— HACKATHON CHALLENGE —

BRIDGING THE GAP BETWEEN MAKING AND BREAKING

Arne Padmos

Context. Compared to the popularity of both hackathons and CTF challenges, as well as the impact that AES has had and that NIST's PQC selection is expected to have, very little research has been done on what we call, for lack of an established term, adversarial engineering design competitions. This is unfortunate, as such competitions appear to be a useful tool for assured technology transfer. Given that NIST will review their guidelines for cryptographic standards development this year, it would be opportune as a WEIS community to explore and provide insights into how the shape of competitions can influence incentives and drive assurance.

Challenge. Can we use competitions to improve the state of security, and if so, how might we structure competitions to include both defensive and offensive aspects in order to bridge the divide between the making and breaking of computer systems?

Concept. Competitions that focus on breaking stuff are a common occurrence at many security conferences, reflecting our field's focus on looking for problems over working on structural solutions. While some competitions focus on security by design, an extensive literature search indicates that there is very little effort around combining both building and breaking of systems. The call for hackathon challenges at WEIS is a case in point, in that it only mentions the generation of ideas and not a concurrent adversarial process for evaluating their effectiveness. As to the few competitions that do combine offence and defence, most are more like implementation challenges than design challenges. We propose exploring how the idea of adversarial engineering design competitions, charrettes, or sprints can incentivise and align both security engineering and assurance efforts. Maybe these ideas could even apply to policy problems, inspiring future WEIS hackathons.

Audience. Security economics and related fields seem to be very fitting disciplines for providing input on different options as to the shape of adversarial engineering design competitions, including potential trade-offs and relevant frameworks. Such competitions might also be a rich field for gathering insights into, and testing the predictions of, the effects of incentive structures on security outcomes, helping to put security economics on a more solid empirical foundation. Both the limited research into competition dynamics as well as the potential for enabling research with broader relevance should make the topic an interesting challenge for security economists and researchers from related fields to contribute to. Those that have experience with security evaluation and/or standardisation processes, whether in technical or policy domains, should also be able to provide valuable input.

REFERENCES

01. R. Anderson (2020). Security engineering, third edition. Wiley.
02. Anonymous (2011). The SAVILLE cryptographic algorithm. Interview at Crypto Museum.
03. D.J. Bernstein (2020). Cryptographic competitions. IACR Cryptology ePrint Archive.
04. M. Bishop (2018). A design for a collaborative make-the-flag exercise. IFIP WISE.
05. L. Buchanan *et al.* (2016). Cyber-security games: building tomorrow's workforce. Katzcy.
06. K.R. Fulton *et al.* (2022). Understanding the how and the why: a course competition. ACM CCS.
07. A.J. Ferguson (2004). IA education or training: blurring the boundaries. FISSEA.
08. D. George (2012). The evolution of information assurance. USENIX Security.
09. I3P (2010). Designing a secure systems engineering competition workshop report. Dartmouth.
10. J. Jordon *et al.* (2021). Hide-and-seek privacy challenge with clinical time-series data. PMLR.
11. H. Kikuchi *et al.* (2016). Ice and fire: quantifying risk in data anonymisation. AINA.
12. N. Kostyuk & S. Landau (2022). Duelling over Dual_EC_DRBG. Harvard NSJ.
13. J. van Kuijk (2022). Hoe moeilijk kan het zijn: beleidshacken. De Volkskrant.
14. D. Lie & M. Satyanarayanan (2007). Quantifying the strength of security systems. USENIX HotSec.
15. N. Mouha (2021). Review of the Advanced Encryption Standard. NIST.
16. T. Murakami *et al.* (2023). Designing a location trace anonymisation contest. PETS.
17. NAS (2015). Peer review and design competition in the NNSA national security laboratories. NAP.
18. T.D. Nguyen & M.A. Gondree (2015). Teaching ICS security using collaborative projects. CyberICS.
19. J. Parker *et al.* (2020). Build it, break it, fix it: contesting secure development. ACM TOPS.
20. D. Ridgeway *et al.* (2021). Lessons learnt from the 2018 differential privacy challenges. NIST.
21. M.E. Smid (2021). Development of the Advanced Encryption Standard. NIST.
22. C. Steketee & P. Lock (2007). Software assignments for a course in secure e-commerce. IFIP WISE.
23. VCAT (2014). Report on the cryptographic standards and guidelines development process. NIST.
24. Y. Vorobeychik *et al.* (2013). Fireaxe: the DHS secure design competition pilot. ACM CSIIRW.
25. D. Walters *et al.* (2016). Collegiate embedded capture-the-flag challenge. MITRE.
26. M.M. Yamin *et al.* (2018). Make it and break it: an IoT smart home testbed case study. ACM ISCSIC.