Integrating Quantum Concepts into Cyber Security

Session 4: Attack Vectors and their Defence

Dr William Joseph Spring

ACSAC 35, Condado Plaza Hilton, San Juan, Puerto Rico, USA

9th – 13th December 2019

Intrusion Prevention and Detection

Authentication
[Piotr Zawadski, 2019 https://doi.org/10.1007/s11128-018-2124-2]
Quantum Tripwire
[Anisimov et al; arXiv:1002.3362v2 [quant-ph]

Authentication

- User authentication is said to be reliant upon:
  - What we know (user name and password)
  - What we have (a shared secret)
  - What we are (fingerprints, face recognition, gait, …)

- One example of quantum based authentication protocol is the following:
  1. Alice and Bob share a secret. An even numbered sequence of bits They set their counter n to zero
  2. Alice selects message mode or control mode randomly and looks at the first 2 bits:

     00 is encoded as the qubit $|0\rangle$
     01 …….. $|1\rangle$
     10 …….. $|+\rangle$
     11 …….. $|-\rangle$

     Alice will continue to encode the bit pairs following the above rule until the sequence is completed
  3. Alice sends each qubit to Bob who measures the incoming state using the even bit in the sequence that Bob has to determine the measuring basis (0 for the Z basis, 1 for the X basis)

Authentication

4. Bob announces that the qubit has been received and Alice confirms that they are measuring either in message mode
5. Bob compares the measured value and the sequence value that he has.
    - If they agree then Bob announces success. They both assign

      n = n + 2 and check to see if the sequence has now been completed. If not they continue, otherwise they stop
    - If the bits are not the same then the abort the exchange and authentication fails

Authentication

Control mode (Check bits)

- The protocol proceeds as above except that for each pair in the sequence the second bit is allotted a new random bit (d = 0 or 1).
- Bob measures as in the message mode and obtains d’
- He informs Alice that he has received the qubit. Alice announces that this stage is in control mode and the value of the random bit d
- If d = d’ then then Bob announces success. They both assign n = n + 2 and check to see if the sequence has completed. If so then success they are authenticated
- If d is not the same as d’ then the protocol is aborted

The Quantum Tripwire

This protocol is a method for detecting an intruder on a system by:

Petr M. Anisimov, Daniel J. Lum, S. Blane McCracken, Hwang Lee, Jonathan P. Dowling

The abstract runs as follows

We present here a quantum tripwire, which is a quantum optical interrogation technique capable of detecting an intrusion with very low probability of the tripwire being revealed to the intruder. Our scheme combines interaction-free measurement with the quantum Zeno effect in order to interrogate the presence of the intruder without interaction. The tripwire exploits a curious nonlinear behaviour of the quantum Zeno effect we discovered, which occurs in a lossy system. We also employ a statistical hypothesis testing protocol, allowing us to calculate a confidence level of interaction-free measurement after a given number of trials. As a result, our quantum intruder alert system is robust against photon loss and dephasing under realistic atmospheric conditions and its design minimizes the probabilities of false positives and false negatives as well as the probability of becoming visible to the intruder.

Quantum Malware

- Quantum Man on the Side Attack

Activity 4

Activity 4

1. Using a shared sequence as in the above authentication protocol simulate a possible exchange between Alice and Bob
2. What would be the effect of a man in the middle attack on the authentication protocol?
3. Follow the link https://arxiv.org/abs/1002.3362 to the quantum tripwire paper and using a search engine as required explain the following:
    1. What is Interaction Free Measurement?
    2. What is a lossless Mach-Zehnder interferometer and a Dark Port?
    3. What is the quantum Zeno Effect?
    4. Explain in overview how an intruder is detected using this system without knowing
4. What is a Quantum Man on the side attack?
5. What other forms of Malware can you find. Include an explanation in overview of each attack.