MARKET BRIEF

Quantum Cryptography

The spectrum of threats and types of attackers targeting corporate business information systems are growing, creating security concerns for businesses. At the same time, public and private standards applied toward information protection are becoming increasingly stringent. In this environment, businesses are paying increased attention to new measures that enhance security. Quantum Cryptography is an emerging security technology that may offer some new protection measures.

Cryptography

Cryptography is a centuries-old method of communicating sensitive information between two parties in such a way that a third party is restricted from obtaining it. For example, Rose and Fred need to communicate sensitive information. Rose uses an algorithm, called a cipher, to convert the message into unintelligible cipher text (encryption), which can then be sent through an open channel. Fred receives the message and must apply a matching cipher to convert the message back into plain text (decryption). The ciphers are controlled by a set of parameters, called a key. The key is a tool used to encrypt and decrypt. Quantum Cryptography is centered around this key. Both parties, Fred and Rose, must have a key.

There are two types of Cryptography, Public Key Cryptography and Private Key Cryptography. The method in which the keys are distributed is the differentiator. The simplest and the most ancient form of key sharing uses private keys. Private Key Cryptography uses identical keys for encryption and decryption. Rose takes a message, puts it in a safe box, locks it with a key, and ships the box to Fred. Fred uses the same key to unlock the message. The issue is that two keys are needed in separate locations. Frequent and reliable key distribution is needed with this type of cryptography. If the key were compromised, it would be difficult to replace.

Public Key Cryptography was ushered into existence by the computer age. With this method, different keys are used for encryption and decryption. Encryption is done with a publicly announced key, which encrypts with bits. Today, 128 bit encryption is being used. Decryption is completed using a private key, which is not shared. The idea is that individuals looking to receive encrypted messages send out encryption keys publicly, while keeping private keys for themselves. The secrecy of the keys relies on computational complexity of certain hard mathematical problems. However, mathematics is constantly advancing. Someone could develop an algorithm that could break or solve the current mathematical problem. In addition, eavesdropping on the key is currently not detectable. That means that users do not know if someone is tampering with their keys. Quantum key distribution can help solve some of these issues.

Architecturally, quantum technology enhances Private Key Cryptology by making the exercise of key sharing difficult to compromise. On a high level, quantum-based transmissions can exist only in uncompromised networks where no third party connections are made. If a quantum-based transmission is wiretapped, it is designed to cease to exist.

Quantum Key Distribution

Quantum Cryptography has nothing to do with the process of encryption by itself. Quantum Cryptography is focused on the actual transmission of the private key from the party that encoded the message to the party that is going to decode it. When applied to cryptography, quantum technology exists in the form of Quantum Key Distribution (QKD) protocol. Proposed in 1984 by two IBM engineers, quantum physics enables the basic principles of QKD operation.

In the case of quantum cryptography, particles used to transfer information are called quantum bits (qubits). An important quality of these particles is that they can only be measured once and in a

What Makes Quantum Key Distribution Desirable?

Quantum Cryptography in general relies on the laws of quantum mechanics. This happens because the transmission is carried by a single particle, which indeed can be measured only once. A consequence of the single measurement is that it is possible to detect eavesdropping.

at&t

pre-set manner (basis). Measurement actually destroys qubits; therefore, measurement only takes place one time. The party doing the measurement has to be aware of the basis (measurement manner) of qubits beforehand. A measurement executed with the wrong basis will create uneven results that won't be useful to encode a message.

If qubits are used as information carriers, they are designed to transport information only once, and to the party intended as the recipient of the exchange. In any other scenario the information should get lost. To set this up, parties would have to be in agreement as to which basis they are going to be using to measure the traffic, and use a reliable line that would enable a single measurement take place.

Quantum Key Distribution Protocol

Transmission and Measurements
There are three random number generators. (2 for Rose, 1 for Fred)

In each time slot:

1. **Rose randomly chooses a bit value (0 or 1) and a basis (B1 or B2)**
2. **Fred randomly picks a basis for his measurement (B1 or B2)**

Basis Reconciliation (happens in the clear after measurements completed):

3. **Both Rose and Fred send to the other what sequence of bases they had used. Using that, they decide which bits to keep (those in matching bases)**

Resulting Key:

4. **Rose records the bits she sent out (during the slots chosen in 3) and Fred knows the bits from his measurements (in those same slots)**
5. **A small fraction of the key is sacrificed (sent back in the clear) to measure the Quantum BER (QBER: Quantum Bit Error Rate) and help detect eavesdropping**

What Happens if a Bit is Intercepted?

- **Jane, a third party, intercepts a bit. Lost bits do not contribute to the final key**
- **Erin, another third party, intercepts a bit and measures it. Since the basis is unknown to Erin at the time of her measurement, she cannot gain any information about that bit**
- **Ben intercepts a bit and sends it to Fred. In practice, Ben can only send a random value in a random basis. This raises the Quantum BER measurement to 25% from the normal level of about 1%, indicative of unusual activity. The transmission is stopped**

From quantum concepts flows the IEEE protocol. The baseline principle underlying the protocol is that the encryption key is developed anew every time a reliable/uncompromised communication pattern is established.

Communication that leads to development and exchange of a private encryption key starts with making the first contact. In a specific time slot the sender picks random (1 or 0) values for bits transmitted. The sender also randomly chooses the basis used to measure these values.

As the second step, these values and basis selections are sent to the receiver of the information. The receiver randomly picks the basis for measuring the values that are being transmitted. A measurement is performed on the bits received and the sender and receiver can now conduct the basis reconciliation. Because qubits are destroyed after they are measured, the reconciliation cannot be conducted on an open channel.

The third step is a reconciliation of basis methods. Having decoded the bits with a certain basis, the receiver sends the decoded information back to the sender. The sender and receiver send each other what sequence of bases they had used. Using that information, they decide which bits to keep: the bits in matching bases. The sender then knows which basis to use to encrypt bits going forward.

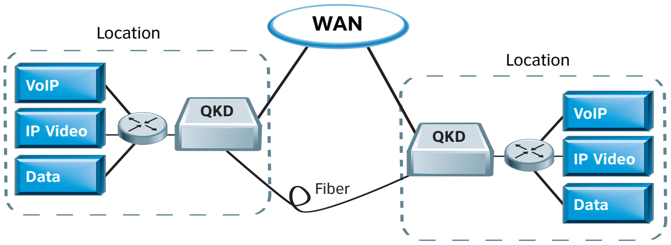
As a final step, the sender uses the basis that is resulting from the bit match to send the sequence of bits that is actually a key needed to decrypt the message.

QKD also prescribes for the receiver to send back a portion of the key upon receiving it to see if any of the data gets destroyed. This would only happen if the wireline connection has been compromised and a third party tapped into the line.

QKD-Based Products and Services
At present time, product development based on QKD is limited, but several communications companies are conducting product research. Thus far QKD is installed as a functionality of a VPN gateway. In one instance, the product is a chassis that supports VPN encryption for data encoding and fiber-based quantum encryption for key distribution. In a deployment scenario, chassis like this are always deployed as a pair, with a single fiber optic strand linking them. The physics of light is such that a signal generated within a fiber strand loses focus and smudges over distances greater than 100 kilometers. Thus if deployed in situations when VPNs have to travel further than the distance that fiber signal can travel without amplification, QKD-based gear has to be deployed in a daisy configuration. More commonly, QKD-based gear is confined to metro deployments at this time.

Today, the architecture of a QKD-based solution allows for VPN encryption to happen as it would ordinarily, and for the private key to be generated and shared via QKD. For now, costs involved in developing such a product make QKD-based VPN service impractical for mainstream deployments. A pair of QKD-supported platforms could cost as much as $100,000, not cost-prohibitive for a reliable communications product, but significantly higher than most other VPN gateways.

Quantum Cryptography



This is an illustration of Quantum Cryptography. Cryptographic keys are agreed upon over the dedicated fiber. Data communication of any IP service is encrypted by these keys (IPSec or AES).

Services enabled by QKD-based gear will invariably be IP VPNs of various types. As product architecture suggests, QKD-based products could exist as stand alone key sharing devices, or to be incorporated into an existing VPN setup.

Summary

QKD-based encryption is just emerging as an option for helping to secure information exchange, and can be used in conjunction with existing VPN service offerings for businesses needing communication services for content requiring a higher degree of confidentiality and protection. Traditionally such services are deployed by government agencies in need of routine protected communications, or by the financial services and healthcare industries that need to help protect sensitive customer information. Businesses are examining various architectural solutions to understand the potential benefits Quantum Cryptography may provide. Future implementations of this technology may make it more available for enterprise businesses.

European researchers recently broke a distance record for transmitting quantum information. Using a laser emitting pulses of light, the team was able to extend signal reach to 144 kilometers. The research team would like to improve the lasers and detectors to enable communication between satellites and ground stations, which would allow encryption keys to be sent from many locations to other locations. The ultimate goal is to create worldwide quantum communication.

For more information contact your AT&T Representative or visit us at www.att.com/business.

09/11/07 AB-1151

at&t
Your world. Delivered.