基于最小熵的完整性度量

彭朝英,席政军
(陕西师范大学计算机科学学院,陕西西安 710062)

摘 要: 在实际计算机系统中可信信息不可避免地会被更改,因此有必要定量刻画信息的完整性,目的在于度量有多少的更改是可容忍的. 本文针对攻击者能够一次最大可能更改可信信息的情况,结合信息流完整性模型,将程序建模为信道,使用最小熵定量描述信息完整性. 首先刻画信息完整性中的污染和抑制两种情形. 基于此,进一步给出污染和信道容量之间的关系;并讨论复合程序的完整性的问题. 最后,分析讨论负信息流的情况.

关键词: 信息流; 完整性; 最小熵; 污染; 信道抑制
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2018)08-1822-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.08.004

Measuring Information Integrity Using Min-entropy

PENG Chao-ying, XI Zheng-jun
(*School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*)

Abstract: It is possible necessary in practice to accept some tampering of trusted information, this motivates the development of theories of quantitative information integrity aimed at showing that some tampering are small and therefore tolerable. In this paper, we focus on the threat model that an attack will modify the trusted information as much as possible in one try. Based on the information integrity model, we use the min-entropy to quantify the trusted information by modeling a program as a communication channel. We quantify the contamination and the channel suppression in information integrity. We then analyze the relationship between the contamination and the capacity of the channel, and consider the integrity in the cascade of the programs. Finally, we discuss the negative value case in quantitative information integrity.

Key words: information flow; integrity; min-entropy; contamination; channel suppression

1 引言

防止机密信息被泄露和可信信息被污染是计算机安全中的两个重要属性,即:机密性和完整性. 目前已有多种检测数据的方法及访问控制的模型来保证系统安全[1~5]. 但是由于网络环境的开放性和复杂性,信息仍然面临机密性和完整性的威胁.

相对于信息流机密性安全模型[6~9],完整性安全模型的研究成果相对较少. 但是随着电子商务和社交软件等网络应用的急速发展,完整性的需求越来越突显. 例如:用户使用电子钱包转账,加密手段能保证交易的机密性. 但是如果该交易的金额被改动系统就是不安全的. 而这就需要保护可信的信息不被恶意的更改,即保证信息的完整性. 目前关于信息完整性的研究大多数是定性的,即:保证可信信息在传输过程中没有被更改,或更改的信息可以被检测出来. 然而在实际应用中定量的要求也是有价值的. 如果不可信信息并没有损坏可信输出结果太多,系统可能允许接收可信信息和不可信信息结合后所得到的信息. 例如:在网上转账过程中,与交易无关的数据可以被添加到数据库中从而达到隐藏敏感信息的目的,而所得到的匿名数据库仍然包含足够的未损坏的信息,这并不影响转账交易的准确进行. 为了定量地刻画信息的篡改和损坏,Clarkson 和 Schneider 较为系统的讨论了信息安全的完整性. 他们将程序建模为信道,从破坏信息完整性的角度出发提出量化污染及信道抑制的信息流完整性模型,并使用香农熵定量地刻画信息流完整性[10]. 对于完整性的研究,Biba 定性地研究了可信和不可信信息之间的流

收稿日期:2017-06-12;修回日期:2017-10-25;责任编辑:蓝红杰
基金项目:国家自然科学基金(No. 61671280, No. 11531009);陕西省创新人才推进计划青年科技新星项目(No. 2017KJXX-92);陕西师范大学优秀青年学术骨干资助计划(No. 16QNGG013);中央高校基本科研业务费专项资金(No. GK201502004)

动,证明了信息的完整性与机密性之间具有相对性[11]. 在机密性的量化研究中,如果攻击者能够一次猜中机密信息,那么使用最小熵量化信息流能够提供一个更好的信息安全保障[12-16]. 从而,基于 Biba 提出的信息流思想,本文尝试使用最小熵来刻画信息流的完整性. 我们的研究结果表明当攻击者最大程度的修改可信信息时,最小熵量化信息流的完整性比基于香农熵的量化更加符合实际.

2　预备知识

本节介绍在本文中将要用到的信息论基本概念[17,18]. 一般情况下,使用三元组$(\mathscr{X},\mathscr{Y},\boldsymbol{M})$表示通信信道,$\mathscr{X}=\{x_1,\cdots,x_n\}$为输入值有限集,可观察的输出值有限集为$\mathscr{Y}=\{y_1,\cdots,y_m\}$,$\boldsymbol{M}$是$|\mathscr{X}|\times|\mathscr{Y}|$的信道矩阵,矩阵元素为$M[y|x]$($M[y|x]:=M[y_j|x_i]$),它表示当输入为$x$时得到输出为$y$的概率,且满足以下性质:给定任意一个输入值则所有可能输出的概率之和为 1. 特别地,如果信道矩阵$\boldsymbol{M}$的元素是 0 或 1,则该信道是确定的. 即表示每个输入只产生唯一输出;否则信道M为概率信道. 若在有限字符集$\mathscr{X}=\{x_1,\cdots,x_n\}$上存在先验分布$\pi(x)$($\pi(x):=\pi(x_i)$),结合信道矩阵,根据贝叶斯规则可以定义一个联合概率分布,即为$p(x,y)=\pi(x)M[y|x]$. 若已知随机变量X和Y的联合概率分布,则得到边际概率为$p(x)=\sum_y p(x,y)$. 同时若$p(x)\neq 0$,则可给出条件概率$p(y|x)=p(x,y)/p(x)$. 类似的,可以给出$p(y)$和$p(x|y)$. 当$p(x,y)$是恢复$\pi(x)$和$M[y|x]$的唯一分布,若$p(x)\neq 0$则$p(x)=\pi(x)$,$p(y|x)=M[y|x]$.

定义 1　设随机变量X的概率分布为$p(x)$,那么该随机变量的 Rényi 熵[19]定义为

$$H_\alpha(X)=\frac{1}{1-\alpha}\log\sum_x p(x)^\alpha,\alpha\in(0,1)\cup(1,\infty) \tag{1}$$

注意在本文中对数都是以 2 为底. 当$\alpha\to 1$时,Rényi 熵退化为香农熵,即:

$$H(X):=\lim_{\alpha\to 1}H_\alpha(X)=-\sum_x p(x)\log p(x) \tag{2}$$

当$\alpha\to\infty$时,Rényi 熵称作最小熵(Min-entropy)即:

$$H_\infty(X):=\lim_{\alpha\to\infty}H_\alpha(X)=-\log\max_x p(x) \tag{3}$$

显然,Rényi 熵是香农熵的一个拓展,在信息论、密码学、统计学、热力学等领域有着广泛的应用和研究. 香农熵是各种事件熵的加权平均,或者说是确定各个结局的一种平均信息量. 但是最小熵没有这样的操作意义,它表示最大概率事件发生的信息量. 因此在文献[12]中,基于攻击者能够一次猜中机密信息的前提下,Smith 提出了易损(vulnerability)的概念,定义了先验易损(prior vulnerability)和后验易损(posterior vulnerability)来定量刻画信息泄露.

定义 2　设随机变量X的概率分布为$p(x)$,则先验易损定义为

$$V(X)=\max_x p(x) \tag{4}$$

设随机变量X和Y的联合概率分布为$p(x,y)$,则后验条件易损定义为

$$V(X|Y)=\sum_y p(y)\max_x p(x|y) \tag{5}$$

显然,对先验易损取负对数就得到最小熵,即:

$$H_\infty(X)=-\log V(X) \tag{6}$$

基于后验易损,Smith 给出了条件最小熵的定义,给定随机变量Y时随机变量X的条件最小熵为

$$H_\infty(X|Y)=-\log V(X|Y) \tag{7}$$

这里的条件最小熵是先取平均再取对数,并不是香农熵的推广.

3　信息的抑制与污染

在定量信息流的研究中,通常将程序建模为信道,使用信息理论来量化信息流. 在文献[10]中,Clarkson 等人建立信息流完整性模型,从破坏信息完整性的出发点刻画了两个概念:污染和抑制,即错误信息出现在程序输出中和正确信息从程序输出中丢失. 如图 1 所示,黑色实线箭头在该图中分别表示污染与抑制. 不可信输入到可信输出的流动称为污染;在可信输入到可信输出的流动中,可信输出中的可信信息的衰减称为信道抑制. 图中四个箭头代表了信息流的所有可能流动. 从安全的角度分析,信息的完整性与有多少可信或不可信的信息流动到不可信输出无关. 因此 Clarkson 等人的研究表明在该信息流模型中污染和信道抑制是比较有价值的完整特性.

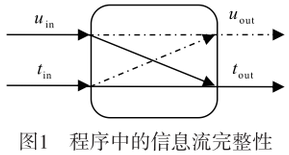

图1　程序中的信息流完整性

3.1　污染

污染是用户观察可信的输入与输出后得到不可信输入的信息量. 污染模型如图 2 所示. 在污染模型中有三个代理参与程序执行,即:系统、用户以及攻击者. 系统执行该程序. 系统具有三个变量:输入变量、输出变量和内部变量. 其中输入变量只能被系统读,输出变量只能由系统写入,而内部变量只能被系统读写. 用户和攻击者只能写入初始的输入变量值以及读取到输出变量的最终值. 该污染模型对用户和攻击者访问变量的权限进行限制. 用户可能仅访问受信任的变量,攻击者可

能仅访问不可信的变量. 但是可信和不可信信息之间的流动并没有被禁止. 攻击者可能被允许读可信的输入或输出,用户可能写入不可信信息. 读到可信输入的攻击者可能自适应地选择不可信输入来增加污染,这一特性通过输入的联合分布来体现.

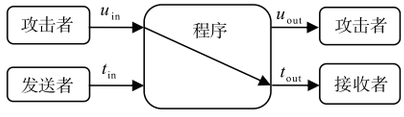

图2 污染模型

记 U_{in}为不可信输入变量,T_{in}为可信输入变量,T_{out}为可信输出变量. 如上图所示污染模型有两个输入分布:可信输入分布 $p(t_{in})$和不可信输入分布 $p(u_{in})$. 两个输出分布:可信输出分布 $p(t_{out})$和不可信输出分布 $p(u_{out})$,其中不可信的输出并不涉及程序可信输出的安全性,因此不对它进行量化分析. 假定已知可信输入分布 $p(t_{in})$,那么在可信输入的条件下不可信输入的条件概率分布为 $\pi(u_{in}|t_{in})$. 将程序建模为信道矩阵 $\boldsymbol{M}$,矩阵元素 $M[t_{out}|u_{in}t_{in}]$表示当已知输入分布时得到可信输出的概率,给定任意输入值则所有可能输出的概率之和为 1. 根据贝叶斯规则可定义联合概率分布为:

$$p(u_{in}t_{in}t_{out}) = p(t_{in})\pi(u_{in}|t_{in})M(t_{out}|u_{in}t_{in})$$

从而,可得 $p(u_{in}t_{in}) = \sum_{t_{out}} p(u_{in}t_{in}t_{out})$. 若 $p(u_{in}t_{in}) \neq 0$,则在可信输入下的可信输出的概率用条件概率来描述,即:$p(t_{out}|u_{in}t_{in}) = p(u_{in}t_{in}t_{out}) / p(u_{in}t_{in})$. 类似地,可以给出概率分布 $p(t_{in}t_{out})$和 $p(u_{in}|t_{in}t_{out})$. 如果当概率分布 $p(u_{in}t_{in}t_{out})$是恢复先验输入分布与信道 $\boldsymbol{M}$ 的唯一联合概率分布时,若 $p(u_{in}t_{in}) \neq 0$ 时,那么 $p(u_{in}t_{in}) = p(t_{in})\pi(u_{in}|t_{in})$,$p(t_{out}|u_{in}t_{in}) = M(t_{out}|u_{in}t_{in})$.

在攻击者最大可能地修改可信信息条件下,假定已知可信输入分布,基于先验输入分布 π 和信道 $\boldsymbol{M}$,类似于定义 2,可定义先验的条件易损和后验的条件易损,分别为:

$$V(U_{in}|T_{in}) = \sum_{t_{in}} p(t_{in}) \max_{u_{in}} p(u_{in}|t_{in}) \tag{8}$$

$$V(U_{in}|T_{out}T_{in}) = \sum_{t_{in},t_{out}} p(t_{out}t_{in}) \max_{u_{in}} p(u_{in}|t_{out}t_{in}) \tag{9}$$

从而,条件最小熵 $H_\infty(U_{in}|T_{in})$ 和 $H_\infty(U_{in}|T_{out}T_{in})$ 定义为:

$$H_\infty(U_{in}|T_{in}) = -\log V(U_{in}|T_{in}) \tag{10}$$

$$H_\infty(U_{in}|T_{out}T_{in}) = -\log V(U_{in}|T_{out}T_{in}) \tag{11}$$

这里 $H_\infty(U_{in}|T_{in})$描述已知可信输入分布的条件下不可信信息的初始不确定性,$H_\infty(U_{in}|T_{out}T_{in})$描述在已知可信输入分布的条件下观察可信输出后不可信信息仍然存在的不确定性. 基于信息论的基本知识可知:信息初始不确定性等于信息流动量加上信息剩余的不确定性. 从而,在已知可信输入分布条件下,假定先验输入分布 π,通过量化可信输出中出现的不可信输入的信息来刻画信息被污染的量.

定义 3 对于污染模型,信息被污染的量定义为给定可信输入条件下的最小熵条件互信息,即:

$$C_\infty(U_{in};T_{out}|T_{in}) = H_\infty(U_{in}|T_{in}) - H_\infty(U_{in}|T_{out}T_{in}) \tag{12}$$

这里量化 $C_\infty(U_{in};T_{out}|T_{in})$在形式上类似于香农条件互信息,为了与之区别,称之为最小熵污染. 事实上基于先验的条件易损和后验的条件易损,最小熵污染可写为:

$$C_\infty(U_{in};T_{out}|T_{in}) = \log \frac{V(U_{in}|T_{out}T_{in})}{V(U_{in}|T_{in})} \tag{13}$$

简记为 C_∞. 基于此定义,下面举例比较香农熵污染和最小熵污染.

例 1 对于程序

$$t_{out} := u_{in} \quad \text{xor} \quad t_{in}$$

假定 t_{out},u_{in}和 t_{in}分别表示两比特位可信输出,不可信输入和可信输入. 若它们都是随机均匀产生时,直观地用户可通过观察可信的输入和可信的输出推断出不可信输入的值,因此可知该程序的污染为 2 比特位. 计算可得最小熵污染为 $C_\infty = 2$,香农熵污染为 $\mathcal{I}(U_{in};T_{out}|T_{in}) = 2$. 此时使用最小熵污染和香农条件互信息刻画污染与直观上的污染一致. 当该程序的输入分布和输出分布并不是完全取自均匀概率分布时,最小熵污染并不一定恰好是污染的位数. 但它仍然表示可信输出被污染的程度,所以说使用最小熵度量的污染和 Clarkson 使用香农互信息度量的污染并不矛盾. 因此使用最小熵度量的完整性也可以应用到数据完整性模型中.

例 2 对于程序

$$\text{if}(u_{in} = t_{in}) \quad \text{then} \quad t_{out} := u_{in} \quad \text{else} \quad t_{out} := -1$$

若可信输入分布为 $p(t_{in}) = (\lambda, 0, 1-\lambda, 0)$,$0 \leqslant \lambda \leqslant 1$. 假定先验输入分布的矩阵表示如下:

$$\pi = p(u_{in}|t_{in}) = \begin{pmatrix} \frac{\omega}{2(1+\omega)} & 0 & \frac{\omega}{2(1+\omega)} & 0 \\ \frac{1}{2(1+\omega)} & 0 & \frac{1}{2(1+\omega)} & 0 \\ \frac{\omega}{2(1+\omega)} & 0 & \frac{\omega}{2(1+\omega)} & 0 \\ \frac{1}{2(1+\omega)} & 0 & \frac{1}{2(1+\omega)} & 0 \end{pmatrix}$$

其中 $0 < \omega \leqslant 1$. 由此可计算最小熵污染量为

$$C_\infty(U_{in};T_{out}|T_{in}) = \log(\omega+1)$$

而此时若使用香农熵量化的污染为

$$\mathcal{I}(U_{in};T_{out}|T_{in})$$

$$= 1 + \log(\omega+1) - \frac{\omega}{2(\omega+1)}\log\omega - \frac{\omega+2}{2(\omega+1)}\log(\omega+2)$$

$$+ \frac{\omega}{2(\omega+1)}(\lambda\log\lambda + (1-\lambda)\log(1-\lambda))$$

由此可知使用最小熵量化的信息污染的量以及香农熵量化的污染的量如图 3 所示.

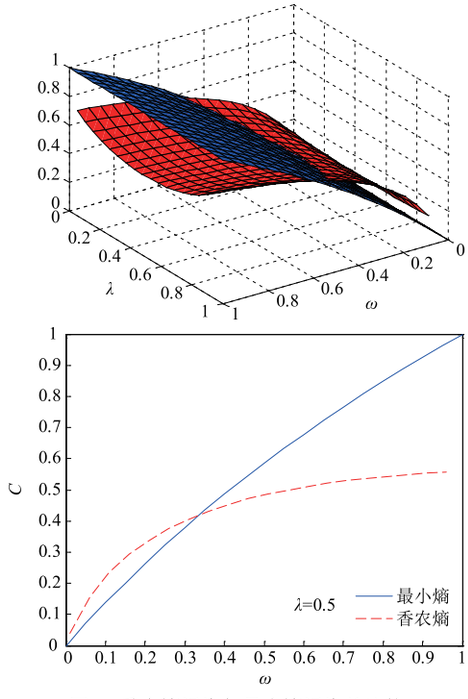

图3　香农熵污染与最小熵污染的比较

由此可知最小熵污染并不总是比香农熵量化的污染大,但是当用户一次猜中不可信的输入时,使用最小熵量化污染更加接近真实的污染.

以上讨论的污染都依赖于已知可信输入的条件下不可信输入的条件概率分布 π,源于信道容量的思想,定义在所有可能的先验分布 π 下最小熵污染的最大值称作最小容量,即:

$$\mathscr{M}(C)=\sup_{\pi} C_{\infty}(U_{\text{in}};T_{\text{out}}\mid T_{\text{in}}) \tag{14}$$

显然最小容量是污染的上界,且基于熵的一些基本性质可知最小容量是易于计算的.

定理 1　当先验分布 π 为均匀分布时,有

$$\mathscr{M}(C)=\log\sum_{t_{\text{out}}}\max_{u_{\text{in}}} C[t_{\text{out}}\mid t_{\text{in}}u_{\text{in}}] \tag{15}$$

证明　当先验分布 π 为均匀分布时,可知 $p(u_{\text{in}}\mid t_{\text{in}})$ 为均匀分布. 由于

$$\max_{u_{\text{in}}} p(u_{\text{in}}\mid t_{\text{in}})=p(u_{\text{in}}\mid t_{\text{in}})=\frac{1}{m}$$

$$\sum_{t_{\text{in}}} p(t_{\text{in}})\max_{u_{\text{in}}} p(u_{\text{in}}\mid t_{\text{in}})=p(u_{\text{in}}\mid t_{\text{in}})=\frac{1}{m}$$

由此可得:

$$\begin{aligned}C_{\infty}(U_{\text{in}};T_{\text{out}}\mid T_{\text{in}})&=H_{\infty}(U_{\text{in}}\mid T_{\text{in}})-H_{\infty}(U_{\text{in}}\mid T_{\text{out}}T_{\text{in}})\\&=\log\frac{\sum_{t_{\text{in}},t_{\text{out}}} p(u_{\text{in}}t_{\text{in}})\max_{u_{\text{in}}} p(t_{\text{out}}\mid t_{\text{in}}u_{\text{in}})}{\sum_{t_{\text{in}}} p(t_{\text{in}})\max_{u_{\text{in}}} p(u_{\text{in}}\mid t_{\text{in}})}\\&\leqslant\log\frac{\sum_{t_{\text{in}},t_{\text{out}}}\max_{u_{\text{in}}} p(t_{\text{out}}\mid t_{\text{in}}u_{\text{in}})\max_{u_{\text{in}}} p(u_{\text{in}}t_{\text{in}})}{\sum_{t_{\text{in}}}\max_{u_{\text{in}}} p(u_{\text{in}}t_{\text{in}})}\\&=\log\sum_{t_{\text{out}},t_{\text{in}}} p(t_{\text{in}})\max_{u_{\text{in}}} p(t_{\text{out}}\mid t_{\text{in}}u_{\text{in}})\\&=\log\sum_{t_{\text{out}}}\max_{u_{\text{in}}} p(t_{\text{out}}\mid t_{\text{in}}u_{\text{in}})\\&=\mathscr{M}(C)\end{aligned}$$

类似地,在所有可能的先验分布 π 上香农熵污染的最大值,称作香农容量,即:

$$\mathscr{M}_S(C)=\sup_{\pi} I(U_{\text{in}};T_{\text{out}}\mid T_{\text{in}}) \tag{16}$$

其中 $I(U_{\text{in}};T_{\text{out}}\mid T_{\text{in}})$ 是先验分布 π 上的香农条件互信息. 进一步可证明:最小容量是香农容量的上界.

定理 2　对于任何信道 M,有

$$\mathscr{M}_S(C)\leqslant\mathscr{M}(C) \tag{17}$$

证明　由 Jensen 不等式,如果 f 是一个凹函数,$\lambda_1,\lambda_2,\cdots,\lambda_n$ 是凸系数,$x_1,x_2,\cdots,x_n$ 是任意值,那么 $\sum_i\lambda_i f(x_i)\leqslant f(\sum_i\lambda_i x_i)$ 设定先验分布 π 是任意的输入分布,由 Jensen 不等式及 log 函数的凹性可知:

$$\begin{aligned}&I(U_{\text{in}};T_{\text{out}}\mid T_{\text{in}})\\&=\sum_{u_{\text{in}},t_{\text{in}},t_{\text{out}}} p(u_{\text{in}}t_{\text{out}}t_{\text{in}})\log\frac{p(u_{\text{in}}t_{\text{out}}\mid t_{\text{in}})}{p(u_{\text{in}}\mid t_{\text{in}})p(t_{\text{out}}\mid t_{\text{in}})}\\&\leqslant\log\sum_{u_{\text{in}},t_{\text{in}},t_{\text{out}}} p(u_{\text{in}}t_{\text{out}}t_{\text{in}})\frac{p(u_{\text{in}}t_{\text{out}}\mid t_{\text{in}})}{p(u_{\text{in}}\mid t_{\text{in}})p(t_{\text{out}}\mid t_{\text{in}})}\\&=\log\sum_{u_{\text{in}},t_{\text{in}},t_{\text{out}}} p(u_{\text{in}}\mid t_{\text{out}}t_{\text{in}})p(t_{\text{out}}\mid u_{\text{in}}t_{\text{in}})p(t_{\text{in}})\\&\leqslant\log\sum_{t_{\text{out}}}\sum_{u_{\text{in}},t_{\text{in}}} p(u_{\text{in}}\mid t_{\text{out}}t_{\text{in}})p(t_{\text{in}})(\max_{u_{\text{in}}} p(t_{\text{out}}\mid u_{\text{in}}t_{\text{in}}))\\&=\log\sum_{t_{\text{out}}}(\max_{u_{\text{in}}} p(t_{\text{out}}\mid u_{\text{in}}t_{\text{in}}))\\&=\mathscr{M}(C)\end{aligned}$$

3.2　抑制

本节使用最小熵量化信道抑制. 抑制模型由 Clarkson 等人给出[10],见图 4. 信道抑制就是接收者观察可信的输出后不能得到的可信输入的量. 注意该模型将用户分为两个代理即发送者与接收者. 发送者写入可信的输入,接收者接收到可信输出的最终值. 接收者通过观察程序的输出来判断由发送者提供的输入. 只有发送者和接受者可以访问可信的变量,而攻击者尝试通过写入不可信输入的初始变量干扰可信的输入. 攻击者仍只可能访问不可信变量. 同样的,可信与不可信信息之间的流动并没有被限制.

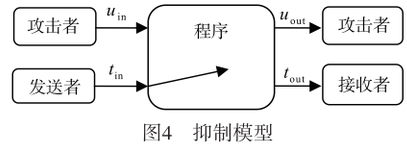

图4　抑制模型

假定可信输入的先验概率分布为 π,将程序建模为信道矩阵 $\boldsymbol{M}$,矩阵元素 $M[t_{out}|t_{in}]$. 根据贝叶斯规则可定义 $p(t_{in}t_{out})=\pi(t_{in})M(t_{out}|t_{in})$,由此可知可信输入的概率分布为 $p(t_{in})=\sum_{t_{out}}p(t_{in}t_{out})$. 当且仅当 $p(t_{in})\neq 0$ 时,则 $p(t_{out}|t_{in})=\dfrac{p(t_{in}t_{out})}{p(t_{in})}$. 同样可定义 $p(t_{out})$ 和 $p(t_{in}|t_{out})$. 同时当 $p(t_{in}t_{out})$ 是恢复先验输入分布与信道 $\boldsymbol{M}$ 的唯一分布,若 $p(t_{in})\neq 0$ 则 $p(t_{in})=\pi(t_{in})$,$p(t_{out}|t_{in})=M(t_{out}|t_{in})$.

在信息流抑制模型中,当发送者最大可能发送可信信息时,使用最小熵量化接收者所能接收到的可信信息的量以及可信信息被抑制的量. 因此,基于先验输入分布 π 和信道 $\boldsymbol{M}$,类似于定义 2,可定义先验的易损和后验的条件易损,分别为:

$$V(T_{in})=\max_{t_{in}}p(t_{in}) \tag{18}$$

$$V(T_{in}|T_{out})=\sum_{t_{out}}p(t_{out})\max_{t_{in}}p(t_{in}|t_{out}) \tag{19}$$

从而,类似于前面的讨论,可以定义:

$$H_\infty(T_{in})=-\log V(T_{in}) \tag{20}$$

$$H_\infty(T_{in}|T_{out})=-\log V(T_{in}|T_{out}) \tag{21}$$

显然,可以用 $H_\infty(T_{in})$ 来描述可信信息的初始不确定性,$H_\infty(T_{in}|T_{out})$ 描述可信信息在传输后仍存在的(或者剩余)不确定性.

定义 4 在信息抑制模型中,可信信息的最小熵传送量定义为初始可信信息不确定度与剩余可信信息不确定度的差,即:

$$CT_\infty=H_\infty(T_{in})-H_\infty(T_{in}|T_{out}) \tag{22}$$

定义 5 在信息抑制模型中,接收者观察输出后可信信息仍然存在的不确定性即为传送失败的量,因此最小熵信道抑制定义为

$$CS_\infty=H_\infty(T_{in}|T_{out}) \tag{23}$$

例 3 对于程序

$$t_{out}:=t_{in}\ \text{xor}\ a$$

假定 t_{out} 和 t_{in} 分别表示两比特位可信输出和可信输入,a 为系统随机产生两比特位. 假定先验分布为

$$\pi(t_{in})=p(t_{in})=\left(\frac{3}{16},\frac{5}{16},\frac{7}{32},\frac{9}{32}\right)$$

则通过计算可得信道的最小熵传送量和最小熵抑制分别为

$$CT_\infty=H_\infty(T_{in})-H_\infty(T_{in}|T_{out})=0;$$

$$CS_\infty=H_\infty(T_{in}|T_{out})\approx 1.68.$$

这表示在此信道中,在先验分布 π 条件下信道的最小熵传送量为 0,信道抑制为 1.68. 直观地,接收者无法从可信的输出中得到可信输入的值,即该程序在可信输出中丢失了可信输入. 由此将由程序引起的抑制叫做程序抑制,由攻击者引起的抑制叫做攻击者控制的抑制,即攻击者能够通过恶意选择输入影响信道抑制的量[10]. 如程序 $t_{out}:=u_{in}\ \text{xor}\ t_{in}$,攻击者可影响在可信输出中可信输入的值,由程序引起的抑制和攻击者控制抑制的详细说明将在以后讨论.

在理想情况下,信道串联后的抑制等于串联信道的每部分抑制之和. 然而,这种理想状况并不一定会经常出现. 但是信道串联的整体抑制以及部分抑制之间的关系可以给出证明. 接下来分析信道串联条件下的信息抑制. 信道串联是指使用第一个信道的输出作为第二个信道的输入,如图 5 所示.

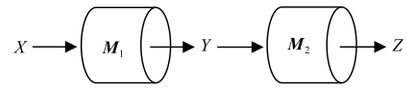

图5 信道$\boldsymbol{M}_1$与$\boldsymbol{M}_2$的串联

Espinoza 和 Smith 在文献[15]中证明在串联的两个信道$(\mathscr{X},\mathscr{Y},\boldsymbol{M}_1)$与$(\mathscr{Y},\mathscr{Z},\boldsymbol{M}_2)$中,若已知先验分布 π,对于任意 $x\in\mathscr{X},y\in\mathscr{Y},z\in\mathscr{Z}$,它们的联合概率分布 $p(x,y,z)=\pi(x)M_1[y|x]M_2[z|y]$;当 $p(x,y)>0$ 时 $p(z|x,y)=p(z|y)$. 即$(X,Y,\boldsymbol{M}_1)$与$(Y,Z,\boldsymbol{M}_2)$的串联信道可表示为$(\mathscr{X},\mathscr{Z},\boldsymbol{M}_1\boldsymbol{M}_2)$. 由此可以建立组合信道的信道矩阵,接下来分析单个信道抑制与串联后的信道抑制的关系. 信道串联后,第一信道被抑制之后的可信输出,作为第二信道的输入. 也就是说串联的信道中在第一信道中被抑制的量不能在第二信道中流动,即串联的信道至少能抑制和第一信道一样多的信息.

定理 3 如果已知输入先验分布 π,使用信道$(\mathscr{X},\mathscr{Z},\boldsymbol{M})$表示信道$(\mathscr{X},\mathscr{Y},\boldsymbol{M}_1)$与$(\mathscr{Y},\mathscr{Z},\boldsymbol{M}_2)$串联的信道,那么

$$CS_\infty(\pi,\boldsymbol{M}_1)\leqslant CS_\infty(\pi,\boldsymbol{M}) \tag{24}$$

证明 由于

$$\begin{aligned}V(X|Z)&=\sum_z\max_x M[z|x]\pi(x)\\&\leqslant\sum_z\sum_y\max_x M[z|y]M[y|x]\pi(x)\\&=\sum_y\left(\sum_z M[z|y]\right)\left(\max_x M[y|x]\pi(x)\right)\\&=\sum_y\left(\max_x M[y|x]\pi(x)\right)\\&=V(X|Y)\end{aligned}$$

故 $-\log V(\pi,\boldsymbol{M}_1)\leqslant -\log V(\pi,\boldsymbol{M})$,由此可得:

$$CS_\infty(\pi,\boldsymbol{M}_1)\leqslant CS_\infty(\pi,\boldsymbol{M})$$

例如当信道 $\boldsymbol{M}_1$ 为程序 $t_{out}:=t_{in}\ \&\ 01$,信道 $\boldsymbol{M}_2$ 为程序 $t_{out}:=t_{in}\ \&\ 10$,信道 $\boldsymbol{M}_1$ 和信道 $\boldsymbol{M}_2$ 信串联后的信道 $\boldsymbol{M}$ 可表示为程序 $t_{out}:=t_{in}\ \&\ 00$. 若 t_{out} 和 t_{in} 分别表示两位独立的可信均匀输出和可信均匀输入,那么可以得到信道 $\boldsymbol{M}_1$ 的抑制为 1 个比特位,串联后信道 $\boldsymbol{M}$ 的程序抑制为 2 个比特位. 而若信道 $\boldsymbol{M}_2$ 为程序 $t_{out}:=t_{in}\ \&$

01,则串联信道 $\boldsymbol{M}$ 可表示为程序 $t_{out}:=t_{in}\ \&\ 01$. 那么可以得到信道 $\boldsymbol{M}_1$ 的抑制为 1 个比特位,串联后信道 $\boldsymbol{M}$ 的程序抑制仍为 1 个比特位.

4　负信息流

由于平均条件互信息总为非负值,因此使用香农熵量化信息时不会出现负信息流. 而使用最小熵和条件最小熵量化信息可能会出现负的信息流. Espinoza 和 Smith 使用最小熵量化信息的动态泄露时,出现负的信息泄露[15]. Ngo 和 Huisman 提出当系统有意地增加噪音到输出中,这个噪音输出会减少秘密输入与输出之间的联系,致使秘密信息后验的不确定性变大,从而出现负的信息流[20]. 负信息泄露表示该信道具有更强的机密性和可靠性. 本文中信道抑制与机密性之间并不具有相对性. 可信信息被抑制的量为:$CS_\infty=H_\infty(T_{in}\mid T_{out})$,由此可知抑制的量化不会出现负值. 而污染与机密性之间具有相对性,因此在使用最小熵量化信息污染时可能会出现负信息流. 信息被污染的量为不可信信息初始不确定度与观察可信输出后不可信信息仍然存在的不确定度之差. 因此若用户猜测攻击者一次最大可能修改可信信息的先验认知正确,且没有“噪音”被系统添加到可信的输出中,此时使用最小熵量化信息不会出现负的信息流[9]. 即若系统不允许程序进行更改,且在用户猜测攻击者最大可能修改可信信息的先验认知正确的条件下,最小熵污染为非负值. 但是当用户对攻击者先验的认知存在错误或系统允许对程序进行更改时就会出现负的信息流. 下面使用例子说明这种情形.

例 4　在下列程序中攻击者尝试污染可信的输出,程序描述如下:

$$\text{if}\ (u_{in}=t_{in})\ \text{then}\ t_{out}:=t_{in}\ \text{else}\ t_{out}:=00$$

假定 t_{out},u_{in} 和 t_{in} 分别表示两比特位的可信输出,不可信输入和可信输入. 假定此时可信输入分布为 $p(t_{in})=(0,1,0,0)$,先验输入分布的矩阵表示如下:

$$\boldsymbol{\pi}=p(u_{in}\mid t_{in})=\begin{pmatrix}0 & 0.125 & 0 & 0\\ 0 & 0.625 & 0 & 0\\ 0 & 0.125 & 0 & 0\\ 0 & 0.125 & 0 & 0\end{pmatrix}$$

因此在可信输入为 01 时,用户猜测攻击者一次最大可能修改可信息的输入为 01,故当用户观察到程序的输出为 01 时的最小熵污染量为

$$C_\infty(U_{in};T_{out}=01\mid T_{in}=01)\approx 0.68$$

上述情况对应与现实中的案例,当自动导航仪根据用户前进方向导航,攻击者通过该程序修改导航仪的输出来污染驾驶员的前进方向. 当可信的输入为 01,用户猜测攻击者可能将前进方向更改为 01,直观地用户观察可信的输出后可得知不可信的输入为 01,所以可信的输出被污染. 但当用户观察到程序的输出为 00,最小熵污染的量为:

$$C_\infty(U_{in};T_{out}=00\mid T_{in}=01)\approx -0.91$$

这说明用户猜测攻击者可能将前进方向更改为 01,但自动导航仪出现的结果为 00,这个结果既不是可信的输入也不是攻击者污染. 这种情况的出现有两种可能性:一种可能的情况是用户对攻击者的先验认知错误,导航仪会出现用户没有猜测到的导航方向,这个没有预料的导航方向使得不可信信息的后验不确定度变大. 即若用户对攻击者的先验认知存在局限性,那么不可信信息的后验不确定度变大. 从而出现负的信息流. 因此最小熵污染只有在用户对攻击者的先验认知正确的条件下才具有可用性. 另一种可能的情况是在用户对攻击者的先验认知不变的条件下,信道可能产生“噪音”干扰预定的输出,即系统可能修改原定的程序从而干扰程序的输出. 当系统有意的增加噪音到输出中,这个噪音输出会减少不可信输入与输出之间的联系,增加不可信信息后验的不确定性,从而可能会出现负的信息流. 这种情况下的污染表示该噪音信道中攻击者能够更好的破坏信息完整性.

因此为了保证信息的完整性,系统有意的增加可信信息到输出中,则这个可信的输出会减少不可信输入与可信输出之间的联系,增加不可信信息后验的不确定性同时减少了可信输出中可信信息的不确定度. 虽然这个条件下可信的输出中仍然可能存在污染,但该信道具有更强的完整性和可靠性. 例如用户对攻击者先验认知正确的条件下,系统将该程序更改为:

$$\text{if}\ (u_{in}=t_{in})\ \text{then}\ t_{out}:=t_{in}\ \text{else}\ t_{out}:=t_{in}$$

显然,更改后的程序总是输出可信的信息,有利于保证信息的完整性.

5　结论

在计算机安全理论中,完整性的刻画已得到越来越多的重视和研究. 本文是完整性度量理论方面的一个尝试. 当已知可信输入分布时,在攻击者尝试最大可能破坏可信信息的条件下,根据 Clarkson 定义的信息流完整性模型,使用最小熵量化程序中信息的完整性. 我们重点讨论了污染和信道抑制,进一步分析了最小熵污染与最小容量,证明了最小容量和香农容量之间的关系. 同时讨论了串联信道中的抑制问题. 最后阐述了度量信息完整性出现的负的信息流的意义. 通过比较最小熵和香农熵量化的污染与抑制,在一次攻击情形下,发现最小熵更加符合实际情形. 在未来的工作中我们将讨论增益函数[14](gain function)在信息完整性度量中的应用.

参考文献

[1] 徐明迪,张焕国,张帆,等. 可信系统信任链研究综述[J]. 电子学报,2014,42(10):2024 – 2031.
Xi Mingdi, Zhang Huanguo, Zhang Fan, et al. Survey on chain of trust of trusted system[J]. Acta Electronica Sinica,2014,42(10):2024 – 2031. (in Chinese)

[2] 王小明,付红,张立臣. 基于属性的访问控制研究进展[J]. 电子学报,2010,38(7):1660 – 1667.
Wang Xiaoming, Fu Hong, Zhang Lichen. Reserch progress on attribute-based access control[J]. Acta Electronica Sinica,2010,38(7):1660 – 1667. (in Chinese)

[3] 吴泽智,陈性元,杨智,等. 信息流控制研究进展[J]. 软件学报,2017,28(1):135 – 159.
Wu Zezhi, Chen Xingyuan, Yang Zhi, et al. Survey on information flow control[J]. Chinese Journal of Software, 2017,28(1):135 – 159. (in Chinese)

[4] Qian Z J, Liu W, Huang H. Research on microkernel integrity semantics model and formal verification[J]. Chinese Journal of Electronics,2014,23(1):43 – 48.

[5] Zhang J M, Tao S Q, Liang J Y. Logical implication of structural integrity constraints for XML[J]. Chinese Journal of Electronics,2009,18(2):243 – 248.

[6] 彭长根,丁红发,朱义杰,等. 隐私保护的信息熵模型及其度量方法[J]. 软件学报,2016,27(8):1891 – 1903.
Peng Changgen, Ding Hongfa, Zhu Yijie, et al. Information entropy models and privacy metrics methods for privacy protection[J]. Chinese Journal of Software, 2016,27(8):1891 – 1903. (in Chinese)

[7] Clarkson M R, Myers A C, Schneider F B. Quantifying information flow with beliefs[J]. Journal of Computer Security,2009,17(5):655 – 701.

[8] Alvim M S, Chatzikokolakis K, Mciver A, et al. Axioms for information leakage[A]. Proceedings of the 29th IEEE Symposium on Computer Security Foundations[C]. Washington DC:IEEE Computer Society,2016. 77 – 92.

[9] Hamadou S, Palamidessi C, Sassone V. Quantifying leakage in the presence of unreliable sources of information[J]. Journal of Computer and System Sciences,2017. 88: 27 – 52.

[10] Clarkson M R and Schneider F B. Quantification of integrity[J]. Mathematical Structures in Computer Science, 2015. 25:207 – 258.

[11] Biba K J. Integrity Considerations for secure computer systems[J]. Austranlian Journal of Statistics, 1977, 13(1):27 – 35.

[12] Smith G. On the foundations of quantitative information flow[A]. Proceedings of the 12th International Conference on Foundations of Software Science and Computational Structures[C]. Berlin Heidelberg:Springer,2009. 5504:288 – 302.

[13] Espinoza B, Smith G. Min-entropy leakage of channels in cascade[A]. Proceedings of the Formal Aspects of Security and Tust Lecture Notes in Computer Science[C]. Berlin Heidelberg:Springer,2012. 7140:70 – 84.

[14] Alvim M S, Chatzikokolakis K, Palamidessi C, et al. Measuring information leakage using generalized gain functions[A]. Proceedings of the 25th IEEE Computer Security Foundations Symposium[C]. Washington DC: IEEE Computer Society,2012. 265 – 279.

[15] Espinoza B, Smith G. Min-entropy as a resource[J]. Information and Computation,2013. 226(2):57 – 75.

[16] Backes M, Köpf B, Rybalchenko A. Automatic discovery and quantification of information leaks[A]. Proceedings of the 30th IEEE Symposium on Security and Privacy [C]. Washington DC:IEEE Computer Society,2009. 141 – 153.

[17] Shannon C E. A mathematical theory of communication [J]. Bell System Technical Journal,1948. 27:379 – 423.

[18] Cover T M, Thomas J A. Elements of Information Theory [M]. Hoboken, New Jersey: Published by John Wiley & Sons, Inc,2006.

[19] Renyi A. On measures of information and entropy[J]. Maximum-Entropy and Bayesian Methods in Science and Engineering,1961,1(2):547 – 561.

[20] Ngo T M, Huisman M. Quantitative security analysis for programs with low input and noisy output[A]. Proceedings of Engineering Secure Software and Systems[C]. Switzerland:Springer International,2014. 77 – 94.

作者简介

彭朝英 女,1991 年生于河南南阳. 硕士研究生,研究方向为智能信息处理、信息安全.

席政军(通信作者) 男,1983 年生于甘肃会宁. 博士(后),副教授,硕士生导师,中国计算机学会高级会员. 研究方向为量子信息论、信息安全等.
E-mail:xizhengjun@snnu.edu.cn