解决方案简介

英特尔® 可编程解决方案事业部
智能建筑安全性

为建筑自动化系统构建面向未来的安全性

Veridify 的 DOME 平台利用英特尔的高级可编程解决方案，通过节省成本的零接触生命周期证书管理，为全新和现有建筑自动化系统提供设备级网络安全保护。

该解决方案简介描述了如何使用 Veridify 和英特尔的创新技术化解建筑安全挑战。

如果您负责以下领域…

- **业务战略：**您将进一步了解建筑自动化控制及其托管“智能”设备面临的安全威胁、运营中断可能性以及代价高昂的网络攻击。
- **技术决策：**您将了解每个设备（无论大小如何及运行什么操作系统）如何获得生命周期管理，以及创建安全可信环境所需的安全性。

作者

Mark Jervis
英特尔® 公司可编程解决方案事业部
Marlow，英国
mark.jervis@intel.com

Louis Parks
Veridify Security Inc.
美国康涅狄格州谢尔顿
lparks@veridify.com

要点综述

如今，互联建筑越来越容易遭受网络攻击，这会威胁到住户的安全，并可能造成财务和声誉损失。这种风险源自于建筑日益使用安全性较差的互连系统，包括 HVAC、照明、门禁、环境传感器和电梯等。更糟的是，控制器和设备由许多不同的厂商供应，计算性能无法满足 PC 和智能手机对可信安全方法的需求。对于黑客来说，未获得安全保护的最简单互联设备也是一种开放后门，可能造成灾难性后果。

Veridify 的 DOME 是一种安全解决方案，旨在通过 BACnet 等现有网络协议保护建筑的管理系统（包括边缘）。该系统提供零接触部署功能，以减少手动配置造成的时间浪费和错误；提供区块链谱系（pedigree），以确保只有授权的控制器才能发出命令；并提供低成本的“嵌入式”工具，以利用英特尔的高级可编程解决方案增强现有系统的安全性。DOME 平台支持设备级安全性，可提供现场配置、固件更新和设备所有权管理等功能，具有简单、经济高效和快速的优势。DOME 平台具有加密敏捷性，支持传统和量子抵抗安全性，并通过建筑所需的长生命周期保护确保所有者/管理者的投资安全。

业务挑战

数字化转型

数字技术正在重塑建筑物。通过将运营技术（OT）中的传感器和制动器与信息技术（IT）中的监控、控制和分析功能进行网络连接，可以实现日益自动化的远程管理，从而提升建筑的响应速度、可靠性、效率和舒适度。现在安装的新智能建筑系统组件必须与系统中的许多其他设备进行交互，并且满足未来需求，适应设备长生命周期内的变化。在保护现有资产方面，建筑所有者和管理者还面临着一个问题：如何以合理价格替换尚可使用几年的建筑系统，以及降低租户流失和租金萎缩方面的成本损失？

解决方案优势

1. **提高安全性** — 强大工具甚至可支持网络边缘的最小设备。
2. **减少部署成本和时间** — 易于实施的软件工具可保护连接到物联网（IoT）网关的现有系统和新的低资源设备。
3. **轻松扩展** — 提供零接触部署功能、生命周期区块链谱系，并支持现场配置和固件更新，及基于设备的所有权管理，无需实施全面的云连接。

网络安全威胁

潜在黑客不断寻找和利用薄弱环节，而智能建筑中的互联物联网提供了访问建筑信息和关键建筑运营技术的多个入口点。相关信息可用于控制物理系统，例如门禁、电梯、照明或电源，以及访问或控制监控系统或互联 IT 方面的数据。例如，黑客通过闭路电视（CCTV）摄像机侵入一家银行，网络罪犯通过鱼缸温度传感器侵入一家赌场，许多酒店和医院的基础设施被勒索软件所破坏，智能建筑物联网设备感染病毒，并被用于发起迄今最大规模的分布式拒绝服务（DDoS）攻击。

对于建筑物所有者而言，增加安全性的价值在于避免安全漏洞未来造成潜在的成本损失与危害。

立法

面对愈演愈烈的物联网（IoT）安全威胁，世界各地的政府都在加快立法步伐，以实施基本的物联网设备安全标准。

美国和英国政府最近发布了新立法提案。英国政府发布了网络安全立法提案，该提案的最近更新时间为 2020 年 10 月；美国国会也发布立法提案（S.734，H.R.1668），拟对出售给政府机构的物联网设备设立新的安全标准。在网络安全立法和指导方面，其他国家和地区也在行动，包括：

- 加利福尼亚物联网法案，该法案要求互联网设备制造商在设备上安装合理的安全功能；
- 欧盟网络安全基准要求（欧盟标准（EN）303 645 v2.1.1）；
- 日本电信商业法，该法要求遵守物联网设备安全标准；
- NIST 草案报告 “物联网设备制造商建议：基础活动和核心设备网络安全功能基准”（2020 年 1 月）；和
- 其他网络安全标准，例如 ISO 27001、NIST 800-53、IEC 62443

保险业很可能在计算建筑的保险费时考虑未来的安全认证，并对满足特定安全级别的建筑收取较低的保险费。

对建筑安全的影响

不断深化的立法举措和日益加剧的威胁形势意味着业界需提高安全意识，视情况更新和调整建筑网络安全措施，确保建筑在整个生命周期内的安全性。网络防御也需深化，纳入从防火墙和数据加密到单个物联网设备安全性的多层防护。

在网络安全方面，几个实际问题急需解决。众多互联物联网组件的安全部署本身可能耗费高昂成本 — 有时可达到设备本身成本的两倍。如果进行改造，标准的网络安全算法（例如基于椭圆曲线的算法）甚至可能无法使用，因为许多端点设备可能只包含很小的微处理器。此外，许多设备甚至都没有用户界面。

全面的安全解决方案还需要考虑到，最薄弱和最易遭受攻击的环节甚至可能存在于供应链中，更别提组件安装了。安全保护需要贯穿系统设备的生命周期 — 从制造和供应，到部署和配置，直至退役。

解决方案价值

DOME 是面向物联网的零接触部署安全解决方案。

DOME 提供现场所有权管理，包括实体之间基于区块链谱系的安全 “所有权转移”，让您安心无忧，确信所有权能够从原始制造商安全地转移给您，从而帮助防范供应链中的安全漏洞。

借助 DOME，设备无需连接到云或网络。该设备仅需要连接到所有者。所有者只需连接到云端即可启用所有权转移功能。

原本需要安全专家耗费大量时间进行的设备手动安全配置工作可被远程自动完成，从而简化这一工作，降低其成本，提升其速度并减少失误。一旦部署完成，用户可继续对设备进行远程安全管理。

在许多情况下，建筑所有者需要增强剩余生命周期仍较长的现有基础设施的安全性，同时最大限度减少业务中断。DOME 安全性也可加入现有的传统基础设施，通常可直接集成到现有设备中，以最大限度减少空间占用，这特别适合小巧的微处理器。如果这不可行，部署使用英特尔 FPGA 的 Veridify 嵌入式网关平台，以便在现有布线环境中添加一个安全网关，同时保持协议兼容性[1]；相比淘汰和更换，该解决方案具有更高的成本效益。

解决方案灵活性

保护建筑基础设施需要多种程度的灵活性。

- 硬件灵活性 — 任何建筑都需要安全集成许多厂商的各类设备。Veridify Security 工具独立于硬件和平台，可在软件或硬件中实施，支持多厂商互操作性。这些工具可与最小的物联网设备配合使用，仅需 8K ROM 即可在部署的处理器或微控制器上实现。
- 协议灵活性 — Veridify 的安全解决方案独立于协议，兼容当前、过去和未来的建筑自动化协议运行，包括多种行业协议（例如 BACnet、Modbus 和 KNX）以及多种数据链路协议（例如 MS/TP、IP 等）。
- 加密敏捷性 — 所有者可以为密钥和固件推送安全的现场更新设备。托管设备将验证并安装更新，及时应用安全更新。它还能够利用一种或多种安全方法，既有传统的又有面向未来的量子抵抗算法，这对于使用寿命较长的基础设施至关重要。
- 可扩展性 — Veridify 的部署和监管链操作甚至可轻松扩展到分布在全球众多建筑中的数百万个设备。

解决方案技术架构

设备所有权管理和注册

DOME 可保护工业厂房/园区中的所有互联设备，并建立 “网络安全边界”，确保边界内的所有设备和处理器得到妥当保护，并保持可信度。

首先，对于需要在建筑中使用的任何设备，在安装前为其提供生命周期区块链谱系，直至设备退役和从建筑中拆除为止。（参见图 1）

区块链供应链

在开始实施 DOME 时，为设备配置 DOME 客户端软件库以及与其原始所有者（例如，制造商）共享的公钥证书。此步骤将帮助设备支持现场的所有权管理和身份验证流程，而无需连接到云或中央服务器。制造商还为设备提供证书，以便轻松识别和实施相互身份验证，无论设备位于何处。DOME 客户端可在软件中实现，仅需要 12K 字节的 ROM。每个设备的证书都经过签名并纳

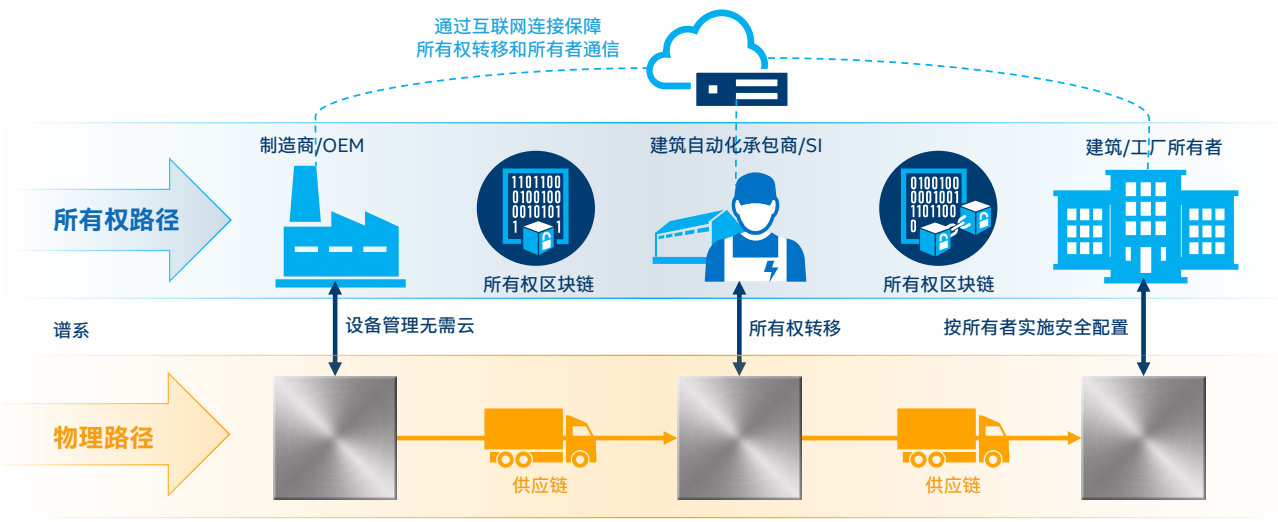

图 1 安全的所有权转移

[1] 对于使用嵌入式安全网关的安装场景，可能需要添加较短的布线

入 “区块” 中，从而为每个设备提供了嵌入到区块链中的特性。该框架可帮助所有者建立所有权证据，无需全面连接云端或网络，并支持设备级安全性管理。

DOME 客户端中的这些根证书还可以支持为用户应用安全分发二级加密密钥，以及现场配置用户应用和固件更新。证书经过签名并纳入设备的区块链中，能够支持每次所有权转移，并为设备在供应链中的移动和每次所有权转移提供支持。

零接触配置

平台在安装前验证设备所有权谱系。在安装过程中，对设备进行身份验证，然后由 DOME 接口设备（DIA）提供现场支持，然后移交给建筑的自动化或系统控制器处理，以安全地执行设备的预期日常功能。在供应链中不具备 DOME 安全性的设备，或经改造也不具备这种安全性的设备，可采用 Veridify 的嵌入式安全保护。（参见图 2）

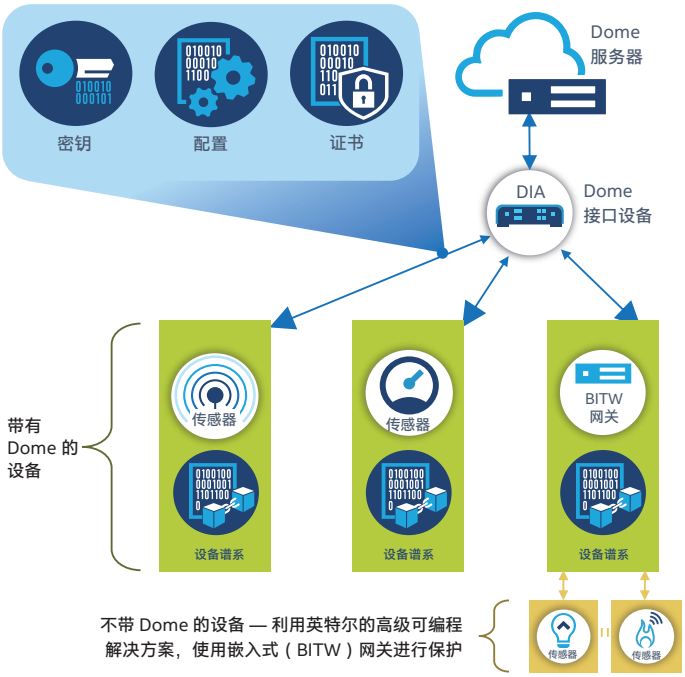

图 2 配置

部署的网络安全边界

DOME 接口设备对其在建筑生态系统中注册的每个设备，以及与这些设备交互的建筑控制器进行识别、身份验证和加密连接等方面的管理。接口设备监控设备状态，并可以提供安全的固件更新程序包和其他配置，例如建筑特定配置更改。接口设备还与建筑的中央管理系统进行通信，以对设备库存、设备状态、网络攻击（使用伪造或未经身份验证的命令）和用户进行报告。

能够对建筑自动化网络进行物理访问或通过缺乏保护的设备利用网络入口点的攻击者，将对受到保护的建筑网络中的组件发起攻击。通过这种方式，他们可能实施恶意活动，例如窃听网络流量以获取有用的数据，或者捕获、修改和播放数据以篡改传感器读数或向制动器发出命令等。此外，他们可控制互联设备以发起 DDOS 攻击，或访问建筑所有者的 IT 基础设施。在缺乏安全措施的情况下引入网络的流氓设备，也是发起攻击的便捷途径。DOME 保护的网络可以检测和阻止未经身份验证的设备及未经授权的访问。（参见图 3）

图 3 部署的安全性

保持生命周期安全性

在选择值得长期投资的安全平台时，加密敏捷性是一个重要的考虑因素。除了安全的远程更新外，用户可能需要在建筑自动化基础设施的长久生命周期内考虑更改基础安全算法。

这可能需要在未来支持量子抵抗算法，同时支持当今的现有标准方法，例如 ECDH/ECDSA。Veridify 可支持量子抵抗协议和未来几年可能兴起的 “下一代” 加密原语，能够确保在当前部署正确的安全方法，且该方法在网络环境的演变过程中不会沦为 “拦路虎” 或漏洞。

结论

Veridify Security 和英特尔携手合作，助力无缝保护建筑或多建筑园区。每个设备（无论大小如何及运行什么操作系统）都可获得创建安全可信环境所需的安全性，支持证书验证，能够实现高效管理和转移，直至退役。

从制造到退役，从传感器到服务器，我们能实现全方位安全性，有效应对不断演变的威胁环境，从而帮助您为智能建筑构建“网络安全边界”。

了解更多信息

请查看以下实用资源：

- 合作伙伴公司：
  veridify.com
- 解决方案产品公司：
  veridify.com/dome，veridify.com/bitw
- 白皮书：下一波安全潮流 – 拨开供应链迷雾
  www.intel.com/content/dam/www/public/us/en/documents/white-papers/next-security-frontier-intel-and-goldman-sachs.pdf

ss-1129-1.0