

On the Heffalump Threat

Peter Gutmann
University of Auckland

pgut001@cs.auckland.ac.nz

Abstract

Over the last few years a new type of attack has been receiving a lot of attention. Unfortunately the technical details can be quite confusing to laypeople. This paper explains it in easy-to-understand terms.

Discussion

A long time ago, in a faraway kingdom... well actually not that long ago, about thirty years to be precise, one of the king's wizards — and he had a lot of wizards, because wizarding was a profession that attracted plenty of funding — announced that he'd come up with a way for heffalumps to knock down castle walls. Now no-one had ever seen a heffalump and in any case it was much easier to knock down castle walls with catapults so like a lot of the stuff the wizards said it was ignored by everyone except other wizards, some of whom got quite excited about it.

Then about seven years later a group of wizards actually managed to come up with a way to breed a sort of micro-heffalump that could do what the first wizard had described. However when it was pointed out that fifteen bricks piled on top of each other didn't really constitute a castle they went back to their towers and applied for more funding because, you know, heffalumps.

Eleven years after that, some new wizards came up with another toy heffalump that could knock over 21 bricks piled on top of each other, the same as a toddler or an enthusiastic puppy. And now a lot more people got excited about it because, as the wizards pointed out, once someone actually produced a proper heffalump no castle would be safe.

This gradually led to an increase in funding and, eventually, work on post-heffalump fortifications that required even more funding. Still no-one had seen an actual heffalump, but that didn't mean that, like ghosts and goblins and trolls, there couldn't be one out there somewhere.

And now, every few months, one or another of the groups of wizards would announce that they had achieved heffalump supremacy, in which a low wall of bricks that was carefully constructed to be easy to knock down by a heffalump but hard to knock down by a catapult had been knocked down by a heffalump, or at least a simulation of a heffalump. Unfortunately for the wizards since heffalump supremacy was announced every few months, over and over again, people began to doubt it about the tenth or twentieth time that it was announced anew. And still no-one had seen an actual heffalump.

Eventually this came to the king's attention and, while he didn't really understand any of it, he understood that the wizards were saying that none of his castles would be safe when someone produced a heffalump, and so he issued royal decree 7535 which required that all of his subjects switch to living in post-heffalump castles. This upset some people who pointed out that they'd already invested billions of thalers in building castles to resist catapults, and it was hard enough the first time round particularly since some of the castles leaked and were difficult to live in, and now they were expected to spend billions more thalers building new, even more awkward post-heffalump castles, some of which fell down once they were built, but the king had decreed it so there was no going back. In any case all the masons who had set themselves up to build post-heffalump castles were beside themselves with glee at all the thalers this royal decree guaranteed them, as were the wizards who now had guaranteed employment for life dreaming up new types of post-heffalump castles and telling each other about them at wizards conclaves.

And still no-one had ever seen a real heffalump.