

Bridging the IoT Security Gap / Graph Database

Hosted by: Victor Ake

Interests:

Device identity, down to silicon, to provide security
Proliferation of things and how we manage them.

Waze got hacked to manage to get a clear route (hacked GPS sent fake coordinates to overload a route, diverting traffic to side roads). How to detect compromised device ?

Blockchain to come to IoT, sequence of information from birth of a chip to recording user buying the GPS. Creates a chain of trust.
Chip manufacturer could be a cert authority for blockchain.

On security front, Tokens with proof of possession can compensate the lack of secure channel.

Not all devices have the capability to store securely a token or key. (Look at the Car industry)
A solution is the Identity Edge Controller, which manages those keys and secrets for the devices.
IEC needs to run on small, lower power devices with secure elements.

Touching on Graph Databases.

Relationships are best described with Graph DB.
Makes more sense in the IoT context with the scale factor as well as physical aspect of devices.
Issues with many different query languages, data models... We need for convergence and emergence of a real standard.

There has to be responsibility from manufacturer for the security of devices ! Dlink was fined for one of its product.