This week I'll present the second stream in the "flashwares" series. We'll get all the way through an end-to-end useful example, then we'll look at a first "controlled channel" attack.

Time: Tuesday, May 21 2024, 7pm UTC (2pm central us)

[

](https://www.youtube.com/watch?v=eUyFUVRessg)

I've prepped a couple demos and some explanation. (slides)

First I want to get all the way through an end-to-end useful application in Gramine. We'll use python for variety. We can write a script that sanitizes a document, or that generates a cryptography trusted setup. Completing the example requires us to deal with remote attestation and document a reproducible build process. We'll walk through this code example: GitHub - amiller/gramine-rsademo

To steer the topic towards security, I'll introduce "Controlled Channel attacks" and how to think like a hypervisor or kernel and exploit an enclave. More specifically, we'll add "spicy printfs" to the untrusted code in Gramine that they use for encrypted files. python example that opens encrypted file. printf statements on 'pwrit… · amiller/gramine@4763624 · GitHub