FiVu Project: List of Threats for GeneVault

- Supply chain compromise: software component(s) produced by third parties and assembled in the final product could have problem(s) on their own or as a whole (when assembled) that allow people to attack it.
- Code Security Vulnerabilities: e.g., not evident or initially detectable programming and/or software design errors.
- API abuse: Application Programming Interfaces allow applications to talk to each other. Abuse can happen in the form of API impersonation for example, fake APIs feeding incorrect information, causing applications to misbehave.
- Exploit public facing application: different strategies to attack Mobile Apps or Web Interfaces that exploit their potential isolation or lack of integration.
- Insider threat. Unintentional insider threat: potential harm caused by former or current employees or business partners who bear no malice against software and users but whose actions unintentionally expose or damage private or confidential information from the app, website, or connections between them. Intentional insider threat: harm cause intentionally to software applications and the information they work with.

-

- I think the main security threat to this system is data confidentiality, and as a facet of that, the complexity of communicating to normal people about what their enrolment and permissions mean.
- I suspect that the Genevault system will want to nudge people towards consenting to information distribution of their data, and that Genevault will assume that the Third-Party applications (see * in Use Case) are all benevolent. There are all sorts of ways such threats could manifest.

-

- I imagine we don’t want user DNA or personal medical information to be available to people who aren’t authorized to see it. Obviously, there’s data confidentiality and access control for raw data. A slightly less obvious data confidentiality threat: data stewardship resulting from legitimate third-party queries (e.g., drug companies; universities who may want to use the data for research). We want to keep them from leaking the data they collect to the best of our ability.
- Those are the main issues. The other issue on the risk of people poisoning the dataset with fake DNA or fake medical data. Given a fixed budget, how much bad DNA/bad health data could a bad actor insert? What could you accomplish by inserting bad DNA/fake medical data? How well can we validate incoming DNA/medical data?