计算机网络软件的威胁模型

王　晖

哈尔滨信息工程学院　黑龙江　哈尔滨　150000

摘　要： 本文强调了识别计算机网络信息安全威胁的问题。研究的目的是增加已识别威胁的数量。首先，对用于识别威胁的计算机网络模型进行了分析，以及建立计算机网络威胁模型的方法。突出了需要纠正的缺陷。基于属性元图的数学工具，开发了一种计算机网络模型，可以描述计算机网络的软件组件及它们之间的所有可能连接。基于元图的基本操作，开发了一种计算机网络软件安全威胁模型，可以编制计算机网络软件完整性和保密性威胁清单。与考虑的类似物相比，这些清单包括更多的威胁。

关键词：计算机网络模型；威胁模型；威胁分类

The Threat Model of Computer Network Software

Wang Hui

Harbin Institute of Information Engineering Heilongjiang Harbin 150000

Abstract: This article emphasizes the issue of identifying computer network information security threats. The purpose of the study is to increase the number of identified threats. Firstly, an analysis was conducted on the computer network models used to identify threats, as well as methods for establishing computer network threat models. Highlighted the deficiencies that need to be corrected. A mathematical tool based on attribute metagraphs has been developed to describe the software components of a computer network and all possible connections between them. Based on the basic operations of metagraphs, a computer network software security threat model has been developed, which can compile a list of threats to the integrity and confidentiality of computer network software. Compared to the considered analogues, these lists include more threats.

Keywords: Computer network model; Threat model; Threat classification

一、序言

从计算机网络出现并广泛分布到今天，为确保计算机网络安全的问题并没有失去其相关性。因此，根据 Positive Technologies 的一项研究，2022 年，将计算机网络安全问题作为外部渗透测试的一部分，92% 的公司的网络周长被突破。与此同时，技术也在不断发展。新型威胁出现，计算机网络的安全正在演变为物联网的安全。

提供安全保障过程中的一个重要步骤是确定相关威胁的清单。然而，在确定相关性之前，有必要编制最广泛的威胁列表，以识别威胁。

网络安全问题对大公司和小型组织都是有关联的。所以，分配给安全的资源显然会有所不同。这不仅影响了技术设备可能产生的成本，还影响了组织可以雇佣的专业人员的资质。专业水平以及专家在利用现有方法构建信息系统威胁清单时的主观意见，都会显著影响结果。

什么是紧迫的任务？就是一个紧迫的任务是制定一种有效的方法论，用于编制信息安全威胁清单，将最大程度地减少专业水平和专家主观意见的影响。这项研究是托木斯克控制系统和无线电电子大学开展的综合评估信息系统安全方法的一部分。

这篇论文讨论了识别计算机网络软件安全威胁的问题。研究的目的是增加已识别威胁的数量。与此同时，确定威胁的相关性以及进一步的风险分析问题仍不在本工作的范围之内。为了实现这一目标，有必要：

1. 分析主题领域的现状：计算机网络模型和建立威胁模型的方法，用于编制威胁列。

2. 开发一个计算机网络模型，该模型允许在足够详细的级别上描述系统的结构，以编制威胁清单。

3. 开发一个考虑到最大威胁数量的计算机网络威胁模型。

对于计算机网络，我们指的是局域网，它是一种在子网、网络节点和安装在其上的软件之间提供数据交换的系统。

二、相关操作

建立威胁模型有许多方法。指出，在威胁建模中，有一些技术集中在攻击者、资产或软件上。这包括 STRIDE 威胁模型、最初由 B. Schneier 提出的攻击树、攻击库和隐私工具。作者们处理了威胁分类问题及其动机。他们将威胁分类方法分为两大类：基于攻击技术的方法和基于威胁影响的方法。

需要澄清的是，在不同作品的背景下，威胁分类和威胁建模的概念可能有所不同。分类被理解为了解已知威胁的特征和性质。威胁建模包括确定系统安全威胁清单或用于进一步风险评估和构建保护系统的信息。

此外，在威胁建模中使用了威胁分类方法，这是合理的。如果有分类，专家更容易在各种现有威胁中导航。这种威胁建模方法被称为高级方法。另一方面，仅使用分类很难获得一份详细的威胁清单，在此基础上可以建立保护系统的结构。这种方法的例子可以在和中考虑。

低级别方法是那些详细描述威胁的方法。这种方法可以基于攻击清单或攻击场景清单的使用。一些方法可以归结为分析系统中漏洞的利用。

在中，提出了一种具有高级别和低级别方法迹象的威胁分类。这项工作旨在描述威胁的阶级影响，而不是威胁影响，因为威胁会随着时间的推移而变化。然而，对于其在实践中的有效应用，还没有足够的形式化。

许多方法的问题是缺乏形式化，这导致了它们对所产生的威胁列表的模糊解释和主观性。有些作品使用了图论的数学工具，但它们旨在将攻击的描述形式化，而不是威胁本身。一些工作旨在描述攻击者，不允许确定威胁列表。

另外，有必要提及在构建威胁模型时经常在实践中使用的威胁、攻击和漏洞数据库，如 *ATT&CK* 矩阵和俄罗斯联邦安全技术委员会的信息安全威胁数据库。结合研究的具体情况，将工作结果与其中提到的威胁列表进行了详细比较。

在分析建立信息系统安全，特别是计算机网络安全威胁模型的方法时，发现了以下缺点：

1. 一些威胁模型包含攻击者模型的元素，或者攻击者模型直接影响威胁列表的形成。

2. 在一个级别的威胁模型中，可能有对威胁的一般描述，也可能有对特殊情况的描述。

3. 不分为针对系统的威胁和针对信息的威胁。

4. 威胁清单的构建是基于信息安全专家的主观意见

所有模型的主要缺点是，它们都没有明确描述对信息系统的威胁。所有的注意力都集中在对信息系统中处理的信息的安全威胁上。

每个考虑的模型都可以考虑到另一个模型中没有描述的某些威胁。

此外，在许多考虑的模型中，没有数学形式化，也就是说，威胁是通过口头描述来呈现的。所考虑的系统威胁的识别顺序由一般说明给出，没有对行动进行逐步描述。这往往导致专家对同一技术的解释不同，此外，专家往往与组织没有直接关系，这在形成威胁模型时会带来额外的不准确之处。

现有方法的另一个缺点是缺乏对威胁分类的理由，因此也缺乏对拟议分类的完整性的理由。

通过分析建立计算机网络模型的方法，我们可以得出结论，在它们的帮助下，不可能详细描述信息系统中的对象是什么(即描述它们的参数)，也不可能描述它们如何相互作用。为了更全面地描述计算机网络信息安全面临的威胁，计算机网络的模型应满足以下要求。有必要考虑：

1. 计算机网络软件的层次结构。

2. 两个元素之间存在若干连接的可能性。

3. 元素及其之间的连接都有参数。

三、方法

(一) 计算机网络模型

基于属性元图的计算机网络模型允许描述计算机网络的软件组件以及它们之间的所有可能连接。该研究仅考虑计算机网络的软件元素(计算机网络软件组件和应用程序) 及其之间的联系。这种情况下的软件包括应用程序、系统和网络软件。中采用了类似的方法对系统元素进行分类。链接不仅隐含在位于同一级别的元素之间，还通过指示一个元素在另一个元素中的嵌套来实现。也就是说，应用软件在操作系统中操作，操作系统是系统软件。反过来，操作系统在通过网络软件实现的局域网(或子网) 的框架内运行。因此，计算机网络软件分为三个层次。为了方便起见，这些级别被指定为应用程序级别、操作系统级别和网络级别。

作为实现模型的数学工具，选择了属性元图。元图包含并协调了系统的两个主要特性：统一性(一组相互关联的元素) 和可分割性(系统的每个元素也是一个系统)。在这方面，可以将子系统与系统区分开来。这允许在需要时将重点放在系统或其子系统上。

嵌套在 n 个深度级别的属性元图表示为有序对：

$G = (X, E)$，

其中 G 是嵌套在 n 个深度级别上的属性元图；$X = \{xi\}$，$i = 1$，n 是非空有限顶点集；$E = \{ek\}$，$k = 1$，m 是非空的有限边集。

还有一些函数指示元图的顶点和边的嵌套：

$f_1^l : g_1^l(x_1^l, e_1^l) \to x_2^\rho$，$f_2^\rho : g_2^\rho(x_2^\rho, e_2^\rho) \to x_3^m$，…，$f_{n-1}^t : g_{n-1}^t(x_{n-1}^t, e_{n-1}^t) \to x_n$，

其中 l，p，r，..，t 是适当级别的顶点和边的数量。

属性元图的顶点和边有许多属性表征：

$x_i = \{atr_j\}$，

$ek = \{atr_1\}$，

其中 x；是元图的一个顶点，x； $\in X$；e；是元图的边，

e； $\in E$；atr；and $atrh$ 分别是顶点和边的属性。

因此，计算机网络应用程序的元素和元素之间的连接由以下对称集合表示：

$X_1 = \{x_1^k\}$，$k = \overline{1, q}$ 是一组应用程序；

$X_2 = \{x_2^l\}$，$l = \overline{1, r}$ 是一组操作系统；$X_3 = \{x_3^m\}$，$m = \overline{1, s}$ 是一组网络结构；

$E_1 = \{e_1^n\}$，$n = \overline{1, t}$ 是应用程序之间的一组连接，在一组 Xi 上定义；

L 是操作系统之间的一组连接，在一组 Xz 上定义；

$E_3 = \{e_3^p\}$，$p = \overline{1, v}$ 是网络之间的一组连接，在一组 X_3 上定义 .

整个计算机网络可以表示为以下属性元图，或六个值的有序序列：

$x_i^o = \{atr_a\}$，

$G = (X_1, X_2, X_3, E_1, E_2, E_3)$.

此外，引入了一条规则，即在第 i 级的两个元素之间存在链路，当且仅当位于第 i 级对象所属的更高级别的所有元素之间存在链接。这意味着，只有当相应的操作系统也互连时，安装在不同操作系统上的应用程序才能互连。同样，不同网络中的操作系统只有在这些网络也相互连接的情况下才能相互连接。

通过使用所开发的模型，可以在系统结构的设计阶段考虑要素的特征及其之间的关系，以满足信息安全工具功能的要求。

（二）威胁模型

所提出的威胁分类方法和开发的威胁模型基于元图上的基本运算[37]。如前所述，计算机网络被认为是相互作用的元素（图的顶点）和它们之间的链接（图的边）的结构。威胁被理解为未经授权对计算机网络结构的更改（图）。

在这个阶段，有必要指出，该研究只考虑对系统安全的威胁，而不是信息。同时，以侵犯财产对威胁的分类为基础：机密性、完整性和可用性。不考虑对系统可用性的威胁，因为当将对信息安全和系统安全的威胁列表组合在一起时，这些威胁将重合。因此，考虑了对计算机网络软件的完整性和机密性的威胁。

属性元图的基本操作包括添加顶点或边、删除顶点或边以及更改顶点或边属性[38]。

基于此，提出了以下几类对计算机网络完整性的威胁：

1. 元素替代的威胁 —$Csix$

2. 链接替换的威胁 —$Cs1E$

3. 元素移除的威胁 —C_2x

4. 链接删除的威胁 —$Cs2E$

5. 元素添加的威胁 —Cs_3x

6. 添加链接的威胁 —$Cs3E$

7. 元素设置更改的威胁 —$Cs4X$

8. 链接设置更改的威胁 —$Cs4E$

元素或链接移除的威胁的特征在于从集合 X 移除顶点或边；或 Ej。因此，对于一组应用程序，其特征如下：

$G' = (X_1, Xz, Xg, E_1, E_2, E_3)$，

其中 X_1 是一组应用程序； x 是一个远程应用程序，并且：$x_1^k \in X_1$

元素或链接添加的威胁的特征在于添加来自集合 X 的顶点或边；或 E;，因此，对于一组应用程序，其特征如下：

元素或链接替换的威胁的特征在于分别从集合 Xi 或 Ej 中移除顶点或边， 并添加顶点或边，而不是删除的顶点或边。

$G'' = (X_1 \cup x_1^{k'}, X_2, X_3, E_1, E_2, E_3)$

元素或链接设置更改的威胁是通过更改的属性来实现的：

$atr_a := atr'_a$

以下威胁类别被提议作为计算机网络机密性威胁的分类：

1. 元素名称泄露的威胁 —Ks_1x

2. 链接名称泄露的威胁 —$KsiE$

3. 元素设置泄露的威胁 —$Ks2x$

4. 链接设置泄露的威胁 —Ks_2E

在图论中，计算机网络的保密威胁被描述为受保护元素集与已知元素集的交集，这些受保护元素的信息应该被隐藏。因此，关于应用程序名称的信息泄露（泄漏）的威胁的特征在于集合 Xi 与集合 Ji 的交集：

$G' = (X_1 \cap J_1, X_2, X_3, E_1, E_2, E_3)$

其中 $X_1 \cup J_1 = \{x_1^k \mid x_1^k \in X_1 \wedge x_1^k \in J_1\}$；$x_1^k$是属于集合 $X1$ 的元素；Xi 是一组需要保护的应用程序；Ji 是一组元素众所周知的应用程序。

这项研究的结果是一个计算机网络威胁模型，它集成了 Ks 和 Cs 类威胁：

Ts = KsUCs

其中 Ks 是对计算机网络元件的机密性的威胁；Cs 是对计算机网络元件完整性的威胁。

同时，12 个威胁类别中的每一个都包含三种类型的威胁：应用层的威胁、操作系统层的威胁和网络层的威胁。总共获得了 36 种类型的计算机网络软件信息安全威胁。

在使用属性元图的基本运算来确定威胁类别的基础上，可以对所提出的计算机网络软件安全威胁分类的完整性进行假设。

四、论述

以下是本文中确定的尝试类型和尝试类型的比较，后者使用了类似的方法对系统元素进行分类。区分了四个级别的系统元素：物理层、网络层、操作系统(OS) 层和应用层。在比较中没有考虑与本文中建立的限制有关的物理层。以下威胁被列为对软件的威胁：

· 网络层：隔离设备的可用性，拦截网络流量，修改网络流量 .

· OS 层：安装恶意软件，破坏系统进程和服务的稳定性，影响信息资源 .

· 应用层：禁用应用程序，影响应用程序的信息资源，修改应用程序的操作 .

其中一些威胁显然是对信息的威胁，因此不在比较中考虑。作者模型的威胁等级线与计算机网络软件级别列的交叉点表明了已识别的威胁类型。标记的单元格意味着发现了与此类型相关的系统安全威胁。未标记的单元格表示未检测到可归因于此类型的威胁。

提供的信息表明，所提出的模型描述的威胁类型明显多于所考虑的对应模型。然而，有些方法允许专家在审查中添加其他威胁，这使得比较不正确。为了进行详细的比较，我们从俄罗斯 FSTEC 的安全威胁数据库中选择了一个威胁列表。

在比较过程中，所有 213 个信息安全威胁都按暴露对象进行了分类。由于数据库将威胁定义为侵犯信息的机密性、完整性和可用性，因此很难识别其中对信息系统的威胁。如果威胁的描述中明确表明它侵犯了系统的任何属性，则将威胁归因于对系统的威胁。描述中的威胁意味着由于访问系统而侵犯信息属性，被视为威胁信息。结果，识别出 68 个信息系统安全威胁。所有这些威胁都与威胁模型开发过程中确定的威胁类型相关。

根据比较结果，发现所提出的建立威胁模型的方法允许信息保护专家在建立信息保护系统时考虑比使用其他方法时多 11 种类型的信息安全威胁。根据作者的分类，总共确定了 36 种对系统机密性和完整性的威胁。

这项工作中提出的方法的最早版本之一是用于编制能源资源商业核算自动化系统的威胁列表。因此，编制了一份对系统完整性构成 70 种威胁的清单。在软件和硬件层面考虑了三种主要类型的系统要素及其之间的联系的威胁。使用作者的方法和模型获得的列表比客户专家之前编制的列表多 18%(59 个对系统完整性的威胁)。

应该指出的是，形式化也有一些缺点。首先，形式化模型的复杂性可以缩小可以应用该模型的人的圈子。其次，使用开发的形式化模型编制威胁列表可能需要专家花费大量时间，尤其是对于包括数十个和数百个元素的大型计算机网络。然而，如果所提出的模型在软件工具中实现，则上述两个缺点都无关紧要。模型的形式化允许对编制威胁列表的过程进行算法化。目前，正在开发软件工具的概念。假设专家的任务是通过指定元素列表及其之间的关系来编译计算机网络模型。此外，还将自动编制威胁列表。

五、结论

分析了主题领域的现状 —— 用于识别威胁的计算机网络模型，以及建立计算机网络威胁模型的方法：

在属性元图的数学装置的基础上，开发了一个计算机网络模型，该模型允许描述计算机网络软件组件(应用程序、系统和网络软件) 及其之间的所有可能连接(网络协议、驱动程序等)

基于元图的基本运算，开发了一个计算机网络软件安全威胁模型，该模型可以编译计算机网络软件完整性和机密性威胁的完整列表。

在这项工作的框架内没有考虑威胁的相关性，然而，应该指出的是，增加一个有必要引入保护机制的威胁，已经足以成为考虑扩大威胁清单的充分理由。

参考文献：

[1] Hambling Brian, Hambling Brian, Morgan Peter, Samaroo Angelina, Thompson Geoff, Williams Peter. Software Testing: An ISTQB-BCS Certified Tester Foundation guide - 4th edition [M]. BCS Learning & Development Limited, 2019: 400.

[2] 张建忠 . 计算机网络技术与应用 [M]. 北京：清华大学出版社，2019：9-11.

[3] 马利 . 计算机网络安全 [M]. 北京：清华大学出版社，2021：9-11.

[4] Pan, J.; Zhuang, Y. PMCAP: A Threat Model of Process Memory Data on the Windows Operating System. Secur. Commun. Netw. 2017. [CrossRef]

[5] Internet Security Threat Report (ISTR) 2019. Symantec. Available online: https://www.symantec.com/security-center/threat-report (accessed on 29 October 2019).