# Securing the internet of the future

*As the internet continues to grow rapidly, guaranteeing our security online becomes more and more critical. Research at the University of Oxford has helped improve the next generation of internet security.*

UNIVERSITY OF OXFORD

www.ox.ac.uk/oxfordimpacts


In 2016, over half the world's population has internet access – 100 times more people than in 1996. Every day, people are involved in billions of online transactions, from banking to emailing, that depend completely on security protocols embedded in the internet. We see the green padlock symbol every time we visit a secure webpage, but how do we know it can be relied upon to protect us?

Behind the green padlock sits Transport Layer Security (TLS), a large set of cryptographic protocols that provide communications security over computer networks. A new version – TLS 1.3 – is about to be released, and Professor Cas Cremers' research in the Department of Computer Science has made a key contribution to its security. Professor Cremers specialises in building software tools that can analyse large and complex sets of protocols like TLS for security vulnerabilities.

TLS was originally built by the Internet Engineering Task Force (IETF). Like many similar systems it has been amended and added to over many years, with the result that it has become very large and hard to analyse. Making sure that there are no security vulnerabilities is a near-impossible task, and previous versions of TLS have been vulnerable to many attacks.

The IETF working group given responsibility for updating TLS was led by security experts working for Mozilla. They approached Professor Cremers, who was working on aspects of cryptographic protocols – specifically how cryptographic building blocks are used within larger systems like TLS, which are made up of many individual components. The way these individual blocks are put together may affect each other and lead to new security flaws in the overall system.

Using his software tools to analyse TLS, Professor Cremers and his students discovered a fundamental design flaw in one of the proposed variants that completely broke the security of the system. It involved the operation of three specific components invoked in one particular order – in other words, an error that was complicated and difficult to find, but which could seriously compromise security. The new TLS 1.3 standard refers directly to Professor Cremers' work, and also highlights the type of error he identified as something that designers should make efforts to avoid.

The impact is enormous, as TLS 1.3 will be implemented in nearly every smart device on the planet – not just computers and phones, but fridges, toasters and central heating systems. Despite the risks of hacking, the internet is still a hugely robust communications system. TLS 1.3 will make its security even more robust – and University of Oxford research has played a key part in this.

***'[This] formal analysis [has been] really helpful in guiding the design [of Transport Layer Security 1.3]. It's really important to have this kind of analysis, especially before the design is completely hardened.'***

**Eric Rescorla, Mozilla Fellow and leader of the TLS Working Group**