REPHRAIN

Protecting citizens online

Home Office consultation: Unauthorised access to online accounts and personal data

This is a submission from the REPHRAIN centre. Specifically, the following contributed to the formulation of this response (in alphabetical order): Prof Madeline Carr, Dr Alicia Cork, Dr Ola Michalec, Prof Steven Murdoch, Prof Jason Nurse, Prof Awais Rashid, Yvonne Rigby, Dr Daniel Woods.

October 2022

UK Research and Innovation · University of Bristol · UCL · The University of Edinburgh · King's College London · University of Bath

Open Consultation: Unauthorised access to online accounts and personal data

(Home Office call for information)

Introduction

Thank you for an opportunity to provide our response to this call for evidence. We are writing on behalf of REPHRAIN, the National **Re**search Centre on **P**rivacy, **H**arm **R**eduction and **A**dversarial **I**nfluence O**n**line. REPHRAIN is the UK's world-leading interdisciplinary community focused on the protection of citizens online. As a UKRI-funded National Research Centre, we boast a critical mass of over 100 internationally leading experts at 13 UK institutions working across 37 diverse research projects and 23 founding industry, non-profit, government, law, regulation and international research centre partners. As an interdisciplinary and engaged research group, we work collaboratively on addressing the three following missions:

- Delivering privacy at scale while mitigating its misuse to inflict harms
- Minimising harms while maximising benefits from a sharing-driven digital economy
- Balancing individual agency vs. social good.

We are addressing this consultation since our researchers have extensive expertise in the regulatory aspects of cyber security, measuring and defining harms, and evaluating authentication solutions. This is a submission from the REPHRAIN centre. Specifically, the following contributed to the formulation of this response (in alphabetical order): Prof Madeline Carr, Dr Alicia Cork, Dr Ola Michalec, Prof Steven Murdoch, Prof Jason Nurse, Prof Awais Rashid, Yvonne Rigby, Dr Daniel Woods. We are happy to arrange a follow up meeting to provide details of our work in progress in the area (specifically, developing "i) appropriate security measures which account providers and organisations processing personal data could implement to ensure users' accounts and their personal data are better protected against attack; and ii) compliance with those measures").

1. **Which online harms from unauthorised access are the most concerning and likely?**

Our state-of-the-art resource, the REPHRAIN Map of Online Harms (https://rephrain-map.co.uk/) outlines a number of most concerning harms to citizens related to the use of digital technologies. The map categorises harms according to their sources, with multiple harms connected to unauthorised access. Each harm is described, together with references to current research challenges, projects and external publications (e.g., peer reviewed publications or white papers).

The Map is a living resource co-designed with our extended community of app. 100 researchers and partners with expertise in policy and civil service. We welcome comments on our work-to-date and invite you to make the most of the website during your consultation.

We would specifically like to outline the following harms to citizens:

- Financial fraud (e.g., through phishing, probing for personal information)
- Child abuse (e.g., through leaking explicit image)
- Gendered violence (e.g., revenge porn, leaking explicit images, use of stalkerware)
- General harms to wellbeing and reputation (e.g., through leaking private documents, doxxing, impersonation)
- Harms to democracy (through surveillance of activists and other citizens)

The above harms can occur as a result of criminal activities, interpersonal conflicts, politically motivated activities or even due to the incorrect legal presumption of correct operation of computer systems (I.e., where citizens are wrongly attributed to an unlawful activity as a result of computer error – Bohm et al., 2022).

In terms of impacts on health our systematic review reported that victims of cyber stalking and/or harassment experienced a multitude of harmful and detrimental consequences for their mental health, including depression, anxiety, suicidal ideation, and panic attacks. Victims recounted the lack of support they received from the criminal justice system and their subsequent distrust of technology post abuse. There is a critical need to devise practical solutions to tackle and minimize this victimization. Furthermore, adult education concerning safer technology use should be a priority (Stevens et al., 2021; Bada and Nurse; 2020).

Defining and measuring the impact of online harms is challenging due to conflation of terms used by multiple taxonomies. A taxonomy designed by a team of REPHRAIN researchers aims to tackle that, while allowing to better anticipate future harms to citizens as well as cascading risks (Cork et al, 2022). Further, a taxonomy of online harms to organisations proposes a set of analytical tools to conceptualise issues like unauthorised access: identifying corporate assets, linking these to different types of cyber-harm, measuring those harms and, finally, considering the security controls needed for the treatment of harm. This taxonomy could be used to conceptualise harms to businesses, rather than citizens. (Agrafiotis et al, 2018).

The government ought to consider the emerging harms from virtual reality (VR) and augmented reality technologies (AR). For example, as more VR technologies develop to allow users to create realistic avatars, the biometric data and unauthorised access to it pose quite distinct risks, e.g., advanced capabilities for impersonation. As VR becomes more common across different settings (e.g., social settings, work settings etc), this risk may escalate. We are currently working on anticipating harms from unauthorised access to AR and VR and happy to provide further references upon request.

Finally, it is important to highlight that the notion of ‘unauthorised access’ is politically contested. For example, it is a matter of an ongoing debate whether security authorities should be able to bypass end-to-end encryption in public communication technologies in order to aid with criminal investigations as this has serious implications for personal liberties and the right to privacy in a democratic society.

References:

- Blythe, J. M., & Johnson, S. D. (2021). A systematic review of crime facilitated by the consumer Internet of Things. Security Journal, 34(1), 97-125.

https://discovery.ucl.ac.uk/id/eprint/10082564/1/SR%20crime%20facilitated%20by%20IoT%20OPEN%20ACCESS.pdf
- Stevens, F., Nurse, J. R., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. Cyberpsychology, Behavior, and Social Networking, 24(6), 367-376. https://www.liebertpub.com/doi/10.1089/cyber.2020.0253
- Cork, A., Smith, L. G., Ellis, D., Fraser, D. S., & Joinson, A. (2022). Rethinking Online Harm: A Psychological Model of Contextual Vulnerability. https://psyarxiv.com/z7re2/
- Bohm, N., Christie, J., Ladkin, P. B., Littlewood, B., Marshall, P., Mason, S., ... & Thomas, M. (2022). The legal rule that computers are presumed to be operating correctly–unforeseen and unjust consequences. https://journals.sas.ac.uk/deeslr/article/view/5476
- Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity, 4(1), tyy006. https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288
- Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In Emerging cyber threats and cognitive vulnerabilities (pp. 73-92). Academic Press. https://www.sciencedirect.com/science/article/pii/B9780128162033000046

2. **Who do you believe should be responsible for ensuring account providers and other organisations processing personal data implement better protection, to reduce levels of cyber crime?**

We believe the government ought to set up the liability regime such that responsibility falls on the right party and let them take appropriate action:

> *"To improve security, responsibilities should be assigned to parties that could effectively discharge them, and could afford to do so. Consumers typically have the least capacity to mitigate risks, while service providers can improve security through system design and implementation, and by taking careful account of real-world use of their products. In most cases this means liability regimes should protect consumers, and prevent system operators from shifting liability to individuals where it is not reasonable to do so. All parties will also need to more clearly understand their responsibilities and potential liabilities if they are to take action to reduce risks."* (The Royal Society)

Responsibilisation (I.e., individualisation of risk, advising citizens how to take care of themselves, and then leaving them to face the consequences if they choose not to follow the advice of cyber security) is, we believe, contributing to the global success of cyberattacks. There is, consequently, a case to be made for governments taking a more active role than the mere provision of advice, which is the case in many countries (Renaud et al., 2018). We, therefore, agree with the proposals to reduce the burden on citizens.

The emerging regulations and industry standards could be key to driving an increased level of security across providers and other organisations. Interesting examples of this can be seen with the GDPR, the NIS Regulations, or the draft Energy Smart Appliances standard. Our current research highlights issues with operationalising security regulations to new domains and context (Michalec et al, in review). There is a tension between prescriptive and outcome-based regulations or standards. Prescriptive standards and regulations outline baseline minimum requirements which is beneficial for stakeholders without previous security expertise who need support in understanding what good level of security provision looks like. However, prescriptive governance is critiqued for its tendency towards technocratic measures and inflexibility in the face of fast-paced technology development. On the other hand, outcome-based regulations outline ideal high-level principles or security without specifying how to achieve them. They allow a degree of interpretation to suit a given context and evolve and technologies develop. However, they're critiqued for excess subjectivity and difficulties with benchmarking (I.e. understanding what 'good security' looks like across the sector and comparison between organisations). We are happy to provide a draft article upon request.

References

- Renaud, K., Flowerday, S., Warkentin, M., Cockshott, P., & Orgeron, C. (2018). Is the responsibilization of the cyber security risk reasonable and judicious?. Computers & Security, 78, 198-211. https://doi.org/10.1016/B978-0-12-816203-3.00004-6
- The Royal Society (n.d.) Progress and research in cybersecurity Supporting a resilient and trustworthy system for the UK https://royalsociety.org/-/media/policy/projects/cybersecurity-research/cybersecurity-report-summary.pdf
- Michalec, O., Shreeve, B. and Rashid, A. (in review). Cyber Security Visions of Future Energy Systems: Design, Support Function or Public Trust? The ACM CHI Conference on Human Factors in Computing Systems

3. **Do you have any comments on using more than one authentication factor when logging into accounts?**

We offer a few comments with regards to usability and feasibility of MFA:

- Usability is a critical element of effectiveness but is commonly not properly considered, for example posing unrealistic expectations for memory factors (Murdoch et al., 2016).
- Furthermore, it is also worth noting here that there has recently been an increase in attacks aimed at bypassing MFA (Dark Reading, 2022).
- Finally, we stress that 'usability' of MFA ought to be considered in the social context, rather as a solely cognitive issue. This means considering accessibility of MFA for people without access to devices, with disabilities or other ways of social marginalisation. Authentication tools should first and foremost facilitate access to services, especially if these are essential services such as benefits, pensions or asylum seekers assistance (Coles-Kemp and Jensen, 2019).

References

- Murdoch et al. Are Payment Card Contracts Unfair? Financial Cryptography and Data Security, 2016. https://murdoch.is/papers/fc16cardcontracts.pdf
- Dark Reading (2022) Uber: Lapsus$ Targeted External Contractor With MFA Bombing Attack https://www.darkreading.com/attacks-breaches/uber-breach-external-contractor-mfa-bombing-attack.
- Coles-Kemp, L., & Jensen, R. B. (2019, May). Accessing a new land: Designing for a social conceptualisation of access. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-12).

4. **Have you conducted any research or studies relevant to this call for information which you would be willing to share with us?**

Authentication tools

- https://arxiv.org/abs/1309.5344 De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2013). A comparative usability study of two-factor authentication. arXiv preprint arXiv:1309.5344.
- https://arxiv.org/abs/1501.04434 Krol, K., Philippou, E., De Cristofaro, E., & Sasse, M. A. (2015). "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. arXiv preprint arXiv:1501.04434.
- https://dl.acm.org/doi/10.1145/3428121 Mathis, F., Williamson, J. H., Vaniea, K., & Khamis, M. (2021). Fast and secure authentication in virtual reality using coordinated 3d manipulation and pointing. ACM Transactions on Computer-Human Interaction (ToCHI), 28(1), 1-44.
- https://ieeexplore.ieee.org/document/8797862/ George, C., Khamis, M., Buschek, D., & Hussmann, H. (2019, March). Investigating the third dimension for authentication in immersive virtual reality and in the real world. In 2019 ieee conference on virtual reality and 3d user interfaces (vr) (pp. 277-285). IEEE.

Gendered violence and Intimate Parter Violence

- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3350615 Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., & Tanczer, L. (2019). 'Internet of Things': How abuse is getting smarter.
- https://dl.acm.org/doi/abs/10.1145/3368860.3368861 Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019, September). Usability analysis of shared device ecosystem security: informing support for survivors of IoT-facilitated tech-abuse. In Proceedings of the new security paradigms workshop (pp. 1-15).
- https://doi.org/10.1332/239868021X16290304343529 Tanczer, L. M., López-Neira, I., & Parkin, S. (2021). 'I feel like we're really behind the game': perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse. Journal of gender-based violence, 5(3), 431-450.

- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8318057/ McManus, S., Bebbington, P. E., Tanczer, L., Scott, S., & Howard, L. M. (2021). Receiving threatening or obscene messages from a partner and mental health, self-harm and suicidality: results from the Adult Psychiatric Morbidity Survey. Social psychiatry and psychiatric epidemiology, 1-11.
- https://www.emerald.com/insight/content/doi/10.1108/978-1-83982-848-520211049/full/pdf?title=threat-modeling-intimate-partner-violence-tech-abuse-as-a-cybersecurity-challenge-in-the-internet-of-things Slupska, J., & Tanczer, L. M. (2021). Threat modeling intimate partner violence: tech abuse as a cybersecurity challenge in the Internet of Things. In The Emerald International Handbook of Technology-Facilitated Violence and Abuse. Emerald Publishing Limited.
- https://www.liebertpub.com/doi/10.1089/cyber.2020.0253 Stevens, F., Nurse, J. R., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. Cyberpsychology, Behavior, and Social Networking, 24(6), 367-376.
- https://pure.port.ac.uk/ws/portalfiles/portal/50080933/Home_office_FINAL_report.pdf Sugiura, L., Button, M., Tapley, J., Frederick, B., Blackbourn, M. D., Hawkins, C., & Belen-Saglam, R. (2021). Computer Misuse as a Facilitator of Domestic Abuse.

Child abuse

- Peersman and Rashid, AI-based advances for law enforcement's response to Online child sexual exploitation and abuse in Southeast Asia – grant announcement, (https://www.end-violence.org/grants/university-bristol-regional)
- https://doi.org/10.1016/j.diin.2016.07.002 iCOP: Peersman, C., Schulze, C., Rashid, A., Brennan, M., & Fischer, C. (2016). iCOP: Live forensics to reveal previously unknown criminal media on P2P networks. *Digital Investigation*, *18*, 50-64.
- https://eprints.lancs.ac.uk/id/eprint/132107/1/2018peersmanphd.pdf Peersman (2018) Detecting deceptive behaviour in the wild: text mining for online child protection in the presence of noisy and adversarial social media communications; PhD thesis
- Peersman, C., De Cristofaro, E., May-Chahal, C., McConville, R., Llanos, J.T. and Rashid, A (2022) Scoping the Evaluation of CSAM Prevention and Detection Tools in the Context of End-to-end encryption Environments; . https://cpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/1/670/files/2022/07/Scoping-the-Evaluation-of-CSAM-Prevention-and-Detection-Tools-in-the-Context-of-End-to-end-encryption-Environments.pdf

Policy

- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978692/The_UK_code_of_practice_for_consumer_IoT_security_-_PETRAS_UCL_research_report.pdf Datta Burton, S.., Tanczer, L.M., Vasudevan, S., Hailes, S., Carr, M. (2021). The UK Code of Practice for Consumer IoT Security: 'where we are and what next'. The PETRAS National Centre of Excellence for IoT Systems Cybersecurity. DOI: 10.14324/000.rp.10117734

- https://discovery.ucl.ac.uk/id/eprint/10132828/1/Lessons_from_the_GDPR_in_the_COVID_19_er.pdf Rana, O., Llanos, J., & Carr, M. (2021). Lessons from the GDPR in the COVID-19 era. Academia Letters, 1-6.
- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8884963 Shukla, M., Johnson, S. D., & Jones, P. (2019, June). Does the NIS implementation strategy effectively address cyber security risks in the UK?. In 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-11). IEEE.
- https://www.usenix.org/system/files/soups2020-michalec.pdf Michalec, O. A., Van Der Linden, D., Milyaeva, S., & Rashid, A. (2020). Industry Responses to the European Directive on Security of Network and Information Systems ({{{{{NIS}}}}}: Understanding policy implementation practices across critical infrastructures. In Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020) (pp. 301-317).
- https://murdoch.is/papers/ieeesp12warereport.pdf Murdoch, S. J., Bond, M., & Anderson, R. (2012). How certification systems fail: Lessons from the Ware report. IEEE Security and Privacy, 10(6), 40.

Education and communication

- https://groups.inf.ed.ac.uk/tulips/papers/massano2020.pdf Mossano, M., Vaniea, K., Aldag, L., Düzgün, R., Mayer, P., & Volkamer, M. (2020, September). Analysis of publicly available anti-phishing webpages: contradicting information, lack of concrete advice and very narrow attack vector. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 130-139). IEEE.
- https://doi.org/10.1093/cybsec/tyz005 Blythe, J. M., Sombatruang, N., & Johnson, S. D. (2019). What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?. Journal of Cybersecurity, 5(1), tyz005.

Financial fraud

- https://dl.acm.org/doi/10.1145/3041021.3053891 Whitty, M., Edwards, M., Levi, M., Peersman, C., Rashid, A., Sasse, A., ... & Stringhini, G. (2017, April). Ethical and Social Challenges with developing Automated Methods to Detect and Warn potential victims of Mass-marketing Fraud (MMF). In Proceedings of the 26th International Conference on World Wide Web Companion (pp. 1311-1314).
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3984005 Woods et al. (2021) Quantifying Privacy Harm via Personal Identity Insurance .Analysis of personal identity insurance shows US insurers rarely exclude losses based on policyholder behaviour (e.g. installing security software), suggesting insurers believe identity theft is largely outside the control of individuals; Daniel Woods
- 10.1109/TIFS.2019.2930479 Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2019). Automatically dismantling online dating fraud. *IEEE Transactions on Information Forensics and Security*, *15*, 1128-1137.

Threats to democracy

- https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf Nagaraja, S., & Anderson, R. (2009). The snooping dragon: social-malware surveillance of the Tibetan movement (No. UCAM-CL-TR-746). University of Cambridge, Computer Laboratory.
- https://ore.exeter.ac.uk/repository/handle/10871/129654 Cybercrime vs Hacktivism: Do we need a differentiated regulatory approach?; Farmer (Phd thesis)
- https://doi.org/10.1080/17419166.2017.1423472 Jones, R., Raab, C. & Székely, I. (2018), 'Surveillance and resilience: Relationships, dynamics and consequences', *Democracy and Security*, Vol. 14(3): 238-275.

General work on harms

- Ioannis Agrafiotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, David Upton, A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, Journal of Cybersecurity, Volume 4, Issue 1, 2018, tyy006, https://doi.org/10.1093/cybsec/tyy006
- Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In *Emerging cyber threats and cognitive vulnerabilities* (pp. 73-92). Academic Press.

5. Do you have any additional comments you would like to add about current Government regulations and initiatives to mitigate cyber crime and protect people online? (see "The aims of this government intervention" in https://www.gov.uk/government/consultations/unauthorised-access-to-online-accounts-and-personal-data/call-for-information-unauthorised-access-to-online-accounts-and-personal-data#about-this-call-for-information)

We agree with the overarching government aim **"to reduce the burden of cyber security on citizens and reduce harms to citizens from unauthorised access and associated harms"**.

"The Home Office believes cyber crime, and the offences facilitated by it, could be substantially reduced via more widespread implementation of secure-by-default principles to protect user accounts and their personal information."

- We support the intention to introduce secure-by-default principles. In particular, we encourage knowledge exchange between the Home Office and the NCSC actors working on Cyber Essentials as well as the DCMS stakeholders working on the IoT security standards. However, we'd like to caution that the 'secure by design' paradigm risks shrinking the stakeholder circle to a small group of technical experts effectively "hardcoding" the right to privacy and security. There might be challenges with sufficient determination of mutlifaceted and contextualised risks to diverse citizens that would be then translated into security controls (Michalec et al., 2021).

"The Home Office also intends to explore options to ensure that providers of online services and accounts, as well as processors and holders of UK citizens' personal data, exercise an appropriate and proportionate degree of responsibility for the protection required of the data, and access to it. This would mean exploring supplementing the current approach to the protection of data, under the Data Protection Act and GDPR, with a greater understanding and consideration of the risk to individuals of the compromise of their data held by organisations."

- We support this notion and welcome further comments on the proposals in the area. Our recent work on the notion of 'appropriateness and proportionality' (based on a case study of the NIS Regulations) shows challenges with arriving at a shared understanding of this clause and risks of excessive subjectivity (Michalec et al, 2021a, 2021b, 2022).
- As noted above, it is important to highlight that the notion of 'unauthorised access' is politically contested. For example, it is a matter of an ongoing debate whether security authorities should be able to bypass end-to-end encryption in public communication technologies in order to aid with criminal investigations as this has serious implications for personal liberties and the right to privacy in a democratic society

"In considering potential new measures, we are keen to ensure that existing and future proposals meet the needs of all users, not just those with good computer literacy. No-one should be inadvertently excluded from a platform by enhanced security measures, nor should new security measures unduly interfere with UK citizens' access to, ease of use, or enjoyment of the internet."

- We agree that inclusivity, usability and accessibility of the proposals ought to be at the forefront of this initiative. In particular, we call for heightened efforts to engage with underserved populations and community groups. Our evidence from the security standardisation work in the area of Energy Smart Appliances shows that there is still a significant gap between contributions from the industrial stakeholders and civil society actors. (Michalec et al., in review).

References

- Michalec, O., Shreeve, B. and Rashid, A. (in review). Cyber Security Visions of Future Energy Systems: Design, Support Function or Public Trust? The ACM CHI Conference on Human Factors in Computing Systems
- Michalec, O., Milyaeva, S. and Rashid, A. (2022) When the future meets the past: can safety and cyber security coexist in modern critical infrastructures? Big Data and Society. https://doi.org/10.1177/20539517221108369
- Michalec, O., Milyaeva, S. and Rashid, A. (2021) Reconfiguring governance: How cyber security regulations are reconfiguring water governance. Regulation and Governance. https://doi.org/10.1111/rego.12423
- **Michalec,** O., van der Linden, D., Milyaeva, S. and Rashid, A. (2020) Industry Responses to the European Directive on Security of Network and Information Systems (NIS): Understanding policy implementation practices across critical infrastructures. *Symposium on Usable Privacy and Security*;

6. Do you foresee any overlaps or risks between such other programmes, and the work on authorised access being considered in this Call for Information?

N/A

7. Are there other issues you think we should take into consideration as part of this call for information?

To conclude, we suggest that further regulatory work on preventing unauthorised access considers the nuanced contexts of different citizens (e.g., their literacy, ownership of accounts and devices, access to stable internet connection, age etc.). This could be particularly important when designing multi-factor authentication requirements, where some citizens might not have the same agency to benefit from MFA. We, therefore, highlight the need to develop security and privacy regulations with a capability approach in mind (Chowdhury *et al*., 2022)

Reference:

- Chowdhury, P. D., Hernández, A. D., Ramokapane, M., & Rashid, A. (2022). From Utility to Capability: A New Paradigm to Conceptualize and Develop Inclusive PETs. In *New Security Paradigms Workshop*. Association for Computing Machinery (ACM).