CENTRE FOR DOCTORAL TRAINING in CYBER SECURITY
EPSRC Engineering and Physical Sciences Research Council
UNIVERSITY OF OXFORD
ANJULI R. K. SHERE
ANJULI.SHERE@CYBERSECURITY.OX.AC.UK

"SECURITY SHOULD BE THERE BY DEFAULT": INVESTIGATING HOW JOURNALISTS PERCEIVE AND RESPOND TO RISKS FROM THE INTERNET OF THINGS (IoT)

Shere ARK, Nurse JRC and Flechais I (2020) "Security should be there by default": Investigating how journalists perceive and respond to risks from the Internet of Things. The 5th European Workshop on Usable Security, Genova, Italy, 7 September 2020, p. 12. IEEE. Available at: https://eusec20.cs.uchicago.edu/eusec20-Shere.pdf.

BACKGROUND

Rapid growth of IoT technologies and associated attack surfaces compounds existing problems for journalists:

1.1tn	USD value of projected global IoT spending in 2023
115bn	USD value of consumer spending on domestic IoT in 2020
9%	of global population lives in countries with "satisfactory" or "good" press freedom
59%	more journalists killed in countries at peace than in war-zones in 2019

UNESCO's Survey of Selected Issues affecting the digital security of journalists noted three threats of the increasing ubiquity of the IoT:

- Attack technologies are becoming less expensive and more pervasive;

- Location tracking technology can identify journalists and their sources;

- Compromised user accounts and devices can be used to identify sources and networks

RESEARCH QUESTIONS

1. To what extent do journalists perceive threats from the IoT?

2. What protective tools and methods do journalists feel are currently effective in increasing their cyber security against all perceived cyber-threats, including any from the IoT?

3. Are the protective measures reported as in use by journalists effective, when compared to the known recommendations from contemporary literature and experts in cyber security?

METHODOLOGY

1. Interviewed and surveyed 16 media experts to discuss their perceptions of IoT threats and what relevant security and privacy behaviours have been adopted

2. Surveyed 34 cyber security experts to assess if and how it may be possible to minimise or mitigate IoT threats

3. Thematically coded and analysed results

FINDINGS FROM MEDIA PARTICIPANTS

1. Media participants' awareness of specific IoT threats was low, but they still expressed fear at device capabilities.

I4: "My assumption is always that the more devices you have, the more entry-points for attackers, just like if there are more windows in your house there are more entry-points for burglars".

All ten journalist interviewees (I1-I9, I11) were concerned that the spread of casual-use IoT devices could remove the confidentiality of source-journalist interactions.

2. Other than minimisation of IoT purchases, no protective measures were identified as specifically to counter IoT threats.

Journalists who understand these threats are unsure how to mitigate them and disclosed that they are returning to analogue methods of working (e.g. use of dead-drops, pen and paper) instead.

Media respondents' techniques for minimising threats resulting from the IoT mainly focused on disconnecting devices and disabling applications when not in use.

I9 mentioned taking Faraday cage bags to meet sources. Interviewees also mentioned using covers over cameras to physically limit the photo-taking functionality of IoT devices.

I7: Having to avoid IoT devices is regressive for newsgathering, as these technologies, "would make the job easier and give us access to sources who were further away or evidence that is harder to find".

FINDINGS FROM CYBER SECURITY EXPERTS

Of our 34 expert respondents, 20 (58.8%) felt that members of the public could not currently opt out of the use of the IoT in some way.

Moreover, 26 (76.5%) felt that within five years the public would find it almost impossible to opt out of having their information vulnerable to IoT devices, even if they avoided personal ownership of them.

Can the public currently opt out of the use of the IoT?

Will the public be able to opt out of having information vulnerable to IoT in 5 years?

The cyber security experts recommend:

1. Prioritising education about potential IoT threats

2. Lobbying governments and industry to create standards, e.g. security and privacy by design, lifecycle and update considerations

3. Activism to push for protective legislation and public education