From: DoNot Reply
To: Submissions
Subject: Submission Received
Date: Thursday, 7 October 2021 1:36:04 PM

The below submission has been lodged and confirmed on the AEMC Web site.

Submission Type: Rule Change

Reference: Governance of distributed energy resources technical standards

Organisation: None

First Name: Siraj

Last Name: Rakhada

Email: [redacted]

Phone Number: [redacted]

Comments: I only came across this today, on the last day of submissions, so my submission is rushed, sorry.
I am actually a retail solar customer, who found some glaringly big holes in the security of a purchased solar battery system, and the potential risks to the Australian power grids due to this insecurity.
I think details might help - my personal solar battery is an Alpha ESS system. All communications from this battery to a central controller are in clear text from my home in NSW to a system hosted at Azure in Singapore. This cleartext information includes passwords, and personally identifiable information - my name, address, and contact details.
I also found that even though the system requires authentication, it is easily bypassed.
I also found that anyone could 'war drive' and find these devices around australia, as they have open wifi, with a common password.
Due to these findings, I have personally decided that I do do not want to add to the insecurity of the power grid and have disconnected my battery from the public Internet.
This however, costs me, as I no longer get the benefit of being part of a virtual power plant.

Australia needs to require far better security of home equipment (inverters, smart meters, batteries) that talk on the Internet to do at least the following:

1. certificate based authentication - on BOTH sides - so that if there is a man in the middle attack, the battery itself won't just trust the attacker and start communicating.
2. encrypted communication - this needs to exist as a bare minimum. There is no need to send data like this in plain text.
3. a more secure local setup system - there should be no way for a person to see that this equipment exists with no physical access to the unit. Access to reconfigure the network should only be allowed if a physical action is taken (a button), AND access to some information that ideally is not printed on the unit, and is also unique per unit.
4. Virtual Power Plant systems should be denied operation if they use equipment that does not follow the above.

There are likely other things that need to be done too - I am not a security expert, I am just a person who works in IT and stumbled upon the total lack of security of the Alpha ESS systems while trying to get information out. There is actually no part of the Alpha ESS system that I would consider secure.

Ideally, and this is likely way off topic for this submission, home battery systems would also allow an open API for consumers to be able to check things like solar/battery power levels, so they can turn on/off things automatically.

I can provide more technical details of the specific insecurities if that is wanted.