安全加社区

公益
译文
项目

2016

关键基础设施系统攻击检测、关联与呈现

SRI International

2010 年 8 月

文档信息			
原文名称	Detection, Correlation, and Visualization of Attacks Against Critical Infrastructure Systems		
原文作者	Linda Briesemeister, Steven Cheung, Ulf Lindqvist, Alfonso Valdes	原文发布日期	2010 年 8 月
作者简介			
原文发布单位	SRI International		
原文出处	http://www.csl.sri.com/papers/PST2010/		
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

“安全加”社区　　小蜜蜂公益翻译组

目录

摘要……1

1.0 概述……2

2.0 系统架构……3

3.0 试验台……6

4.0 攻击场景……7

5.0 通过关联确认网络遍历攻击……8

6.0 呈现……11

7.0 相关工作……12

8.0 结论……13

参考文献……14

致谢与免责声明

在此，我们要特别感谢项目合作伙伴桑迪亚国家实验室，特别是 Regis Cassidy。感谢他们帮助建立试验台，并模拟攻击，扮演系统红队。斯坦福研究院的马丁·方（Martin Fong）和哈尔·亨特利（Hal Huntley）在实施和运行试验台过程中给予了我们巨大的帮助。我们还要感谢那些在实现系统过程中为我们提供帮助的 ArcSight 和 ArcSight 用户社区成员。

本文是在美国能源部支持下拟就的（资助项目编号：DE-FC26- 07NT43314）。无论是美国政府还是其任何代理机构，还是他们的雇员，都不会以明示或暗示的方式对信息、仪器、产品或过程说明的准确性、完整性、有效性进行任何担保，或承担任何法律责任，也不会声称它的使用不侵犯任何人的权利。本文中涉及的任何具体的商品、工艺或服务的商品名称、商标、制造商或其他方面，并不意味着美国政府或其任何代理机构对其的认可、推荐或帮助。本文作者的观点和看法并不代表美国政府或其代理机构的观点和看法。

摘要

数控系统对于电力、油气、水处理及制造行业的各种工业流程的安全、高效运行起着至关重要的作用。现代控制系统不仅要与其他控制系统连接，还会与企业系统连接，这种现象越来越常见。此外，这些系统还越来越多地采用传统企业系统中的组网技术以及系统与应用软件。这种趋势下，控制系统容易受到网络攻击，或会影响物理过程，导致环境危害或损伤。

本文介绍了 DATES（能源部门威胁检测与分析）项目的部分研究成果，针对控制系统，我们修改、开发了几种入侵检测技术，并将整套检测技术集成并连接至 ArcSight 的商业安全事件关联框架。我们在两个相连的试验台环境论证了检测与关联方案的效用，重点关注的是对于网络遍历攻击的检测、关联与呈现。网络遍历攻击中，攻击者可连续穿透各网络层，侵入直接控制下层流程的关键资产。控制系统若是典型的分层架构，尤其需要关注这种攻击。

关键词

关键基础设施安全；控制系统安全；入侵与异常检测；告警关联；安全信息事件管理

1.0 概述

因为要运行复杂的信息物理系统，能源部门对于数据采集与监控系统（SCADA）之类的数字工控系统（ICS）越来越依赖。老旧控制系统独立运行，使用私有协议，因为难以被外界理解而实现了一定程度的安全。现代系统则越来越频繁地使用开放标准（如互联网协议），彼此互联。虽然这会使运营更为安全，成本效益也更高，然而，人们却担心系统本身易于遭受网络攻击，这些攻击长期以来威胁着企业系统的安全。就控制系统而言，人们更担心的是，攻击一旦成功，不仅会导致经济损失，更可能对环境与安全带来影响。

DATES 项目开发了一种分布式的多算法入侵检测能力，适用于能源基础设施广泛使用的数控系统。这种检测能力使用了贝叶斯统计方法与基于学习的异常检测方法，将传统的特征检测法集成于新型部件中。据观察，这些部件对于控制系统环境颇为有效，因为这些环境中的流量有规律，协议数量也有限 [1]。我们将检测能力集成至 ArcSight 的业界领先的安全信息事件管理系统（SIEM）中，形成了整体监控方案，对边界防护进行补充，并针对各种控制系统攻击，为 ICS 安全操作员提供了更高水平的态势感知能力。

本文以网络遍历攻击为例介绍了该综合系统。基础设施系统因为使用的是分层架构，尤其要关注这种攻击。典型的控制系统通过非军事区（DMZ）与其他网络分段架构将公共与企业网络隔离开来。网络间需进行受控连接以满足运营需求。因此，连续渗透网络各层的攻击利用了网络间的信任关系，从公共网络为攻击者提供了遍历路径，使其长驱直入各种高优先级现场设备。

为定义网络遍历攻击，我们假设每个主机 H 有一个重要性分值，用 criticality(H) 表示，评分基于主机的功能或所管理数据的重要性。模拟网络遍历攻击时，我们将其描述为如 $H_1 \rightarrow H_2 \rightarrow \cdots\cdots \rightarrow H_k$ 这种顺序的网络连接，H_i 代表主机，$criticality(H_{i-1}) \leq criticality(H_i)$，其中，$i \in \{2, ..., k\}$。再假设每个 $H_{i-1} \rightarrow H_i$ 连接对应违反安全策略（如网络访问策略）的一个或多个事件。

网络遍历攻击与踏脚石攻击（例 [2] [3]）类似，但是在动机上不同。在踏脚石攻击中，攻击者使用多个中间主机，使攻击源难以辨识。在网络遍历攻击中，攻击者利用主机间的信任关系攻击其无法直接访问的高价值目标主机。

2.0 系统架构

假定有一个企业网（或可以连接至互联网），其中的客户端可访问各种资源，如企业区域与控制区域之间 DMZ 区中的数据记录服务器。这些服务器接收的数据来自于控制区域中的现场控制处理器（FCP）或前端处理器（FEP），这些处理器向现场网络中的设备发布控制命令、轮询数据。控制网络中的资产一般包括人机界面（HMI）及在传统计算机平台上运行控制系统应用程序的其他工作站。现场网络设备直接监控如提炼、制造或发配电 / 电力输送之类的物理过程。利用双防火墙防护的 DMZ 区将企业网与控制网隔离开来，这在控制系统领域普遍使用，是比较成熟的做法 [4]。

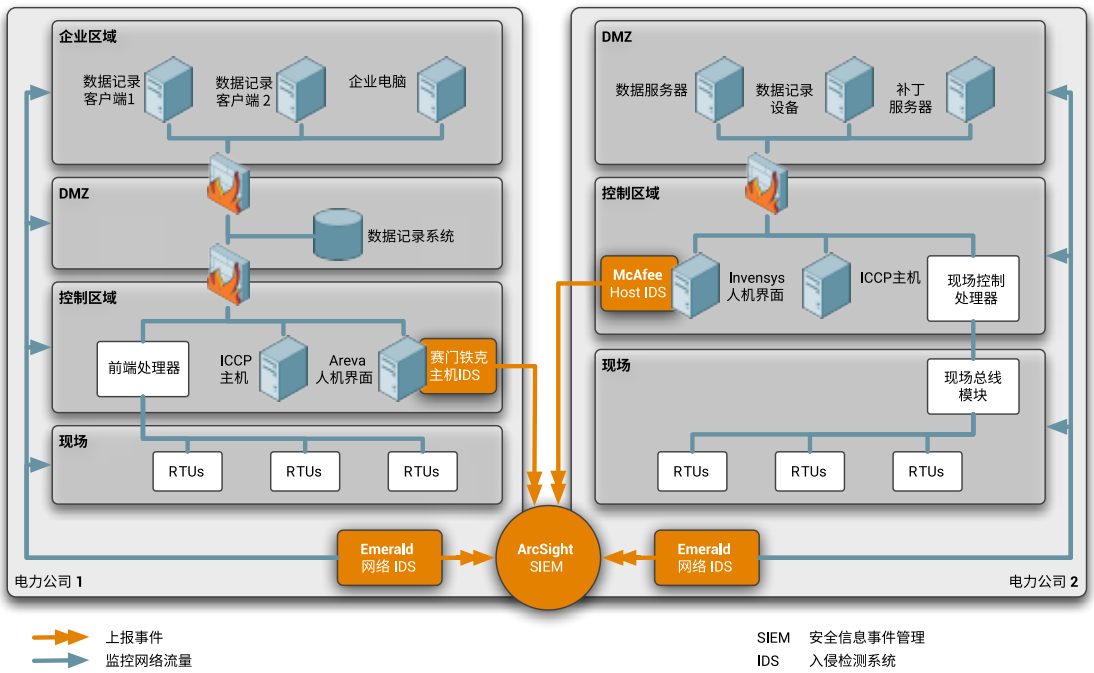

图 1 试验台架构概览

没有 DMZ 服务器，控制系统也可以运行。很多时候，甚至在控制网络短暂断连情况下，控制系统仍可运行。这种情况下，现场网络会暂时自主运行或由逻辑正交安全仪表系统（SIS）安全关闭。所以说，现场网络优先级最高，控制网络其次，DMZ 区居中，而企业网络优先级最低。与企业网络中的流量相比，现场网络中的预期流量更规律。企业区域中的客户端可通过防火墙访问 DMZ 区，通信只能使用数据记录服务器允许的协议。实际场景中，也会有 Windows 远程过程调用（RPC）之类的流量，这类流量中存在已知漏洞。同样，防护方必须了解所允许协议中存在的漏洞利用情况以及 TCP 连接被劫持的可能性。可疑流量从一个区域进入到另一个区域时会触发告警，但是可疑流量并不是判断系统是否受到攻击的唯一标准。所以，要进行深度防护，深度报文检测（DPI）和资产健康监控之类的其他技术必不可少。

图 1 所示的试验台架构是对这种参考架构的实例化展示，将企业、DMZ、控制及现场网络区域进行了逻辑分隔。

A．控制系统入侵检测

因为过程控制系统一般包含企业商用现成（COTS）部件（如运行于微软 Windows 系统上的商业数据库系统）及过程控制专用部件（如通过 Modbus TCP 进行通信的远程终端单元 RTU），我们的入侵监控方法采用的入侵检测传感器既适用于企业网络，又适用于过程控制子系统，以扩大攻击检测范围。

企业网络与主机入侵检测：为监控企业网络（如图 1 参考架构中的企业网络）与 COTS 部件（如商业数据库系统和操作系统），我们使用入侵检测传感器来监控网络与主机级别的事件。

针对网络监控，我们使用 Snort[5] 作基于特征的检测，用贝叶斯传感器检测几种重要的攻击如侦测与资产损害（asset distress）[6]，用 Emerald eXpert 传感器对几种关键的网络协议如 HTTP 执行深度报文检

测与状态分析 [7] [8]。

针对主机检测，我们使用商业安全解决方案（这里特指 Symantec Endpoint Protection [9] 与 McAfee VirusScan Enterprise [10]）监控运行微软 Windows 系统的机器。这些基于主机的安全部件可检测网络监控部件不易察觉的恶意活动（如修改目标主机中的关键安全文件或通过加密网络连接进行扩散的攻击），因而扩大了检测范围。

过程控制子系统入侵检测：我们的控制系统监控方案既使用了基于特征的方法，又使用了基于模型的检测方法，对控制系统环境及过程控制系统（PCS）协议（如 Modbus、分布式网络协议 DNP3、控制中心间通信协议 ICCP 等）进行监控。

对于特征检测方法，我们使用的是 Snort[5]，其中的控制网络规则由 Digital Bond 开发 [11]。这种方法能够可靠地检测已知恶意活动。

至于基于模型的检测，我们分析系统的预期行为特征，当系统行为偏离该特征时，则认为攻击存在。这种方法可检测未知攻击，能够作为特征检测方法的补充，扩大检测范围。我们注意到，控制系统的通信模式具有规律性及可预测的特点，这大大简化了这些模型的规范或学习过程。

我们开发了几个基于模型的过程控制系统监控器，包括 eModbus（用于检测 Modbus 服务器的变化或服务可用性）、eFlowmon（用于检测流异常，监控单个网络流的流量模式）及 Snort 规则集（用于检测违反 Modbus 协议规范的行为）。关于我们在基于模型的检测方法方面所做的研究，详见 [1] 和 [12]。

B. 事件管理

控制系统监控物理过程,其核心功能是收集过程参数,提供过程告警。过程告警警告的不一定都是恶意活动。将入侵监控与态势感知能力如 DATES 集成在产品中可能会产生额外告警（由入侵检测框架发出），增大操作员工作量。因此，将入侵检测系统中的告警进行关联变得至关重要，这可以缩小范围，准确显示系统的潜在网络攻击，包括攻击的严重性及更详细的下钻信息。

我们的告警关联方法基于几个基本的概念构建，包括安全事件分类、网络区域及资产类型。此外，为简化安全事件排名，使安全管理员可集中精力优先处理最重要的安全事件，我们制定了事件类别与网络区域和资产类型重要性优先级划分方案，这里涉及的网络区域和资产类型基于常见过程控制系统的特征划分。

入侵检测部件可上报大量的告警类型，例如，仅 Snort 就内置了数千种攻击特征。针对这一问题，我们提供了相应的地图，涵盖 Emerald 报表与 DATES 内部其他部件产生的告警，将其划分为几大类安全事件类别。

将安全事件分类为制定总体关联策略及进行跨传感器关联提供了便利。具体说，基于抽象分类的安全事件，可更概括地制定关联条件，使关联系统具有更好的扩展性与复用性。此次项目，我们使用了之前告警关联研究中开发的安全事件分类标准 [13]。

基于过程控制系统安全目标之间的相对重要性，我们制定了安全事件类型优先级划分方案。一般情况下，资产所有者将可用性作为最重要的安全目标，然后依次是完整性和保密性。我们将安全事件分成四大类，并为每类给出严重性评分，以反映这些事件对于控制系统的重要性。例如，“资产损害”大类优先级最高，因为此类事件可能会影响目标资产的可用性。优先级最低的“行为日志”与“探测”大类一般不那么重要。表 1 列举了安全事件类别与对应优先级。

表 1 安全事件分类与优先级划分

	安全事件类别	严重性分值
1 类	拒绝服务 资产损害	4
2 类	系统环境破坏 完整性破坏 二进制控制（Binary Subversion） 权限破坏	3
3 类	可疑使用 用户控制（User Subversion） 用户环境破坏	2
4 类	违法访问 违法连接 探测 渗漏 行为日志	1

目标重要性是影响事件重要性的另一个因素。我们使用资产的两个属性来确定其重要性：资产类型与所属网络区域。数据记录系统与 RTU 就是两种不同的资产类型。我们为不同的资产类型与网络区域根据其重要性分配权重。与安全事件类别一样，资产类型与网络区域具有高度概括性，用于为各类资产（而非具体的资产实例）制定总体关联标准。表 2 和表 3 分别列举了资产类型和网络区域及其相关重要性分值。

表 2 资产类型重要性

资产类型	重要性	重要性分值
远程终端单元（RTU）	非常高	5
前端处理器	高	4
ICCP 主机	高	4
HMI 服务器	中	3
HMI 客户端	低	2
数据记录服务器	低	2
数据记录客户端	非常低	1

表 3 网络区域重要性

网络区域	重要性	重要性分值
现场	非常高	5
控制	高	4
DMZ	中	3
企业	低	1

3.0 试验台

为研究跨站攻击检测与关联，我们用了两个试验台进行试验与验证。这两个试验台分别位于斯坦福研究院（SRI）与桑迪亚国家实验室内，模拟了两家电力公司。此外，在试验中，两个试验台通过安全连接进行互联，所以它们产生的告警可安全发送至同一台 ArcSight SIEM 服务器进行事件关联。图 1 呈现了测试台概要示意图。

SRI 测试台基于英维斯过程系统（IPS）公司的 IA 系列分布式控制系统（DCS），具有如下关键部件：

- 用于配置、呈现与控制的应用工作站（AW）
- 基于冗余 Enterasys 光纤以太网交换机（两台以形成冗余）的控制局域网
- 英维思现场控制处理器（FCP）模块
- 现场总线，用于将 FCP 连接至两个以太网现场总线模块（FBM）
- 现场局域网，用于连接 FBM 与运行在虚拟机上的模拟 Modbus 设备（Modbus 模拟器由 Modbustools.com 与 Calta 提供）
- 网络与主机入侵检测传感器，用于向 ArcSight SIEM 服务器发送安全事件

桑迪亚试验台基于虚拟控制系统环境（VCSE）[15] 构建，这是一种灵活的、面向工具的分布式环境，将真实、仿真与模拟组件连接在一起，便于分析针对信息物理系统这一类威胁的影响。

两个试验台都对 SRI 的 Emerald 系统（其中集成了前述网络入侵检测技术）进行了实例化。我们对 Emerald 进行了修改，输出采用 ArcSight 的公共事件格式（CEF），这种格式是 ArcSight 使用 SmartConnector 技术开发的。试验过程中，用 CEF 传输源 / 目的 IP 地址与端口以及告警名称、描述及安全事件类别（使用“设备事件分类”字段），并配置基于主机的入侵检测系统（如赛门铁克和迈克菲的系统）生成 syslog 格式的消息，ArcSight 用自己的 syslog SmartConnector 接收这些消息。

本项目中，桑迪亚与 SRI 的研究者们通过 VCSE 实例化开发、测试了控制系统入侵检测、SIEM 以及大型威胁分析技术。此外，我们使用各种 VCSE 模型以检测现有 IT 安全技术无法检测到的威胁。这种工具化 VCSE 经过了各种正常运行模式及多种攻击场景的验证。

4.0 攻击场景

SRI 与桑迪亚针对两种测试环境模拟了一系列攻击场景，其中一个场景使用 ICCP 从一个被入侵公司向另一个公司发动攻击 [16]。

有一个攻击场景使用公司内部多台被入侵计算机攻击某单一目标，形成分布式拒绝服务攻击。DATES 框架检测到各种利用程序，在攻击成功阻断预期通信流后，异常检测组件进行告警。

这里重点描述的另一个攻击场景涉及的是网络遍历攻击，攻击者在攻击中成功穿透了控制系统架构的多层防护。网络遍历的实施分多个步骤，使用到的扫描与利用程序利用了常见漏洞，以及针对控制系统协议与资产的特定攻击。攻击者的策略是根据重要性从低到高逐个攻击节点，在每个节点试探能够攻击的目标，然后继续攻击下一个目标。

在我们模拟的场景中，攻击者入侵了第一家电力公司的企业电脑，以这台电脑为据点，攻击者接着控制了同在企业区域的数据记录客户端，而该客户端可访问 DMZ 区的数据记录服务器。攻击者在数据记录服务器中发现漏洞后对其发起攻击，并以其为跳板，攻击了控制网络中的前端处理器。从这个节点，攻击者试图关闭现场网络中的 RTU（并未成功）并攻击人机界面。虽然这些攻击并未成功，但却被网络与主机防护组件成功检测。攻击者入侵了第一家电力公司的 ICCP 主机，这台主机可同第二家电力公司的对应 ICCP 主机通信。利用这条信道，攻击者可入侵第二家公司的 ICCP 主机。

5.0 通过关联确认网络遍历攻击

我们用 ArcSight SIEM 组件检测和呈现网络遍历攻击，以识别事件模式。因此，ArcSight 处理和储存的低级别事件以及可能包含误报的具体事件被归纳为操作者易于理解的案例呈现（详细描述，见第 VI 节）。

在我们的攻击场景中，我们对系列事件以及不断发展的事件（源起网络危险性由低至高）进行关联。主要思想是依据如下发现：过程控制网络中不同区域的主机之间的通信模式可预测，并分层进行。有了配置正确的防火墙，一个只能潜在访问企业网络的外部攻击者在获得对现场网络中高价值目标的访问前，可能需要通过一系列的网络区域（从 DMZ 区到控制网络）来攻击机器。由于跨越了过程控制网络中的区域，我们的方法可对攻击进行关联和呈现。根据区域的重要性分值，我们对优先级分配如下：现场区域中资产的优先级为最高，控制区域的优先级为高，DMZ 区的优先级为中，公司网络的优先级为最低（见表 III）。在下面的算法中，跨区或跨公司的 IDS 告警可能会按照源 IP 地址、目的 IP 地址判断重要性并进行关联，并将一个告警中的源 IP 地址与另一事件中的目的 IP 地址进行匹配。

假设有三个告警：A1、A2 和 A3。如果满足以下条件，基于区域的重要性升级算法将把它们关联为一个事件。

- zone(dst(Ai)) 为“内部区”。
- dst(Ai) = src(Ai+1)
- zone(src(Ai)) 的重要性 < zone(dst(Ai)) 的重要性

zone(src(Ai)) 区为“外部区”。

utility(zone(src(Ai))) = utility(zone(dst(Ai)))

其中：

dst(A) 返回的是告警 A 的目的 IP 地址；

src(A) 返回的是告警 A 的源 IP 地址；

zone(X) 返回的是 IP 地址 X 所在的区；

如果被 IDS 监控，Z 为内部区；

如果 Z 不为内部域，则为外部域；

criticality(Z) 返回的是 Z 区的重要性分值；

utility(Z) 返回的是 Z 区所在公司的标识符。

条件（1）确定的边界条件为：如果不再监控上一个事件的目的区，则事件链过程停止。条件（2）是为了满足将一个事件的目的 IP 地址与另一事件的源 IP 地址进行匹配的要求。条件（3）是为了满足不降低区域重要性的要求（例如，对应某一事件目的 IP 地址的区域的重要性应至少与源 IP 地址的重要性相同）。该标准有以下 2 种例外情况：一种外部源的情况下，重要性分值不确定；另一种情况是两个不同公司之间的事件。

为了检测系列事件构成的攻击，我们首先定义一个能够捕捉潜在攻击或事件的过滤器。图 2 显示了 ArcSight SIEM 中此类过滤器的定义。ArcSight SIEM 寻找目的地址在公司网络内的基本或聚合事件，源和目的地址的重要性相同或有所增加。如果重要性满足下列条件之一：a）源区域重要性分值小于或等于目的区域，b）源在公司网络之外或 c）事件跨公司网络，我们认为事件的重要性渐次增长。

图 2 ArcSight 针对潜在遍历事件对过滤器的定义

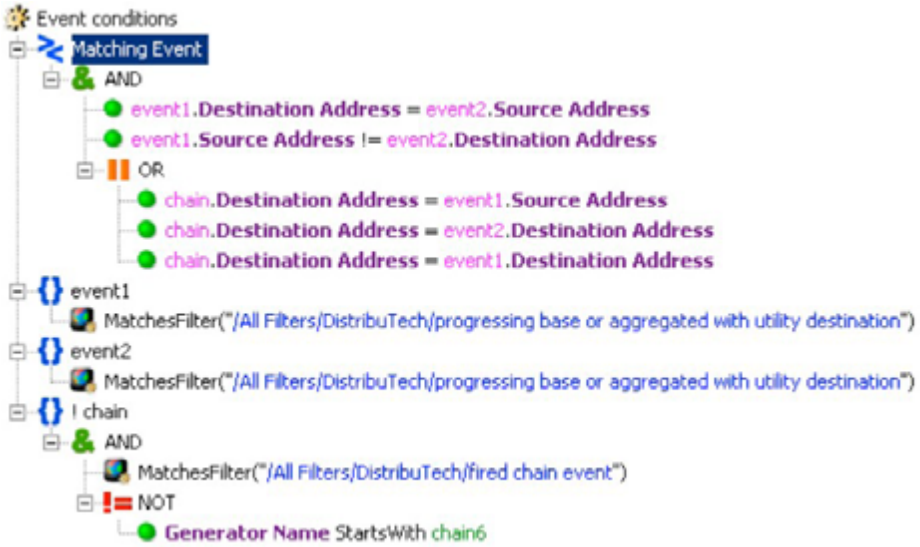

图 3 ArcSight 对规则“chain2”的定义

下一项挑战是制定规则。当事件的潜在事件形成一个链，其中新攻击步骤中的源是前一攻击步骤中的目标时，该规则被触发实现这一事件链，我们决定不采用简单的递归解决方法，以避免环路风险。相反，我们为每个第 i 链元素定规则（起始规则为 chain2）来匹配前两个事件，然后匹配现有的连锁事件“chainn”。每个事件为链条上的一环。在原型实现中，我们在链条上的最后一环是 chain6，来匹配原型实现中的 6 个事件。在实际部署中，我们建议创建更多规则。使用该方法的原因之一是考虑到 ArcSight 中规则匹配引擎的作用。触发规则用来创建进入事件流的元事件，该元事件可被任何规则检测到，就好像是由连接到 ArcSight 的传感器创建的事件一样。在实现中，我们常用此功能，但使用时很谨慎。因为不合理的规则在系统负荷过重时容易导致回路或消耗太多内存和处理能力，这反过来又可能导致 ArcSight 自动禁用这些规则，以维护整个系统的运行。

图 3 表明 ArcSight 中规则“chain2”的定义。该规则的目标在两个事件最初被确定为链长为 2 时使用。这些条件定义了 e1 和 e2 两个事件。它们构成的是一个链，而不是一个环。

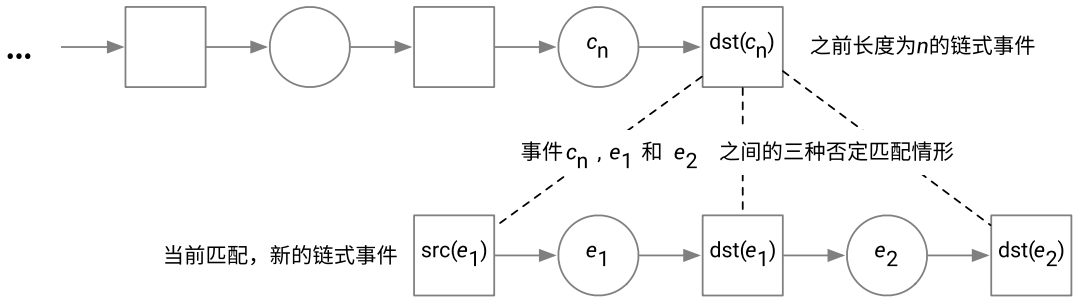

图 4 “chain2”的三种否定匹配情形

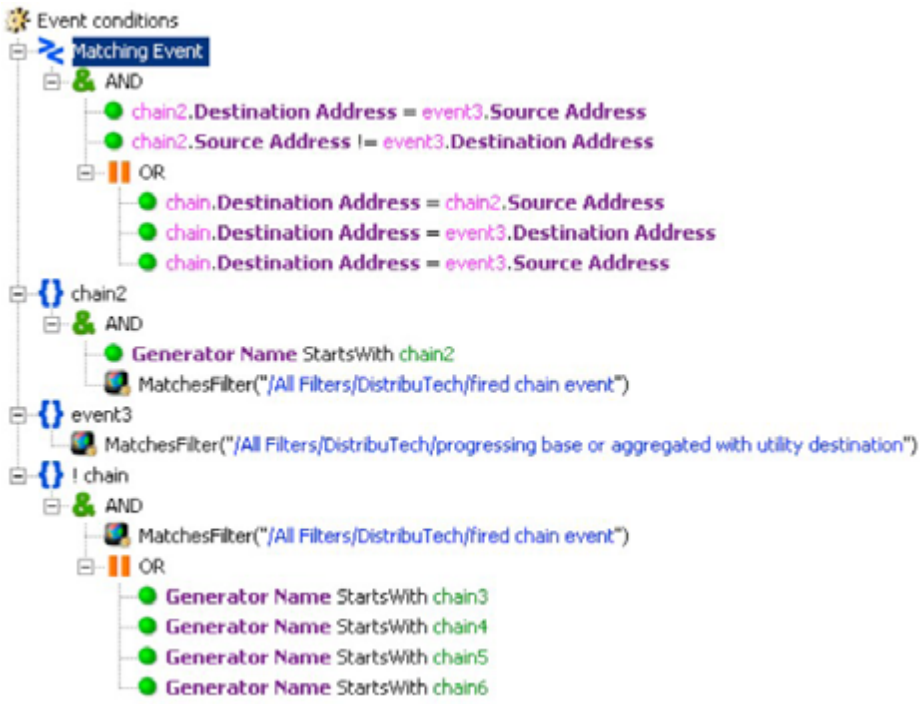

图 5 ArcSight 对规则“chain3”的定义

例如，dst(e1) = src(e2) 且 src(e1) ≠ dst(e2)。这两个事件都必须与图 2 中定义的“处理处理目的地址中在公司网络中的基本或聚合”过滤器匹配。

除了这种声明初始链长度为 2 的肯定的描述，我们还在 ArcSight 中采用否定事件的概念，防止在 e1 或 e2 所在的事件链已经存在的情况下触发该规则。使用否定事件要求在评估规则时无任何匹配事件。这里，否定事件 c 表示之前触发的“chain2”至“chain5”的规则（“chain6”除外，因为它是原型实现中的最后一条链式规则）。然后，在树形顶端的 JOIN 条件（标记为“匹配事件”）下，我们将防止图 4 所示的三种情况触发规则。如果在长度为 n 的事件链中有一项之前启用了规则的链事件 cn，其目的地址与当前匹配到的“chain2”的 3 个位置（src(e1)、dst(e1) 和 dst(e2)）中的一个相匹配，然后我们要防止建立一个新的长度为 2 的链。相反，链长为 n+1 的另外一条可能会分别匹配事件 e1 或 e2，扩展之前的事件链 cn。因此，在否定事件中我们排除了可能最长的链式规则（原型实现中的“chain6”），因为链长为 n+1 的规则不存在。在这种情况下，明智的做法是触发“chain2”，并启用新的长度为 2 的链式规则。

然后我们定义“chain3”到“chain6”规则。这里“chain3”仅用作示例，如图 5 所示。假设我们尝试匹配长度为 n 的事件链。在本例中，“chain3”中的 n = 3。我们匹配到之前的链式事件 c2，指长度为 n – 1 = 2 的链，意味着相应的规则已触发，并在事件流中创建了元事件，即另一个“处理目的地址中在公司网络中的基本或聚合”事件 e3。再次，这两个事件必须形成一个链条但不是一个回路，例如 dst(c2) = src(e3) 且 src(c2) ≠ dst(e3)。然后，与规则“chain2”相似，我们还要求不存在长度 ≥ n 并采用否定事件 c 概念的链式事件。运用否定事件逻辑类似于上面所说与“chain2”规则相关的逻辑，如图 4 所示。

6.0 呈现

一旦一系列事件使链式规则在 ArcSight 中触发，我们收集所有端点上的此类事件，构成活动列表（Active List）中的事件对。然后，后续所有具有与活动列表相匹配的端点的事件都会被加以收集并呈现，从而全面了解网络中正在进行的网络遍历攻击。

图 6 中的呈现使用 ArcSight 事件图数据监控器，将端点描绘为正方形，事件描绘为圆形。为了显示网络遍历攻击如何穿透各层从而实现攻击高度关键的现场设备的目的，甚至进入不同的公司网络，我们在图中划分了主机所属的区域。

红色（中度灰）正方形代表事件的源，蓝色（深灰色）正方形代表源和目的，白色正方形代表事件的目标。正方形标记了我们在试验台中模拟的 2 个公用网络中 ArcSight 网络模型中 IP 地址的主机名。还标记了主机的位置：U1 表示公司 1，U2 表示公司 2。

每个事件圆圈有大小之分，与检测到的该类型事件的数量成比例，并且每个圆圈下的标签显示事件名称。图 6 所示的事件名称反映出底层检测组件所发挥的呈现作用。与新的或丢失的流量相关的事件由流量异常检测组件生成。数字标签对应的是 Snort 标识符；例如，1:2002903 表示检测指定的 shellcode 段的 Snort 规则，针对 Wintel 机器上的漏洞利用。呈现表明了攻击者在从企业网络到 DMZ 区以及公司网络 1 的控制网络时使用的各种扫描和漏洞利用，他们试图攻击现场资产并通过用于 ICCP 的信道攻击公司网络 2。关于网络遍历攻击介绍，见第 IV 节。如图所示，图中描绘了完整遍历攻击的结果；在 ArcSight 收到匹配相关规则的事件时自动生成不同的节点和边界，操作员可以查看攻击图，攻击顺序从左到右（参见 [17]，DATES 演示视频）。

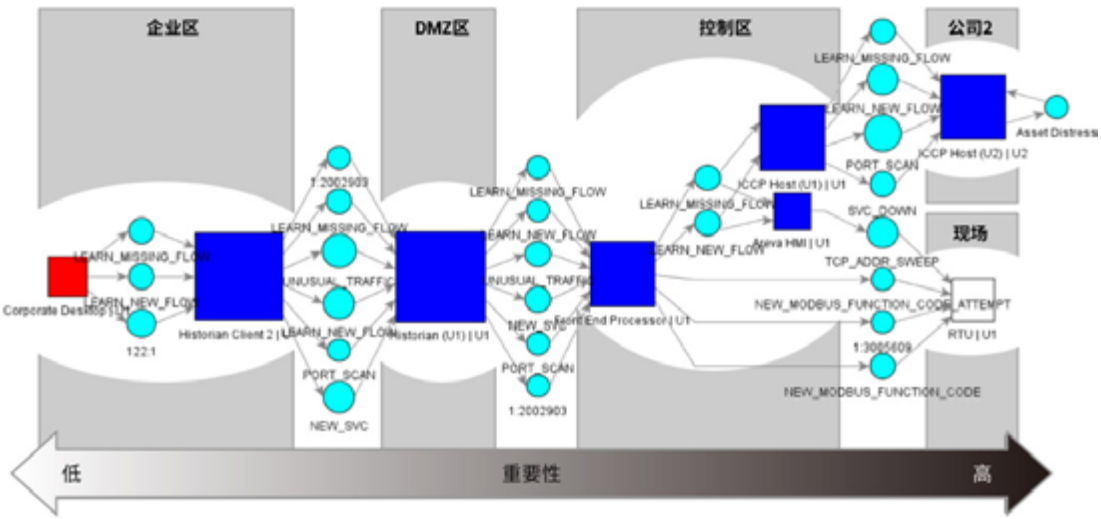

图 6 ArcSight 中网络遍历攻击呈现

由于该网络遍历攻击图中的事件中所含信息比事件图所示的要多得多，我们在图下还制作了一个自定义仪表盘表格，操作员可快速查找每个事件的详情，例如时间戳、更详细的信息和事件分类。最后，ArcSight 还提供更多的通知操作员的方法，例如通过电子邮件或寻呼。当链条达到一定长度、到达某些区域或满足了其他重要标准，在采用此系统来发出自动警报的公司网络中执行具有特定参数的规则是简单有效的。

7.0 相关工作

随着工控系统互联变得无处不在以及这些系统向商品平台（例如 Windows 的人机界面、TCP/IP 网络和现场设备的嵌入式操作系统）的迁移，近年来人们对这些环境中的网络安全的兴趣日益浓厚。美国能源部牵头进行持续产业路线图文件的开发，以推进能源部门控制系统 [18] 的网络安全。该路线图中将监控作为开发安全、能从攻击中快速恢复的控制系统目标的重要支持。

很多机构已经开发出连接控制系统和企业系统的最佳实践架构 [4]、[19]。构成 DATES 试验台的桑迪亚 VCSE，对虚拟和物理组件 [15] 中的各类控制架构进行了实例化。

关于控制系统中的入侵检测，Digital Bond 开发了一套针对攻击多个重要控制协议的 Snort 特征，并继续维护该特征库 [11]、[5]。我们的 DATES 检测套件在其他算法组件中都有该特征库。

异常检测系统利用控制系统中流量的规律性。Cheung 等人证明了异常检测系统的有效性 [1]。DATES 并入了这些概念，并将之扩展到流量异常检测，还引入了一种自适应学习功能。

DHS LOGIIC（在油气行业中提高网络安全）相关项目早期已验证了控制系统环境中集成式检测和 SIEM，是 DATES[20] 的基础。DATES 项目在展示了异常检测、跨站点呈现和区域遍历攻击呈现方面取得了进步。

从行业方面看，入侵检测防护的商业解决方案可多方获取，主导产品有 Tofino 和 Industrial Defender 产品 [21]、[22]。供应商系统通常还包括商业安全组件，例如在我们的试验台中的 Invensys IA 系统就包括了迈克菲主机入侵检测系统 [14]、[10]。

8.0 结论

虽然数控系统在许多方面采用了传统企业计算，但在几个关键方面不同于企业系统。数控系统需要应急操作员干预和连续操作，因此很多企业安全实践难以应用数控系统。另一方面，控制系统的任务范围比企业系统要小得多。控制系统通常运行一小组相对简单的协议，并展示各个网络区域资产之间的规律通信模式。这一规律性使异常检测方法在检测灵敏度和误报率方面比企业更为有效。

分层防御使网络遍历攻击检测尤为重要。因为从本质上讲，这些攻击利用多个漏洞来攻击离价值最高的现场组件越来越近的资产，入侵检测系统必须采用关联和呈现框架提供有意义的态势感知。

我们的研究成果是根据 DATES 项目而来。在该项目中，我们结合多种检测方法，包括使用基于学习的异常检测新方法和 ArcSight SIEM 系统，以提供一个适合于广泛应用于能源领域的控制系统的态势感知解决方案。我们展示了两个互联的试验台上的组件套件。项目团队发起了多个针对试验台的跨站和网络遍历攻击。这些攻击被传统特征技术和 DATES 开发的异常检测技术检测到。SIEM 提供了特别丰富的网络遍历攻击呈现。

参考文献

1. S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, "Using model-based intrusion detection for SCADA networks," in *Proceedings of the SCADA Security Scientific Symposium*, Miami Beach, Florida, Jan. 2007.
2. A. Blum, D. Song, and S. Venkataraman, "Detection of interactive stepping stones: Algorithms and confidence bounds," in *Recent Advances in Intrusion Detection (RAID)*. Springer, 2004, pp. 258-277.
3. S. Staniford-Chen and L. Heberlein, "Holding intruders accountable on the Internet," in *Proceedings of the 1995 IEEE Symposium on Security and Privacy*, 1995, pp. 39-49.
4. British Columbia Institute of Technology (BCIT), "NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks. Revision 14," Feb. 2005.
5. M. Roesch, "Snort: Lightweight intrusion detection for networks," in *Proceedings of LISA '99: 13th Systems Administration Conference*, Seattle, Washington, Nov. 7-12, 1999, pp. 229-238.
6. A. Valdes and K. Skinner, "Adaptive, model-based monitoring for cyber attack detection," in *Recent Advances in Intrusion Detection (RAID 2000)*, ser. LNCS, H. Debar, L. Me, and F. Wu, Eds., Toulouse, France, Oct. 2000.
7. P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," in *Network Information Security Conference*, 1997.
8. U. Lindqvist and P. A. Porras, "Detecting computer and network misuse through the production-based expert system toolset (P-BEST)," in *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, Oakland, California, May 9-12, 1999, pp. 146-161.
9. "Symantec Endpoint Protection System," last accessed March 25, 2010. [Online]. Available: http://www.symantec.com/business/ endpoint-protection
10. "McAfee Antivirus Enterprise," last accessed March 30, 2010. [Online]. Available: http://www.mcafee.com/us/enterprise/products/system_security/servers/virusscan_enterprise.html
11. Digital Bond, "IDS signatures," last accessed April 20, 2010. [Online]. Available: http://www.digitalbond.com/index.php/research/scada-idsips/ ids-signatures/
12. A. Valdes and S. Cheung, "Communication pattern anomaly detection in process control systems," in *2009 IEEE International Conference on Technologies for Homeland Security*, Waltham, MA, May 11-12, 2009.
13. P. Porras, M. Fong, and A. Valdes, "A mission-impact-based approach to INFOSEC alarm correlation," in *Proceedings of Recent Advances in Intrusion Detection*, October 2002, pp. 95-114. [Online]. Available: http://www.csl.sri.com/papers/mcorrelator/
14. "Invensys process systems," last accessed March 23, 2010. [Online]. Available: http://www.ips.invensys.com/en/products/autocontrols/Pages/ DistributedControl-IASeries-P018.aspx
15. M. McDonald, J. Mulder, B. Richardson, R. Cassidy, A. Chavez, N. Pattengale, G. Pollock, J. Urrea, M. Schwartz, W. Atkins, and R. Halbgewachs, "Modeling and Simulation for Cyber-physical System Security Research, Development and Applications," Sandia National Laboratories, Tech. Rep. Sandia Report SAND2010-0568, Feb. 2010.
16. "ICCP," last accessed April 21, 2010. [Online]. Available: http://intelligrid.ipower.com/IntelliGrid_Architecture/New_Technologies/Tech_IEC_60870-6_%28ICCP%29.htm
17. "DATES demo at DistribuTech 2010," last accessed April 21, 2010. [Online]. Available: http://www.csl.sri.com/projects/dates/distributech. html
18. J. Eisenhauer, P. Donnelly, M. Ellis, and M. O' Brien, "Roadmap to secure control systems in the energy sector." [Online]. Available: http://www.oe.energy.gov/Roadmap — to — Secure — Control_Systems_in_the_Energy_Sector.pdf
19. J. Stamp, M. Berg, and M. Baca, "Reference Model for Control and Automation Systems in Electrical Power," Sandia National Laboratories, Tech. Rep., 2005.
20. "Linking the oil and gas industry to improve cybersecurity," last accessed March 23, 2010. [Online]. Available: http://www.cyber.st.dhs. gov/logiic.html
21. "Tofino," last accessed April 20, 2010. [Online]. Available: http: //www.tofinosecurity.com/products/Tofino-Firewall-LSM
22. "Industrial defender," last accessed April 20, 2010. [Online]. Available: http://www.industrialdefender.com/

关键基础设施系统攻击检测、关联与呈现

安全加社区

公益译文项目

2016

网络安全公益译文项目旨在分享国外先进网络安全理念，将网络安全战略性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。该项目由安全加社区发起，安全加社区是国内的网络安全社区，社区欢迎网络安全人士的加入，并致力于交付网络安全问题的解决能力。