

# 实物保护系统脆弱性评估技术综述

班级：网工 1801 吴斌

学号：18408020129

## 实物保护系统：

实物保护系统是指利用实体屏障、探测延迟技术及人员的响应能力，阻止盗窃、抢劫或非法转移核材料以及破坏核设施行为的安全防范系统。

实物保护系统是**人防、物防和技防**的有机结合：人防由核电厂保卫、公安及武警负责组织实施响应；而物防是通过设置各级实体屏障达到有效延迟的目的；技防是通过出入口控制系统、防入侵探测系统、电视监视系统及保安通信系统等技术手段提供有效的探测。

## 软件（系统）脆弱性定义：

对于什么是软件脆弱性，目前没有形成一个一致接受的定义，由于软件脆弱性的复杂性和考虑的角度不同，对脆弱性存在着各种定义。

但总的说来有两类：一类是**精确定义**，试图对系统及其行为给出精确描述，并基于此给出系统脆弱性的精确定义，这对于形式化证明、计算机理论研究有较大的价值。第二类是**模糊定义**，通过描述性语言，对脆弱性的本质进行描述。这类定义通常出现在字典或各种脆弱性数据库中。

目前，软件脆弱性分类法很多，有一定影响的至少有 20 多个，如基于引入原因、基于语法、基于错误分析、基于属性、基于起源、基

于访问需求、基于利用难度、基于部件、基于影响、基于威胁、基于利用复杂性、基于攻击、基于生命周期、基于入侵检测和基于特定系统等。

### **脆弱性评估技术：**

(1) 基于规则的脆弱性分析：2005 年，Vipin 等提出提出一种基于规则的脆弱性分析方法。该方法定义了一种不干扰规则，单独攻击为一种基于规则系统的转移规则，用状态节点表示计算机网络的配置信息和攻击者的能力。根据规则集属性匹配关系，提供了一种有效的脆弱性分析算法，实现了网络中的攻击路径，具有较好的可扩展性。

(2) 基于贝叶斯网络的评估方法：贝叶斯网络是将多元知识图解可视化的一种概率知识表达与推理模型，可以判断网络节点变量间的因果关系及条件相关关系。Marcel 等提出用贝叶斯网络和攻击图度量网络安全风险，精确推理计算了攻击路径成功的概率。Xie 等通过对脆弱性利用和攻击者实施攻击行为的不确定性建模分析了评估网络系统的安全风险，提出了一种基于贝叶斯网络的系统安全评估方法。针对攻击结构的不确定性、攻击行为的不确定性和报警的不确定性进行分析，引入本地检测模型描述安全检测行为。

(3) 基于脆弱点依赖图的脆弱性评估：马俊春等为弥补目前网络脆弱性评估简单、评估结果不准确的缺陷，提出一种基于脆弱点依赖图的网络脆弱性评估方法，并开发了相应的评估系统。该方法将通用弱点评价体系和目标网络脆弱点依赖图结合起来，实现了对网络

脆弱性的客观评价。此外，在计算时，脆弱性可利用性和脆弱性影响分别计算，与实际网络中的脆弱点依赖图结合，使计算值更有参考价值。

#### **参考文献：**

- [1] 实体保护系统 - 维基百科。
- [2] 李新明, 李艺, 徐晓梅, 韩存兵. 软件脆弱性分析. 计算机科学.
- [3] 邢栩嘉, 林闯, 蒋屹新. 计算机系统脆弱性评估研究[J]. 计算机学报, 2004(1):1-11.