Wireless networks exposed as electricity grid weakest link

December 31 2013, by Nic White

The technology also helps make the grid more efficient and protect it from blackouts as power companies can plan ahead to optimise their use of extra generators and shut down power-hungry devices that the meter allows them to directly communicate with. Credit: Ian Britton

Smarter, more efficient electricity meters aim to revolutionise energy distribution but WA researchers fear hackers could easily exploit numerous security flaws and wreck havoc on power grids.

Smart meters measure a customer's electricity consumption every half hour, including which devices are turned on and how much energy they draw from the grid, and send it to the power company.

Not only does this eliminate the need for human meter readers, it allows

energy providers to monitor how the network is functioning, detect faults, and remotely manage connections.

The technology also helps make the grid more efficient and protect it from blackouts as power companies can plan ahead to optimise their use of extra generators and shut down power-hungry devices that the meter allows them to directly communicate with.

However, ECU Security Research Institute director Professor Craig Valli says because the smart grid system relies on inherently insecure wireless networks to transmit information through parts of the system, there are significant vulnerabilities for determined cyber criminals to attack.

"There's a lot of economic benefit to this but the security around it sucks," he says.

"A lot of it is poor implementation, there's an unwillingness to put in a lot of the available controls.

"[Using full security features] is not going to be popular but do you want electricity coming down that cable or do you want a free-for-all for cyber criminals to cause havoc?"

Prof Valli says even with all security controls enabled it "would be the difference between stealing a car with broken lock verses a car with a good alarm system".

In an experiment he and a team of ECU researchers were able to intercept communications between smart grid devices using eavesdropping software.

Prof Valli says while they were unable to find the key to decrypt it

someone with more time and resources could, and that in a few years it would be possible with freely available programs.

Once they had the key, cyber criminals could shut off a building's power to infiltrate it, or cause mayhem by knocking out entire suburbs or potentially cities.

Verve Energy chief engineer Andy Wearmouth says an entire blackout of Perth would take several hours to restore.

However it could take much longer if hackers were able to corrupt meters that would have to be manually reset, he says.

"That would be a really ugly scenario, if someone was able to get in and effectively turn the power supply off to everyone's house," he says.

Provided by Science Network WA