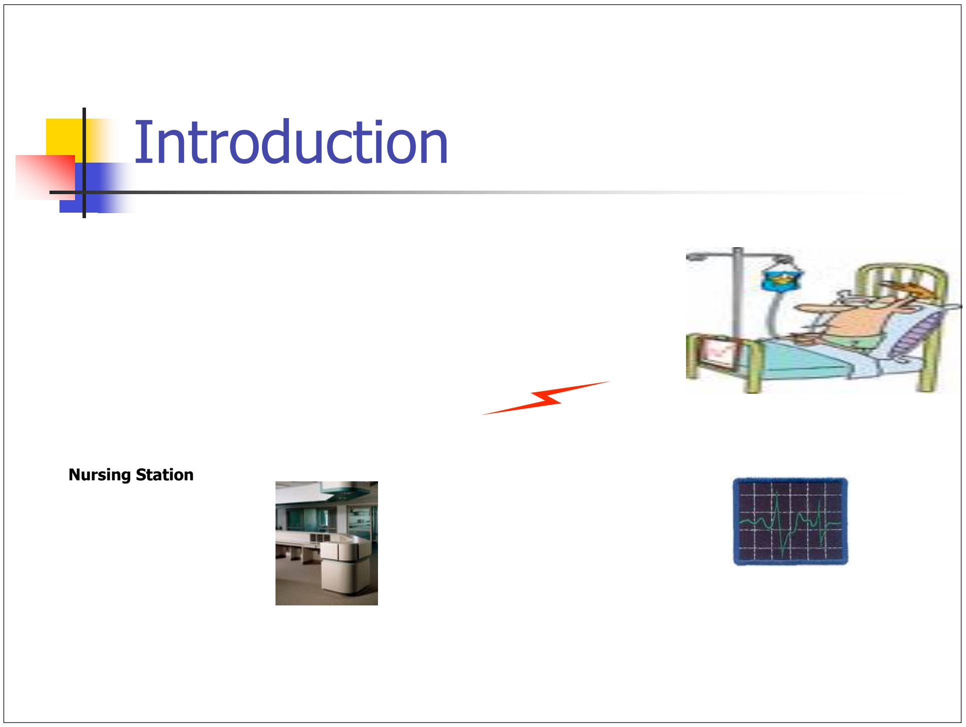
The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks

Frank Stajano and Ross Anderson

CS818 Presentation By Venkatesh Ramanathan

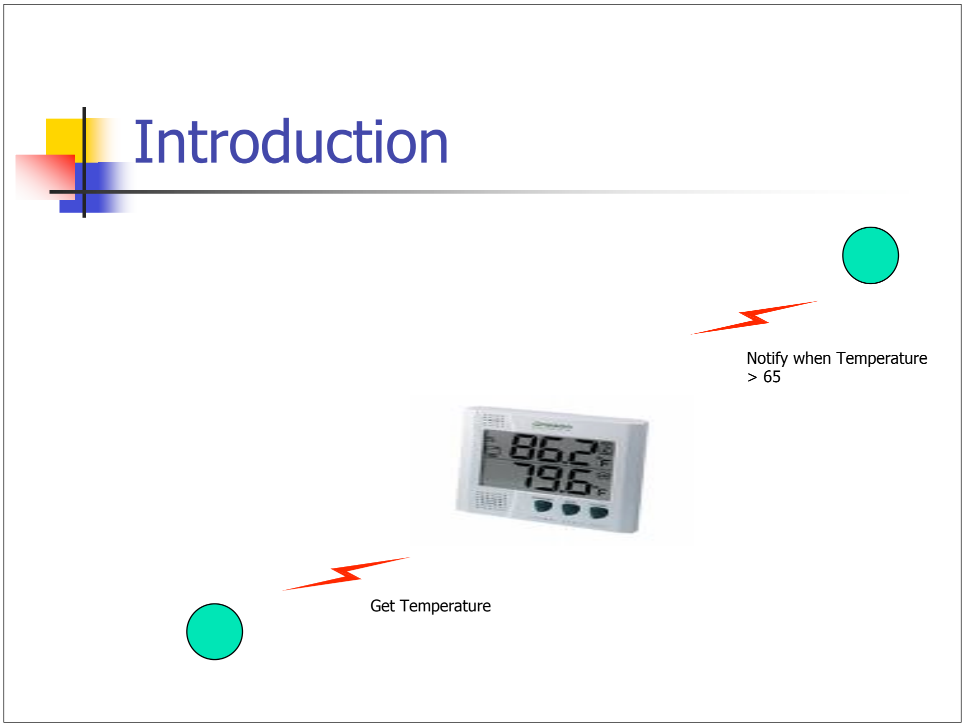
Introduction

- Electronic devices communicate with each other over a wireless channel.



Introduction

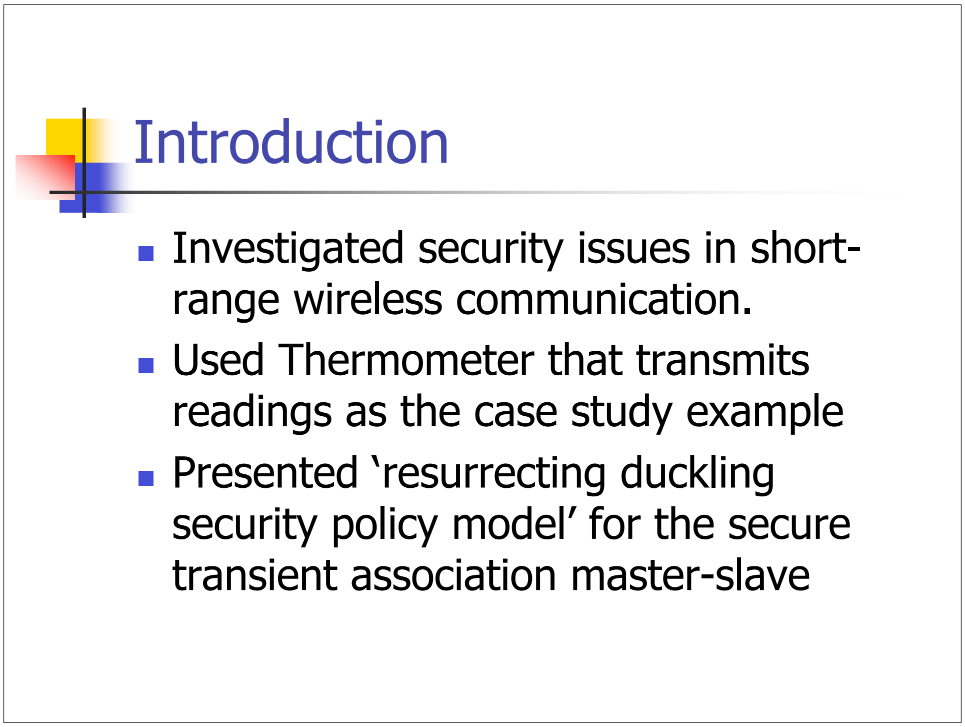
Nursing Station



Introduction

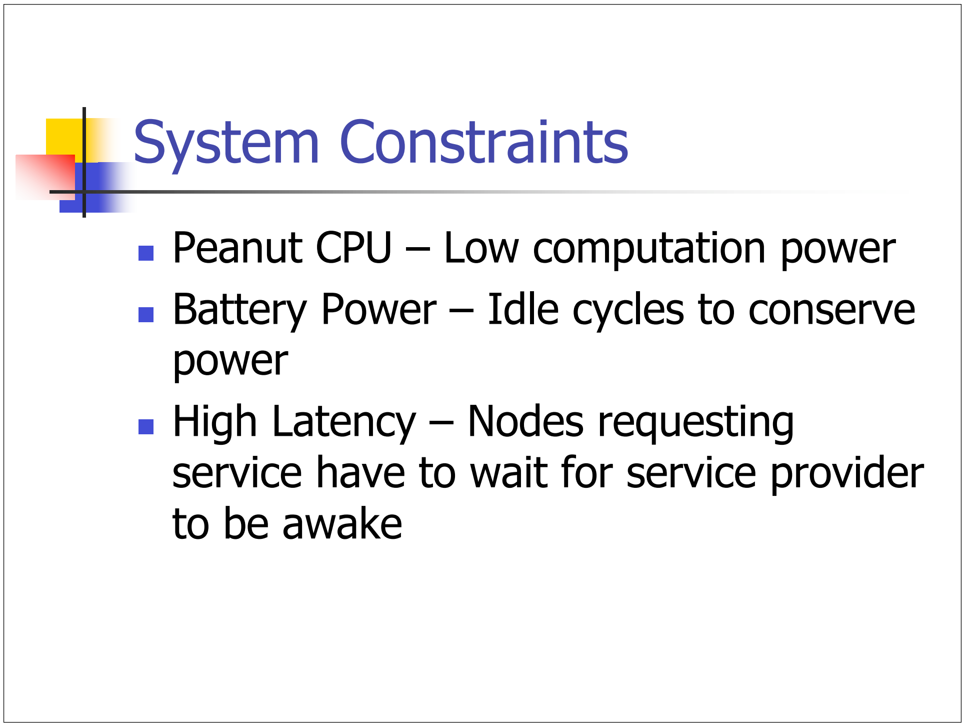
Notify when Temperature > 65

Get Temperature



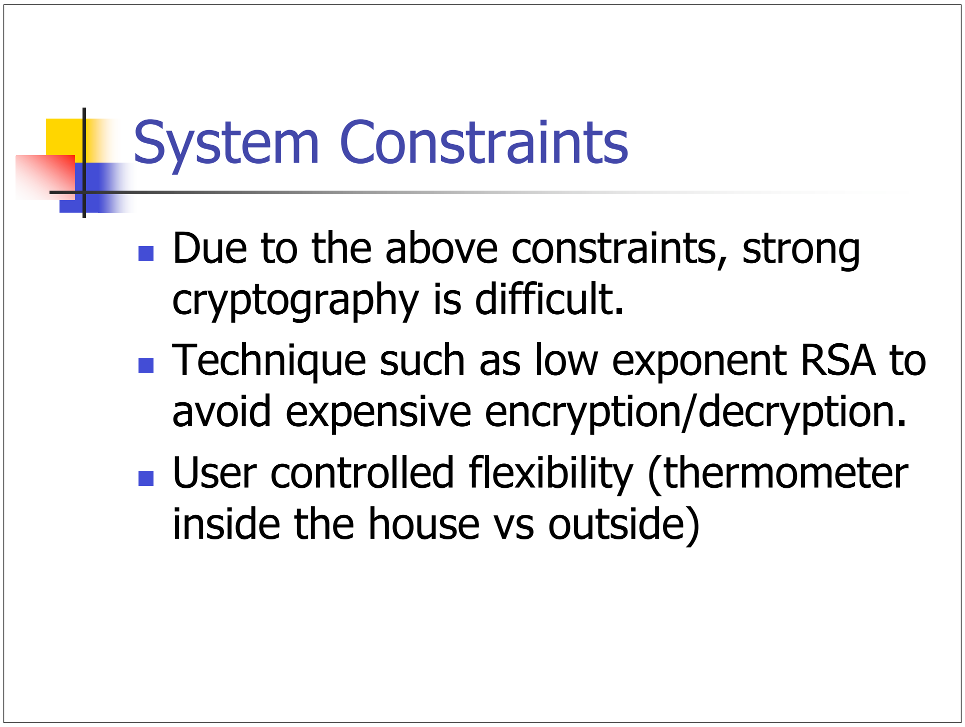
Introduction

- Investigated security issues in short-range wireless communication.
- Used Thermometer that transmits readings as the case study example
- Presented ‘resurrecting duckling security policy model’ for the secure transient association master-slave



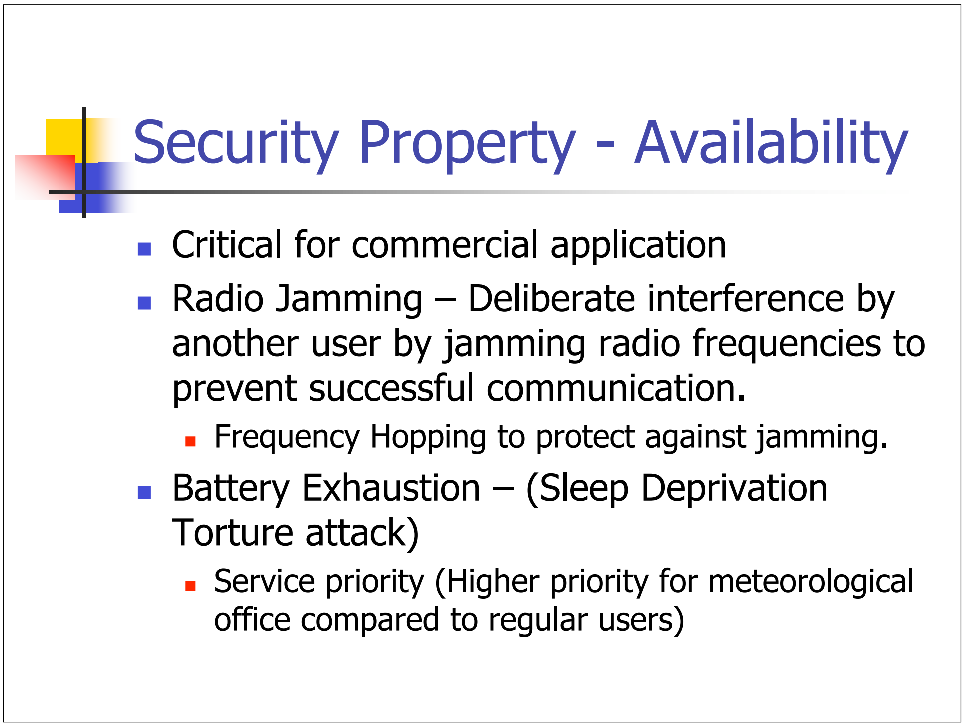
System Constraints

- Peanut CPU – Low computation power
- Battery Power – Idle cycles to conserve power
- High Latency – Nodes requesting service have to wait for service provider to be awake



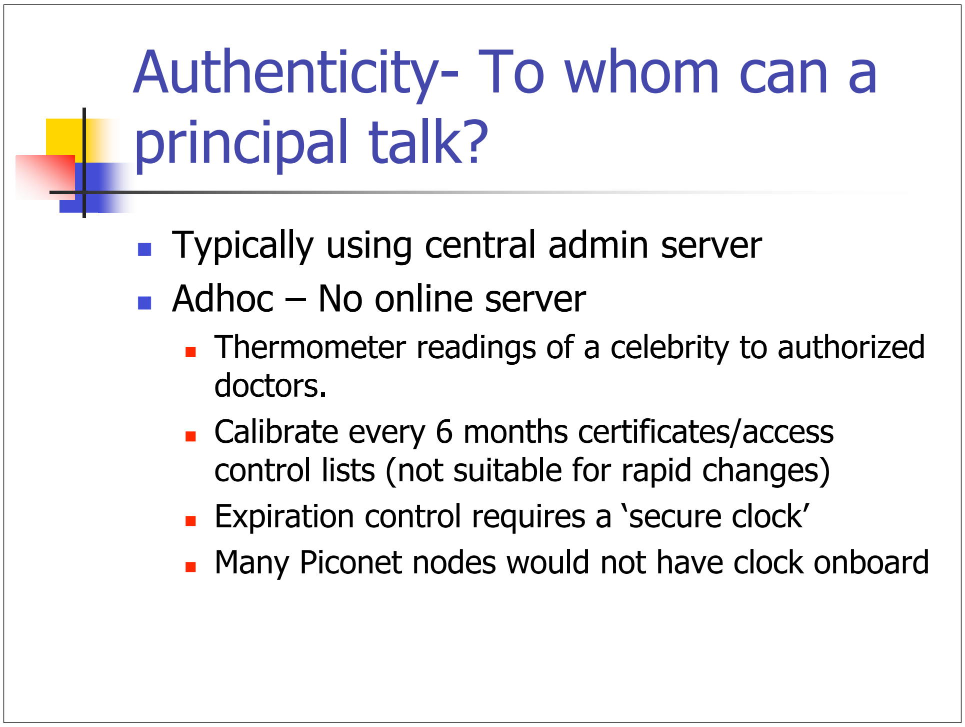
System Constraints

- Due to the above constraints, strong cryptography is difficult.
- Technique such as low exponent RSA to avoid expensive encryption/decryption.
- User controlled flexibility (thermometer inside the house vs outside)



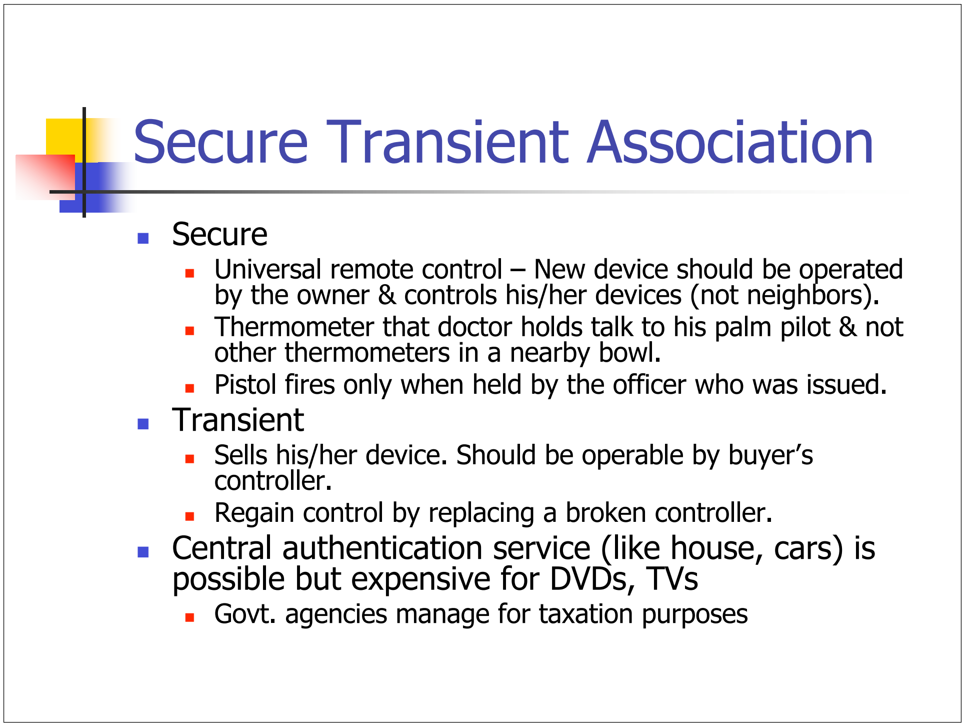
Security Property - Availability

- Critical for commercial application
- Radio Jamming – Deliberate interference by another user by jamming radio frequencies to prevent successful communication.
  - Frequency Hopping to protect against jamming.
- Battery Exhaustion – (Sleep Deprivation Torture attack)
  - Service priority (Higher priority for meteorological office compared to regular users)



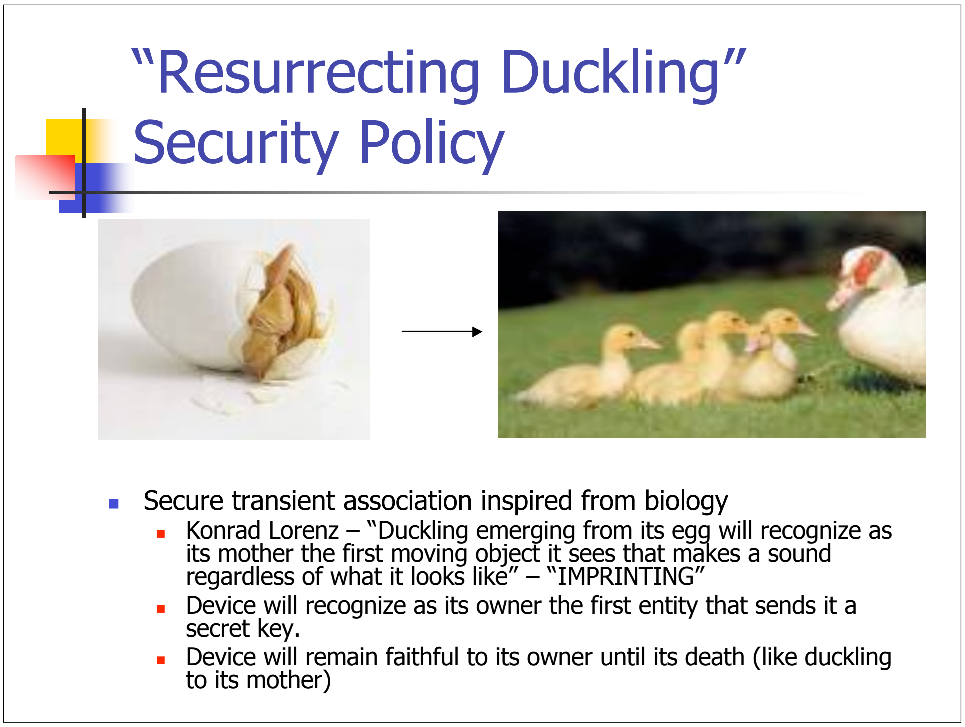
Authenticity- To whom can a principal talk?

- Typically using central admin server
- Adhoc – No online server
  - Thermometer readings of a celebrity to authorized doctors.
  - Calibrate every 6 months certificates/access control lists (not suitable for rapid changes)
  - Expiration control requires a ‘secure clock’
  - Many Piconet nodes would not have clock onboard



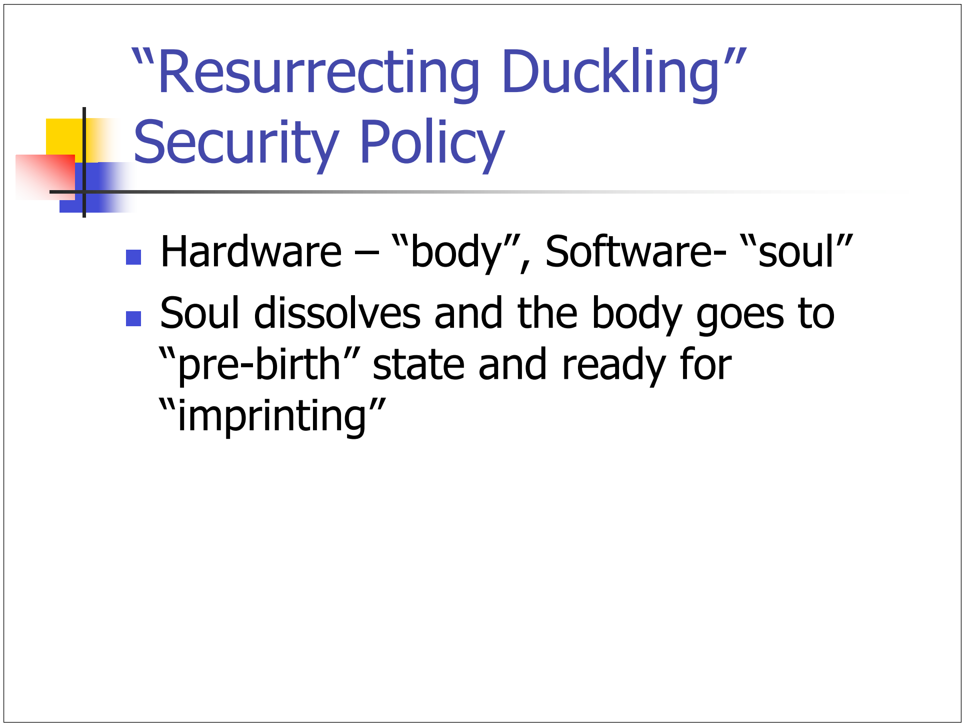
Secure Transient Association

- Secure
  - Universal remote control – New device should be operated by the owner & controls his/her devices (not neighbors).
  - Thermometer that doctor holds talk to his palm pilot & not other thermometers in a nearby bowl.
  - Pistol fires only when held by the officer who was issued.
- Transient
  - Sells his/her device. Should be operable by buyer’s controller.
  - Regain control by replacing a broken controller.
- Central authentication service (like house, cars) is possible but expensive for DVDs, TVs
  - Govt. agencies manage for taxation purposes



"Resurrecting Duckling" Security Policy

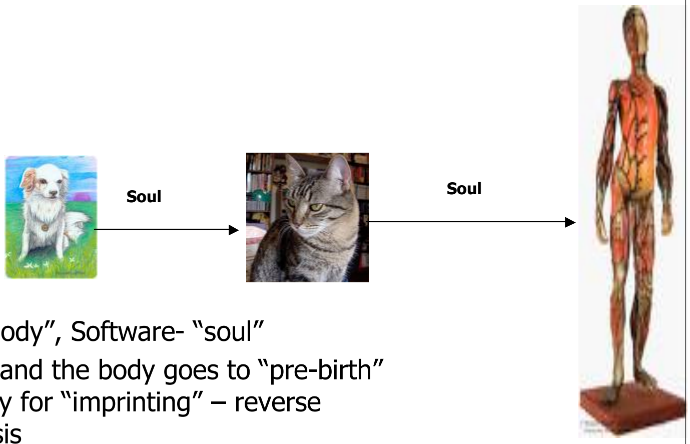
- Secure transient association inspired from biology
  - Konrad Lorenz – "Duckling emerging from its egg will recognize as its mother the first moving object it sees that makes a sound regardless of what it looks like" – "IMPRINTING"
  - Device will recognize as its owner the first entity that sends it a secret key.
  - Device will remain faithful to its owner until its death (like duckling to its mother)



"Resurrecting Duckling" Security Policy

- Hardware – "body", Software- "soul"
- Soul dissolves and the body goes to "pre-birth" state and ready for "imprinting"

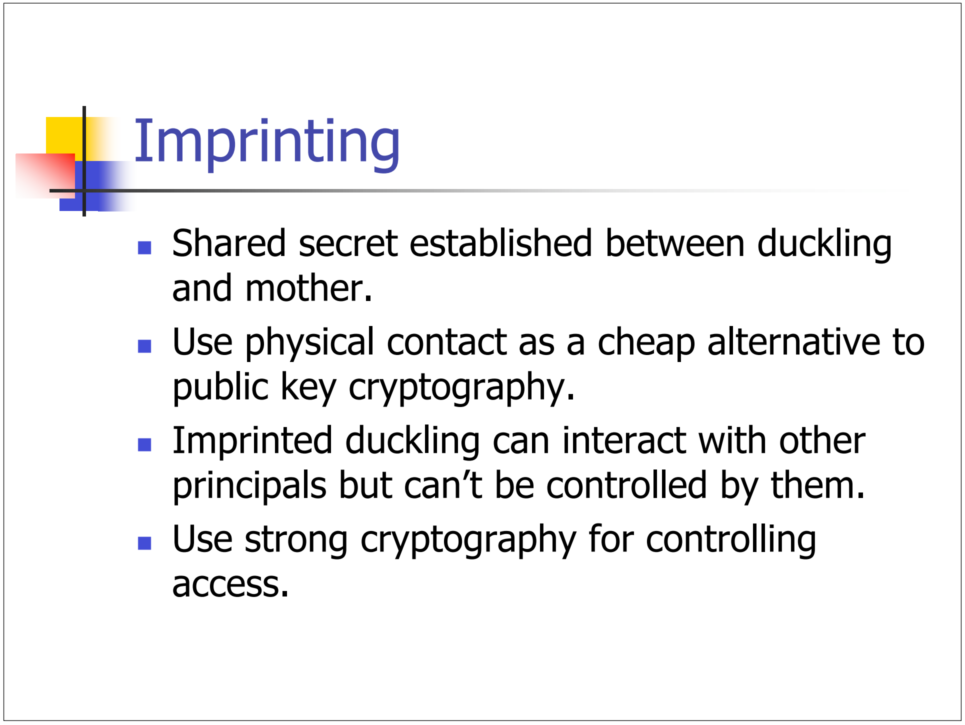
Metempsychosis



- Hardware – "body", Software- "soul"
- Soul dissolves and the body goes to "pre-birth" state and ready for "imprinting" – reverse metempsychosis

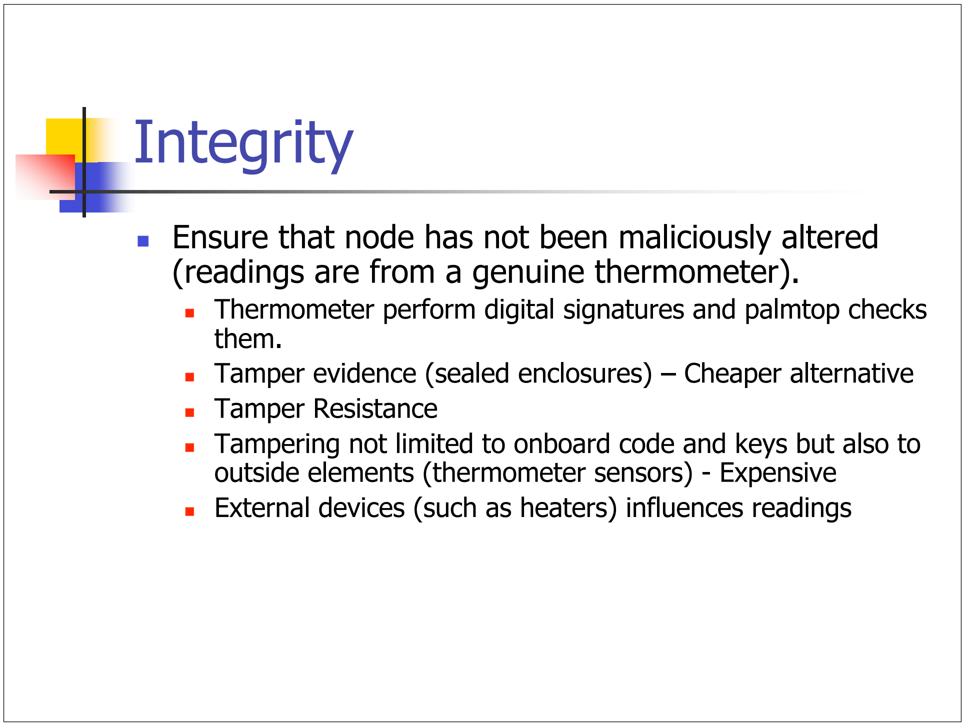
"Resurrecting Duckling" Security Policy

- Death upon specific event or timeout or when instructed - Thermometer dies when put in a disinfectant bowl.
- Recover from lost shared secret – Allow "escrowed seppuku" (manufacture commands the device to die)
- Perish "part of the soul" – Cleansing a disinfectant thermometer should erase only user data, key and not calibration data.
  - Use multi-level security concepts such as Biba



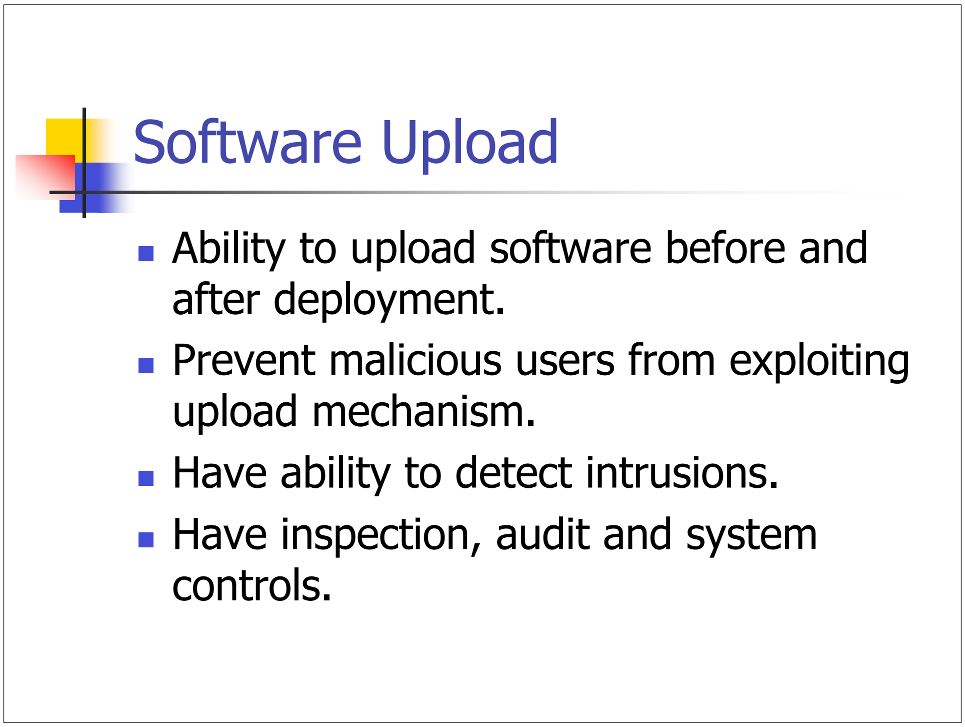
Imprinting

- Shared secret established between duckling and mother.
- Use physical contact as a cheap alternative to public key cryptography.
- Imprinted duckling can interact with other principals but can’t be controlled by them.
- Use strong cryptography for controlling access.



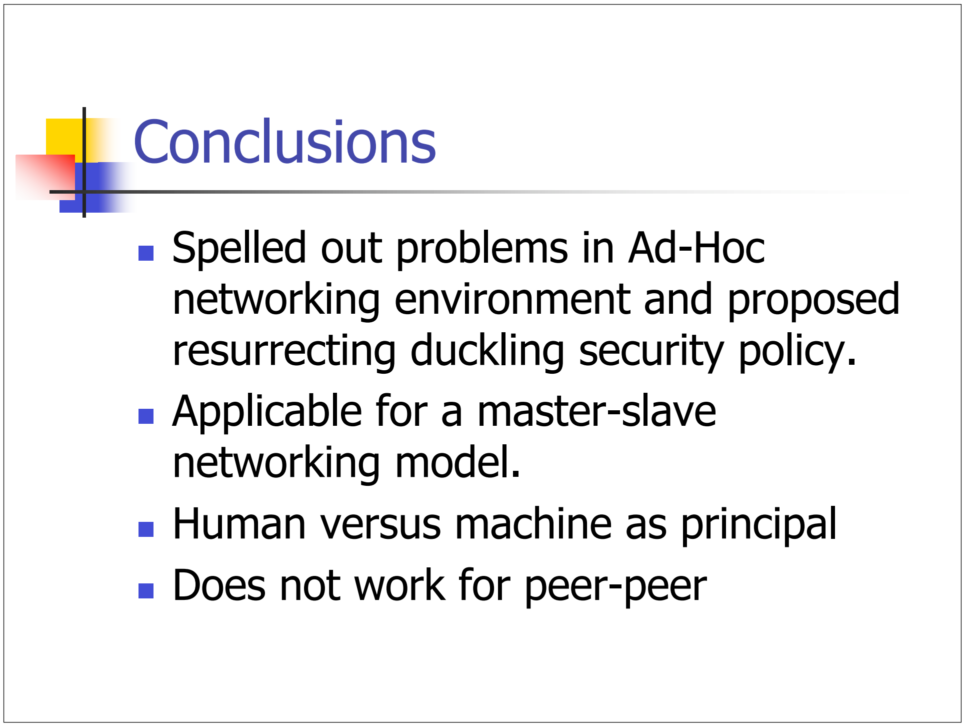
Integrity

- Ensure that node has not been maliciously altered (readings are from a genuine thermometer).
  - Thermometer perform digital signatures and palmtop checks them.
  - Tamper evidence (sealed enclosures) – Cheaper alternative
  - Tamper Resistance
  - Tampering not limited to onboard code and keys but also to outside elements (thermometer sensors) - Expensive
  - External devices (such as heaters) influences readings



Software Upload

- Ability to upload software before and after deployment.
- Prevent malicious users from exploiting upload mechanism.
- Have ability to detect intrusions.
- Have inspection, audit and system controls.



Conclusions

- Spelled out problems in Ad-Hoc networking environment and proposed resurrecting duckling security policy.
- Applicable for a master-slave networking model.
- Human versus machine as principal
- Does not work for peer-peer