World Cup Security Uses Physics To Thwart Hackers

June 21 2010, By Devin Powell

South African physicists working to protect data networks at the World Cup hope to provide something that no goalkeeper can promise: perfect defense. They're tapping the laws of physics to prevent hackers from monitoring videos, emails and phone calls relayed between Durban's Moses Mabhida Stadium and a nearby operations center for police, firefighters, and military personnel.

The stadium's quantum cryptography system, installed by researchers at the University of KwaZulu-Natal in Durban, is an emerging technology thought to be in regular use by military and intelligence organizations but rarely showcased on such a public stage.

"The goal is to ensure not only the confidentially but also the integrity of this information," said Gregoire Ribordy, CEO of ID Quantique in Geneva, which developed the system with Senetas Corporation in Australia. ID Quantique, whose clients are primarily military and financial organizations, used similar technology to secure ballot information in the 2007 Swiss elections.

Data -- whether ballots or stadium security footage -- flows over fiber optic cables as a series of ones and zeros that can be stolen by hackers, who can tap into and monitor a line. To protect the information, it is often encoded in a way that can only be unlocked with a key. This key is often a second string of ones and zeros transmitted over the same line as the data.

Traditional means of encrypting such a key use mathematical functions that are difficult -- but not impossible -- to undo.

Quantum cryptography, on the other hand, uses the principles of quantum mechanics to provide theoretically uncrackable security. It sends the key as a series of particles of light, or photons. Because the act of observing one of these "quantum bits" fundamentally changes it, eavesdroppers can't help but reveal themselves -- in theory.

In practice, the equipment developed to send photons back and forth is not perfect -- some of the photons are lost, some are transmitted incorrectly -- so anyone receiving a quantum key must expect a certain level of error. A clever hacker might be able to figure out a way to disguise eavesdropping as error, said Hoi Kwong Lo of the University of Toronto. Last month his team was the first to hack an ID Quantique system in a laboratory -- albeit a less secure version than the one in use at the World Cup.

"I think it's premature to say whether commercial systems are secure or

not," said Lo. "It's much easier to hack a system than to make a system secure."

First proposed more than three decades ago, quantum cryptography has only been developed into commercial systems in recent years. The World Cup system, installed in April by researchers at the University of KwaZulu-Natal's Centre for Quantum Technology, is part of a larger plan to deploy quantum security systems throughout Durban.

Provided by Inside Science News Service