2021-2022学年春季学期

网络空间安全态势感知

Cyber security situation awareness

授课团队：刘宝旭 卢志刚 刘玉岭

助　　教：李　宁

网络空间安全态势感知

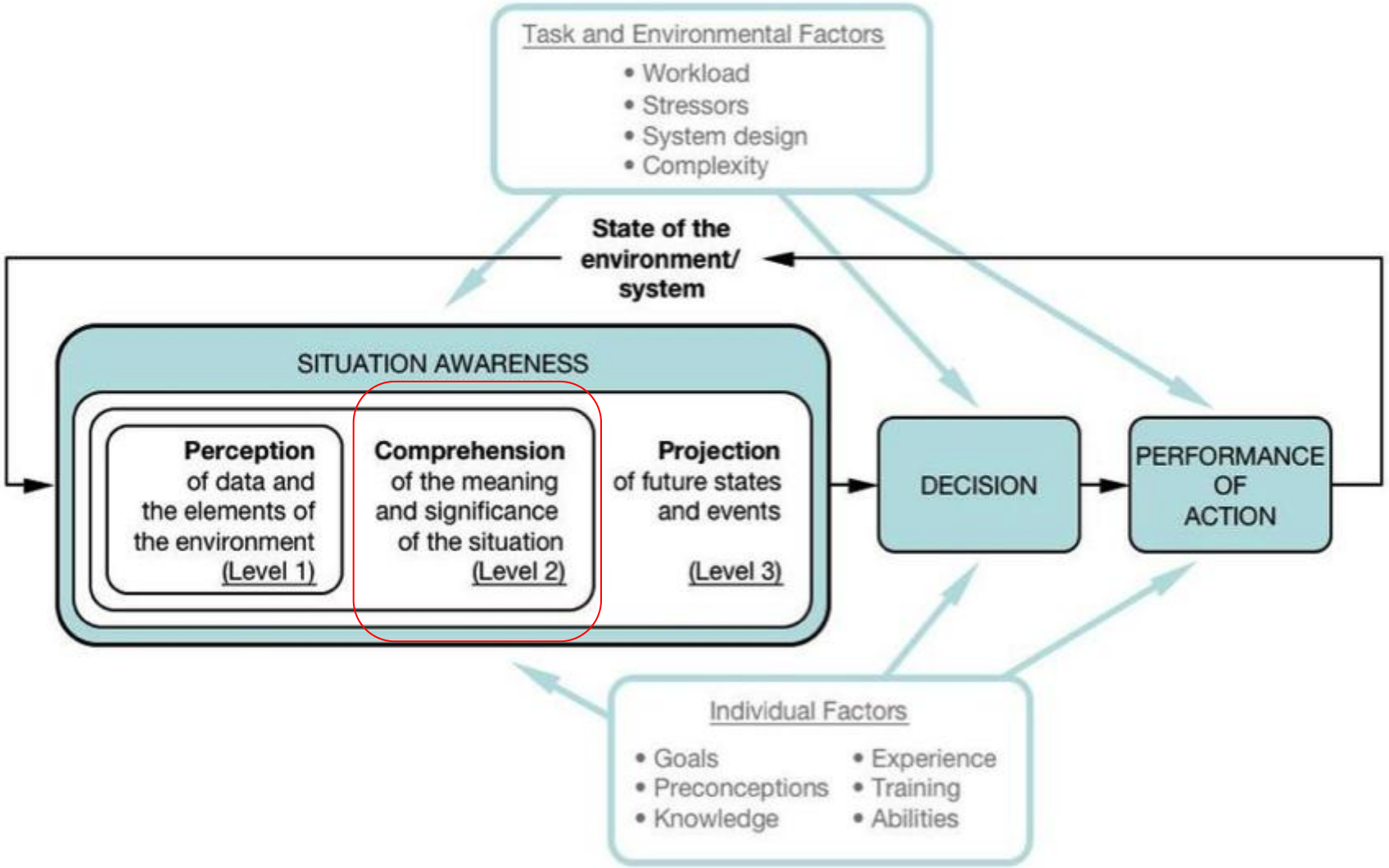
Cyber security situation awareness

[第10次课] 网络安全态势评估技术

授课教师：刘玉岭

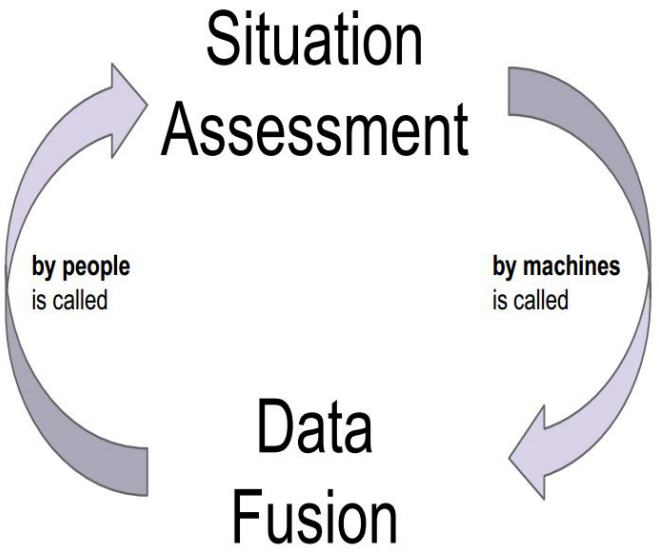
授课时间：2022.3.24

态势感知技术体系


Task and Environmental Factors
• Workload
• Stressors
• System design
• Complexity
State of the environment/ system
SITUATION AWARENESS
Perception of data and the elements of the environment (Level 1)
Comprehension of the meaning and significance of the situation (Level 2)
Projection of future states and events (Level 3)
DECISION
PERFORMANCE OF ACTION
Individual Factors
• Goals
• Preconceptions
• Knowledge
• Experience
• Training
• Abilities

内容概要

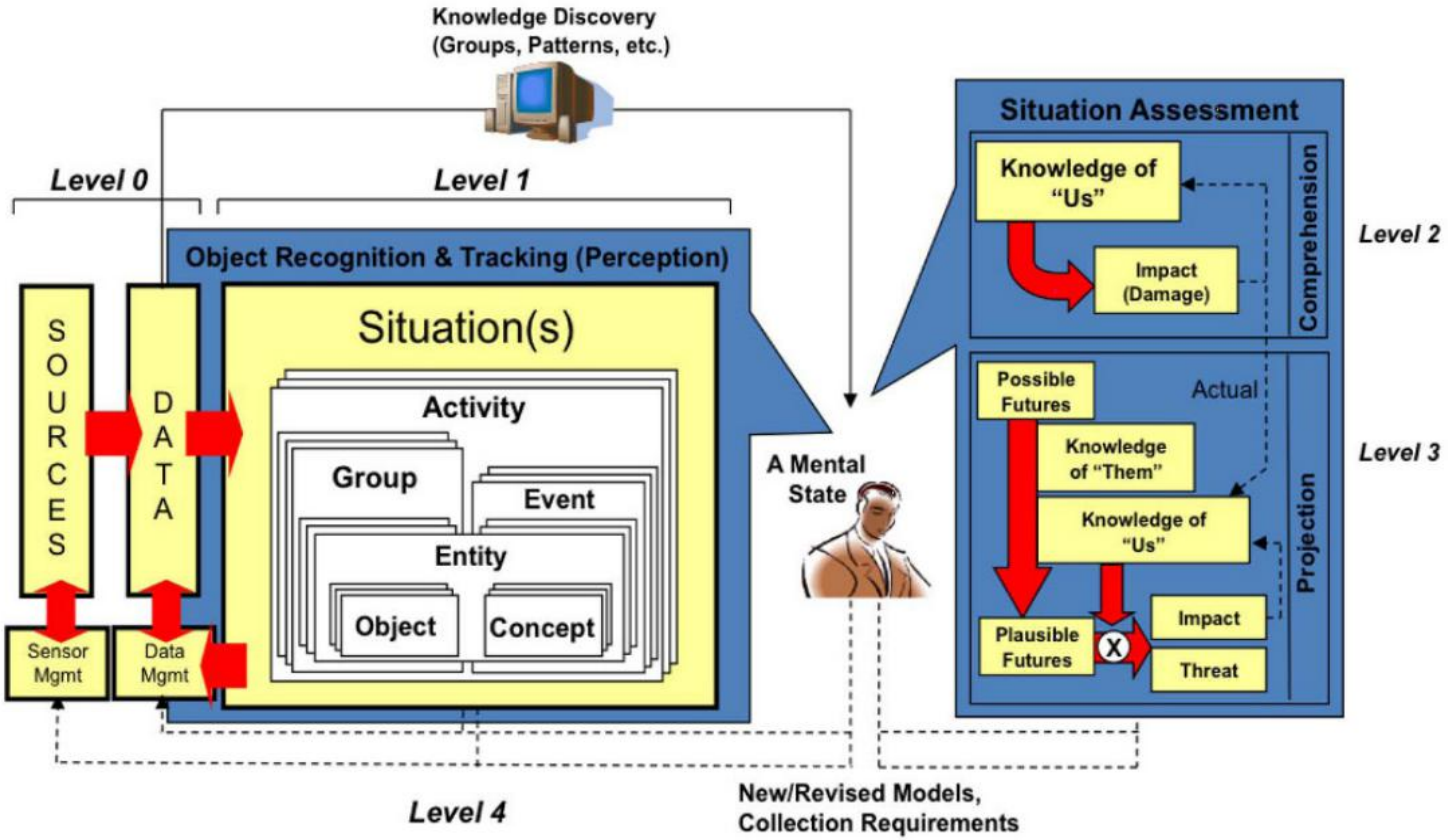
- 态势评估技术
  - 网络安全状态及可能趋势的理解



"**Situation assessment**... [is] the process of achieving, acquiring, or maintaining [situation awareness]"

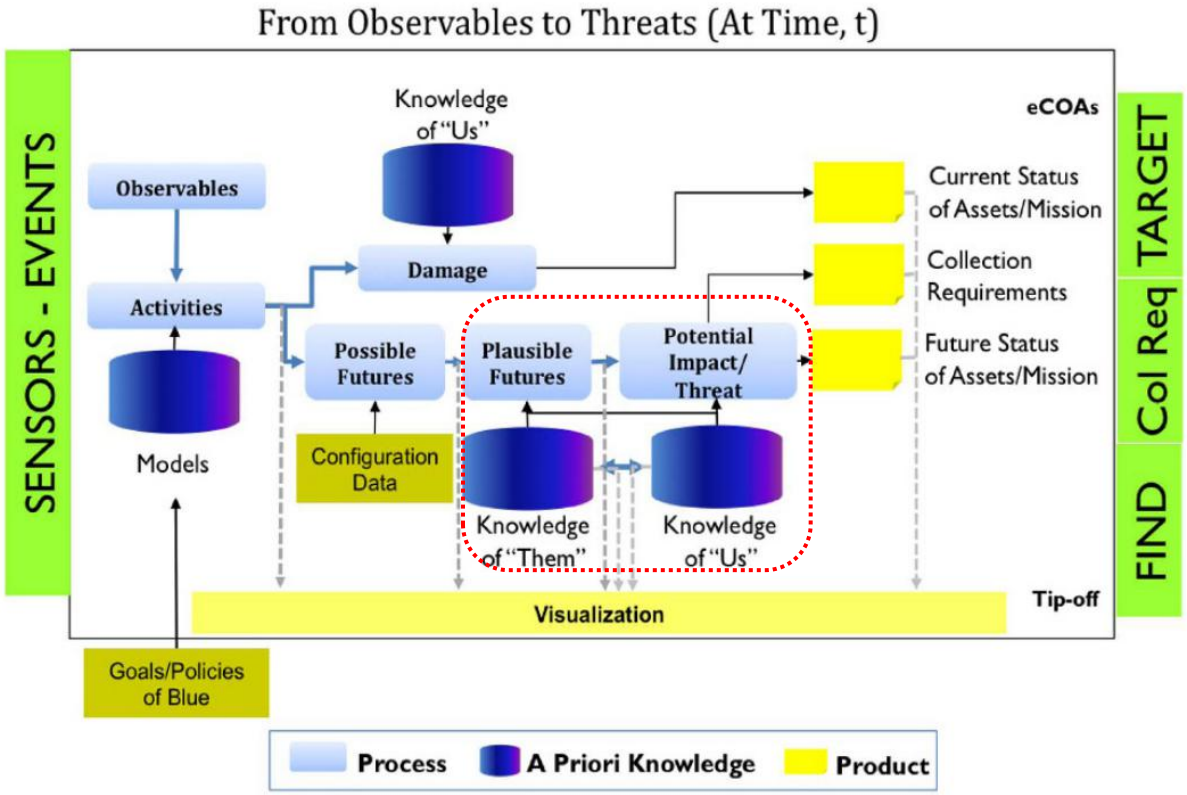
Endsley，Toward a theory of situation awareness in dynamic systems，1995
Lambert, D. The State Transition Data Fusion Model, in High-Level Information Fusion Management and System Design, Artech House (2012)

- 典型态势评估技术
  - 态势感知参考模型：“知己”、影响（损失）



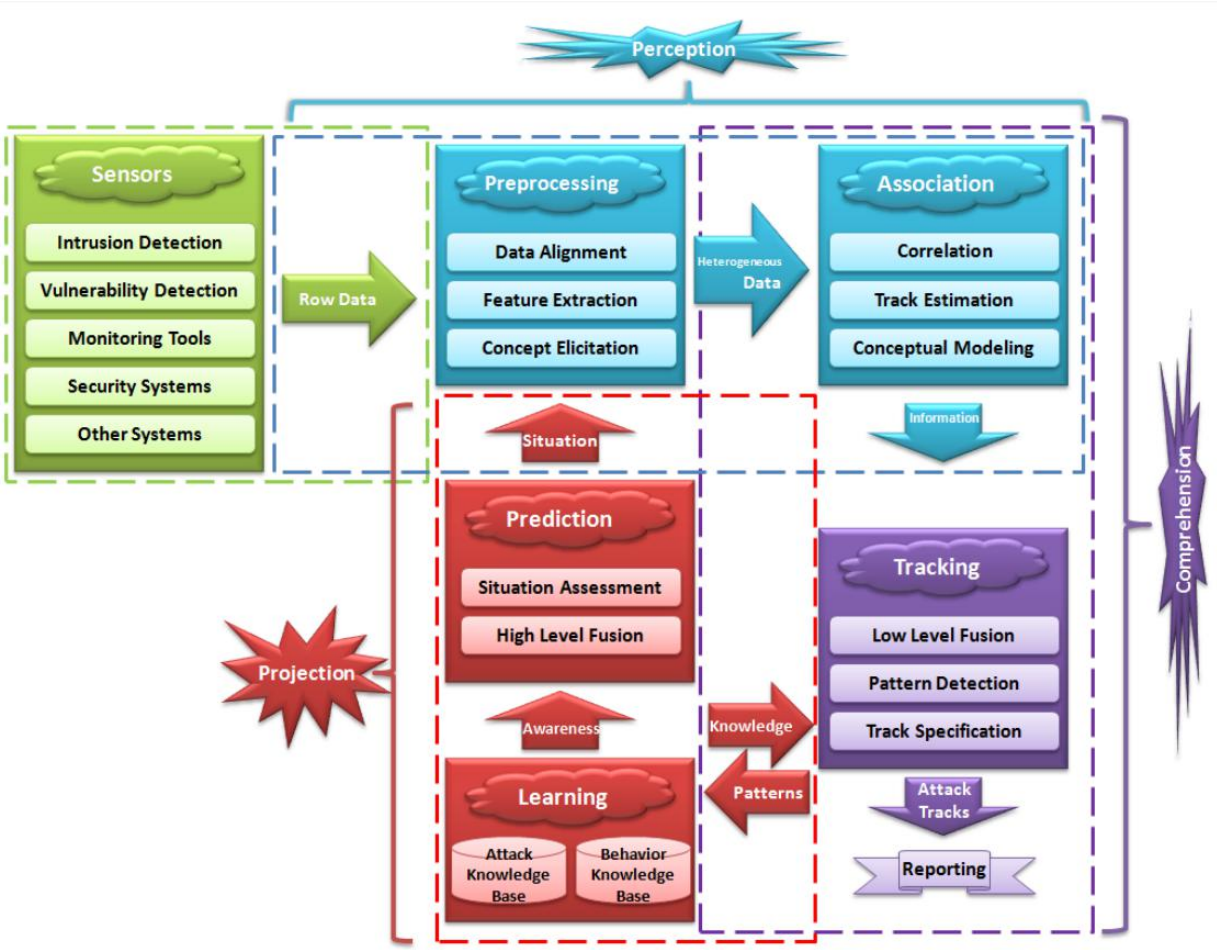
Chapter 2 Overview of Cyber Situation Awareness，George P. Tadda and John S. Salerno

- 典型态势评估技术
  - 态势感知过程模型



Chapter 2 Overview of Cyber Situation Awareness，George P. Tadda and John S. Salerno

- 典型态势评估技术
  - 智能信息驱动的融合引擎
    - 识别：预处理、关联
    - 理解：关联、追踪
    - 映射：预测、学习



Cyber Situational Awareness using Intelligent Information Fusion Engine，Ali J. RASHİDİ，2015

- 典型态势评估技术
  - 威胁分析、依赖和影响分析、可替代性分析、应对策略

A comprehensive suite of CDSA capabilities includes four core areas:

1. **Threat Analysis** – Understand and track threat landscapes and actors, along with the tactics, techniques, and procedures (TTPs) that they employ.
2. **Dependency & Impact Analysis** – Understand the mission and asset interdependencies to identify resiliency weaknesses and extrapolate mission impact.
3. **Analysis of Alternatives (AoA)** – Identify potential Courses of Action (CoAs) and other threat mitigations, explore efficient reconstitution methodologies, and evaluation architecture modernization impacts.
4. **Emerging Solutions** – Continue to advance the state of practice with new solutions that fill key gaps.

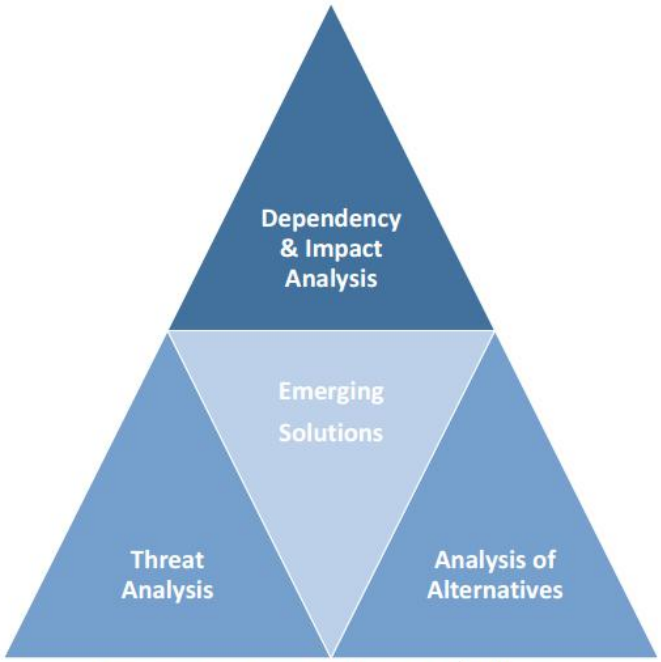


Figure 1: Core CDSA Capabilities

An Overview of MITRE Cyber Situational Awareness Solutions，MIRTE，2015

内容概要

二、面向攻击的态势评估方法

- 围绕攻击方的安全态势理解方法
  - NIST提出的策略、技术和过程(Tactics, techniques, and procedures, TTP)
  - 刘鹏等提出的能力机会意图（Capability，Opportunity、Intent，COI)
  - 面向攻击目的（主旨），分析：
    - 攻击源头、类型等；（属于态势识别层面）
    - 攻击能力、机会等；（属于攻击迭代学习）
    - 攻击影响范围和影响程度等（属于攻击后果分析）

二、面向攻击的态势评估方法

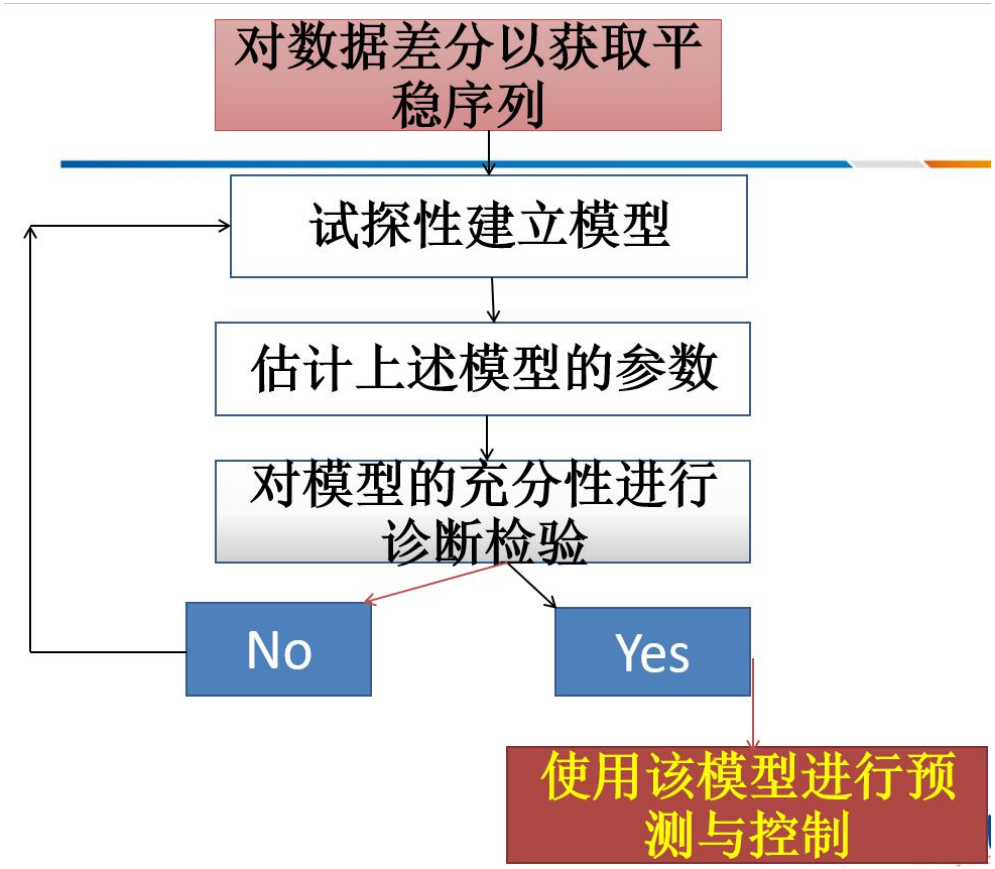
- 基于攻击迭代学习的评估方法
  - 本质上是一种攻击行为模式的学习方法
    - 时间序列分析方法
    - 马尔可夫模型方法
    - 博弈论
    - 深度学习方法

- 基于攻击迭代学习的评估方法-时间序列分析方法
  - 时序数据表示

$$\left\{y_t^*\right\}=\left\{y_1^*,y_2^*,y_3^*,\cdots,y_T^*\right\}$$

  - 随机过程
    - 利用上述时序数据来探索数据的生成机制和原理
    - 基于随机过程的结果对数据进行各种预测和检验

- 基于攻击迭代学习的评估方法-时间序列分析方法
  - 方法过程



- 基于攻击迭代学习的评估方法-时间序列分析方法
  - 自回归模型（AR模型）：通过时间序列过去时点的线性组合加上白噪声即可预测当前时点，它是随机游走的一个简单扩展
  - 移动平均模型（MA模型）：历史白噪声的线性组合，认为历史白噪声的影响是间接影响当前预测值的
  - 自回归滑动平均模型（ ARMA模型）：

$$X_t = c + \varepsilon_t + \sum_{i=1}^{p} \varphi_i X_{t-i} + \sum_{j=1}^{q} \theta_j \varepsilon_{t-j}$$

整合移动平均自回归模型（ ARIMA模型）： ARIMA（p，d，q），其中

- AR是"自回归"，p为自回归项数
- MA为"滑动平均"，q为滑动平均项数，d为使之成为平稳序列所做的差分次数（阶数）

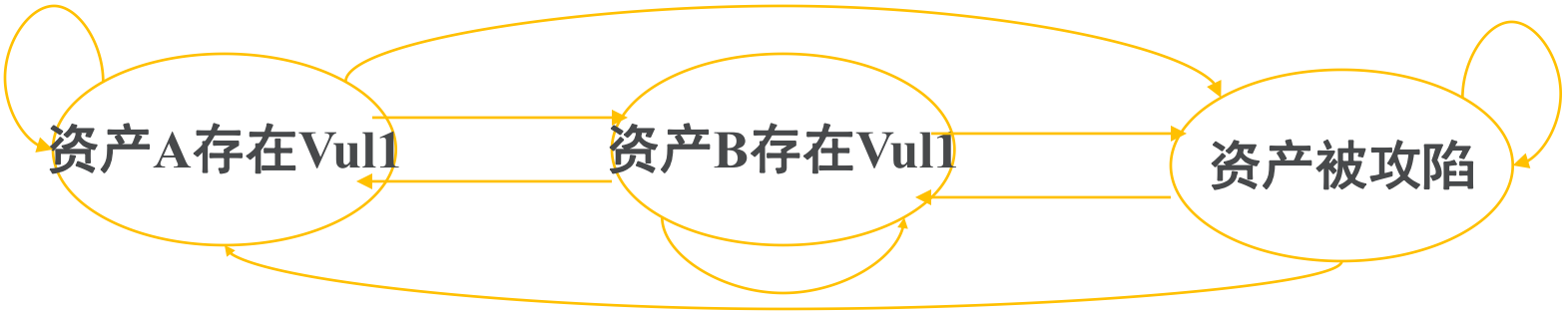
- 基于攻击迭代学习的评估方法-时间序列分析方法
  - 自回归条件异方差模型（ARCH模型）
    - 放宽了时间序列变量波动幅度恒定（方差恒定）的假设
    - 获得2003年诺贝尔经济学奖的计量经济学成果之一
  - 广义自回归条件异方差模型（GARCH模型）
    - 对误差的方差进行了进一步的建模
    - 特别适用于波动性的分析和预测

GARCH（p，q）模型为

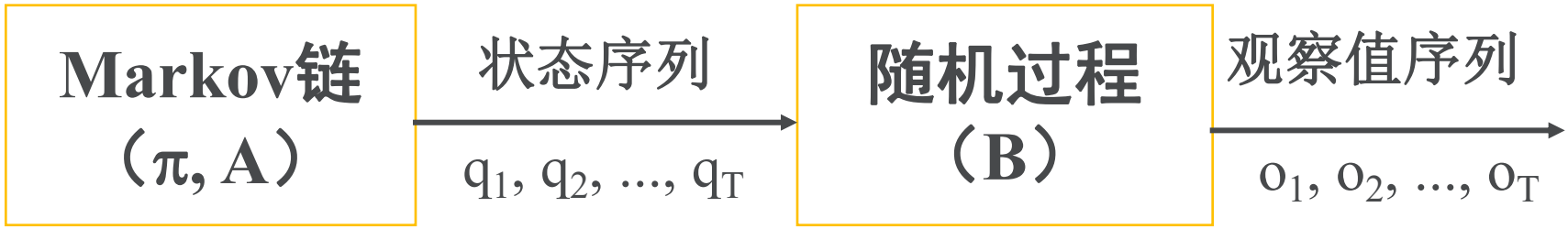
$$\sigma_t^2 = \alpha_0 + \alpha_1 \varepsilon_{t-1}^2 + \cdots + \alpha_q \varepsilon_{t-q}^2 + \beta_1 \sigma_{t-1}^2 + \cdots + \beta_p \sigma_{t-p}^2$$

一定程度上假设安全规律的周期性，无法处理海量数据

- 基于攻击迭代学习的评估方法-马尔科夫方法
  - 马尔可夫链
    - 状态空间中从一个状态到另一个状态转换的随机过程
    - 该过程要求具备“无记忆”的性质：下一状态的概率分布只能由当前状态决定，在时间序列中它前面的事件均与之无关
    - 转移概率，如下图所示
  - 隐马尔可夫模型HMM
  - 可变长马尔科夫模型VLMM



- 基于攻击迭代学习的评估方法-马尔科夫方法
  - 隐马尔可夫模型HMM
    - HMM的状态是不确定或不可见的，只有通过观测序列的随机过程才能表现出来
    - 观察到的事件与状态并不是一一对应，而是通过一组概率分布相联系
    - HMM是一个双重随机过程，两个组成部分：
      - 马尔可夫链：描述状态的转移，用转移概率描述
      - 一般随机过程：描述状态与观察序列间的关系， 用观察值概率描述



- 基于攻击迭代学习的评估方法-马尔科夫方法
  - 隐马尔可夫模型HMM组成元素
  - 一般用模型五元组　　=（N, M, π，A，B）用来描述HMM，或简写为　=(π，A，B)

参数	含义	实例
N	状态数目	攻击过程的数目
M	每个状态可能的观察值数目	资产安全状态的数目
A	与时间无关的状态转移概率矩阵	在选定某个攻击过程的情况下，选择另一个攻击过程的概率
B		安全状
p		程的概率

马尔科夫性的假设并不都不满足；转移概率刻画较难，且扩展性差

- 基于攻击迭代学习的评估方法-博弈论方法
  - 综合考虑攻击方、防御方、攻防环境三方面的因素，强调对抗性
  - 合作博弈VS非合作博弈：相互发生作用的当事人之间有没有一个具有约束力的协议，如果有，就是合作博弈，如果没有，就是非合作博弈
  - 静态博弈VS动态博弈：从行为的时间序列性上划分：静态博弈是指在博弈中，参与人同时选择或虽非同时选择但后行动者并不知道先行动者采取了什么具体行动；动态博弈是指在博弈中，参与人的行动有先后顺序，且后行动者能够观察到先行动者所选择的行动
  - 完全信息博弈VS不完全信息博弈：从参与人对其他参与人的了解程度上划分；完全博弈是指在博弈过程中，每一位参与人对其他参与人的特征、策略空间及收益函数有准确的信息
  - 重复博弈VS单次博弈

- 基于攻击迭代学习的评估方法-博弈论方法
  - 标准式博弈由三种元素组成：参与人、纯策略、收益函数
    - 纯策略；
    - 混合策略是在纯策略上的概率分布
  - 实例
    - 类型空间：参与者类型的集合
    - （先验）信念空间：先验信念是指每个参与者在进行博弈时认为其它参与者是某种类型的先验概率，参与者的先验信念空间是该参与者先验信念的集合
    - 行动空间：每个参与者在博弈时依据其类型可以做的某种具体选择，参与者的行动空间是指该参与者的行动集合
    - 效用：参与者在博弈时依据其类型和所选择的行动所能获得的收益

- 基于攻击迭代学习的评估方法-博弈论方法

  - 纳什均衡：如果博弈中的任意一个参与人选择的纯策略，都是对其他人选择的纯策略的最优反应，那么这样的纯策略组合为一个标准式博弈的纯策略纳什均衡：

$$\forall s_i \neq s_i^*, u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*).$$

  - 严格占优策略：任意给定其他博弈参与人的纯策略选择组合，如果某一个特定的纯策略满足如下条件，则称这个纯策略为严格占优策略：

$$\forall s_{-i}, \forall s_i' \neq s_i^*, u_i(s_i^*, s_{-i}) > u_i(s_i', s_{-i})$$

- 基于攻击迭代学习的评估方法-博弈论方法

- 二十世纪八十年代之后，研究工作围绕着修正经典博弈论中的完全理性假设展开研究，并试图为纳什均衡的概念寻找动态结构下的解释。研究表明：经典博弈论在应用中遇到困难，主要是存在三种缺陷：假设缺陷、方法缺陷、实证缺陷。
- 为了解决经典博弈论的以上三种缺陷，从二十世纪九十年代发展了演化博弈论的研究工作。

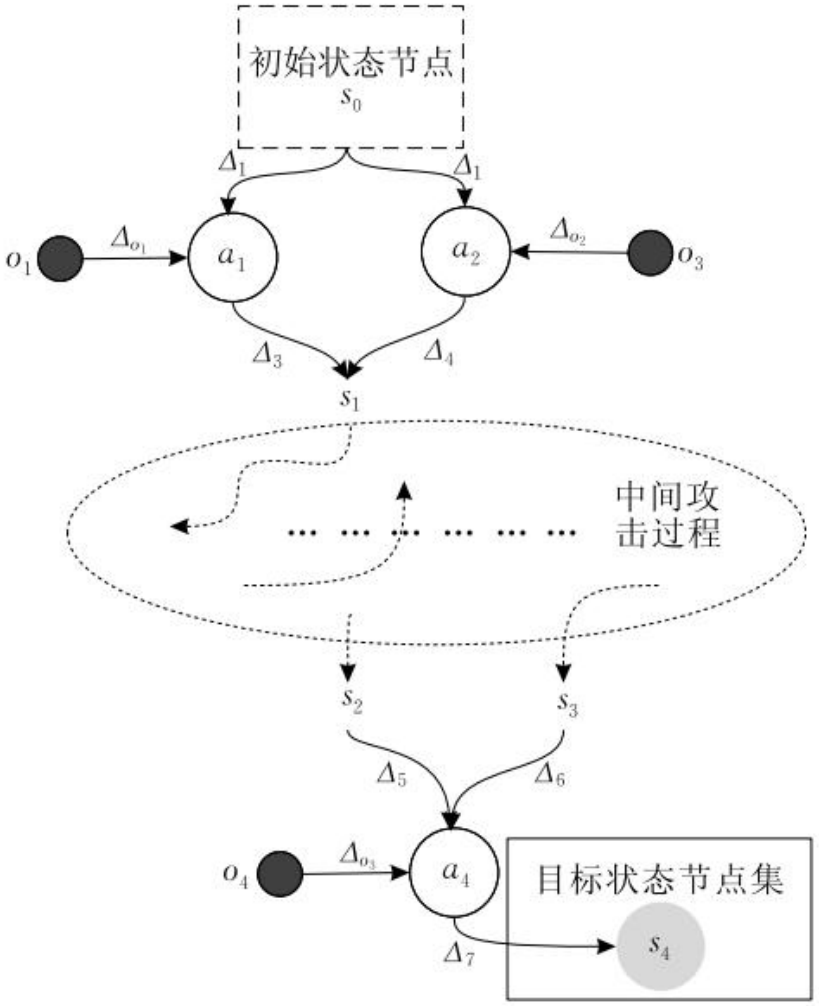
- 基于攻击迭代学习的评估方法-博弈论方法
  - 假设缺陷：完全理性假设，即假定参与人完全了解其对手的策略集合以及使用每个策略的概率，同时也了解博弈规则与收益结构。参与人也具有通过精确计算推理得到最优策略的能力。但现实中的参与人只具有有限理性(Bounded Rationality)
  - 方法缺陷：经典博弈论关注的重点是如何求解博弈的平衡结构，但不能解释博弈的各参与方是如何通过参与博弈而趋向于这些均衡状态的(H.P. Young)
  - 实证缺陷：多数解析型博弈论的预测都是基于理想的假设和精确的数学推导，需要实证的经验规律来充实经典博弈论(Colin Camerer)

- 基于攻击迭代学习的评估方法-博弈论方法
  - 演化博弈研究具有普遍意义的有限理性的参与人：惰性、近视、遗传、突变、变异。Kandori, Mailath和Rob (1993)
  - 演化博弈不仅关注博弈的稳定结构，还通过引入不同的动态机制研究博弈系统的稳定结构和演化过程之间的关系
  - 演化博弈模型可以和个人学习机制相结合，可以探讨微观层面上参与人的互动和宏观层面上群体的均衡现象之间的关系
  - 演化博弈的假设条件与建模方法更加有利于进行模拟实验来获得实证数据

考虑因素众多，建模较为复杂；攻防的行动空间规模可能很大，方法很难扩展

二、面向攻击的态势评估方法

- 基于攻击后果分析的评估方法
  - 攻击成功可能性：前面的学习方法
  - 攻击影响范围：风险传播方法
  - 攻击影响程度：攻击性质+攻击对象重要性程度



基于概率攻击图的内部攻击意图推断算法研究，陈小军等，计算机学报，2014

二、面向攻击的态势评估方法

- 基于攻击后果分析的评估方法-风险传播分析
  - 风险传播模型
    - 节点影响力
    - 传播动力学
  - SIR模型
    - 最经典的模型，其中S表示易感者，I表示感染者，R表示移出者
  - SIS模型
  - SIRS模型
  - …

1）如果一个传播节点与一个未感染节点接触，则未感染节点会以概率 p_1 成为传播节点.

2）如果一个传播节点与一个免疫节点接触，则传播节点会以概率 p_2 成为免疫节点.

3）传播节点不会无休止地传播下去，会以一定的速度 v 停止传播而变为免疫节点，且无需与其他节点接触.

传播规则实例

二、面向攻击的态势评估方法

- 基于攻击后果分析的评估方法-攻击影响程度
  - 网络安全人员根据网络安全态势觉察识别出来的攻击活动和其他检测设备的报告内容，借助数学工具等模型，分析它对网络、系统资源等诸因素已经产生的影响
  - 基于知识推理的方法
  - 基于统计的方法
  - 基于灰度理论的方法

网络安全态势感知综述，龚俭，软件学报，2017

- 基于攻击后果分析的评估方法-攻击影响程度
  - 基于知识推理的方法
    - 基于知识推理的方法是凭借专家知识及经验建立评估模型，通过逻辑推理分析整个网络的安全态势
    - 基本思想是：借助概率论、模糊理论、证据理论等来表达和处理安全属性的不确定性，通过推理汇聚多属性信息
    - 相关方法有两类：
      - 基于图模型的推理， 如贝叶斯网络、模糊认知图 (fuzzy cognitive map, 简称FCM)等
      - 基于证据理论的推理， 如D-S证据推理

网络安全态势感知综述，龚俭，软件学报，2017

- 基于攻击后果分析的评估方法-攻击影响程度
  - 基于统计的方法
    - 统计分析的目的是综合考虑影响网络安全的态势要素，构建一个评估函数，实现态势要素和整个网络态势空间的映射
      - 权重分析方法
      - 层次分析法 (analytic hierarchy process, 简称AHP)

网络安全态势感知综述，龚俭，软件学报，2017

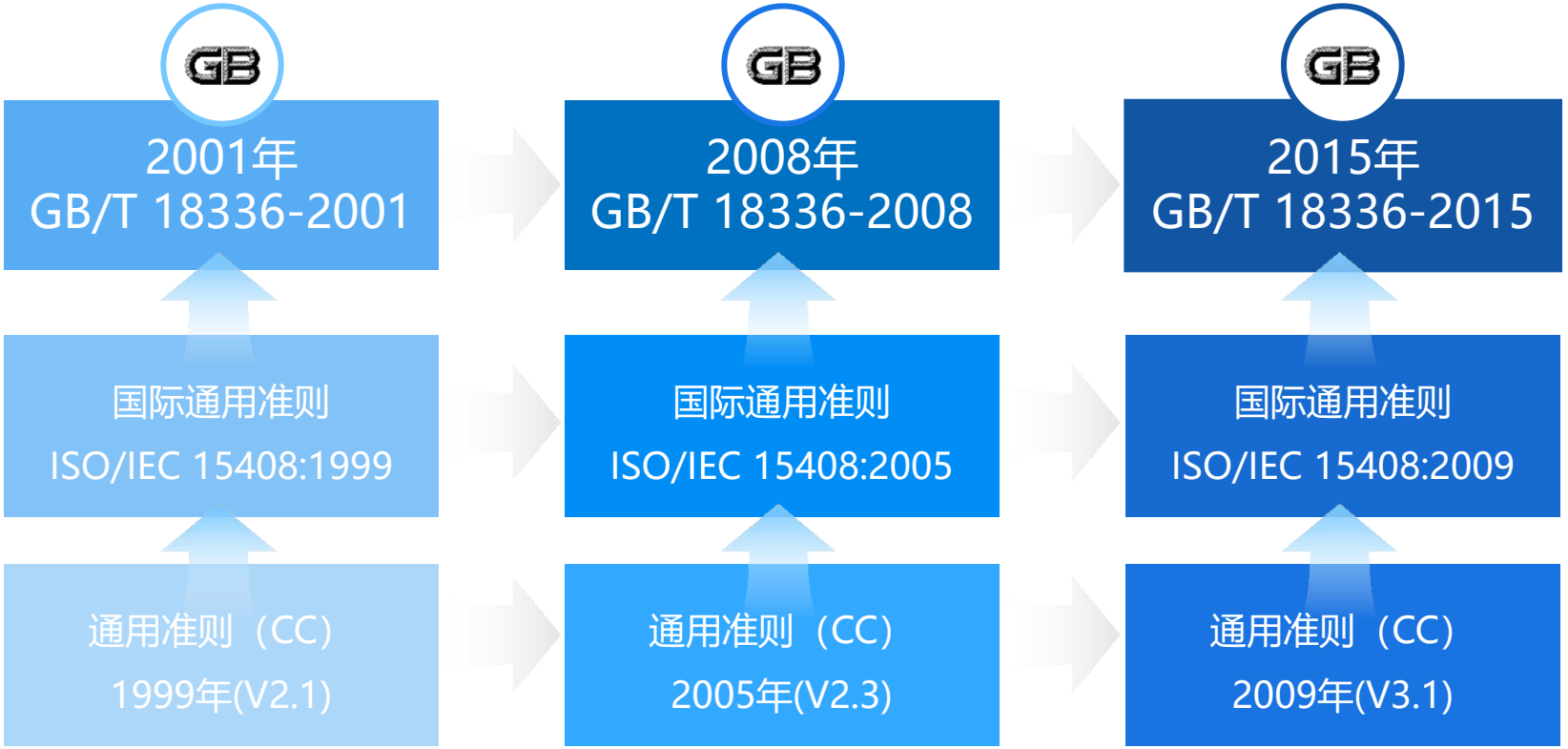
- 基于攻击后果分析的评估方法-攻击影响程度
  - 基于灰色理论的方法
    - 安全态势的趋势变化既有已知信息，也有未知和不确定信息，这种特点决定了安全态势风险值的变化作为一个“灰色系统”而存在
    - 灰色系统理论以“部分信息已知, 部分信息未知的小样本、贫信息”的不确定性系统作为研究对象，并在此基础上提取有用信息
    - 灰色系统利用累加生成或逆累加生成的新数据进行建模，有利于找出数据的变化规律，具有弱化原始数据的随机性、所需样本少、短期预测精度高等特点

网络安全态势感知综述，龚俭，软件学报，2017

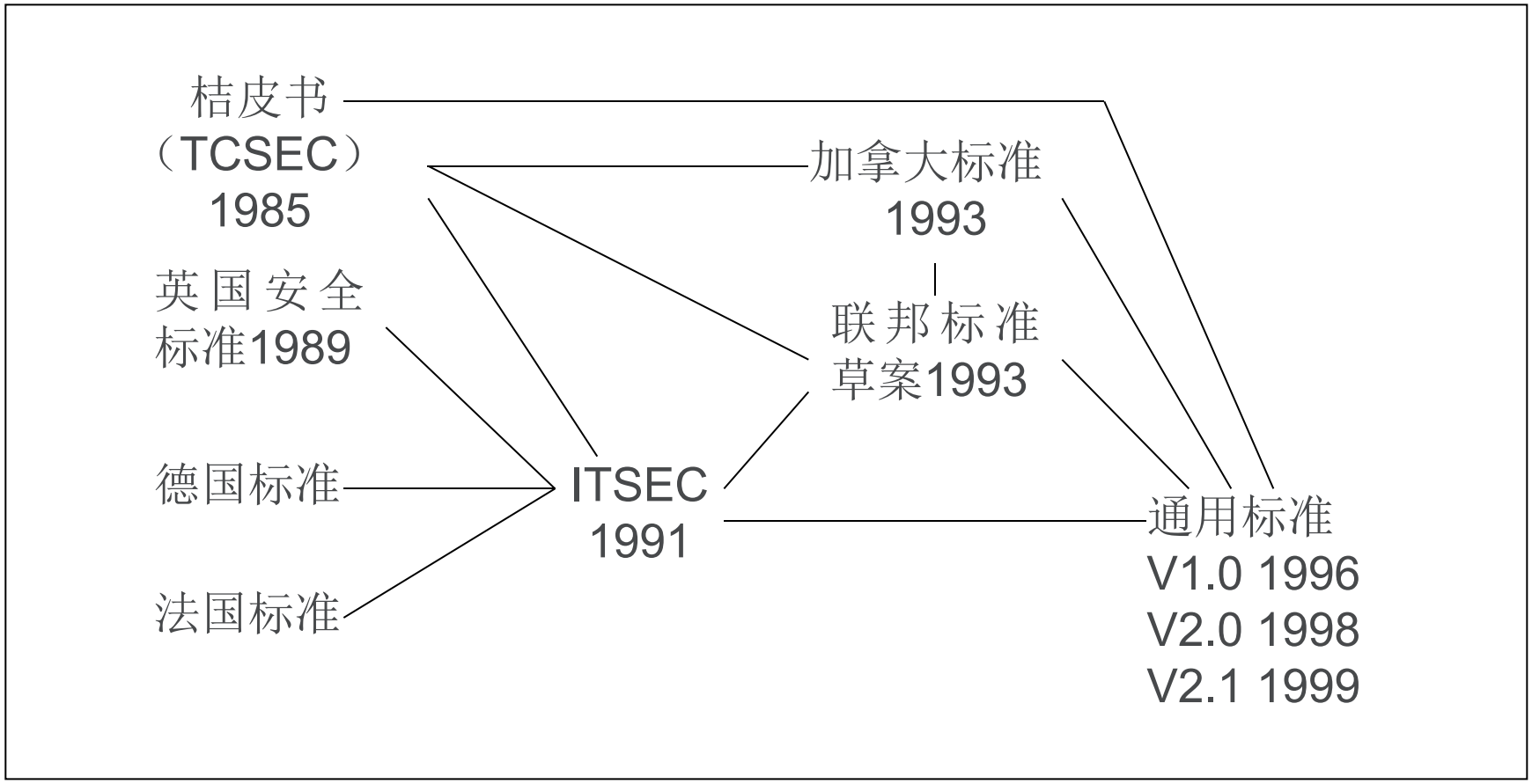
内容概要

- 基于防护方的态势评估方法
  - 自己方防护能力的评估
    - 产品级：通用准则（Common Criteria）评估
    - 系统级：等级保护评估
    - 数据级：数据安全能力成熟度评估
  - 自己方弱点的评估
    - 脆弱性利用可能性及后果的评估

- 基于防护方的态势评估方法-通用准则评估



- 基于防护方的态势评估方法-通用准则评估



基于防护方的态势评估方法-通用准则评估

- PP (Protection Profile) :

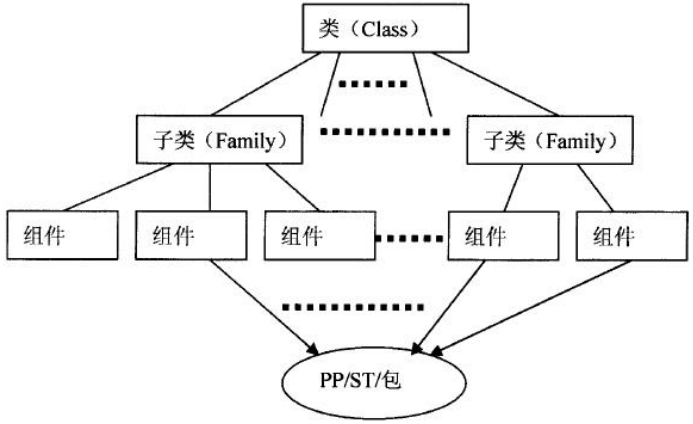
  PP是一类TOE基于其应用环境定义的一组安全要求，不管这些要求如何实现，实现问题交由具体ST实现，PP确定在安全解决方案中的需求

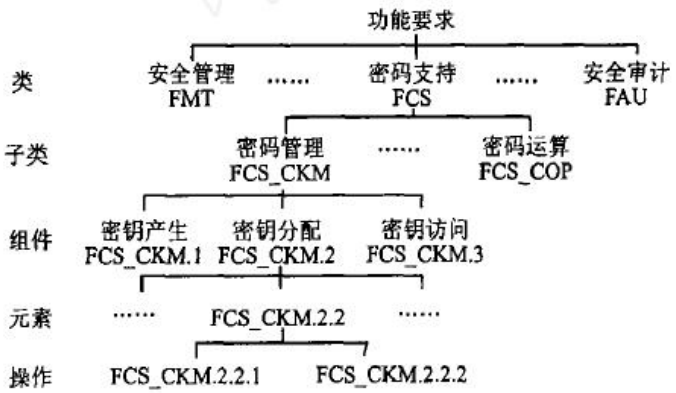
- ST (Security Target) :

  ST是依赖于具体的TOE的一组安全要求和说明，用来指定TOE的评估基础

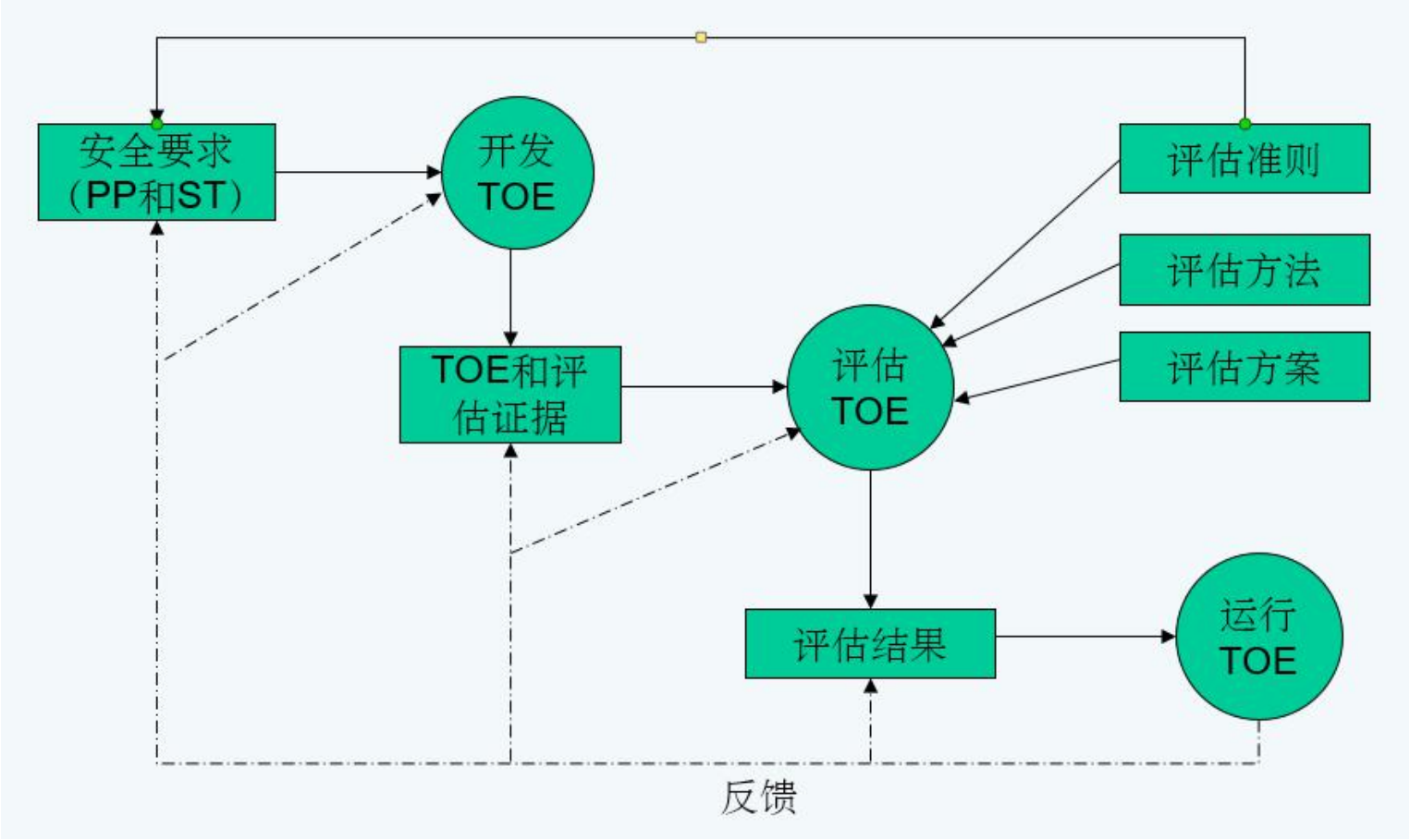
- TOE (Target of Evaluation) :

  TOE评估对象，作为评估主体的IT产品及系统以及相关的管理员和用户指南文档

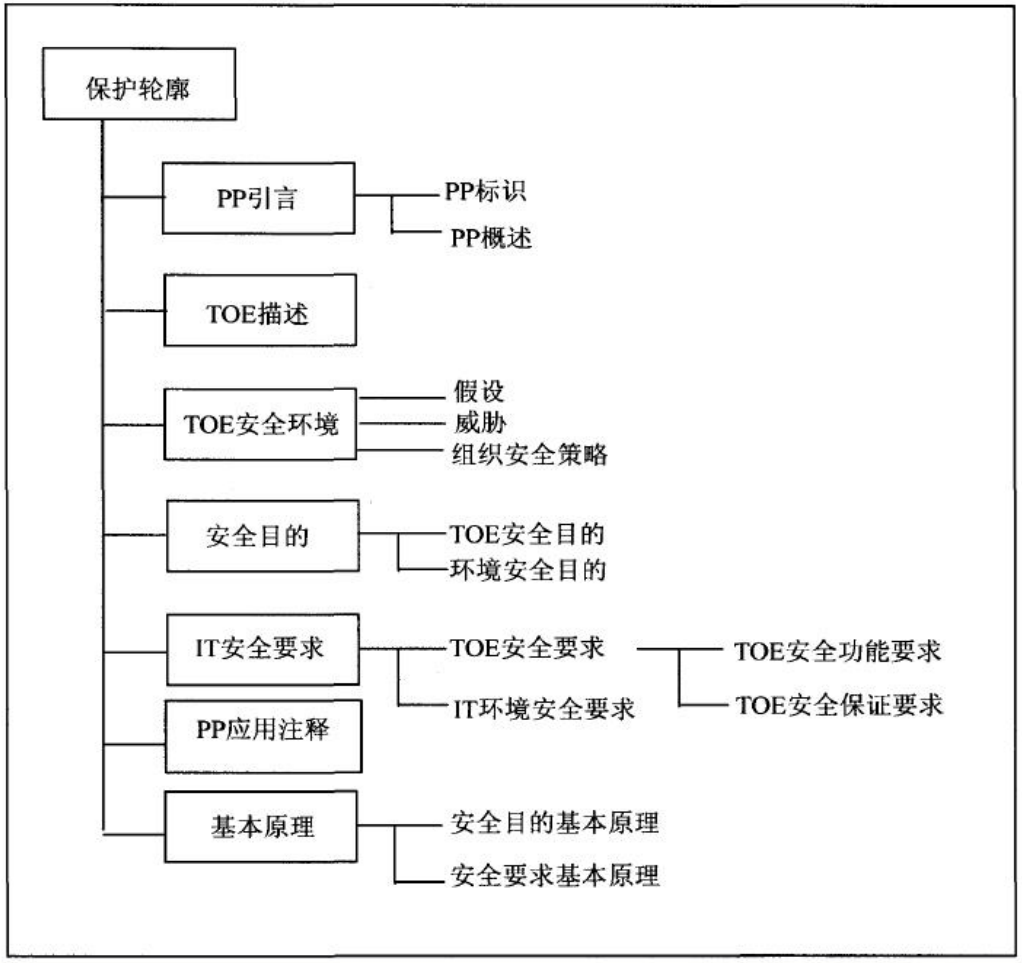




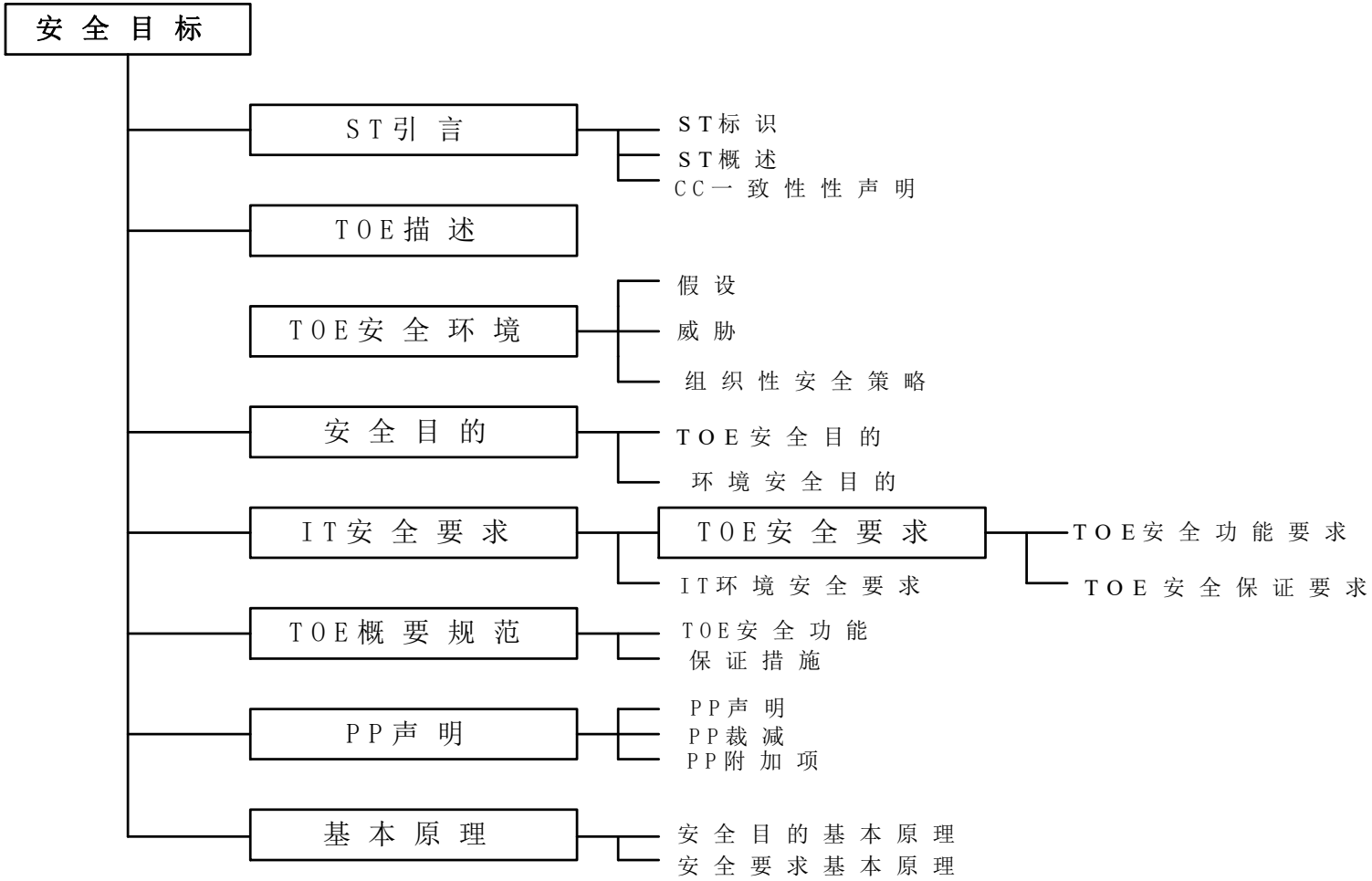
- 基于防护方的态势评估方法-通用准则评估
  - TOE评估过程



- 基于防护方的态势评估方法-通用准则评估
  - 保护轮廓结构



- 基于防护方的态势评估方法-通用准则评估
  - 安全目标结构



- 基于防护方的态势评估方法-通用准则评估

- 基于防护方的态势评估方法-自己方弱点评估
  - 攻击图方法
    - 攻击图技术能够把网络中各主机上的脆弱性关联起来进行深入地分析，发现威胁网络安全的攻击路径并用图的方式展现出来
    - 安全管理人员利用攻击图可以直观地观察到网络中各脆弱性之间的关系，选择最小的代价对网络脆弱性进行弥补
    - 攻击图生成技术是指利用目标网络信息和攻击模式生成攻击图的方法，是攻击图技术中的基础
    - 攻击图分析技术是指分析攻击图，得到关键节点和路径或者对脆弱性进行量化的方法

- 基于防护方的态势评估方法-自己方弱点评估
  - 攻击图方法
    - 攻击图生成方法
      - MulVAL（多主机、多阶段的脆弱性分析）
        - MulVAL具有强大的网络数据采集能力和性能优势，MulVAL最后生成的逻辑攻击图的规模随着网络规模大小的变化为O（n^2）
      - 麻省理工
        - Net
          数量

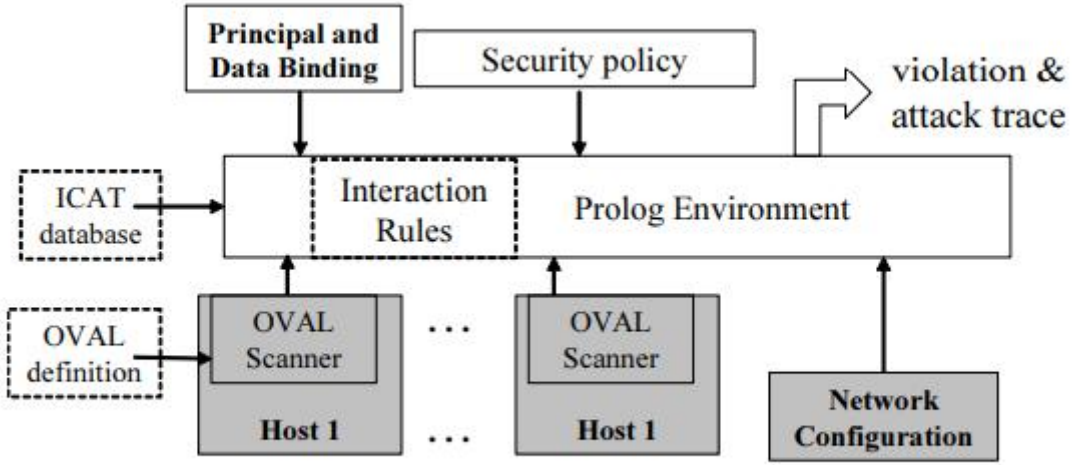


Figure 1: The MulVAL framework

- 基于防护方的态势评估方法-自己方弱点评估
  - 攻击图方法

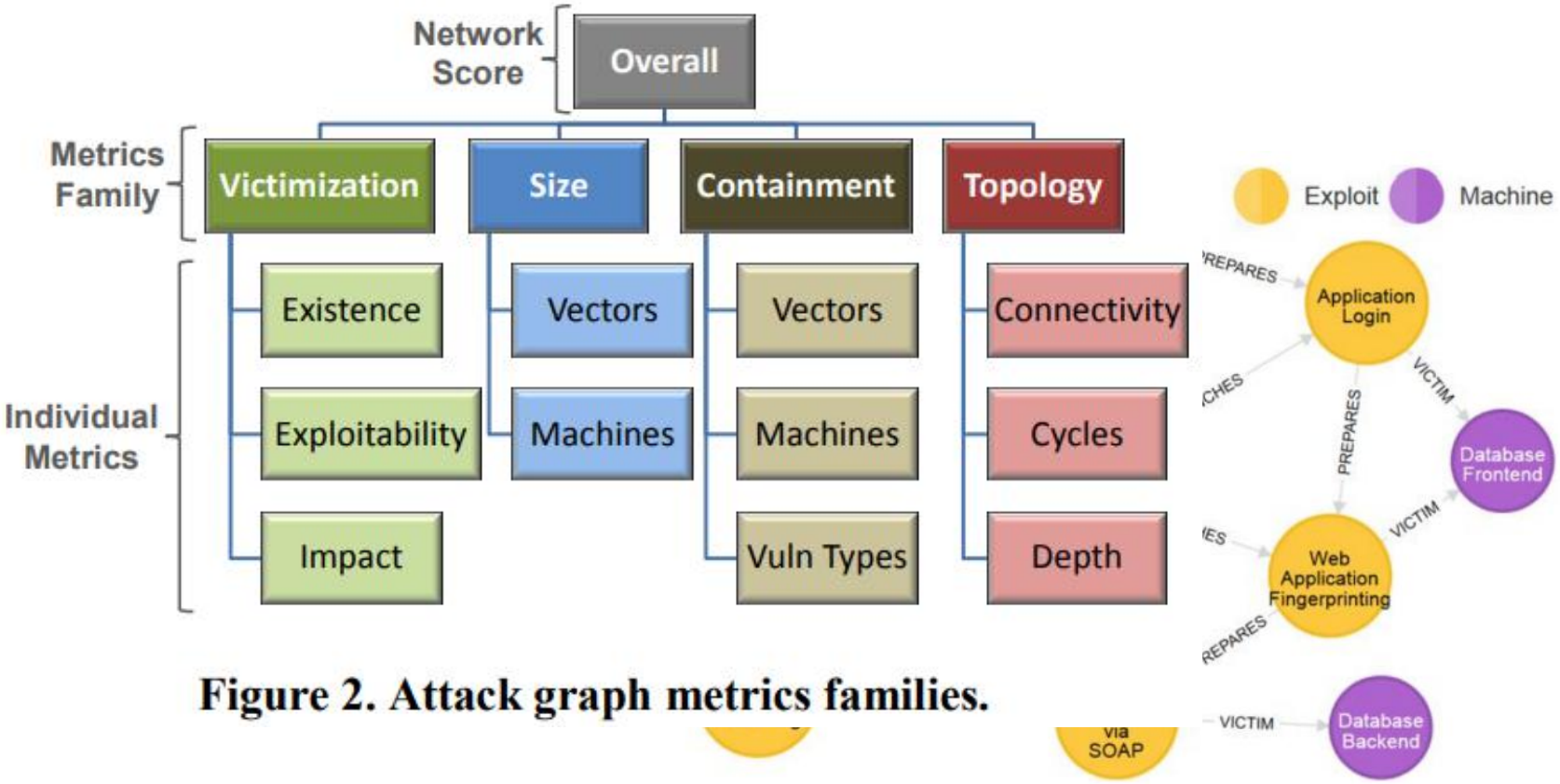
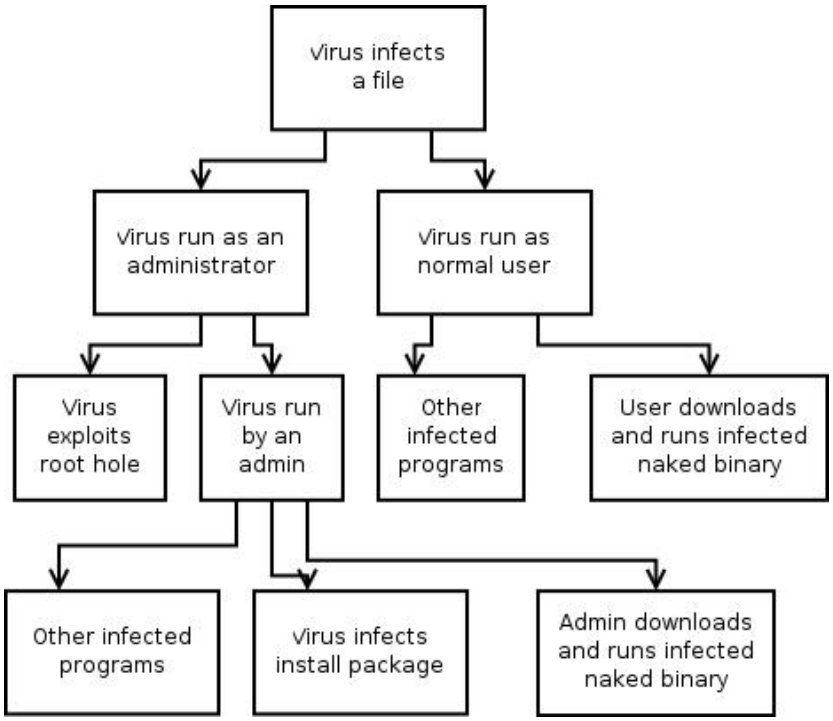


Figure 2. Attack graph metrics families.

Figure 11. Chain of potential exploits with attackers and victims.

Big-Data Architecture for Cyber Attack Graphs,2015

- 基于防护方的态势评估方法-自己方弱点评估
  - 攻击树方法
    - 用树型结构来表示系统面临的攻击，其中根节点代表被攻击的目标，叶节点表示达成攻击目标的方法



- 基于防护方的态势评估方法-自己方弱点评估
  - 攻击防护树方法The Attack-Defense Tree
    - 对攻击场景进行建模和分析的方法

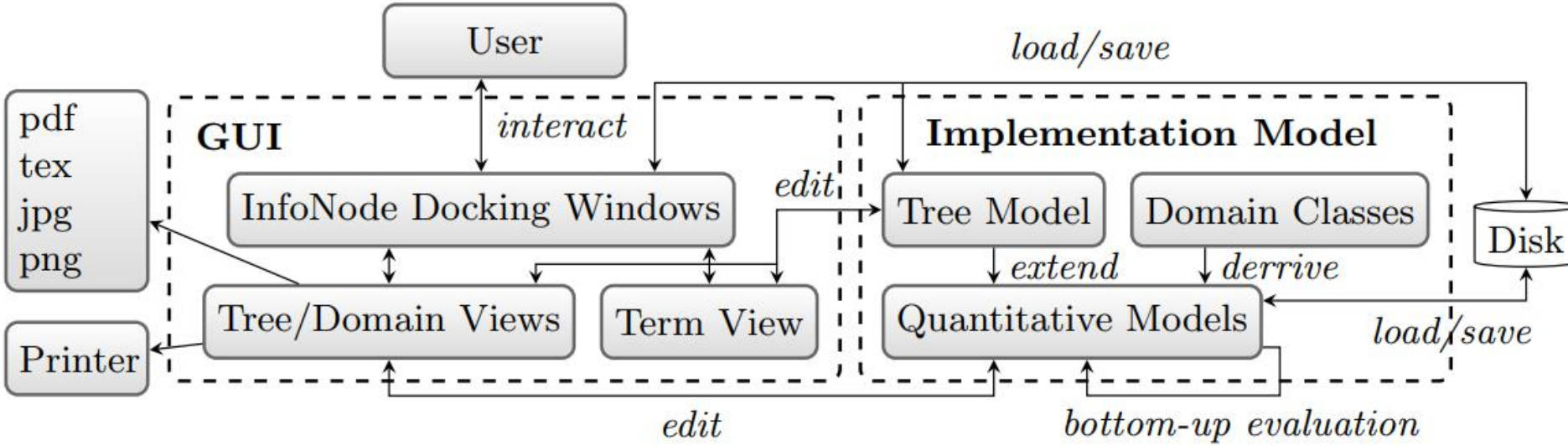
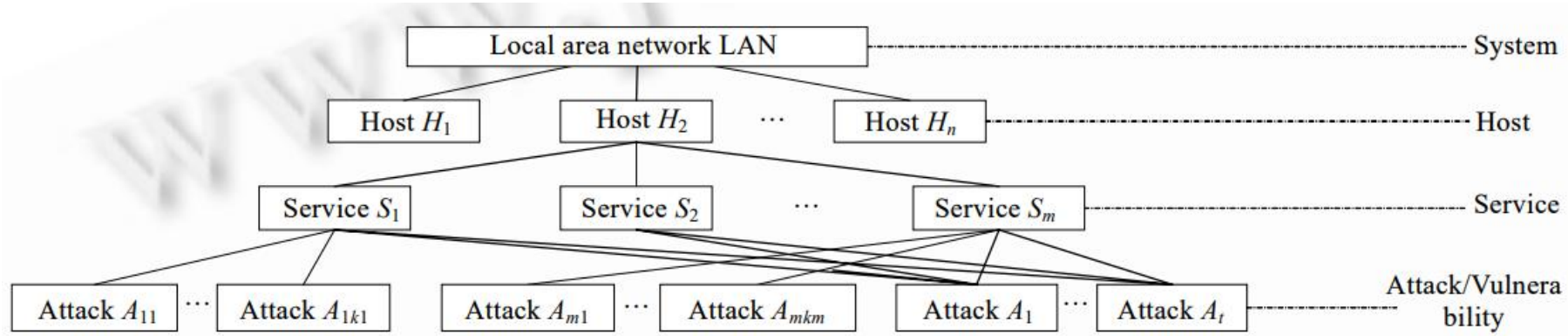


Fig. 6. An overview of the ADTool architecture

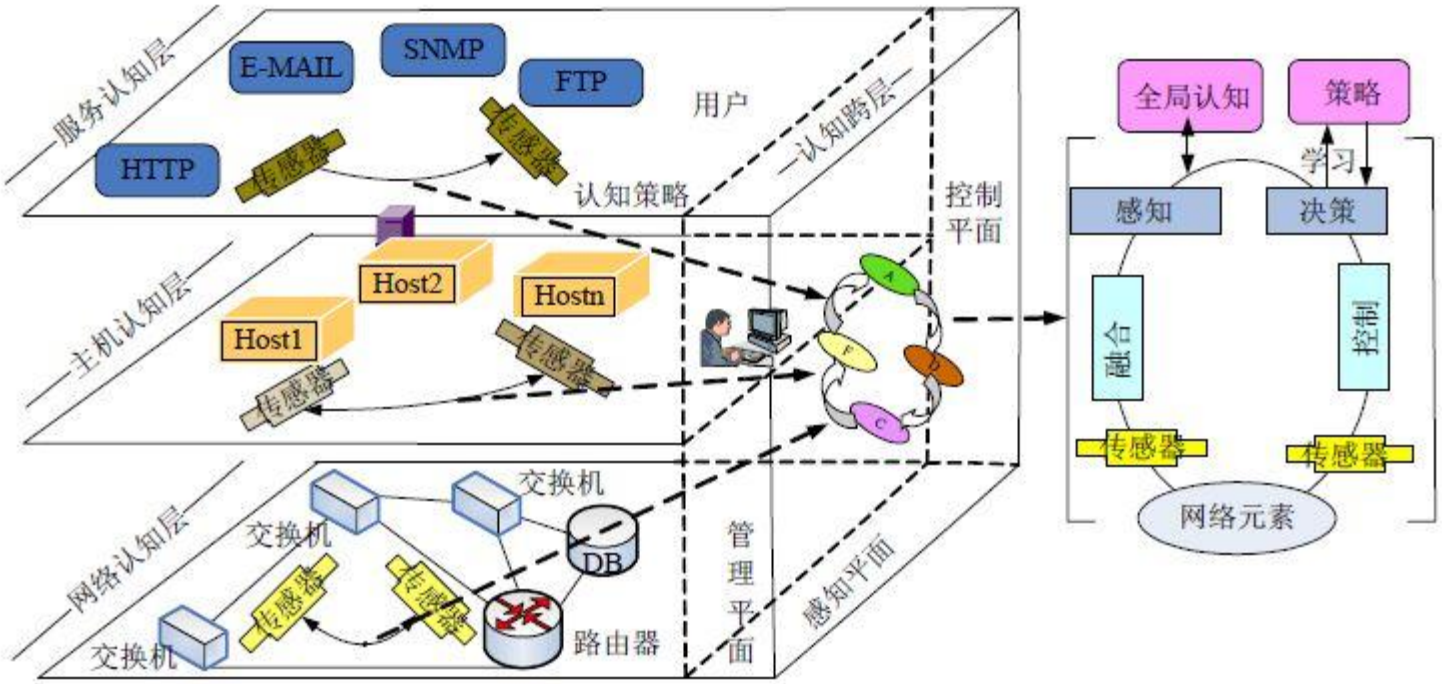
http://satoss.uni.lu/members/piotr/adtool/

- 基于防护方的态势评估方法-自己方弱点评估
  - 分层评估方法
    - 服务层
    - 主机层
    - 网络层



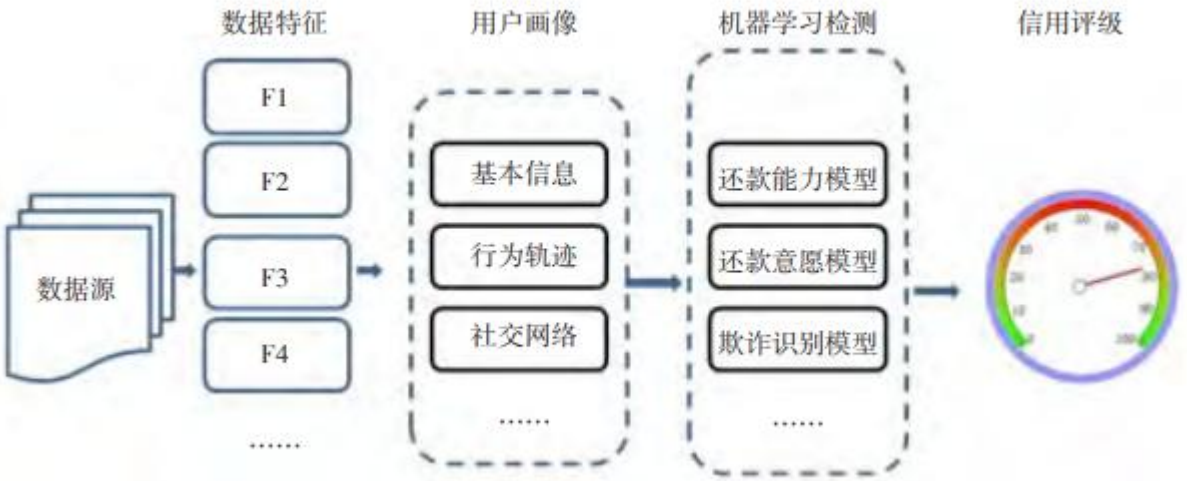
层次化网络安全威胁态势量化评估方法，软件学报，2006

- 基于防护方的态势评估方法-自己方弱点评估
  - 分层评估方法
    - 服务层
    - 主机层
    - 网络层



网络安全态势认知融合感控模型，软件学报，2016

- 基于防护方的态势评估方法-自己方弱点评估
  - 分域评估方法
    - 攻击方
    - 防护方
    - 人物地事



内容概要

- 态势评估技术示例

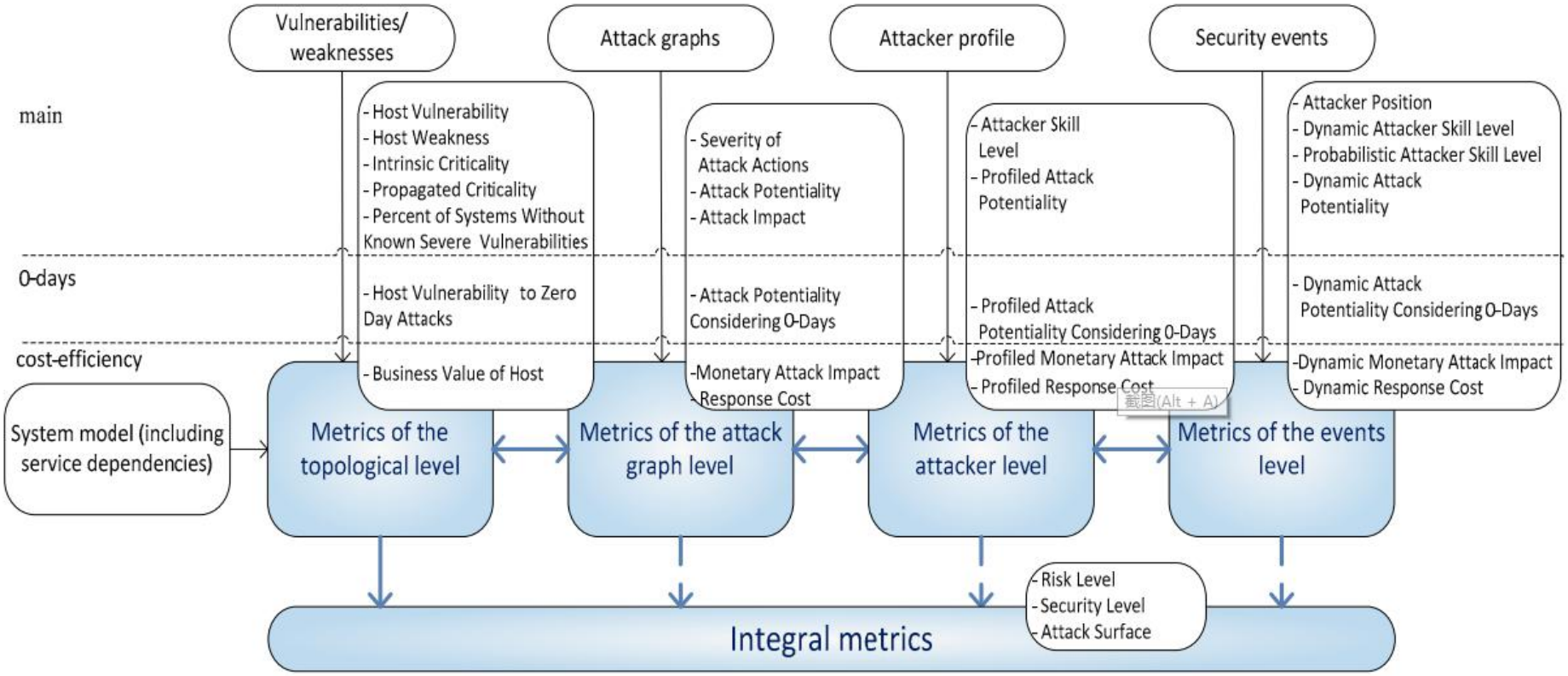


Fig. 1. Security metrics overview

Security Evaluation for Cyber Situational Awareness，I Kotenko，2014

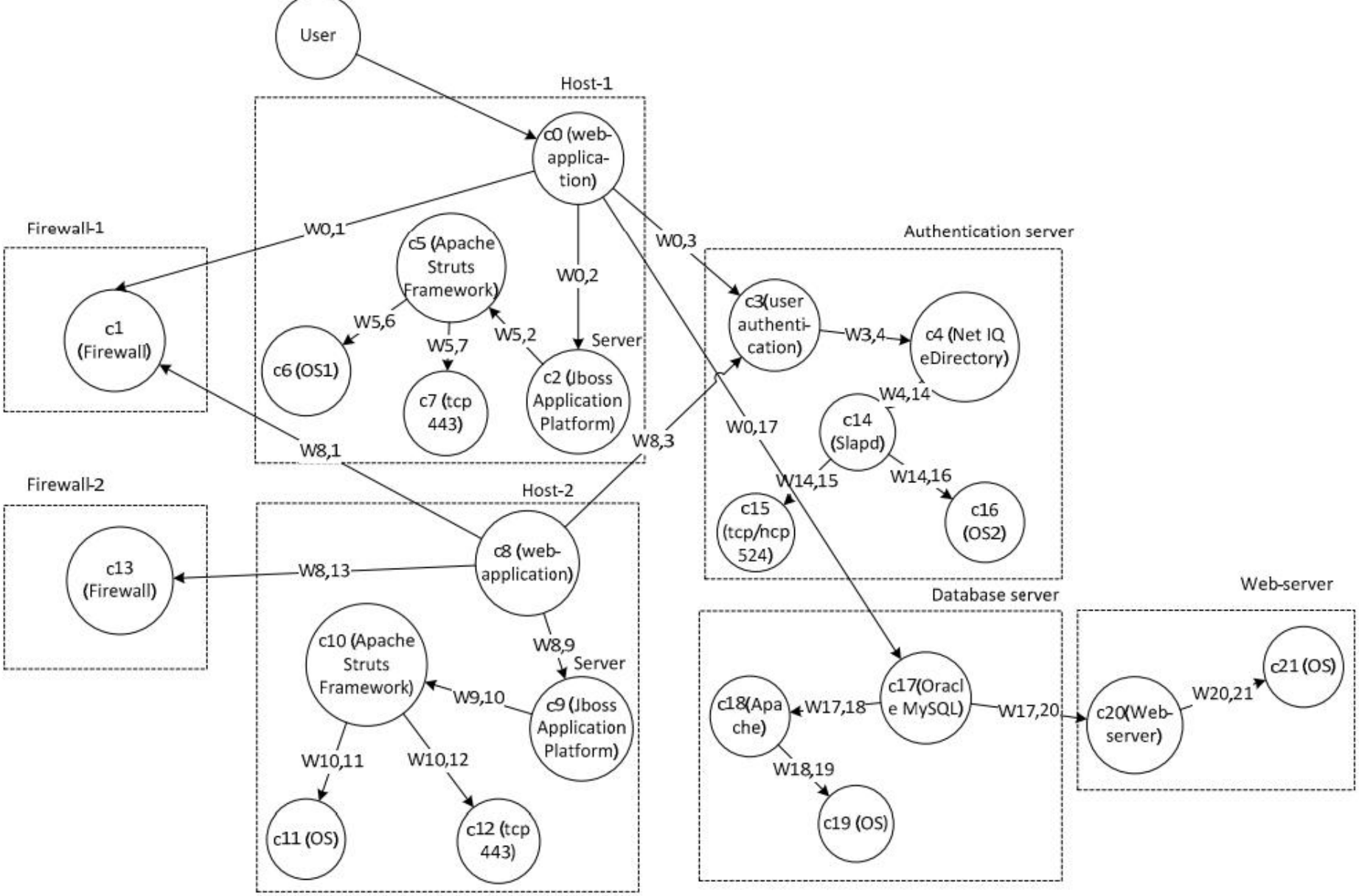


Fig.3. Service dependencies

Security Evaluation for Cyber Situational Awareness，I Kotenko，2014

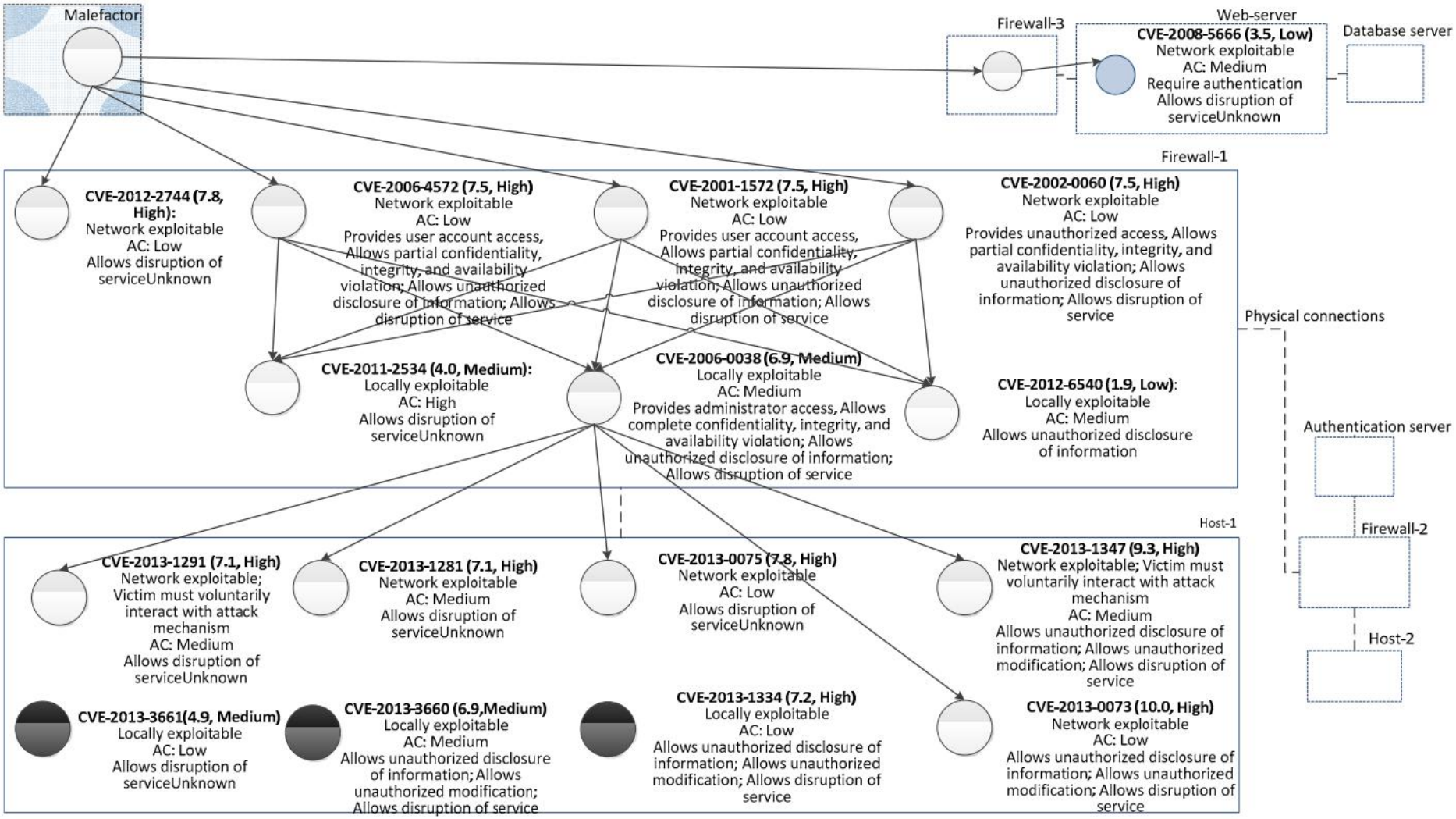


Fig.4. Attack graph

Security Evaluation for Cyber Situational Awareness，I Kotenko，2014

内容概要

- 评价体系方面
  - 统一有效的评价体系：范围、方法、意义的统一
- 评估模型方面
  - 模型完备性：考虑要素是否全面
  - 模型扩展性
  - 高层建模的问题：如语义级的建模及分析
- 知识融合方面
  - 不确定知识融合
  - 海量知识的融合
  - 冲突知识的融合
  - 小样本的知识发掘：缺量数据下的知识模式发掘

网络安全态势评估技术

Q&A