Lecture 1

Welcome to this lecture 1 (slides with voiceover), on the impact of future technologies and the implications for security and risk management.

In this lecture we will be looking at current and future technologies and highlighting the problems and challenges facing security and risk management.

We will also look at cryptography, its current role, and the possible impact future and emerging technologies might have on traditional methods and how new ways of working will be essential to meet new demands.

Accelerated production of digital technologies is creating exciting advances to businesses and society but also a darker side where threats and risks are on the increase, and are giving rise to increased challenges for security and risk management.

The Internet of Things (IoT), is a powerful digital revolution where connected devices create new global service opportunities based on real time physical world data. The integration of physical-world time with event-driven computation, is highlighted as a unique challenge for Cyber-Physical Systems (CPS).

With the volumes of data being generated by these new services, there will also be vast amounts of data distributed over networks and undoubtedly new problems of ownership, security, and control, whereby decisions will be made by proxy

A report by the National Intelligence Council in the US on Disruptive Civil Technologies [1], states that Nations will be challenged by the IoT as a result of changing demographic structures and new psychologies: “to the extent that everyday objects become information security risks, the IoT could distribute those risks far more widely than the Internet has to date”.

Many new issues and concerns will also arise with protecting the privacy of personal information as it will no longer be under human control or intervention. The majority of IoT attacks were worms and bots, but in 2018 a new breed of threat emerged where routers and connected cameras were the most infected devices and accounted for 75 and 15 percent of the attacks respectively.

The Mirai distributed denial of service (DDoS) worm is malware that turns networked devices running Linux into remotely controlled bots and was responsible for 16% of the attacks and was the third most common threat in 2018.

An emerging technology that could have a revolutionary effect on traditional cryptography practice, is Quantum Computing.

Let's take a brief look at cryptography and its history. "Cryptography is the study and practice of techniques for secure communication that is protected from adversaries". [2]

Cryptography involves encryption that is a process to encode information to prevent access from unauthorised parties to read data. Encryption is a process that uses an algorithm to encode a message/file providing assurance that it can only be read by certain people. A key is used for the receiving party to unscramble, or decrypt the information.

Historically, cryptography has been in existence since the Roman times when a process called 'Caesar Cipher' was used by Julius Caesar to encrypt messages. This process was carried out by shifting letters to the right by the same number of letters every time.

Cryptography now includes more than encryption since the development of the Internet where a need for computers and advanced mathematical algorithms use large prime numbers, fast processors, and combinations of complex technologies to secure data.

Asymmetric encryption is used where it relies on key pairs with both public and private keys used in the encryption algorithm. Each key uses very large prime numbers. Public Key encryption ensures confidentiality, message integrity, authentication and

nonrepudiation. The Private key is intended to be private to enable the authenticated recipient to decrypt the message. By the way, 'Nonrepudiation' is a legal concept used to provide proof of the origin of data whereby ensuring that authenticity of a signature. It gives assurance that the party sending the information is provided with proof of delivery and vice versa, the recipient is provided with proof of the sender's identity.

Symmetric encryption only involves one secret key, the same key both encrypts and decrypts data. The sender and the recipient have identical copies of the key.

Quantum cryptography is based on physics, not mathematics and uses light particles called photons, and uses theories of quantum mechanics to perform decryption and encryption. It relies on our ability to measure certain properties of photons and on Heisenberg's uncertainty principle, which allows senders and receivers in quantum communication to easily detect eavesdroppers. Implementation of quantum cryptography remains in the prototype stage, as creating practical photon guns and receivers is technically difficult. The advantages for its future use will be less time to decrypt traditional encryption and Quantum encryptions are almost impossible to break. The disadvantage however, is the possibility to render traditional cryptosystems useless which pose many problems for cryptographers. Quantum computing will undoubtedly be more prevalent in the future and it is difficult to forecast what its future use might bring. Lecture 2 will look at these issues in more detail.

The preceding slides are an overview of technologies and cryptography, and problems and issues for security and risk management.

Now, please take a break and reflect on what we have learned so far before moving on the next task which is to read a report on good practices for security of the IoT in the context of Smart Manufacturing.