: Social Threats, Eavesdropping, Interception and Modification, Service Abuse, and Interruption. These primary categories are subdivided into secondary categories. Some of the secondary categories are, in turn, subdivided into tertiary categories. The VoIP Specific DoS tertiary category has a total of eighteen threats in two additional levels of categorisation.

The definition of the Social Threat category is predicated on an explicit, but informal, analysis of the rights and privileges of VoIP users and VoIP service providers in a Hohfeldian framework [6]. User privileges include privacy and freedom of communication. Each user's privileges are limited. For example, Alice's freedom of communication does not extend to Unwanted Contact to other users. All privileges are limited by applicable laws, and also by "other vital needs such as return on investment and convenience." The VOIPSA taxonomy does not cover the security issues arising when a user's legitimate security goals, their limited understanding of the conditions of the VoIP service provision, or their jurisdiction, differs from the assumptions of the VOIPSA security model. Instead, this category of the VOIPSA threat taxonomy covers just three types of misbehaviour which would harm other users or a VoIP service provider: Misrepresentation, Theft of Services, and Unwanted Contact.

The Misrepresentation subcategory of Social Threat is of particular interest to steganographers. In the VOIPSA security model, a user has a limited privilege to maintain anonymity "where there is communications between parties consenting to a false marking of identity or where communication would reasonably be understood to be under a pseudonym for privacy e.g. 'Jane Doe'." The feasibility of providing, and attacking, anonymous and untraceable VoIP was explored recently by Chen et al. [7], in a security model where Alice and Bob are members of peer group which maintains an anonymising network. Their use of an anonymiser would, presumably, be *prima facie* evidence of their personal consent to a false marking of identity, so the model of Chen et al. seems consistent with the VOIPSA model. However we note that a third party (perhaps Alice's employer) may be paying for Alice's VoIP services. The consent of this third party may also be required, if Alice (and the VoIP service provider, and the other participants in the anonymising network) are to survive a legal challenge, by the third party, to Alice's privilege (as defined in the VOIPSA service model) of anonymity.

The Eavesdropping category covers cases where "an attacker is able to monitor the entire signaling and/or data stream between two or more VoIP endpoints, but cannot or does not alter the data itself." All threats in this category are limited to attacks by outsiders, for any form of eavesdropping is allowed if it is authorised. Any illegal abuse of this authority by an insider would, presumably, be considered unauthorised in retrospect, after the legal judgement has been handed down. In particular, if any VoIP user has a legal right to privacy which could be violated by a stegodetection, then this would constitute a Call Pattern Tracking threat.

Interception and Modification threats are similar to eavesdroppings, with additional security concerns arising because the attacker can "modify the traffic as an intermediary in the

conversation."

Service Abuse is any "improper use of services." Regrettably, no definition of "improper" is provided in the taxonomy. Several of its subcategories (e.g. Improper Bypass or Adjustment to Billing) refer to fraudulent activities which may also be covered by the Theft of Services subcategory of Social Threat.

An Interruption threat is any violation, whether intentional or unintentional, of the normal expectation of continuous VoIP service. This part of the taxonomy is highly developed, but it is not relevant to steganography.

It is difficult to classify stegocommunication as a threat in the VOIPSA taxonomy. It could be considered either a Theft of Services (in the Social Threat category) or an Improper Bypass or Adjustment to Billing (in the Service Abuse category), if Alice and Bob use a stegochannel which wasn't properly billed to their (or their employer's) VoIP account. Such improper billing might occur in the second stegochannel scenario of Figure 1 in Lucena et al. [8], where Alice and Bob communicate by modifying messages which were sent, and which will ultimately be received, by other parties. However an improper billing is not a typical goal of steganography, so it seems inappropriate to classify stegocommunication as a threat to billing.

In the first stegochannel scenario of Lucena et al., Alice and Bob "hide secret information in some of their own harmless messages" by running "a modified version of the communicating software". This is the traditional model of steganography. The stegobandwidth available in an overt VoIP conversation between Alice and Bob was upper-bounded by Mazurczyk et al. [9]. This activity might be classified as Misrepresenting Content, if it is considered to be a social threat involving "the intentional presentation of false content as if it were true content with the intent to mislead."

Alternatively, as suggested by a referee, we might consider a stegocommunication threat to be an instance of "Other Improper Access to Services". Indeed, this category includes "Misconfiguration of end-points" so it seems appropriate at first. After some reflection, it seems dangerous to suppress any explicit mention of the stegocommuncation threat in the VOIPSA taxonomy. This omission may cause some business owners or governmental agencies to overlook the stegocommunication threat they face with any employee or agent who is contractually or legally obliged to maintain confidentiality constraints. Such individuals should not be allowed arbitrary access to stegochannels. Because a number of stegochannels are already known for VoIP, we were rather surprised to discover that the threat of stegocommunication was *not* already explicit in the VOIPSA taxonomy. Subsequently, we realised that standard taxonomies of network security also omit the threat of stegocommunication. It seems that stegocommunication is a stegothreat in most network security models: it exists, but is not overt!

III. Extension of Network Security Models

The fundamental threats in network security are commonly understood to be interruption, interception, modification, and fabrication. We have found this taxonomy in the 1995 edition of William Stallings' influential textbook [2], but we see no explicit claim to originality. We would welcome pointers to earlier sightings of this taxonomy in the published literature.

In his current edition [3], Stallings introduces a top-level distinction between active and passive threats, he renames some threats, and he subdivides several of the fundamental threats. The fundamental threat of interception has been subdivided into "release of message contents" and "traffic analysis." The fundamental threat of fabrication has been renamed "masquerade". The fundamental threat of modification is subdivided into "modification of message" and "replay"; the first form of modification also requires an interruption. The fundamental threat of interruption has been renamed "denial of service".

We find no mention of a stegocommunication threat in either edition of Stallings' textbook. Both editions adopt the OSI definition of a security attack as "any action that compromises the security of information owned by an organization." The omission of a stegocommunication threat only makes sense if we assume that the security and functionality goals of the communicating parties (Alice and Bob) are identical to the security and functionality goals of their organizations.

Stegocommunication is a fifth fundamental threat to network security. Any security analysis which omits this threat will miss some insider threats to confidentiality. The stegocommunication threat illustrated in part (f) of Figure 1 is distinct from the other four threats, as illustrated parts (b) through (e). The message flow during stegocommunication is almost the same as in the normal flow case part (a), except for the stegomessages which might be detected by an eavesdropping Oscar. The stegocommunication threat bears a superficial resemblance to the interception threat of part (c), except that the threat of interception is that Oscar might intercept, whereas the threat of stegocommunication is that Eve might *not* stegodetect. The situation in part (f) is reminiscent of a comic strip (http://xkcd.com/177) in which Eve argues that she should not be considered the attacker in an Alice-Bob-Eve scenario. Note that in the stegocommunication threat, Alice and Bob are adversaries of Charles, who owns the communication system they are misusing. In the other four threats, Oscar is an adversary of the system-owning Charles who isn't shown in the simplified threat diagrams.

The fundamental threat shown in part (f) is the second stegocommunication scenario of Lucena et al. [8], where Alice and Bob have no overt communication. If Alice and Bob have overt communication, as in the first (traditional) stegocommunication scenario, then we have a combination of normal flow (a) with stegocommunication (f).

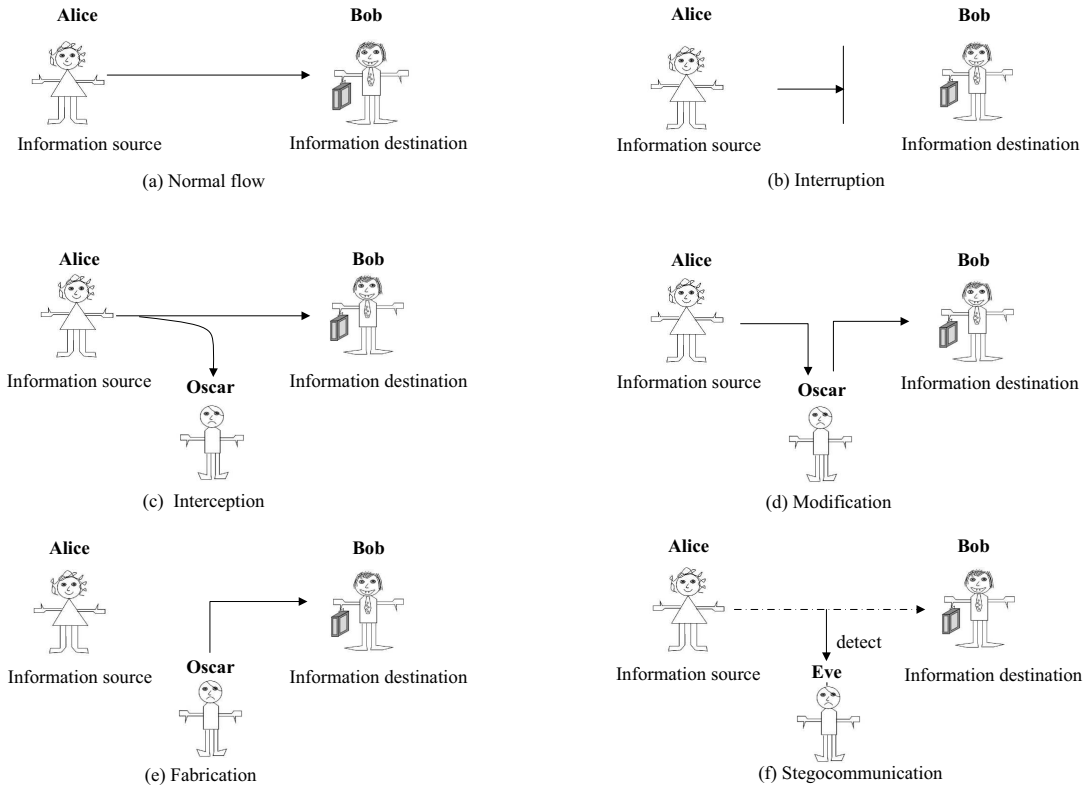

Fig. 1. Normal message flow, and five fundamental threats to this flow.

IV. A Stegocommunication Threat in a Business Scenario

One of the authors of this paper has recently proposed a general framework for security analysis [5]. In this section, we show how an analyst can use our framework to identify a stegocommunication threat in a business scenario.

The analyst's first step is to identify the principal human actors. In this case, the analyst observes that Charles is a business owner while Alice is one of his employees. Bob is someone adversarial, who isn't employed by Charles. The fourth actor Wendy is Charles' security manager. Wendy is the person conducting this security analysis. We note that it can be important to include a security analyst as a first-class actor in a security analysis. An unscrupulous analyst poses manifold threats to security, and some of these threats can be mitigated – for example by hiring an analyst whose current professional reputation is more valuable than what they could gain by subverting their current set of clients.

Wendy's next step is to identify the primary security and functionality goals of each human actor. In the framework,

1) security goals are determined by human fears, and
2) functionality goals are determined by human desires.

Generally a security analyst must work with incomplete information. In particular, external adversaries are rarely available for interview, and internal threat agents rarely reveal their motivations.

Our analyst Wendy has been hired by Charles, and she is analysing the system from Charles' point of view. She'll construct likely motivations for each actor, and these goals (along with her technical knowledge, and her professional experience as a security analyst) will form the basis of her threat assessment.

Wendy discovers, after talking to Charles, that he is somewhat mistrustful of Alice. She knows one of his business secrets. Her employment contract contains a confidentiality clause, but this doesn't seem a sufficient mitigation. Invoking this clause to fire Alice won't save Charles' business from bankruptcy, if Alice reveals his secret.

After writing down a (presumed) set of goals for each actor, Wendy can discover the threats and opportunities arising from this set of motivational assumptions. Generally a security threat arises when a functional goal of one actor is in conflict with a security goal of another actor. A security threat can be mitigated if a functional goal of one actor is aligned with a security goal of another actor. Wendy may make a functional analysis as well: a functional opportunity can be obtained when two actors' functional goals are congruent; and functional degradation may be difficult to avoid when two actors' functional goals are in conflict. The only other cases to consider are when the security goals of two actors

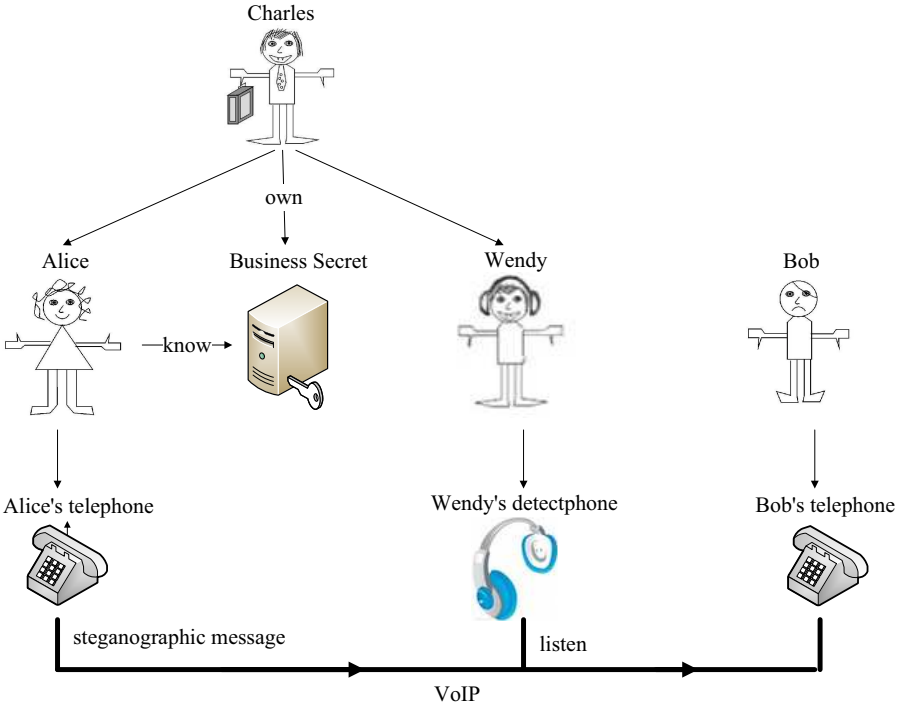

Fig. 2. A system with a stegocommunication threat.

are congruent or in conflict. In the former case, the two actors are natural allies and they may find it appropriate to work together against a common threat. In the latter case, the two actors are natural adversaries and are unlikely to find cooperate on security matters.

Wendy's threat analysis is sketched briefly below.

Alice

- Desire: Sell Charles' business secret to Bob, for financial advantage.
- Fear: Charles will learn that I'm negotiating with Bob, and I'll lose my job.

Bob

- Desire: Buy Charles' business secret from Alice, for financial advantage.
- Fear: Charles will overhear my negotiations with Alice, and then he'll tell other business owners about my unethical behaviour.

Charles

- Desire: Retain Alice as a productive employee, for financial advantage.
- Fear: Alice will sell a business secret to an outsider, and it will ruin my business.

Wendy

- Desire: Maintain information security for Charles, in part for financial advantage and also as a matter of professional pride.
- Fear: Some breach of Charles' security will occur, which may cost me my job and will make me feel I haven't met my professional obligations.

Wendy should realise that she is a natural ally of Charles, and that Alice is a natural ally of Bob. These alliances arise because the security goals of these pairs of actors are congruent. Wendy could increase the level of her congruence with Charles by focussing her rather generalised concern about security to align with Charles' current pre-occupation with a confidentiality risk. However, alliances are rarely total. Usually, an alliance is limited to a subset of a multi-objective goal or to a particular approach toward meeting a goal.

In the case of Alice's alliance with Bob, their mutual fear is of discovery. This fear can be mitigated if they meet in secret i.e. if they negotiate via stegocommunications. If they place sufficient trust in their stegotechnology, they can exploit their functional opportunity by negotiating a mutually-acceptable price for the revelation of Charles' business secret to Bob.

In the case of Wendy and Charles, their mutual fear is that Bob will learn Charles' business secret. This fear can be mitigated if they employ stegodetection on the communication channels available to Alice and Bob. Another approach would be to use a detectophone, i.e. to employ technology which allows Wendy to understand what is being said on a stegochannel. If Charles believes that it is a cost-effective mitigation, then he will include stegodetection or detectophony in Wendy's job description – thereby making it a new functional goal for Wendy.

V. Conclusion and future work

We claim three contributions in this paper. First of all, we noted the absence of a stegocommunication threat in the VOIPSA taxonomy, and we proposed that it be added to the Service Abuse category. We argue that an explicit mention of this threat is important, because stegochannels are known for VoIP and confidentiality breaches are important to some organisations.

Secondly, we noted the absence of a stegocommunication threat in both the 1995 and 2007 edition of Stallings' influential textbook on network security. We analysed Stallings' definition of attack, noting that it included confidentiality breaches. We noted that he didn't explicitly consider any insider threats, and we pointed out that a stegocommunication threat can be illustrated in the same fashion as his other four fundamental threats to network security.

Thirdly, we discussed the stegocommunication threat in the context of simple business scenario, where an employee is in possession of a business secret. The analysis in this section was conducted a security framework that relates security requirements to human fears and functional requirements to human desires. Motivational conflicts give rise to functional faults or security threats; and motivational congruences point toward functional opportunities and security alliances.

In our analysis of Section 4, the communicating party Alice was in an inferior power relationship to her employer Bob. There are three other fundamental forms of control, as noted by Lessig [4]: Alice may be a peer in an economic marketplace that sells the communication service she is using; Alice may be subject to judicial penalty if she abuses a communication service; and Alice may lose social standing in her peer group if she uses a communication service in a way that her group deems improper. Alice's controller (i.e. her peer group or government) may face a steganographic threat in any of these situations. We leave it to the reader or future analysts to consider Alice's functional motivations for employing stegocommunication, the relevant fears of her controller, and how the resulting threat might be mitigated in specific scenarios.

We have found that stegocommunication is a fifth fundamental threat (after interception, interruption, fabrication, and modification) to network security in a model where Alice and Bob communicate on a system that is owned by a third party Charles whose security goals may, or may not, coincide with those of Alice and Bob. We leave it as an open question whether we now have a complete list of threats, or whether there is a sixth fundamental threat in this model.

Acknowledgment

We would like to thank Changjiang Zhang for stimulating discussions. This work is supported by the National Basic Research Program of China (No. 2007CB310802) and the National Natural Science Foundation of China (No. 90718010).

References

[1] Threat Taxonomy Working Group of VOIPSA, "VoIP security and privacy threat taxonomy," Public Release 1.0, 24 October 2005.

[2] W. Stallings, *Network and Internetwork Security Principles and Practice*. New Jersey, USA: Prentice Hall, 1995.

[3] W. Stallings, *Network Security Essentials: Applications and Standards*. New Jersey, USA: Prentice Hall, 2007.

[4] L. Lessig, *Code version 2.0*. Basic Books, 2006.

[5] C. Thomborson, "A framework for system security," in *Handbook of Computer and Information Security* (M. Stamp, ed.), Springer, 2009.

[6] L. Wenar, "Rights," in *The Stanford Encyclopedia of Philosophy* (E. N. Zalta, ed.), 2008.

[7] S. Chen, X. Wang, and S. Jajodia, "On the anonymity and traceability of peer-to-peer voip calls," *IEEE Network*, September/October 2006.

[8] N. B. Lucena, J. Pease, P. Yadollahpour, and S. J. Chapin, "Syntax and semantics-preserving application-layer protocol steganography," in *Information Hiding* (J. J. Fridrich, ed.), vol. 3200 of *Lecture Notes in Computer Science*, pp. 164–179, Springer, 2004.

[9] W. Mazurczyk and K. Szczypiorski, "Steganography of voip streams," in *OTM Conferences (2)* (R. Meersman and Z. Tari, eds.), vol. 5332 of *Lecture Notes in Computer Science*, pp. 1001–1018, Springer, 2008.