Shedding Light on Quantum Cryptography

ICTN 6875

Curby Simerson

Shedding Light on Quantum Cryptography

Abstract

In a networked environment, hosts exchange data at, sometimes, near the speed of light. Even with this speed, an interceptor with minimum effort can easily find himself in the possession of someone else's information. To that end, users must insure that it is protected by all means. In this document, the technique of cryptography is explored and discussed at a low level to include algorithmic methods and various versions. More specifically, quantum cryptography will be discussed at first from its inception, its categories and families of protocols, and then disclosing the latest findings and information on this innovative technology.

Introduction

As data is stored on hard drives, flash drives, discs, and such it would be satisfying to have a peace of mind that its integrity will maintain uncompromised. Data can become vulnerable to devastation by hard drive failures or malfunctions in the electronics of the PC. It is for this reason data backups are created, or arrays of disks for data retrieval is established by having it spread out amongst other discs and create an index of where it all is stored. But while data remains intact and appears to be safe from hardware failures, the need to protect it from prying eyes or foreign systems has become a must. Several ideas in the form of intellectual property, or system designs for a corporate airline are desired to be kept secure and away from those that would benefit from their exposure. There are many cases of data or information being stolen and used to profit the scandalous. In recent years, we've seen medical records from government agencies, credit card users' personal information, including social security numbers, and even financial records from banking institutions taken and become the illegal property of the common criminal. Efforts are made to secure the data by keeping them behind locked doors, posting data handling policies, and examining critical areas of business for data abduction. A common exertion to safeguard steady state data is, amongst the aforementioned methods, to also password protect or encrypt the data. In the undesirable event the data is then stolen, thieves are then less easily able to retrieve their bounty.

When data is propagated across a network, it is obviously more vulnerable than data stored on hard drive. Like a parents' sixteen-year-old taking his first drive by himself, network traffic is

more susceptible to harm or confiscation due to traveling within unsecured zones and without the protection of a guardian. There are many various software programs that allow hosts, other than the proper recipients, to retrieve packets unbeknownst to the source host. When data, such as a business' mission critical data, is transmitted, it is best to secure it with an encryption method. The art of encryption, cryptography, has been in existence for ages. Cryptography's origin dates back to the Egyptian's practice of hieroglyphics around 2000 B.C. and then again with Julius Caesar, overwhelmed with suspicion, encrypted his messages to his governors and officials (Pawliw, 2006). Data transfers over networks are simply another method of this century for communication with an understandable need for discretion.

Cryptography

Cryptography has a Greek foundation that is translated to mean 'hidden' or to be 'secret'. As mentioned above, hidden messages have existed for centuries, but modern day cryptography has an assumed meaning to apply with computer systems and their storage or transmitting of data. More specifically, cryptography involves the process and utilization of mathematics, engineering, and computer science to turn ordinary data into an unreadable nonsense cluster of data that only the intended recipient should be able to translate (Vittorio, 2002). In order to decipher the data message, the recipient would find it necessary to obtain a key to the cryptographic method. In other words, the recipient would need to know how the message was encrypted so it can undo what was done to make it gibberish. Though there are many types and methods of encrypting, or hiding, data within a data communication network, for example steganography, the main focus of this paper is quantum cryptography.

Quantum Mechanics

In order to understand quantum cryptography, a basic understanding of quantum mechanics needs to be discussed. Quantum mechanics refers to the principles surrounding all physical systems at the subatomic level. Amongst other objects, as it applies to the topic here, it describes the characteristics of light waves, or photons, and the prediction of probabilities these particles with undergo in application. The direction and movement of photons are better understood, applying the theorem of quantum mechanics, and appear to be able to be regulated in such a way that they are controlled (Wikipedia, 2009).

Cryptography Tribulations

The main function of cryptography is to hide messages (data) from the interceptor or eavesdropper. In order to successfully decrypt a message that has been encrypted is by knowing the method of encryption, cipher, and having the key for decrypting it. In the modern era of encryption, the key is used in conjunction with the plaintext as an input to the algorithm that encrypts the data, and in the same respect, decrypts it. These keys are essential to having the decrypting solution and are considered sacred. As long as the key is secure, the encrypted text, cryptogram, can be sent entirely across public networks without much worry. If it is intercepted, the message cannot be deciphered without the key.

Two hosts that are going to transfer an encrypted method across a network will have to negotiate a key. The symmetric-key cryptography describes the early method of encryption algorithms by which the same key is used to encrypt as well as decrypt the message. The key must be negotiated, and if an interceptor eavesdropping on the negotiation compromises the key, the message can be seized, decrypted, and becomes the illegal property of the hacker. This key distribution (negotiation) problem was carefully considered and a better replacement in the mid-1970's was created with the public key cryptography (PKC) (Lutkenhaus, 2009).

In public key cryptography (also called asymmetric-key cryptography) there are two keys, the public key, which is typically used to encrypt the message, and the private key, which is typically used to decrypt it. These two keys are mathematically related to one another, however, the algorithm used to determine the private key from the public key is an intricately complicated mathematical function with an input of at least 128 bits can have an output of approximately 10^38 possible choices. To understand the relative improbability of the keys being discovered, Salvatore Vittorio explains, "a billion computers doing a billion operations per second would require a trillion years to decrypt it." (Vittorio, p. 3) Although the probability of a public and private key being compromised after successfully configured on the proper machines, the problem arises in the fact of how the end hosts obtain the keys they should be configured with. Some sort of communication is required to exist in order to properly configure the hosts that are geographically separated. Whether the distribution method is by mail carrier, by telephone, or via e-mail, there is a sense of insecurity involved that could compromise the key's veracity.

A method of key distribution that claims to have unquestionable safeguarding is quantum cryptography.

Quantum Cryptography

The idea of quantum cryptography began with Stephen Wiesner in the late 1960s and early 1970s. He introduced quantum conjugate coding that went unrecognized by the Institute of Electrical and Electronics Engineers until approximately a decade later when it was revised and applied specifically to securing communications by Charles H. Bennett and Gilles Brassard. Photons were discovered to more appropriately be applied to data transmissions instead of storage, as Wiesner had mainly presented in the 1970s (Bennett, 1991).

The primary purpose of the quantum cryptography technology is only to establish the key distribution. It is not used to send the actual encrypted message.

Although it is theoretically possible to implement quantum cryptography on copper cabling, the most practical and widely used application is with fiber optic cabling and the properties of the light propagating through the medium. The premise of quantum cryptography lies with the polarization of light through a polarization filter, and its expected angle once polarized.

The sender will choose from one of two orthogonal basis, rectilinear or diagonal, to transmit the bit. The rectilinear basis is using a polarization filter is either vertical, represented by 0 degrees, or horizontal, represented by 90 degrees. The diagonal basis is using a polarization filter that is either at 45 degrees or 135 degrees. The sender then prepares the bit with the chosen basis and transmits the signal. The sender then records the basis, angle, and time of the photon sent.

When the signal is received at the recipient, the recipient does not know which orthogonal basis was chosen and randomly chooses a basis. The recipient will then measure the photon and record its basis, angle, and time.

Both hosts continue this process until all bits for the message are completely sent. Once all the photons are sent and received, the two hosts send their recorded basis, angle, and time for each bit transmitted.

The principle behind quantum cryptography is the Heisenberg uncertainty principle, which states, “certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other” (Vittorio, p. 3). This principle applies to this process because the recipient doesn’t know the basis chosen by the sender and the probability of the recipient choosing the correct basis is uncertain. Once the transmission is complete and the two hosts have exchanged their chosen bases, all the bits where the recipient chose incorrectly are discarded. It is expected that about half of the bases will be correctly chosen. The shared key will be the remaining bits.

Attacks on Quantum Cryptography

In the event the public quantum channel has an eavesdropper, the properties of the photons received by the recipient will be so disturbed that they would have given erroneous results to the correctly chosen bases. The eavesdropper would have intercepted the bit and had to randomly choose the basis and then send the intended recipient the result it got, where the recipient would then randomly choose a basis on what the eavesdropper had randomly chosen. If the eavesdropper chose correct then the intended recipient would then see a bit that would appear unattested and pure. However, if the eavesdropper chose incorrectly, it would send the intended recipient the incorrect polarization basis and then the intended recipient may or may not chose the correct basis. In this event, if the recipient chose the incorrect basis, then it would discard the bit once it sends the source its summation of the negotiation at the end of the transfer and nothing is noticed. But if the recipient chose the correct basis, on a bit that was disturbed from the eavesdropper, then when the recipient sends the summation to the sender and that particular bit should have matched the senders, then it will be recognized that an eavesdropper is present. If this occurs, the randomly chosen bits creating the secret key would be discarded and the entire key distribution process would have had to be completed again. It is essential that the two end hosts do not discuss the summary of the basis and angles until the transmission is complete. If this information is offered during the process, the eavesdropper could modify its signals to the intended recipient and neither host would know that it existed.

If the transmitted bits used in quantum key distribution have errors in excess of the twenty percent globally recognized threshold (Wikipedia Quantum_Cryptography), it is understood that there is either an eavesdropper on the line, or there are imperfections in the quantum channel. Since it is virtually impossible to determine which is causing the errors, it is suspected to be an eavesdropper, and the key distribution process is restarted.

Another common attack that could be imposed on hosts negotiating a key is the man in the middle attack. If a computing device has sufficient processing and transmission speeds, it can impersonate both hosts. The interceptor can completely receive and respond to the sender of the original source, and can also become the source for the intended recipient. With this attack, the two hosts are completely unaware of the existence of the interceptor because their negotiation is conducted without any flaws. To combat the "man-in-the-middle" attack, the sender and recipient should configure authentication protocols.

As described by Fu-Guo Deng and his associates in their paper, "Robustness of two-way quantum communication protocols against Trojan horse attack", there are three types of Trojan horse attacks that can be ran on quantum channels (Deng, 2006). The first is a common Trojan horse that simply sends a large photon burst to any transmitting host between transmissions. The host will then have its polarized state reflected back to the hacker's machine. To guard a machine from this first Trojan horse attack, an optical isolator can be placed on inline to keep light from entering the machine.

The second and third types of Trojan horse attacks are the delay-photon and invisible Trojan horses. The interceptor in both cases will intercept a signal and place a fake photon with a delay time shorter than the time window (delay-photon attack) and an invisible photon (invisible attack) within the signal before sending it to its destination. The recipient's machine doesn't detect either of the photons and when it resends a signal, the interceptor can retrieve the inserted photon and learn about the machine's operation with measurement.

Summary

Quantum cryptography has come from being considered an impossibility in the 1970s, to currently being a reality in mainly governments and corporations that require high-levels of security. It has gone from allowing transfers at 10kbps (Johnson) to over 1Mbps (Lutkenhaus) and according to a group from Cambridge they have made successful attempts quantum cryptography data transfers at a distance of 20km with a transfer speed of 10Mbps (Johnson). Recent evidence of a push to make this technology standardized for quantum key distribution is evidence of a growing acceptance in the industry. Quantum cryptography has a promising future and is getting its necessary attention with its robust security potential.

Works Cited

Bastien, Greg & Degu, Christian Abera. (2004). *CCSP Self-Study CCSP SECUR Exam Certification Guide*. Indianapolis, IN: Cisco Press.

Bennett, Charles H. et al. (September 1991). Experimental Quantum Cryptography. *Journal of Cryptology*, 5, 1, pages 3-28.

Cisco Systems, Inc. (2004). *Fundamentals of Network Security*. Indianapolis, IN: Cisco Press.

Deng, Fu-Guo et al. (June 25, 2006). Robustness of two-way quantum communication protocols against Trojan horse attack. Retrieved July 2, 2009, from http://www.citebase.org/fulltext?format=application%2Fpdf&identifier=oai%3AarXiv.org%3Aquant-ph%2F0508168

Institute of Physics (2009, May 2). Computer Hackers R.I.P.: Making Quantum Cryptography Practical. *ScienceDaily*. Retrieved July 2, 2009, from http://www.sciencedaily.com/releases/2009/04/090430065454.htm

Johnson, Bobbie. (May 1, 2009). Cambridge team makes quantum cryptography practical, at last. Retrieved on June 26, 2009, from http://www.guardian.co.uk/technology/blog/2009/may/01/quantum-cryptography.

Le, Mr. Tom K. & Yu, Dr. James H. (2001). Internet and Network Security. *Journal of Industrial Technology*, 17, 1.

Leurent, G. (2008) 'Practical key-recovery attack against APOP, an MD5-based challenge-response authentication', *International Journal of Applied Cryptography*, Vol. 1, No. 1 pp.32–46.

Lutkenhaus, N and Shields, A. J. (2009). Focus on Quantum cryptography: Theory and Practice. New Journal of Physics. Retrieved on July 3, 2009, from http://www.iop.org/EJ/abstract/1367-2630/11/4/045005.

Minty, Dr. Gordon (2003). The Future History of Industrial Technology. *Journal of Industrial Technology*, 20, 1.

Pawliw, Borys. (January 13, 2006). Cryptography. Retrieved on June 21, 2009, from http://searchsoftwarequality.techtarget.com/dictionary/definition/214431/cryptography.html.

Rosenthal, David A. (2002). Cryptography Decrypted – Book Review. *Journal of Industrial Technology*, 18, 2.

Wikipedia Contributors. (2009). *Quantum Cryptography*. Retrieved on June 21, 2009, from http://en.wikipedia.org/wiki/Quantum_cryptography.

Wikipedia Contributors. (2009). *Cryptography*. Retrieved on June 23, 2009, from http://en.wikipedia.org/wiki/Cryptography.

Vittorio, Salvatore. (October, 2002). Quantum Cryptography: Privacy Through Uncertainty. Retrieved on June 26, 2009, from http://www.csa.com/discoveryguides/crypt/overview.php.