[论文阅读] (07) RAID2020 Cyber Threat Intelligence Modeling Based on Heterogeneous GCN

《娜璋带你读论文》系列主要是督促自己阅读优秀论文及听取学术讲座，并分享给大家，希望您喜欢。由于作者的英文水平和学术能力不高，需要不断提升，所以还请大家批评指正，非常欢迎大家给我留言评论，学术路上期待与您前行，加油。

前一篇文章分享了生成对抗网络GAN的基础知识，包括什么是GAN、常用算法（CGAN、DCGAN、infoGAN、WGAN）、发展历程、预备知识，并通过Keras搭建最简答的手写数字图片生成案例。这篇文章将详细介绍北航老师发表在RAID 2020上的论文《Cyber Threat Intelligence Modeling Based on Heterogeneous Graph Convolutional Network》，基于异构图卷积网络的网络威胁情报建模。希望这篇文章对您有所帮助，这些大佬是真的值得我们去学习，献上小弟的膝盖~fighting!

Cyber Threat Intelligence Modeling Based on Heterogeneous Graph Convolutional Network

Jun Zhao[1,2], Qiben Yan[3,*], Xudong Liu[1,2,*], Bo Li[1,2,*], Guangsheng Zuo[1,2]

[1] *School of Computer Science and Engineering, Beihang University, Beijing, China*

[2] *Beijing Advanced Innovation Center for Big Data and Brain Computing, Beihang University, Beijing, China*

[3] *Computer Science and Engineering, Michigan State University, East Lansing, Michigan, USA*

原文作者：Jun Zhao, Qiben Yan, Xudong Liu, Bo Li, Guangsheng Zuo

原文标题：Cyber Threat Intelligence Modeling Based on Heterogeneous Graph Convolutional Network

原文链接：https://www.usenix.org/system/files/raid20-zhao.pdf

发表会议：RAID 2020 / CCF B

同时，本文参考了“安全学术圈”公众号文章，推荐大家关注该公众号，非常棒。

- https://mp.weixin.qq.com/s/TszbHM__hpYvdHsCoMmkUQ

> 注意，本文代码采用GPU+Pycharm实现，如果你的电脑是CPU实现，将相关GPU操作注释即可。这里仅做简单的对比实验，不进行参数优化、实验原因分析及详细的效果提升，后面文章会介绍优化、参数选择、实验评估等。

前文赏析：

文章目录

摘要

网络威胁情报（CTI，Cyber Threat Intelligence）已在业界被广泛用于抵御流行的网络攻击，CTI通常被看作将威胁参与者形式化的妥协指标（IOC）。然而当前的网络威胁情报（CTI）存在三个主要局限性：

- IOC提取的准确性低
- 孤立的IOC几乎无法描述威胁事件的全面情况
- 异构IOC之间的相互依存关系尚未得到开发，无法利用它们来挖掘深层次安全知识

本文提出了基于异构信息网络（HIN， Heterogeneous Information Network）的网络威胁情报框架——HINTI，旨在建模异构IOCs之间的相互依赖关系，以量化其相关性，对CTI进行建模和分析。

本文的主要贡献如下：

- **提出了基于多粒度注意力机制（ multi-granular attention）的IOC识别方法，可以从非结构化威胁描述中自动提取网络威胁对象，并提高准确性**
- **构建一个异构信息网络（HIN）来建模IOCs之间的依赖关系**
- **提出一个基于图卷积网络（Graph Convolutional Networks）的威胁情报计算框架来发现知识**
- **实现了网络威胁情报（CTI）原型系统**

实验结果表明，本文提出的IOC提取方法优于现有方法，HINTI可以建模和量化异构IOCs之间的潜在关系，为不断变化的威胁环境提供了新的线索。

Abstract

Cyber Threat Intelligence (CTI), as a collection of threat information, has been widely used in industry to defend against prevalent cyber attacks. CTI is commonly represented as Indicator of Compromise (IOC) for formalizing threat actors. However, current CTI studies pose three major limitations: first, the accuracy of IOC extraction is low; second, isolated IOC hardly depicts the comprehensive landscape of threat events; third, the interdependent relationships among heterogeneous IOCs, which can be leveraged to mine deep security insights, are unexplored. In this paper, we propose a novel CTI framework, HINTI, to model the interdependent relationships among heterogeneous IOCs to quantify their relevance. Specifically, we first propose multi-granular attention based IOC recognition method to boost the accuracy of IOC extraction. We then model the interdependent relationships among IOCs using a newly constructed heterogeneous information network (HIN). To explore intricate security knowledge, we propose a threat intelligence computing framework based on graph convolutional networks for effective knowledge discovery. Experimental results demonstrate that our proposed IOC extraction approach outperforms existing state-of-the-art methods, and HINTI can model and quantify the underlying relationships among heterogeneous IOCs, shedding new light on the evolving threat landscape.

> IOC（Indicator of Compromise）是MANDIANT在长期的数字取证实践中定义的可以反映主机或网络行为的技术指示器。

Ⅰ.前言

> Introduction是论文的开头，是极为重要的部分，介绍了为什么要做这份工作，建议大家仔细阅读，尤其是写英文论文的读者。因此，作者将该部分进行了详细总结。

当今社会，我们正在目睹复杂的网络威胁攻击（如0-day攻击、高级持续威胁攻击 APT）的快速增长。这些攻击可以轻易绕过传统防御，如防火墙和入侵检测系统(IDS)，破坏关键基础设施，并造成灾难。为了应对这些新出现的威胁，安全专家提出了 网络威胁情报（CTI），并包含 IOCs指标 。

与著名的安全数据库（如 CVE 、 ExploitDB ）不同，当系统遇到可疑威胁时，CTI可以帮助组织主动发布更全面和更有价值的威胁警告（例如，恶意IP、恶意DNS、恶意软件和攻击模式等）。

- http://cve.mitre.org/
- https://www.exploit-db.com/

近年来，CTI越来越多地被安全人员和行业用来分析威胁环境。原始的CTI提取和分析需要对攻击事件描述进行大量的手动检查，耗时耗力。最近提出了从非结构化安全文本中提取CTI的自动化方法，如 CleanMX 、 PhishTank 、 IOC Finder 和 Gartner peer insight ，并且都遵循OpenIOC标准，并利用正则表达式提取特定类型的IOC（如恶意IP、恶意软件、文件哈希等）。

然而，这种提取方法面临着三个主要的限制。

- 首先，IOC提取的精度低，不可避免地导致关键威胁对象遗漏。
- 其次，孤立的IOC没有全面描述威胁事件的概况，这使得CTI用户无法对即将到来的威胁获得完整的了解。
- 最后，缺乏一个有效的计算框架来有效地衡量异构IOCs之间的交互关系。

为了应对这些限制（To combat these limitations）：
本文提出了一种基于异构信息网络的威胁情报框架HINTI，来对CTI进行建模和分析。值得注意的是，HINTI提出了一种基于多粒度注意力机制的IOC识别方法，以提高IOC提取的准确性。

然后，HINTI利用HIN来建模异构IOC之间的依赖关系，这可以描述一个更全面的威胁事件。此外，本文提出了一个新的CTI计算框架来量

化IOC之间相互依赖的关系，这有助于发现新的安全信息（security insights）。

综上，本文的主要贡献总结如下：

- 基于多粒度注意力机制的IOC识别（Multi-granular Attention based IOC Recognition）
  可以从多源威胁文本中自动提取网络威胁对象，学习不同尺度的特征，提高准确率和召回率，共从非结构化的威胁描述中提取397730个IOCs。
- 异构威胁智能建模（Heterogeneous Threat Intelligence Modeling）
  使用异构信息网络来建模不同类型的IOC，引入各种元路径捕获异构IOC之间的相互依赖关系，描述更全面的网络威胁事件概况。
- 威胁智能计算框架（Threat Intelligence Computing Framework）
  提出网络威胁智能计算的概念，设计一个通用的计算框架。该框架利用基于权重学习的节点相似度来量化异构IOCs之间的依赖关系，然后利用基于注意力机制的异构图卷积网络来嵌入IOCs及交互关系。
- 威胁情报原型系统（Threat Intelligence Prototype System）
  实现了一个CTI原型系统，确定6类攻击对象之间的1262258种关系，包括攻击者、漏洞、恶意文件、攻击类型、设备和平台。

Ⅱ.背景

1.动机

本研究的主要目标是通过建模异构IOCs之间的依赖关系来解决现有CTI分析框架的局限性。举一个有趣的安全示例：

> Last week, Lotus exploited CVE-2017-0143 vulnerability to affect a larger number of Vista SP2 and Win7 SP devices in Iran. CVE-2017-0143 is a remote code execution vulnerability including a malicious file SMB.bat.

大多数现有的CTI框架可以提取特定的IOC，但却忽略了它们之间的关系，如图1所示。很明显，这些IOC无法全面了解威胁形势，更不用说量化它们的互动关系以进行深入的安全调查。

与现有的CTI框架不同，HINTI旨在实现一个CTI计算框架，它不仅可以有效提取IOC，而且还可以建模和量化它们之间的关系。

```
<? Xml version=1.0 encoding=utf-8>
  <indicator id=1a0ee12, op=OR>
    <Description>
      <Actor>Lotus</Actor>
      <Vul>CVE-2017-0143</Vul>
      <Dev>Vista SP2</Dev>
      <Dev>Win7 SP1</Dev>
      <Type>Remote code execution</Type>
      <File>SMB.bat</File>
    </Description>
```

Figure 1: An example of extracted IOCs without any relations among them.

在这里，我们使用该示例来说明HINTI是如何一步一步工作（四个步骤）。

- **(i) 首先，通过B-I-O序列标注方法对安全相关帖子进行标注，用于构建IOC提取模型。**
  其中，B-X表示X类型的元素位于片段的开头，I-X表示X类型的元素位于中间片段，O表示其他类型的非基本元素。在研究中，我们从5000个威胁描述文本中标注了3万个这样的训练样本，这些文本是用来构建我们IOC提取模型的原始材料。

Last$_{(O)}$ week$_{(O)}$, Lotus$_{(B\text{-}Attacker)}$ exploited$_{(O)}$ CVE-2017-0143$_{(B\text{-}Vul)}$ vulnerability$_{(O)}$ to$_{(O)}$ affect$_{(O)}$ a$_{(O)}$ large$_{(O)}$ number$_{(O)}$ of$_{(O)}$ Vista SP2$_{(B\text{-}Device)}$ and$_{(O)}$ Win7 SP1$_{(B\text{-}Device)}$ devices$_{(O)}$ in$_{(O)}$ Iran$_{(O)}$. CVE-2017-0143$_{(B\text{-}Vul)}$ is$_{(O)}$ a$_{(O)}$ remote$_{(B\text{-}Type)}$ code$_{(I\text{-}Type)}$ execution$_{(I\text{-}Type)}$ vulnerability$_{(O)}$ involving$_{(O)}$ a$_{(O)}$ malicious$_{(O)}$ file$_{(O)}$ SMB.bat$_{(B\text{-}File)}$.

- **(ii) 然后将标记的训练样本输入我们提出的神经网络，如图6所示，以训练提出的IOC提取模型。**
- **(iii) HINTI利用句法依赖性解析器（e.g.，主-谓-宾，定语从句等）提取IOC之间的关联关系，每个关系都表示为三元组（IOC_i、关系、IOC_j）。在此实例中，HINTI提取三元组关系如下：**
  – (Lotus, exploit, CVE-2017-0143)
  – (CVE-2017-0143, affect, VistaSP2)

> 注意，提取的关系三元组可以增量地合并到一个HIN中，以模拟IOCs之间的交互作用，从而描述一个更全面的威胁环境。图3以图形表示显示了从示例中提取IOC描述之间的交互关系，g该图表示攻击者利用CVE-2017-0143漏洞入侵VistaSP2和Win7SP1设备。CVE-2017-0143是一个涉及恶意文件“SMB.bat”的远程代码执行漏洞。与图1相比，很明显，HINTI可以描绘一个比以往方法更直观、更全面的威胁环境。在本文中，我们主要考虑6种不同类型的IOC之间的9个关系（R1~R9）（详见第4.2节）。

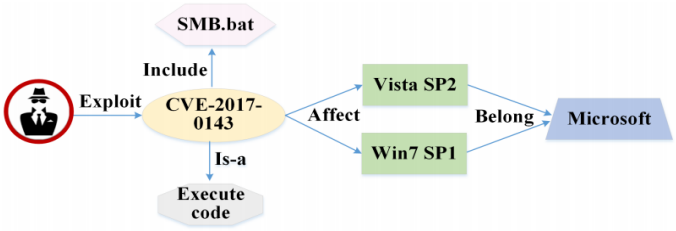


Figure 3: A miniature of a constructed CTI includes attacker, vulnerability, malicious file, attack type, device, and platform, which describes a particular threat: an attacker utilizes *CVE-2017-0143* vulnerability to invade *Vista SP2* and *Win7 SP1* devices. *CVE-2017-0143* is a *remote code execution* vulnerability that involves a malicious file *“SMB.bat"*.

- **(iv) 最后，HINTI集成了基于异构图卷积网络的CTI计算框架（见第4.3节），以有效量化IOC之间的关系并进行知识发现。**
  特别是，本文提出的CTI计算框架描述了IOC及其在低维嵌入空间（low-dimensional embedding space）中的关系，在此基础上，CTI用户可以使用任何分类（如SVM、朴素贝叶斯）或聚类算法（K-Means、DBSCAN）来获得新的威胁见解，例如预测哪些攻击者可能入侵其系统，以及在没有专家知识的情况下识别哪些漏洞属于同一类别。

2.前期工作

- Definition 1 Heterogeneous Information Network of Threat Intelligence (HINTI)
- Definition 2 Network Schema
- Definition 3 Meta-path

威胁智能的异构信息网络(HINTI)被定义为有向图 `G=(V, E, T)`，其中v表示对象，e表示链接，r表示关系类型。具有对象类型映射函数ϕ：V→M和链路类型映射函数Ψ：E→R。本文重点研究了6种常见类型，连接不同对象的链接代表了不同的语义关系。

- attacker (A)
- vulnerability (V)
- device (D)
- platform （P）
- malicious file (F)
- attack type (T)

接着采用模式描述元关系的网络架构，图4展示了网络模式（知识图谱中本体概念）和一个网络实例。比如“软件设备属于系统平台”为模式图，“Office2012属于Windows系统软件”为实例。

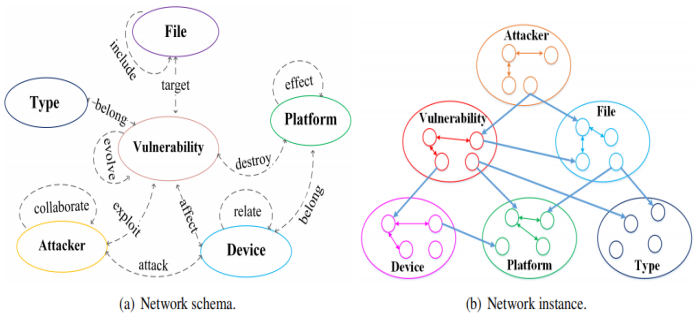


Figure 4: Network schema and instance of HIN containing 6 types of IOCs. (a): The network schema of HIN, which depicts the relationship template among different types of IOCs, such as $Device \xrightarrow{belong} Platform$. (b): An instance of network schema, which describes the concrete relationships between IOCs by following a network schema, e.g., $Office\ 2012 \xrightarrow{belong} Windows$.

最后定义元路径，指网络模式S=(N, R)的路径序列，其定义了符合关系。表1显示了HINTI中所考虑的元路径。例如，“攻击者(A)利用相同的漏洞(V)”的关系可以通过长度为2的元路径表示：

$$attacker \xrightarrow{exploit} vulnerability \xrightarrow{exploit^{-}} attacker$$

称为 $AVA^T(P_4)$ 来描述，这意味着两个攻击者利用相同的漏洞。同样， $AVDPD^TV^TA^T(P_{17})$ 描绘了IOC之间的密切关系，即“两个利用同一漏洞的攻击者入侵同一类型的设备，并最终摧毁同一类型的平台”。

Table 1: Meta-paths used in HINTI.

ID	Meta-path
P_1	Attacker-Attacker
P_2	Device-Device
P_3	Vulnerability-Vulnerability
P_4	Attacker-Vulnerability-Attacker
P_5	Attacker-Device-Attacker
P_6	Device-File-Device
P_7	Device-Platform-Device
P_8	Vulnerability-File-Vulnerability
P_9	Vulnerability-Type-Vulnerability
P_{10}	Vulnerability-Device-Vulnerability
P_{11}	Vulnerability-Platform-Vulnerability
P_{12}	Attacker-Device-Platform-Device-Attacker
P_{13}	Attacker-Vul-Device-Vul-Attacker
P_{14}	Attacker-Vul-Platform-Vul-Attacker
P_{15}	Attacker-Vul-Type-Vul-Attacker
P_{16}	Vul-Device-Platform-Device-Vul
P_{17}	Attacker-Vul-Device-Platform-Device-Vul-Attacker

Ⅲ.HINTI总体架构

HINTI作为一个网络威胁智能提取和计算框架，能够有效地从威胁描述中提取IOC，并描述异构IOC之间的关系，以揭开新的威胁见解。如图5所示，HINTI由四个主要部件组成，包括：

- 收集与安全相关的数据并提取即IOC
  使用Xpath提取安全数据（博客、安全论坛、新闻、公告），利用基于多粒度注意力机制的IOC识别方法收集信息。
- 将IOC之间的相互依存关系建模为异构信息网络
  该网络可以自然地描述异构IOC之间的相互依赖关系。比如图4显示的模型，它可以捕获攻击者、漏洞、恶意文件、攻击类型、平台和设备之间的交互式关系。
- 使用基于权重学习的相似性度量将节点嵌入到低维向量空间中
  元映射是构造HIN中IOC语义关系的有效工具。本文设计了17种元路径（见表1）来描述IOC之间的相互依赖关系，利用这些元路径，提出了一种基于权重学习的相似计算方法来将节点嵌入到这些关系，作为威胁智能计算的前提。
- 基于图卷积网络和知识挖掘来计算威胁情报
  通过图卷积网络(GCN)来量化和测量IOC之间的相关性，本文提出的威胁情报计算框架可以在更全面的威胁环境中揭示更丰富的安全知识。

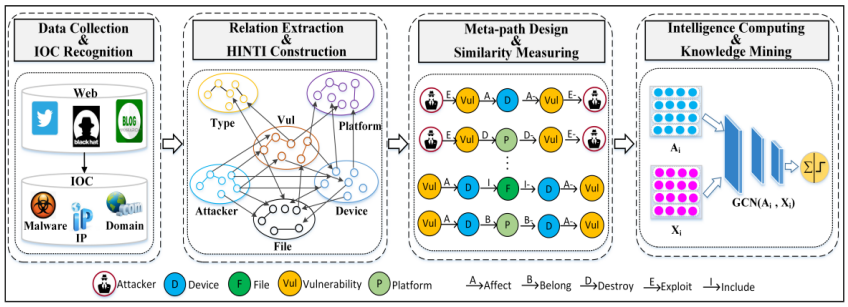


Figure 5: The overall architecture of HINTI. HINTI consists of four major components: (a) collecting security-related data and extracting threat objects (i.e., IOCs); (b) modeling interdependent relationships among IOCs into a heterogeneous information network; (c) embedding nodes into a low-dimensional vector space using weight-learning based similarity measure; and (d) computing threat intelligence based on graph convolutional networks and knowledge mining.

Ⅳ.方法论

1.基于多粒度注意力的IOC提取

近年来，BiLSTM+CRF在命名实体识别领域取得良好的性能，但不能直接应用于IOC提取，因为威胁文本通常包含大量不同尺寸和规则结构的对象。因此，本文提出一种基于多粒度注意机制的IOC提取方法，它可以提取具有不同粒度的威胁对象。

此外，它引入了具有不同粒度的新词嵌入功能，以捕获具有不同大小的IOC的特征，其模型如图6所示，利用自注意力机制来学习功能的重要性，以提高IOC提取的准确性。

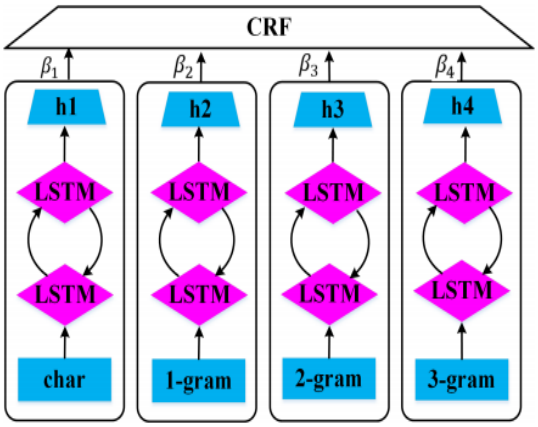


Figure 6: The framework of multi-granular IOC extraction.

由图可知，它将句子分割成了char（字符级）、1-gram、2-gram、3-gram，从而从多粒度注意力机制训练数据。LSTM计算公式如下：

$$\begin{aligned} \overrightarrow{h_i^j} &= LSTM_{forward}([e_{x_0}^j, e_{x_1}^j, \cdots, e_{x_i}^j]) \\ \overleftarrow{h_i^j} &= LSTM_{backward}([e_{x_0}^j, e_{x_1}^j, \cdots, e_{x_i}^j]) \end{aligned} \tag{2}$$

接下来是多粒度注意力机制及LSTM+CRF的计算过程。同时，本文设计了一个客观的目标函数来最大化概率p(Y|X)，以实现针对不同IOC的最高标签得分。通过求解目标函数，我们为n-gram分量分配正确的标签，根据这些标签，我们可以识别不同长度的IOC。我们基于多粒度注意力机制的IOC提取方法能够识别不同类型的IOC，其评估方法在第5部分提出。

$$\begin{aligned} argmax\ log(p(Y|X)) = argmax\ (S(X,Y) - \\ log(\sum_{\tilde{y} \in Y_X} e^{S(X,\tilde{y})})) \end{aligned} \tag{6}$$

2.网络威胁情报建模

CTI建模是探索异构IOC之间复杂关系的一个重要步骤。本文通过引入HIN，以探索不同类型的IOC之间的交互关系。为了模拟IOCs之间复杂的依赖关系，我们在6种类型的IOC之间定义了以下9种关系：

- R1：attacker-exploit-vulnerability
  攻击者利用漏洞
- R2：attacker-invade-device
  攻击者入侵设备
- R3：attacker-cooperate-attacker
  攻击者之间合作
- R4：vulnerability-affect-device
  漏洞影响设备
- R5：vulnerability-belong-attack type
  脆弱性属于攻击类型
- R6：vulnerability-include-file

漏洞包括恶意文件

- R7：file-target-device
  恶意文件针对设备
- R8：vulnerability-evolve-vulnerability
  脆弱性演化脆弱性
- R9：device-belong-platform
  设备属于平台

基于上述9种关系，HINTI利用句法依赖解析器（the syntactic dependency parser）从威胁描述中自动提取IOC之间的9种关系，每种关系用三元组（IOCi，relation，IOCj）表示。同时进一步定义表1所示的17种元路径，以调查攻击者、漏洞、恶意文件、攻击类型、设备、平台之间的相互依赖关系。通过检查17种类型的元路径，HINTI能够传达更丰富的事件上下文，并揭示异构IOC的深层信息。

3.威胁情报计算

本节说明了威胁智能计算的概念并设计了一个基于异构图卷积网络的一般威胁智能计算框架，它通过分析基于元路径的语义相似性来量化和衡量IOCs之间的相关性。在此，我们首先提供了一个基于异构图卷积网络的威胁智能计算的正式定义：

- 给定威胁情报图G =（V，E）和元路径集M = {P1，P2，…，Pi}
- i）基于元路径Pi计算IOC之间的相似度，以生成相应的邻接矩阵Ai
- ii）通过将IOC的属性信息嵌入到向量空间中，构造节点Xi的特征矩阵
- iii）进行图卷积GCN（Ai，Xi），通过遵循元路径Pi量化IOC之间的相互依赖关系，将其嵌入到低维空间中

Definition 4 Threat Intelligence Computing Based on Heterogeneous Graph Convolutional Networks. *Given the threat intelligence graph $G = (V, E)$, the meta-path set $M = \{P_1, P_2, \cdots, P_i\}$. The threat intelligence computing: i) computes the similarity between IOCs based on meta-path P_i to generate corresponding adjacency matrix A_i; ii) constructs the feature matrix of nodes X_i by embedding attribute information of IOCs into a latent vector space; iii) conducts graph convolution $GCN(A_i, X_i)$ to quantify the interdependent relationships between IOCs by following meta-path P_i, and embeds them into a low-dimensional space.*

威胁智能计算的目的是对IOC之间的语义关系进行建模，并基于元路径度量其相似度，可用于高级安全知识发现，如威胁对象分类、威胁类型匹配、威胁进化分析等。直观地说，由最重要的元路径连接的对象往往具有更相似的。

在本文中，我们提出了一种基于权重学习的威胁智能相似度测量方法，它利用自注意力机制来提高任意两个IOC之间的相似度测量方法的性能。此方法的形式化定义如下，定一组对称元路径集合 $P = [P_m]_{m=1}^{M'}$，任意两个IOC（hi和hj）之间的相似度S（hi，hj）定义为：

$$S(h_i, h_j) = \sum_{m}^{M'} \vec{w} \frac{2 \cdot |\{h_{i \to j} \in P_m\}|}{|\{h_{i \to i} \in P_m\}| + |\{h_{j \to j} \in P_m\}|} \quad (7)$$

利用交叉熵损失来优化提出的威胁情报框架的性能：

$$Loss(Y_{lf}, Z_{lf}) = -\sum_{l \in Y_l} \sum_{f=1}^{F} Y_{lf} \cdot lnZ_{lf} \qquad (10)$$

使用这个框架，安全组织能够挖掘隐藏在iOC之间相互依赖的关系中的更丰富的安全知识。

V.数据集及实验结果

本文开发了威胁数据收集器，自动收集网络威胁数据，包括73个国际安全博客（例如，fireeye，cloudflare），黑客论坛帖子（例如，Blackhat，Hack5），安全公告（例如，Microsoft，Cisco），CVE详细说明和ExploitDB。已经收集了超过245,786个描述威胁事件的与安全相关的数据。为了训练和评估我们提出的IOC提取方法，利用B-I-O序列标记方法对5,000个文本中的30,000个样本进行了标注（60%训练集，20%验证集，20%测试集）。

最终模型最佳执行的超参数如表2所示，学习率对比了0.001,0.005,0.01,0.05,0.1,0.5。

Table 2: Hyperparameters setting in the multi-granular based IOC extraction method.

Parameter	value	Parameter	Value
Embedding_dim	300	Hidden_dim	128
Sequence_length	500	Epoch_num	5,000
Learning_rate	0.001	Batch_size	64
Dropout_rate	0.5	Optimizer	Adam

本文提取的13种主要的IOC性能如表3所示。总的来说，我们的IOC提取方法在精确率、召回率、平均F1字都表现出了优异的性能。然而，我们观察到在识别软件和恶意软件时的性能下降，这是因为大多数软件和恶意软件是由随机字符串命名，如md5。

Table 3: Performance of IOC extraction w.r.t. IOC types.

IOC Type	Precision	Recall	Micro-F1
IP	99.56	99.52	99.54
File	94.36	96.88	95.60
Type	99.86	99.81	99.83
Email	99.32	99.87	99.49
Device	93.26	92.78	93.02
Vender	93.07	94.45	94.24
Version	96.98	97.99	97.48
Domain	96.58	95.89	96.23
Software	88.25	89.31	88.78
Function	95.03	95.59	95.31
Platform	94.31	92.57	93.43
Malware	89.76	91.23	90.49
Vulnerability	99.25	98.73	98.99
Other	98.29	98.42	98.35

为了验证多粒度嵌入特征的有效性，我们评估了具有不同粒度（字符级、1-gram、2-gram、3-gram和多粒度特征）的提取性能。实验结果如图7所示，从图中可以观察到提出的多粒度嵌入特征优于其他特征，因为它利用注意机制同时学习多粒度的IOC特征的不同模式。

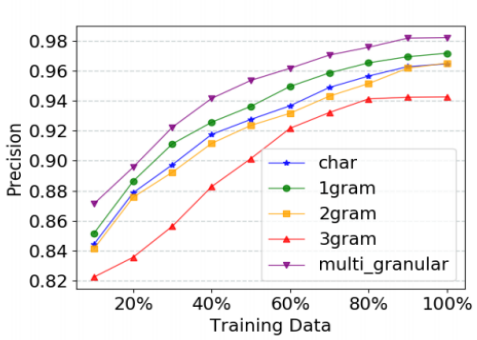


Figure 7: Performance of IOC extraction using embedding features with different granularity.

表4是本文方法与其他命名实体识别方法的性能对比，本文方法的效果更好。

- (1) 与Standford NER和NLTK NER方法相比，它们一般使用新闻语料库训练，本文使用自定义收集的安全语料训练模型。
- (2) 与基于规则的提取方法（如iACE和Stucco）不同，本文提出的基于深度学习的方法提供了一个性能更好的端到端系统来表示各种IOC。
- (3) 与基于RNN的方法（如BiLSTM和BiLSTMCRF）相比，本文的方法引入了多粒度嵌入尺寸（字符级、1-gram、2-gram和3-gram），以同时学习不同大小和类型的IOC特征，可以识别更复杂和不规则的IOC。
- (4) 本文的方法利用注意机制来学习不同尺度特征的权重，以有效地描述不同类型的特征，进一步提高了IOC识别的准确性。

Table 4: Performance of threat entity recognition using different methods.

Method	Accuracy	Precision	Micro-F1
NLTK NER	69.45	68.51	67.49
Stanford NER	68.35	66.74	68.58
iACE	92.14	91.26	92.25
Stucco	91.16	92.21	91.47
CRF	92.64	91.80	92.65
BiLSTM	94.78	95.21	94.35
BiLSTM+CRF	96.38	96.42	96.27
Multi-granular	**98.59**	**98.72**	**98.69**

VI.威胁智能计算技术的应用

本文提出的基于异构图卷积网络的威胁智能计算框架可以用来挖掘异构IOC背后新的安全知识。在本节中，我们使用三个真实世界的应用程序来评估它的有效性和适用性：

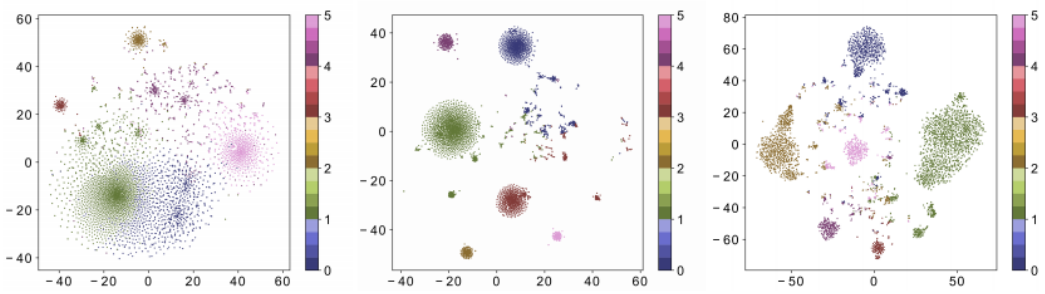
- CTI威胁分析和排名
- 攻击偏好建模
- 漏洞相似性分析

不同类型IOC的排名如表5所示，具有不同元路径的攻击偏好实验结果如图8所示。具体而言，本文首先利用提出的威胁智能计算框架将每个攻击者嵌入到一个低维向量空间中，然后对嵌入式向量执行DBSCAN算法，将具有相同偏好的攻击者聚集到相应组中。

图8显示了不同类型元路径下的前3个聚类结果，其中元路径 AVDPDTVTAT(P17) 在紧凑和分离良好的集群中性能最好，这表明它比其他元路径在描述攻击偏好方面具有更丰富的语义关系。

Table 5: The significance ranking of different types of IOCs. ($CVE1$: CVE-2017-0146, $CVE2$: CVE-2006-5911, $CVE3$: CVE-2008-6543, $CVE4$: CVE-2012-1199, $CVE4$: CVE-2006-4985; AR: Authoritative Ranking, DC: Degree Centrality value.)

Vulnerability			Attacker			Platform			Attack Type		
No.	AR	DC	Monicker	AR	DC	Category	AR	DC	Exploit_type	AR	DC
$CVE1$	0.2713	7,643	Meatsploit	0.2764	549	PHP	0.4562	17,865	Webapps	0.5494	11,648
$CVE2$	0.2431	7,124	GSR team	0.1391	327	windows	0.2242	13,793	DOS	0.1772	8,741
$CVE3$	0.2132	6,833	Ihsan	0.0698	279	Linux	0.0736	8,792	Overflow	0.1533	7,652
$CVE4$	0.1826	6,145	Techsa	0.0695	247	Linux86	0.0623	8,147	CSRF	0.0966	5,433
$CVE5$	0.1739	5,637	Aurimma	0.0622	204	ASP	0.0382	5,027	SQL	0.0251	2,171



(a) $AVDV^TA^T$ (P_{13}) (b) $AVDPD^TV^TA^T$ (P_{17}) (c) $AVPV^TA^T$ (P_{14})

Figure 8: The performance of attack preference modeling with different meta-paths, in which the preference of attacker i is reduced to a two-dimensional space (x_i, y_i) and each cluster represents a group with a specific attack preference.

为了验证攻击偏好建模的有效性，我们确定了5297个不同的攻击者（每个唯一的IP地址被视为一个攻击者）。在标记样本和清洗数据后，进一步评估不同元路径在模型上的性能。在攻击建模场景中，我们只关注起始节点和结束节点都是攻击者元路径的情况，实验结果详见表6。显然，不同的元路径在描述网络入侵者的攻击偏好方面表现出不同的能力。使用P17的性能要优于其他元路径，这表明P17在描述网络罪犯攻击偏好时具有更高价值的信息，因为P17包含P1、P4、P5和P12~P15的语义信息。

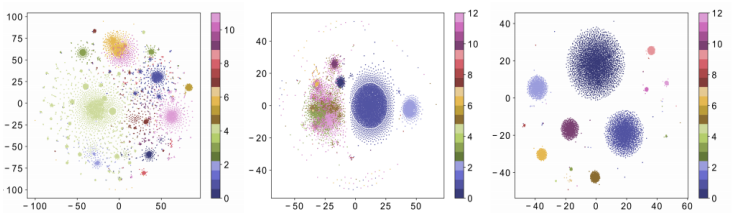
Table 6: Performance of modeling attack preference with different meta-paths.

Metapath	Accuracy	Precision	Micro-F1
P_1	74.31	76.22	75.25
P_4	71.16	73.27	72.16
P_5	69.15	71.43	70.27
P_{12}	72.14	76.46	74.24
P_{13}	79.65	81.31	80.47
P_{14}	77.48	79.34	78.40
P_{15}	80.17	79.76	79.96
P_{17}	**81.39**	**81.72**	**81.55**

最后是漏洞相似性分析，基于不同元路径的漏洞相似性分析如图9所示。其中漏洞i可以简化为二维空间（xi、yi），每个集群表示特定类型的漏洞，聚类的准确率如表7所示。

Table 7: Accuracy of vulnerability clustering.

Cluster ID	Vulnerability type	Accuracy
cluster1	Denial of Service	80.12
cluster2	XSS	83.53
cluster3	Execute Code	81.50
cluster4	Overflow	76.50
cluster5	Gain Privilege	91.56
cluster6	Bypass Something	71.74
cluster7	CSRF	93.27
cluster8	File Inclusion	61.72
cluster9	Gain Informa	70.42
cluster10	Directory Traversal	69.49
cluster11	Memory Corruption	81.56
cluster12	SQL Injection	80.67
average	#	**78.51**



(a) $AVDV^TA^T$ (P_{13}) (b) VDV^T (P_{10}) (c) $VDPD^TV^T$ (P_{16})

Figure 9: Illustration of the vulnerability similarity analysis based on different meta-paths, in which vulnerability i can be reduced into a two-dimensional space (x_i, y_i) and each cluster indicates a particular type of vulnerability.

讨论

- Data Availability
- Model Extensibility
- High-level Semantic Relations
- Security Knowledge Reasoning.

Ⅶ.结论和个人感受

1.结论

本文的工作探索了威胁智能计算的一个新方向，旨在发现不同威胁向量之间关系的新知识。我们提出了一个网络威胁情报框架HINTI，通过利用异构图卷积网络来建模和量化不同类型IOC之间的依赖关系。我们开发了一个多粒度注意力机制来学习不同特征的重要性，并使用HIN来建模IOC之间的依赖关系。此外，本文提出了威胁智能计算的概念，并设计了一个基于图卷积网络的通用智能计算框架。

实验结果表明，基于多粒度注意力机制的IOC提取方法优于现有的先进方法，提出的威胁智能计算框架可以有效挖掘隐藏在IOC之间相互依赖关系中的安全知识，使关键的威胁智能应用，如威胁分析和排序、攻击偏好建模和脆弱性相似性分析。

在未来，我们计划开发一个基于HINTI的预测和推理模型，并探索预防性的应对措施，以保护网络基础设施免受未来的威胁。我们还计划增加更多类型的IOC和关系，以描述一个更全面的威胁环境。此外，我们将利用元路径和元图来表征IOC及其交互作用，以进一步提高嵌入性能，并在模型的准确性和计算复杂度之间取得平衡，还将研究基于HINTI的安全知识预测的可行性，以推断漏洞和设备之间潜在的潜在关系。

2.个人感受

我的整体感受如下，写得不好的地方还请海涵。

- 这篇文章和我对威胁情报自动化提取的想法及实验非常相似（NER实现），但我的方法没有本文系统，尤其是算法创新和后面的应用实践，包括引言部分和动机都非常值得我去学习。真诚地感谢北航老师们的分享，让我学得很多，也进一步验证我的想法是有价值的。虽然撞车，但我学到的更多，后续我将进一步去优化自己的实验和idea，加油~
- 之前做过很多BiLSTM和CNN+Attention的实验研究，原来多粒度注意力机制就是这样的，字符级、n-gram相结合，和我2016年做的多视图融合算法有相似之处，当时实体对齐从text和inforbox两个视图优化。
- NLP和安全结合来增强语义，图神经网络及GAN与二进制结合都是非常好的结合点，而且有很多内容可以去做，该篇论文在NLP领域是常见的命名实体识别（NER）问题，其模型仍然有很多优化的点，但是在CTI领域仍然比较新，且应用价值巨大。
- 就我自己而言，虽然英文论文能够独立阅读，但英文写作和听读是致命的弱点，后续需要不断加强。此外，英文论文看得太少太少，好在现在已经放弃技术博客更新，转而扎进论文的学习，好好珍惜这些奋斗的日子吧！读博不易，珍惜当下。

这篇文章就写到这里，希望对您有所帮助。同时，也欢迎大家讨论，继续加油！且行且珍惜。

Ⅷ.英文优美十句

摘要

- Cyber Threat Intelligence (CTI), as a collection of threat information, has been widely used in industry to defend against prevalent cyber attacks.
- In this paper, we propose a novel CTI framework, HINTI, to model the interdependent relationships among heterogeneous IOCs to quantify their relevance.

前言

- Nowadays, we are witnessing a rapid growth of sophisticated cyber attacks (e.g., zero-day attack, advanced persistent threat). Such attacks can effortlessly bypass traditional defenses such as firewalls and intrusion detection systems (IDS), breach critical infrastructures, and cause devastating catastrophes. To combat these emerging threats, security experts proposed Cyber Threat Intelligence (CTI) that consists of a collection of Indicators of Compromise (IOCs).
- Recent studies have proposed automated methods to extract CTI in the form of Indicator of Compromise (IOC) from unstructured security-related texts [4, 22]. Most of existing IOC extraction methods, such as CleanMX, PhishTank, IOC Finder, and Gartner peer insight, follow the OpenIOC [10] standard and extract particular types of IOCs (e.g., malicious IP, malware, file Hash, etc) by leveraging a set of regular expressions.
- However, such extraction approaches face three major limitations. First, the accuracy of IOC extraction is low, which inevitably leads to the omission of critical threat objects [22]. Second, isolated IOC hardly depicts the comprehensive landscape of threat events, making it virtually impossible for CTI subscribers to gain a complete picture into the incoming threat. Third, there is a lack of an effective computing framework to efficiently measure the interactive relationships among heterogeneous IOCs.
- To combat these limitations, HINTI, a cyber threat intelligence framework based on heterogeneous information network (HIN), is proposed to model and analyze CTIs.

动机

- Different from the existing CTI frameworks, HINTI aims to implement a computational CTI framework, which can not only extract IOCs efficiently but also model and quantify the relationships between them. Here, we use the motivating example to illustrate how HINTI works step-by-step in practice as follows.
- Compared with Figure 1, it is obvious that HINTI can depict a more intuitive and comprehensive threat landscape than the previous approaches.

- Particularly, our proposed CTI computing framework characterizes IOCs and their relationships in a low-dimensional embedding space, based on which CTI subscribers can use any classification (e.g., SVM, Naive Bayes) or clustering algorithms (K-Means, DBSCAN) to gain new threat insights, such as predicting which attackers are likely to intrude their systems, and identifying which vulnerabilities belong to the same category without the expert knowledge. In this work, we mainly explore three real-world applications to verify the effectiveness and efficiency of the CTI computing framework: IOC significance ranking (see Section 6.1), attack preference modeling (see Section 6.2), and vulnerability similarity analysis (see Section 6.3).

模型实现

- Recently, Bidirectional Long Short Term Memory+Conditional Random Fields (BiLSTM+CRF) model [15] has demonstrated excellent performance in text chunking and Named-entity Recognition (NER). However, directly applying this model to IOC extraction is unlikely to succeed, since threat texts usually contain a large number of threat objects with different grams and irregular structures.
  Consequently, we need an efficient method to learn the discriminative characteristics of IOCs with different sizes. In this paper, we propose a multi-granular attention based IOC extraction method, which can extract threat objects with different granularity.

(By:Eastmount 2021-04-30 周五夜于武汉 http://blog.csdn.net/eastmount/)

CSDN还是非常爱我的，上首页了，哈哈。当然，我也很爱CSDN，在这里写文早已渗透到了血液，我还和涛哥约定要在这里再写二十年，五十年，一辈子。

感谢所有人的祝福，第一次向19万人发私信，博友们的祝福和鼓励真的很感动，是真感动这或许就是分享的魅力，知识的甘甜吧。无以为报，只希望未来分享更好的文章，帮助更多初学者。握不住的沙子，就随手扬了它，接下来沉下心去，继续享受奋斗的过程。短暂停更技术博客只为更好的遇见，愿我这只笨鸟归来仍是少年。且行且珍惜，爱你们喔，小珞太乖了，晚安娜~

致敬大佬，江湖再见　　要多写一些像博主这样的内容丰富，干货满满的知识分享。　恭喜，恭喜，祝贺博士小弟弟前途似锦。

很厉害！看齐！　加油，大佬　　致敬大佬　　情意满满！杨老师心中有爱，认真又可爱。

在这浮躁的社会里不卑不亢，砺砺前行。看你们的这些文章，有时真的能让人更沉下心来，致谢，共勉。望博士之旅顺利。

付出才会有收获,一起加油　　10年了 大佬头发依然这么茂盛　　致敬大佬，江湖再见　　大佬有缘再见!

放弃不难，但坚持一定很酷,加油，奥里给！　　赞，大佬　　初入行业，初始大佬，希望可以读完大佬的文章，江湖再见

致敬，学习　虽然只是第一次看到您的文章，却已经被您的胸怀，您的精神，您的能力折服了，大佬加油，期待您的归来

致敬大佬，感谢分享　　待您归来仍是少年，我也要加油！共勉，爱码士！！！　　大佬，一起加油~~~　　加油

前路似锦　　加油，杨博士开启闭关修炼模式了　　杨老师加油！　　为大佬点赞，榜样，值得学习

祝大佬博士科研顺利！　加油呀！　　十年的陪伴，感恩　　加油、杨博士！　看似鸡汤文，实则技术文

大佬加油

第一次看到老师的文章，江湖再见或是等您归来！致敬　　一直关注您的博文，可谓受益良多，感谢您的帮助和分享！

文章干货满满　　大佬牛逼，之前问过问题，居然回复过我。很激动，共勉！今年顺利考研成功了，希望赶上大佬步伐

师弟加油！！三年磨一剑，一定更上一层楼！！！　　我竟然间接认识一位博士，加油！　　杨博士

杨博士一致都是我的偶像，也一直都是我以后要成为的人。　　路漫漫其修远兮，吾将上下而求索 向博主大佬学习