学校编码：10384　　分类号_____密级_____
学　　号：23020101153051　　UDC_____

厦门大学

硕士学位论文

基于云模型的网络安全风险评估研究

Research of Network Security Risk Accessment based on Cloud Model

王　曦

指导教师姓名：江　弋　副教授
专业名称：计算机系统结构
论文提交日期：2013 年　　月
论文答辩时间：2013 年　　月
学位授予日期：2013 年　　月

答辩委员会主席：
评　阅　人：

2013 年　　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：王曦

2013年06月04日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：王曦

2013 年 06 月 04 日

摘要

互联网的飞速发展给人们的工作和生活带来了便利，然而网络安全事故频发，无疑给网络世界蒙上了一层阴影，一旦重要的私人信息在网络安全事故中被泄露的话，就有可能造成非常严重的后果，不仅有可能是财产上的损失，甚至有些不法分子还会收集和利用这些信息对人身造成伤害，因而网络领域的安全问题已经引起了人们的广泛的关注。而网络安全风险评估是该领域的最基础的工作，能够帮助我们对于网络的整体状况有一个大致的了解，从而能够为如何改善网络，提升网络的安全性能提供可靠的参考，是一个值得研究的方向。

目前使用的网络安全风险评估理论和方法中，历史资料扮演了十分重要的角色，整个评估的过程需要对历史资料进行仔细的研究，并且评估结果在一定程度上取决于评估者的水平，然而网络信息世界日新月异，新威胁、新漏洞层出不穷，旧有的思维方式已经无法跟上节奏，并且如果要想得到理想的评估结果的话，评估者的水平也需要不停地提升，因而在新环境下，需要我们对网络安全风险评估问题进行重新审视。

根据历史经验判断网络安全风险“高”或者“低”，是一种定性的做法，然而在自动评级的过程当中，就不会再有人工的参与，而是要进行定量上的计算，并且定量计算也要和定性的概念、定性的级别融合在一起，针对现有网络安全风险评估模型的不足，本研究主要采用云模型来解决这类定性定量相互转换问题。为此本文首先进行了网络建模，构建访问图模型。其次，基于访问图模型，本文对威胁事件可能发生的概率和威胁事件可能造成的信息资产损失的进行估算，以此为基础计算网络信息系统的综合风险值。最后本文将网络安全风险评估和云模型相结合，网络安全风险综合值作为云模型的参数，通过采样、计算得到云模型的特征值，构建出确定的云模型，然后用随机的采样值作为云模型的输入，经过云模型的判断之后，确定网络安全风险的级别。

关键词:云模型；访问图模型；安全风险评估

ABSTRACT

The rapid development of Internet brings convenience to our work and life. However , when we hear about network security events , we become anxious. As a technology to make network information system more secure and robus, risk assessment not only takes many security factors such as threatens， assets， vulnerabilities into account， but also helps administrators take an active attitude to identify those potential threatens that their system will be exposed to.

Exsiting network risk accessment theories and methods rely on a great quantity of historical data and long-term experience. However, network information world alters from day to day. New threatens and vulnerabilities emerge in an endless stream. The old modes of thinking can not adapt themselves to the new changes. So new technologies and modologies should be developed according to the specific characters, the pattern of behavior of vulnerabilities and threatens in the network.

The tasks this article has completed are as follows:

1. This article carries out network modeling. Starting from the pattern of behavior of vulnerabilities and threatens in the network, we build the access graph, which can describe the threat scenarios of target network. In the process of network risk accessment, access graph can show the global risk that every vulnerability brings due to the effects of high interactions of network. The access graph generation algorithm is with high accuracy. Futher on, it optimizes according to the feature that most large-scale network is divided into subnets. As a result, it reduces the computational cost and makes the access graph extendible and suitable for realistic size network.

2. Using access graph, this article proposes an algorithm to estimate the probability of occurance for threat event based on reliability principle. Reliability principle is a traditional theory which is used to estimate the reliability degree of component. This article introduces it to construct the function of the probability of occurance for threat event using both the vulnerability's cost and the level of effort of the attacker. So the result is more precise and objective. This article also proposes a security policy-oriented algorithm to estimate the loss of assert caused by threat event.

The algorithm estimates the impact on information assert caused by threat event using the violation degree to the security policy. Based on access graph, using algorithm for estimating occurance probability of threat event and algorithm for estimating loss of information assert, we can figure out network risk integration value.

3.This article introduces the concept of cloud model, which is used to grade the degree of network risk. It is qualitative when we say the network risk is high or low according to past experience. But in the process of automatic grading, there is no more human intervention. So we need quantitative calculation, which should be consistent with qualitative concept. Here comes the cloud model , which is a good choice to realize the transition between qualitative concept and quantitative calculation. This article combines network risk accessment with cloud model. Cloud model uses network risk integration value as its parameter. By sampling and calculating, we obtain the characteristic value of cloud model and contructs fixed cloud model. Then we enter random sampling value into cloud model . After the grading of cloud model, we can get the grade of network risk.

Key words: Cloud model; Access graph; Security risk assessment

目录

Catalogue

第一章 绪论

1.1 研究背景

半个世纪以来，信息安全(Information Security)经历了前所未有的发展[1]，在计算机还未发明之前，信息基本上存储于纸质材料当中，信息安全也大部分借助于物理措施(例如把重要的资料存放于封闭的资料室中)和管理措施(对员工定期检查)来保障。第一次变革是计算机安全(Computer Security)，计算机渐渐走进千家万户，人们也渐渐将信息通过电子文件的方式存放于私人计算机中，进行归档和整理，因而需要考虑如何对私人计算机中的信息进行保护。第二次变革是网络安全(Network Security)，互联网飞速发展和壮大，信息技术和信息产业的发展如火如荼，给人类的生活带来了翻天覆地的变化，人们通过电脑、手机等等这些工具，可以随时随地连接互联网，获取资源，分享信息，逐渐搭建属于自己的生活空间，然而与此同时，互联网也给计算机带来了风险，我们时不时地听到关于信息泄露事件的报道，尤其是用户信息，这给网络生活中的私人信息的安全保障带来了极大的破坏，这对于整个信息行业来说是一个极大的挑战，不过也给整个信息行业敲响了警钟，行业不得不致力于信息安全防护的研究。在分布式环境下，网络安全主要对信息载体和信息提供安全保护，保护的主要操作包括传输、存储、访问以及防止数据、信息内容或能力被非授权使用、篡改和拒绝服务[2]。

在互联网的环境下，信息的传播也越来越迅速，这样的变化，对世界范围内的经济、政治、科教及社会等等产生了深远的影响。在信息安全关乎国家和社会稳定的21世纪[3]，网络安全问题俨然已经成为影响全球战略部署和社会经济发展的重要因素之一，它也作为信息安全领域中非常前沿的研究方向被国际社会共同关注。

网络安全历经了多个阶段，其中有三个主要阶段如下所述[4]：

第一阶段主要是通过构建堡垒模型(Fortress Model)来保证相对安全的计算机系统[5]。“堡垒’模型指运用隔离技术分割外界环境和内部系统。隔离主要通过设置机密性、完整性和不可否认的安全指标，与其相关的研究内容包括存取控制和权限管理。

当试图登入系统的用户不存在时，或者权限不匹配时，系统则予以拒绝，以此来维护网络的安全；例如，原先系统的层次可能比较多，各层的协议也比较复杂，这给攻击者提供了可乘之机，因此研究人员为了能够更好地阻止安全事件的发生，采用完善安全细节和优化协议设计等手段进一步提升安全系数;而且通过合理地设计权限等级，使得每个等级的用户都分配有自己的资源，级别高的用户资源多一些，资源的价值也相对来说更高，级别较低的用户只能访问自己的资源，其他较高级别或者是同一级别用户的信息自然屏蔽，借助于这样的方式达到信息资源的保护。防火墙和口令保护作为第一阶段研发的主要技术在一段时期内被研究者们广泛关注。

第二阶段主要采用实时监控技术检测网络入侵行为达到信息保障(Information Assurance)的目的。对于熟悉甚至是精通计算机知识和网络知识的人来说，只要充分了解网络的组成，就能够找到网络的漏洞，实施对网络的攻击，而所谓的信息安全的保护技术在这些情况下是无法起到防范作用的。然而信息系统俨然已经成为支撑社会顺利运营的基础设施，与此同时，风险、漏洞、威胁又存在于网络的角角落落里，没有及时得到修补或解决，并且信息资产越来越多，也就意味着网络信息系统需要来承担保护这些信息资产的重要责任。随着网络攻击的多样化，人们越来越急迫地需求信息保障技术[6]。1998 年，美国国家安全局为了深化信息安全的概念，他们编写了《信息保障技术框架》(IATF)。这篇关于信息安全技术的文档开启了人们对于信息安全概念认识的新纪元，从原先单纯的信息安全知识提升到了融合防护、检测、预警、响应和恢复的信息保障。为了更好地诠释文档中的内容，PPDRR 安全模型应运而生，它能够充分体现信息保障完整生命周期。借鉴其它领域的优秀成果，比如遗传免疫等，进行入侵检测是第二阶段网络安全技术的热点研究。

第三阶段是研究者们开始考虑网络的生存性和鲁棒性，这一阶段基于信息保障技术他们开始研究如何使得网络在发生故障之后能够迅速地恢复，尽量减少对于业务的不良影响进而减少因故障而造成的社会影响和经济上的损失等问题，充分地保障网络的业务水平。

随着网络安全技术水平的不断提高，安全评估技术作为一项基础步骤，它的层次也逐渐地得到了提升。安全评估技术主要涉及从产品安全到宏观系统安全的

评估。《可信计算机系统安全评估准则》(TCSEC)[7]主要是为了评价不同计算机系统的保密性而提出的;《信息技术安全评估标准》(ITSEC)[8]主要是为了评价多种安全产品的信息安全性而提出的;《信息技术安全通用评估准则》(CC)[9]主要是为了能够在相比于 ITSEC 更加开放的使用环境下评价不同安全产品的信息安全性而提出的;信息保障主要是为了基于宏观信息系统的信息安全保障角度，考虑从单一技术因素，被动保护，绝对安全为目的的局面到结合众多方面的综合因素，积极、动态、反馈保护，追求适度安全风险保障的局面。适度安全风险的保障希望通过加强风险的承受能力进而达到多种分析评估的目的，比如威胁分析，脆弱性分析等[10]。在文献[11]中，沈昌祥院士指出在 PDRR 模型完整信息安全生命周期的基础上，等级保护、风险评估、应急处理和灾难恢复是构建信息安全保障体系的四个主要环节。

除此之外，网络安全风险评估能够让网络系统变得更安全和更可靠，和其它各种各样的评估技术相比，有其独特的优势，比如网络安全风险评估将许多可以帮助用户更加积极地发现网络系统中存在的漏洞和网络系统面临着的潜在的安全威胁的安全评估的元素与包含漏洞、威胁、资产等的模型相互结合。为了进一步提升该方法的评估能力和加强网络系统的安全性能，研究者们基于当前获得的评估成果继续制定有针对性的安全计划，以此更好地避免了威胁事件的发生。

总而言之，网络安全风险评估这一在网络安全领域中不可或缺的评估手段，已经成为网络安全保障体系中的重要环节。我们的日常工作和生活越来越离不开计算机网络所营造的信息世界，计算机网络空间下的安全风险评估，即网络安全风险的研究和探索，是目前最流行的网络安全的研究方向。

1.2 网络安全风险评估研究现状

在二十世纪五六十年代，欧美核电厂中最早在安全性评估体系中加入了风险评估的环节[12]，之后逐渐开始向航天、交通、经济、环境、化学、医疗等众多领域推广，并且得到了广泛的应用。

在信息安全领域中，风险评估的相关研究最早始于十九世纪六十年代末的美国。当时，美国国防科学委员会授权多家国防工业公司配合以兰德公司为首的综合性战略研究机构开展以计算机的安全问题为重点的研究活动。到了十九世纪七

十年代初，经过许多研究人员的不懈努力，针对当时大型机以及远程终端展开的安全性研究工作取得了阶段性进展，工作对它们进行了相对全面的分析以及进行了第一次大规模的风险评估[13]。

当计算机网络不断发展之后，不仅要关注计算机的安全问题，更要关注整体的网络安全问题。在上述三个阶段的影响下，网络安全风险评估也取得了自身的发展，从最早单纯地关注计算机系统安全到将研究重点放在多种网络产品的信息安全性，其内容包括保密性，完整性和可用性，并且尝试借助于多种评估手段，保证安全产品的质量，进而提高系统的安全性能，发展到目前主要集中在信息系统的开发实施和信息安全基础设施。

在这个漫长艰难，但是振奋鼓舞的过程中，网络安全风险评估在评估模型、评估理论与方法方面都有着深入的研究和发展。

1.2.1 网络安全风险评估模型

长久以来，许多专家学者希望能够从网络整体出发,判断每个单独的结点是否存在安全威胁和隐患，进而全面客观地评估这些威胁对于整体网络系统所带来的危害程度。国内外学者对基于设备互联和信任关系的网络安全风险评估展开研究，建立了多种安全评估模型，其中被人们所熟知的主要是攻击树模型、特权提升图模型和攻击图模型，下面我们分别对这三个模型进行详细的介绍：

1、攻击树模型

为了更加直观地识别攻击者的具体行为进而评估系统的安全性，研究者采用攻击树结构来刻画攻击行为，攻击树的基本结构包括“与”结构和“或”结构，如图 1.1 所示，其中根结点 T0 表示系统安全的最终破坏，子树 T1,… ,Tn 表示与根结点 T0 相关的防御结点。“与”结构顾名思义就是如果所有子树 T1,… ,Tn 都被攻击成功之后，那么根结点 T0 被攻击成功;“或”结构是如果子树 T1,…,Tn 中的任意一个被攻击成功，那么根结点 T0 被攻击成功。攻击树结构可以由任意的“与”结构和“或”结构组合而成，“与或”复合关系表示造成最终破坏的一系列低层环节。

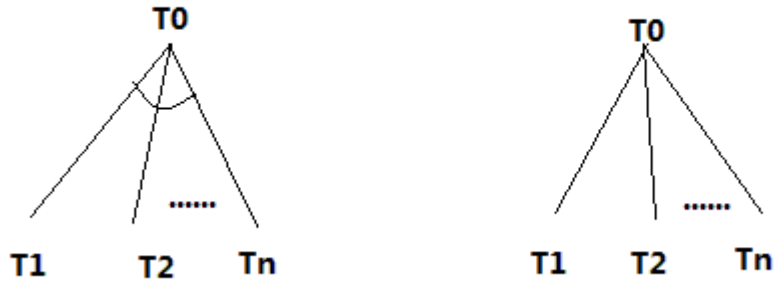

图 1.1 攻击树的两种基本结构

通过攻击树结构来刻画 Unix 系统的入侵过程，如图 1.2 所示。从图中可以看出，入侵者可以通过获得系统的远程访问权限或者获得局域访问权限方式来获得系统的访问权限，获得系统的远程访问权限和获得局域访问权限这两种方式之间是“或”关系，也就是说，只要入侵者采用其中一种方式取得成功就能够获得系统的访问权限；猜测密码的前提必须是获得密码文件。多层攻击树表示网络攻击行为的多阶段性，每个非根结点都表示入侵的一个子目标，为了能够更好地区分每个子目标对于最终攻击目标的安全级别，可以为它们赋予不同的权重。通过每个结点的权重以及子目标入侵成功的概率，我们可以利用自底向上的方式递推估计最终目标入侵成功的概率[4]。

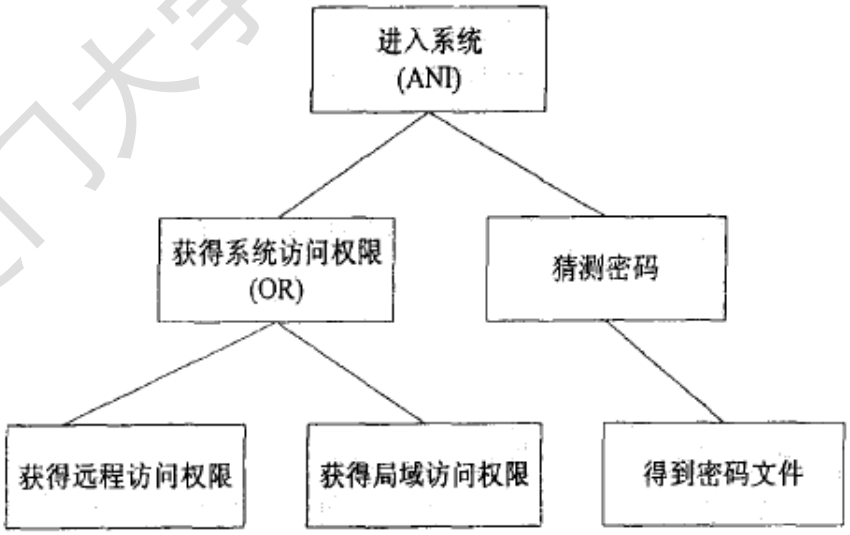

图 1.2 Unix 系统入侵的树结构

研究人员们基于攻击树模型展开了许多研究，也获得了一些令人欣喜的结果，这些研究成果涉及语言形式化描述[14]、大规模入侵检测[15]以及系统安全性分析[16]。但是，由于攻击树模型存在自身的局限性在多种情况下很难得以突破，比如对多重尝试攻击建模、时间依赖等，并且攻击树模型由于非根结点往往具有很高的冗余性导致无法进行全局考虑。

2、特权提升图模型

法国学者 Dacier[17][18]和 Ortalo[19][20]等人提出了特权图的概念。

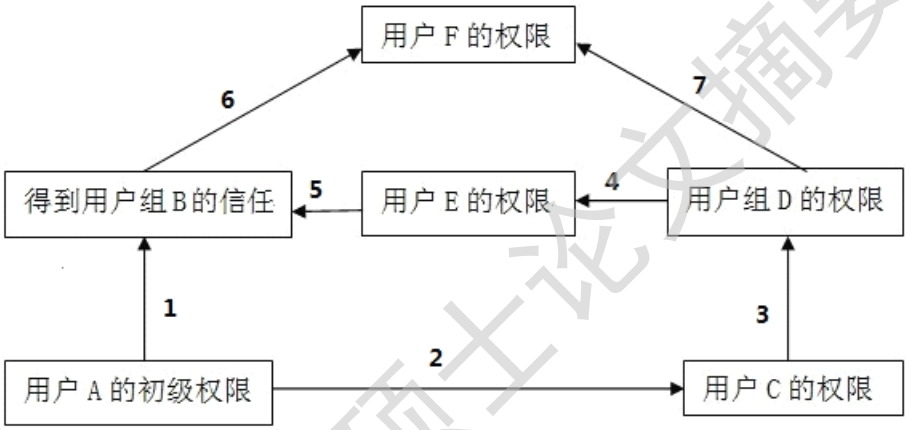

图 1.3 简单入侵的特权图实例

通过特权提升图来描述 Unix 系统的入侵过程，如图 1.3 所示，图中连接弧 1-7 分别代表不同的脆弱性类别，每个结点分别代表具有不同权限的用户。从图中可以看出，结点用户 A 为了得到根用户 F 的高级权限可以通过多种不同的路径实施攻击。Dacier 定义了 METF(mean effort to failure) 度量方式用于衡量弱点攻击的成功概率，并且利用多种经验算法得出入侵在每条路径上的攻击代价。通过对这些攻击代价取均值来说明入侵的整体成功率，也可以说明整个系统的安全性高低。但是单纯取均值缺乏理论依据，主要是依据主观经验，因此量化结果不能很好地反映实际系统的安全性。

3、攻击图模型

在文献[21]中，Phillips 和 Swiler 首次基于攻击图理论提出网络弱点分析方法。