Chaffing and Winnowing

How to provide security in plain sight

An idea by Ron Rivest (1998)

Not quite steganography

- Imagine the following transmission from someone to Bob:
  - X1: „Hello Bob, meet me at“
  - X2: „Hello Bob, Zoe will meet you at”
  - Y1: „the library at 7 pm.“
  - Y2: „the shopping mall at 8 pm.“
  - Z1: „Yours, Alice“
  - Z2: „Yours, Carol“.

  For each X, Y, Z, only one of the sentences is the right one. The other is just masquerade. But which one?

Wheat vs. chaff

Winnowing Separation thereof, common in agriculture since the Bronze Age.

Chaffing Mixing the two back together. No sane people ever do that.
(well, cryptographers may …)

MAC separates wheat from chaff

- MAC is basically a symmetrically keyed hash, which only Alice and Bob can produce/verify.
- Imagine that both parties have a shared secret and thus ability to produce keyed MACs.
- They can separate genuine messages from the rest by adding:
  - Correct MACs to the „wheat“.
  - Binary rubbish of the same length to the „chaff“.

Security aspects

- Only Alice and Bob can produce and verify valid MACs.
- ***Anyone in the middle*** can produce „chaff“, by generating bogus messages and appending random pseudo-MACs of the same length.
- For example, a firewall can do that automatically.
  - No one can distinguish messages from Alice and messages from the robotic firewall.
- **No encryption or steganography ever takes place!**

Practical aspects

- Abuses the bandwidth and the processor.
- The ratio of chaff to wheat can be made very high.
- ***In extremis***, we can send individual bits like this:
  - X1: 1 - Y1: 1 - Z1: 1
  - X2: 0 - Y2: 0 - Z2: 0

  where the ratio may be well over 300 : 1.