Keep your enemies close

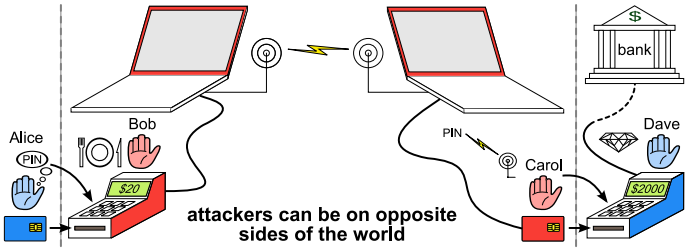
Distance bounding against smartcard relay attacks

Saar Drimer and Steven J. Murdoch

UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

Relay attacks

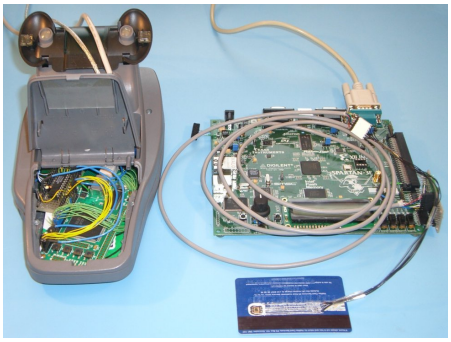
In the "mafia-fraud" scenario, an unsuspecting restaurant patron, Alice, inserts her smartcard into a terminal in order to pay $20. The terminal looks just like any other she has used in the past. This one, however, was tampered with by the waiter, Bob, to communicate with a laptop placed behind the counter, instead of the bank.



As Alice inserts her card, Bob sends a message to his accomplice, Carol, who is about to pay $2 000 for a expensive diamond ring at honest Dave's jewellery shop. Carol inserts a counterfeit card into Dave's terminal. This card is wired to a laptop in her backpack, which communicates with Bob's laptop using mobile phones. The data to and from Dave's terminal is relayed to the restaurant's counterfeit terminal such that the diamond purchasing transaction is placed on Alice's card. The PIN entered by Alice is recorded by the counterfeit terminal and is sent, via a laptop and wireless headset, to Carol who enters it into the genuine terminal when asked. **The result is that the crooks have paid for a diamond ring using Alice's money, who got her meal for free, but will be surprised when her bank statement arrives.**

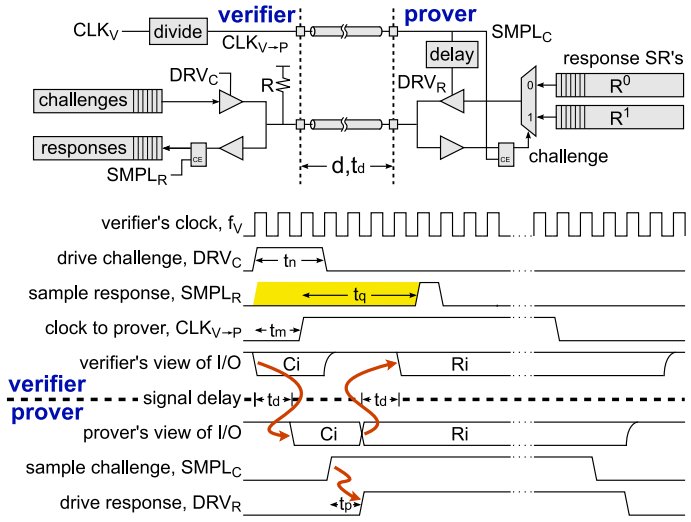
Implementing the attack on Chip & PIN

This really works. For less than $500 worth of commodity hardware and custom software, we modified a payment terminal, created a fake card and control circuitry, and designed a system that can reliably transmit data wirelessly between terminals anywhere in the world. We then executed the attack on live "Chip & PIN" systems, thus demonstrating that they are indeed vulnerable to these types of attacks. **To show that we have full control over the terminal, we also made it play Tetris.**

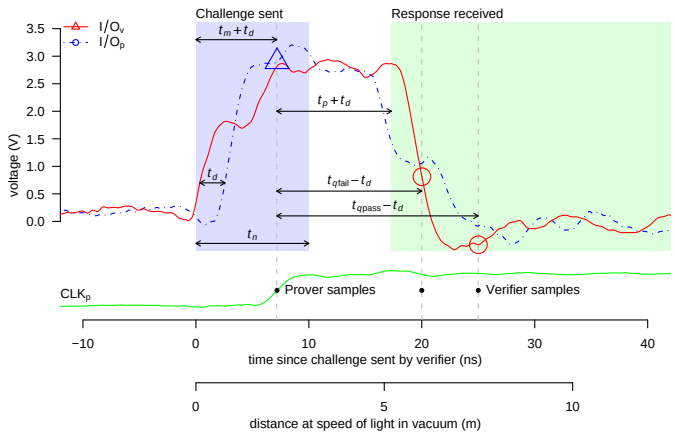


Distance bounding defence

Procedural changes are not adequate to completely defend against relay attacks. We therefore proposed and implemented a "distance bounding" protocol tailored for smartcards as used by Chip & PIN. This prevents an attacker from extending the intended distance between the terminal and card ("verifier" and "prover", respectively). Using the Hancke-Kuhn protocol as a base for our implementation, we adapted it to use synchronous half-duplex wired transmission. Our additions were designed such that most of the cost is added to the terminal, rather than the cheaper smartcards. The cardholder experience stays the same as does the interface between card and terminal: a clock and bi-directional I/O line.



The distance resolution we can achieve is defined by the operating frequency of the verifier and so should have a fast clock, whereas the prover can operate at low frequencies and use delay lines to derive critical signals. **We have tested the system with various transmission lengths and confirmed that it is indeed able to detect small additions to the signal transmission distance.**



For more information see `http://www.cl.cam.ac.uk/research/security/banking/`

2007-07-05