

WEBINAR

IoT Security Issues and MQTT



HIVEMQ



Speaker



Gaurav Suman

Product Marketing Director @HiveMQ

 gaurav.suman@hivemq.com

 <https://www.linkedin.com/in/grvsmn/>

 @grvsmn

- Product Marketing lead at HiveMQ
- Telecoms, Unified Comms, Networking, Software technology
- Solutions Architect and Product Manager
- Based in Ottawa, Canada



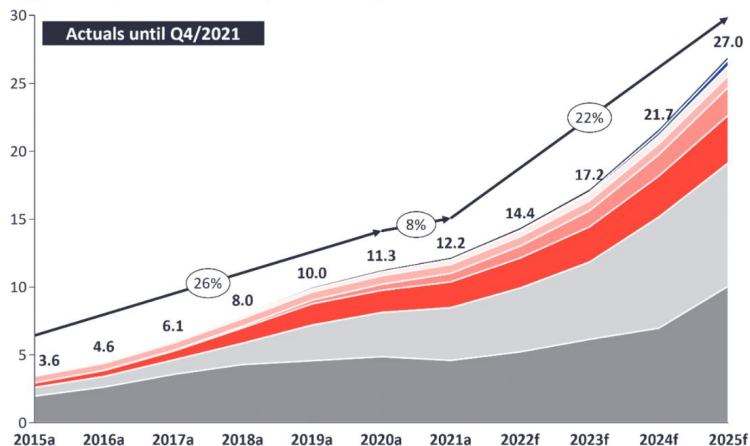


Why is IoT Security on
top-of-mind for devs and
architects?

The Internet of Things is HUGE

Global IoT Market Forecast [in billion connected IoT devices]

Number of global active IoT Connections (installed base) in Bn



CONNECTIVITY TYPE	CAGR 20-21	CAGR 21-25
Wireless Neighborhood Area Networks (WNAN)	17%	11%
5G IoT	-	159%
Other	22%	20%
Wired IoT	4%	7%
LPWA	42%	34%
Legacy Cellular (2G/3G/4G)	16%	17%
Wireless Local Area Networks (WLAN)	19%	24%
Wireless Personal Area Networks (WPAN)	-6%	22%

XX% = CAGR

Note: IoT Connections do not include any computers, laptops, fixed phones, cellphones or tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes Ethernet and Fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G; LPWAN includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-fi and related protocols; WNAN includes non-short range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.

Source: IoT Analytics Research 2022. We welcome republishing of images but ask for source citation with a link to the original post and company website.

The risks are clear

CNN BUSINESS

Markets Tech Media Success Video

FDA confirms that St. Jude's cardiac devices can be hacked

Economy | Business and Economy | **Bloomberg**

Recent cyberattacks reveal US utilities' extreme vulnerability

Highly inadequate digital security poses a national threat as hackers shift focus to utilities' networks.



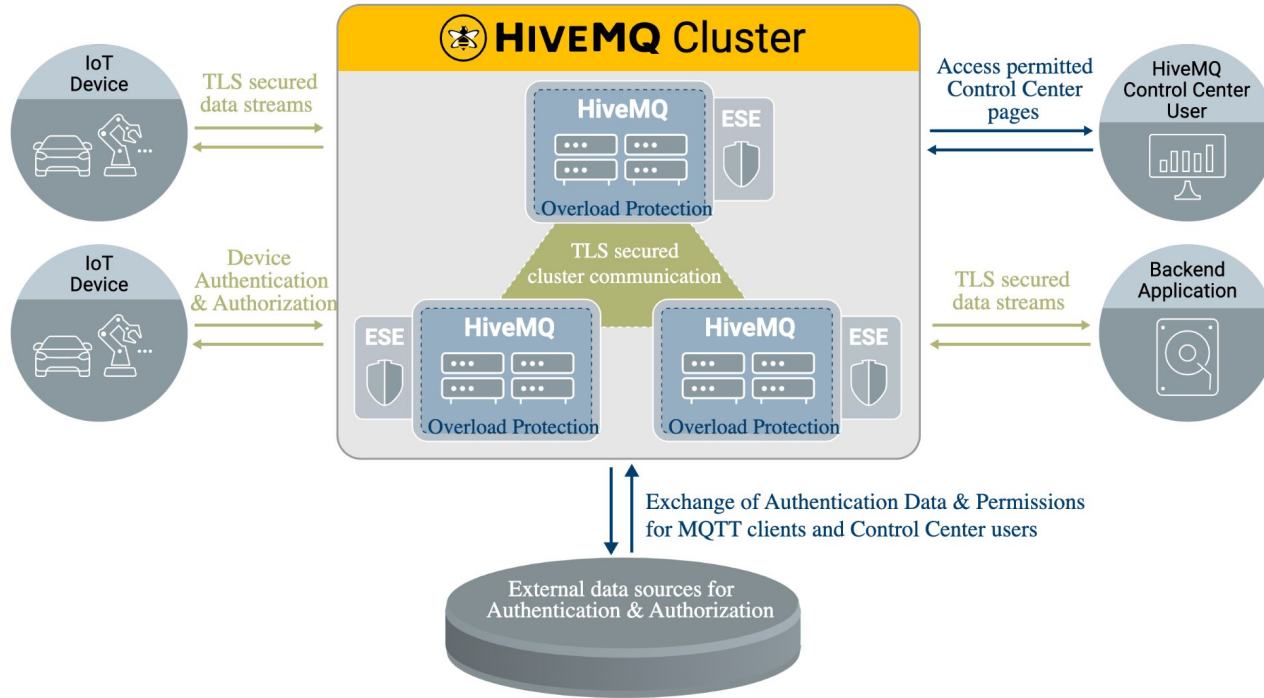
Shock at the wheel: your Jeep can be hacked while driving down the road kas.pr/7xnm



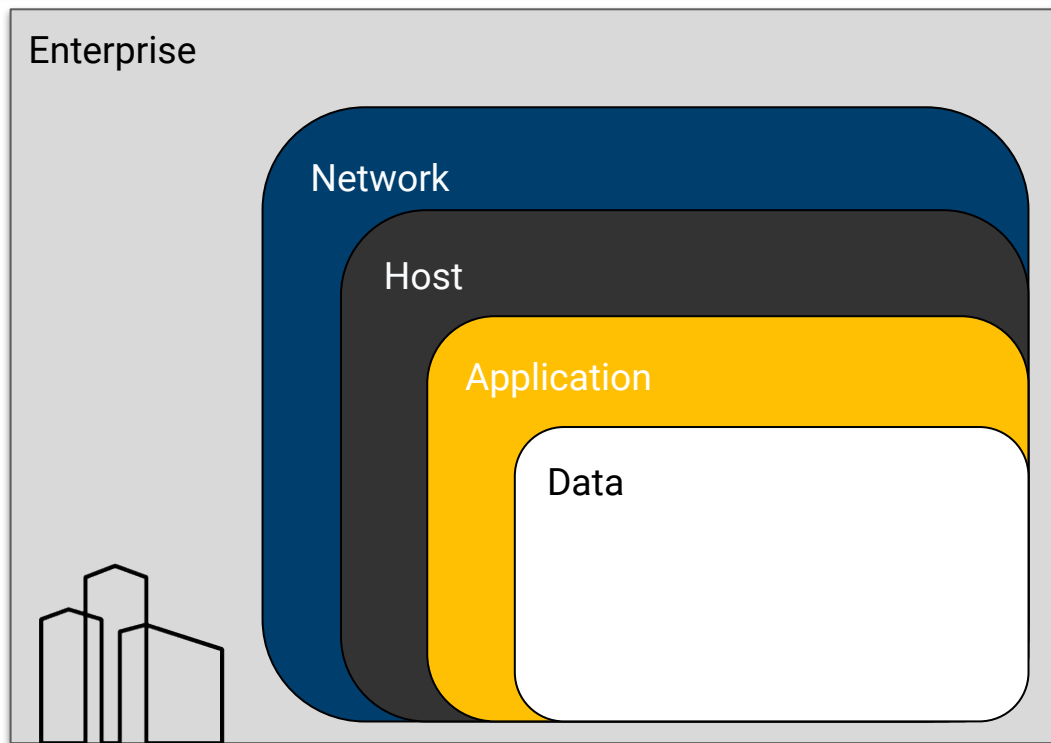
IoT security challenges are unique

- Low-power devices
- Spread far and wide
- Long lifecycle of devices

HiveMQ: Security



Multiple Security Layers



We will bankrupt ourselves in the vain search for absolute security.

- D.E. Eisenhower

Securing the IoT connectivity stack

	Unauthorized Access	Eavesdropping	Denial of Service	MITM, Replay Attacks	Remedy
Application	●		●		Authentication and Authorization
Transport		●		●	Securing the Transport layer with TLS
Network	●	●	●	●	VPN



What's special about **MQTT?**

What Is MQTT?



- (I)IoT Messaging Protocol
- Created for extreme scale and instant data exchange
- Publish/Subscribe based architecture
- Easy on the device side, pushes all implementation complexity to the server
- Built for machines and constrained devices (binary, data agnostic)
- Designed for reliable communication over unreliable channels

MQTT Use Cases

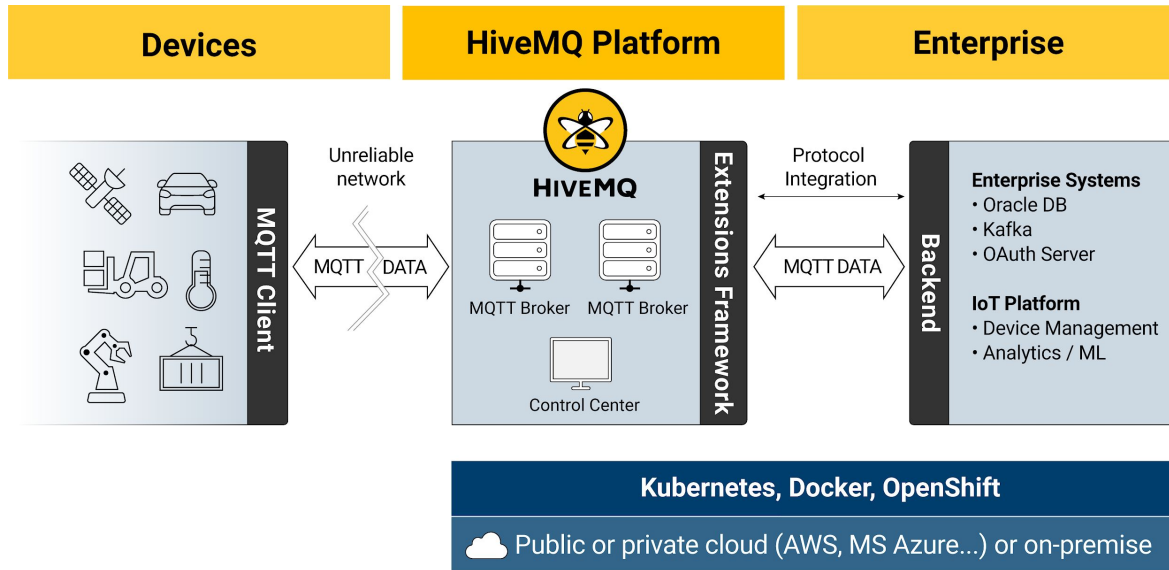


The MQTT specification 'specifies'

MQTT solutions are often deployed in **hostile communication environments**. In such cases, implementations will often need to provide mechanisms for:

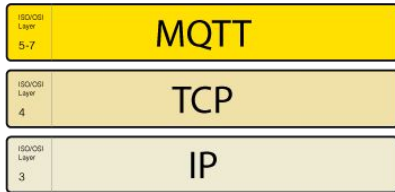
- **Authentication** of users and devices
- **Authorization** of access to Server resources
- **Integrity** of MQTT Control Packets and application data contained therein
- **Privacy** of MQTT Control Packets and application data contained therein

MQTT Broker



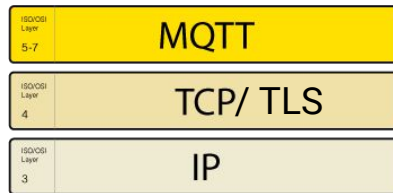
- Conserve
- Decouple
- Centralize Policy

Transport Encryption



- MQTT is based on **TCP / IP Stack**
- **Port 1883:** MQTT over TCP

- TCP connection can be **secured by TLS**
- **Port 8883:** MQTT over TLS





How MQTT helps secure IoT

Authentication and Authorization



Authentication



- Client ID
- Username
- Password
- Digital Certificates
- OAuth, JWT

Advanced Authentication Options



- Digital Certificates
- Wire the broker and the auth store

Using certificates for TLS

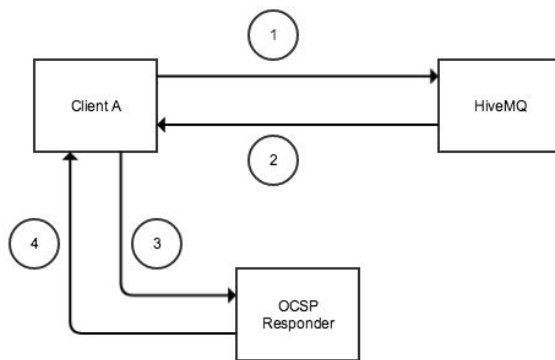


- Typically relies on a public certificate authority
- Can also work with private certificates
 - Only for closed networks

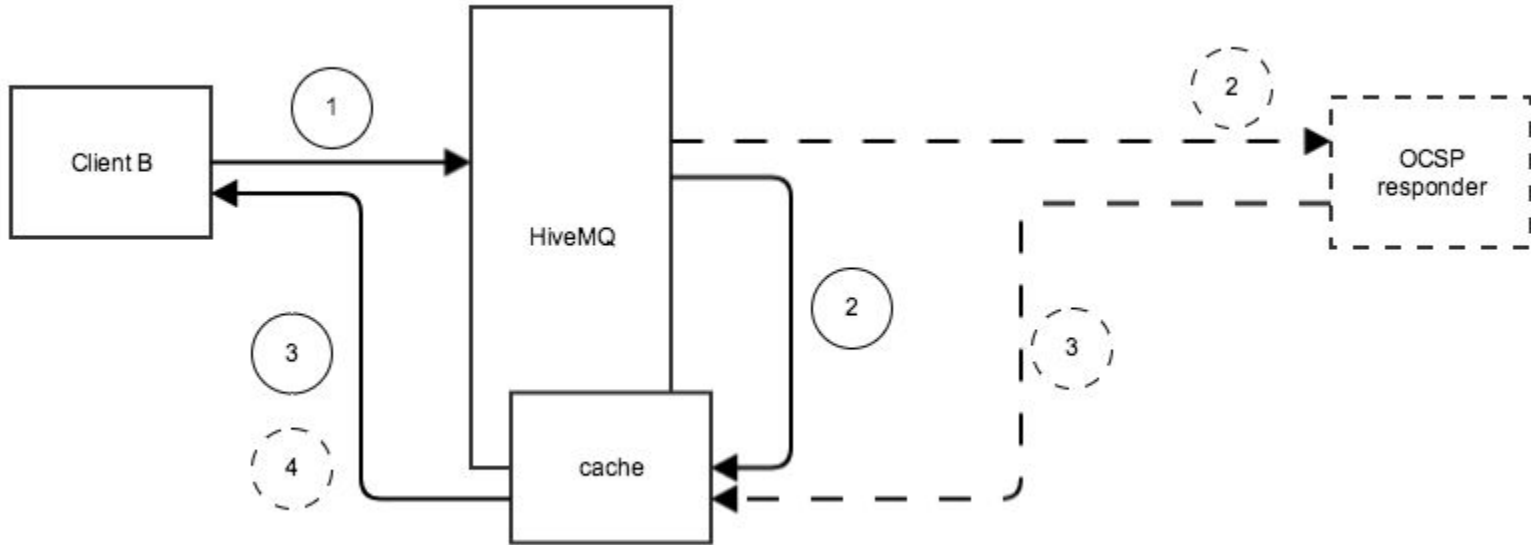


Consider these when using X.509 based Authentication


- You need control over the MQTT client
- Managing the Certificate lifecycle
 - Certification Revocation Lists (CRLs)
 - Online Certificate Status Protocol



OCSP Stapling: Authentication at Scale



Client Authentication (Identity and Access Management Systems)

MQTT-Packet: CONNECT 	
contains:	Example
clientId	"client-1"
cleanSession	true
username (optional)	"hans"
password (optional)	"letmein"
lastWillTopic (optional)	"/hans/will"
lastWillQos (optional)	2
lastWillMessage (optional)	"unexpected exit"
lastWillRetain (optional)	false
keepAlive	60

Caution:

Not all brokers support a pluggable authentication and authorization system!

- Different **external systems** can be used to authenticate clients at a broker
- Client provides **authentication data in the CONNECT packet**
- Broker **looks up the authentication data** in the connected external systems
- External authentication systems:
 - LDAP
 - OAuth2.0
 - Databases
 - ACL
 - ...

Creating Custom Authentication Logic

```
1 public class AuthWithUsernamePasswordCallback implements OnAuthenticationCallback {
2     @Override
3     public Boolean checkCredentials(ClientCredentialsData clientCredentialsData) throws AuthenticationException {
4         {
5
6         // Custom Authentication Logic
7
8     }
9 }
```


Authorization

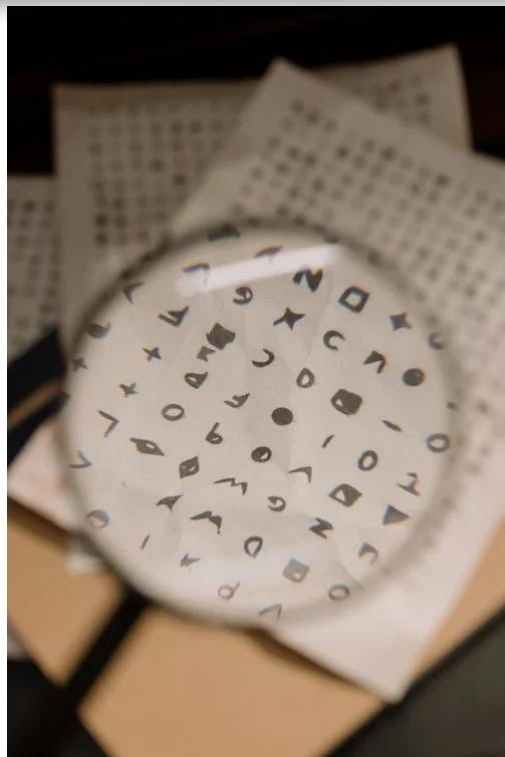


- Publisher and Subscriber Authorization
 - Whether they can publish/subscribe
 - Which QoS level
 - Operations (read, write)

Permissions

```
1  @Override
2  @Cached(timeToLive = 5, timeUnit = TimeUnit.MINUTES)
3  public List<MqttTopicPermission> getPermissionsForClient(ClientData clientData) {
4      List<MqttTopicPermission> mqttTopicPermissions = new ArrayList<MqttTopicPermission>();
5      mqttTopicPermissions.add(
6          new MqttTopicPermission(
7              clientData.getClientId() + "#",           // Topic
8              MqttTopicPermission.ALLOWED_QOS.ALL,      // QoS
9              MqttTopicPermission.ALLOWED_ACTIVITY.ALL)); // Publish, Subscribe, All
10
11     return mqttTopicPermissions;
12 }
```

Encryption



Transport Encryption - Best Practices



- **Use transport encryption (TLS)**
- **Use certificates from trusted CAs**
- **Use highest TLS version and secure cipher suites**

Payload Encryption

On very constrained devices transport encryption may be not possible!

- Use payload encryption instead
- Every clients needs to have key & secret
- *BUT!: It leaks metadata*

DoS and Overload Protection

- Limit Connections and Connection Idle times
- Throttle Connection Rates including Burst Rates
- Throttle SSL Handshakes
- Throttle Network Bandwidth
- Cluster Overload Protection throttles overactive publishing clients to prevent cluster overload
- Limit ClientID and topic length to prevent malfunctioning IoT access

Criteria for selecting the right MQTT Broker

- Performant, scalable and high available broker
- Compliance to the entire MQTT specification
- Monitoring of broker and tracing of devices
- Pluggable authentication & authorization system
- Overload Protection
- Supports TLS
- Professional support

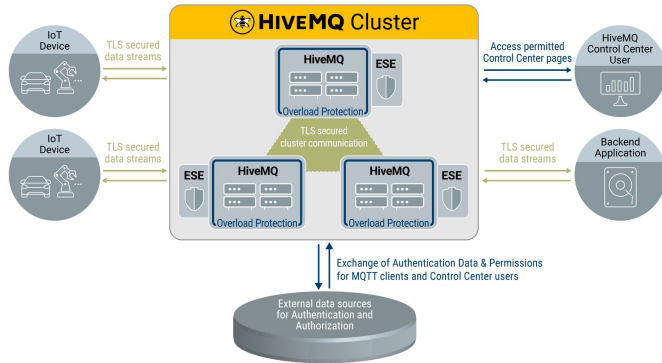


HIVEMQ
ENTERPRISE



 RabbitMQ

HiveMQ Security Architecture



- Pluggable Authentication and Authorization System
- Prebuilt Security Extension
- TLS secured communication
- Overload Protection and (D)DOS detection
- Fine grained permission system for MQTT clients and HiveMQ Control Center users
- Chaining of auth mechanisms
- Default Deny-All behaviour
- Integrated monitoring system and over 1500 metrics
- 24/7 professional support



HiveMQ Enterprise Security Extension



HIVEMQ Enterprise Security Extension

- Central management for **IoT device and HiveMQ Control Center authentication and authorization**
- Flexible and easy **integration with multiple external authentication systems and data sources** (e.g. databases, LDAP, OAuth 2.0)
- High **Scalability and reliability**
- Default **Whitelisting Concept**
- **Access log** (rolling on daily basis)
- Provides maximum flexibility in defining authorization rules

Resources



[Get Started with MQTT](#)



[Evaluate HiveMQ](#)



[Try HiveMQ Cloud](#)



[HiveMQ Enterprise Security Extension](#)



Blog Series | [MQTT Security Fundamentals](#)



[Watch Our Previous Security Webinar Recording](#)



ANY QUESTIONS?

Reach out to community.hivemq.com



THANK YOU

Contact Details

Gaurav Suman

✉ gaurav.suman@hivemq.com

[in https://www.linkedin.com/in/grvsmn/](https://www.linkedin.com/in/grvsmn/)

