北京大学
PEKING UNIVERSITY

Digital Forensics 数字取证

IEEE Computer and Reliability Societies 2017.11

杨雨月 刘艳伟 何家乐 林森

北京大学

目录
CONTENTS

北京大学

第一部分

Recent Advancements in Digital Forensics

数字取证技术的最新进展

最新进展 | Recent Advancements

1. 云计算、智能手机、可穿戴设备、互联网接入、数字钱包服务

现代数字取证必须在复杂和快速移动的场景中工作

2. 物联网（IoT） → 收集有关非数字环境信息

3. 恶意软件和网络威胁越来越多地配备了复杂的反取证技术

4. 现代数字取证是一个多学科的工作，包括法律、计算机科学、金融、网络、数据挖掘和刑事司法等。

北京大学

第二部分

The Future of Digital Forensics

数字取证的未来

本文探讨了数字取证技术的未来，重点讨论了这些挑战和有效保护现代社会和追捕网络罪犯所需的进展。

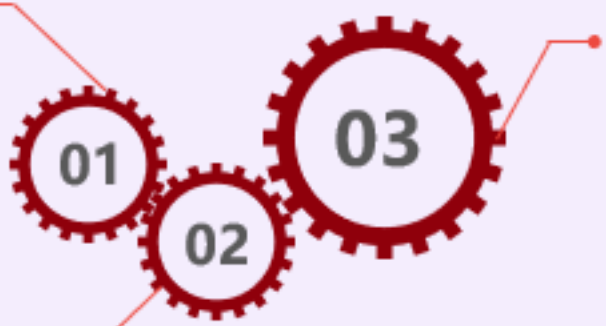
现代技术的缺陷

分析成本高

设备数量、数据总量飞速增长

一些系统为共享区加密

分析数据存储空间以及文件系统耗时



网络取证困难

经济效益差，相关设备较昂贵

大量数据使得设备过饱和

信息隐藏、流量加密、洋葱路由

逆向工程失效

反取证对策的部署

隐藏信息的恶意软件

挑战与未来 | Challenges and the Road Ahead

未来形式

1 创建工具和技术

※ 分析大量数据，并将可能的线索可视化地报告给检查者
※ 以自动或无人看管的方式
※ 缺乏统一的标准和不凡的计算要求

2 利用云计算的特性

※ 卸载取证过程中苛刻的操作
日志分析、数据索引、多媒体处理
※ 取证作为实用程序，如FaaS
将软件集中在单点上，容易更新改进
隐藏终端用户的复杂性
※ 利用软件定义的网络技术
提供了额外的抽象层，可以用于分析攻击或感染，而不需要消耗资源

3 数字物联网取证

※ 收集有关非数字环境信息
※ 正开始扭转取证的命运

IOT与CPS案例

挑战

节能（例如，太阳能节点）经常导致不连续和部分不完整的信息

具有专有接口的IoT设备的普及可能导致访问存储值很困难，可能需要反向工程

嵌入式系统中的资源限制，智能物品具有有限的内存和计算性能，持久记录不容易实现

历史传感器数据和执行器状态不一定总是对调查者可访问的

物联网和网络物理系统设备的特性及其对现代数字取证的影响

属性	与取证的关系	典型挑战
设备部署密度	影响在物理环境中发生事件的分辨率	基于部署不均匀的设备重构物理事件，可以根据所考虑的环境而变化
设备类型	影响信息的类型	为事件重建提供计算机辅助、证据驱动和取证证明框架
设备位置	影响用于数字取证调查的设备物理可访问性，并影响设备覆盖物理环境的区域界定	需要成本效益分析，以确定位于难到达地区的物联网设备是否值得访问
历史记录	IOT设备上的所有可用信息都可以在本地或云中记录。本地存储通常是有限的。	将物联网设备自动集成到物理重建过程中，需要获取传感器的记录历史并将其正确地放置在时间范围内，可能需要视觉分析工具的支持
设备接口	用于访问证据的接口高度影响可检索的信息量。某些类型的信息可能不被某些接口提供，而其他类型则会，供应商甚至可能没给接口	为物联网取证提供统一的元接口，覆盖大量不同的设备和一些供应商的低级接口

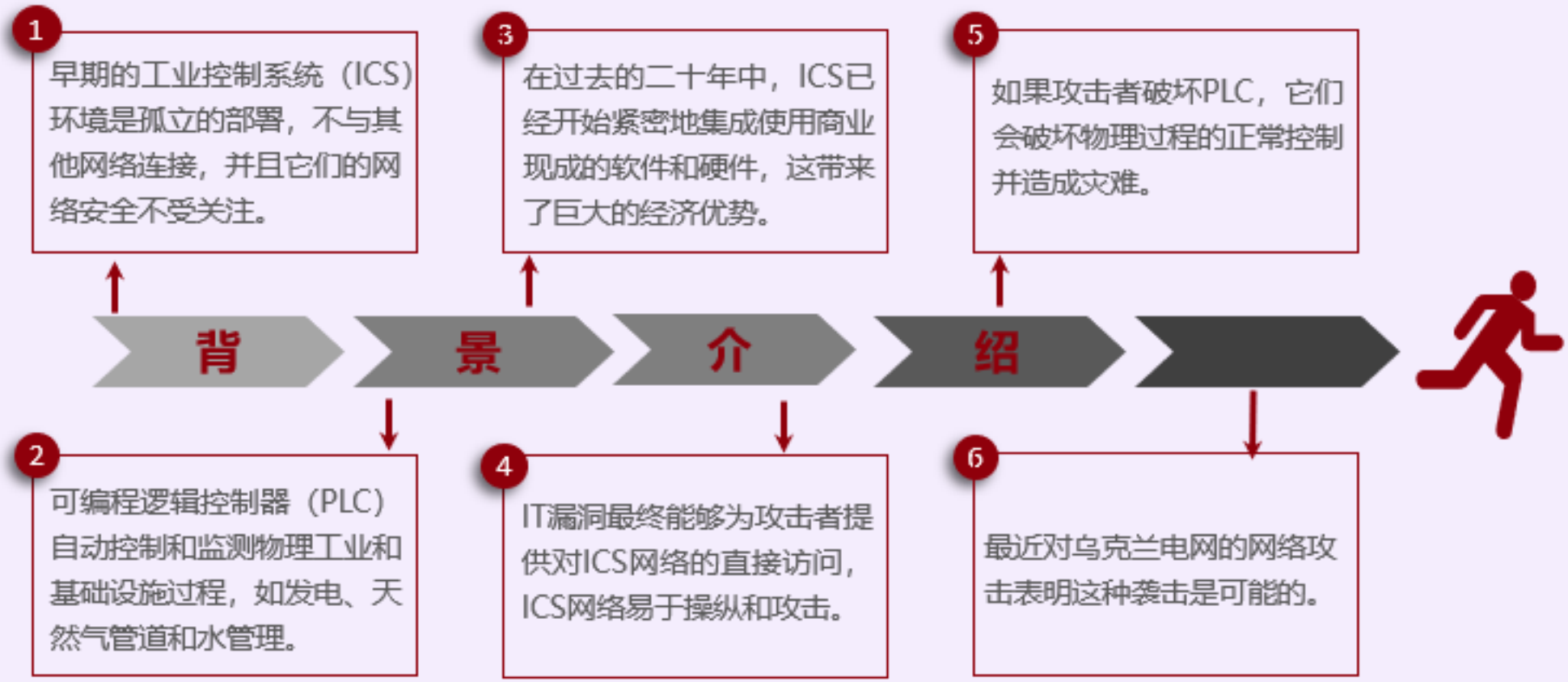
北京大学

第三部分

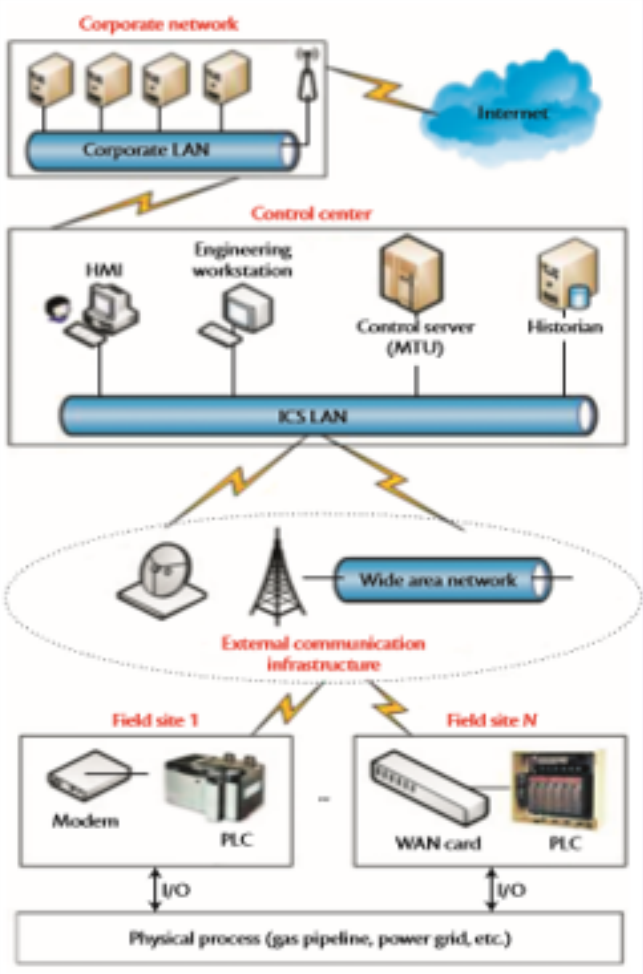
Programmable Logic Controller Forensics

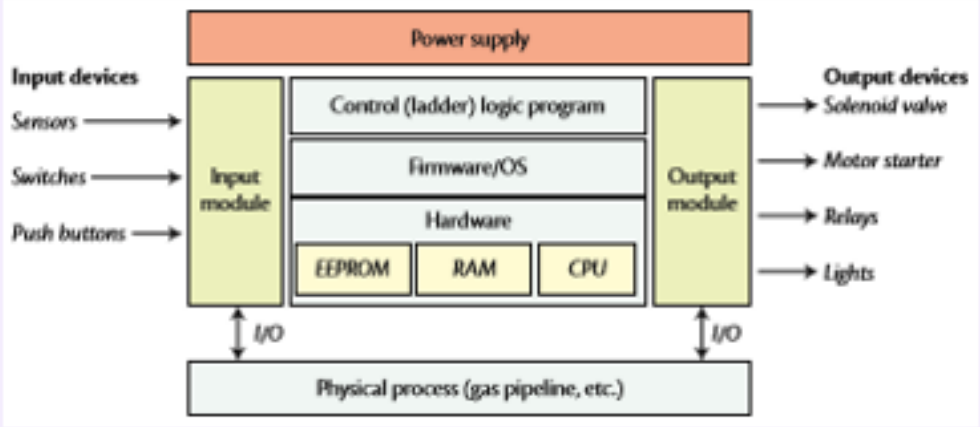
可编程控制器（PLC）取证

可编程逻辑控制器（PLC）自动控制和监测物理工业和基础设施过程，如发电、天然气管道和水管理。由于网络基础设施的趋同，PLC可能受到网络上的网络攻击，具有潜在的灾难性后果。本文介绍了针对各种攻击的基本机制，可以对它们进行检测、分析和最终补救。


1
早期的工业控制系统（ICS）环境是孤立的部署，不与其他网络连接，并且它们的网络安全不受关注。
3
在过去的二十年中，ICS已经开始紧密地集成使用商业现成的软件和硬件，这带来了巨大的经济优势。
5
如果攻击者破坏PLC，它们会破坏物理过程的正常控制并造成灾难。
背
景
介
绍
2
可编程逻辑控制器（PLC）自动控制和监测物理工业和基础设施过程，如发电、天然气管道和水管理。
4
IT漏洞最终能够为攻击者提供对ICS网络的直接访问，ICS网络易于操纵和攻击。
6
最近对乌克兰电网的网络攻击表明这种袭击是可能的。

PLC取证 | PLC Forensics





ICS环境

※ 控制中心：运行ICS服务
人机接口（HMI）、工程工作站、历史记录、控制服务器

※ 现场站点：安装在本地以监测和控制物理过程
传感器、执行器、可编程逻辑控制器（PLC）

PLC体系结构

输入输出模块、电源、存储器，如RAM和EEPROM

取证分析

侦察

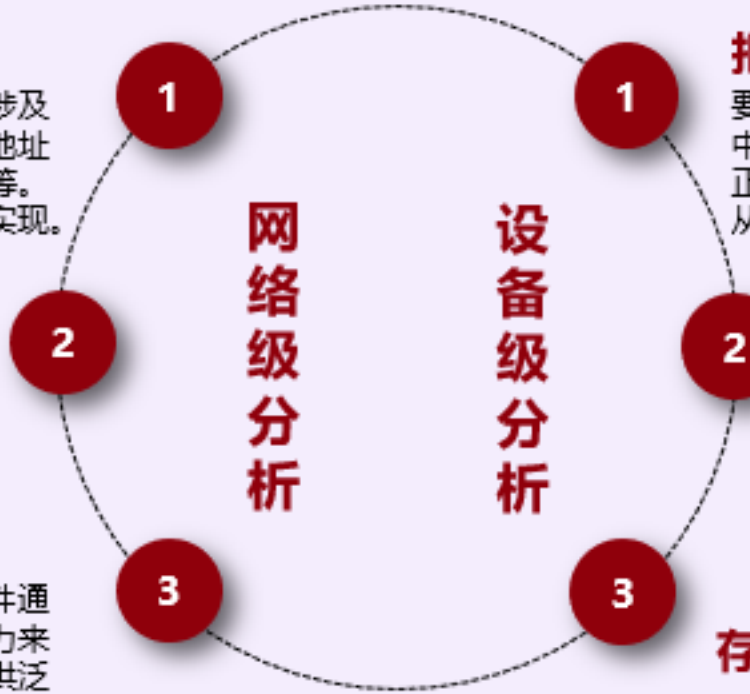
先于实际攻击的信息收集。涉及支持功能代码的识别、PLC地址的分配、制作、模型、固件等。可通过被动窃听或主动查询实现。

中间人MITM

所有通信量都通过攻击者的机器，允许他随意窃听和操纵消息内容。可通过地址解析协议（ARP）实现。

拒绝服务DoS

通过拒绝PLC与其他ICS组件通信或执行控制逻辑程序的能力来干扰其正常处理，可通过包洪泛来实现。



拒绝服务

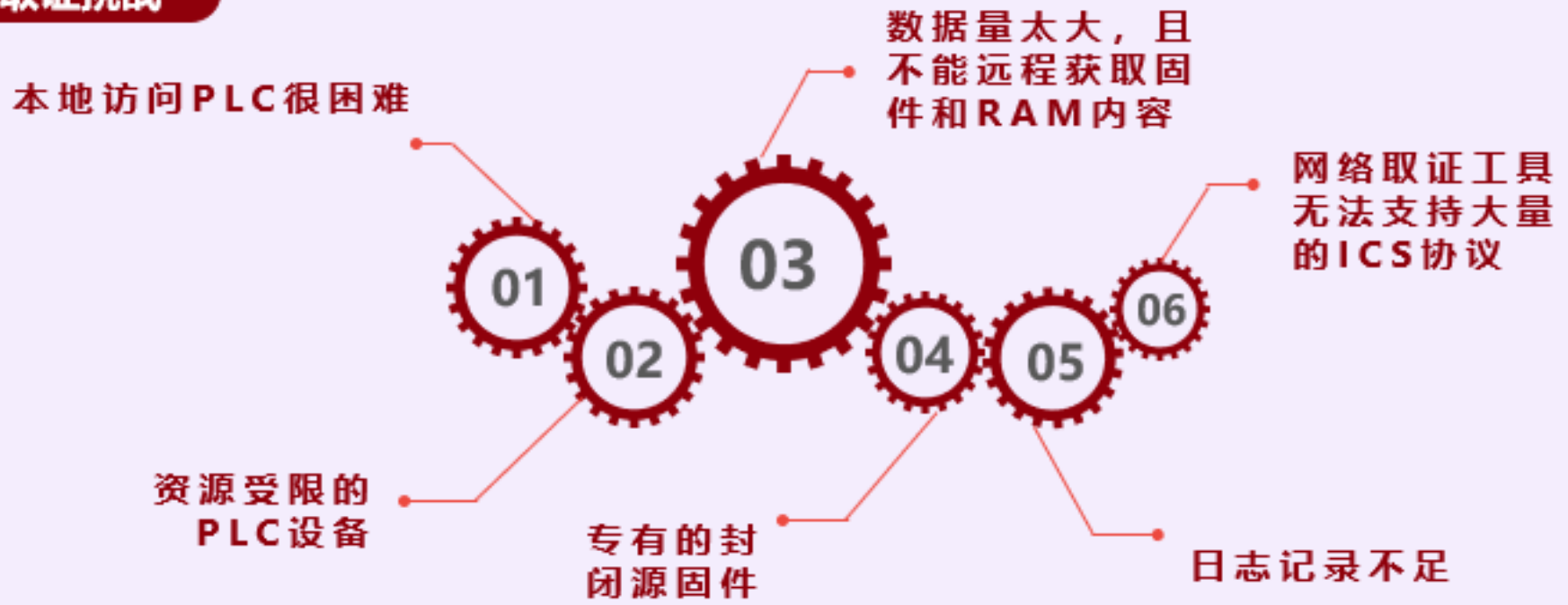
要么针对PLC组件（例如固件）中的漏洞，要么以恶意方式利用正常功能，或改变PLC操作模式从RUN到PROGRAM。

命令注入

向计算机系统中注入不需要的代码来执行的，从而获得对系统的未经授权的控制。分为状态注入、参数注入和功能代码注入

存储/固件损坏

取证挑战


本地访问PLC很困难
数据量太大，且不能远程获取固件和RAM内容
网络取证工具无法支持大量的ICS协议
01
02
03
04
05
06
资源受限的PLC设备
专有的封闭源固件
日志记录不足

PLC取证 | PLC Forensics

取证工具和方法

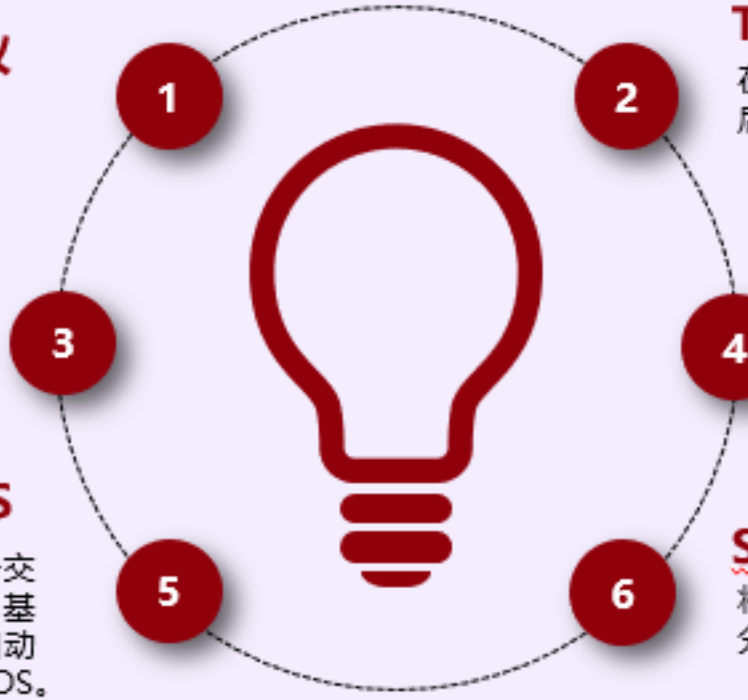
PCCC：分析ICS协议的网络通信日志

Ken Yau：控制程序逻辑变化检测器

使用梯形逻辑程序导出一组检测规则。利用这些规则分析运行逻辑程序的网络流量。

Amit Kleinmann：IDS

分析了西门子S7 PLC的网络交通流，观察到很强的周期性。基提出了一种利用确定性有限自动机来精确对网络流量建模的IDS。



Tim Kilpatrick：网络取证架构

在某些战略位置捕获网络数据包，然后根据捕获的数据包重构网络事件。

Craig Valli：Snort入侵检测系统(IDS)

创建用于异常检测的环境扫描，执行每个漏洞的生产和重放，分析每个漏洞，创建IDS规则集。

Saman A. Zonouz

将符号执行和模型检查结合起来，分析恶意注入的PLC代码的代码边界

北京大学

第四部分

Botnet Fingerprinting : Anomaly Detection In SMTP Conversations

僵尸网络指纹：SMTP会话中地异常检测

网络流量——具体来说，在电子邮件传递过程中观察到的简单邮件传输协议命令的序列和语法——可以帮助调查人员检测和识别垃圾邮件僵尸网络。

背景介绍

垃圾邮件危害

1

※ 使用者不方便
※ 浪费各种资源
（磁盘空间、可用带宽）
※ 网络钓鱼

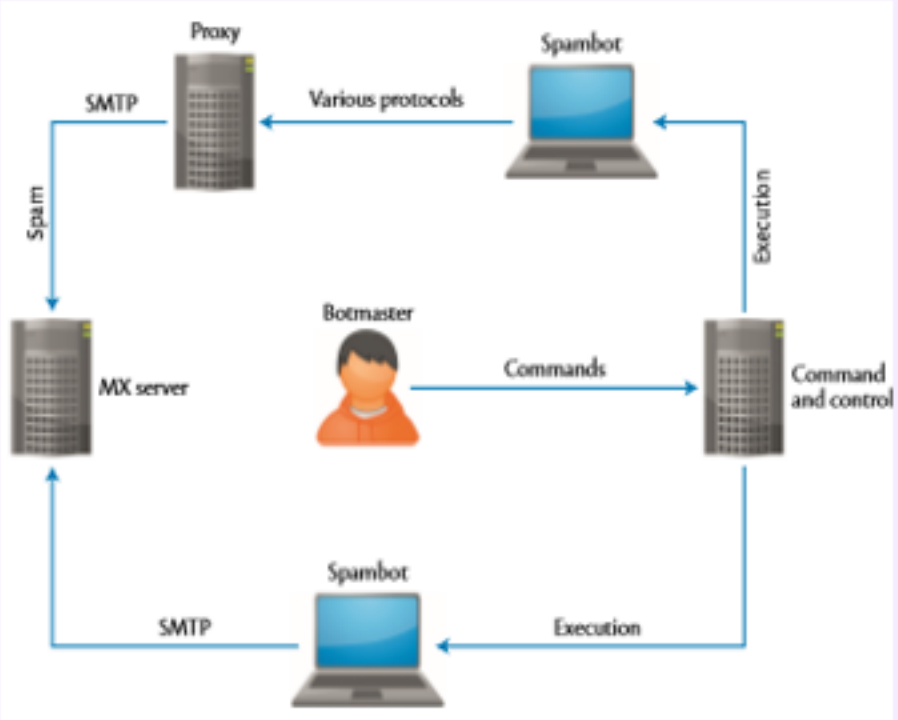
传统方法：分析邮件标题和内容

2

垃圾邮件来源

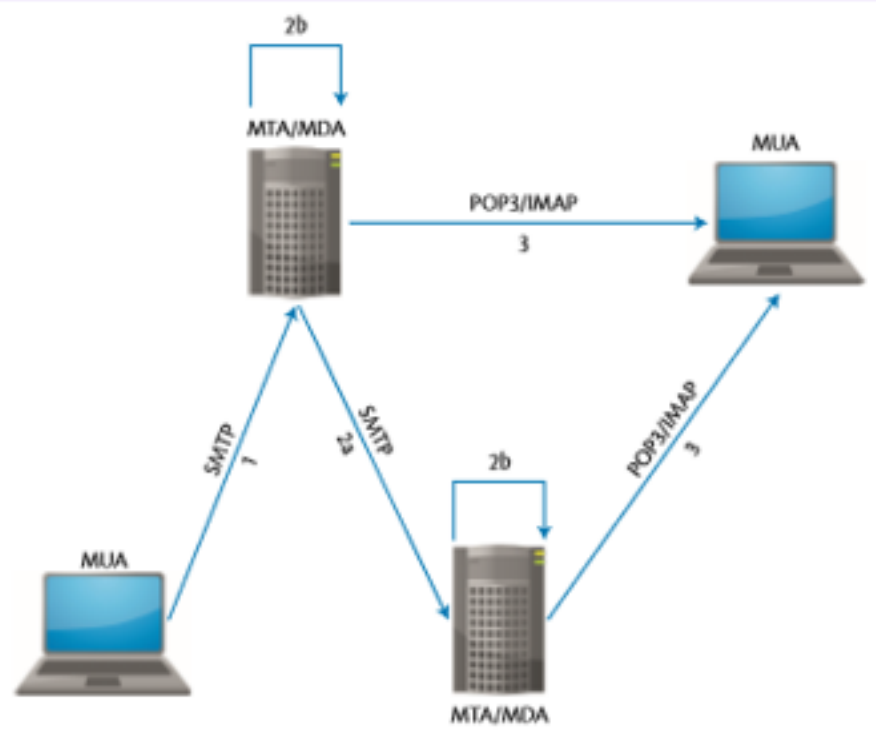
3

错误配置、受损的邮件服务器、专门准备的代理商（代理）
使用现有库或他们自己实现SMTP电子邮件客户端，因此黑名单过滤对其无效



僵尸网络发布垃圾信息。垃圾邮件程序通过代理发送邮件（上半部分）和直接（下半部分）与服务器通信。

SMTP方言



直接和间接的电子邮件传递

```
S: 220 smtp.server.com
C: EHLO my.example.com
S: 250 smtp.server.com
C: MAIL FROM:<sender@example.com>
S: 250 2.1.0 Ok
C: RCPT TO:<recipient@server.com>
S: 250 2.1.5 Ok
C: DATA
S: 354
C: Test message.
C: .
S: 250 2.0.0 Ok
C: QUIT
S: 221 2.0.0 Bye
```

双方都必须遵守规则才能理解SMTP会话，但是小的语法差异通常不会对会话的结果产生很大的影响。

SMTP命令的各种等效形式导致区分不同的SMTP实现及其源的可能性。

SMTP方言扩展

三种操作模式

※ 方法0（M0），解析对话直到DATA命令，就像B@ BEL;
※ 方法1（M1），在没有SMTP扩展的情况下.解析整个会话;
※ 方法2（M2），用SMTP扩展解析整个会话.

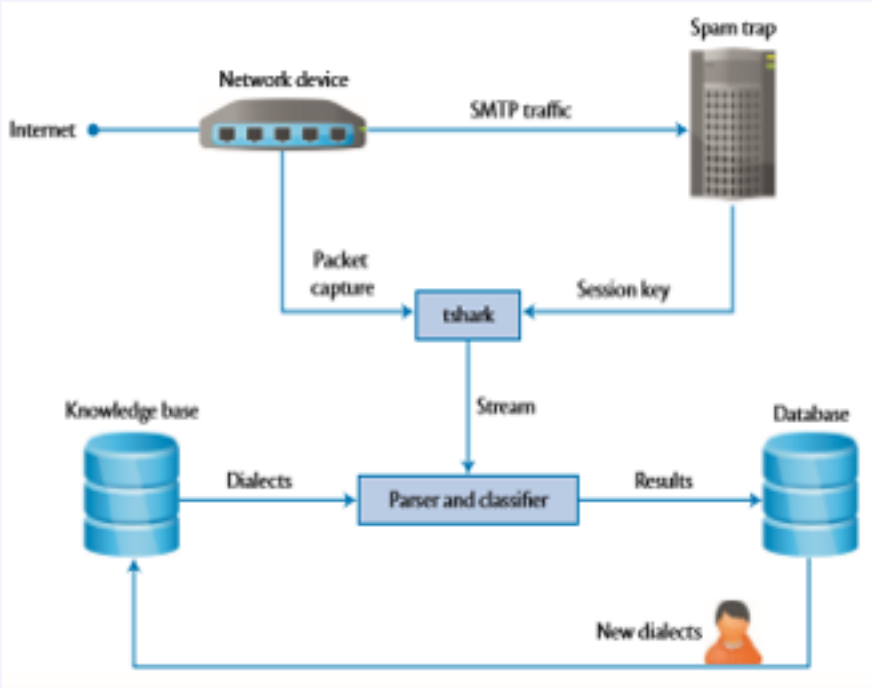
两个可用字段

※ 第一个用于分析的字段通知MTA关于MUA客户端类型和版本，如User-Agent和X-Mailer
※ IMF Received跟踪字段，告知MTA消息的真实路由

三类电子邮件发送者

良性、可疑、恶意

测试结果



测试环境的体系结构

操作模式	M0	M1	M2
已知良性	29	50	70
已知可疑	4	19	23
已知恶意	34	44	46
总计	67	113	139

结论：

1、分析越复杂，我们能够区分的方言就越多

2、在每个操作模式中，命令变体的数量显著地增加了已知方言的数量，表明僵尸网络的SMTP实现中有许多错误或不准确。

3、发现了一些未知的客户端命令，根据SMTP标准，这些命令是不正确的

测试结果

结果分类：未知、恶意、已知

分类	模式		
	M0	M1	M2
真阳性（%）	59.4	61.5	61.6
假阴性（%）	40.6	38.5	38.4
	IMF扩展的M0	IMF扩展的M1	IMF扩展的M2
真阳性（%）	78.9	80.1	95.0
假阴性（%）	21.1	19.9	5.0

类型	未知M0	未知M1	未知M2
样本数	95	506	505
总比例（%）	0.5	2.6	2.6
IMF不一致性	87	88	87
告警率（%）	91.6	17.4	17.2
类型	恶意M0	恶意M1	恶意M2
样本数	11459	11465	11474
总比例（%）	58.9	58.9	59.0
IMF不一致性	6711	6715	6716
告警率（%）	58.6	58.6	58.5
类型	已知M0	已知M1	已知M2
样本数	7899	7482	7474
总比例（%）	40.6	38.5	38.4
IMF不一致性	3792	3608	6507
告警率（%）	48.0	48.2	87.1

相关案例

※ 恶意方言用HELO域打招呼，
良性方言与EHLO [IP]打招呼。
※ 恶意方言在MAIL FROM和
RCPT TO命令的“:”和“<”
之间插入空格字符。
※ 良性方言使用QUIT命令。

行终止符是<LF>，
而不是<CR><LF>

负责垃圾邮件传播的恶意客户端
使用解析为QUIT space<CR>
<LF>的命令完成会话，该命令
在命令和行终止符中插入了空格

将我们的方法与其他基于对消息内容分析的方法联系起来，这将提供有效的垃圾邮件检测方法的共生。

北京大学

第五部分

PROFORMA : Proactive Forensics with Message Analytics

PROFORMA：利用消息分析主动取证

主动取证利用数字取证的调查原理，来开发预防网络犯罪的自动化技术。这种以预防为目的的方法之一是PROFORMA，它是一个原型系统，不断评估社会通信的可信度和风险。

PROFORMA

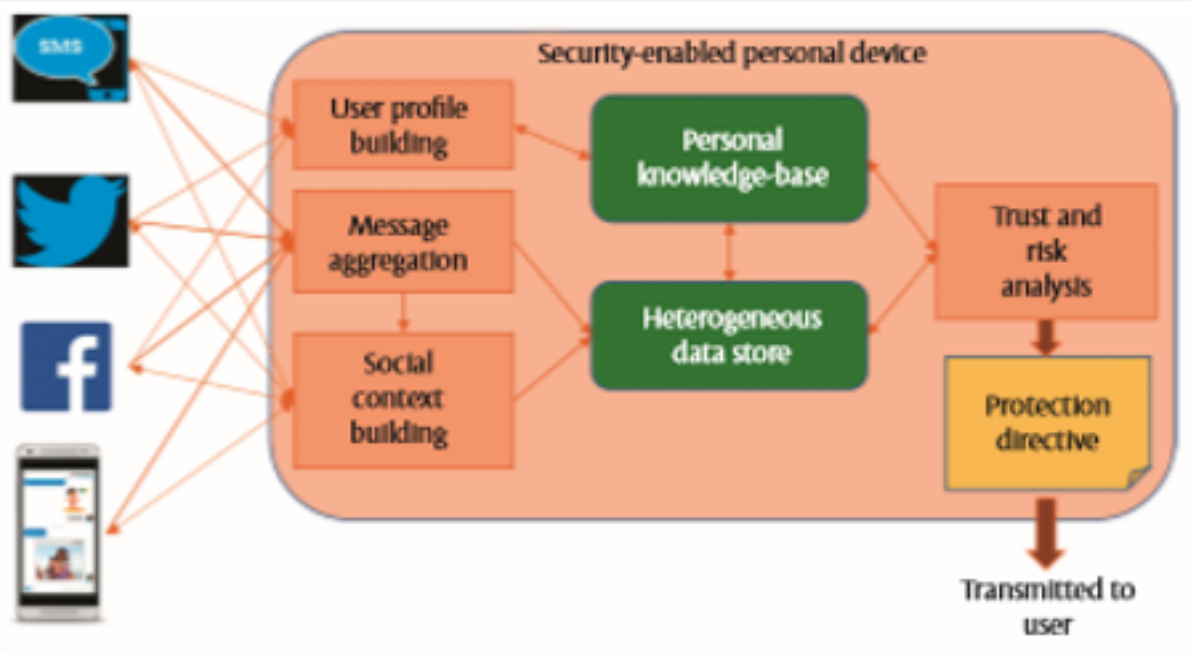
1. **主动取证：**利用数字取证的相同调查原则，发展自动化技术，在犯罪实际发生之前预防犯罪。

2. 主动取证可以应用于在线欺诈，利用了受害者和对手之间的长期通信，受害者通过逐步向对手透露敏感信息，直接参与犯罪的执行。主动取证的目的是通过向可能的受害者发出预警，将人类交流的这些显著特征应用于预防犯罪。

3. **可行性分析**

- 正确访问社交媒体公司的公共API，可以获得用户活动痕迹
- 信息集成技术成熟，能有效集成和关联，在单个系统中使用多模型数据
- 决策技术也已非常成熟。

PROFORMA



主动取证系统PROFROMA的高级体系结构

社交环境构建器：
试图在所有媒体通道上重建用户社交网络的可见部分（基于权限设置），并将此信息存储在个人知识库中

信息整合器：
扫描来自不同源的消息，并将它们放置在异构数据存储中，以便进行下游的分析操作

信任和风险分析模块：
风险分析涉及为每个消息计算信任分数。更重要的是，它监视用户的书面答复，并根据用户的消息的内容、对接收器的信任以及信任和风险的历史来评估风险。

为了实用，将允许用户创建"安全列表"以及风险阈值。

PROFORMA

建立用户轮廓

用户轮廓是关于被保护的人的数据记录。

这些事实是使用系统可访问的社交网络的相应API收集的，并存储在安全的个人知识库中。

这些收集到的事实作为知识实例存储在资源描述框架/Web本体语言（RDF/OWL）中，该资源描述框架是用于表示语义信息的万维网标准。

```
livesAt(Joe, "123 Elm St, Modesto, CA 99999", [3/1/1995-10/14/2006]),
```

```
error <- livesAt(p:Person; a1:Address; T1:TimeInterval) ^ not(p:TravelingPerson) ^livesAt(p:Person; a2:Address; T2:TimeInterval) ^ not(equal(a1; a2)) ^ overlaps(T1; T2),
```

```
livesAt(Joe, "456 Palm St, Modesto, CA 99969", [8/10/2005-9/19/2014])
```

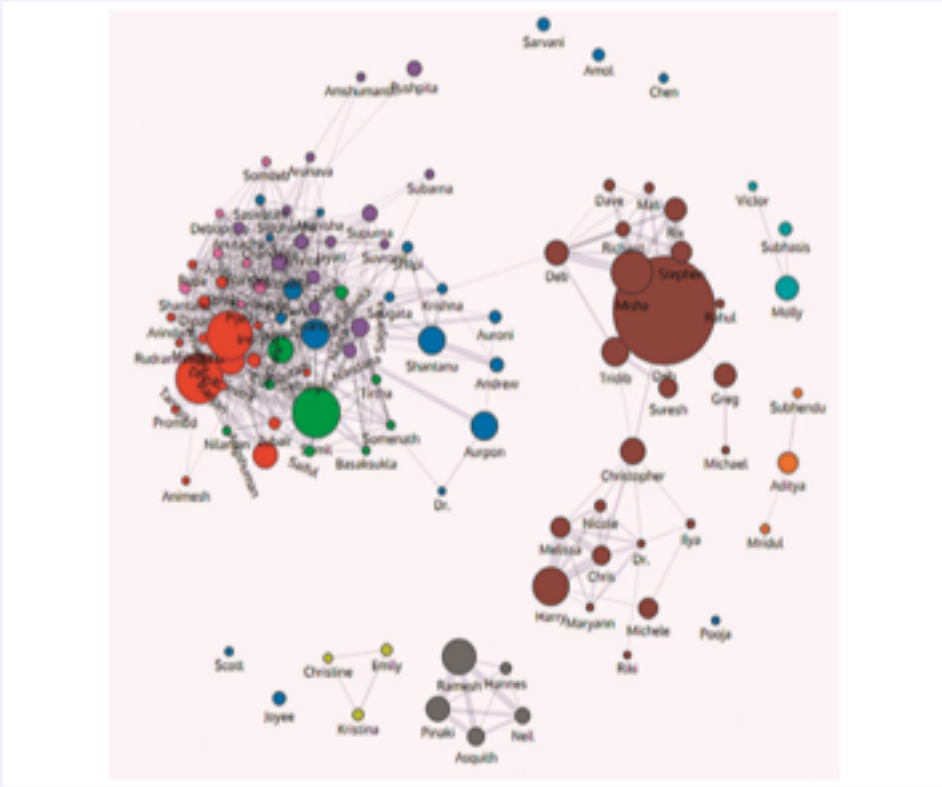
PROFORMA

构建社交环境

用户在Facebook（或其他社交频道）上的朋友和粉丝构建的自我网络构成了**社交环境**。

用户的社交图是在第一次注册系统时构建的。将社交环境图存储在异构数据存储中，接下来，通过估计每个人和组织节点的初始信任值来丰富“裸”网络。。

※ 用户与节点之间的通信程度
※ 链路强度
※ 消息交换的质量



PROFORMA

消息整合过程

整合存储

消息整合器将来自不同源的单个消息格式转换为公共的内部形式，并将其存储在具有强文本内容的专门用于半结构化数据的组件存储中。

处理

通过分析工作流处理消息。

计算信任值

当识别出这些结构时，聚合器从当前用户和消息发送者之间交换的先前消息的缓存中计算当前消息的信任值，如果需要，计算存储在系统中的先前会话的信任值。

$$A=\frac{1}{n}\times\sum_{x=1}^{n}I_x, \quad (1)$$

$$T_x=\frac{I_x}{(A+\frac{1}{n}\times\sum_{x=1}^{n}|A-I_x|)}, \quad (2)$$

I_x表示用户与另一个成员x的交互次数
A是n个这样的成员之间的平均交互次数

当信任T_x的计算显示出交互量突然超过平均A时，信任值会降低，因为它表明成员x部分存在交互异常。

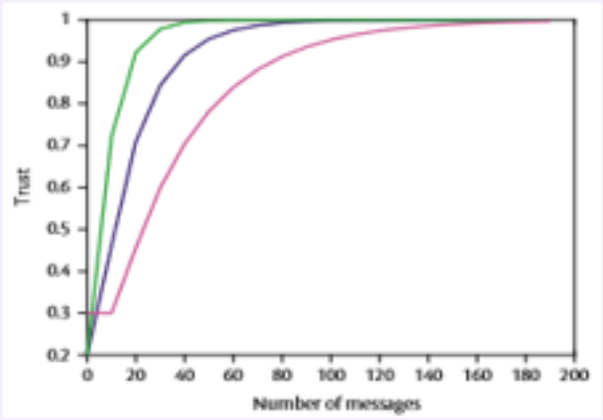
PROFORMA

渐进性分析

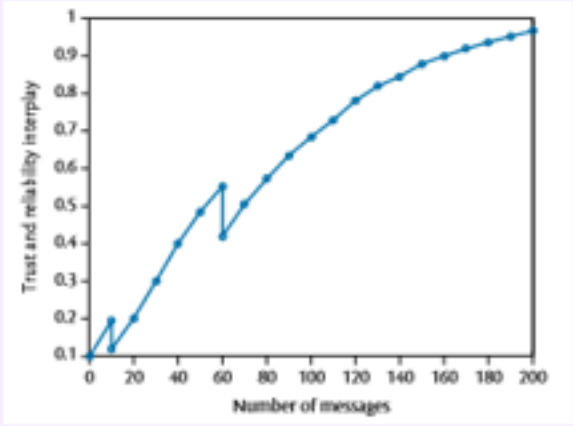
信任函数 $\mathbf{T} = max\left(\mathbf{I}, (\mathbf{1} - \alpha^{n})\right)$

T表示当前信任值，n表示消息的数量，α表示学习率

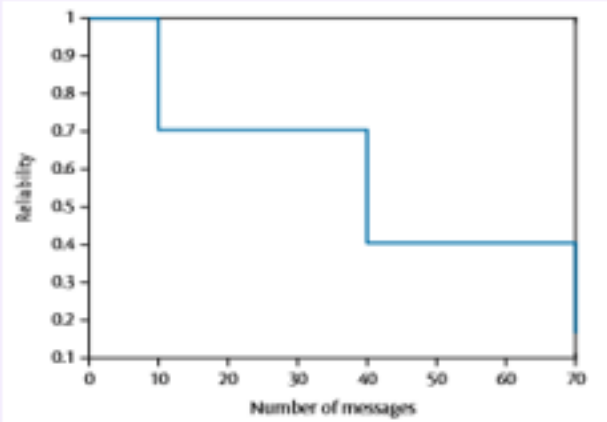
隐私问题?



对于不同的学习率α，具有相同初始信任值的两个人的信任度上升趋势可能不同



可靠性和信任之间的相互作用



随着潜在对手信息中不同敏感术语的出现，可靠性逐渐降低，相关风险增加

北京大学
PEKING UNIVERSITY

敬请老师同学批评指正