Journal of Zhejiang University SCIENCE A
ISSN 1673-565X (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

Integrated criteria for covert channel auditing*

Chang-da WANG†[1,2], Shi-guang JU[1]

([1]*School of Computer Science and Telecommunications Engineering, Jiangsu University, Zhenjiang 212013, China*)

([2]*School of Computer Science, Carleton University, Ottawa, Ontario K1S 5B6, Canada*)

†E-mail: changda@ujs.edu.cn

Received Sept. 24, 2007; revision accepted Mar. 7, 2008

Abstract: A new concept, the security level difference of a covert channel, is presented, which means the security level span from the sender to the receiver of the covert channel. Based on this, the integrated criteria for covert channel auditing are given. Whereas TCSEC (Trusted Computer System Evaluation Criteria) or CC (Common Criteria for Information Technology Security Evaluation) only use the bandwidth to evaluate the threat of covert channels, our new criteria integrate the security level difference, the bandwidth sensitive parameter, bandwidth, duration and instantaneous time of covert channels, so as to give a comprehensive evaluation of the threat of covert channels in a multilevel security system.

Key words: Multilevel security, Covert channel, Covert channel auditing
doi:10.1631/jzus.A071510 **Document code:** A **CLC number:** TP309.2

INTRODUCTION

The Bell-LaPadula model prevents the direct flow of information from a higher access class to a lower access class, but the conditions are not sufficient to ensure that security is not violated indirectly through what are known as covert channels (Lampson, 1973). A covert channel allows the indirect transfer of information from a subject at a higher access class to a subject at a lower or incompatible access class (Son *et al.*, 2000). A typical example of covert channels is presented as follows. Process *p* is to be confined such that it cannot communicate with process *q*. However, processes *p* and *q* share a file system. In order for process *p* to send a message to process *q*, it creates a file called send in a directory that both processes can read. Just before process *q* is to read the information, *q* deletes the send file. Process *p* then transmits a bit by creating a file named 0 bit or 1 bit, as appropriate. When *q* detects either file, it records the bit and deletes the file. This continues until *p* creates a file called end, at which point the communication ceases (Matt, 2003).

Covert channels present a serious risk to data security in computer systems and networks. These channels are an illicit means of leaking sensitive or private information through global system variables that usually are not part of the interpretation of data objects in the security model (Huskamp, 1978). Covert channels can be classified into two types, i.e., storage channels and timing channels (Lipner, 1975). Although fundamentally the same, storage channels and timing channels differ in the way that information is encoded. In a storage channel, there is a shared global variable in the system that acts as the medium for information transfer, where a user can potentially change its value by invoking a TCB (trusted computing base) primitive, and another user can potentially view the change directly or indirectly. A timing channel requires the ability of cooperativeness to reference a real-time clock so that the receiver can detect a timing difference that can be used as the basis for encoding data for information transfer (Shieh, 1999).

Not only are covert channels in a single host (Liu *et al.*, 2007; Qing and Shen, 2007), but also in net-

* Project supported by the National Natural Science Foundation of China (No. 60773049), the Natural Science Foundation of Jiangsu Province (No. BK2007086), the Fundamental Research Project of the Natural Science in Colleges of Jiangsu Province (No. 07KJB520016), and the Person with Ability Project of Jiangsu University (No. 07JDG053), China

works and application protocols (Murdoch and Lewis, 2006; Zander *et al.*, 2007a). Moreover, stereographic techniques and subliminal channels in cryptosystems are also related research areas (Beauquier and Lanotte, 2007; Wang *et al*., 2007). Actually, covert channels have been noted in various security related areas since 1973. Readers are encouraged to read more references to learn of the latest progress.

It should be emphasized that often even ordinary employees may want to use covert channels to bypass their company firewalls in order to access Internet resources (Zander *et al.*, 2007b). Even if only one bit per packet can be covertly transmitted, a large Internet site could lose 26 GB of data annually (Fisk *et al.*, 2002). From this point of view, the threats of covert channels are real and critical. The National Computer Security Center (NCSC) developed requirements for the information rate estimation of covert channels in multilevel secure systems at level B2 or above in 1983 (DoD STD-5200.28, 1985; Millen, 1999). Since 1999, CC (Common Criteria for Information Technology Security Evaluation) has instructed that covert channel analysis must be conducted at level EAL5 (AVA_CCA.1), EAL6 (AVA_CCA.2) and EAL7 (AVA_CCA.3) (ISO CCIMB-99-033, 1999).

Unfortunately, during the past three decades since the covert channel was first presented, most researchers have paid more attention to detection and mitigation methods for covert channels. A few known works about auditing were limited in scope to how one calculates the bandwidth/capacity of covert channels (Tsai and Gligor, 1988; Jajodia and Kogan, 1990; Costich and Moskowitz, 1991; Millen, 1993; Venkatraman and Newman-Wolfe, 1995; Simmons, 1998; Shieh, 1999; Wang *et al.*, 2003; Wang and Ju, 2004). Nobody has challenged yet the audit criteria of TCSEC (Trusted Computer System Evaluation Criteria) or CC (Common Criteria for Information Technology Security Evaluation) relating to covert channels. Recently, in further research concerning covert channel auditing, we have observed some deficiencies in these criteria.

The outline of this paper is as follows. Section 2 uses two cases to illustrate the vulnerabilities of TCSEC audit criteria, i.e., it is inadequate to only use bandwidth to evaluate the threat of covert channels. In Section 3, the formal definition of the security level difference of a covert channel is given. Section 4 presents two new concepts, i.e., the threat degree and threat rate of covert channels. The new criteria, Integrated Criteria, are presented in Section 5 for covert channel auditing. Finally, our conclusions are discussed in Section 6.

VULNERABILITY OF CURRENT AUDIT CRITERIA

Compared with TCSEC, CC only requires an estimation of the bandwidth of covert channels, but provides a threshold, i.e., a bandwidth under 1 bit/s is acceptable, between 1 bit/s and 100 bits/s it will depend on specific situations, and beyond 100 bits/s it is denied (ISO CCIMB-99-033, 1999). It is hard to think of 100 bits/s as high today, now that we know that there are hardware-based channels, for example bus contention channels, of thousands of bits per second, which are nearly unavoidable. On the other hand, the most valuable information is probably your 512-bit encryption key. How long is that going to be kept secret even at one bit per second (Millen, 1999)?

Only using bandwidth as the criteria for auditing covert channels is not enough. Let us read the following cases:

In a multilevel security system, assume that in the same compartment the sensitivity levels are set as {*Unclassified*, *Restricted*, *Confidential*, *Secret*, *Top Secret*}. The partial order relationship '<' on this set can be described as *Unclassified*<*Restricted*<*Confidential*<*Secret*<*Top Secret*. Under such circumstances, if there are two covert channels, cc_1 and cc_2, and both bandwidths are 200 bits/s, then the threat from them would be considered as equal according to TCSEC and CC. If cc_1 leaks sensitive information from *Top Secret* to *Unclassified* while cc_2 only leaks sensitive information from *Top Secret* to *Secret*, does this mean that the threat from cc_1 is really equal to the threat from cc_2? The allied case is that cc_1 only worked 1 s while cc_2 worked 30 min, so how do we evaluate the threat from them?

This paper will clarify these confusions by presenting integrated criteria for covert channel auditing. Actually, we should consider not only bandwidth, but also the security level difference (refer to Section 3), bandwidth sensitive parameters (refer to Section 4), the security level of the sender, the duration and/or instantaneous time of the covert channel, when evaluating the threat from covert channels.

SECURITY LEVEL DIFFERENCE OF COVERT CHANNEL

Definition 1 (Security level) Security level $\mathcal{L}$ is the combination of a hierarchical classification $\mathcal{C}$ and a set of non-hierarchical categories $\mathcal{K}$ that represent the sensitivity of information, i.e., $\mathcal{L}=\{(C,K)|C\in\mathcal{C}\wedge K\in\mathcal{K}\}$. The security level of entity X is denoted by $L(X)$.

$\mathcal{C}$ is a set of sensitivity levels, e.g., *Unclassified*, *Restricted*, *Confidential*, *Secret*, *Top Secret*, etc. There is a partial order relationship '<' in hierarchical classification $\mathcal{C}$, i.e., *Unclassified*<*Restricted*<*Confidential*<*Secret*<*Top Secret*. On the other hand, no obvious partial order relationships can be found in non-hierarchical categories $\mathcal{K}$ whose members are compartments, e.g., Compartment *A*, Compartment *B*, Compartment *C*, etc. Fig.1 demonstrates the structure of the security level.

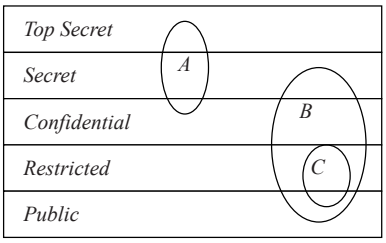

Fig.1 Structure of the security level

Definition 2 (Relationships between security levels)

(1) Equal '='

$\forall L_1=(C_1, K_1)\in\mathcal{L}$, $\forall L_2=(C_2, K_2)\in\mathcal{L}$, $L_1=L_2$ iff $C_1=C_2\wedge K_1=K_2$.

(2) Dominative '>'

$\forall L_1=(C_1, K_1)\in\mathcal{L}$, $\forall L_2=(C_2, K_2)\in\mathcal{L}$, if $C_1>C_2\wedge K_1\supseteq K_2$ then $L_1>L_2$.

(3) Incompatible '<>'

$\forall L_1=(C_1, K_1)\in\mathcal{L}$, $\forall L_2=(C_2, K_2)\in\mathcal{L}$, if $K_1\not\subset K_2\wedge K_2\not\subset K_1$ then $L_1<>L_2$.

Convention 1 $\mathcal{S}$ is the set of subjects. $\mathcal{O}$ is the set of objects. *CC* is a set consisting of all covert channels in a given multilevel security system.

Convention 2 $\forall cc\in CC$, *head*(*cc*) and *rear*(*cc*) are sender and receiver subjects of *cc*, respectively.

Definition 3 Class(*X*) is a function defined in hierarchical classification set $\mathcal{C}$. All sensitivity levels sort from the lowest to highest and will map $\mathcal{C}$ into a series $\{a_i\}$, $1\le i\le n$. $\forall X\in\mathcal{S}\cup\mathcal{O}$, if the sensitivity level of *X* is mapped to *i*, then *Class*(*X*)=*i*.

Since covert channels are used for the leakage of sensitive information violating security policies (information can only flow from lower to higher security levels), that is to say, through covert channels information can flow from a high security level to a lower one or between incompatible security levels, so the sender's security level should dominate or be incompatible with the receiver's security level.

Definition 4 (Security level difference U_{cc}) $\forall cc\in CC$, $L(head(cc))=\{(C_1, K_1)|C_1\in\mathcal{C}\wedge K_1\in\mathcal{K}\}$, $L(rear(cc))=\{(C_2, K_2)|C_2\in\mathcal{C}\wedge K_2\in\mathcal{K}\}$,

(1) if $L(head(cc))>L(rear(cc))$,

$$U_{cc}=\begin{cases}|Class(C_1)-Class(C_2)|, & K_1=K_2,\\ |Class(C_1)-Class(C_2)|+1, & K_1\supset K_2.\end{cases}$$

(2) if $L(head(cc))<>L(rear(cc))$,

$$U_{cc}=|Class(C_1)-Class(C_2)|+2.$$

Corollary 1 $U_{cc}\ge 1$ and $U_{cc}\in\mathbb{N}$.

Intuitionally we knew that sensitive information leaks from *Top Secret* to *Secret* do less harm than from *Top Secret* to *Public*. The significance of the security level difference lies in providing a measurement for the security level span from the sender to the receiver of the covert channel. Unfortunately, no linear order relationships exist among security levels due to non-hierarchical categories. Contrast to the definition of *Class*(*X*) for hierarchical classification set $\mathcal{C}$, in Definition 4, we enumerate all possible scenarios for non-hierarchical categories $\mathcal{K}$ of covert channels, i.e.,

$$U_{cc}=\begin{cases}|Class(C_1)-Class(C_2)|, & K_1=K_2,\\ |Class(C_1)-Class(C_2)|+1, & K_1\supset K_2,\\ |Class(C_1)-Class(C_2)|+2, & K_1\not\subset K_2\wedge K_2\not\subset K_1,\end{cases}$$

where $K_1, K_2\in\mathcal{K}$; $C_1, C_2\in\mathcal{C}$.

We postulate that a sensitive information leak within the same department is of less threat than that between different departments, so 0, 1 and 2 were selected in connection with $|Class(C_1)-Class(C_2)|$ to make U_{cc} in three scenarios, respectively. Actually 0, 1 and 2 can be substituted by other fine-grain numbers according to concrete situations. So each covert channel has a U_{cc} to evaluate the security level span

from the sender to the receiver. A greater U_{cc} means a larger span.

Corollary 2 The threat from a covert channel and its security level difference are in direct proportion.

THREAT DEGREE AND THREAT RATE OF COVERT CHANNEL

Definition 5 (Threat degree) $\forall cc\in CC$, U_{cc} and I_{cc} denote the security level difference and bandwidth of cc, respectively.

$$W(U_{cc}, I_{cc}, \Delta t)=U_{cc}^{\alpha} I_{cc}\Delta t\ , \tag{1}$$

where W is the threat degree of cc in duration $[t_1, t_2]$, $\Delta t=t_2-t_1$. $\alpha\in[0, +\infty)$ is a constant. α is a bandwidth sensitive parameter, which will be discussed later within this section.

Generally, U_{cc} is a constant for a given $cc\in CC$, whereas I_{cc} is a variable usually, i.e., I_{cc} is the function of time t, so I_{cc} is denoted as $I_{cc}(t)$ also. That is to say, Eq.(1) can be revised as

$$W(U_{cc}, I_{cc}, \Delta t)=U_{cc}^{\alpha} I_{cc}(t)\Delta t. \tag{1′}$$

Definition 6 (Threat rate) $\forall cc\in CC$,

$$WP(U_{cc}, I_{cc})=U_{cc}^{\alpha} I_{cc}(t_0), \tag{2}$$

where WP is the threat rate of cc in an instantaneous time t_0, and $\alpha\in[0, +\infty)$ is a constant.

Threat degree is a guideline to audit covert channels in duration $[t_1, t_2]$ while threat rate is a guideline to audit covert channels in an instantaneous time t_0. According to Definitions 5 and 6, the relationship between W and WP can be presented as follows:

$$\lim_{\Delta t\to 0}\frac{W}{\Delta t}=WP. \tag{3}$$

Bandwidth sensitive parameter α

Generally, security level difference and bandwidth do not have the same importance in covert channel auditing. Sometimes the security level difference is more sensitive than bandwidth, and sometimes quite the reverse. So $\alpha\in[0, +\infty)$ in Definitions 5 and 6 provide an option when determining which one is worthy of more attention while auditing, viz. the security level difference, the bandwidth, or both.

Assume $\alpha=1$ can be looked at as an example of the security level difference and bandwidth being treated equally in the definitions of threat degree and threat rate. According to Corollary 1, we know that $U_{cc}\geq 1$ and $U_{cc}\in\mathbb{N}$, so if α was selected as $\alpha>1$, then the impact of U_{cc} would be amplified in W or WP, whereas if $0\leq\alpha<1$, the impact of U_{cc} would be reduced. From this point of view, if the impact of the security level difference was amplified, the impact of bandwidth can be looked at as having dwindled in the final result, or vice versa. Details can be found in the appendix to this paper.

Calculation of threat degree

For a given instantaneous time t_0, WP can be derived from Definition 6 directly, whereas W cannot be calculated from Definition 5 unless I_{cc} is a constant in $[t_1, t_2]$. Actually, I_{cc} is the function of time usually, i.e., $I_{cc}(t)$. In this kind of situation, the duration $[t_1, t_2]$ can be sliced into some tiny units Δ_i, $i=1, 2, \ldots, n$. Thus in each Δ_i, $I_{cc}(t)$ can be looked at as approximately a constant. Assume that Δt_i denotes the length of Δ_i, i.e., if $\Delta_i=[t_{i-1}, t_i]$, then $\Delta t_i=t_i-t_{i-1}$, $\|\Delta t_i\|=\max_{1\leq i\leq n}\{\Delta t_i\}$. So the increment of W in Δt_i can be denoted as

$$\Delta W_{cci}\approx U_{cc}^{\alpha} I_{cc}(\xi_i)\Delta t_i,\quad \xi_i\in\Delta_i,\ cc\in CC.$$

For $W_{cc}=\sum_{i=1}^{n}\Delta W_{cci}$,

$$W_{cc}=\lim_{\|\Delta t_i\|\to 0}\sum_{i=1}^{n} U_{cc}^{\alpha} I_{cc}(\xi_i)\Delta t_i$$

can be concluded. Furthermore, for a given α and a certain covert channel $cc\in CC$, U_{cc}^{α} is constant, thus

$$W_{cc}=U_{cc}^{\alpha}\lim_{\|\Delta t_i\|\to 0}\sum_{i=1}^{n} I_{cc}(\xi_i)\Delta t_i,$$

$$\text{viz.}\quad W_{cc}=U_{cc}^{\alpha}\int_{t_1}^{t_2} I_{cc}(t)\mathrm{d}t. \tag{4}$$

If $I_{cc}(t)$ is a constant in $[t_1, t_2]$, viz. I_{cc}, then

$$W_{cc}=U_{cc}^{\alpha}\int_{t_1}^{t_2} I_{cc}(t)\mathrm{d}t=U_{cc}^{\alpha} I_{cc}\int_{t_1}^{t_2}\mathrm{d}t=U_{cc}^{\alpha} I_{cc}(t_2-t_1).$$

This is the definition of W_{cc} in Definition 5, so we can substitute Eq.(4) for Eq.(1′) in Definition 5.

Definition 5′ (Threat degree) $\forall cc\in CC$, U_{cc} and I_{cc} denote the security level difference and bandwidth of cc, respectively.

$$W(U_{cc}, I_{cc}, \Delta t) := U_{cc}^{\alpha}\int_{t_1}^{t_2} I_{cc}(t)\mathrm{d}t,$$

where W is the threat degree of cc in duration $[t_1, t_2]$, $\Delta t=t_2-t_1\geq 0$, and $\alpha\in[0, +\infty)$ is a constant.

Whether $I_{cc}(t)$ is a constant or variable of t, the physical meaning of $\int_{t_1}^{t_2} I_{cc}(t)\mathrm{d}t$ is all the bits that were transmitted by cc in duration $[t_1, t_2]$.

INTEGRATED CRITERIA FOR COVERT CHANNEL AUDITING

$\forall cc_1, cc_2\in CC$,

1. In duration $[t_1, t_2]$, the duple $(W_{cc}, SL(head(cc)))$ is used to evaluate the threat of cc_1 and cc_2. If the threat of cc_1 is greater than that of cc_2 asserted, at least one of the following conditions must be fulfilled:

(1) $W_{cc_1} > W_{cc_2}$;

(2) $W_{cc_1} = W_{cc_2}$, $SL(head(cc_1))>SL(head(cc_2))$.

2. In instantaneous time t_0, the duple $(WP_{cc}, SL(head(cc)))$ is used to evaluate the threat of cc_1 and cc_2. If the threat of cc_1 is greater than that of cc_2 asserted, at least one of the following conditions must be fulfilled:

(1) $WP_{cc_1} > WP_{cc_2}$;

(2) $WP_{cc_1} = WP_{cc_2}$, $SL(head(cc_1))>SL(head(cc_2))$.

$SL(head(cc))$, the sender's security level of cc, is the second weight parameter for evaluating the threat of covert channels. It means that if W or WP of different covert channels are equal respectively, then $SL(head(cc))$ is active. The higher $SL(head(cc))$ is, the more sensitive the leaked information is, i.e., the threat brought by covert channels to system security is more serious.

By the integrated criteria, bandwidth is the critical parameter when auditing covert channels, and also when the security level differences, duration and/or instantaneous time of the covert channel are equal, respectively. This is consistent with the traditional pure bandwidth criteria for covert channel auditing.

When bandwidths of different covert channels are equal, the traditional pure bandwidth criteria cannot distinguish the difference in threat between them, whereas the integrated criteria mentioned above can.

Example 1 $\forall cc_1, cc_2\in CC$, suppose that both security level differences for them are 3; cc_1 and cc_2 have the same bandwidth function $I_{cc}(t)$; the duration of cc_1 and cc_2 is $[t_1, t_2]$ and $[t_1, t_3]$, respectively.

Assume the security level difference and bandwidth are treated equally in this instance, i.e., $\alpha=1$, thus,

$$W_{cc_1} = U_{cc_1}\int_{t_1}^{t_2} I_{cc_1}(t)\mathrm{d}t = 3\int_{t_1}^{t_2} I_{cc}(t)\mathrm{d}t,$$

$$W_{cc_2} = U_{cc_2}\int_{t_1}^{t_3} I_{cc_2}(t)\mathrm{d}t = 3\int_{t_1}^{t_3} I_{cc}(t)\mathrm{d}t.$$

$I_{cc}(t)$ is the bandwidth function of cc_1 and cc_2, so $I_{cc}(t)\geq 0$. Thus if $[t_1, t_2]\supset[t_1, t_3]$, then $W_{cc_1}\geq W_{cc_2}$ can be concluded, viz. the threat of cc_1 is not less than that of cc_2. If $[t_1, t_2]=[t_1, t_3]$, i.e., $\int_{t_1}^{t_2} I_{cc}(t)\mathrm{d}t = \int_{t_1}^{t_3} I_{cc}(t)\mathrm{d}t$, then $W_{cc_1} = W_{cc_2}$. So $head(cc_1)$ and $head(cc_2)$ need to be known. If $SL(head(cc_1))=5$ and $SL(head(cc_2))=4$, then $SL(rear(cc_1))=2$ and $SL(rear(cc_2))=1$ can be inferred according to Definition 4. So we know that $W_{cc_1} = W_{cc_2}$ in connection with $SL(head(cc_1))>SL(head(cc_2))$, viz. it can be concluded according to the integrated criteria that the threat of cc_1 is higher than that of cc_2.

This example illustrates the integrated criteria while auditing covert channels of a certain duration. In instantaneous time, the outcome is similar.

Example 2 $\forall cc_1, cc_2\in CC$, assume the security level differences of cc_1 and cc_2 are 2 and 3, respectively; bandwidths of cc_1 and cc_2 are 150 and 110 bits/s, respectively; the duration of both cc_1 and cc_2 is $[t_1, t_2]$, $t_2>t_1$.

Case 1: Assume the security level difference and bandwidth are treated equally in this example, i.e., set $\alpha=1$, then W_{cc_1} and W_{cc_2} can be calculated as follows:

$$W_{cc_1} = U_{cc_1}\int_{t_1}^{t_2} I_{cc_1}(t)\mathrm{d}t = 2\int_{t_1}^{t_2} 150\mathrm{d}t = 300(t_2 - t_1),$$

$$W_{cc_2} = U_{cc_2}\int_{t_1}^{t_3} I_{cc_2}(t)\mathrm{d}t = 3\int_{t_1}^{t_2} 110\mathrm{d}t = 330(t_2 - t_1).$$

For $t_2-t_1>0$, we have $W_{cc_1} < W_{cc_2}$, i.e., the threat of cc_2 is higher than that of cc_1 according to the integrated criteria.

Case 2: Assume cc_1, $cc_2 \in CC$ are in a bandwidth sensitive system, e.g., let $\alpha=1/2$, then

$$W_{cc_1} = U_{cc_1}^{\alpha}\int_{t_1}^{t_2} I_{cc_1}(t)\mathrm{d}t = \sqrt{2}\int_{t_1}^{t_2} 150\mathrm{d}t \approx 212(t_2 - t_1),$$

$$W_{cc_2} = U_{cc_2}^{\alpha}\int_{t_1}^{t_3} I_{cc_2}(t)\mathrm{d}t = \sqrt{3}\int_{t_1}^{t_2} 110\mathrm{d}t \approx 191(t_2 - t_1).$$

For $t_2-t_1>0$, we have $W_{cc_1} > W_{cc_2}$, i.e., in such circumstances, the threat of cc_1 is higher than that of cc_2 according to the integrated criteria.

DISCUSSION AND CONCLUSION

The traditional criteria for covert channel auditing only use bandwidth as a parameter (DoD STD-5200.28, 1985; ISO CCIMB-99-033, 1999). These criteria neglect many factors, such as the security level difference, the bandwidth sensitive parameter, the security level of the sender, the duration and instantaneous time of covert channels, etc., which can also determine the threat of covert channels. So they cannot give a comprehensive evaluation of the threat of covert channels. Whereas the new criteria—the integrated criteria—for covert channel auditing integrate all of the factors mentioned above to audit covert channels. Moreover, it can also be compatible with the former pure bandwidth criteria for auditing covert channels. If all of the other factors are the same for the integrated criteria, the bandwidth is also the critical parameter for covert channel auditing. Actually, *WP* will degrade to pure bandwidth criteria if α is set to 0, i.e., pure bandwidth criteria can be looked at as a special example of the integrated criteria.

The integrated criteria not only distinguish the concept of threat degree and threat rate, but also provide their computation methods, so the audit of covert channels can cover either the duration or the instantaneous time. The integrated criteria are the most comprehensive ones for covert channel auditing up until now.

In closing this paper it is worth mentioning another significant point of view in covering covert channel auditing, namely that the bandwidth of the covert channel is only the bandwidth of the communication between the sender and the receiver, that is to say, this bandwidth is not the real bandwidth of effective sensitive information leakage. In fact, to ensure the reliability of communication through covert channels, the users of covert channels, e.g., the Trojan programs, use special protocols in such communications. Since some bits must be consumed in the synchronization of the communication, the effective bandwidth for sensitive information leakage is less than the bandwidth of covert channels. This important fact had been ignored since covert channels were first presented.

Generally, different protocols can generate different effective bandwidths on the same covert channel. If there are no protocols for the communication through covert channels, our experiments in (Wang and Ju, 2006) show that covert channels are almost good for nothing because they cannot transfer classified files exactly, even in a noiseless environment. One of the most interesting characteristics of communication protocols for covert channels lies in the fact that some synchronization bits must occupy part of the bandwidth of covert channels, and some of them need not. This is because in most security models, e.g., the Bell & LaPadula model, the information flows from a low security level to a higher level to be acceptable, whereas in the reverse direction or to an incompatible security level this is prohibited, except that transferred by TCB primitives. So only the synchronization bits from a high security level to a lower one or to an incompatible level need to occupy part of the bandwidth of covert channels, whereas the synchronization bits flowing from a lower to a higher security level do not.

ACKNOWLEDGEMENT

We would like to thank Professor Evangelos Kranakis and Professor Michel Barbeau, who are the members of the Digital Security Group of Carleton University, Ottawa, Canada, for providing their useful comments on this paper.

References

Beauquier, D., Lanotte, R., 2007. Hiding information in multi level security systems. *LNCS*, **4691**:250-269. [doi:10.1007/978-3-540-75227-1_17]

Costich, O., Moskowitz, I., 1991. Analysis of a Storage Channel in the Two Phase Commit Protocol. Proc. Computer Security Foundations Workshop IV, p.201-208. [doi:10.1109/CSFW.1991.151587]

DoD STD-5200.28, 1985. Trusted Computer System Evaluation Criteria. National Computer Security Center, USA.

Fisk, G., Fisk, M., Papadopoulos, C., Neil, J., 2002. Eliminating steganography in Internet traffic with active wardens. *LNCS*, **2578**:18-35. [doi:10.1007/3-540-36415-3_2]

Huskamp, J.C., 1978. Covert Communication Channels in Timesharing Systems. Technical Report UCB-CS-78-02.

ISO CCIMB-99-033, 1999. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance, Requirements. Version 2.1.

Jajodia, S., Kogan, B., 1990. Transaction Processing in Multilevel-Secure Databases using Replicated Architecture. Proc. Symp. on Research in Security and Privacy, p.360-368. [doi:10.1109/RISP.1990.63864]

Lampson, B.W., 1973. A note on the confinement problem. *Commun. ACM*, **16**(10):613-615. [doi:10.1145/362375.362389]

Lipner, S.B., 1975. A comment on the confinement problem. *ACM SIGOPS Oper. Syst. Rev.*, **9**(5):192-196. [doi:10.1145/1067629.806537]

Liu, W.Q., Han, N.P., Chen, Z., 2007. Identifying and dealing with covert channel of the secure OS-SLinux. *J. Electr.*, **35**(1):153-156 (in Chinese).

Matt, B., 2003. Computer Security: Art and Science. Pearson Education, Inc.

Millen, J., 1993. Covert Channel Capacity. Proc. IEEE Symp. on Research in Security and Privacy, p.60-65. [doi:10.1109/SP.1987.10013]

Millen, J., 1999. 20 Years of Covert Channel Modeling and Analysis. Proc. IEEE Symp. on Security and Privacy, p.113-114. [doi:10.1109/SECPRI.1999.766906]

Murdoch, S.J., Lewis, S., 2006. Embedding covert channels into TCP/IP. *LNCS*, **3727**:247-261. [doi:10.1007/11558859_19]

Qing, S.H., Shen, C.X., 2007. Design of secure operating systems with high security levels. *Sci. China Ser. F–Inf. Sci.*, **50**(3):399-418. [doi:10.1007/s11432-007-0028-3]

Shieh, S.P., 1999. Estimating and measuring covert channel bandwidth in multilevel secure operating systems. *J. Inf. Sci. Eng.*, **15**:91-106.

Simmons, G.J., 1998. Results concerning the bandwidth of subliminal channels. *IEEE J. Sel. Areas Commun.*, **16**(4):463-473. [doi:10.1109/49.668970]

Son, S.H., Mukkamala, R., David, R., 2000. Integrating security and real-time requirements using covert channel capacity. *IEEE Trans. on Knowl. Data Eng.*, **12**(6):865-879. [doi:10.1109/69.895799]

Tsai, C.R., Gligor, V.D., 1988. A Bandwidth Computation Model for Covert Storage Channels and Its Applications. Proc. IEEE Symp. on Security and Privacy, p.108-121. [doi:10.1109/SECPRI.1988.8103]

Venkatraman, B.R., Newman-Wolfe, R.E., 1995. Capacity Estimation and Auditability of Network Covert Channels. Proc. IEEE Symp. on Security and Privacy, p.186-198. [doi:10.1109/SECPRI.1995.398932]

Wang, C.D., Ju, S.G., 2004. Searching Covert Channels by Identifying Malicious Subjects in the Time Domain. Proc. 5th IEEE Information Assurance Workshop, p.68-73. [doi:10.1109/IAW.2004.1437799]

Wang, C.D., Ju, S.G., 2006. Simulation analysis of covert channels. *J. Syst. Simul.*, **18**(6):1488-1492 (in Chinese).

Wang, C.D., Ju, S.G., Guo, D.C., Yang, Z., Zheng, W.Y., 2003. Research on the methods of search and elimination in covert channels. *LNCS*, **3032**:988-991. [doi:10.1007/b97162]

Wang, Z.H., Deng, J., Lee, R.B., 2007. Mutual Anonymous Communications: A New Covert Channel Based on Splitting Tree MAC. Proc. 26th IEEE INFOCOM, p.2531-2535. [doi:10.1109/INFCOM.2007.315]

Zander, S., Armitage, G., Branch, P., 2007a. An Empirical Evaluation of IP Time to Live Covert Channels. Proc. 15th IEEE Int. Conf. on Networks, p.42-47. [doi:10.1109/ICON.2007.4444059]

Zander, S., Armitage, G., Branch, P., 2007b. A survey of covert channels and countermeasures in computer network protocols. *IEEE Commun. Surv. Tutor.*, **9**(3):44-57. [doi:10.1109/COMST.2007.4317620]

APPENDIX

Generally, in a multilevel security system, if the sizes of classified files are relatively small for the bandwidth, then this system is a bandwidth sensitive one, and then the bandwidth sensitive parameter α should be selected in [0, 1); otherwise α should be selected from [1, +∞). We do not give a clear standard here for what is "bandwidth sensitive", which is beyond the research interests of this paper. Intuitively, if the minimum size of classified files is 100 M and the bandwidth of the covert channel is only 100 bits/s, then we can say this multilevel security system is not a bandwidth sensitive one. We recommend that the value of α be determined by the covert channels' auditors according to their situations.

For $y=x^{\alpha}$, if $x_1>x_2\geq 1$, we know that

$$\begin{cases} x_1^{\alpha} \geq x_2^{\alpha}, & \alpha \geq 0, \\ x_1^{\alpha} < x_2^{\alpha}, & \alpha < 0. \end{cases}$$

Corollary 2 tells us that the threat from a covert channel and its security level difference are in direct proportion, so if α can be selected as $\alpha<0$, then the threat from a covert channel and its security level difference are in inverse proportion, which causes a contradiction. So the domain of α is [0, +∞) in the definitions of threat degree and threat rate.