Thursday December 5, 2019, 2 - 6 pm
18th Ethical Forum of the University Foundation
Academics as soldiers? Is defence-related research a scandal or a duty?

Joos Vandewalle KU Leuven

A plea for maximal openness and public scrutiny in information security research at universities.

Modern society depends strongly on internet, social media and digital exchange of information via the web, electronic payment and so on. Most of these civil services have important security issues, that can be solved by *cryptography*.

My statement is that the cryptographic algorithms should be open and the design criteria should be open for independent scrutiny.

In cryptography there are two important elements : *the algorithm and the key*. Moreover the cryptographers perform two types of tasks : *Design new algorithms and new services using these algorithms, and evaluate the strength of the algorithms and services by trying to break these (codebreaking)*.

The designers can always build a trapdoor in their algorithms. This is a shortcut only known to them and to those they inform about it, or to whom this information leaks (closed circle). They can use it to find the cleartext without having to know the key. It is crucial that the algorithm and the software/hardware are open, so that during public scrutiny the eventual presence of a trapdoor can be detected. This can give confidence in the strength of the system and hence democratic value. The security of the algorithms and services should hence only depend on the secrecy of the keys.

Also the breaking efforts should be openly published, eventually in case an algorithm is broken the public announcement should be after a grace period to give the service providers the time to transfer to another algorithm for vital services. Moreover, when the algorithms are public they can be standardized and widely used.

The national security services work secretly for the military or diplomatic purposes. There is a long history of secret communication with methods like cryptography that had for centuries strong military and diplomatic value. Since the early 1980'ies the open scientific approach to cryptography and data security has become an interesting research topic at universities. With the advent of electronic payment, internet, and smart phones and social media, there is indeed an important non-military need. Sometimes the secret and open research were in conflict and there were several attempts of the secret services to block open research on cryptography in universities. Standardizing secret algorithms does not make sense. Too much secrecy is highly undemocratic, since it opens the door for mass surveillance and criminal use. **So when academic researchers perform information security projects for civil or military applications and for cyber security, one should have maximal openness in algorithms, software and hardware. This is a hard and not negotiable condition for universities to engage in such research.**