The breakfast says: Hi!

Scholars say that all stories can be boiled down to three basic archetypes:

1. *The voyage and the return.*
2. *A stranger comes to town.*
3. *Spaghetti can suddenly talk.*

–*Nerdroid Picture Diary, http://nedroid.com/2006/07/1458-tutorial-writing/*

This adventure is one of the third kind.

The PCs wake up and have breakfast. Ask them what they want from their domestic system. It will be nicely laid out at their usual breakfast spot… and it will talk back. The rice and natto will cheerfully bid them good morning. The cheese sandwich will complain that you woke it up. The croissant will politely (and with a French accent) beg for its life.

What is really going on? A practical joke of course: a resident juvenile prankster figured out how to get fabbers to add edible electronics running small AIs. Just the kind of bizarre thing one should learn to expect in the accelerating future.

Except that this is a serious matter. Being able to hack around the restrictions in a fabber is nothing to sneeze at: even at the most liberal anarchist habitats have some software security so that when you print a product nobody else can tamper with the design. Anything else would be a wide open hole that could be exploited by malware, antisocial crazies or enemies. In the inner system a failure of DRM can lead to a very nasty visit from Oversight and the Nanosys. The security hole needs to be found and patched quickly.

People are likely confused at first, trying to check whether it is *they* who have been hacked or quietly gone insane, or just the world. The next natural reaction might be to think it is a marketing trick or a recruitment ad.

As the PCs and others wake up to this, the problem is spreading. The prankster made the code viral, and it is infecting every fabber, cornucopia and hive in the habitat. It is not just food that talks. Newly printed pillows, guns and transplant organs are all equipped with chatty, fun micropersonalities. In some cases this interferes with their function directly or indirectly, and sometimes it just crashes the fabbing when the blueprints conflict. The issue has gone from an annoyance to a security issue to a real problem.

Of course things turn worse. The little AIs are all simple open source joke AIs, downloaded from some mesh site somewhere. They are not secure at all. In fact, they can fairly easily be hacked with the right exploit, an exploit that has been around for years. That might not have mattered much for the original joke – who would seriously try to hack a breakfast sandwich?! – but now there are security holes just about everywhere. And sharks are rapidly moving in to use them.

At best the little AIs become entry points for random meshlife: spam, worms, escaped search requests, vapor forks and less recognizable entities that try to find exploitable hardware to run more copies of them. They degrade performance, worm their way into other processing nodes, and jam the mesh with their nonsense. But there are worse things out there: rampant hacking AIs, smart viruses, remnant seed AGI code from the Fall, the exsurgent virus in all its forms. As the AIs mutate they become increasingly linked together as successful invaders take over more and more of the vulnerable nodes. If this goes on long enough the habitat will have a serious and deadly infestation.

Fixing the situation is another matter. Getting everybody to stop fabbing things will just slow down the spread. Resetting fabbers will not help unless they are properly air-gapped, since the virus is already embedded in the local mesh. Finding and disassembling the virus is a fairly tricky combination of InfoSec and Nanoprogramming – the software defenses and DRM of fabbers work against owners trying to find it.

The best approach is to catch the originator and ask – or beat – them nicely to reveal the exploit. Once found it should be fairly easy to make a vaccination virus that infects all vulnerable systems and prevents them from being exploited. Then it is just a matter of recycling everything manufactured with the AIs (despite their protests and comments) and things should be back to normal. Of course, finding the prankster might be nontrivial. In a small habitat it will be easy to figure out who is behind it, but on a larger habitat it might be tough. Especially if the prankster has realized the mess they have created and now is trying to hide from angry mobs and authorities.

Somebody clever enough to find an exploit this powerful might make a great ally or resource. Or was their discovery of the exploit really a case of random genius, or part of something more sinister? It could be a more serious attack on the habitat, hidden in the guise of something inocous. The prankster might simply have been given code that would allow them to make a big security scare while the real attack occurred somewhere else… have you checked your medichine updates today?

But that problem might be for after lunch.