Central University Administration

Communication and Marketing Division

Press release

From	Katrina Jordan
Phone	+49 851 509 1439
Fax	+49 851 509 1433
E-mail	communication @uni-passau.de
Date	13 May 2015

Who Can Hijack Your Smart Meter? Weak Security Threatens Energy Grid

Recent findings by two security researchers, Philipp Jovanovic of the University of Passau (Germany) and Samuel Neves of the University of Coimbra (Portugal), have exposed major flaws in a widely deployed smart grid system. As it turns out, the Open Smart Grid Protocol (OSGP), an essential pillar of the energy distribution technology, does not deliver the security required for critical infrastructures, such as smart grids, that potentially connect meters in millions of homes. OSGP was originally developed by the Energy Service Network Association (ESNA) and became a standard of the European Telecommunications Standards Institute (ETSI) in 2012. It is currently deployed in over four million devices worldwide, according to members of OSGP Alliance.

In their paper Practical Cryptanalysis of the Open Smart Grid Protocol, presented at the annual workshop on Fast Software Encryption (FSE) in March 2015, Jovanovic and Neves identified multiple attack vectors which would allow an adversary to recover secret keys used in the underlying OSGP protocol. Using these, the attacker could decrypt the protected communication within the smart grid and might even take over control by manipulating exchanged messages. The attacks have varying levels of applicability and are based on different assumptions about the capabilities of an attacker. The most practical of the attacks merely requires that the adversary intercepts and slightly modifies encrypted messages to recover the secret key. Attackers would not need physical access to the smart meters themselves – remote communication is sufficient. These attacks make use of the fact that each message is checked for authenticity. The researchers showed that there is a dependency between the successful authentication of manipulated messages and the values of individual bits of the secret key. Exploiting this, as little as 168 manipulated encrypted messages are sufficient on average to fully expose the secret key.

“Basically, all our FSE’15 reviews pointed out how simple these attacks are on a conceptual level. We were quite a bit surprised that our paper got accepted in the end,” remarked Philipp Jovanovic, one of the co-authors of the paper. The success of the attacks is based on the weaknesses of the deployed cryptographic primitives and the way they are combined in OSGP. The RC4 stream cipher is used for encryption and the OMA Digest for message authentication. It has been already known for a long time that RC4 has security issues and

cryptographers have been advising for years against its usage. Due to the dwindling trust in its security, RC4 was recently prohibited for usage in TLS, the protocol that secures communication on the Internet (see RFC7465 for more information). However, the far more serious problem in OSGP is the OMA Digest. This is a homespun primitive which has been found to be extremely weak and cannot be assumed to provide any authenticity whatsoever, as explained in the paper. This function is also the main reason that the presented attacks are so exceptionally simple. Finally, the fact that the RC4 encryption keys are derived from the secret keys used in the OMA Digest leads to the complete compromise of OSGP.

“These attacks show once more that cryptographic primitives must undergo a thorough analysis by qualified scientists before deployment,” said Professor Ilia Polian, who supervises Philipp Jovanovic. Professor Polian holds the Chair of Computer Engineering and is the Dean of the Faculty of Computer Science and Mathematics. “This is not only a technological issue,” added Professor Gerrit Hornung (Chair of Public Law, IT Law and Legal Informatics and speaker of the University’s Institute of IT Security and Security Law). “Particularly in critical infrastructures like energy supply, the state is responsible for the prevention of security vulnerabilities. This is why we are discussing an EU Directive which aims at improving IT security in such infrastructures and obliges the providers to report incidents.” Hornung also believes that the described attack endorses the Institute’s interdisciplinary research approach, which looks at IT security from both the technical and the legal point of view: “There is a clear need for integrated work in this area.”

The researchers pointed out that the published attacks have been developed at the conceptual protocol level and have not been carried out in an actual smart grid installation. Demonstrating the attack would require access to proprietary hardware and substantial interfacing efforts. The uncovered weaknesses were communicated to OSGP Alliance members in November 2014. Although it is unlikely that these attacks have already been launched in practice, the warning signs are obvious. As Klaus Kursawe and Christiane Peters from the European Network for Cyber Security (ENCS) recently wrote in “Structural Weaknesses in the Open Smart Grid Protocol” an overview article on OSGP’s security which was released independently of the work of Philipp Jovanovic and Samuel Neves: “...like cracks in a dam — a last warning sign that something needs to be fixed before the real damage has been done.”

Notice for editors: Please address your enquiries about this press release to Philipp Jovanovic (jovanovic@fim.uni-passau.de) or the University's Media Relations Section, phone: +49 851 509 1439.