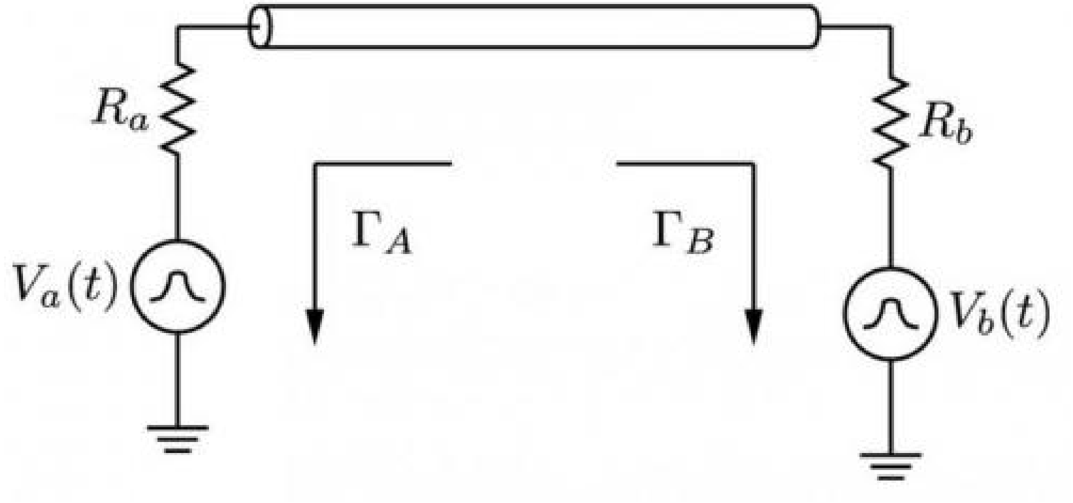
Attack on classical cryptography system raises security questions

December 17 2014, by Lisa Zyga



In the Kish key distribution (KKD) system, the two resistance values represent the states of an information bit. A cryptographic key is transmitted along the wire by randomly switching between the two resistance values, which can be detected by the sender and receiver via their thermal noise on the line. Since no net power flows through the line, the only way that an eavesdropper can measure the resistance values is by injecting current into the wire and measuring the voltage and current changes in each direction, but the extra current would be quickly noticed. Credit: Gunn, et al. ©2014 *Nature Scientific Reports*

(Phys.org)—How secure is completely secure? In the world of secure communication, a scheme may be completely secure until it's not—that is, until an attack is proposed that reveals a weak spot in the scheme. This is what's currently going on for Kish key distribution (KKD), which claims to derive total and unconditional security using classical rather than quantum techniques, thus avoiding the complexity and expense of quantum cryptographic schemes. But now a new paper has uncovered a vulnerability in KKD that enables an eavesdropper to correctly determine more than 99.9% of the transmitted bits. Fortunately, countermeasures may exist to protect against this attack and regain the system's security.

"The worthiness of a cryptographic scheme is measured by the number of papers that try to attack it," Derek Abbott, Professor at The University of Adelaide in Australia and coauthor of the new paper, told *Phys.org*. Abbott and coauthors Lachlan J. Gunn and Andrew Allison have published their paper in a recent issue of Nature's *Scientific Reports*.

By Abbott's measure, KKD has proven to be very appealing (as many people have tried to attack it) since it was first proposed in 2005. Notably, KKD has stood up to attacks from Amnon Yariv (2009 winner of the National Medal of Science) from Caltech, as well as Charles H. Bennett of IBM. Bennett co-developed the first ever quantum cryptography protocol in 1984 (he is the first "B" in the so-called BB84 protocol).

Security from thermal noise

In the 2005 paper that first introduced KKD, Laszlo B. Kish, Professor at Texas A&M University, described a system that promises unconditional security from the second law of thermodynamics. The scheme transmits a cryptographic key along a wire by randomly switching between two resistor values, which represent the states of an information bit, at the two ends of the line. The sender and receiver passively detect each other's resistance values via the thermal noise on the line. Each time the two parties determine each other's resistance values, they secretly share one bit of information.

Because the second law prohibits net power from flowing from one resistor to another when the system is at equilibrium, a potential eavesdropper cannot determine the resistance values. The only way an eavesdropper could intercept the bits is by injecting current into the wire and measuring the voltage and current changes in each direction to determine the resistance values, but the extra current would be quickly noticed.

The design of the KKD system relies on a thorough understanding of the physics of waves traveling through a transmission line. One debatable requirement for unconditional security in KKD is that transmission lines prohibit the propagation of waves that are below a certain frequency, $v/(2L)$, where L is the transmission line length and v the signal propagation velocity. This restriction is claimed to arise from the fact that wave modes do not propagate below this frequency.

In the new paper, the researchers show in simulations and experiments that waves with frequencies below this critical value do actually propagate along the transmission line. The reason, they explain, is that at low frequencies a coaxial cable supports TEM (Transverse Electromagnetic) modes, which have no low frequency cutoff.

The researchers detected the existence of propagating TEM waves on a coaxial cable by constructing a directional wave measurement device, which they then used to successfully eavesdrop. They showed that, merely by measuring the TEM waves traveling along the transmission line, an eavesdropper can determine both resistor values, allowing them to correctly intercept more than 99.9% of the bits without being caught.

Attacks, counterattacks: the cycle continues

Although this sounds bad for KKD, it in no way spells the end for the cryptographic scheme.

Already, several critiques of the new attack have been proposed in response to a preprint of the paper. Several critiques argue that the signals in the transmission line are not actually waves for a variety of reasons, such as flaws in the model, insufficient power on the line to excite wave modes, and not meeting the definition of a wave. However, the Adelaide team refutes each of these arguments, in the latter case by pointing out that there is no definitive definition of a wave.

Returning to defend his system, Kish, along with coauthor Claes-Goran Granqvist, has proposed a countermeasure to the attack. They suggest that increasing the noise temperature on the side with the smaller resistance compared to the side with the greater resistance can remove an eavesdropper's information. The Adelaide researchers agree that this countermeasure may be effective as long as the sender and receiver are able to account for the noise difference in their measurements.

"The countermeasure has yet to be demonstrated in practice, and this is the next step," Abbott said. "It will be promising if it can be shown to work for practical bandwidths and cable lengths; this remains to be seen."

Looking at the bigger picture of secure communication, Abbott explains that even a system that is completely secure in theory is vulnerable to attack. In other words, there is no such thing as a completely secure scheme in the first place.

"The concept of 'unconditional security' is a Platonic idealization that is true only for the mathematical description of a cryptographic scheme," Abbott said. "Any physical realization can never be fully captured by such idealizations, and therefore in my opinion any cryptographic scheme is open to attack. Math is watertight, but the physical world leaks. At the end of the day, what matters is how many decades a given scheme can hold off an attack for. But this is notoriously difficult to predict."

More information: Lachlan J. Gunn, et al. "A directional wave measurement attack against the Kish key distribution system." *Scientific Reports*. DOI: 10.1038/srep06461

Citation: Attack on classical cryptography system raises security questions (2014, December 17) retrieved 25 April 2024 from https://phys.org/news/2014-12-classical-cryptography.html