第 41 卷　第 5 期　2017 年 3 月 10 日
DOI：10.7500/AEPS20160709004
电力系统自动化
Automation of Electric Power Systems
Vol.41 No.5 Mar.10，2017

基于云安全的高级计量体系恶意软件检测方法

苏　盛[1]，李志强[1]，谷　科[1]，石东源[2]，钱　斌[3]
（1. 智能电网运行与控制湖南省重点实验室（长沙理工大学），湖南省长沙市 410004；
2. 强电磁工程与新技术国家重点实验室（华中科技大学），湖北省武汉市 430074；
3. 南方电网科学研究院，广东省广州市 510080）

摘要：高级计量体系（AMI）中，智能电表主要依赖嵌入式硬件加密（ESAM）提供保护，遭破解后可能遭恶意软件攻击威胁。针对智能电表通信和计算资源有限的特征，提出了基于白名单的云安全防护方法。首先利用运行环境封闭固定的特点，在计量中心云端安全服务器中建立并维护合法进程白名单；然后在智能电表中安装运行进程检测模块，由其枚举出所有运行进程，计算唯一标识各进程的哈希值特征码并提交到云端安全服务器，与白名单进行对比即可检出含非法进程的表计。该模式仅需在智能电表中计算并上传进程特征码，可在有限的计算和通信资源约束下满足恶意软件检测需求，能够强化 AMI 的网络安全防护水平。

关键词：高级计量体系；云安全；哈希值；白名单；智能电表

0　引言

高级计量体系（AMI）是实现电网与电力用户网络互动，优化资源配置的基础[1-2]。为实现数据实时双向可靠传送，AMI 还必须采用开放的系统和共享的信息模式，在异构通信环境下传输电价及控制指令等敏感信息，存在突出的信息安全风险[3-4]。

针对智能电表、数据集中器和负荷控制终端（下文统称智能电表）的网络攻击，不仅可获取用户隐私信息、篡改用电数据，造成电量损失，还可大面积发送错误信息，造成大量用户停电[3-5]。2009 年，美国黑帽大会上就曾演示验证蠕虫病毒可在 1 d 内感染 1.5 万户智能电表并造成大面积停电。与调度及变电站自动化系统相比，AMI 的网络安全防护具有以下鲜明特点。

1）智能电表点多面广，难以构建专用通信网，多采用载波、通用分组无线业务（GPRS）等方式无线通信，通信带宽和媒介具有显著异构性。

2）智能电表通信传输的是直接涉及经济利益和隐私的敏感信息，易遭利益相关方攻击。

3）智能电表一般基于嵌入式系统开发，需集成计量、显示、通信及自身状态监测等反窃电功能[6]，可用计算资源有限。限于成本，难以采用要求较高的安全防护措施。

为满足集成新型应用的需要（如双向计费等）[7]，智能电表已开始采用 ARM 等 32 位嵌入式处理器，并使用 μCLinux 等嵌入式操作系统以方便多进程管理[8-9]，操作系统存在的故障将放大遭网络攻击的风险。

国内智能电表的第一道安全防线是表盖出厂封印和编程开关封印。此外，还采用硬件加密安全模块进行身份认证和加密通信，应用内置 SM1 对称密钥算法以 128 bit 分组长度和密钥长度对称加密，可用于通信身份认证和传输加密[10-11]。因智能电表网络安全取决于密钥的安全性，研究人员根据其计算和通信资源有限的特点，提出了资源开销小的轻量级密钥协商协议[12]和改进的密钥分发管理模式[13-14]。

需要指出的是，一旦破解加密算法，智能电表将直面网络攻击的威胁。2014 年，研究人员在欧洲黑帽大会上破解了西班牙电网公司智能电表采用的 AES-128 bit 对称加密算法，侵入表计后注入并执行恶意代码，不但可篡改电表标识码、调整电量读数实现窃电，还可以此为跳板攻击相邻电表，甚至可能控制切断用户供电。

AMI 的入侵检测系统可检测网络流量、节点响应时延等指标诊断智能电表是否遭到攻击[15]。通过逆向工程熟悉被攻击智能电表的入侵者在突破密钥防护后，可注入恶意代码进行精确攻击。入侵检

收稿日期：2016-07-09；修回日期：2016-11-11。
上网日期：2017-01-05。
湖南省教育厅科研基金资助项目（15A005）。

测在流量和响应时间无明显变化条件下也无从识别入侵行为。因智能电表计算和通信资源极为有限，当前对于如何检测侵入其中的恶意软件，缺乏有效手段。本文提出基于云安全的智能电表恶意软件检测方法，将对计算资源有高要求的恶意软件检测等工作转移到云端服务器完成，可在智能电表有限的计算和通信资源条件下完成恶意软件检测。

1　基于云安全的恶意软件检测

21 世纪以来，通过网络汇聚的计算、存储、数据和应用资源随网络规模扩大而不断增加，使得网络从传统意义的通信平台转化为泛在计算平台。云计算整合分布在网络上的大量数据、存储和计算资源，协同形成一体化工作环境，可以按需提供服务，使用户便捷共享和利用开放网络上的资源[16]。因云计算可通过规模经济和资源共享降低成本，削减为满足短暂尖峰需求而购置和维护大量资源所需付出的代价，近年来得到了快速发展，在电力行业也有探索应用[17]。云安全可视为云计算理念在网络安全领域的应用。

传统恶意软件查杀机制主要通过目标文件特征码鉴定方式查杀木马和病毒，需下载恶意软件特征代码库，然后将目标文件特征码和特征库内病毒特征逐条比对，若能匹配上则判定为病毒文件，病毒检测准确程度取决于特征库是否完整全面[18-19]。新型病毒需要在部分用户中毒并反馈后，才能给出病毒特征码，再由用户下载升级病毒库后完成本地查杀防护。

随着互联网技术的深入发展，各类新型病毒不断涌现，病毒特征库容量随病毒数量增长而日渐膨胀，占用内存和系统资源越来越多。在基于云安全病毒查杀技术出现前，主流安全软件需下载近百兆、记录上百万病毒特征码的病毒特征库文件。病毒数量的爆炸式增长使得传统杀毒软件扫描效率不断下降，系统性能受到极大影响[20]。

为克服传统杀毒技术的瓶颈，360 等国内安全厂商结合云计算技术，率先提出了云安全的概念[21]。云安全是 P2P、网格、云计算等分布式计算技术混合发展和演化融合的结果。在基于云安全的病毒查杀机制下，用户计算机的病毒查杀不再单独依赖本地病毒特征库，而是通过互联网连接用户和安全厂商服务器集群，可依赖庞大的网络服务，实时采集、分析和处理恶意软件信息，从而将参与其中的所有计算机及服务中心形成捕捉与分析恶意软件的整体，并将病毒查杀作为服务提供给互联网用户[18-19]。基于云安全的恶意软件检测系统结构组成如图 1 所示。

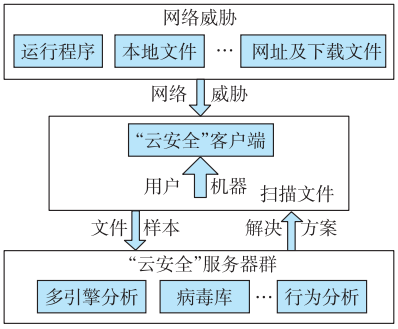

图 1　云安全系统结构组成
Fig.1　Composition of cloud security system

在云安全病毒检测体系下，用户计算机采用轻客户端策略，将可疑文件的分析和病毒特征库对比等工作转移至云端服务器。客户端软件发现可疑文件时，将可疑文件的信息推送到云端服务器，按文件哈希值比对、文件样本启发式分析和基于规则的行为监测分析等三种模式进行分析和判断处理[20]。

1）发现可疑文件时，上传该文件哈希值至云端服务器，服务器端将该文件哈希值与黑名单进行比对，发现在黑名单之列时生成解决方案发送至客户端。

2）文件哈希值分析未发现异常时，客户端提取文件样本，由云端服务器端对该文件样本进行启发式分析检测，发现异常则生成解决方案推送至客户端。

3）若文件样本分析未发现异常，客户端搜集该文件运行过程中的行为特征上传至云端服务器，云端服务器通过行为特征的模式最终判定该文件是否可信，并向客户端发送解决方案。

云安全病毒检测体系不但能显著降低安全软件的资源占用，还可将海量客户端计算机转化为恶意软件监测站点，及时监测网络中的异常行为，截获各种恶意程序的最新状况，并将这些信息推送到服务器端进行分析、处理，然后把相关解决方案分发到客户端进行防护，显著加快应对新兴病毒软件的反应速度，缩短恶意软件生命周期，有效应对网络威胁泛滥的严峻局势[18-20]。

2　基于云安全的 AMI 恶意软件检测

前述以非法程序黑名单为特征的计算机系统云安全方案能有效降低对客户端计算能力的要求，对于提高智能电表安全防护能力具有借鉴价值。然而，因 AMI 应用环境与普通计算机系统存在显著的差异，应用该方法进行 AMI 的恶意软件检测并不可行，其原因主要有以下两点。

1)普通计算机系统与嵌入式系统应用环境存在突出差异，很难用攻击普通计算机系统的恶意软件来攻击基于嵌入式系统的智能电表，网络安全公司针对普通计算机系统制定的恶意软件黑名单无助于AMI的恶意软件检测。

2)基于黑名单的云安全防护是一种被动安全防御手段，它必须在恶意软件攻击造成破坏、客户端上报异常并检测确定恶意软件特征代码后，才可对比检测恶意软件。基于嵌入式系统开发的智能电表、数据集中器和用电负荷管理终端计算资源有限，尽管足以承担进程扫描、计算和上传进程哈希值特征码的计算工作，但难以具备检测和分析自身运行异常的能力，在客户端未上报异常条件下，无法形成智能电表的恶意软件黑名单，也就无从施行基于黑名单的AMI恶意软件云端检测。

与黑名单相比，白名单采用的是基于授权许可运行的机制，仅允许获得授权的合法进程运行，而将未获授权的进程视为非法入侵进程。因AMI运行环境封闭而固定，往往就是嵌入式操作系统本身和厂家初始安装的几个业务进程。利用智能电表为封闭的专用系统且同一批号设备运行进程相同的特点，在每一批号表计安装接入电网前，检测其中的运行进程，并将各进程的名称、大小、哈希值特征码及功能描述等相关信息作为合法进程信息记录于云端形成白名单。当云端安全服务器数据库中的合法进程信息发生变化时，能起到维护和更新白名单的作用。

AMI中，只需在计量中心架设云端安全服务器，然后由智能电表定期将枚举进程的哈希值特征码和电量、电费等信息一并上传到计量中心，即可实现基于云安全的智能电表病毒检测[22]。

1)该机制将消耗大量计算资源的进程合法性判断转移到云端完成，显著降低对客户端计算性能的要求。

2)带操作系统的智能电表可定期枚举运行进程，利用散列函数计算各进程哈希值特征码后上传到计量中心云安全服务器。实现简单，能满足有限计算资源约束。

3)只要在智能电表侧计算出进程哈希值特征码上传至云端比对即可完成非法进程检测，智能电表寿命周期内恶意软件的升级换代对检测准确度没有影响。

4)采用白名单不存在技术上的障碍，并可有效规避因智能电表难以支持本地异常行为分析导致无法形成黑名单的技术瓶颈。

AMI中基于云安全的智能电表恶意软件检测流程如图2所示。

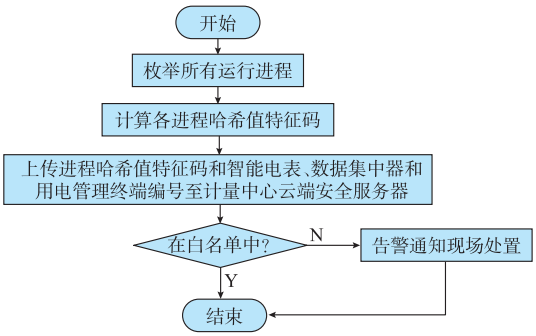

图2　基于云安全的智能电表病毒检测流程
Fig.2　Flow chart of malware detection of smart meters with cloud security

1)智能电表定期枚举所有运行进程，计算各进程的哈希值特征码后提交到计量中心云端安全服务器。

2)云端安全服务器的恶意软件检测系统将各进程哈希值特征码与白名单逐条对比，发现特征码存在于白名单时，不作处理。

3)若进程不在白名单之列，云端安全服务器要求相关表计上报对应进程模块，进行该进程的功能性和安全性检测。如通过安全性检测则将其列入白名单；否则告警并安排工作人员现场查勘处理。

当前，企业用户的三相电能表、数据集中器和负荷控制终端功能复杂，已有相当数量采用ARM芯片，并利用μCLinux等操作系统进行内存管理。该部分智能电表在技术上已具备条件，可利用云安全技术实现基于白名单的恶意软件检测，从而构建云安全平台的雏形。在基于云安全的AMI恶意软件检测中，需要注意的问题有以下几点。

1)白名单存储于计量中心云端安全服务器，是AMI恶意软件检测机制的核心。因计量中心为AMI系统关键中枢，不存在计算与通信资源的约束，并部署有完善的网络安全防护措施，入侵者需攻破所有安全壁垒方可伪造白名单，而此时其获取的权限已足以直接遥控智能电表拉闸停电，进行任意破坏。因此，在AMI的智能电表云安全防护中不考虑白名单的安全问题。

2)若智能电表无法上传不在白名单之列的进程模块，也可考虑由人工现场处置，通过功能性和安全性检测后更新云端的白名单。

3)因智能电表计算能力有限，当云端安全中心检测到电表中存在非法进程时，需警告工作人员现场处置，而难以像普通计算机系统一样下发解决方案，由客户端自行杀毒。

基于云安全的智能电表安全防护与现有技术对

比如表 1 所示。若入侵检测系统未能检测到破解密钥侵入智能电表的恶意软件，恶意软件即可能潜伏其中，进行窃电或偷取个人隐私；此外，还可在无阻碍条件下大面积传播后再行破坏，扩大危害。引入基于白名单的云安全防护机制后，可显著缩短智能电表恶意软件的生命周期，从而限制、缩小恶意软件破坏效果。在此，智能电表上传进程哈希值特征码的周期决定了恶意软件在电表中的生存周期。因智能电表数量庞大且通信带宽有限，需要结合恶意软件扩散传播的一般规律，合理确定智能电表上报进程哈希值的周期间隔。

表 1　AMI 安全防护技术对比

Table 1　Real & fabricated lines according to their criticality

技术方案	防护效果分析
密钥防护	针对传输加密和身份认证，保护隐私和敏感信息。受资源约束难以采用高强度密钥，遭破解后智能电表将直面攻击
入侵检测	检测网络通信流量、节点响应时间等指标，再利用模式识别等算法诊断是否存在入侵行为。对于不造成明显异常的针对性精确攻击易失效
基于白名单的云安全	建立授权许可白名单；表计侧枚举计算进程哈希值特征码后，交由云端诊断安全性

3　工程实现说明

智能电表主要使用 μCLinux，μC/OS 等嵌入式操作系统，以下结合 μCLinux 说明在智能电表上枚举进程任务并计算相应哈希值特征码的具体实现方法。

μCLinux 系统从 Linux 2.0/2.4 内核派生而来，可以使用几乎所有 Linux API 函数。它针对嵌入式微控制领域进行定制裁剪和优化，形成高度优化、代码紧凑的嵌入式操作系统，具有体积小、稳定、良好的移植性、优秀的网络功能，以及对各种文件系统广泛支持等优点。该系统常用于具有很少内存或 Flash 的嵌入式系统，已成功应用于路由器、机顶盒、PDA 等领域[23]。

为减少系统复杂程度、降低硬件开发成本和运行功耗，嵌入式系统在硬件设计上取消了内存管理单元模块。可执行文件启动时系统不能自动为进程分配内存空间，需要开发者自行管理所需物理内存及存储方式。为适应无内存管理单元的特殊运行环境，μCLinux 系统采用了 flat 可执行文件格式，其结构如图 3 所示。

Linux 系统中，进程一般由代码段、存放已初始化全局变量的数据段、存放未初始化的全局变量和静态变量的 BSS 段和存放自动变量、局部变量的堆栈段构成。进程启动载入内存时，由内存管理单元分配虚拟地址空间。因嵌入式系统没有内存管理单元管理虚拟内存，μCLinux 采用实存储器管理策略，通过地址总线直接访问物理内存。所有进程访问的地址都是实际物理地址，并在同一运行空间运行。因缺乏系统内存管理单元，μCLinux 中加载的应用程序都是静态编译连接的，而不能使用动态库。连接器只给相对应段基地址的偏移量，将偏移量放到统一的 reloc 段中，实际加载该程序时，将实际段基地址和偏移量相加即可获取实际物理地址[23]。

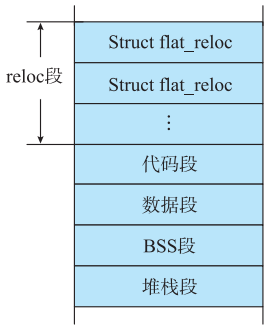

图 3　flat 可执行文件格式

Fig.3　Format of executable file

μCLinux 系统中，安全模块可扫描得到所有进程的进程名和进程号等信息，然后逐个获得各进程占用内存大小等详细信息，根据 reloc 偏移量即可找到该进程代码段对应内存区间；读取该段内存后，可利用 MD5 等算法计算哈希值特征码，上传到云端安全服务器中比对白名单判断合法性。

哈希值是由哈希算法将任意长度的二进制值散列映射得到的较短的固定长度二进制值，可唯一表征输入的二进制值[20]。任何对原文件的改动都会改变哈希值，且无法改动文件而不改变哈希值。为检验哈希计算的计算性能要求，在 1.8 GHz 主频、1 GB 内存、Intel Atom N450 单核 CPU 上网本计算机上，安装 cygwin 和 μCLinux 仿真环境，应用 MD5 算法对 10 kB 文件进行哈希值计算。测试表明，因哈希算法主要涉及位运算，计算简单高效，平均单次哈希值特征码计算所耗时间约为 497 μs，对计算资源要求不高，在基于 ARM 等芯片的智能电表上也可实现。

4　结语

针对 AMI 中智能电表的通信和计算资源有限，且难以按照传统方法检测恶意软件的问题，提出了基于白名单的云安全防护方法。采用白名单的形式在计量中心云端安全服务器中建立并维护合法进程列表；然后在智能电表中安装运行进程检测模块，由其枚举出所有运行进程，计算唯一标识各进程的哈

希值特征码并提交到云端安全服务器，与白名单进行对比即可检出含非法进程的表计。所述方法可在有限的计算和通信资源约束下满足恶意软件检测需求，缩短侵入智能电表的恶意软件生存周期，避免造成重大危害，有助于强化 AMI 中智能电表的安全防护。

参 考 文 献

[1] 蒋玮，汪梁，王晓东，等.面向用电双向互动服务的信息通信模型[J].电力系统自动化，2015，39(17)：75-81. DOI：10.7500/AEPS20150326002.
JIANG Wei，WANG Liang，WANG Xiaodong，et al. An information communication model for two-way interactive service of power utilization[J]. Automation of Electric Power Systems，2015，39(17)：75-81. DOI：10.7500/AEPS20150326002.

[2] 赵鸿图，周京阳，于尔铿.支撑高效需求响应的高级量测体系[J].电网技术，2010，34(9)：13-20.
ZHAO Hongtu，ZHOU Jingyang，YU Erkeng. Advanced metering infrastructure supporting effective demand response [J]. Power System Technology，2010，34(9)：13-20.

[3] 路保辉，马永红.智能电网 AMI 通信系统及其数据安全策略研究[J].电网技术，2013，37(8)：2244-2249.
LU Baohui，MA Yonghong. Research on communication system of advanced metering infrastructure for smart grid and its data security measures[J]. Power System Technology，2013，37(8)：2244-2249.

[4] 刘念，张建华.互动用电方式下的信息安全风险与安全需求分析[J].电力系统自动化，2011，35(2)：122-131.
LIU Nian，ZHANG Jianhua. Cyber security risks and requirements for customer interaction of smart grid [J]. Automation of Electric Power Systems，2011，35(2)：122-131.

[5] 丁冠军，樊邦奎，兰海滨，等.智能电网信息安全威胁及防御策略研究[J].电力信息与通信技术，2014，12(5)：58-63.
DING Guanjun，FAN Bangkui，LAN Haibin，et al. Research on information security threats and defense strategies for smart grid [J]. Electric Power Information and Communication Technology，2014，12(5)：58-63.

[6] 孟珺遐，朱宁辉，白晓民，等.基于 DL/T 645—2007 协议的智能电表嵌入式通信软件研发[J].电网技术，2010，34(9)：7-12.
MENG Junxia，ZHU Ninghui，BAI Xiaomin，et al. Research and development of embedded communication software for smart meters based on DL/T 645—2007 protocol[J]. Power System Technology，2010，34(9)：7-12.

[7] 栾文鹏，余贻鑫，王兵.AMI 数据分析方法[J].中国电机工程学报，2015，35(1)：29-36.
LUAN Wenpeng，YU Yixin，WANG Bing. AMI data analytics [J]. Proceedings of the CSEE，2015，35(1)：29-36.

[8] 静恩波.基于嵌入式系统的智能电表设计与研究[J].低压电器，2011，53(3)：26-30.
JING Enbo. Design and research of smart meter based on ARM system[J]. Low Voltage Apparatus，2011，53(3)：26-30.

[9] 吕小强，张涛，白燕羽，等.基于 ARM 和 ATT7022B 的智能电表系统[J].中国测试，2012，38(1)：94-96.
LÜ Xiaoqiang，ZHANG Tao，BAI Yanyu，et al. Smart watt-hour meter based on ARM and ATT7022B [J]. China Measurement & Test，2012，38(1)：94-96.

[10] 张明远，徐人恒，张秋月，等.智能电能表数据通讯安全性分析[J].电测与仪表，2014，51(23)：24-27.
ZHANG Mingyuan，XU Renheng，ZHANG Qiuyue，et al. Data communication security analysis of the smart electric energy meter[J]. Electrical Measurement & Instrumentation，2014，51(23)：24-27.

[11] 国家电网公司企业标准.电力用户用电信息采集系统安全防护技术规范：Q/GDW 377—2012[S].2012.

[12] 赵兵，高欣，郜盼盼，等.适用于用电信息采集的轻量级认证密钥协商协议[J].电力系统自动化，2013，37(12)：81-86.
ZHAO Bing，GAO Xin，GAO Panpan，et al. A light weight authenticated protocol with key agreement for power utilization information collecting [J]. Automation of Electric Power Systems，2013，37(12)：81-86.

[13] 梁建权，金显吉，佟为明，等.高级量测体系中无线传感器网络的密钥管理方案[J].电力系统自动化，2016，40(19)：119-126. DOI：10.7500/AEPS20160313005.
LIANG Jianquan，JIN Xianji，DONG Weiming，et al. Key management scheme for wireless sensor networks in advanced metering infrastructure [J]. Automation of Electric Power Systems，2016，40(19)：119-126. DOI：10.7500/AEPS20160313005.

[14] LIU Nian，CHEN Jinshan，ZHU Lin，et al. A key management scheme for secure communications of advanced metering infrastructure in smart grid [J]. IEEE Trans on Industrial Electronics，2013，60(10)：4746-4756.

[15] RASCHE G. Intrusion detection system for advanced metering infrastructure[R]. 2012.

[16] DIKAIAKOS M D，KATSAROS D，MEHRA P，et al. Cloud computing：distributed internet computing[J]. IEEE Internet Computing，2009，13(5)：10-13.

[17] 郭晓利，于阳.基于云计算的家庭智能用电策略[J].电力系统自动化，2015，39(17)：114-119. DOI：10.7500/AEPS20150310017.
GUO Xiaoli，YU Yang. A residential smart power utilization strategy based on cloud computing[J]. Automation of Electric Power Systems，2015，39(17)：114-119. DOI：10.7500/AEPS20150310017.

[18] 李智勇，李蒙，周悦，等.大数据时代的云安全[M].北京：化学工业出版社，2016.

[19] 俞能海，郝卓，徐甲甲，等.云安全研究进展综述[J].电子学报，2013，41(2)：371-381.
YU Nenghai，HAO Zhuo，XU Jiajia，et al. Review of cloud computing security[J]. Acta Electronica Sinica，2013，41(2)：371-381.

[20] 徐迎迎，高飞，尚锋影，等.新的云安全解决方案及其关键技术[J].华中科技大学学报：自然科学版，2012(S1)：74-78.
XU Yingying，GAO Fei，SHANG Fengying，et al. New cloud security solutions and its key technologies [J]. Huazhong University of Science and Technology：Natural Science Edition，2012(S1)：74-78.

（下转第 152 页　continued on page 152）

(上接第 138 页　continued from page 138)

[21] 深圳市腾讯计算机系统有限公司.一种云安全系统中的未知文件安全信息确定方法和装置:中国,ZL201210194013.8[P].2012-06-13.
[22] 苏盛,陈凤,李志强,等.基于云安全的高级计量体系恶意软件检测方法:中国,ZL2016105977017[P].2016-07-27.
[23] 任哲,潘树林,房红征.嵌入式操作系统基础 μC/OS-Ⅱ和 μCLinux[J].北京:北京航空航天大学出版社,2006.

苏　盛(1975—),男,通信作者,博士,副教授,主要研究方向:电力系统大停电风险分析。E-mail:346078890@qq.com

李志强(1991—),男,硕士研究生,主要研究方向:电力系统信息安全防护。E-mail:492054753@qq.com

谷　科(1980—),男,博士,副教授,主要研究方向:网络与信息安全。E-mail:282399837@qq.com

(编辑　章黎)

Cloud Security Based Malware Detection in Advanced Metering Infrastructure

SU Sheng[1], *LI Zhiqiang*[1], *GU Ke*[1], *SHI Dongyuan*[2], *QIAN Bin*[3]

(1. Hunan Province Key Laboratory of Smart Grids Operation and Control (Changsha University of Science and Technology), Changsha 410004, China;
2. State Key Laboratory of Advanced Electromagnetic Engineering and Technology (Huazhong University of Science and Technology), Wuhan 430074, China;
3. Electric Power Research Institute of China Southern Power Grid, Guangzhou 510080, China)

Abstract: Smart meters in advanced metering infrastructure (AMI) are protected by encryption/decryption of embedded secure access module (ESAM) and may undergo intrusion of malware once the key is compromised. Since smart meters have limited computation and communication resources, a cloud security based approach is proposed to detect malware in smart meters. A software module is installed to enumerate all processes in smart meters. Thereafter, Hash code of all processes is calculated and uploaded to the server over cloud and the malware detection module in the server can identify malware just by comparing Hash code with that in blacklist and whitelist. Since the jobs with a high requirement on computation are implemented in server over cloud, its requirement on meters is notably lower than on the traditional approach.

This work is supported by the Education Department of Hunan Province (No. 15A005).

Key words: advanced metering infrastructure; cloud security; Hash code; whitelist; smart meters