RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

共享威胁情报分析以实现协作式攻击分析

Samir Saklikar
EMC 的安全产品分公司 RSA

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

专题会议 ID：TH-1005
专题会议分类：高级

议程

- 先进的有针对性的威胁和挑战
- 需要协作和威胁情报共享
  - 现有标准
- 共享事件分析过程详细信息方面的限制
- 建议 – 通过以下方式拓展威胁情报共享：
  - 基于机器的分析表示形式
    - 利用现有标准
  - 分析师操作表示形式
    - 建议新标准
- 结论

攻击

- 先进的有针对性的威胁
  - 确定的网络对手
  - 自定义恶意软件、零时差攻击、社交工程
  - 少而慢的多阶段横向移动
  - 多样化的并发攻击媒介
  - P2P 加密的 C&C 活动
  - 隐藏在醒目位置（http、社会媒体）

目标

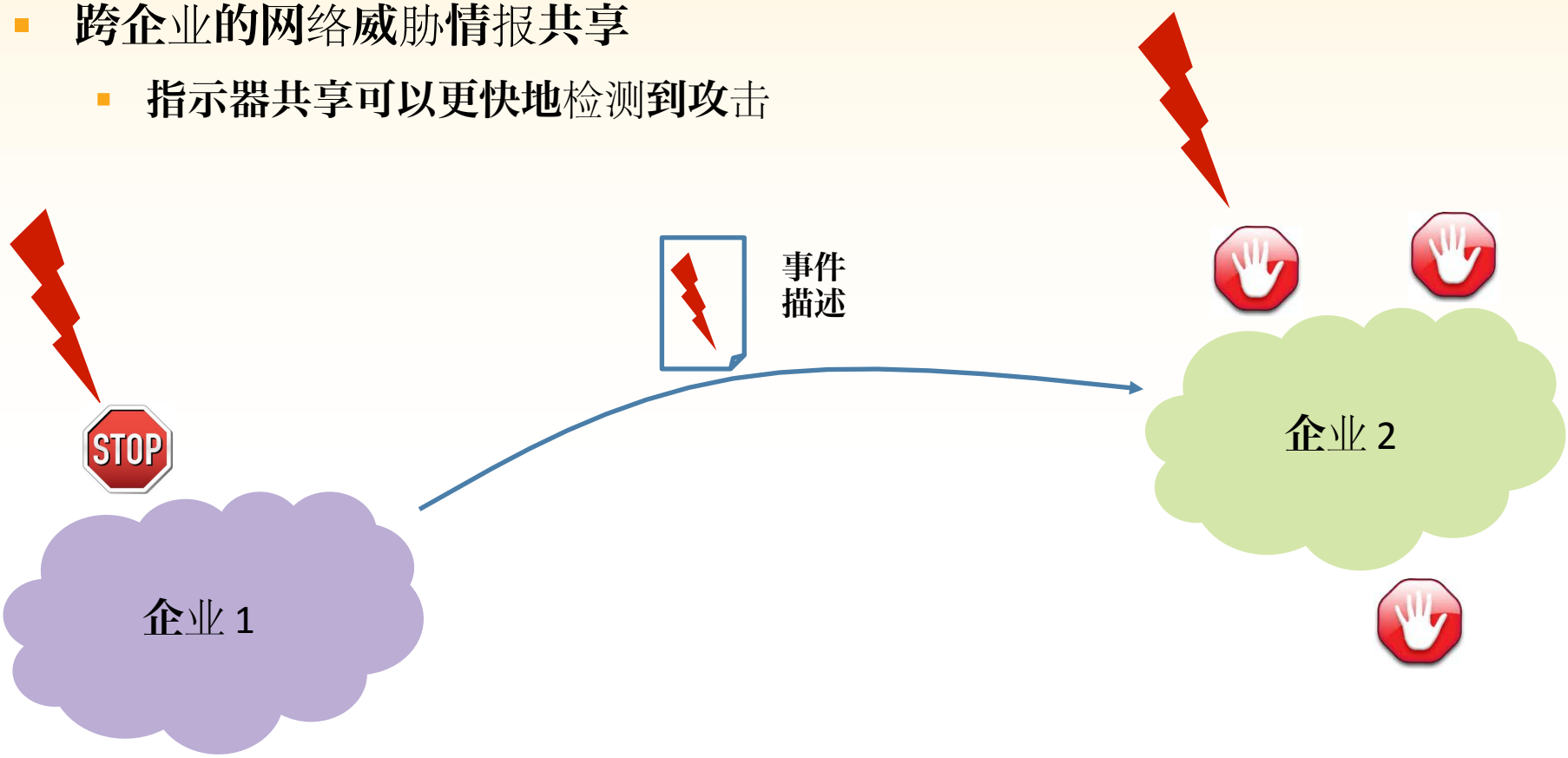
- 不断发展和复杂的 IT 形势
  - 移动到云
    - 大型相互依赖的堆栈、较新的攻击插入点
  - IT 堆栈中的层数增加
    - 虚拟化（服务器/网络）
    - 移动客户端 –“自带设备”
    - 更多层→更多日志
  - 较新的安全数据源
    - Netflow、完整数据包捕获、沙盒指示器

防御

- 工具
  - 入侵检测
    - 基于主机和终结点的工具
  - 安全事件管理
  - 漏洞扫描程序
  - 内存/磁盘分析
- 专业知识
  - CIRT/SOC 团队负担过重
  - 缺乏足够的内部专业知识
    - 恶意软件分析、网络入侵检测、修正

协作是关键

- 跨企业的网络威胁情报共享
  - 指示器共享可以更快地检测到攻击



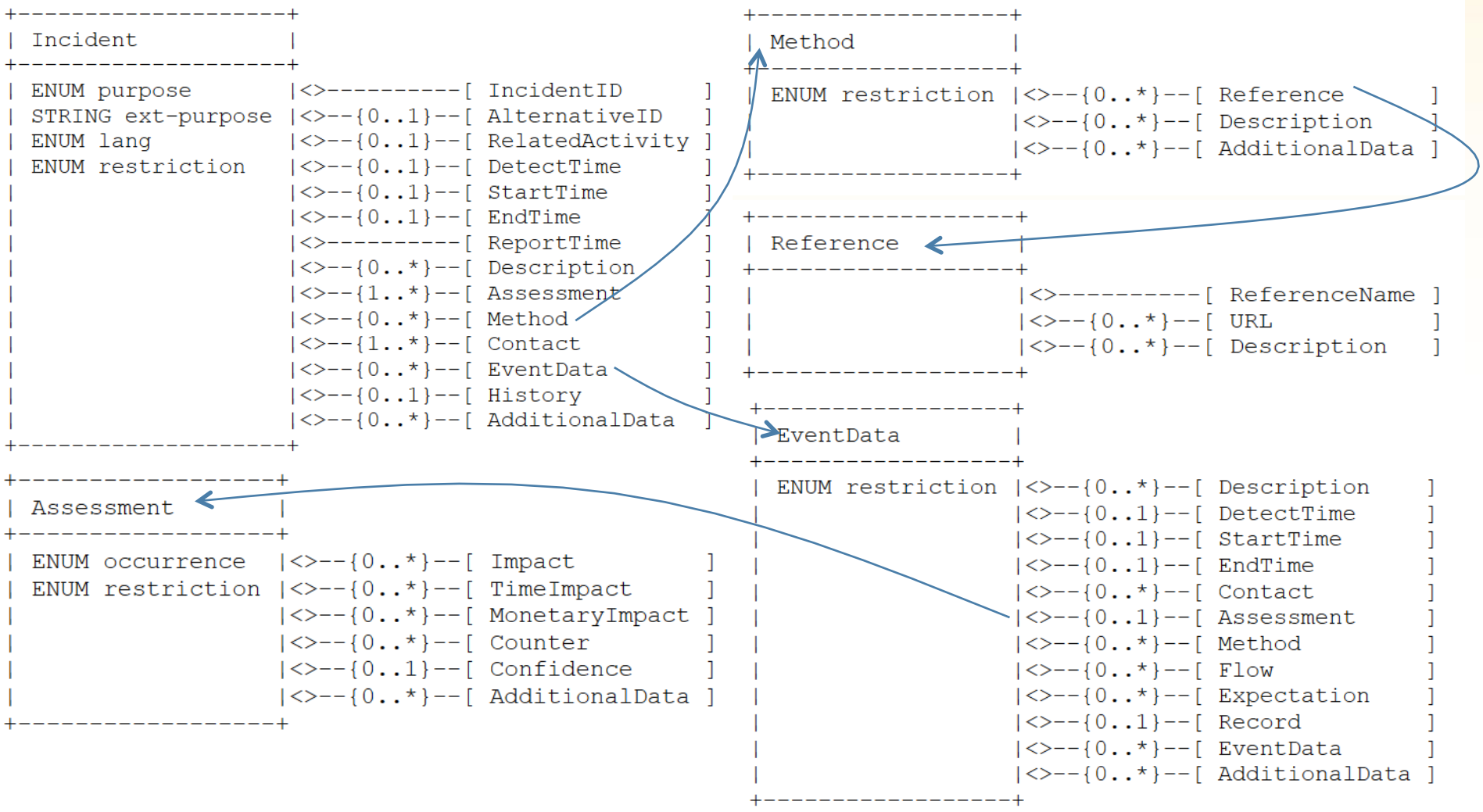
威胁情报共享挑战

- 缺乏可互操作的标准
- 验证数据质量和可靠性方面的挑战
- 信息泄露风险
- 用于治理敏感信息使用的未经测试的方法
- 缺乏熟练的安全专业知识
- 法律和数据机密性要求

救援标准

- 事件对象说明交换格式 (IODEF)
  - 编码威胁信息
- 实时网络互连防御 (RID)
  - IODEF 及其他电子事件的“信封”
- 恶意软件属性枚举和分类
  - 描述恶意软件及其行为
- 常见攻击模式枚举和分类 (CAPEC)
  - 破坏软件等行为的常见方法
- 网络可观测的 eXpression (CybOX)
  - 任何可观测事件；活动的抽象架构
- 高级取证框架 (AFF4)
- 安全内容自动化协议 (SCAP)

IODEF – 数据模型


Incident
ENUM purpose
STRING ext-purpose
ENUM lang
ENUM restriction
IncidentID
AlternativeID
RelatedActivity
DetectTime
StartTime
EndTime
ReportTime
Description
Assessment
Method
Contact
EventData
History
AdditionalData
Assessment
ENUM occurrence
ENUM restriction
Impact
TimeImpact
MonetaryImpact
Counter
Confidence
AdditionalData
Method
ENUM restriction
Reference
Description
AdditionalData
Reference
ReferenceName
URL
Description
EventData
ENUM restriction
Description
DetectTime
StartTime
EndTime
Contact
Assessment
Method
Flow
Expectation
Record
EventData
AdditionalData

现有的威胁情报共享

- 回答如下问题
  - 攻击是什么
  - 它是何时发生的
  - 在哪里发现它的
  - 攻击看起来像什么
  - 谁发现了它
  - 它如何影响环境
  - 多快解决了它
  - 影响是什么
  - 周围上下文是什么
  - …

机会 – 扩展指示器共享

- 告知指示器识别过程
  - 如何识别指示器　基于机器的分析，分析师专业知识
  - 哪些分析效果较好？为什么？分析师观点，比较结果
  - 什么内容发生更改？哪些更改有助于识别攻击？分析师策略
  - 指示器中的可信度是什么？　分析师观点
- 指示器真实性验证
  - 无法使用备份数据传达指示器真实性　支持数据集
- 指示器可移植性指南
  - 移植指示器检测主要需要人们使用威胁源　分析和环境之间的映射
- 多个指示器的组合 – 多阶段攻击
  - 需要人们了解并编写更高级的指示器　分析，可实现组合的专业知识标记

建议 – 指示器共享扩展

- 通过以下方式扩展指示器共享说明
  - 机器分析表示形式，用以
    - 介绍使用哪些基于机器的分析技术来识别攻击以及如何使用这些技术
      - 例如，基于规则的技术、数据挖掘技术或机器学习技术
    - 包括输入数据取样以帮助简化机器分析技术的可移植性
  - 分析师操作表示形式，用以
    - 介绍分析师手动执行了什么操作来识别攻击
    - 分析师如何解释基于机器的分析的结果
    - 分析师对攻击的观点是什么

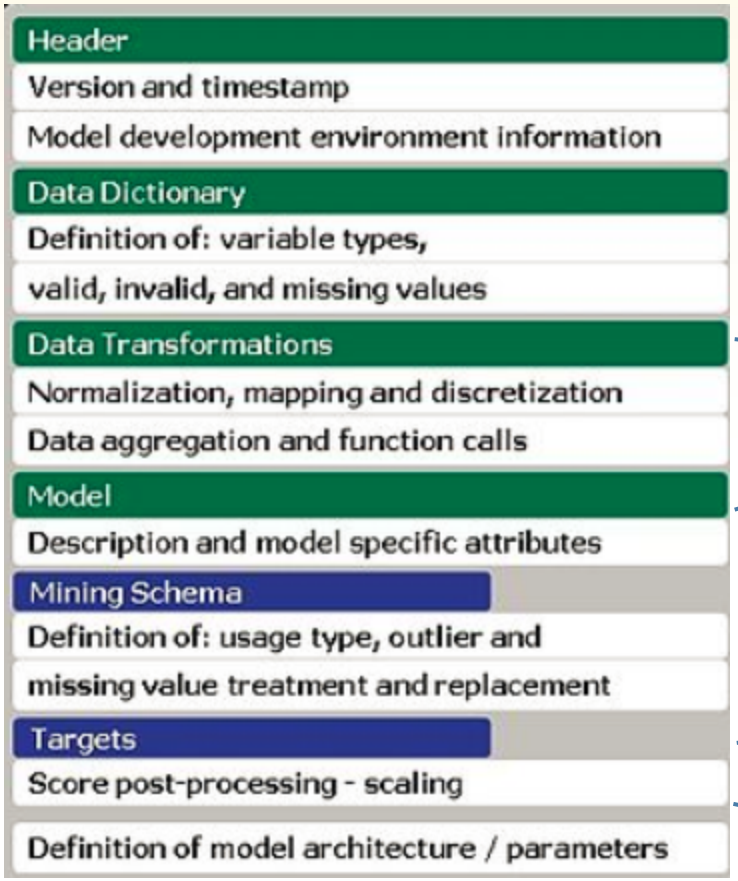
分析和操作表示形式

- 机器分析表示形式
  - 利用并扩展现有标准
  - 预测建模标记语言 (PMML)
    - 用于表示数据挖掘技术和机器学习技术
- 分析师操作表示形式
  - 制定/建议新标准

预测建模标记语言

- 挖掘模型和数据的标准化表示形式
- 包括典型的数据挖掘/分析任务中的各个阶段
  - 数据字典定义
  - 数据转换
  - 处理缺少的或离群的数据值
  - 模型定义
  - 输出
  - 后期处理步骤
  - 模型解释
  - 模型验证
- 受领先的数据分析工具供应商（商业和开源）支持

PMML – 映射到威胁情报



说明分析了哪些安全事件数据
可以利用 CybOX 和类似标准

源企业对事件数据执行的任何预处理

分析师用于处理事件数据的分析（数据挖掘）模型

在分析中针对缺失值等执行的任何特定处理

安全分析结果的任何后期处理

必须与 IODEF 对象中共享的事件数据匹配
可以利用 CybOX 和类似标准

建议的 PMML 扩展

- 出于隐私原因，允许不完整的数据和挖掘模型
  - 例如，允许挖掘模型仅显示数据关系而不显示实际权重
  - 允许共享事件检测中使用的相关安全事件数据，但不允许共享数据与共享企业的关系
- 允许通配符/模式匹配的数据模型和挖掘模型表示形式
  - 允许接收企业将挖掘模型用于自己的企业网络体系结构
- 允许对共享的数据和挖掘模型进行版本控制
  - 允许源组织随时间共享数据和挖掘模型的多个版本
  - 允许接收组织了解挖掘模型的演变并根据自己的网络模型进行适当的更改
- 允许模型筛选器模板 – 通常通过独立的子组织处理情报共享

基于机器的分析是不够的

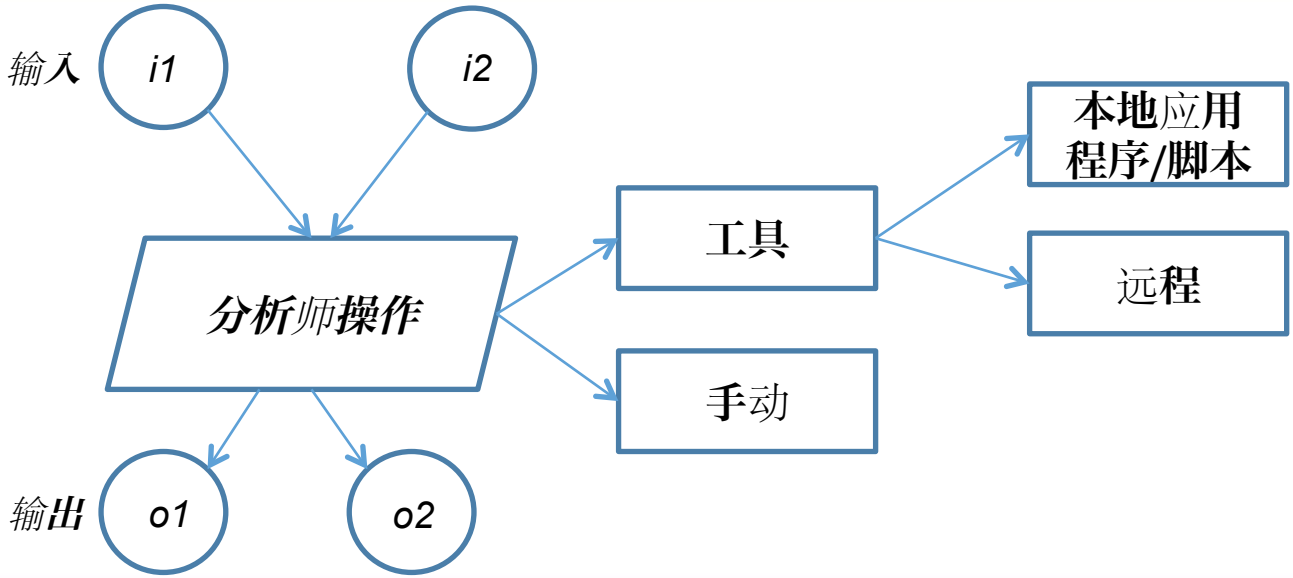
- 安全分析师使用各种工具和过程来分析事件
  - IODEF 和建议的机器分析扩展可传达工具信息
- 但事件分析过程错综复杂，有时需要人的聪明才智和试错法
  - “看图连线”需要人的专业知识
  - 不连续的、脆弱的、需要人配合的分析链
- 共享标准化机器分析信息有帮助但不够
  - 需要共享分析师针对威胁情报源的操作

分析师操作表示形式

- 监视、记录和报告分析师在处理特定事件时的操作
  - 相关的监视和日志记录工具部署在分析师工作站上
- 监视的分析师操作可以包括
  - 分析师与工作站的交互（键盘输入、单击等）
  - 网络交互数据（服务器访问、下载、网络工具）
  - 与事件分析中使用的本地或远程应用程序的交互
- 建议
  - 为处理特定事件的每个分析师创建多个分析师操作图表
  - 输出对分析师在处理事件时执行的各种操作进行整理的单个最终操作图表

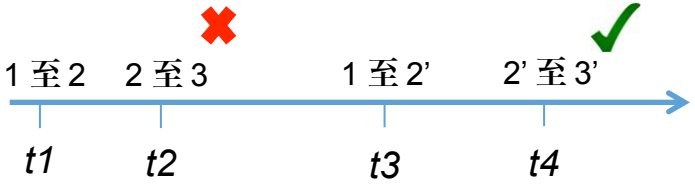
分析师操作图表数据模型

- 通过以下方式捕获每个分析师操作/步骤
  - 步骤中使用的工具/过程说明
  - 过程可以是分析师的直观解释
  - 工具/过程的输入
  - 工具/过程的输出
  - 步骤的前置/后置条件

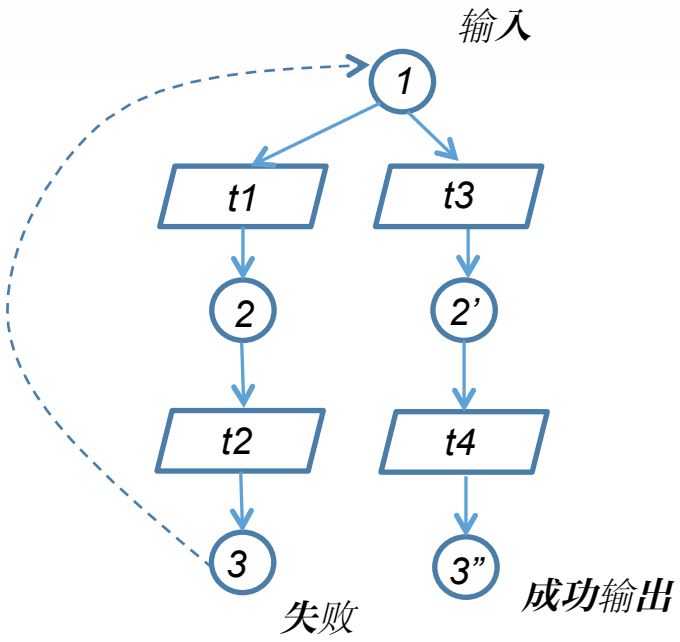


分析师操作关联

- 各个步骤相互关联；上一步的输出 = 下一步的输入
- 按时间顺序监视分析师活动，但可能导致死胡同
- 在图形结构中，失败的路径导致死胡同
- 显示从输入到最终事件分析输出的成功路径



分析师对输入 1 执行操作
以达到输出 3'



分析师活动图表注释

- 分析师注释
  - 人对结果的推断（对特定结论的推断）
  - 有关输出的大量元数据
    - IP 地址、字符串、提取的文件/证书、作者签名等
  - 区分行为签名以识别 APT
  - 区分（APT 使用的）恶意软件的二进制签名
  - 攻击归因观点

支持不同的分析类型

- 自动的（基于机器的分析）
  - 链接到基于机器的分析（数据挖掘、沙盒结果等）
- 半自动活动（基于人和工具的分析）
  - 从工具提取结果并进行一些处理
  - 例如，搜索 IDB 文件查找内存转储文件
  - 可通过监视人的活动来进行记录
- 手动活动（完全基于人的活动）
  - 分析师对之前的结果的直观解释
  - 人为推断
  - 由人编码的任务，例如设置断点、识别字符串、对加密/解密例程进行解码、识别挂钩进程
  - 可能需要人协助的注释

结论

- 需要更丰富的威胁情报共享
- 机器分析和分析师操作表示形式
- 完整的事件说明、识别和分析
- IODEF 扩展建议、利用 PMML 标准

谢谢大家！

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012