MQTT安全篇

3 (http://dataguild.org/?p=6866#comments)

Posted on 2015年12月27日 (http://dataguild.org/?p=6866) by 张 琪 (http://dataguild.org/?author=1)

物联网的核心是连接万物，通过交换并分析数据使得生活更舒适与便捷。不过，敏感数据泄露或者设备被非法控制可不是闹着玩的。比如前段时间国内某著名家电企业的智能洗衣机，使用了某著名电商基于XMPP协议的物联网平台，不费吹灰之力便被黑客攻破并远程遥控，给智能家居的发展带来了一些阴影。究其本质，并不是物联网技术本身有缺陷，而是在物联网系统的设计中最基本的安全设计被工程师轻视了，才导致整个系统的崩塌。

在这里我们将介绍为何以及如何运用MQTT提供的安全特性来保证物联网项目的顺利实施。

安全对于几乎所有的项目都是一个挑战，对于物联网项目更是如此：

- 设备安全性与设备可用性之间往往是零和博弈。
- 加密算法需要更多的计算能力，而物联网设备的性能往往非常有限。
- 物联网的网络条件常常要比家庭或者办公室的网络条件差许多。

对于以上挑战，MQTT提供了多个层次的安全特性：

1. 网络层：有条件可以通过拉专线或者使用VPN来连接设备与MQTT代理，以提高网络传输的安全性。
2. 传输层：传输层使用TLS加密是确保安全的一个好手段，可以防止中间人攻击（Man-In-The-Middle Attack）。客户端证书不但可以作为设备的身份凭证，还可以用来验证设备。
3. 应用层：MQTT还提供客户标识（Client Identifier）以及用户名密码，在应用层验证设备。

虽然MQTT提供了多重安全设计，不过世界上并没有银弹能够保障数据的绝对安全，所以应该在设计的时候就把安全放在设计目标之中并拥有相当的优先级，否则上文提到的智能洗衣机就是一个活生生的教训。

网络层可以使用专线或者VPN超出了本文的范围，下面我们结合Mosquitto仔细了解一下传输层和应用层的MQTT安全特性。

加密

MQTT是基于TCP的，默认情况通讯并不加密。如果你需要传输敏感信息或者对设备进行反控，使用TLS几乎是必须的。打个比方，如果你在咖啡店用免费Wi-Fi上网，登录互联网金融的网站不支持HTTPS传输，那么你的账号信息多半已经在咖啡店的Wi-Fi日志里面躺着了……

TLS是非常成熟的安全协议，在握手的时候便可以创建安全连接，使得黑客无法窃听或者篡改内容了。使用TLS的时候有以下注意点：

- 尽可能使用高版本的TLS。
- 验证X509证书链防止中间人攻击。
- 尽量使用有CA发布的证书。

当然，TLS会增加连接时开销，对低运算能力的设备而言是额外的负担，不过如果设备是长连接的话就会避免反复连接的开销。

Mosquitto原生支持了TLS加密，生成证书后再配置一下MQTT代理即可。

关键词…
搜索

近期文章

魔兽世界大数据分析 (http://dataguild.org/?p=7206)

为什么开源开放的大数据平台才能成功 (http://dataguild.org/?p=7190)

WordPress日志分析 (http://dataguild.org/?p=7169)

讲故事的艺术 (http://dataguild.org/?p=7129)

谈谈OAuth（下） (http://dataguild.org/?p=7090)

近期评论

流行的爆碎点穴 – 数据工会 (http://dataguild.org/?p=6934)发表在《《从0到1》读书笔记 (http://dataguild.org/?p=6461#comment-320)》

魔兽世界大数据分析 – 数据工会 (http://dataguild.org/?p=7206)发表在《使用百度开放云分析网站日志 (http://dataguild.org/?p=6739#comment-275)》

WordPress日志分析 – 数据工会 (http://dataguild.org/?p=7169)发表在《使用百度开放云分析网站日志 (http://dataguild.org/?p=6739#comment-259)》

miumiuforyou发表在《MQTT实战篇 (http://dataguild.org/?p=6957#comment-251)》

春泥面包 (http://huntinux.github.com)发表在《MQTT实战篇 (http://dataguild.org/?p=6957#comment-250)》

文章归档

2016年九月 (http://dataguild.org/?m=201609)

2016年八月 (http://dataguild.org/?m=201608)

2016年七月 (http://dataguild.org/?m=201607)

2016年五月 (http://dataguild.org/?m=201605)

2016年四月 (http://dataguild.org/?m=201604)

2016年三月 (http://dataguild.org/?m=201603)

2016年二月 (http://dataguild.org/?m=201602)

首先我们需要生成证书权威（Certificate Authority，CA）的认证和密钥，生成过程中Common Name一定要填写Fully Qualified Domain Name（测试起见用IP地址也凑合）：

```
openssl req -new -x509 -days 365 -extensions v3_ca -keyout ca.key -out ca.crt
```

接下来生成MQTT代理使用的密钥：

```
openssl genrsa -des3 -out server.key 2048
```

并去除密码：

```
openssl genrsa -out server.key 2048
```

然后为MQTT代理准备一个认证注册请求（Certificate Signing Request，CSR），这里的Common Name也要写对：

```
openssl req -out server.csr -key server.key -new
```

最后通过CA签署这个CSR生成MQTT代理证书：

```
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -ou
```

现在配置/etc/mosquitto/mosquitto.conf，确保8883端口的设置如下：

```
listener 8883
cafile /etc/mosquitto/tls/ca.crt
certfile /etc/mosquitto/tls/server.crt
keyfile /etc/mosquitto/tls/server.key
```

重启Mosquitto服务就可以用以下命令订阅和发布消息了，当然所有消息都由TLS加密，可以无忧无虑地传递私密信息啦：

```
mosquitto_sub -h host -p 8883 -t 'topic' --cafile ca.crt
mosquitto_pub -h host -p 8883 -t 'topic' -m '15' --cafile ca.crt
```

其中，host需要与前面指定的Common Name一致，否则TLS连接会报错，错误信息也不是很直观……

认证

认证是验证设备身份的过程。拿旅行做比方，在换登机牌的时候需要出示护照以验明正身，即使别人能够假冒你的名字，但是拿不出护照便无法伪造身份。买房的时候，需要通过户口本证明你妈是你妈。

MQTT支持两种层次的认证：

- 传输层：传输层使用TLS不但可以加密通讯，还可以使用X509证书来认证设备。
- 应用层：MQTT支持客户标识、用户名密码以及X509证书，在应用层验证设备。

通过传输层和应用层来解释认证并不直观，下面我们直接从客户标识、用户名密码以及X509证书的角度来了解认证。

客户标识

用户可以使用最多65535个字符作为客户标识（Client Identifier），UUID或者MAC地址最为常见。

使用客户标识来认证并不可靠，不过在某些封闭的环境中或许已经足够。

用户名密码

MQTT协议支持通过CONNECT消息的username和password字段发送用户名和密码。

用户名密码的认证使用起来非常方便，不过再强调一下，由于用户名密码是以明文形式传输，在通过互联网时使用TSL加密是必须的。

Mosquitto支持用户名/密码认证方式，只要确保/etc/mosquitto/mosquitto.conf有如下设置：

```
password_file /etc/mosquitto/passwd
allow_anonymous false
```

其中passwd文件是用来保存用户名和密码的，可以通过mosquitto_passwd来维护用户名密码。之后便可以通过如下命令订阅和发布消息了：

```
mosquitto_sub -h host -p 8883 -t 'topic' --cafile ca.crt -u user -P pwd
```


2016年一月 (http://dataguild.org/?m=201601)
2015年十二月 (http://dataguild.org/?m=201512)
2015年十一月 (http://dataguild.org/?m=201511)
2015年八月 (http://dataguild.org/?m=201508)
2015年七月 (http://dataguild.org/?m=201507)
2015年六月 (http://dataguild.org/?m=201506)
2015年五月 (http://dataguild.org/?m=201505)
2015年二月 (http://dataguild.org/?m=201502)
2015年一月 (http://dataguild.org/?m=201501)
2014年十二月 (http://dataguild.org/?m=201412)
2014年十一月 (http://dataguild.org/?m=201411)
2014年九月 (http://dataguild.org/?m=201409)
2014年八月 (http://dataguild.org/?m=201408)
2014年七月 (http://dataguild.org/?m=201407)
2014年六月 (http://dataguild.org/?m=201406)
2014年四月 (http://dataguild.org/?m=201404)
2013年十二月 (http://dataguild.org/?m=201312)
2013年十一月 (http://dataguild.org/?m=201311)
2013年十月 (http://dataguild.org/?m=201310)
2013年九月 (http://dataguild.org/?m=201309)
2013年八月 (http://dataguild.org/?m=201308)
2013年六月 (http://dataguild.org/?m=201306)
2013年五月 (http://dataguild.org/?m=201305)

分类目录

云计算 (http://dataguild.org/?cat=2)
产品经理 (http://dataguild.org/?cat=8)
大数据 (http://dataguild.org/?cat=3)
数据分析 (http://dataguild.org/?cat=5)
物联网 (http://dataguild.org/?cat=6)
软件工程 (http://dataguild.org/?cat=7)

功能

登录 (http://dataguild.org/wp-login.php)
文章RSS (Really Simple Syndication) (http://dataguild.org/?feed=rss2)
评论RSS (Really Simple Syndication) (http://dataguild.org/?feed=comments-rss2)
WordPress.org (https://cn.wordpress.org/)

```
2 mosquitto_pub -h host -p 8883 -t 'topic' -m '9' --cafile ca.crt -u user -P pw
```

这里端口使用8883是假设已经配置了TLS加密的。

结合TLS加密的用户名密码认证，已经是相对完善的安全体系了。

X509证书

MQTT代理在TLS握手成功之后可以继续发送客户端的X509证书来认证设备，如果设备不合法便可以中断连接。

使用X509认证的好处，是在传输层就可以验证设备的合法性，在发送MQTT CONNECT之前便可以阻隔非法设备的连接，以节省后续不必要的资源浪费。

如果你可以控制设备的创建和设置，X509证书认证或许是个非常好的选择。不过代价也是有的：

1. 需要设计证书创建流程。如果你对设备有着完全的控制，在设备出厂前就能烧录X509证书到设备中，那么这条路是非常合适的。但是，对于移动设备等无法实现烧录证书的场景，用户名/密码认证或许是更好的选择。
2. 需要管理证书的生命周期，最好通过PKI（Public-Key-Infrastructure）来管理。
3. 如果证书泄露了，一定要立即使证书失效。一个选择是使用证书黑名单（Certificate Revocation Lists），另一个选择是提供在线证书状态协议（Online Certificate Status Protocol），方便MQTT代理及时了解证书的状态。

MQTT原生支持X509认证，生成客户证书后再配置一下MQTT代理便可。

首先生成设备密钥：

```
1 openssl genrsa -des3 -out client.key 2048
```

然后为准备一个设备认证注册请求：

```
1 openssl req -out client.csr -key client.key -new
```

最后通过CA签署这个CSR生成设备证书：

```
1 openssl x509 -req -in client.csr -CA ca.crt -CAkey ca.key -CAcreateserial -ou
```

现在配置/etc/mosquitto/mosquitto.conf，确保8883端口的设置如下：

```
1 listener 8883
2 cafile /etc/mosquitto/tls/ca.crt
3 certfile /etc/mosquitto/tls/server.crt
4 keyfile /etc/mosquitto/tls/server.key
5 require_certificate true
```

重启Mosquitto服务就可以用以下命令订阅和发布消息了，当然所有消息都由TLS加密，可以无忧无虑地传递私密信息啦：

```
1 mosquitto_sub -h host -p 8883 -t 'topic' --cafile ca.crt --cert client.crt --
2 mosquitto_pub -h host -p 8883 -t 'topic' -m '95' --cafile ca.crt --cert clien
```

可以看到，X509同时提供了完善的加密和验证，只是证书的生命周期管理的代价要比用户名密码高一些。

授权

授权是对资源的访问权限。继续拿机场做例子，在使用护照认证了用户之后，系统会根据预定决定用户可以上特定时间和班次的飞机，这就是授权。

对MQTT而言意味着对主题的订阅和发布权限。Mosquitto内置了基本的授权，那就是基于Access Control List的授权。

由于ACL是基于特定用户的，所以需要使用用户名密码认证方式。然后，
在/etc/mosquitto/mosquitto.conf中指定ACL文件：

```
1 acl_file /etc/mosquitto/acl
```

在这个ACL文件便可以指定用户的读写权限，比如下面便可以授权用户tom读写指定主题的权限：

```
1 user tom
```

```
2 topic readwrite company/building/floor/#
```

Mosquitto只提供了基本的基于ACL的授权，更高级的基于RBAC的授权可能需要通过插件的形式自行开发了。

体系

在MQTT项目实施时，还可以考虑通过防火墙保护MQTT代理：

- 仅允许相关的流量传递到MQTT代理，比如UDP、ICMP等流量可以直接屏蔽掉。
- 仅允许相关端口的流量传递到MQTT代理，比如MQTT over TCP使用1883，而MQTT over TLS使用8883。
- 仅允许某些IP地址段来访问MQTT代理，如果业务场景允许的话。

篇幅有限，本文只涉及了MQTT安全体系设计的冰山一角，如果读者感兴趣还可以参考HiveMQ发布的Introducing the MQTT Security Fundamentals (http://www.hivemq.com/blog/introducing-the-mqtt-security-fundamentals)系列博文。堡垒往往最容易从内部攻破，只有在系统在设计的时候就把安全放在首要位置并且积极地去做威胁模型分析，这才能有效保护用户数据。

MQTT系列索引：

1. MQTT入门篇 (http://dataguild.org/?p=6817)
2. MQTT进阶篇 (http://dataguild.org/?p=6846)
3. MQTT安全篇 (http://dataguild.org/?p=6866)
4. MQTT实战篇 (http://dataguild.org/?p=6957)

物联网 (http://dataguild.org/?cat=6) MQTT (http://dataguild.org/?tag=mqtt), 安全 (http://dataguild.org/?tag=%e5%ae%89%e5%85%a8)

张 琪

MORE POSTS (HTTP://DATAGUILD.ORG/?AUTHOR=1)

❮ MQTT进阶篇 (HTTP://DATAGUILD.ORG/?P=6846)

《大数据思维与决策》读书笔记 ❯ (HTTP://DATAGUILD.ORG/?P=6875)

3 COMMENTS

Pingback: MQTT进阶篇 – 数据工会 (http://dataguild.org/?p=6846)
Pingback: MQTT入门篇 – 数据工会 (http://dataguild.org/?p=6817)
Pingback: MQTT实战篇 – 数据工会 (http://dataguild.org/?p=6957)

发表评论

电子邮件地址不会被公开。 必填项已用*标注

评论

姓名 *

电子邮件 *

站点

发表评论