用于数据采集的Wi-Fi安全技术入门

概述

在过去十年中，IT 界的 Wi-Fi 无线网络的安全性能得到了极大的提高，使之成为数据采集应用中的一个可行的解决方案。因为 Wi-Fi 采用空气作为其物理传输媒介，相比于其它有线网络系统，它面临着更大的安全挑战。以下将简要介绍采用 NI 公司无线数据采集设备（DAQ）进行数据保护的工业标准安全技术。

Wi-Fi安全体系的历史

最初的 802.11 标准中引入了有线等效协议 (WEP)技术作为保护措施，以防不必要的无线网络访问。每台客户端电脑的都有一个访问网络接入点的密码。这个密码用于获取对网络的访问权，并且是网络接入点和客户机之间的所有消息加密的基础。

[+] Enlarge Image

因为 WEP 易于设置，所以大多数家庭和小型办公网络都使用 WEP。但是，WEP 容易受到攻击，特别是使用不当的时候。WEP 采用 RC4 密码对数据进行加密，采用 40 位密钥对消息进行编码和解码。攻击者们已经找到了这个协议中的漏洞，并开发了一些方法来入侵这种没有适当保护的 WEP 网络：

- **字典攻击** — 很多用户都保留着无线网络接入点和网卡的出厂默认设置。而其它一些用户则使用一些比较“弱”的 WEP 密钥，这些密钥都可以在字典中找到。一些潜在的攻击者通过“猜测”安全性设置来利用这些网络。有些攻击者采用蛮力攻击方式，同时还存在其它一些更复杂的方法。选择一些比较复杂的密码就可以轻松预防字典攻击。
- **中间人攻击** — 大多 Wi-Fi 网络接入点都将其 SSID 发布出来，这样客户们可以方便地找到这些接入点并与之相连。如果某个伪装的网络接入点发布相同的 SSID，就可以诱骗客户发送其安全信息，从而使得攻击者可以访问真实网络。常见最好的预防措施就是关掉路由器的 SSID 广播。
- **重放攻击** — 当攻击者窃听无线网络通信数据包并记录传输数据时，就产生了重放攻击。然后，攻击者使用这些数据来重放包含伪造的或者错误的数据消息，欺骗接入点去发送额外的地址解析协议(ARP)数据包。当数据包达到足够数量(50,000–100,000)时，攻击者就可以破解 WEP 密钥了。

NI 的无线数据采集设备支持 WEP 安全体系。但是，很多无线数据采集应用需要更强大的安全协议。

NI 无线数据采集网络安全组件

NI 无线数据采集设备支持多种无线安全协议，包括 WEP、Wi-Fi 保护访问(WPA)和 IEEE 802.11i(即所熟知的 WPA2)。WPA 通过阻止重放攻击，提供比 WEP 更好的安全性能。WPA2 则具有最优的无线网络安全性能，同时具备更强大的数据保护(加密)和访问控制(认证)性能。

加密

为了有效地保护无线数据传输，Wi-Fi 网络必需具备一种强大的加密算法(密码)和某种密钥管理形式。现在广泛采用两种 Wi-Fi 网络加密标准：TKIP 和 AES。

IEEE 802.11i 任务组为 WPA 引入了瞬时密钥集成协议(TKIP)，作为对现有 WEP 网络进行改进的一个权宜之策。接入点和客户可以通过一个简易的固件或软件升级将 WEP 升级到 WPA/TKIP。尽管加密算法还是一样的(RC4)，但 TKIP 优于 WEP 的一个地方在于 TKIP 使用了 128 位而非 40 位的密钥。一个更重要的区别在于，TKIP 对每个消息包都使用一个不同的密钥，这就是其名称中“瞬时”的出处。将已知的成对瞬时密钥(PTK)和客户的 MAC 地址以及数据包的序列号进行混合，动态创建这种瞬时密钥。当客户使用一个预共享密钥(PSK，所有网络用户都知道的一种短语密码)和随机数生成器来连接到接入点时，PTK 就生成了。序列号在每次发送新数据包时递增。这就意味着重放攻击不可能再发生了，因为每个数据包都不会再使用相同的密钥。当攻击者企图重发旧的数据包时，接入点就可以检测到这种行为。

作为最终的安全解决方案，IEEE 802.11i 任务组选择了高级加密标准(AES)作为 Wi-Fi 网络的首选加密算法。不同于 TPIK，AES 需要对大多数 WEP 装置进行硬件升级，因为 AES 的密码算法对处理器要求更高。AES 使用 128 位密码，所以比 TPIK 和 WEP 中所使用的 RC4 算法更加难于破解。实际上，NIST(国家标准与技术协会)要求所有美国政府机构选择 AES 作为加密标准。(FIPS publication 197 详细描述了这些要求)。政府和军方的任何无线数据采集应用都很可能必需采用 AES 来传输数据。

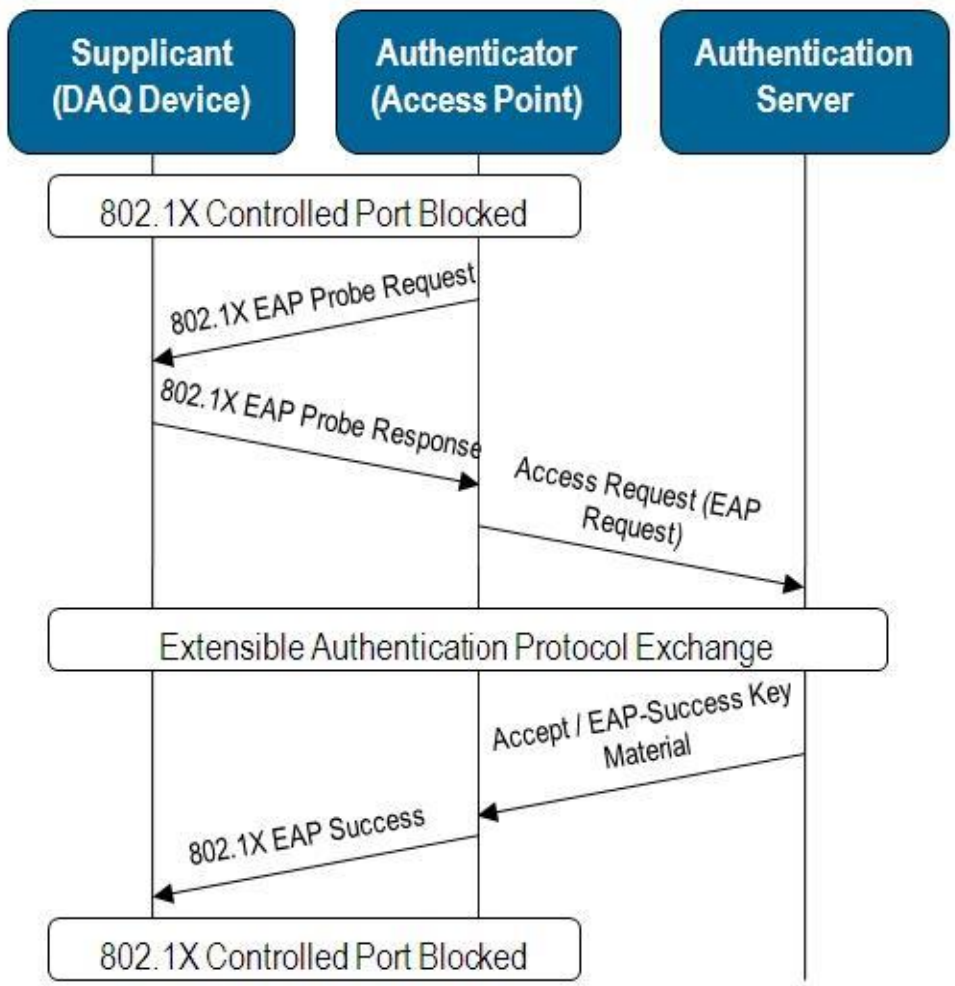
认证

本质上来说，网络认证就是客户访问控制。在客户可以与无线接入点进行通信之前，必须与网络进行认证。有两种认证形式：基于服务器的和基于 PSK 的。

大多数企业网络都有至少一个认证服务器，通常执行远程认证拨号用户服务(RADIUS)。WPA2 网络安全体系采用基于端口的 IEEE 802.1X 认证标准，包括以下几个部分：

- **Supplicant(申请者)**－访问网络的客户端无线设备
- **Authenticator(认证装置)**－无线接入点：控制申请者可以访问哪些网址

- **Authentication Server(认证服务器)**－为认证装置提供认证服务(通常是 RADIUS)



当申请者要求访问网络时，认证装置提供对未受控端口的访问。认证装置将访问请求传给认证服务器，再由认证服务器决定接受还是拒绝申请者的访问。然后，认证装置再将该响应从认证服务器传给申请者：要么允许访问可控端口，要么继续阻止被拒绝的申请者。

成功的认证过程生成一个成对主密钥(PMK)以加密无线传输。这种交换的细节取决于该网络支持何种扩展认证协议(EAP)方式。以下是几种最常见的 EAP 方式(NI 无线数据采集设备支持所有这几种方式)：

- **LEAP**(轻量级 EAP) － 由 Cisco 公司开发的古老而私有的 EAP 方法。任何微软操作系统中都不直接支持 LEAP。
- **EAP-TLS** (EAP-传输层安全) － 被大多数无线制造商所支持的开源标准。EAP-TLS 同时需要服务器认证和客户端认证，所以安装比较困难。
- **EAP-TTLS**(EAP-隧道传输层安全) － 与 EAP-TLS 方法相比是一种无需客户端认证的协议，适用于经常升级的网络
- **PEAP** (受保护的 EAP) －由 Cisco 公司、微软和 RSA 实验室开发的开源标准。这是一种流行的 EAP 方法，仅仅需要服务器端认证。PEAPv0/EAP-MsCHAPv2 是这种方法的最常见的变体。

所有上面所列的 EAP 方法都支持双向认证，这样可以阻止中间人攻击——因为客户需要对服务器进行认证，反之亦然。伪造的无线接入点无法伪造服务器端安全认证。

并非所有网络都有认证服务器，这就使得前述的认证方式无法实现。一些小型办公室或家庭办公室(SOHO)网络可以在客户端(无线数据采集设备)和接入点之间使用预共享密钥(PSK)来取代这些认证方式。本质上来说，预共享密钥是一种短语密码，是用户用来初始化网络认证的。

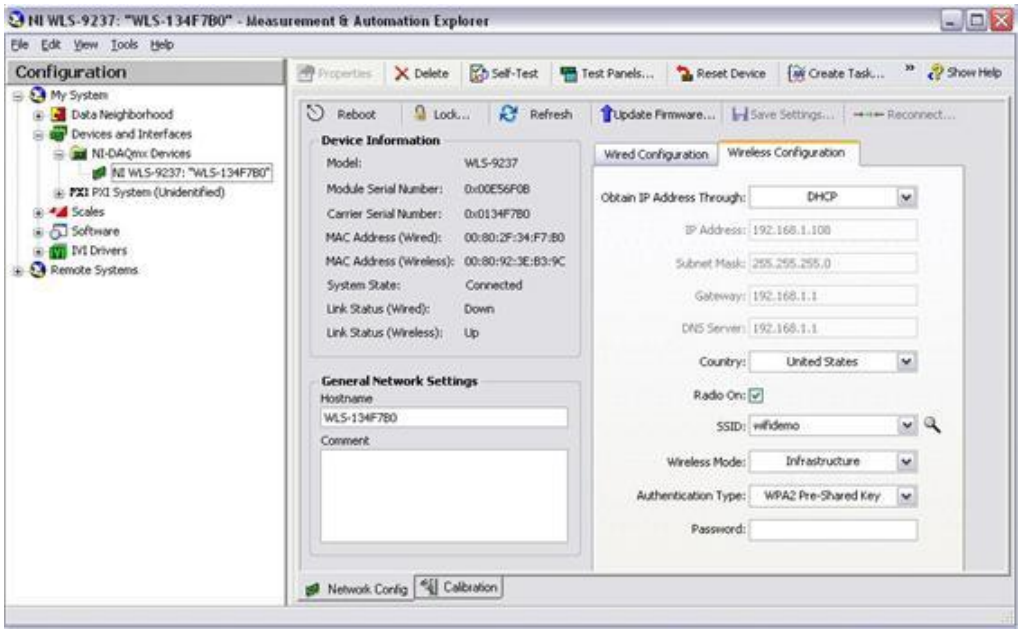
采用NI 无线数据采集设备实现安全网络

NI 无线数据采集 (DAQ)设备支持完整的 IEEE 802.11i 安全标准，包括 AES 加密和最流行的 EAP 认证方法。这是市场上最容易获得的无线网络安全设备，可以保护你的敏感数据不被侵犯。实际上，如果你的应用程序是用在政府或军方机构中，那么很可能强制要求使用 AES 加密。对于其它的应用，你就可以选择 WPA 和一些现有的接入点硬件。

如果你要连接到一个企业网络，你应该与 IT 部门共同决定采用何种你们的服务器所能接受的安全协议以及 EAP 方法。因为 NI 无线数据采集设备支持各种最常见的 EAP 方法(LEAP、PEAP、EAP-TLS 和 EAP-TTLS)，所以你可以自由选择其中一种以最佳匹配你的应用程序和网络构架。

无线数据采集设备的安全设置非常易于使用。在测量和自动化管理器(MAX)中，在“NI-DAQmx Devices”下选择你的无线数据采集设备，然后在屏幕底部单击“Network”标签页；选择“Wireless”标签页，在一系列的下拉菜单中，配置你的网络安全选项。

如果你的 EAP 方法需要客户端认证，请确保在装配 DAQ 设备之前获取该认证。如果要在没有认证服务器的条件下来装配你自己的网络，请确保采用一个复杂的 PSK 短语密码(WPA 和 WPA2 网络中)。



使用 MAX 配置无线数据采集设备加密和认证设置

MAX 采用一种加密、只写的过程将所有的配置和安装数据发送到 Wi-Fi 或者以太网网 DAQ 设备，包括用户名、密码和客户端认证，以进一步保护你的网络。

获取更多详细说明，请参考 NI WLS-9163 使用者手册。

无线数据采集设备网络安全最优方法清单

- 如果你的网络可以使用认证服务器(例如 RADIUS 服务器)，则使用 802.1X (EAP)
- 如果没有认证服务器，则使用较复杂的 PSK 密码。避免使用字典中常见的习语或单词，并混合使用大写字母、小写字母和数字字符。
- 创建无线接入点或路由器时，避免使用公共的或者出厂默认设置的 SSID。
- 如果接入点硬件支持 AES 加密技术，则在 TKIP 上使用该技术
- 尽量不要使用 WEP。将接入点升级到 WPA，或者下载 Windows XP WPA2 补丁