## Alloy Success Stories

Here are examples in which people found serious problems in real systems:

1. In one of the first applications of Alloy, Sarfraz Khurshid found that a published scheme for resource called Intentional Naming did not work correctly. Using Alloy, he showed how to fix it. The developers later fixed the problems their own way in the code; Sarfraz showed using Alloy that those fixes were broken too. See: <https://www.semanticscholar.org/paper/Exploring-the-Design-of-an-Intentional-Naming-with-Khurshid-Jackson/039c93372e7d6a97844194ac6b2683478e41ec09>

2. Pamela Zave famously showed that the Chord algorithm is not correct. This is significant because (a) the paper claimed that a merit of Chord was that it was “provably correct”, and (b) the paper is one of the most widely cited in CS.

3. Barth et al showed the standard browser security mechanisms (such as the referrer field) designed to prevent CSRF and XSS attacks don’t work. This project involved building a library of reusable models of the WWW.

4. Emine Gokce Aydal’s thesis analyzed Tokeneer, a system built by Praxis Critical Systems for the NSA as a demonstration of a secure system. Although Tokeneer had been developed using advanced proof techniques, Aydal found serious security loopholes (to do, for example, with how configuration files are loaded).

5. Apurva Kumar (IIT) used Alloy in his thesis to analyze various authentication protocols, and found several bugs, including a vulnerability in OAuth 1.0 that had not been previously reported.

6. Robert Seater wrote: We were working on modernizing air traffic control data systems.  As part of that, we needed to understand the workflows of users, the flow of external data sources, and the flow of the airport surface itself.  As part of this, someone else had already built a text document describing scenarios and procedures for how aircraft move around the surface, are passed between different control authorities, and the risks present at each stage.  I spent a couple of days building a model of part of the informal (but thorough) documentation and showed that I could reproduce the handful of manual scenarios meeting the written constraints.  They then asked me to finish modeling the entire document, and I ended up finding several logical errors in the document.  For example, according to the document, it was technically impossible to ever land at certain classes of airports, which would have been a bad foundation for our decision aids and support software.

7. Tim Nelson used Alloy to find a problem in a program that he is working on for Software Defined Networks (SDNs). Tim and his team created a language for describing SDNs, that language is called Flowlog. Flowlog is a simple, declarative network programming language. They also created a Flowlog-to-Alloy compiler. Thus, a Flowlog program can be automatically converted to Alloy and thereby a Flowlog program can be analyzed via Alloy. For more info, see <http://cs.brown.edu/people/tbn/publications/nfsk-flowlog-nsdi14.pdf>