TITLE : Placing your trust in suppliers

Recently, the debate about Huawei and the 5-G network returned to the news.

The argument surrounds the use of Huawei supplied equipment to create the core of the new 5-G mobile phone network currently under construction.

Government and high-level Security experts will continue to argue about whether this is a safe choice to make, but Huawei also make a lot of equipment for the corporate IT market including network routers, ADSL modems, CCTV cameras and smartphone handsets.

So should we be concerned about using these other Huawei-made devices ?

No one appears to be questioning the build quality and functional reliability of Huawei equipment.
And as potential customers we are free to carry out reliability and quality tests for ourselves.

We can be fairly confident that these test results will be comparable to the more well known brands from South Korea, the USA and Europe. Much like when we heard about exploding batteries and bendy smartphones, we would soon get to know if there were any major visible problems with the Huawei equipment.

Indeed, the Huawei equipment may even be manufactured in the same electronics plants as the more well known brands.

So we can be confident that the argument is not with the testable visible quality of the equipment.
But there is one major component that we can't easily test – this is the product's software.

It takes significant amounts of man-power to make a thorough assessment of the software quality. Without access to the source materials any tester needs to attempt to 'reverse engineer' what the original creators have done - this is a time-consuming process that is not totally accurate.

So we can't realistically test the software to our total satisfaction, and we have to place our trust in the supplier making a secure product.

But does it actually matter that we have to trust our software supplier ?

We each have an example of this trust relationship in action for ourselves with the Anti-Virus utility that we install on our laptops and PCs.

Every morning our AV software connects to the AV supplier's website and updates itself to learn about all the new malware that's been detected since the last update.

Every time we let it install a new update, we have to trust that our Anti-Virus supplier is giving us a safe and secure product.

We could attempt to audit today's product, which would be hard and take a long time as we don't have access to the source materials. But what happens when we receive a new update tomorrow. To be certain of it's safety we'd have to re-do the audit again as we have just updated to a completely new product release.

We saw a public failure to trust a software supplier with the recent case of Kaspersky Anti-Virus and the US government.

The US announced they would no longer use Kaspersky Anti-Virus on their internal IT systems and advised other security conscious corporations to take the same precautions.

The ability of Kaspersky Anti-Virus to detect & prevent malware is not in question as it performs very well in comparison tests with other AV suppliers. So the Kaspersky product is very effective and does the job which it is designed to do.

We have to conclude that this was a decision by the customer to withdraw their on-going trust in the product.

Likewise, the quality of Huawei products has not been brought into question.
If Huawei's equipment was ineffective then they would already have been excluded as a potential supplier.

It is simply a question of whether the 'customer' has the faith to place their on-going trust in them to always produce a safe and secure product.

We each have to make our own decision on that.

You can find out more by visiting : **www.fabric8n.com** and clicking on '**development**'

Steven Bishop

Head of Technology for Fabrication Systems

Email : steven.bishop @ fabric8n.com