Security and User roles

Minutes of the meeting held at the 37th TANGO Community workshop

Brainstorming:

- Encryption (with TLS certificate, mutual), every DS should have a different certificate

- Policy: Specify endpoints (device servers) which a client can talk to

- Authentication: OpenID

Lorenzo:

- Authentication and Authorization, before Encryption, optional

- Encryption, optional

- Level you want to do things:

- User roles:

- Do everthing

- Attributes/Commannds but not properties

- Just read attributes

Every single device class.

Nice to have it on the attribute/command level.

The device would be a user as well and would have roles as well.

Matteo:

- Would like to not have user roles in the code written down

- Taranta as it is:

- TangoGQL: Checks the JWT (JSON Web Token), this is a secret,

- global read access or global read/write access (including writing

attributes, execution of commands, read/write properties)

- Proper authentication

Jakub:

- Allow to expose tango TCP/IP ports to the internet in a secure way

- Allow to have encrypted properties

Marco:

- In the transport layer we need to know who is the user interacting.

- Authorization should not be defined in the code. No code change.

- Would be nice to have what is inside Taranta in tango

Vincent:

- We currently rely on the network being protected against the user

- Problem that support staff should have limited roles as well

- Works with taranta but can be circumvented with user other clients

- Encryption is a nice thing

- Authorization: What is in taranta is enough.

- Simple use case:

- Read/write access on a device server level

- Look into omniORB 4.3 security features (HTTPS)

Stefano:

- Read/write user roles

- Look at how taranta does stuff

All agree that we should:

Deprecate TAC and remove it from TSD.

Recent hacks on Alma and Helmholtz.

Vision:

- Security means encryption, authorization and authentication, all based on open standards

- Encryption will be kryptoagile

- Encryption will also mean integrity

- Security is optional within tango controls

- Support multiple providers for authentication/authorization

- Authentication and User roles are managed outside of tango controls

- Three user roles on a device class level:

- Read

- Read/Write

- Changing configuration

- Should interact well with the logging for audit trials

Next steps:

- Look at the SCADA competition if there is something we can learn from (WinCC, Beckhoff, OPC-UA

- Look into how the token will be passed within the network messages

- Look into what omniORB and zeromq already offers

Useful links:

- https://blogs.cisco.com/internet-of-things/what-is-opc-ua-and-how-does-it-manage-security
- https://www.youtube.com/watch?v=2mPGeddA65E