Speculative Future Energy Security Vulnerabilities Questionnaire

The intention of this study is to seek the opinions of experts in the energy sector and cyber security sector to assess and rate a number of speculative security/privacy events possible in a smart grid scenario (Table 1). The scenarios are based upon an assessment of academic literature and security appraisals of smart grids/smart metering.

Your responses and those of other panel members (who we will recruit independently) will be kept in strict confidence. In any publications produced from this research you will be identified only by the demographics provided below, e.g. "Power Engineer, 49 years old, 22 years experience working in an Australian energy network"

Please answer the questions below before filling out each row and column of Table 1. Any questions please email: s.snow@uq.edu.au or m.glencross@uq.edu.au

Demographics

Age (highlight correct bracket): 18-24 24-34 35-44 45-54 55-64 65+

Job title (e.g. power engineer):

Length of time working in organisation (years, months):

Length of time working in energy sector (years, months):

(If less than 2 years), specify previous employment sector:

State and country, I work in predominantly:

Existing security/privacy vulnerabilities

In your own words, what are the three biggest **security** threats currently facing the sector of the energy industry in which you work:

1:

2:

3:

Why are these the highest?:

In your own words, what are the three biggest **privacy** threats currently facing the sector of the energy industry in which you work:

1:

2:

3:

Why are these the highest?:

Speculative security/privacy vulnerabilities

1. Please read through Table 1 (below) in its entirety and complete points 2-6 below.

2. Please fill in the matrix for Likelihood, Consequence, Potential Entry Point(s) and insert comments regarding: (1) Why you consider this particularly feasible/likely or impossible/unlikely, (2) justify your assertions under the Likelihood and Consequence, and (3) provide further information, e.g. where/when this might happen (or why won't it happen), who is most vulnerable to the attack, and who might be most affected by it.

3. At the bottom of Table 1, add any potential privacy/security risks that are not already covered in Table 1 and fill in each column for them.

Table 1: Speculative potential energy network privacy/security vulnerabilities.

#	Scenario	Feasibility Rank between 1 (impossible) and 10 (has already happened)	What is the Likelihood of this event happening in the next 20 years Rank between 1 (extremely unlikely and 10 (almost certain)	Consequence- what are the harms from this? Rank between 1 (harmless) and 10 (catastrophic)	Comments Please justify your ratings here and add any further comments
1	Energy retailers sell high granularity energy data to insurance companies for improved insurance risk analyses				
2	Use of deception to distract command center and technician resources to allow for further cyber crime, or physical attacks such as forcing access to a substation or similar				
3	A security weakness in an IoT smart home device is used to gain full admin access to the household's smart meter or other behind-the-meter measurement technology; and from there, gain access to the computer systems of the energy utility				
3a	With access obtained to an energy utility's computer systems (see question 3): Large-scale data theft of personal data, account details and energy use details				

#	Scenario	Feasibility Rank between 1 (impossible) and 10 (has already happened)	What is the Likelihood of this event happening in the next 20 years Rank between 1 (extremely unlikely and 10 (almost certain)	Consequence- what are the harms from this? Rank between 1 (harmless) and 10 (catastrophic)	Comments Please justify your ratings here and add any further comments
	(similar to the Yahoo attacks of 2013, 2014, and 2016)				
3b	With access obtained to an energy utility's computer systems (see question 3): Hackers use the compromised energy utility systems to gain access to network providers systems to shut off a network sector's electricity, other large-scale attacks				
4	Automotive electric charging infrastructure is hacked overnight, preventing cars from being charged and causing wide scale disruption to commuters the next morning				
5	Disruptors hack the Bureau of Meteorology's industry API arm, sending erroneous weather data to energy networks, causing them to greatly under-estimate the expected load of solar and wind, resulting in multiple transformers				

#	Scenario	Feasibility Rank between 1 (impossible) and 10 (has already happened)	What is the Likelihood of this event happening in the next 20 years Rank between 1 (extremely unlikely and 10 (almost certain)	Consequence- what are the harms from this? Rank between 1 (harmless) and 10 (catastrophic)	Comments Please justify your ratings here and add any further comments
	tripping and other safety issues associated with over-voltage on the grid				
6	Historic energy use data used as evidence in court, e.g., proof someone was at home/on their computer at a given time and date				
7	A household in 2019 agrees to sharing sub-second energy use information based on knowledge of what can be gleaned from it in 2019. Re-analysis of the data in 2029 with greatly improved disaggregation techniques (to the level of individual LED energy signatures on OLED TV's) finds evidence of household member streaming illegal on the TV 10 years ago and info is sent to police to prosecute				
8	Multiple burglaries occur when a security weakness/ vulnerability is identified in a commercial smart home device, allowing criminals to remotely disable security alarms and unlock IoT door locks				

#	Scenario	Feasibility Rank between 1 (impossible) and 10 (has already happened)	What is the Likelihood of this event happening in the next 20 years Rank between 1 (extremely unlikely and 10 (almost certain)	Consequence- what are the harms from this? Rank between 1 (harmless) and 10 (catastrophic)	Comments Please justify your ratings here and add any further comments
9	Hackers gain access to network command centre				
9a	*[Answer only if likelihood for Q9 is not rated as 0-"impossible"] having gained access to network command center, hackers shut off power to suburbs. (note this may enable terrorist activity/mass burglary/other crime)*				
10	Online/remote theft of power (individual(s) taking power without being billed)- enabled by hacked access to energy networks				
11	Physical theft of power by using street-based, super-high voltage EV chargers to charge multiple batteries which are then transported elsewhere, so the theft cannot be traced to a specific house once the authorities realise there has been a theft				
12	Supply chain security: Overseas-manufactured smart meters have malware or nefarious hardware modifications inserted in them during manufacture. This				

#	Scenario	Feasibility Rank between 1 (impossible) and 10 (has already happened)	What is the Likelihood of this event happening in the next 20 years Rank between 1 (extremely unlikely and 10 (almost certain)	Consequence- what are the harms from this? Rank between 1 (harmless) and 10 (catastrophic)	Comments Please justify your ratings here and add any further comments
	would mean 10,000'|s of compromised smart meters rolled out over a city. Could be used for (1) simultaneous deactivation causing manipulation of demand frequency attack, or (2) theft of data				
13	Manipulation of demand attack: Botnet-style malicious commandeering and simultaneous activation/de-activation of thousands of vulnerable high-power smart home devices (eg iot enabled air conditioners or water heaters) to cause frequency disruption				
14	Attacks on the hardware/firmware of a smart meter: Computer worm phlash (permanently disable or "brick") smart meters, meaning power cannot be restored until the smart meter is replaced				
15	Attacks on the metrology system of a smart meter: Energy theft, or cover-up of hydroponic labs, etc..				

#	Scenario	Feasibility Rank between 1 (impossible) and 10 (has already happened)	What is the Likelihood of this event happening in the next 20 years Rank between 1 (extremely unlikely and 10 (almost certain)	Consequence- what are the harms from this? Rank between 1 (harmless) and 10 (catastrophic)	Comments Please justify your ratings here and add any further comments
16	Hackers gain full admin access to many household's smart meters				
16a	Using NILM on the smart metered data, hackers determine the use of Sleep Apnea machines or other life support equipment				
16b	Hackers commit remote murder through turning off power to the house remotely through their (hacked) smart meter during the night				
	ADD ANY ADDITIONAL THREATS YOU FEEL ARE SALIENT				