

**Speaker 2:**

Prof. William (Bill) J Buchanan, OBE, PhD, FBCS, PFHEA, CEng, BSc (Hons)

Professor of Applied Cryptography

School of Computing

Edinburgh Napier University

United Kingdom

**Title: A Vision of Cryptography: The Next 10 Years**

**Abstract:** The Internet we have created is often still based on protocols that were created decades ago. We have thus ended up with a sticking-plaster approach to integrating security, and where it has often been seen as an after-thought. Over the next decade, though, we are likely to see a large-scale shift of the integration of cryptography into every aspect of data storage, data analysis and data transmission. There are, though, many challenges ahead especially in areas of the usage of homomorphic encryption, zero knowledge proofs, blockchain, privacy-preserving machine learning, self-sovereign identities and digital signatures. The standardization of areas such as quantum robust cryptography and light-weight cryptography will also see a drive to improve our existing flawed methods. This presentation will thus look at where we have been, where we are, and where we are going. It will also touch-base on the increasing tension of the usage of cryptography against the requirements of law enforcement agencies to undertake their pro-active detection of crime, and in criminal investigations.

**Biography:** William (Bill) J Buchanan OBE is a Professor in the School of Computing at Edinburgh Napier University, and a Fellow of the BCS and Principal Fellow of the HEA. He was appointed an Officer of the Order of the British Empire (OBE) in the 2017 Birthday Honours for services to cybersecurity. Bill currently leads the Blockpass ID Lab and the Centre for Cybersecurity and Cryptography. He works in the areas of blockchain, cryptography, trust and digital identity. He has one of the most extensive cryptography sites in the World ([asecuritysite.com](http://asecuritysite.com)), and is involved in many areas of novel research and teaching. He has published over 30 academic books, and over 350 academic research papers. Along with this, Bill's work has led to many areas of impact, including three highly successful spin-out companies (Zonefox, Symphonic Software and Cyan Forensics), along with awards for excellence in knowledge transfer, and for teaching. Bill recently received an "Outstanding Contribution to Knowledge Exchange" award, and was included in the FutureScot "Top 50 Scottish Tech People Who Are Changing The World".