M2M-Communication: From one Machine to Another

But what exactly are the machines doing?

They're not talking since their communication has to be non-verbal by default.

They're not having a conversation since they will hardly be chatting about topics like films or music.

Making contact fits better than communication and seems to hit the target dead-centre.

Systems of machines working together have been around for a while now. In these – let's call them "classic systems" – an integrator has determined which components contact each other, and how they are supposed to accomplish this.

In M2M communication, this previously determined order will not exist any more. In some way, the machines themselves will decide when to make contact with another machine to exchange information.

Actually, "machine" is not the right term – or at least not if you go with the commonly accepted definition. The "machines" concerned here, are computers, either individual ones or ones that have already been connected into clusters. Each of them consists of function defining software and hardware to execute that.

The challenge lies in connecting an unpredictable number of computers of different and unknown origin in such a way that they can exchange meaningful information in order to fulfil the overall purpose of the entire system. To ensure the security of the entire system, each individual computer within the system must be secure. The computers available on the market today are not up to this challenge! Put simply, they cannot tell, whether a communication request from another computer is a meaningful data exchange or a hacking attack loaded with malware.

The weakness of these systems exists in the hardware of the computers. Practically all commonly available objects of this class are based on an architecture that has existed for about eight decades. They suffer from missing distinction between data (the objects they are supposed to manipulate) and instructions (the “tools” to perform that manipulation). Three functional areas need to be corrected with this respect: Exchanging binary information, storing binary information, and installing software.

By using the term “binary information” I ant to stress the fact, that a sequence of bits, as found inside computers, by itself is not recognizable whether it is a value of some kind, an address, or a machine readable instruction code. Hackers make use of this fact by sending instructions of malware disguised as data.

A new hardware architecture, could remedy these issues. It revises the manner, processors and memory units work together at PCB-level. This new hardware does not only prevent malware from being executed, but also supports further security measures such as clean separation of networks with different access criteria, which will also be required for secure M2M communication. This hardware architecture is patented and succeeded in the hardware category of competition "INNOVATION PRIZE – IT 2015". - IT security "Made in Germany".