Preface

How can high-trust online spaces be developed? Trust is a technologically mediated social phenomenon.

A software-as-a-service company's product security team stood up its own infrastructure for performing regular out-of-band application security testing. I developed this system from nonexistent to validated prototype by hosting an instance of Interact.sh, a beacon detection service, and using it for various methods of security testing. The first step was to work locally and show that I could positively identify a vulnerable service using Interact.sh. After local validation, I performed similar steps and configuration for an instance of Interact.sh available on the Internet, a requirement for a production instance. With a demonstrably effective instance running, I moved on to integrating Interact.sh with a variety of security testing tools, both automated and manual. I used Interact.sh with three tools on production systems while learning about out-of-band vulnerabilities. With this infrastructure in place, the team can move toward more advanced security testing, both automated and manual, and know that any relevant data is under the company's control.

Social trust is both important and difficult to establish on modern media platforms. False information can spread between users at unprecedented speed and scale. Information on Twitter can spread rapidly to enormous audiences. Misinformation ultimately spreads on Twitter because the platform is structured to enable it. It does not just allow misinformation, but it incentivises users to submit misinformation for personal gain. It hampers opposition to misinformation by limiting the reach of sources of accurate information. It also delays features surfacing context alongside misinformation, if context is shown at all.