文章编号:1671-4598(2018)10-0250-05 DOI:10.16526/j.cnki.11—4762/tp.2018.10.054 中图分类号:TP391 文献标识码:A

工业控制网络中 APT 攻击检测系统设计

赵 澄, 方建辉, 姚明海
(浙江工业大学 信息工程学院, 杭州 310023)

摘要: 高级持续性威胁 (advanced persistent threat, APT) 是当今工控网络安全首要威胁, 而传统的基于特征匹配的工业入侵检测系统往往无法检测出最新型的 APT 攻击; 现有研究者认为, 敏感数据窃密是 APT 攻击的重要目的之一; 为了能准确识别出 APT 攻击的窃密行为, 对 APT 攻击在窃密阶段受控主机与控制与命令 (Control and Command, C&C) 服务器通信时 TCP 会话流特征进行深入研究, 采用深度流检测技术, 并提出一种基于多特征空间加权组合 SVM 分类检测算法对 APT 攻击异常会话流进行检测; 实验表明, 采用深度流检测技术对隐蔽 APT 攻击具备良好的检测能力, 而基于多特征空间加权组合 SVM 分类检测算法较传统单一分类检测的检测精度更高, 误报率更低, 对工控网络安全领域的研究具有推进作用。

关键词: 高级持续性威胁; 工控网络; 深度流检测; 组合分类检测算法

Design of APT Attack Detection System in Industrial Control Network

Zhao Cheng, Fang Jianhui, Yao Minghai
(College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China)

Abstract: The advanced persistent threat (APT) is the foremost threat to industrial network security today, and traditional feature detection-based industrial intrusion detection systems are often unable to detect the latest APT attacks. Existing researchers believe that theft of sensitive data is one of the important goals of APT attacks. In order to accurately identify the stealing behavior of the APT attack, the APT attack in the stealing phase controlled host and the control and command (C&C) server communication TCP flow characteristics in-depth study, the use of depth flow detection technology, and proposed a a multi-feature spatial weighted combined SVM classification detection algorithm which is used to detect abnormal APT attack session flows. Experiments show that the use of depth flow detection technology has a good ability to detect hidden APT attacks, and the multi-feature spatial weighted combined SVM classification detection algorithm has higher detection accuracy and lower false alarm rate than traditional single classification detection, and it is also safe for industrial control security. The research has a promoting effect.

Keywords: advanced persistent threat; industrial network security; deep flow detection; combined SVM classification

0 引言

随着工业化, 信息化的发展与深入, 新一代的高级持续性威胁 (advanced persistent threat, APT) 已成为当今工业控制系统安全的首要威胁[1]。据美国国土安全部下属的工业控制系统网络应急响应小组 (ICS-CERT) 发布的报告披露, 2014 年 9 月~2015 年 2 月期间共发生了 245 起网络安全事件, 其中超过半数属于 APT 攻击, 并且对重要能源工业, 化工, 核工业等均造成了重大的危害[2-3]。尽管企业在网络安全防护领域的能力有所提高, 传统的基于模式匹配的入侵检测系统已经能够检测出大部分的网络攻击, 如分布式拒绝服务 (Distributed Denial of Service, DDOS), 蠕虫病毒, 已知的木马病毒等, 但是却无法有效检测出攻击手段高明, 持续时间长久, 隐蔽性极高的 APT 攻击, 因为 APT 攻击者通常利用零日漏洞, 并使用标准协议和加密通信 (如 HTTPS) 来逃避检测[4-5]。针对未知 APT 攻击的防范, 全球一些安全公司在对 APT 攻击展开持续跟踪与分析后的报告[6-7]中指出, 虽然无法预知新变体的文件特征, 但是 APT 攻击中恶意软件在窃密阶段与 C&C 服务器的通信模式却是不变的, 因此分析恶意软件与控制命令 (Control and Command, C&C) 服务器建立通信时产生的深度流特性是 APT 攻击检测一个重大的突破口。戴震, 程光等人根据安全公司对已有 APT 活动通信特征的描述, 将全球安全公司 APT 活动报告中出现的特征进行提取并存入特征库, 并提出一种双层特征匹配的方法对网络报文进行分析[8]。该方法对已有的 APT 攻击检测具有较高的检测率, 但是利用传统特征匹配的方法缺乏对未知攻击的检测能力。Sana Siddiqui 等人分析 APT 攻击时恶意软件与 C&C 服务器产生的 TCP 流特征, 提出一种利用分形维数并使用机器学习思想的 APT 攻击检测方法[9], 该方法能较为有效地检测出 APT 攻击, 但是提取的特征只有单个 TCP 会话的数据包总数以及 TCP 会话的持续时间, 两类特征并不能很好的区分正常流量与异常流量。孙易安等人认为传统以单纯隔离为手段的工业防护系统已经无法检测出新型 APT 攻击, 提出一种以纵深防御为手段的 "4+1" 安全防护模型, 对工业控制系统进行全网防护, 该模型只是提出一种可行的框架[10], 但是并未对具体的检测模块进行相应的分析论

收稿日期:2018-04-02; **修回日期**:2018-04-08。

作者简介:赵 澄(1985-),男,浙江绍兴人,博士,高级工程师,主要从事人工智能、计算机网络和量化金融方向的研究。

姚明海(1963-),男,浙江省嘉善人,教授,博士生导师,主要从事人工智能,无线传感网络方向的研究。

证。MircoMarchetti 等人利用大数据方法以天为检测时间窗口提取某大型企业的主机流量特征，从特征向量与特征中心点的欧式空间测度与向量时间变化测度对主机流量行为进行评分，最后输出系列可疑主机名单用于人工分析判别[11]。然而目前针对的 APT 攻击流量异常检测方法大多基于骨干网流量异常分析或者基于应用层流量异常分析[12-14]的方法，而这些基于粗粒度检测方法很难检测出擅长隐匿潜伏的 APT 攻击，并且实时性不足，容易在攻击被发现前就造成巨大的危害。

为此，设计了一种基于深度流特性的 APT 攻击检测系统，提取最能反映 APT 可疑通信行为的深度流特征，利用基于多特征空间的加权组合 SVM 分类器对 APT 可疑行为进行判别。实验表明，本文提取的可疑 APT 攻击行为的深度流特征对检测 APT 攻击具有良好的检测效果，而利用基于多特征空间的组合 SVM 分类器方法能进一步提高检测精度并且降低误报率，对工控网络安全防护具有较高的借鉴价值。

1　系统结构与原理

随着工业控制系统的“两化融合”的逐步推进，原本处于隔离状态的工业控制系统与管理系统可以直接通信，甚至能直接连入互联网。使得工业控制系统也面临了来自互联网的威胁。而工控系统管理网络通常会是 APT 攻击者攻击的首要目标。为此，本文设计了一套应用于工控网络环境下的深度流检测软件系统，针对工控网络中的管理网络层的深度流数据进行异常检测。深度流检测技术应用在工控网络环境下 APT 攻击检测中即是以流为检测单位，提取 APT 窃密通信产生的异于正常通信行为的流的特征，并利用机器学习方法判别流是否异常。由于基于深度流的 APT 攻击检测方法不对应用层数据深入分析，只对流特征数据进行深入挖掘与分析，因而即使对利用加密隧道通信的隐匿 APT 攻击也具备良好的检测性能。基于深度流检测模型框架分为数据采集模块，数据预处理模块，检测模块和报警模块 4 个部分。系统总体架构如图 1 所示。

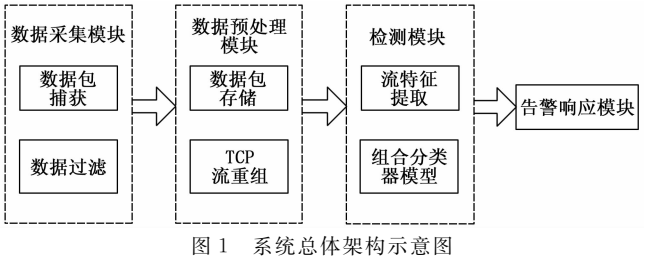

图 1　系统总体架构示意图

1）数据采集模块：系统的数据采集模块部署在工控网络系统的脆弱节点与敏感节点处，在 linux 系统环境下利用 Libpcap 函数库实现对数据包的采集，通过 BPF（BSD packet filter）算法进行数据包过滤，由于本文只分析基于 TCP 流的通信特征，并以 TCP 流数据作为特征提取的基础数据，因而需要对其它协议的数据包进行丢弃。

2）数据预处理模块：对于采集到的数据包需要将其暂时存储到内存中，为了节省内存空间，只提取数据包部分信息存储以作为下一步 TCP 流重组的元数据，元数据记录信息包括数据包采集时间戳，源目 IP，源目端口，数据包长度，SYN 位数值，FIN 位数值。将采集到的数据包进行会话还原，消除因网络条件造成的乱序，重传，延迟等异常对判别造成干扰，并从非结构化的数据流中抽取结构化的元数据信息。进一步，采用 TCP 流重组算法提取 TCP 会话流。

3）检测模块：从会话流元数据中通过简单组合计算等获取所需的检测特征并向量化，将检测向量输入到组合 SVM 检测模型中判定是否为异常会话流，检测模块是本文研究的关键技术与方法，因此将在下一节作详述。

4）告警模块：当检测模块的输出结果大于给定阈值时，记录异常的时间戳，源目 IP，源目端口信息，并向网络管理员发出告警。

2　检测模型设计

2.1　特征提取与分析

在一个深度流检测系统中，特征选取往往决定检测模型性能的好坏，本文对 APT 恶意软件与工控网络 C&C 服务器通信特征进行深入分析，提取最具代表性的 7 维特征。其中 APT 攻击流量样本数据来自于 Contagio malware database[15]，正常流量数据则是利用浙大中控的 WebField JX－300XP 工业控制系统搭建实验平台，采集管理用户与外界联网的流量数据。

2.1.1　间隔时间特征

大多数正常 TCP 通信模式是一个简单的客户端请求资源并得到服务器端响应的过程，工控环境中数据包的传输时间间隔往往比较稳定，并且由于服务器的性能较高，处理客户端请求的速度往往很快，所以时间间隔也比较小。而 APT 攻击则是一个交互的通信过程，攻击者对恶意软件发出指令得到响应后可能还需要一定的思考时间发送下一个指令，所以时间间隔序列的平稳性更低，并且被控主机作为服务器端完成攻击者的指令任务，其处理能力肯定不如服务器，因此数据包时间间隔较大。因此选取一条 TCP 流的平均间隔时间 $T_{ave\Delta}$，最大间隔时间 $T_{max\Delta}$，间隔时间序列的标准差 σT_{Δ} 作为该项检测特征。对数据集中 APT 与正常通信产生的 TCP 流间隔时间特征进行统计分析，统计结果如表 1 所示，APT 攻击的间隔时间相对较大并且时间间隔序列标准差也更高。

表 1　间隔时间特征比较

特征	最小值		最大值		平均值	
描述	正常	APT	正常	APT	正常	APT
$T_{ave\Delta}$/s	0.000021	0.001538	48.792724	152.352737	12.165465	34.023476
$T_{max\Delta}$/s	0.000024	0.000362	118.538422	387.604381	18.204755	52.068364
$\sigma_{T\Delta}$/s	0	0.002803	75.347956	165.427168	9.184656	25.457682

2.1.2　数据包特征

恶意软件与 C&C 服务器通信时内网工控主机会接收到

大量来自服务器端的小数据包，这些小数据包往往攻击者的指令数据，因此数据包的长度往往较短，而正常通信情况内网主机接收的下载数据包则为服务器对主机请求的响应，通常采用大数据包传输，因而数据包长度总体偏大。根据经验，定义数据包字节长度小于 100 byte 的数据包为小数据包。

提取下载数据包平均长度 L_{ave} 以及下载小数据包数与下载数据包总数之比 F_{sp} 作为待检测检测特征。

$$L_{ave} = \frac{L_{cocal}}{N_{pdown}} \tag{1}$$

$$F_{sp} = \frac{N_{spdown}}{N_{pdown}} \tag{2}$$

其中：l_{total} 表示下载数据包总字节数。N_{spdown} 代表下载小数据包总数，N_{pdown} 代表下载数据包总数。

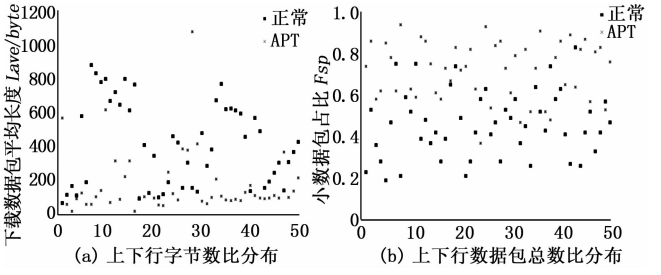

图 2 数据包特征分布

数据包特征的实验分析结果如图 2（a），图 2（b）所示，我们发现 APT 攻击产生的下载数据包平均长度 L_{ave} 大多分布在 150 byte 以内，下载小数据包数占总下载数据包总数之比 F_{sp} 大多分布在 0.6 以上，而正常通信数据中 L_{ave} 则大多分布在 200 byte 以上，而 F_{sp} 值则大都分布在 0.6 以内。

2.1.3 上下行流量比特征

正常情况下，工控主机向外网服务器发出资源请求，资源请求的数据包一般都很小，服务器响应该请求并发送相应内容，此时服务器传输的数据包一般较大。因此，正常通信情况下上行流量会明显小于下行流量。而受攻击的工控主机与 C&C 服务器通信时的情况正好完全相反，外网 C&C 服务器作为控制端向被控主机发送指令，工控主机返回指令结果，并且回传相应的数据信息这就导致了存在 APT 攻击行为的 TCP 流的上行流量常常会大于上行流量。提取一条 TCP 流中上传数据包与下载数据包数量之比 F_p 与上传数据包字节长与下载数据包字节长度之比 F_l 作为待检测的特征向量。

$$F_p = \frac{N_{pup}}{N_{pdown}} \tag{3}$$

其中：N_{pup} 代表上传数据包总数，N_{pdown} 代表下载数据包总数。

$$F_l = \frac{N_{lup}}{N_{ldown}} \tag{4}$$

其中：N_{lup} 代表上传数据包字节数总长，N_{ldown} 代表下载数据包字节数总长。

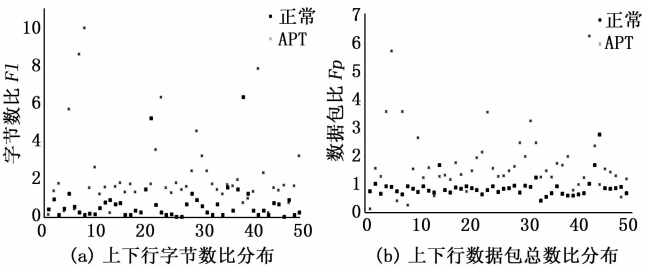

图 3 上下行流量比特征分布

上下行流量比特征的实验分析结果如图 3（a），图 3（b）所示，APT 攻击样本的上下行流量比特征分布区间 F_l 与 F_p 大多大于 1，而正常样本此类特征的值分布为 F_p 大都分布在 0.5～1 之间，而 F_l 大多分布在 0～0.6 之间。

构建由上述 7 种特征组成的特征表，如表 2 所示。

表 2 特征表

特征指标(符号)	特征说明
$T_{ave\Delta}$	TCP 流中数据包传输序列平均间隔时间
$T_{max\Delta}$	TCP 流中数据包传输序列最大间隔时间
$\sigma_{T\Delta}$	TCP 流中数据包传输序列间隔时间序列的标准差
L_{ave}	TCP 流中下载数据包平均长度
F_{sp}	TCP 流中下载小数据包数占总下载数据包总数之比
F_p	TCP 流中上传数据包与下载数据包数量之比
F_l	TCP 流中上传数据包字节长与下载数据包字节长度之比

2.2 组合 SVM 分类检测算法

传统的机器学习算法往往是由单一特征描述与单一分类器对样本进行分类，这样的分类算法往往会由于单一训练特征空间无法全面描述事物各个方面而导致在某些情况下分类器性能下降，误报率增多。为了克服由单一特征集训练造成的弊端，提高分类器的性能，本文采用基于特征空间的分类器构造方法，训练了由 3 个不同特征集训练出的 3 个 SVM 分类器。这 3 个 SVM 基分类器并联组成一个新分类器，训练之后的每个分类器模型的输出为发生 APT 攻击事件的预测值 p_i，$i=\{1,2,3\}$。根据不同 SVM 分类器的置信度，为每个分类器赋予不同的投票权值，通过投票法得出组合分类器预测结果。对于待评估样本 Q，SVM 基分类器的信用度取决于其自身分类能力在 Q 领域上决策准确率的一致程度[16]。根据经验评估法，以 SVM 决策分界面的几何间隔 $\frac{1}{\|w\|}$ 和测试样本使用 SVM 分类器的决策正确率 k 作为 SVM 基分类器信用度的度量。设 $\lambda=-\frac{\|w\|}{k}$，定义基分类器的置信度 $\gamma=\frac{1-e^{-\lambda}}{1+e^{-\lambda}}$，因此分类器的几何间隔越大，分类准确率越高，分类器信用度就越高，决策时投票权重越大。假定由多个 SVM 投票得出预测值为 p。假定

由多个 SVM 投票得出预测值为 p。

$$p = p_1 S_1 + p_2 S_2 + p_3 S_3 \tag{5}$$

其中：$S_1 = \frac{r_1}{r_1 + r_2 + r_3}$，$S_2 = \frac{r_2}{r_1 + r_2 + r_3}$，$s_3 = 1 - S_1 - S_2$，分别代表了三个 SVM 基分类器投票时的权重。为了提高分类器的检测能力，降低误报率，设定算法决策准则为：

$$(p_1 > \delta) \cap (p_2 > \delta) \cap (p_2 > \delta) \cap (p > \tau) \tag{6}$$

正是由于输入数据的海量性，并且针对 APT 攻击的防范，流量检测只是其中的一个关键环节，因而更希望检测分类结果趋向于正常，以减少虚警率。因此，取 $\delta = 0.4$，$\tau = 0.6$。这样设定的意义在于 δ 是每个分类器的否决阈值，当三个基分类器中的任意一个的得分小于设定阈值时，都可以将直接将样本归于正常样本，而 τ 则表示最终的投票得分输出的判定阈值，因此适当提高阈值则能够降低误报率。检测模型如图 4 所示，将提取到的特划分为 3 个特征子空间模块，输入到不同以不同特征集训练的 SVM 基分类器中，每个 SVM 基分类器输出一个 APT 攻击预测值，将这些预测值输入当决策器中，如果满足公式（6）的判别条件，则认为该样本数据为可疑攻击数据，否则为正常通信会话流数据。

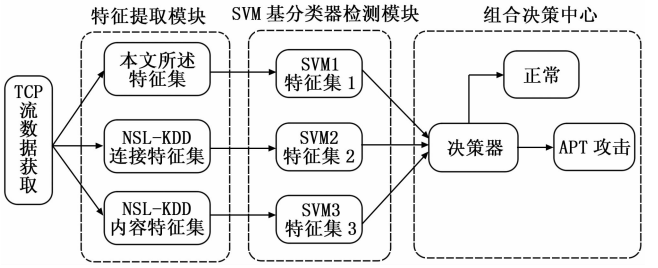

图 4　组合分类器检测模型

3　实验结果与分析

3.1　实验数据与评价指标

本文的实验环境包括操作系统 64 位 Ubuntu16.04，处理器英特尔酷睿 i5 2467M，4 核 8 线程，内存 32G，硬盘大小 1TB，使用 Libcap 库对离线流量数据进行处理，机器学习模块使用 LIBSVM 库。实验数据主要来自于两方面，APT 攻击数据样本来自于 Contagio malware database[15]，正常流量数据则是采集浙大中控的 WebField JX－300XP 工业控制系统管理用户与外界联网的流量数据。将 APT 攻击数据注入到背景流量当中的融合流量数据输入到检测系统中，经过数据包采集与预处理，提取出会话流特征，并输入到组合分类器检测模型进行异常会话流检测。

为了准确评价检测模型的性能，引入准确率，精确率，召回率（True Positive Rate，TPR），误报率（False Negative Rate，FPR），F 值（F－measure），曲线面积（Area Under Curve，AUC）6 个评价指标。其中，准确率表示所有预测正确的样本数目占样本总数目的比例，精确率表示预测为 APT 攻击数据的分类正确率，召回率表示正确预测 APT 攻击的样本数目占所有 APT 攻击样本数目的比例，误报率正常通信数据被预测为 APT 攻击数据占正常样本数目的比例，F－measure 与 AUC 用于评价分类器 ROC 曲线，F－measure 是精确率与召回率的加权调和平均，AUC 表示 ROC 曲线下面的面积。

3.2　实验结果与分析

将本文的基于并联 SVM 组合分类器检测模型检测结果与基于单一特征集的 SVM 单分类器检测模型检测结果进行比较，实验结果如表 3 所示。

表 3　不同 SVM 检测模型效果

分类器	准确率/%	精确率/%	召回率/%	误报率/%	F－measure/%	AUC
SVM1	91.6	78.1	87.6	7.2	82.5	0.941
SVM2	88	71.5	78.1	9.1	74.7	0.897
SVM3	88.4	72.8	77.2	8.7	74.7	0.886
组合 SVM	92.9	80.5	90.4	6.3	80.5	0.955

由表 3 可知，选用本文所述的特征集训练的 SVM1 分类器的性能比选用 NSL－KDD 特征集训练出的分类器精确率更高而误报率更低，说明本文选取的特征对 APT 攻击描述更加具有代表性，而 SVM2 与 SVM3 的召回率分别为 78.1%与 77.2%误报率为 9.1%与 8.7%，说明 SVM2 与 SVM3 选用的特征空间也能较为有效地描述 APT 攻击特性。准确率比召回率高 10%左右，这是因为制定的决策准则适度提高了的判定攻击阈值，因此正常通信样本被误分数目减少，误报率显得更低，而正常通信样本的数目远多于 APT 攻击样本数目，因而准确率比召回率更高。通过对比本文组合 SVM 分类器与其余分类器的实验结果，我们发现本文所述组合分类器方法在大多数时候的性能都优于 SVM1 分类器，组合分类器的准确率召回率更高，而误报率更低。这是因为不同特征描述的单一分类器误分集合并不完全重叠，因此不同特征训练得到分类器往往拥有互补信息，本文组合分类器的检测模型正是综合利用这些互补信息而提高了分类器的性能。

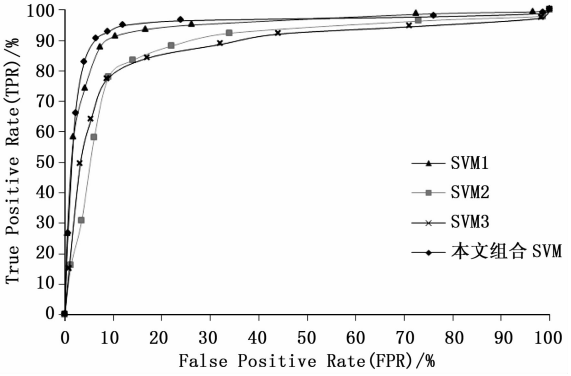

图 5　组合 SVM 与单一分类器 ROC 曲线对比图

各 SVM 分类器检测效果 ROC 曲线图如图 5 所示，ROC 曲线图的检测阈值为决策准则中的投票判定阈值。图 4 中组合 SVM 分类器的 F－measure 值以及 AUC 值在绝大

多数时候均是所有分类器里面最高的，说明组合 SVM 分类器的检测性能最优。而 SVM1 与组合 SVM 分类器的 AUC 值都达到 90%以上，说明二者的性能都较为不错。

4 结论

APT 攻击是当今工业控制系统安全的首要威胁，针对传统基于模式匹配的入侵检测系统无法有效检测新型 APT 攻击，设计了一种基于深度流特性的 APT 攻击检测系统，在工控网络脆弱节点与敏感节点部署流量采集模块，将采集到的数据经过预处理后输入组合 SVM 分类检测模型进行异常会话流判别，实验结果表明，基于深度流特性的 APT 攻击检测方法具有较高的准确率，同时，基于投票法的组合分类器算法较传统单一分类器检测精度更高，误报率更低，具有良好的实用价值。然而，APT 攻击是一系列极为复杂的攻击过程的总和，仅仅根据异常会话流无法断定存在攻击，在今后的研究中，还应对可疑邮件，可疑 HTTP 传输等作进一步深入研究，关联 APT 攻击各个阶段的异常行为事件，准确快速地发现威胁所在，降低工业控制系统受害的风险与损失。

参考文献：

[1] Inkyung J，Youngsook L，Dongho W. A practical study on advanced persistent threats [A]. Computer Applications for Security，Control and System Engineering [C]. Springer，2012：144－152.

[2] 李术夫，李 薛，王 超. 典型 APT 攻击事件案例分析 [J]. 信息网络安全，2016 (s1)：85－88.

[3] Industrial Control System Cyber Emergency Response Team. ICS－CERT Year in review 2014 [R]. https：//ics－cert. us－cert. gov/sites/default/files/Annual _ Reports/Year _ in _ Review _ FY2014 _ Final. pdf.

[4] Yang G，Tian Z，Duan W. The prevent of advanced persistent threat [J]. Journal of Chemical & Pharmaceutical Research，2014.

[5] 王晓琪. 高级持续性威胁中隐蔽可疑 DNS 行为的检测 [J]. 计算机研究与发展，2017，54 (10)：2334－2343.

[6] Manggalanny M S，Ramli K. Real time DNS traffic profiling enhanced detection design for national level network [A]. International Seminar on Intelligent Technology and ITS Applications [C]. IEEE，2017：11－15.

[7] Friedberg I，Skopik F，Settanni G，et al. Combating advanced persistent threats [J]. Computers & Security，2015，48 (C)：35－57.

[8] 戴 震，程 光. 基于通信特征的 APT 攻击检测方法 [J]. 计算机工程与应用，2017，53 (18)：77－83.

[9] Siddiqui S，Khan M S，Ferens K，etal. Detecting advanced persistent threats using fractal dimension based machine learning classification [A]. Proceedings of the 2016 ACM on International Workshop on Security and Privacy Analytics [C]. ACM，2016：64－69.

[10] 孙易安，井柯，汪义舟. 工业控制系统安全网络防护研究 [J]. 信息安全研究，2017，3 (02)：171－176.

[11] Marchetti M，Pierazzi F，Colajanni M，et al. Analysis of high volumes of network traffic for advanced persistent threat detection [J]. Computer Networks，2016，109：127－141.

[12] 郑黎明，邹 鹏，韩伟红，等. 基于多维熵值分类的骨干网流量异常检测研究 [J]. 计算机研究与发展，2012，49 (09)：1972－1981.

[13] Zhao G，Xu K，Xu L，et al. Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis [J]. Access IEEE，2015，3：1132－1143.

[14] 郑黎明，邹 鹏，贾 焰. 多维多层次网络流量异常检测研究 [J]. 计算机研究与发展，2011，48 (08)：1506－1516.

[15] Parkour M. Contagio malware database [DB/OL]. https：//www. dropbox. com/sh/wje7mxs4nour40k/AAC3Zpoa5 wL-NwsGRvKxR9AnVa? dl＝0，2013－04－21/2017－06－23.

[16] 凌 萍，周春光. SVM 置信度在线评估以及决策改进 [J]. 计算机科学与探索，2008 (02)：192－197.

(上接第 249 页)

[3] Kocher P，Jaffe J，Jun B，et al. Introduction to differential power analysis [J]. Journal of Cryptographic Engineering，2011，1 (1)：5－27.

[4] 张 鹏，邓高明，陈开颜，等. 针对 AES 密码芯片的远场相关性电磁分析攻击 [J]. 华中科技大学学报 (自然科学版) 2009，37 (8)：31－34.

[5] Kocher P，Jaffe J，Jun B. Differential power analysis [A]. Advances in Cryptology — CRYPTO' 99 [C]. Lecture Notes in Computer Science Volume 1666，1999：388－397.

[6] Whitnall C，Oswald E. Profiling DPA：Efficacy and Efficiency Trade－Offs [A]. Cryptographic Hardware and Embedded Systems－CHES 2013 [C]. Lecture Notes in Computer Science Volume 8086，2013：37－54.

[7] Choudary O，Kuhn M G. Efficient template attacks [A]. Smart Card Research and Advanced Applications [C]. Lecture Notes in Computer Science 2014，253－270.

[8] Whitnall C，Oswald E. Profiling DPA：efficacy and efficiency trade－Offs [A]. Cryptographic Hardware and Embedded Systems－CHES 2013 [C]. Lecture Notes in Computer Science Volume 8086，2013：37－54.

[9] 余 凯，贾 磊，陈雨强，等. 深度学习的昨天、今天和明天 [J]. 计算机研究与发展，2013，50 (9)：1799－1804.

[10] Krizhevsky A，Sutskever I，Hinton G E. ImageNet classification with deep convolutional neural networks [J]. Communications of the Acm，2012，60 (2)：2012.

[11] 邓高明，赵 强，张 鹏，等. 针对密码芯片的电磁频域模板分析攻击 [J]. 计算机学报，2009，32 (4)：602－610.

[12] Mangard S，Oswald E，Popp T. 能量分析攻击 [M]. 冯登国，等译. 北京：科学出版社，2010.