tHTP

« An OTA Solution designed with security* in mind »

* And fun ! ☺

Goals

- Common OTA solutions suffer from critical vulnerabilities that severely affect and lower the security level.

- But OTA solutions are easily deployed and low-cost.

- Need to build an OTA solution that benefits from both physical network security features and wireless softness.

- Solution : RFCs 1149/2549

RFCs 1149

- Pros
    - Free OTA Transport solutions
    - Medium easily avalaible
    - Low cost
    - Used for/by military communications applications
    - Easy rerouting features

- Cons
    - High delay
    - Low throughput
    - Low data transfer capabilities
    - Subject to many threats and vulnerabilites
    - Does not support fragmentation
    - No more fitted to modern usages.

Good basis : just need to improve & modernize -> tHTP

tHTP

- ## RFCs 1149/2549 Improvements
  - Lower delay
  - Higher throughput
  - Data transferred Crypted (AES) and signed (GnuPG)
  - All OS compatibilty
  - RFCs & De facto standards compliant
  - Secured by design*

- ## Capabilities
  - 13 Mb/sec min. throughput
    - Volume of data does not depend on transport media, can increase easily.
  - ZeroConf-like network routing (dynamic rerouting supported).
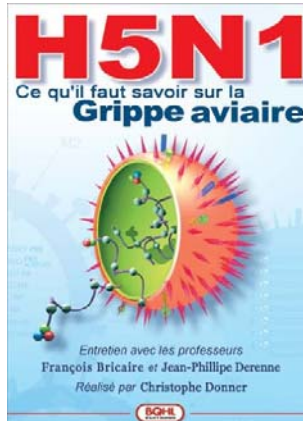
* And funny !

Demonstration

RFC1149 Implementations

Some typical RFC1149 OTA Implementations :

Typical RFC1149 Threats & Vulnerabilities :

tHTP Implementation

- Tiny Helicopter Transport Protocol

- MooSSTIC v1 : 1st tHTP operational implementation :

What's Next ?

- Capacity improvement
  - Better throughput
    - Up to TeraBytes transferred at once
    - Already in test in our Lab (Issy les Mlx Heliport)
- HPTables
  - HTP Firewalling solutions for Linux kernel
    - Unknown or unauthorized HTP messages are dropped by USB driven RST packets.
- IPv6 support
  - No, just kidding… ☺

Thanks !