Vegas 'Quantum Spookshow' Demos On-the-Fly Encryption of Streaming Video

August 6 2008

Las Vegas shows often are on the cutting edge. Following this tradition, researchers from the National Institute of Standards and Technology (NIST) and their colleagues at the National University of Singapore (NUS) have landed gigs this week at Caesar's Palace and the Riviera Hotel and Casino to perform live demonstrations of quantum cryptography, theoretically the most secure form of encryption.

Appearing at two major venues of the information security industry, known as the Black Hat and DEFCON meetings,* the researchers will showcase the increasing practicality of quantum cryptography.

In the NIST portion of the "Quantum Spookshow," an exhibit-hall demonstration presented with NUS, a web cam will capture live video, scramble it using quantum cryptography, and broadcast the decrypted video. The bit rate of the quantum-encrypted video is targeted to exceed 300,000 bits per second (bps), a quality higher than that of popular video-sharing Web sites. The NUS group will demonstrate a reduced-size next-generation quantum cryptography system that uses pairs of interlinked or "entangled" photons and very simple hardware.

Aptly enough for the City of Lights, these two systems employ photons—particles of light—to create the secret key, a random series of digital bits, each representing 0 or 1, which is used to encrypt and decrypt messages in real time. In the NIST high-speed wireless setup, an infrared laser generates the photons while small telescopes with 8-inch mirrors send and receive the photons over the air. The system uses the

most secure version of quantum key distribution (QKD), known as the "one-time pad," in which one bit of key is produced for every bit of video that is transmitted.

Once a secret key is created, it is used to encrypt video data, which then are sent over an Ethernet cable. The data are decrypted by a receiver in real time using PC-compatible circuit boards designed and built at NIST. With a transmission capability of up to a billion bps, the NIST system makes QKD practical for encrypting streaming video and other applications.

Nonetheless, there are points of weakness in any quantum cryptography system. At the demonstrations, participants will have a chance to discover vulnerabilities through hands-on interactions with the systems. In NIST's simplified setup, participants can put a filter in front of the telescopes, causing error rates to skyrocket and making it impossible to generate enough key to encrypt video. Identifying subtler security loopholes in real-world environments is a major research objective of practical quantum cryptography. Participants are invited to find and discuss security loopholes in the system: the NUS group has made their code open source, and it can be found at code.google.com/p/qcrypto .

The NIST work in this field was supported by the Defense Advanced Research Projects Agency, and includes researchers who work at the Joint Quantum Institute, a research partnership of NIST and the University of Maryland. The NUS component was supported by Singapore's Centre for Quantum Technologies and its Defense Science and Technology Agency (DSTA).

* Quantum Spookshow, at Black Hat Briefings, Caesar's Palace, Wednesday, Aug. 6, 1:30-7:30 p.m., and Thursday, Aug. 7, from 12:00 to 6:00 p.m.. At Defcon 16, Riviera Hotel and Casino, Friday, Aug. 8, and Saturday, Aug. 9. Also: Joshua Bienfang, "Free-Space Quantum Key

Distribution at GHz Transmission Rates," Turbo Talk at Black Hat Briefings, Thursday, Aug. 7, 4:45 p.m.

Provided by NIST