Relay-Proof Channels using UWB Lasers

Bruce Christianson[1], Alex Shafarenko[1], Frank Stajano[2], and Ford Long Wong[2]

[1] University of Hertfordshire
[2] University of Cambridge

Consider the following situation: Alice is a hand-held device, such as a PDA. Bob is a device providing a service, such as an ATM, an automatic door, or an anti-aircraft gun pointing at the gyro-copter in which Alice is travelling.

Bob and Alice have never directly met before, but share a key as a result of secure hand-offs. Alice has used this key to request a service from Bob (dispense cash, open door, don't shoot). Before complying, Bob needs to be sure that it really is Alice that he can see in front of him, and not Mort.

Mort and her accomplice Cove are planning a wormhole attack along classic man-in-the-middle lines. They wait until Alice is in a situation where she expects to be challenged by Bob, and then Mort pretends to Bob that she is Alice, while Cove pretends to Alice that he is Bob.

Mort and Cove relay the appropriate challenges and responses to one another over a channel hidden from Alice and Bob, in order to allow the dual masquerade to succeed, following which Alice waits impatiently in front of a different ATM, or the wrong door, or another gun.

How can such an attack be prevented? Obviously it suffices if Alice and Bob both have a secure way of identifying their (relative) location to sufficient accuracy. But how can they do this?

Suppose that we could enclose Bob inside a Platonic Faraday cage, which blocks all information-bearing signals, not just the RF ones. At the end of the protocol run, Bob could be confident that Alice was also inside the Faraday cage. Provided the Platonic Faraday cage was of sufficiently small size and shape to satisfy the appropriate proximity requirement, Bob could proceed.

One way of providing such a Platonic Faraday cage is to use the laws of physics: for example distance-bounding protocols use the fact that the speed of light is finite[3].

In this position paper, we argue that the laws of information theory can be used instead. The key insight is that it doesn't matter if the Platonic Faraday cage leaks some information[4], provided the amount of information that Mort and Cove need to exchange is greater.

Previous work in this direction has relied upon restricting the rate at which Mort and Cove can communicate, essentially using a variant of covert channel analysis to reduce the rate of leakage. We propose the converse approach, using Ultra Wide Band (UWB) lasers to transfer so much information from Bob to

[3] Although there is some doubt in the case of entanglement: imagine a Josephson junction 30m wide changing state.
[4] Even Plato allowed for some information leakage.

the location where he believes Alice to be that only a fraction of it could be relayed by Mort.

The real Alice knows where to look for the crucial signal bits, which are hidden at different time and wavelength positions according to a pseudo-random series seeded by the shared key, but Mort is stymied.

The use of UWB is widespread at microwave frequency bands, but we believe the use of it in visible light spectrum (where the information packing density is higher) to be novel. The continuous pulse rate is high (Pbps) and the power is very low. Normally in UWB receiver and transmitter are matched. Here the objective is that they should be deliberately mis-matched, with the transmitter sending more pulses than it is possible for the receiver to distinguish.

Consequently, by the Nyquist-Shannon Theorem (Signal to Noise Ratio version), a receiver who does not know precisely which pulses to capture will be unable to capture more than a small proportion of them. Effectively the attacker cannot relay the whole side-channel signal without amplifying the noise to the point where the signal is undecipherable. The beam contains too much information for a feasible transponder array to re-broadcast, and cannot be reflected using known mechanical or optical means.

This makes the proposed UWB laser approach ideal for use outdoors: simultaneous use of two[5] narrow beam directional lasers from different positions on a baseline of suitable direction and length allows the position of a remote object to be accurately determined in three dimensional space.

In contrast, although the use of multiple simultaneous distance bounding protocols allows triangulation within the convex hull of the base points[6], objects cannot be located outside the convex hull with the distance bounding technique.

At the other extreme, on the small (tabletop) scale, the use of a single UWB laser allows a Platonic Faraday cage to be provided by a cardboard box.

References

1. Christianson and Shafarenko, 2006, Vintage Bit Cryptography, Security Protocols 14, LNCS 5087, 261–275
2. Clulow, Hancke, Kuhn and Moore, 2006, So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks, ESAS 2006, LNCS 4357, 83–97
3. Damgard, Nielson and Wichs, 2008, Isolated Proofs of Knowledge and Isolated Zero Knowledge, EUROCRYPT 2008, LNCS 4965, 509–526
4. Stajano, Wong and Christianson, 2010, Multi-Channel Protocols to Prevent Relay Attacks, Financial Cryptography 2010, LNCS 6052, 4–19

[5] In the variable position case it may be necessary to have three fixed-position lasers and choose which two to use depending on the desired position of Alice.

[6] For example, an accurate upper bound on distance from four non-coplanar points allows the responder to be located accurately within the tetrahedron which is their convex hull.