1.1 Theme

Quantum Cryptography and Quantum Computing

1.2 Title

In Crypto We Trust, or do we? Dragging privacy back to the 90's

1.3 Overview

We currently live in an age where we can make transactions and purchases, transfer funds and communicate online knowing that our activities are securely encrypted by trusted ciphers. But for how long will this remain the case?

Recently a 'former NSA contractor' has released documents highlighting a program entitled 'Penetrating Hard Targets', which shows the NSA is seeking to build a quantum computer that can break 'nearly every type of encryption'. While as far as we know this has yet to be achieved, they're spending an alleged $79.7 million dollars on the project. So it's only a matter of time.

Quantum computing heralds a new age of technology which brings exciting new possibilities, however the fact that this same technology can be used to subsequently subvert existing and trusted encryption methods has far reaching implications.

This presentation aims to bring awareness to the progress of quantum computing with a focus on the progress of quantum cryptography, within both Government and Private Enterprise. This will be completed by looking at;

- The history of cryptography
- Recent cipher attacks and exploits
- Current industry standards
- What is quantum computing?
- How can quantum computing be used for cryptography?
- The future of cryptanalysis

The introduction of Quantum computing capable of quantum cryptography may return us to a similar online security landscape of the 1990's. The general public had the ciphers available but lacked the hardware capable to feasibly secure data for exchange. Will our current encryption methods still be feasible in a world where Governments and Private Enterprise have access to technology able to break them?

1.4 Slide Outline (10-15 slides)

I propose to deliver a presentation that brings awareness to the implications of the introduction of quantum cryptography to the general public;

1. History of Cryptography
   a. Uses
   b. Implications when it breaks?
   c. Why do we need quantum?

2. Recent attacks on ciphers
    a. BEAST
    b. CRIME
    c. PFS
    d. Efforts and hardware used
3. What is quantum computing?
4. Current status of quantum computers
5. What is quantum cryptography?
    a. Shor's algorithm
6. How can we use quantum cryptography?
    a. Is it for everyone?
7. Post-quantum cryptography
    a. What are our options?

1.5 Aims, Objectives and Relevance to Delegates

This is a subject that affects us all. The aim is to bring awareness to the topic of quantum cryptography and the implications of this new technology. Generating awareness and discussion around the topic is the main focus.

1.6 Biography

Joshua is a Security Consultant with Sense of Security, a leading Australian information security and risk management consulting practice delivering industry leading services and research to organisations throughout Australia and abroad. He is an Offensive Security Certified Professional and Expert (OSCP, OSCE) and has been involved in the IT industry since 1997.

Shawn Thompson (BIT, CISSP, GIAC-GREM, GIAC-GCIH) is a security consultant with Sense of Security focusing on network and web application penetration testing and social engineering. Shawn has ten years of information security experience and has worked for the Australian Federal Government and private sector organisations. Shawn has experience reverse engineering the Nortel UniSTIM VoIP protocol and written programs to take control of Nortel VoIP systems.

1.7 Contact Details

Joshua Cavalier

Information Security Consultant

M: +61 412 647 939

E: joshuac@senseofsecurity.com.au