When amateurs do the job of a professional, the result is smart grids secured by dumb crypto

May 15 2015, by Bill Buchanan

Bright colours, dumb ideas. Credit: Oast House Archive, CC BY-SA

Security relies upon good programming and correct adherence to well-designed standards. If the standards are sloppy, then security has been compromised from the outset.

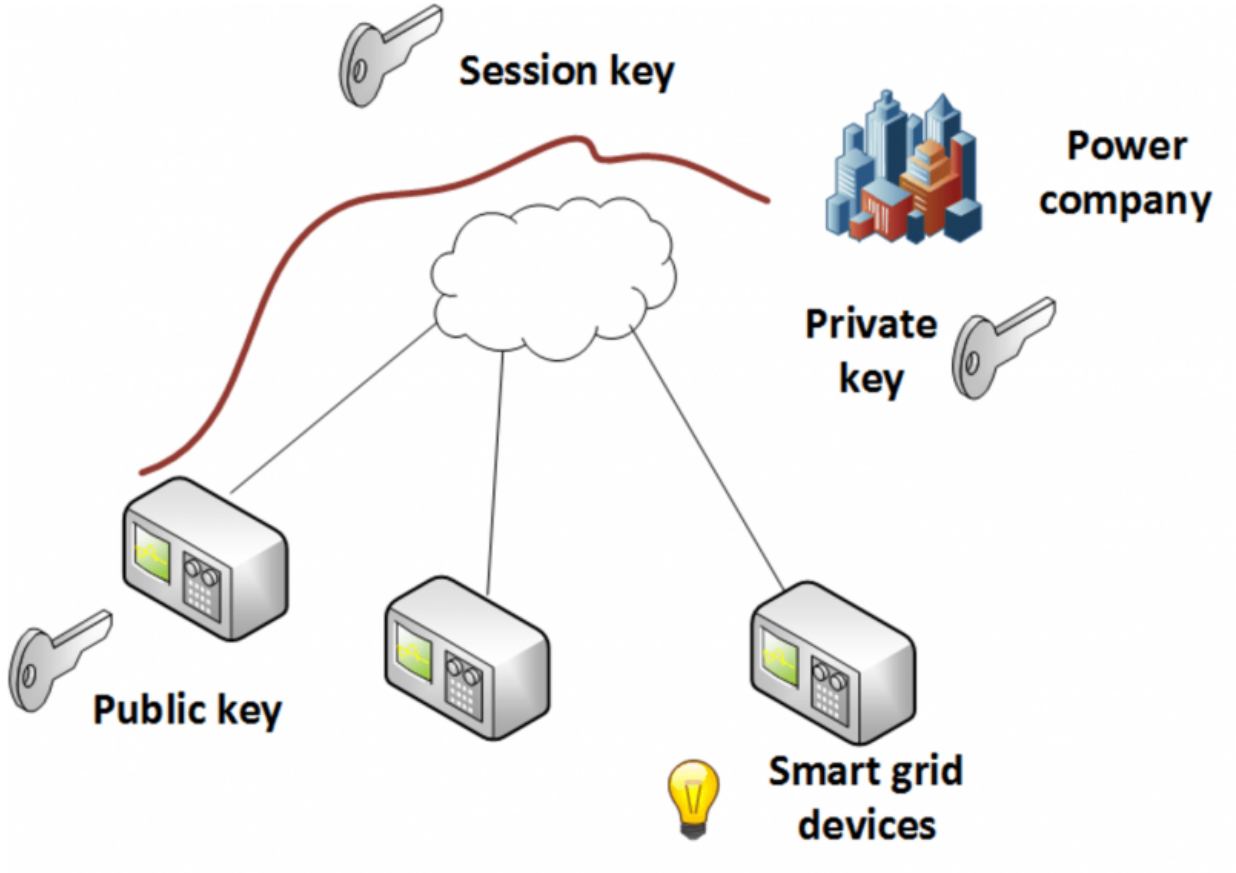
Smart grids, which include the smart meters being rolled out to millions of homes and the upstream equipment used by electricity suppliers, are often secured by the Open Smart Grid Protocol (OSGP), developed by the Energy Service Network Association (ESNA). It's estimated there are more than 4m devices using OSGP.

If there's one rule about cryptography it's that it is difficult to prove there are no weaknesses. Newly developed ciphers and methods are subjected to thorough cryptanalysis and peer review – and it's not advisable to try and re-invent the wheel and develop a new form of cryptographic method or cipher. And yet the ESNA did just that. Ever since OSGP was standardised in 2012 ESNA has been under fire for its decision, and now researchers have discovered just how bad that decision was.

What is the smart grid?

The smart grid is an internet of devices such as electrical meters and electricity distribution equipment. The idea is that network connectivity provides better monitoring of energy use, locating faults, and no need to send out someone to read the meter. But with this convenience comes the insecurity of being attached to the public internet – hence the need for protection.

Normally these devices communicate using secure tunnels. This shows a secure tunnel created between the power company and the home device.



Internet connected smart grid devices. Credit: Bill Buchanan, Author provided

The power company sends its public key to the smart meter, which creates a new session key, encrypts this with the power company's public key, and passes it back. The power company, using its private key, decrypts this to determine the session key for the connection. Both sides will then use their copies of the session key to encrypt traffic passed between them during the session.

If someone determines the private key of the power company, they can then find out the session key and read – even alter – the

communications. The same happened with the Superfish vulnerability, where the private key could be easily determined by trying a few well-known pass phrases.

What's the weakness?

The current problem with OSGP lies in ESNA's decision to cook up its own, flawed, cryptographic methods and its non-standard implementation of the RC4 cipher – rather than using any of the well-defined, well-designed cryptography standards that are available.

This vulnerability makes it easy to acquire private keys, something highlighted by academic researchers Philipp Jovanovic and Samuel Neves, who demonstrated how easy it was to crack OSGP's encryption using easy-to-implement key-recovery attacks.

Their focus was on the OMA digest, which is the core of the authentication infrastructure. A digest is a means of turning data into a cryptographic fingerprint, known as a hash, which is encrypted ("signed") using the secret, private key. There are many well-defined methods for this, such as HMAC-SHA256 and AES-GMAC, which use standard crytographic methods to produce a signed hash signature.

However, OSGP uses a combination of the OMA digest, the EN 14908 algorithm, and the RC4 cipher. The choice of RC4 seems strange, especially as it has known key- and plaintext-recovery attacks, but the home-brew OMA digest leaves the OSGP with security so weak that the researchers were able to recover private keys using just 13 queries.

We need better locks

For something as important as our energy infrastructure, where the tenth

decimal point can mean a cost of millions and where a large-scale outage could lead to serious economic losses, it's just incredible that ESNA has decided to go it alone and subsequently made a hash of it (if you'll excuse the pun).

OSGP is currently used in over 4m smart grid devices, which can now be seen as having little in the way of real security. As we scale-up the Internet of Things, there's a quite reasonable concern that too little thought has been given to how they will be secured.

Also, I think the public key infastructure we have created for the internet is deeply flawed, especially in the cryptographic methods used, many of which are past their useful life. While onion routing, as exemplified by Tor, often gets a bad press because of its use for nefarious activities in the deep web, it's methods are well-proven and secure.

We really need to start kicking the tyres of our internet infrastructure, pension off those aspects that are past their use-by date and introduce better, newer methods. The more that our economy goes online, the more is at stake. I can't see someone wishing to patch millions of smart meters or devices as new vulnerabilities are found, but can certainly imagine a load of rogue actors who'd take advantage of them.

This needs to be right, right from the outset. After all, there's no greater threat to the internet than no electricity to power it.

Source: The Conversation

Citation: When amateurs do the job of a professional, the result is smart grids secured by dumb

crypto (2015, May 15) retrieved 24 April 2024 from https://phys.org/news/2015-05-amateurs-job-professional-result-smart.html