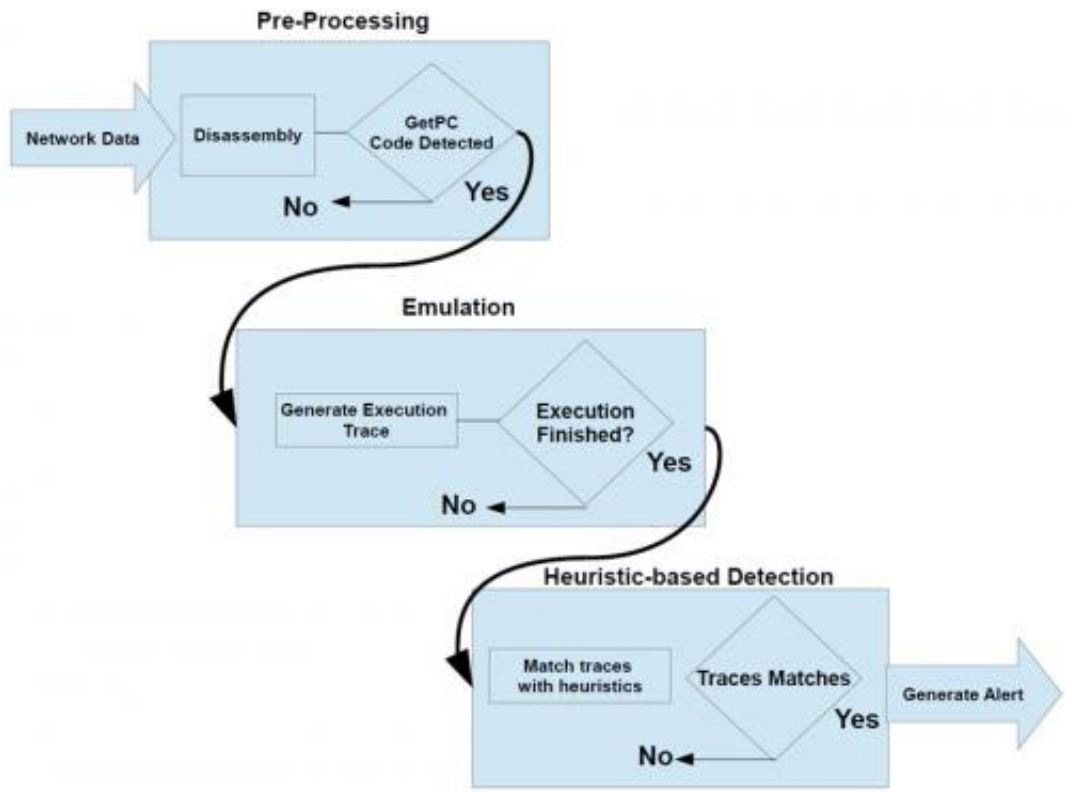
Even the latest malware detection systems can be bypassed

October 16 2014



The three subsequent steps in an Emulation Based Network Intrusion Detection system. Credit: EBNIDS

Unwanted intruders are finding it more and more difficult to hack computer systems and networks thanks to today's advanced detection technologies. With the help of emulation-based technologies, many attacks can be detected at an early stage. However, even these

technologies are not watertight, as UT researchers Ali Abbasi and Jos Wetzels of CTIT will demonstrate during the Black Hat conference, October 16 in Amsterdam.

We discovered how vulnerable our computer systems are when the first major viruses emerged in the 1990s and were doubly reminded of this during the Stuxnet attacks in 2010. Simple viruses are no longer the issue today; they have been supplanted by computer programs that can partially or completely take over a system. These are not just attempted hacks for no reason other than 'to demonstrate that it's possible', they also include advanced persistent threats used for espionage and other illegal activities. While the hackers' methods are getting ever more clever, the detection systems to stop them are becoming more advanced too. In the past the aim was to detect a 'signature', but today even a suspicious piece of code can be detected and tested under controlled conditions - known as emulation. Emulation based network intrusion detection systems (EBNIDs) can also detect Zero Day Exploits: attacks for which no remedy yet exists.

PhD candidate Ali Abbasi and student Jos Wetzels will present their extensive research on EBNIDs at the Black Hat conference. EBNID systems track down intruders in three phases: pre-processing, emulation and heuristics detection. In the first phase the network traffic is analysed, in the emulation phase the suspect code is isolated and tested and in the last phase the decision is made whether or not to sound an alarm. Abbasi and Wetzels have demonstrated how this technology is a major leap forward, but they have also shown how others could circumvent the system, for example by fragmenting the suspect code and so bypassing the emulator (if no suspect is recognized then no alarm will go off).

Finding weak spots is all very well, but the next step in Abbasi and Wetzels' research is to find new solutions. Abbasi, who studied in China,

previously led a research group in Iran that studied vulnerability analysis and penetration testing during the Stuxnet attacks. Wetzels is in his graduation year. Both researchers are attached to the Services, Cyber Security & Safety Research group led by prof. Roel Wieringa. The group is part of Twente University's CTIT research institute.

Provided by University of Twente