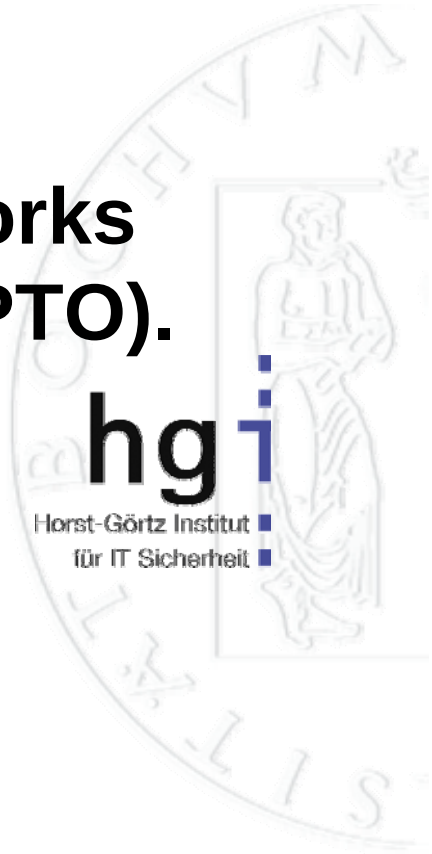
KeeLoq attack demo that usually works (or: Murphy's Law also holds at CRYPTO).



hgi
Horst-Görtz Institut
für IT Sicherheit

CRYPTO 2008 Rump Session

August 19, 2008

Timo Kasper, Christof Paar

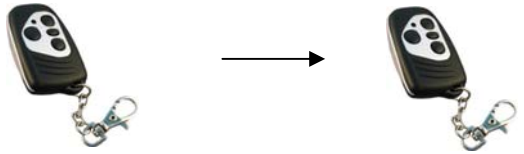
We are not alone

Horst-Görtz Institut für IT Sicherheit

So what can we do now (1) ?

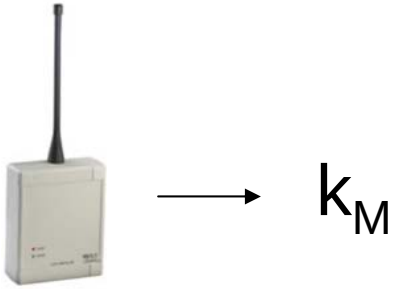
Horst-Görtz Institut für IT Sicherheit

1. If we have access to a remote:



   Recover device key and clone the device

2. If we have access to a receiver:

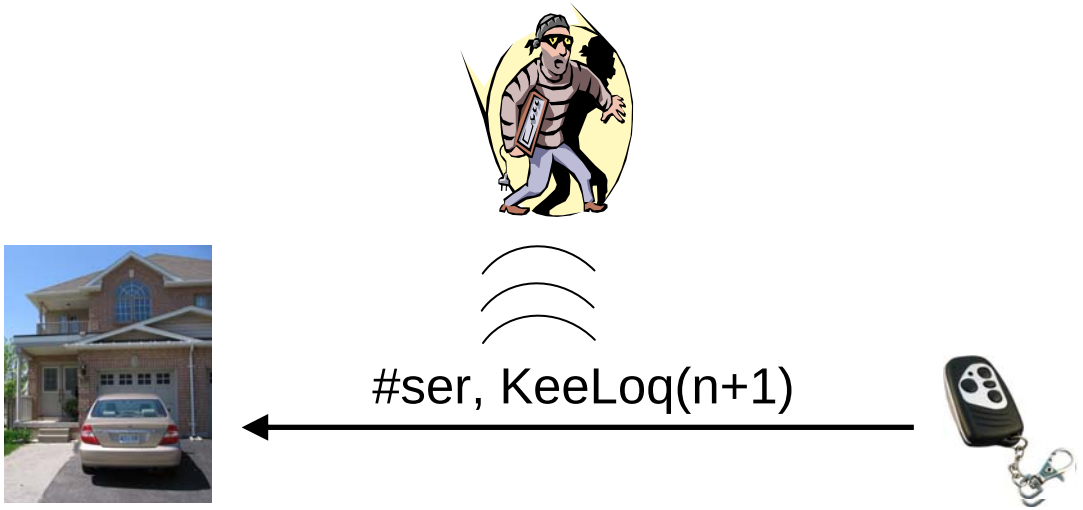


   Recover manufacturer key

So what can we do now (2) ?

After extracting of manufacturing key:

Remotely eavesdrop on 1-2 communications & clone key!



- works for all key derivation schemes
- might require a few hours of computation
  (Rem: not necessary for any system we‘ve analysed.)
- SCA attack is not specific to KeeLoq, e.g., unprotected AES is vulnerable too.

**! Side-channel step (recovery of manufacturer key, difficult)
can be outsourced to criminal cryptographers !**