In our ubiquitous environment, we desire:[1]

Availability
Sleep deprivation torture

Authenticity
Resurrecting duckling

Integrity
Tamper evident-ness

Confidentiality

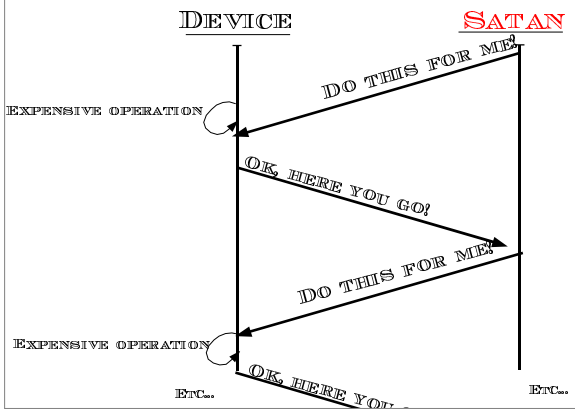
[1] The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks

Availability
vs.
Sleep deprivation torture

Sleep deprivation torture

Target battery powered, untethered devices:

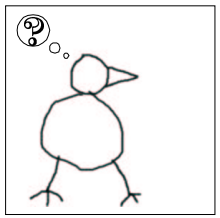
A unique denial of service attack



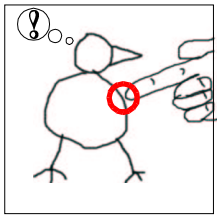
Authenticity
with
Resurrecting duckling

RESURRECTING DUCKLING:
IMPRINTING

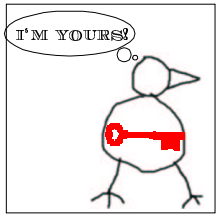
1



2

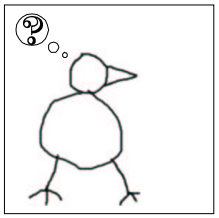


3



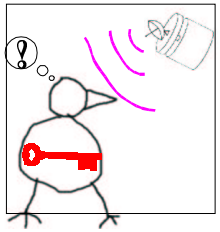
RESURRECTING DUCKLING:
REVERSE METEMPSYCHOIS

AND SO.°°



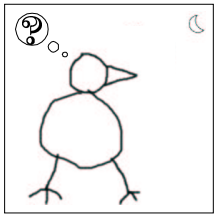
IT LIVES!

RESURRECTING DUCKLING:
ESCROWED SUPPUKU



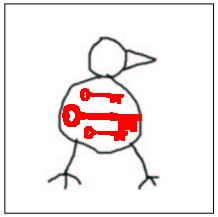
I

II



III

RESURRECTING DUCKLING:
ONE DUCK, MULTIPLE SOULS



MULTIPLE DEATH POLICIES

MULTIPLE OWNERS

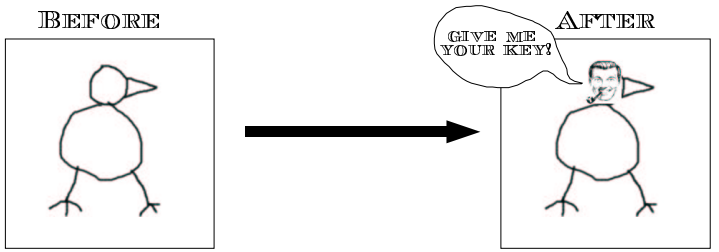
Integrity

thanks to

Tamper evident-ness

Integrity:

Tampering should be evident



Confidentiality

sayeth the paper:

> "easy once authentication has been solved."

Some Things To Note About Resurrected Duckling Protocol

It attempts to solve an authenticatioin problem.

Can it work for programs that wish to authenticate each other?

eg: my PDA wants to authenticate with the projector on the ceiling.

MORE SECURITY ISSUES TO CONSIDER

- ANONYMITY, PRIVACY WITHOUT AUTHENTICATION
- TRUST, OR AUTHENTICATION OF DEVICE
  - EG, DUCKLING AUTHENTICATES OWNER
- AUDIT LOGS
  - INTEGRITY, IRREFUTABILITY
- COMMUNICATIONS PROTOCOLS
  - BLUETOOTH, 801

BIBLIOGRAPHY

The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks, F. Stajano, et al., *Security Protocols, 7th International Workshop Proceedings*, 1999.

The Computer for the 21st Century, Mark Weiser, *Scientific American*, 9/91.

Security and Privacy, Nigel Davis, *IEEE Pervasive Computing*, vol.2 no.1, 3/03, p.20.