Cryptography and security at ISC'13

Michael Hortmann, a leading expert in cryptography from the University of Bremen will be chairing a session on cryptography and security at this year's International Supercomputing '13 conference.

This year, the EGI Community Forum was hosted by the University of Manchester, an institution steeped in the history of scientific computing. Of course, no figure stands taller in this history than Alan Turing, the world-famous mathematician and computer scientist, who was based at the University of Manchester from 1948 until his untimely death in 1954. During this time spent in Manchester, he developed the well-known 'Turing test' for artificial intelligence, which still forms the basis of tests used to this day. Nevertheless, the work for which Turing is today most well remembered is undoubtedly his major contribution to cracking the German Enigma machine code during the second world war, thus

Posted on APR 17 2013 9:49AM

Andrew Purcell
European editor

Share this story

Alan Turing memorial statue in Sackville Park, by the University of Manchester. Image courtesy Kurt Seebauer, Wikimedia Commons.

significantly expediting the cessation of that conflict.

Now, 70 years later, cryptography has moved on an awful long way since Turing's time, becoming a ubiquitous part of our daily lives. We now have it in our personal computers, mobile telephones, televisions, voting systems, bank accounts, and email. Today, cryptography is not just vital for the protection of our society's military infrastructures, but also almost all civilian ones, too.

Michael Hortmann, a leading expert in cryptography from the University of Bremen, Germany, will be chairing a session on this subject

Tags

cryptanalysis

cryptography

International Supercomputing Conference

ISC'13

Leipzig

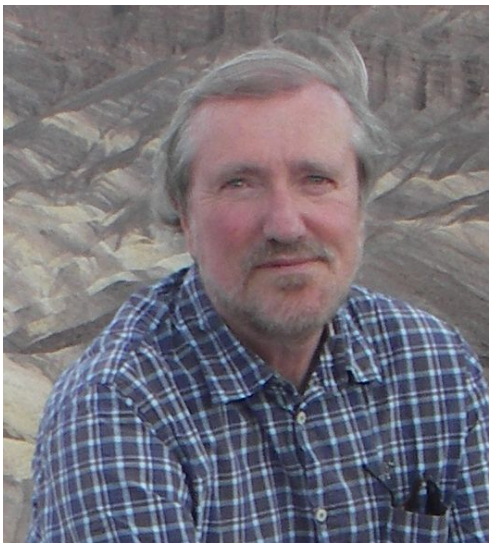
Security

at this year's International Supercomputing '13 conference. He explains that despite cryptography now playing a major part in many aspects of our lives, there are just a few 'cryptographic primitives' which underpin most of the technologies used. These, he says, can essentially be grouped into two categories.

The first category consists of hash algorithms and combinatoric block and stream ciphers. These derive strength from the cryptographic experience of their designers and that of the cryptographic community as a whole; there is an extended process of peer review and security-proof in years of practice. A hash algorithm is essentially an algorithm that takes an arbitrary block of data and returns a fixed-size bit string. A good example of one would be SHA-2, which was published by the US National Institute of Standards and Technology in 2001 and which is often used for tasks such as password verification or checking integrity of files or messages. By contrast, block ciphers, such as the Advanced Encryption Standard, also published by the National Institute of Standards and Technology in 2001, are deterministic algorithms operating on fixed-length groups of bits. Block ciphers are often referred to as 'symmetiric' methods, on account of the same key being used to both encrypt and decrypt the information.

Meanwhile, Hortmann's second category is very different, indeed. This category consists of methods such as RSA and elliptic curves, which are based on deep mathematical problems, namely factoring and

discrete logarithms. These methods form the base of most public key cryptosystems, says Hortmann, but he adds: "No proofs currently exist to show that these mathematical problems are truly as difficult as they appear; we don't know if they really are inherently difficult to solve."



Michael Hotmann will be chairing a session on cryptography at ISC'13.

Once quantum computers come on the scene, these public key cryptosystems will be compromised, Hortmann warns. "The problem really comes if one group has quantum computers and another group doesn't know about it."

"Some say we could have powerful quantum computers in just 15 years, but in my opinion it is unlikely that we will see them in the next 30 years or so," says Hortmann. "Basically, it's just a case of there being an awful lot of hype wherever a lot of money is involved." Nevertheless, Hortmann adds: "There's been lots of work on developing cryptographic techniques which are resistant to

attacks from quantum computers, since as far back as the early nineties."

Yet, despite quantum computers still being some way off becoming a reality, advances in high performance computing are causing changes to the world of cryptography. "If we look at supercomputers and highly parallel systems, brute force attacks are now possible in such a way as we could previously never imagine," says Hortmann. Consequently, he explains, as computers get faster, security becomes ever more tricky to achieve.

So, what about password systems? "Password systems are fine," says Hortmann. "But people are inevitably always going to be the weak point, because they do things like writing passwords down, or choose simple ones, or get their passwords stolen by trojans." Equally, Hortmann says that security systems based on biometric data, such as iris scans, or even DNA, are no panacea. "There are still major problems with biometry-based security systems," he says. "Biometry always sounds good, but these systems are not sufficiently analyzed by the cryptographic community and there are ways to trick them." He continues: "These systems will clearly be widely used in the future, but they are harder to test than mathematics-based cryptographic systems. Thus, we won't really know how secure they are until they become more widely used."

Generally, with most cryptographic or security systems, successful attacks are achieved not by solving the underlying mathematical problems,

explains Hortmann. Instead, they are achieved by utilizing side channels or infiltrating the computer systems on which they run. Supercomputers, he explains, have a fundamental role to play in both aiding such attacks and in designing secure systems.

Want to find out more? Be sure to attend Michael Hortmann's session at this year's ISC'13 conference in Leipzig, Germany.

Join the conversation

Contribute

Do you have story ideas or something to contribute? **Let us know!**

OUR UNDERWRITERS

Thank to you our underwriters, who have supported us since the transition from International Science Grid This Week (iSGTW)

CATEGORIES

Advanced computing

Research networks

CONTACT

Science Node
Email:
editors@sciencenode.o

into Science Node in 2015. We are incredibly grateful.

View all underwriters

Big data

Tech trends

Community building

Website:
sciencenode.org