14 May 2015, 5.10pm BST

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

AUTHOR

Bill Buchanan

Head, Centre for Distributed Computing, Networks and Security at Edinburgh Napier University

DISCLOSURE STATEMENT

Bill Buchanan does not work for, consult to, own shares in or receive funding from any company or organisation that would benefit from this article, and has no relevant affiliations.

Edinburgh Napier UNIVERSITY

Provides funding as a Member of The Conversation UK.
napier.ac.uk/Pages/home.aspx

Bright colours, dumb ideas. Cast 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). ItÕs estimated there are more than 4m devices using OSGP.

If thereÕs one rule about cryptography itÕs that it is difficult to prove there are no weaknesses. Newly developed ciphers and methods are **subjected to thorough cryptanalysis and peer review** Ð

Submissions) Ñ Melbourne, Victoria

Sydney School for Critical Social Thought Ñ North Sydney, New South Wales

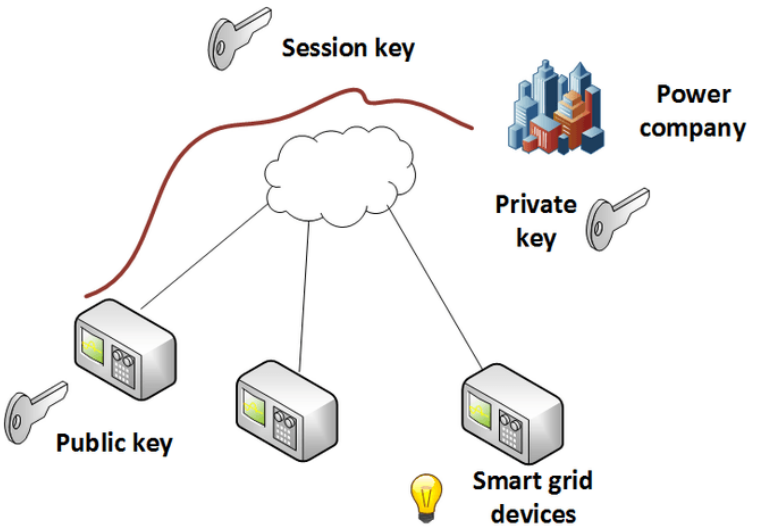
MORE EVENTS

and itÕs 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 Ð 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. 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 companyÕs 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 Ð even alter Ð the communications. The same happened with the **Superfish vulnerability**, where the private key could be easily determined by

Email
Twitter 17
Facebook 16
LinkedIn 48

2 Comments
Print

TAGS

Cyber security, Internet of Things, Cryptography, Smart grids

ARTICLES BY THIS AUTHOR

February 24 2015
LenovoÕs security debacle reveals blurred boundary between adware and malware

January 22 2015
If Obama is talking about securing the net, it should be on everyone elseÕs lips too

January 14 2015
If you seek to Ôswitch offÕ encryption, you may as well switch off the whole internet

November 24 2014
Codebreaking has moved on since TuringÕs day, with dangerous implications

November 5 2014
Better locks to secure our data are the inevitable result of too many prying eyes

RELATED ARTICLES

Online voting is convenient, but if the results aren't verifiable it's not worth the risk

trying a few well-known pass phrases.

What's the weakness?

The **current problem with OSGP** lies in ESNAÕs decision to cook up its own, flawed, cryptographic methods and its non-standard implementation of the RC4 cipher Ð 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 OSGPÕs 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 (ÒsignedÓ) 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, itÕs just incredible that ESNA has decided to go it alone and subsequently made a hash of it (if youÕll 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, thereÕs 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, itÕs methods are well-proven

‘Windows 10 on everything’ is Microsoft’s gambit to profit from its competitors

Has Tesla cracked the grid energy storage problem?

Manifesto Check: Plaid Cymru’s defence policy is ‘vague and uncosted’

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 canÕt 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 whoÕd take advantage of them.

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

Join the conversation

Sign in to comment

2 comments sorted by Oldest | Newest

lenod knarf
citizen

Only 4 million? I'm sure there are a lot more smart meters than that.also another critical issue is with a built-in disconnect switch they can ignite propane(see Hydro Quebec) and other gas, vapor.

a day ago ¥ report

George Michaelson
Person

I'm going with http://cryptech.is/ -a community driven HSM being designed by people I know, and so on a personal level trust to understand the design goals. Its an FPGA based design which has openly available Verilog/VHDL and its compontents, such as the random number generator are out there for people to test by themselves.

I know its not going to fix the core issue you talk about, but in the light of misplaced trust in the centrally managed crypto economy, I think its worth pursuing. I am particularly concerned about the fall from grace of NIST, in terms of their oversight of technology we

Read more

4 hours ago ¥ report