Although other performers began DARPA's Automated Program Analysis for Cybersecurity (APAC) program hoping for fully-automated solutions, our team at ISU was convinced that detecting novel, sophisticated, and domain-specific Android malware requires human insight. We proposed a human-in-the-loop malware detection approach that would amplify the user's natural intelligence. This philosophy led to our first research question: How should a software analysis platform be built to facilitate both automation and human comprehension? Existing tools supported either automation or static visualizations, but we needed a flexible query-model-refine system. We tasked our subcontractor, EnSoft, with developing Atlas, a novel graph-based analysis platform to fill our requirements.

Given Atlas, we faced a second research question: How can a man-machine analysis system detect novel, sophisticated, and domain-specific malware? Existing approaches detected only simplistic malware, or else placed unreasonable manual burden on the user. Thus we designed the ISU Security Toolbox, a suite of semi-automated detection tools and program analysis primitives with an intuitive Dashboard interface. The potent combination of Atlas and the ISU Security Toolbox propelled us to become the top performer in APAC Phase I.

Despite the unprecedented flexibility afforded by our human-in-the-loop approach, it became clear that Android itself was a barrier to automation. Applications interact extensively with the massive Android framework, using APIs and receiving callbacks. Critical behaviors, particularly information flows, are missed if Android itself is not included in an analysis-- unfortunately, doing so is infeasible for scalability. These observations informed our third research question: How can expressive, compact information flow summaries be mined from a library for accurate and scalable partial program analysis? We created a novel library data-flow summary tool called FlowMiner to solve this problem. This thesis covers each research question in detail.