

引用格式:许钦百 王彩芬. 基于密码学理论的私密信息安全风险评估方法[J]. 科学技术与工程, 2019, 19(7): 172-176

Xu Qinbai, Wang Caifen. Privacy information security risk assessment method based on cryptography theory[J]. Science Technology and Engineering, 2019, 19(7): 172-176

基于密码学理论的私密信息安全风险评估方法

许钦百 王彩芬 *

(西北师范大学计算机科学与工程学院, 兰州 730070)

摘要 为了解决传统方法没有考虑针对私密信息的防控措施, 得到的私密信息安全风险评估结果不准确的问题, 通过密码学理论研究了私密信息安全风险评估方法。在将资产-威胁-脆弱性作为核心对风险值进行计算的基础上, 引入安全防控措施功能进行分析。按照相关原则, 建立阶梯层次式私密信息安全风险评估指标体系, 通过熵系数对各评估指标的权重进行计算。在不考虑防控措施的情况下计算风险值, 通过密码学理论对私密信息安全性进行保护后风险值进行计算, 将二者结合在一起, 获取考虑密码学理论下防控措施后, 私密信息风险值, 实现私密信息安全风险评估。结果表明: 所提方法可有效实现私密信息安全风险评估; 所提方法风险评估结果准确合理。可见所提方法评估性能准确。

关键词 密码学理论 私密信息 安全风险评估方法

中图法分类号 TP393.08; **文献标志码** A

随着信息化发展, 信息化、数字化和网络化变成信息发展的必然趋势。因为网络自身的开放性, 给私密信息带来了很大的威胁, 网络环境下私密信息的安全性面临很大的挑战^[1,2]。所以, 研究一种有效的私密信息安全风险评估方法具有重要的理论价值与社会价值^[3]。

私密信息安全主要是指私密信息原始真实性、完整性与保密性, 网络结构威胁性较大, 在数据传输时容易被拦截, 或受到攻击^[4,5]。

当前私密信息安全风险评估大多仅考虑了资产、威胁与脆弱性, 忽略了已有安全措施的考虑, 为此, 提出一种新的基于密码学理论的私密信息安全风险评估方法。

密码学为当代信息和网络安全的重要技术, 主要包括密码编码学与密码分析学, 实现消息保密的技术被称作密码编码学, 破译密码技术被称作密码分析学, 即在密钥未知的状态下依据密文获取明文或密钥^[6]。明文即原始私密信息, 密文为已经加密后的信息, 密钥为用于加密的参数, 密码学加密理论即把明文转换成密文, 解密即对密文进行恢复, 得到

原始明文。通过密码学理论将已有安全措施考虑进去, 实现私密信息安全风险评估^[7]。

1 基于密码学理论的私密信息安全风险评估方法

1.1 私密信息安全风险值计算

在对私密信息进行安全保障的过程中, 大都通过私密信息安全风险评估方法进行评估。在实际应用中, 通常从安全风险控制的角度分析, 将资产-威胁-脆弱性作为核心对风险值进行计算, 实现评估^[8,9]。设资产为 Z , 即对组织有价值的信息, 为安全保护对象, 可通过保密等级进行描述; 威胁为 T , 即在很大程度上造成组织受到入侵的潜在原因; 脆弱性为 C , 即可能被威胁利用的薄弱环节。则私密信息安全风险值 R 为

$$R(Z, T, C) = R[P(T, C), Q(p_a, C_a)] \quad (1)$$

式(1)中, R 为私密信息安全风险计算函数; p_a 为私密信息安全事件起到作用的资产价值; C_a 为脆弱程度; P 为威胁借助资产脆弱性引起安全风险事件出现的可能性; Q 为私密信息安全事件出现后造成的损失。

在实际应用中, 通常会采取一定的安全措施保护私密信息, 当前风险计算通常忽略了这些安全防控措施^[10]。现通过密码学理论对私密信息进行安全保护, 以减少私密信息安全风险发生概率, 降低产生的损失。所以, 在上述风险三要素的基础上引入安全防控措施功能 g , 则私密信息安全风险评估

2018年10月31日收到 国家自然科学基金(61202395, 61562077, 61662069, 61662071)、甘肃省自然科学基金(145RJDA325)和甘肃省高等学校科研项目(2017A-003, 2018A-207)资助
第一作者简介: 许钦百(1992—), 男, 汉族, 甘肃兰州人, 硕士研究生。E-mail:xuruanbai_0613326@163.com。

*通信作者简介: 王彩芬(1963—), 女, 汉族, 河北安国人, 博士, 教授、博士研究生导师。E-mail:xuruanbai_0613326@163.com。

值为

$$R = F(Z, T, C, g) \quad (2)$$

1.2 私密信息安全风险评估指标体系建立

私密信息安全风险评估指标体系的建立按照评估目标与评估内容的具体要求实现,主要目的为建立一组体现私密信息安全水平的相关指标^[11]。按照建立原则,可将指标建立成阶梯层次式,见表1。

表1 私密信息安全风险评估指标体系

Table 1 Private information security risk assessment index system

准则	指标
资产	影响有形资产
	影响无形资产
威胁	恶意软件
	操作程序
	网络风险
	通信攻击
脆弱性	加密等级
	易攻击程度
防控措施	私密信息访问控制
	私密信息保护控制
	网络访问管理

1.3 指标权重计算

对评估因素集进行确定,研究表1中不同指标。 $S = \{s_1, s_2, s_3, s_4\}$ 即把安全风险划分成四个评估因素,依次是资产、威胁、脆弱性和防控措施,与 s_i 相应的权重为 w_j 。 $S_1 = \{s_{11}, s_{12}\}$,把 s_1 划分成2个评估指标,与 s_{1j} 相应的权重为 w_{1j} 。安全同样的方式获取 S_2, S_3, S_4 及其元素相应权重。

在对私密信息安全风险进行评估时,不同风险因素的不确定性较大,现通过熵系数对权重进行计算^[12,13]。

熵为系统不确定性体现,不确定性令熵针对处理模糊风险指标具有优势。假设系统出现 m 中差异状态概率是 p'_1, p'_2, \dots, p'_m , $0 \leq p'_i \leq 1$, 其中 $\sum_{i=1}^m p'_i = 1$, 那么熵可通过式(3)求出。

$$B = -k \sum_{i=1}^m p'_i \ln p'_i \quad (3)$$

熵的性质如下:

- (1) 非负性: $B(x) \geq 0$ 。
- (2) 可累加性: 系统熵为不同状态熵之和。
- (3) 确定型: 在 $p'_i = 1$ 的情况下, 存在 $B(p'_1, p'_2, \dots, p'_m) = 0$, 同时系统状态确定。
- (4) 极值性: 在 $p'_i = \frac{1}{m}$ 的情况下, 系统熵值达到最大值 $B(p'_1, p'_2, \dots, p'_m) = \ln m$ 。

在式(3)符合 $B(p'_1, p'_2, \dots, p'_m) \leq \ln m$ 、 $B(p'_1, p'_2, \dots, p'_m) = B(p'_1, p'_2, \dots, p'_m, 0)$ 、 $B(XY) = B(X) + H(\frac{Y}{X})$ 时存在唯一条件:

$$B(p'_1, p'_2, \dots, p'_m) = - \sum_{i=1}^m p'_i \ln p'_i \quad (4)$$

熵权能够有效解决因主观因素导致的误差,某安全风险评估指标 r_i 支持度 p'_{ij} 值相差越大,认为该评估指标在风险评价中的作用越大^[14]。若某风险评估指标针对各指标支持度均一致,则信息熵达到最大值,认为当前求解的不同评价指标风险度太分散,评价效果不好,可标识当前熵权是0。

信息熵 $B(p'_1, p'_2, \dots, p'_m) = - \sum_{i=1}^m p'_i \ln p'_i$, 代表有序程度。依据熵的极值性可知 p'_i 相似的情况下, 熵值相对较大, 风险评估指标针对风险的评估作用相对较小, 所以可通过信息熵求解不同评估指标的权重。按照风险因子针对评估体系各指标的支持度 p'_{ij} 实现。评估指标 r_i 的相对重要程度可通过式(5)衡量。

$$B_i = - \sum_{i=1}^m p'_{ij} \ln p'_{ij} \quad (5)$$

依据熵的极值性可以看出, 熵的最大值是 $\ln m$, 通过 $\ln m$ 完成对公式的归一化处理^[15], 可获取风险评估指标 r_i 的相对重要熵值, 即:

$$E_i = - \frac{1}{\ln m} \sum_{i=1}^m p'_{ij} \ln p'_{ij} \quad (6)$$

通过上述分析可知, 在熵值达到最大的情况下, 风险评估指标对风险评估结果的影响最小, 可通过 $1 - E_i$ 对风险评估指标的权进行衡量, 则归一化的风险评估指标 r_i 的权值 W_i 可通过式(7)求出:

$$W_i = \frac{1 - E_i}{m - \sum_{i=1}^m E_i} \quad (7)$$

1.4 未考虑防控措施时风险值计算

完成私密信息安全风险评估指标权重确定后,首先在不考虑防控措施的情况下进行风险计算。

设 $U = \{u_1, u_2, \dots, u_k\}$ 为评语集, u_q , $q = (1, 2, \dots, k)$ 为详细评语, $U = \{u_1, u_2, u_3, u_4, u_5\}$, 其中 $u_1 \sim u_5$ 依次代表极低风险、低风险、一般风险、高风险和极高风险^[16]。用 $D(U) = \{d(u_1), d(u_2), \dots, d(u_k)\}$ 为专家针对 u_q 给出的风险事件危害程度。依据可信值 $l(u_q)$ 获取可信度:

$$\xi(u_q) = \sum_{u \subseteq u_q} l(u_q) \quad (8)$$

由此实现不考虑防控措施的情况下风险评估,计算公式为

$$R = \sum_{q=1}^k D(u_q) \xi(u_q) \quad (9)$$

1.5 考虑密码学理论防控措施时风险值计算

在实际应用中,通常通过密码学理论对私密信息安全性进行保护。专业技术人员利用密码学理论对私密信息进行加密,处理获取输出结果与结论,对加密私密信息进行解密,使得得到结果和原始结果一致,提高了安全性^[17]。

针对某私密信息资产 A ,进行了 N 项依据密码学理论的安全措施 $H = \{H_1, H_2, \dots, H_N\}$,所有措施均对资产面临威胁 C_ε 产生影响,包括减少威胁发生可能性影响 H_{aj} 与减少威胁破坏程度影响 H_{bj}, H_{aj} 与 H_{bj} 均在 0~1 范围内取值,取值越大,认为影响程度越小。

在密码学理论防护下,威胁发生概率表示为

$$P(T_N) = P(Z_\varepsilon) \left\{ 1 - \prod_{N=1}^M [1 - P(C_{NM})] \right\} \prod_{j=1}^N H_{aj} \quad (10)$$

式(10)中, $P(Z_\varepsilon)$ 表示第 ε 个信息发生的概率。

假设威胁 $T_\varepsilon (\varepsilon = 1, 2, \dots, N)$ 对应的脆弱点集合为 $C_\varepsilon = \{C_{\varepsilon 1}, C_{\varepsilon 2}, \dots, C_{\varepsilon M}\}$,任意脆弱点 $C_{\varepsilon M}$ 被威胁 T_ε 利用为一概率事件,则威胁发生产生的影响为

$$Y(T_\varepsilon) = \sum_{\varepsilon=1}^M \left\{ \left[P(C_{\varepsilon M}) \prod_{j=1}^{\varepsilon} H_{aj} \right] \left(D_{\varepsilon M} \prod_{j=1}^{\varepsilon} H_{bj} \right) \right\} \quad (11)$$

式(11)中, $D_{\varepsilon M}$ 表示脆弱点造成的损坏度。

在上述分析的基础上,可获取考虑密码学理论风险值:

$$E(Z) = Z \sum_{\varepsilon=1}^N \sum_{j=1}^M \left\{ \left[P(C_{\varepsilon M}) \prod_{j=1}^{\varepsilon} H_{aj} \right] \left(D_{\varepsilon M} \prod_{j=1}^{\varepsilon} H_{bj} \right) \right\} \quad (12)$$

考虑密码学理论下防控措施后,私密信息资产 Z 的风险值 R' 可通过式(13)求出:

$$R' = R(Z, T, C)[1 - E(Z)] \quad (13)$$

2 实验结果及分析

2.1 本文方法实例分析

现以某私密信息数据库为例展示本文方法安全风险评估过程。经研究,发现研究数据库面临计算机病毒、蠕虫攻击、拒绝服务攻击以及漏洞攻击等风险。

现采用本文方法对其安全风险进行评估。首先针对私密信息安全风险评估指标体系,计算指标相应权值,结果见表 2。

表 2 安全风险评估指标权值

Table 2 Weights of safety risk assessment indicators

准则	权值	指标	权值
资产	0.15	影响有形资产	0.44
		影响无形资产	0.56
威胁	0.4	恶意软件	0.26
		操作程序	0.19
		网络风险	0.32
脆弱性	0.2	通信攻击	0.23
		加密等级	0.59
		易攻击程度	0.41
防控措施	0.25	私密信息访问控制	0.39
		私密信息保护控制	0.26
		网络访问管理	0.35

本文方法风险等级及风险发生造成导致后果危害程度见表 3。

表 3 风险等级及相应危害程度情况

Table 3 Risk level and corresponding hazard level

参数	风险等级				
	极低风险	低风险	一般风险	高风险	极高风险
风险值	[0, 2)	[2, 4)	[4, 6)	[6, 8)	[8, 10]
危害程度	[0, 0.2)	[0.2, 0.4)	[0.4, 0.6)	[0.6, 0.8)	[0.8, 1.0]

在此基础上,通过式(8)计算未考虑防控措施的私密信息安全风险评估值,得到的结果为 3.4。

在考虑防控措施的情况下,通过式(12)计算风险值,为 0.35。将二者代入式(13)得到最终私密信息安全风险评估值为 2.21。

由评估结果可知,本文方法对研究私密信息的安全风险评估等级为低风险。

2.2 和其他方法的对比测试

为了对本文方法、灰色关联分析方法和熵权模糊集方法三种评估方法用于私密信息安全风险评估的效果,选择 2 个私密信息数据库,采用三种方法依次对其进行详细评估。

进行私密信息安全风险评估方案制定、资产识别和分析、威胁识别和分析、脆弱性识别和分析,获取不同风险要素取值。依次通过本文方法、灰色关联分析方法和熵权模糊集方法把不同风险要素转变为相应评分分支,获取私密信息安全风险值,同时转换成相应风险等级值。

参与测试的数据库 1 涉及的私密信息数量为 1 260,依次通过三种方法获取其安全风险等级值分布情况,得到的结果见表 4。参与测试的数据库 2 涉及的私密信息数量为 685,依次通过三种方法获取其安全风险等级值分布情况,得到的结果见表 5。

需要注意的是,实际上数据库 1 与数据库 2 的

大部分私密信息风险较低。

表 4 采用三种方法对数据库 1 的风险评估结果

Table 4 Using three methods to evaluate the risk of database 1

参数	风险级别	评估方法		
		熵权模 糊集	灰色关 联分析	本文
评估安全风险 相应信息量	极低风险	-	11	92
	低风险	29	110	915
	一般风险	912	506	247
	高风险	319	471	6
	极高风险	-	162	0
风险信息占总 量之比/%	超过一般风险	97.698	77.540	20.079
	超过高风险	25.317	50.238	0.476

注:“-”表示无此级别。

表 5 采用三种方法对数据库 2 的风险评估结果

Table 5 Uses three methods to evaluate the risk of database 2

参数	风险级别	评估方法		
		熵权 模糊集	灰色关 联分析	本文
评估安全风险 相应信息量	极低风险	-	115	295
	低风险	156	219	321
	一般风险	411	216	62
	高风险	118	75	7
	极高风险	-	15	0
风险信息占总 量之比/%	超过一般风险	77.262	49.051	10.073
	超过高风险	17.262	13.139	1.022

注:“-”表示无此级别。

分析表 4 和表 5 中的数据可知,熵权模糊集方法对私密信息安全风险等级的区分度过小,风险等级值较高,针对数据库 1,高于 97% 的私密信息超过一般风险,高于 25% 私密信息处于高风险。针对数据库 2 的情况稍微合理,然而大部分私密信息依旧分布于一般风险以上,和实际情况不符。

采用灰色关联分析法后,区分度情况优于熵权模糊集方法,然而仍存在私密信息风险等级偏高的情况。采用灰色关联分析法对数据库 1 进行私密信息安全风险评估时,高风险和极高风险的私密信息占比 50% 左右,一般风险以上的私密信息占比 77% 左右,需对大部分私密信息进行风险控制。采用灰色关联分析法对数据库 2 进行私密信息安全风险评估时,得到的私密信息风险等级较数据库 1 低,但仍存在 49% 左右的私密信息风险在一般等级以上,不满足实际数据库风险情况。

采用本文方法后,区分度情况较优,且对私密信息风险等级的评估和实际情况基本相符,针对数据库 1,私密信息风险高于一般风险的仅有 20% 左右,高风险和极高风险私密信息很少。针对数据库 2,

私密信息风险高于一般风险的仅有 10% 左右,高风险和极高风险私密信息只占 1% 左右,和实际情况相符,说明本文方法评估结果最可靠合理。

将三种方法应用于私密信息安全风险评估的测试结果表明,三种方法均可实现私密信息安全风险评估中,然而三种方法评估结果在准确性方面有很大的差异,整体看来,本文方法最优,熵权模糊集方法评估性能最差,这主要是因为其只将风险等级划分成三级,区分度小。

3 结论

为了保护私密信息安全性,提出一种基于密码学理论的私密信息安全风险评估方法。

(1) 从安全风险控制的角度分析,将资产-威胁-脆弱性作为核心对风险值进行计算。在此基础上引入安全防控措施功能,按照私密信息安全风险评估指标体系建立原则,建立阶梯层次式风险评估指标体系,对评估指标权重进行计算。

(2) 在不考虑防控措施的情况下进行风险计算。通过密码学理论对私密信息安全性进行保护,利用密码学理论对私密信息进行加密,处理获取输出结果与结论,对加密私密信息进行解密,使得得到结果和原始结果一致,提高了安全性。计算考虑密码学理论下防控措施下风险值。

(3) 将考虑密码学理论下防控措施与未考虑密码学理论下防控措施风险值结合在一起,获取最终私密信息安全风险评估结果。

(4) 经验证,所提方法评估准确性与合理性高。

参 考 文 献

- 陈宇,王亚弟,王晋东,等.模糊认知图在信息安全风险评估中的应用研究[J].计算机工程,2016,42(7):109-116
Chen Yu, Wang Yadi, Wang Jindong, et al. Application research on fuzzy cognitive map in information security risk assessment[J]. Computer Engineering, 2016, 42(7):109-116
- 过辰楷,许静,司冠南,等.面向移动应用软件信息泄露的模型检测研究[J].计算机学报,2016,39(11):2324-2343
Guo Chenkai, Xu Jing, Si Guannan, et al. Model checking for software information leakage in mobile application[J]. Chinese Journal of Computers, 2016, 39(11): 2324-2343
- Shameli-Sendi A, Aghababaei-Barzegar R, Cheriet M. Taxonomy of information security risk assessment (ISRA)[J]. Computers & Security, 2016, 57(C):14-30
- 武文博,康锐,李梓.基于攻击图的信息物理系统信息安全风险评估方法[J].计算机应用,2016,36(1):203-206
Wu Wenbo, Kang Rui, Li Zi. Attack graph based risk assessment method for cyber security of cyber-physical system [J]. Journal of Computer Applications, 2016, 36(1):203-206
- 柴继文,王胜,梁晖辉,等.基于层次分析法的信息安全风险

- 评估要素量化方法[J]. 重庆大学学报, 2017, 40(4):44-53
 Chai Jiwen, Wang Sheng, Liang Huihui, et al. An AHP-based quantified method of information security risk assessment elements [J]. Journal of Chongqing University(Natural Science Edition), 2017, 40(4):44-53
- 6 熊金波, 李凤华, 王彦超, 等. 基于密码学的云数据确定性删除研究进展[J]. 通信学报, 2016, 37(8):167-184
 Xiong Jinbo, Li Fenghua, Wang Yanchao, et al. Research progress on cloud data assured deletion based on cryptography[J]. Journal on Communications, 2016, 37(8):167-184
- 7 南开辉, 归三荣, 王静怡, 等. 分布式电源配电网造价风险评估仿真研究[J]. 计算机仿真, 2017, 34(3):96-99
 Nan Kaihui, Gui Sanrong, Wang Jingyi, et al. Cost of the distributed power distribution network risk assessment simulation research [J]. Computer Simulation, 2017, 34(3):96-99
- 8 郭 良. 数据集中环境下云计算中私密信息安全攻防方法[J]. 科学技术与工程, 2017, 17(24):242-246
 Guo Liang. Data set in the cloud computing under the environment of private information security defense method research [J]. Science Technology and Engineering, 2017, 17(24):242-246
- 9 郝丽萍, 张容波, 任永伟, 等. 基于风险评估方法的综合预警系统设计[J]. 电子设计工程, 2018, 26(3):138-141
 Hao Liping, Zhang Rongbo, Ren Yongwei, et al. Design of comprehensive early-warning system based on risk assessment[J]. Electronic Design Engineering, 2018, 26(3):138-141
- 10 高志方, 盛冠帅, 彭定洪. 妥协率法在信息安全风险评估中的应用[J]. 计算机工程与应用, 2017, 53(23):82-87
 Gao Zhifang, Sheng Guanshuai, Peng Dinghong. Information security risk assessment method based on compromise rate method [J]. Computer Engineering and Applications, 2017, 53(23):82-87
- 11 周才学. 几个签密方案的密码学分析与改进[J]. 计算机工程与科学, 2016, 38(11):2246-2253
 Zhou Caixue. Cryptanalysis and improvement of some signcryption schemes[J]. Computer Engineering and Science, 2016, 38(11):2246-2253
- 12 吴 广, 孙 杨, 闫春香, 等. 无线传感器网络密钥管理技术在空间网络中的应用研究[J]. 计算机测量与控制, 2017, 25(9):307-310
 Wu Guang, Sun Yang, Yan Chunxiang, et al. Research on application of wireless sensor network key management technology in space networks[J]. Computer Measurement & Control, 2017, 25(9):307-310
- 13 王 娇, 范科峰, 莫 珮. 基于模糊集和 DS 证据理论的信息安全风险评估方法 [J]. 计算机应用研究, 2017, 34(11):3432-3436
 Wang Jiao, Fan Kefeng, Mo Wei. Method for information security risk assessment based on fuzzy set theory and DS evidence theory [J]. Application Research of Computers, 2017, 34(11):3432-3436
- 14 Wangen G. Information security risk assessment: A method comparison[J]. Computer, 2017, 50(4):52-61
- 15 周景贤, 王帅卿, 韩迎亚, 等. 基于资产相关性的信息系统安全评估模型[J]. 计算机工程与设计, 2017, 38(7):1691-1696
 Zhou Jingxian, Wang Shuaiqing, Han Yingya, et al. Model of information system security evaluation based on assets association degree [J]. Computer Engineering and Design, 2017, 38(7):1691-1696
- 16 石红岩, 王江涛. 有限域上多变量线性代数方程求解密码学分析[J]. 科技通报, 2017, 33(4):195-198
 Shi Hongyan, Wang Jiangtao. Cryptanalysis of multivariate linear algebraic equations in finite fields[J]. Bulletin of Science and Technology, 2017, 33(4):195-198
- 17 Basallo Y A, Senti V E, Sanchez N M. Artificial intelligence techniques for information security risk assessment [J]. IEEE Latin America Transactions, 2018, 16(3):897-901

Privacy Information Security Risk Assessment Method Based on Cryptography Theory

XU Qin-bai, WANG Cai-fen*

(College of Computer Science & Engineering Northwest Normal University, Lanzhou 730070, China)

[Abstract] In order to solve the problem that traditional methods do not consider the inaccuracy of the evaluation results of the prevention and control measures against private information, the risk assessment method of private information security is studied by cryptography theory. On the basis of calculating the risk value with the asset-threat-vulnerability as the core, the function of security prevention and control measures is introduced to analyze. According to the relevant principles, the hierarchical risk assessment index system of private information security was established, and the weight of each evaluation index was calculated by entropy coefficient. The risk value was calculated without considering the preventive measures, and the risk value was calculated after the privacy information security was protected by cryptography theory. Combining the two, the risk value of privacy information was obtained after considering the preventive measures under cryptography theory to realize the risk assessment of privacy information security. The results show that the proposed method can effectively realize the risk assessment of private information security, and the risk assessment results of the proposed method are accurate and reasonable. It can be seen that the proposed method is accurate in evaluating performance.

[Key words] cryptography theory private information security risk assessment methods