第三章 恶意软件检测

概述

- 恶意软件（Malware）已成为网络空间安全（Cyber Security）的主要威胁之一，它在未经授权的情况下，在系统中进行安装、执行，以达到不正当的目的。广义地讲，恶意软件又称为恶意程序（Malicious Program）或恶意代码（Malicious code）。

概述

- **恶意软件的表现形式**

- 恶意软件的早期表现形式主要是计算机病毒。随着信息技术的不断发展以及互联网的广泛应用，恶意软件呈现出了形式多样化的趋势。
- 恶意软件通常可以表现为计算机病毒（Virus）、蠕虫（Worm）、特洛伊木马（Trojan Horse）、后门程序（Backdoor）、RootKit、“间谍软件”（Spyware）、“垃圾信息发送软件”（Spamware）、“垃圾广告软件”（Adware）、恶意移动代码（Malicious Mobile Code）、组合恶意代码（Combination Malware）等形式。

概述

- **恶意软件的危害**

- 恶意软件的危害性主要体现在窃取信息、泄露隐私、破坏数据、损害系统、消耗资源等方面。在恶意软件数量大规模增加的同时，其传播速度也急剧加快，这给恶意软件检测技术带来了新的难题。

目录

恶意软件检测技术

1. 恶意软件检测技术的发展
2. 常用恶意软件检测技术
3. 恶意软件特征提取技术

- **恶意软件检测技术**是反恶意软件技术的首要技术，它旨在对大量的文件特征数据进行分析，从而判别被分析的文件是否为恶意软件，它的准确性是彻底清除恶意软件、消除恶意软件危害的关键。

恶意软件检测技术的发展

- **计算机病毒扫描技术**

- 在恶意软件发展的早期，计算机病毒爆发后，专业人员获取病毒样本文件，根据经验提取特征码，然后将特征码发布给用户，用户的计算机扫毒引擎根据特征码与计算机中文件信息进行比对，达到检测出恶意软件的目的。

恶意软件检测技术的发展

- **计算机病毒扫描技术**
  - **优点**
    - 准确率很高，可靠性好，适用于早期小规模恶意软件
  - **缺点**
    - 提取特征码的专业人员需具有丰富的经验，特征码提取耗力耗时，病毒清除的周期长，无法检测到变种恶意软件、多态恶意软件、新型恶意软件等

恶意软件检测技术的发展

- **静态广谱特征扫描技术**

- 该技术可以检测到变种的恶意软件。它对变种恶意软件进行分类，将若干相似的变种恶意软件归为一类，并分析出它们共有的恶意软件特征码，即广谱恶意软件特征码，恶意软件检测工具可以利用这个广谱恶意软件特征码检测出变种病毒。

恶意软件检测技术的发展

- **静态广谱特征扫描技术**
  - **优点**
    - 不但可以检测出固定特征码的恶意软件，还可以检测出相关特征码的变种恶意软件
  - **缺点**
    - 特征码判定方法存在不确定性，由此会带来一定的误报率，从而导致反恶意软件的工具将正常的文件当成恶意软件进行清除

恶意软件检测技术的发展

- **动态仿真跟踪技术**

- 计算机网络的发展和应用的丰富急剧加大了恶意软件的规模和传播速度。为了进一步检测多态甚至新型恶意软件，并提高检测恶意软件的自动化程度，研究人员研制出了动态仿真跟踪技术。
- 这种恶意软件检测技术监视系统中进程的运行方式，并与正常软件的运行方式进行对比，如果不一致，则判别为可疑软件。

恶意软件检测技术的发展

- **动态仿真跟踪技术**
  - **优点**
    - 不受恶意软件特征码的约束，能够检测出变种、多态和新型恶意软件
  - **缺点**
    - 占用大量的系统资源，并且存在一定程度的误判

恶意软件检测技术的发展

- 为了进一步遏制恶意软件的肆意发展，人们也陆续研究出了智能检测、“云安全”等恶意软件检测及其相关的新技术。

常用恶意软件检测技术

- **特征码检测技术**

- 特征码检测技术依赖领域专家的行业经验和个人能力提取恶意软件的特征码，让该特征码唯一性地映射到对应的恶意软件。
- 特征码检测技术的前提是必须先捕获恶意软件样本，捕获样本的常见方法有用户上报、蜜罐技术、定向采集等，然后根据恶意软件样本进行特征码抽取。

常用恶意软件检测技术

- **特征码检测技术**
  - **优点**
    - 准确快速检测恶意软件，可识别恶意软件的名称，误报率低，检测结果完全可以用于恶意软件的清除处理
  - **缺点**
    - 只能查找已知的、被彻底研究过的恶意软件，不能检测变种及未知的恶意软件，必须不断更新版本

常用恶意软件检测技术

- **校验和技术**

- 该技术采用文件的校验和作为检测恶意软件的依据，在系统中建立新文件时，计算并保存正常文件的校验和。在文件使用时，计算文件当前的校验和，并将其与先前的校验和进行比较，如果不一致，判断该文件感染了恶意软件。

常用恶意软件检测技术

- **校验和技术**
  - **优点**
    - 实现方法简单，可以发现已知和新型的恶意软件，有效检测恶意软件给宿主文件带来的细微变化
  - **缺点**
    - 不能识别恶意软件的种类和名称，对文件内容的变化太敏感从而导致误报，无法检测出隐蔽性恶意软件

常用恶意软件检测技术

- **行为分析技术**

- 采用行为特征序列来作为判别恶意软件的依据，根据领域专家多年的经验，找出恶意软件的一些共通性行为，建立行为序列特征库。该技术在检测恶意软件时，监测程序运行过程中产生的行为信息，分析程序的执行流程及其对系统的影响，构建程序行为特征序列，并将该行为序列与特征库进行比较，如有一致，则判断正在执行的程序为恶意软件。

常用恶意软件检测技术

- **行为分析技术**
  - **优点**
    - 检测出已知的恶意软件，准确地检测出未知的多数恶意软件
  - **缺点**
    - 需占用大量的系统资源，降低了检测恶意软件的效率，技术实现较难，不能识别恶意软件的名称，可能导致误报

常用恶意软件检测技术

- **虚拟机技术**

- 采用程序代码虚拟CPU寄存器和硬件端口，用调试程序调入可疑恶意程序样本，将每个语句放到虚拟环境中执行，通过虚拟的内存、寄存器以及端口的变化来了解程序的执行，可以让变种病毒特别是加密病毒自动解密露出原形，而不用研究各个恶意程序的解密算法及密钥。

常用恶意软件检测技术

- **虚拟机技术**
  - **优点**
    - 能有效检测出变种恶意软件、多态恶意软件或加壳、加密的恶意软件
  - **缺点**
    - 检测速度较慢，需要占用较大的系统资源，对未被触发执行的恶意软件无能为力

常用恶意软件检测技术

- **启发式检测技术**

- 该技术采用领域专家分析的经验，建立经典指令集，如典型感染指令集、典型传播指令集、典型破坏指令集等，对每个经典指令集赋以不同的权值。在检测恶意软件时，在用恶意软件特征码未查到已知恶意软件的情况下，再搜索这个指令集库，如果找到符合的记录的权值之和超过某一阈值，则会判断被检测的文件是一个恶意软件。

常用恶意软件检测技术

- **启发式检测技术**
  - **优点**
    - 能够对特征码检测技术形成补充，对于已知恶意软件的变种能达到一定的检测和防范效果
  - **缺点**
    - 该技术比较依赖专家经验，具有一定的误报率

恶意软件特征提取技术

- **恶意软件特征表达**

- 对恶意软件的特征表达通常有静态特征和动态特征两种：
  - 静态特征：不运行程序的情况下，将程序的指令、代码、控制流或其他特征抽取出来
  - 动态特征：将程序在真实环境或虚拟环境下运行起来，并监视其各种行为
- 特征表达应该的条件：
  - 特征的有效性
  - 特征提取的自动化程度
  - 检测的时空效率

恶意软件特征提取技术

- **恶意软件特征提取**

- Win API函数
- 文件字符串信息
- 文件资源信息
- 文件指令信息

恶意软件特征提取技术

- **Win API函数**

- PE文件所包含的Win API函数可以作为文件特征很好的描述。
- 输入函数是指被程序调用但其执行代码又不在程序中的函数
- 引入表则保存输入函数名和其驻留的动态链接库名字等动态链接所需的信息。

恶意软件特征提取技术

- **Win API函数**

- 从引入表中静态提取PE文件所包含的Win API函数的具体提取步骤：
- （1）检验文件是否是有效的PE。
- （2）从DOS Header定位到PE Header。
- （3）获取位于OptionalHeader数据目录地址。
- （4）转至数据目录的第二个成员，提取其VirtualAddress值。
- （5）利用上值定位第一个IMAGE_IMPORT_DESCRIPTOR结构。
- （6）检查OriginalFirstThunk值：若不为0，沿着OriginalFirstThunk里RVA值转入RVA对应的数组；否则，改用FirstThunk值。
- （7）对每个数组元素，判断其元素值的最高二进位是否为1，若是，则函数是由序数引入的，可以从该值的低字节提取序数；若不是（即元素值的最高二进位为0），则可将该值作为RVA转入IMAGE_IMPORT_BY_NAME数组，跳过Hint即为函数名。
- （8）跳至下一个数组元素提取函数名一直到数组底部（以NULL结尾）。
- （9）当遍历完一个DLL的引入函数，接下去处理下一个DLL；即跳转到下一个IMAGE_IMPORT_DESCRIPTOR并处理之，循环直到数组底部（IMAGE_IMPORT_DESCRIPTOR数组以一个全0域元素结尾）。

恶意软件特征提取技术

- **文件字符串信息**

- 文件字符串特征是指PE文件中同一字符集的连续字符序列。
- 文件字符串特征提取方法为：通过反编译PE文件，从文件头开始读取文件连续的字符，直至遇 ‘0X00’ 或字符与前面的字符序列不在同一个字符集为止，这里的字符集包括：ASCII、GB2312、GBK、Big5和Unicode等。

恶意软件特征提取技术

- **文件资源信息**

- Windows程序的各种界面称为资源。文件资源用类似于磁盘目录结构的方式保存，目录通常包含3层。
- 按照文件资源的树状结构进行相应资源信息的提取，提取的资源信息主要有：cursor、bitmap、icon、menu、dialog、stringtable、fontdirector、font、accelerators、RC_data、messagetable、groupcursor、groupicon、versioninformation、dialogdata、toolbar和unkownedresource等。

数据挖掘在恶意软件检测中的应用

- **基于分类方法的恶意软件检测**
- **基于聚类分析方法的恶意软件归类**
- **基于数据挖掘技术的钓鱼网站检测**

- 目前，研究人员将多种数据挖掘方法和机器学习技术用于检测恶意软件，比较成熟的技术有分类技术、聚类技术等。这些技术突破传统恶意软件检测技术的弊端，在分析海量变种甚至未知样本、智能检测、提高检测的速度和准确率等方面，对传统的恶意软件检测技术进行了大力改进，并取得了良好的成效。

基于分类方法的恶意软件检测

- **分类技术是数据挖掘中的一个重要任务**

- 基于分类技术的恶意软件检测采用了分类方法的基本原理，它对已知恶意软件和正常文件样本数据进行学习，采用合适的分类算法构建恶意软件的分类模型，然后通过这个分类模型实现对未知文件进行检测，判断其是否为恶意软件。

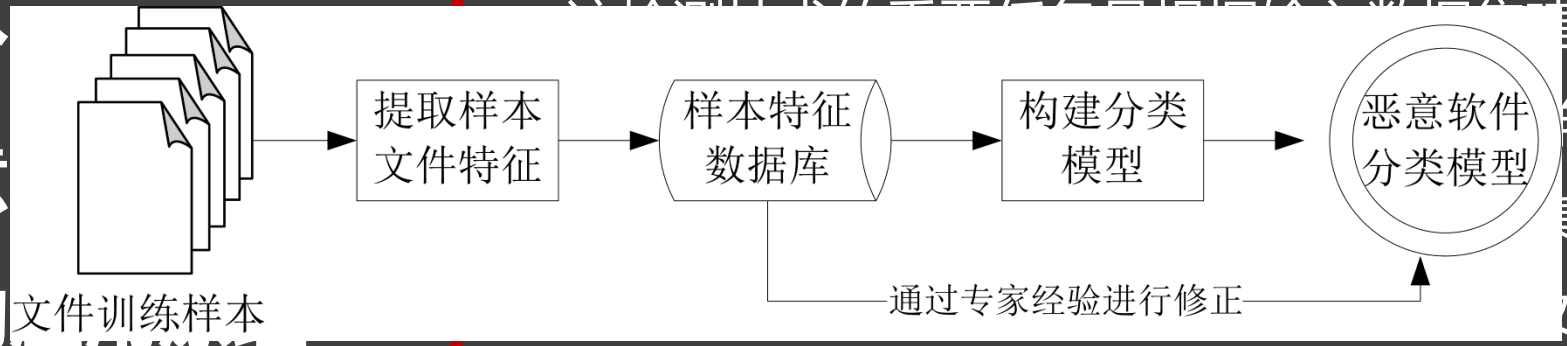
基于分类方法的恶意软件检测

- **分类方法在恶意软件检测中的应用原理**

- 该检测技术的重要任务是根据输入数据集建立用于检测恶意软件的分类模型，输入数据是文件样本数据的集合，它把文件样本数据分类为训练数据集和检测数据集，其中，将表示已知恶意软件和正常文件的文件样本数据作为训练数据集，将待检测的未知文件样本数据作为检测数据集。
- 该检测过程包含两个步骤：训练恶意软件分类模型、检测恶意软件。

基于分类方法的恶意软件检测

- 分
意
的



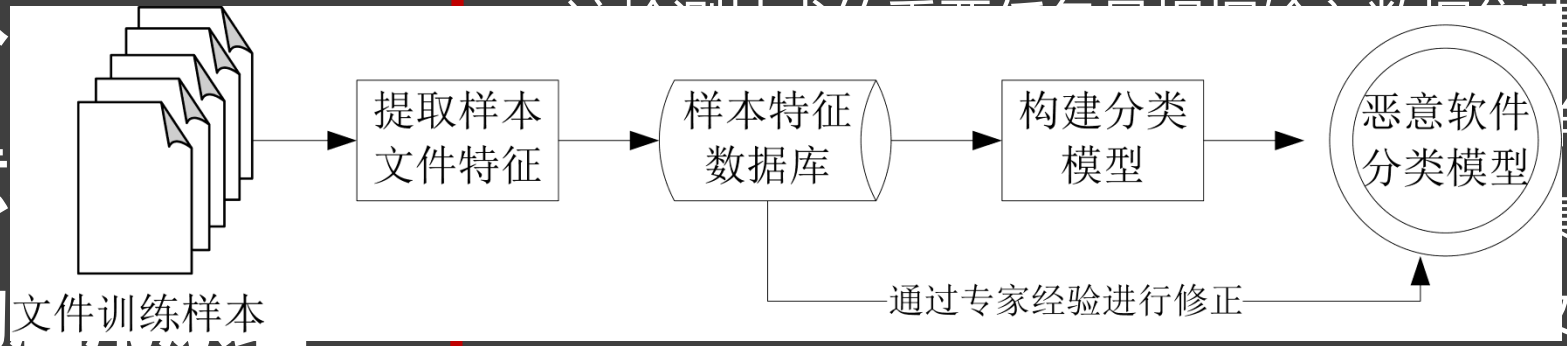
建立用于检
样本数据的
集和检测数
文件的文件

样本数据作为训练数据集，将待检测的未知文件样本数据作为检测数据集。

- 该检测过程包含两个步骤：训练恶意软件分类模型、检测恶意软件。

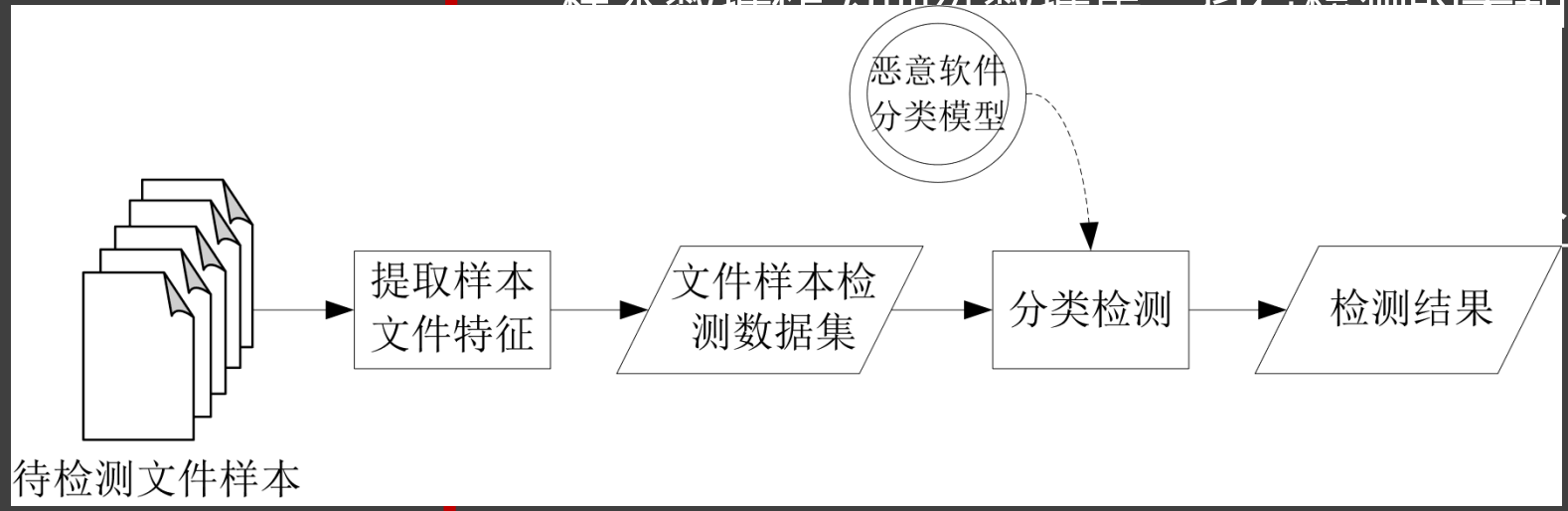
基于分类方法的恶意软件检测

- 分
意
的



建立用于检
样本数据的
集和检测数
文件的文件

样本数据作为训练数据集，将待检测的未知文件样本



类模型、

基于分类方法的恶意软件检测

- **决策树分类方法在恶意软件检测中的应用**

- 决策树（Decision Tree）分类方法可以从一组无次序、无规则的训练样本数据中学习出分类规则。一棵决策树含有三种结点：根结点、内部结点（非终止结点）、叶结点（终止结点），它采用自顶向下的递归方式，在决策树的内部结点进行属性值的比较并根据不同属性判断从该结点向下的分支，从根结点到叶结点对应着一条分类规则，整棵决策树对应着一组分类规则。决策树构建技术可以通过大量的已知恶意文件样本快速地建立恶意软件分类模型，同时，决策树可以在庞大的未知文件样本中构建判定规则。基于决策树的以上特点，它已被较好地应用到恶意软件检测中。

基于分类方法的恶意软件检测

- **贝叶斯分类方法在恶意软件检测中的应用**

- 贝叶斯分类器是数据挖掘技术中的一种分类方法，它基于贝叶斯定理（Bayes Theorem），是把类的先验知识和从数据中收集的新证据相结合的统计学分类方法。朴素贝叶斯分类器（NBC）是贝叶斯分类器的一种，在独立性假设成立的情况下，它是一种精确而又高效的概率分类方法。

基于分类方法的恶意软件检测

- **关联分类方法在恶意软件检测中的应用**

- 关联规则挖掘（Association Rule Mining）可以发现隐藏在大型数据集中的有意义的重要规律，它已经被有效地应用于分类中。关联分类的基本思想是：搜索频繁模式（属性-值对的合取）与类标号之间的强关联，即关联规则的产生和分析旨在用于分类。

基于聚类分析方法的恶意软件归类

- 聚类（Cluster）是将数据划分成有意义或有用的组（簇）的数据挖掘方法，它把数据按照相似性归纳成若干类别，同一类中的数据彼此相似，而不同类中的数据相异，聚类分析方法的这些特性使它可以应用在恶意软件的归类中。在恶意软件的归类中，一个簇就是一组传播途径、功能、内容或行为相同或相似的恶意软件集合，即一个恶意软件家族。聚类分析方法可以自动地把具有共性的恶意软件分成同一个簇，同时把差异较大的恶意软件区分开来。

基于聚类分析方法的恶意软件归类

- **层次聚类方法在恶意软件归类中的应用**

- 恶意软件特征
- 行为特征近似度计算
- 构建层次聚类关系树
- 恶意软件归类

层次聚类方法在恶意软件归类中的应用

- 恶意软件特征

网络行为特征举例

Label	MD5	P/F/R/N	McAfee	Trend
A	71b99714cddd66181e54194c44ba59df	8/13/27/0	Not detected	W32/Backdoor.QWO
B	be5f889d12fe608e48be11e883379b7a	8/13/27/0	Not detected	W32/Backdoor.QWO
C	df1cda05aab2d366e626eb25b9cba229	1/1/6/1	W32/Mytob.gen@MM	W32/IRCBot-based!Maximus
D	5bf169aba400f20cbe1b237741eff090	1/1/6/2	W32/Mytob.gen@MM	Not detected
E	eef804714ab4f89ac847357f3174aa1d	1/2/8/3	PWS-Banker.gen.i	W32/Bancos.IQK
F	80f64d342fddcc980ae81d7f8456641e	2/11/28/1	IRC/Flood.gen.b	W32/Backdoor.AHJJ
G	12586ef09abc1520c1ba3e998baec457	1/4/3/1	W32/Pate.b	W32/Parite.B
H	ff0f3c170ea69ed266b8690e13daf1a6	1/2/8/1	Not detected	W32/Bancos.IJG
I	36f6008760bd8dc057ddb1cf99c0b4d7	3/22/29/3	IRC/Generic Flooder	IRC/Zapchast.AK@bd
J	c13f3448119220d006e93608c5ba3e58	5/32/28/1	Generic BackDoor.f	W32/VB-Backdoor!Maximus

层次聚类方法在恶意软件归类中的应用

- **行为特征近似度计算**

- 以恶意软件特征之间的近似度来表征恶意软件之间的相似性。采用归一化压缩距离（NCD）来衡量两个恶意软件行为特征之间的近似度，NCD的定义如下所示。

$$NCD(x,y)=\frac{C(x+y)-\min(C(x),C(y))}{\max(C(x),C(y))} \quad (3\text{-}1)$$

- 其中，“*x*+*y*”表示特征向量*x*和*y*的关联结果，*C(x)*表示向量*x*的zlib-compressed length。

层次聚类方法在恶意软件归类中的应用

- **行为特征近似度计算**

- 采用NCD方法，计算出前述各网络行为特征之间的相似度，如下表所示。

	A	B	C	D	E	F	G	H	I	J
A	0.06	0.07	0.84	0.84	0.82	0.73	0.80	0.82	0.68	0.77
B	0.07	0.06	0.84	0.85	0.82	0.73	0.80	0.82	0.68	0.77
C	0.84	0.84	0.04	0.22	0.45	0.77	0.64	0.45	0.84	0.86
D	0.85	0.85	0.23	0.05	0.45	0.76	0.62	0.43	0.83	0.86
E	0.83	0.83	0.48	0.47	0.03	0.72	0.38	0.09	0.80	0.85
F	0.71	0.71	0.77	0.76	0.72	0.05	0.77	0.72	0.37	0.54
G	0.80	0.80	0.65	0.62	0.38	0.78	0.04	0.35	0.78	0.86
H	0.83	0.83	0.48	0.46	0.09	0.73	0.36	0.04	0.80	0.85
I	0.67	0.67	0.83	0.82	0.79	0.38	0.77	0.79	0.05	0.53
J	0.75	0.75	0.86	0.85	0.83	0.52	0.85	0.83	0.52	0.08

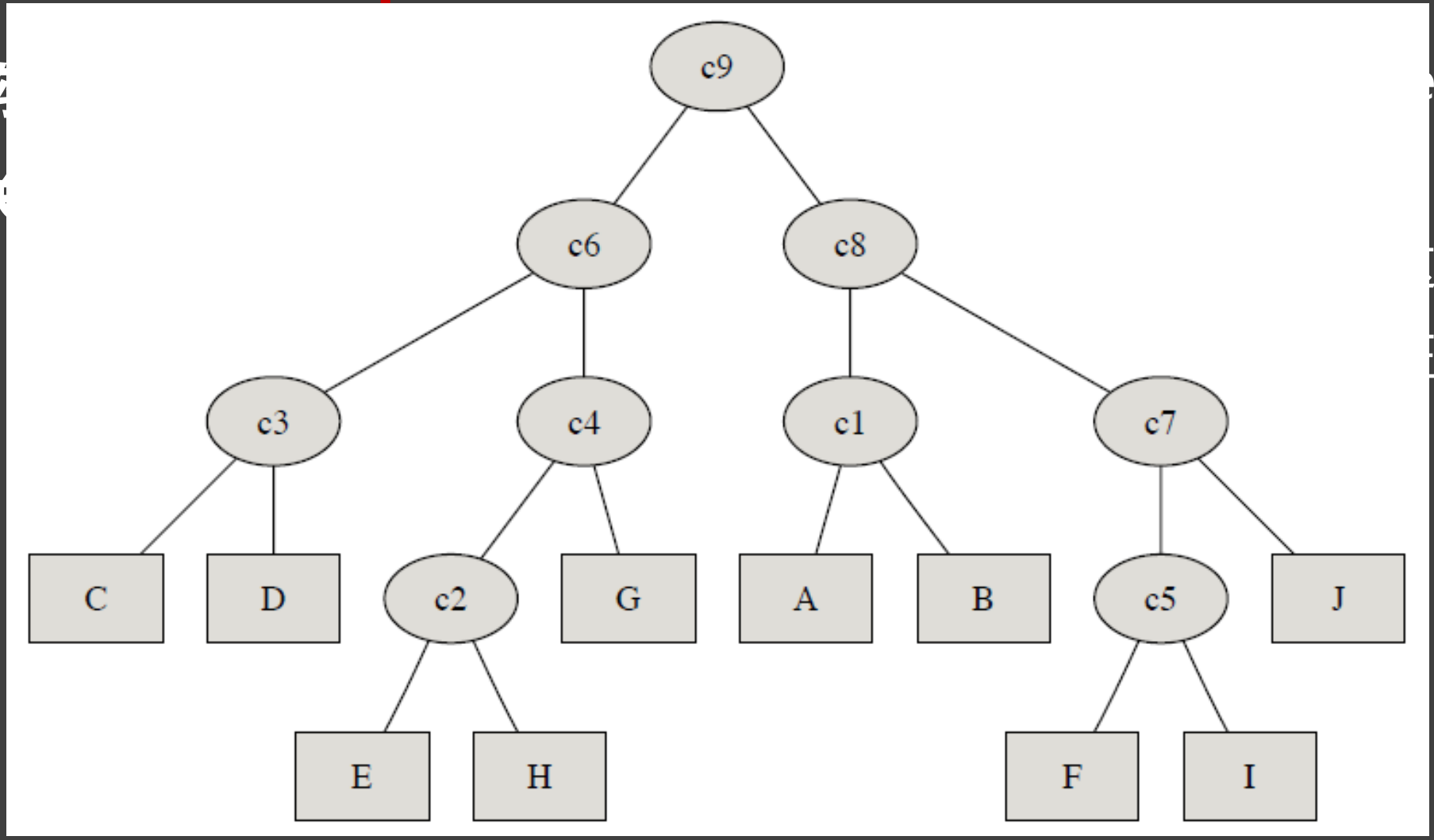
层次聚类方法在恶意软件归类中的应用

- **构建层次聚类关系树**

- 采用单连锁聚类（Pairwise Single-linkage Clustering）方法构建层次聚类关系树，该方法将两个簇的元素间的最短距离定义为这两个簇的距离。前述表中恶意软件行为特征示例的关系树如图所示。

层次聚类方法在恶意软件归类中的应用

- 构
  关



层次聚类方法在恶意软件归类中的应用

- **恶意软件归类**

- 通过计算每个簇的不一致性系数（Inconsistency Coefficient），并采用不一致性测量方法计算簇之间的距离，以此为依据，确定每个恶意软件的归类信息。示例的恶意软件列表的归类结果如图所示。

Cluster	Elements	Overlap	Example
c1	C, D	67.86%	scans 25
c2	A, B	97.96%	installs a cygwin rootkit
c3	E, G, H	56.60%	disables AV
c4	F, I, J	53.59%	IRC

基于聚类分析方法的恶意软件归类

- **加权子空间的 *k*-medoids 聚类方法在恶意软件归类中的应用**

- 提取样本文件特征
- 聚类算法的过程

加权子空间的*k*-medoids聚类方法在恶意软件归类中的应用

- **提取样本文件特征**

- 该方法提取基于函数的指令序列，作为待归类的样本文件的特征。首先，将样本文件进行反汇编，提取样本文件中所包含的所有函数，并剔除函数中的操作数，只保留汇编指令。然后，以函数为单位，将每个函数的指令序列隔指定的步长以指定的片长进行切片，统计每个文件出现的指令片段，生成一个指令片段的集合，作为样本文件的特征表征。

加权子空间的*k*-medoids聚类方法在恶意软件归类中的应用

- **聚类算法的过程**

- WKM聚类算法的主要步骤如下：
- （1）接受用户输入的分类簇数*k*，然后从所有样本文件中随机选取*k*个样本点作为*k*个簇初始中心点;
- （2）将每个维度的权值设置成1/*d*，其中*d*为样本全集的维度总数;
- （3）根据下式计算所有*k*个初始中心点以外的其它样本点与这*k*个初始中心点的差异度后，将相应的样本点划分到与之差异度最小的初始中心点所属的簇中；

$$WJD_{\mathrm{mn}} = \frac{w_{\mathrm{m}} \cdot X_m \cup w_n \cdot X_n - w_m \cdot X_m \cap w_n \cdot X_n}{w_m \cdot X_m \cup w_n \cdot X_n} \quad (3\text{-}2)$$

加权子空间的*k*-medoids聚类方法在恶意软件归类中的应用

- **聚类算法的过程**

- （4）划分结束后，划分结束后，根据式(3-1)定义式重新确定*k*个簇的中心点（即与同一个簇中所有样本距离和最小的样本点）。确定完中心点后，根据式(3-2)重新计算各个维度在各个簇中的权值。

$$w_{ij}=\begin{cases}\dfrac{\sum_{l=1}^{d}D_{il}-D_{ij}+E_{ij}}{(d-1)\sum_{l=1}^{d}D_{il}+\sum_{l=1}^{d}E_{il}}, \sum_{l=0}^{d}D_{il}>0 \\ \dfrac{1}{d}, \sum_{l=0}^{d}D_{il}=0 \wedge E_{ij}=0\end{cases} \quad (3\text{-}3)$$

加权子空间的*k*-medoids聚类方法在恶意软件归类中的应用

- **聚类算法的过程**

- 从而得到簇*i*（*i*=1,…,*k*）的权值向量如式(3-23)所示。
- （5）所有*k*个簇的权值向量更新完成之后，检查各个簇的中心点与上一次迭代的结果相比是否不再发生改变，若不再改变即收敛，则算法结束（或者对样本点的划分到达指定的迭代次数，则算法结束）,以此时所划分的*k*个簇为最后的聚类结果；否则，以新确定的*k*个中心点文件作为新的初始中心点文件，并返回以上步（3），直到算法收敛或达到指定迭代次数。

基于数据挖掘技术的钓鱼网站检测

- **钓鱼网站**

- 钓鱼网站（Phishing Site）通常指模仿真实网站地址和页面来欺骗用户的网站，它利用社会工程学手段，一般要求访问者提交账号、密码等私密信息，从而达到窃取用户信息的目的。

基于数据挖掘技术的钓鱼网站检测

- **钓鱼网站检测技术**

- 基于黑白名单的约鱼网站检测技术
- 基于页面的启发式约鱼检测技术
- 基于页面的启发式钓鱼检测技术

基于数据挖掘技术的钓鱼网站检测

- **数据挖掘在钓鱼网站检测中的应用**

- 采用一种基于关联分类的多标签分类器（Multi-label Classifier based Associative Classification，MCAC）发现钓鱼网站问题，该方法能生成其它算法无法发现的隐蔽规则，从而提高用于钓鱼网站检测的分类器的精确性。
- 采用基于MCAC策略的钓鱼网站分类规则学习含有三个步骤：规则发现、分类器构建和网站分类。

小结

- **数据挖掘技术已被应用在恶意软件检测的研究中**

- 本章首先概述了恶意软件及其危害性。
- 其次，介绍了恶意软件检测技术的发展状况、及常用恶意软件检测技术。
- 然后，重点介绍了几种数据挖掘技术在恶意软件检测中的应用。
- 其中，分类方法部分介绍了分类技术在恶意软件检测中的应用原理，决策树、贝叶斯和关联分类方法在恶意软件检测中的应用实例。聚类分析方法部分介绍了层次聚类方法和加权子空间的*k*-medoids聚类方法在恶意软件归类中的应用实例。钓鱼网站检测部分介绍了多标签关联分类方法在钓鱼网站检测中的应用实例。

Thanks!