Response to BEIS Call for Evidence on a Smart, Flexible Energy System

Peter Bernard Ladkin PhD FIET
Professor of Computer Networks and Distributed Systems
at Bielefeld University,
Director, Causalis Limited,
Geschäftsführer (CEO), Causalis Ingenieurgesellschaft mbH
2016-11-17

I wish to respond to two questions, on p71 of the Call.

> Question 41. Can you provide evidence demonstrating how smart technologies (domestic or industrial/commercial) could compromise the energy system and how likely this is?
>
> Question 42. What risks would you highlight in the context of securing the energy system? Please provide evidence on the current likelihood and impact.

I shall answer both these questions together, and provide summary details at the end of this document of how I have done so.

Cybersecurity researchers at the Weizmann Institute in Israel have recently demonstrated how to take control of smart lightbulbs and reprogram their firmware to control their behaviour at will. They were able to do this with an entire building on the Weizmann campus when driving by in a car, also by means of a drone which they flew near the building. The technical paper is at http://www.wisdom.weizmann.ac.il/%7Eeyalro/iotworm/iotworm.pdf .

Key points are:

- The compromised devices were made by an established European hi-tech manufacturer, which has deep technical and financial resources, as well as a long-standing reputation for reliable product lines. It is not the first time that products which the average citizen would be likely to trust have been compromised.
- The compromised ZigBee protocol is one developed by a broad industry consortium, containing the “major players”, specifically for these kinds of uses. It is not the first example of a flawed protocol developed by such a consortium.
- The weaknesses were exploited through expert knowledge of cryptology (the design of crypto protocols) and cryptography (algorithms for encoding and decoding, as well as authenticating, the contents of confidential communications) in ways which the designers of the cryptology used in the devices did not anticipate. It is not the first time that experts have discovered exploitable weaknesses in industrial cryptography. Indeed, there is a whole mini-industry built up around doing so, with its own conferences and industrial fairs.

The scope of the attack is, however, new. The researchers explain how their specific attack can scale up from one building trivially to large numbers of buildings, potentially an entire city centre. Controlling a substantial number of electrical devices at will, an attacker can potentially cause power surges which would effect the electricity supply network.

Some mitigation can come through

- Diversity. Installing “smart” lightbulbs from ten different manufacturers rather than one would make a cracker’s task, say, ten times harder. But raising the hurdle does not mean eliminating it. The general experience in cybersecurity is that, with the passage of time, merely theoretical exploits become at some point practical.
- Rigour in digital-systems engineering. There are means of discovering flaws in communications protocols such as ZigBee through techniques such as model checking and other so-called “formal methods”. However, much of industry concerned with digital products still considers such rigourous methods too resource-intensive for the presumed benefits they bring, and does not use them. This has been true throughout the development of digital communications technologies, and is a factor in most cybersecurity vulnerabilities which have occurred in digital communications in the last twenty years. There is thereby a good argument for considering the prevalence of poor cybersecurity to be a “market failure”. The good news is that this can potentially be fixed – see below.

I emphasise that these are mitigations, not panaceas.

Questions arise about the scope of this demonstration.

- Is this a one-off? I do not believe so. Cybersecurity expert Bruce Schneier has pointed out in a recent article which originally appeared in the Washington Post how the characteristics of this attack generalise to other populations of “smart” building devices https://www.schneier.com/crypto-gram/archives/2016/1115.html#4
- Indeed, this attack is similar to, but more sophisticated in its outcomes than, many such compromises of smart devices. The so-called “Mirai” botnet, which consists of such compromised devices, has been used to construct successful “distributed denial-of-service” attacks on prominent cybersecurity authority Brian Krebs as well as a major provider, Dyn, of a key internet service known as DNS. We emphasise that these successful attacks targeting major installations run by major providers of communication services. In themselves, they were no threat to the electricity supply network. However, such attacks could in principle be targeted against a variety of key “smart” nodes in an electricity supply network, intended to produce a large outage in sum, with concomitant supply-network control problems.

In summary,

- Ad Question 41. I have shown, by means of one recent exploit and its feasible extension, that and how smart technologies can compromise the energy system. The likelihood of such compromises, in the current state of the art, is close to, or is, certainty.
- Ad Question 42. I would highlight the risk that large-area sectors of heavy variegated electricity use (e.g., large clusters of buildings, say in a city centre; I am not addressing here large industrial plants) can be commanded at will by external

entities, who could thereby cause uncontrolled and uncontrollable fluctuations in electric-power supply sufficient to cause large-scale outage in, or even damage, the large-area electricity-supply system (the “grid”).

If I may, I would also like to offer a view as to how this highly unsatisfactory, and potentially dangerous, situation could be addressed.

Concerning rigour in engineering and “market failure”, it has been pointed out by many, including Schneier op. cit., that market externalities are in play. The sufferers are those who undergo interruption of normal electricity-dependent services, and the power companies who have to mitigate the effects of such attacks. They are not, directly, the suppliers, installers, or providers of the compromised devices, nor the developers of the compromised protocols, all of which/whom lie in the causal chain leading to the damaging incident. The crackers, if they can be found, can be prosecuted somewhere for criminal offences and sanctioned, but it is notoriously hard to find such crackers and extradite them, and they are in fact in most current cases not sanctioned.

Could suppliers, installers, providers of compromised devices and developers of compromised protocols used in a damaging incident be held grossly negligent or negligent under existing civil and criminal law? I am not a legal expert, but I guess that such would be a hard case to make under current law. For example, a supplier which is ISO 9001 certified has development records, and these records would likely show for such a supplier as in the Weizmann vulnerability demonstration that they developed their kit as well as anybody and better than most. Similarly for the consortial development of the ZigBee protocol. In the case of safety-related systems based on digital technology, with which I am very familiar, this appears to be currently sufficient to avoid a successful accusation of negligence or gross negligence.

Some possible changes in the law might help to remedy the market failure, and to introduce more rigorous, more formal, methods in digital-systems engineering. The following possibilities are being discussed in the cybersecurity community:

- There could be a product security law along the lines of the existing product safety law stemming from EU Directive 765/2008.
- Suppliers of equipment with digital components could be made strictly liable for the exploitation of cybersecurity vulnerabilities in their products
- Developers of products involving digital components could be required to provide a security case for each of their products, along the lines of the safety case which is required under standards for many products which can engage in possibly damaging behaviour. However, safety cases can be poor (see the Nimrod incident, for example). Specific requirements, say for the appropriate use of model checking and other formal methods to assure objective properties of the digital components, could ensure the quality of the security case.

I suggest that such possible remedies be considered, as a means of mitigating the current, to me very unsatisfactory, bordering on dangerous, state of cybersecurity.