IN OUR UBIQUITOUS ENVIRONMENT, WE DESIRE:

**Availability**
Sleep Deprivation Torture

**Authenticity**
Resurrecting Duckling

**Integrity**
Tamper Evident-ness

**Confidentiality**

---

**Availability**
Sleep Deprivation Torture

**Authenticity**
Resurrecting Duckling

**Confidentiality**

---

**Sleep Deprivation Torture**
Target: Battery Powered, Untethered Devices

**Device**

- Do this for me.
- OK, here you go.
- Do this for me.
- OK, here you go.

**Authenticity**
Resurrecting Duckling
INTEGRITY
THANKS TO TAMPER EVIDENCE-NESS

CONFIDENTIALITY
SAYETH THE PAPER:
"EASY ONCE AUTHENTICATION HAS BEEN SOLVED"

INTEGRITY:
TAMPERING SHOULD BE EVIDENT

BEFORE

AFTER

GIVE ME YOUR KEY!

SOME THINGS TO NOTE ABOUT RESURRECTED DUCKLING PROTOCOL

IT ATTEMPTS TO SOLVE AN AUTHENTICATION PROBLEM

CAN IT WORK FOR PROGRAMS THAT WISH TO AUTHENTICATE EACH OTHER?

EG: MY PDA WANTS TO AUTHENTICATE WITH THE PROJECT OR ON THE CEILING.
MORE SECURITY ISSUES TO CONSIDER

# ANONYMITY WITHOUT AUTHENTICATION

# TRUST OR AUTHENTICATION OF DEVICE
EG: DUCKLING AUTHENTICATES OWNER

# AUDIT LOGS
INTEGRITY & REPUTABILITY

# COMMUNICATIONS PROTOCOLS
BLUETOOTH & 802

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.

BIBLIOGRAPHY