Zero-Power Authentication

University of Massachusetts Amherst, University of Washington

Problem:

Devices are not always accessible.
Devices often have finite battery.
Radio communication uses battery power.

Risk: sleep deprivation; power DoS.

(Standard Yacht Fabergé egg. Image: Wikipedia.)

Example scenario:

Weather measurement node in unfriendly conditions; finite battery. Warns a community of impending danger. Able to transmit its vital signs (voltage, etc.) to a nearby maintenance person.

Problem: misanthropic teenager figures out how to query the device over, and over, and over...

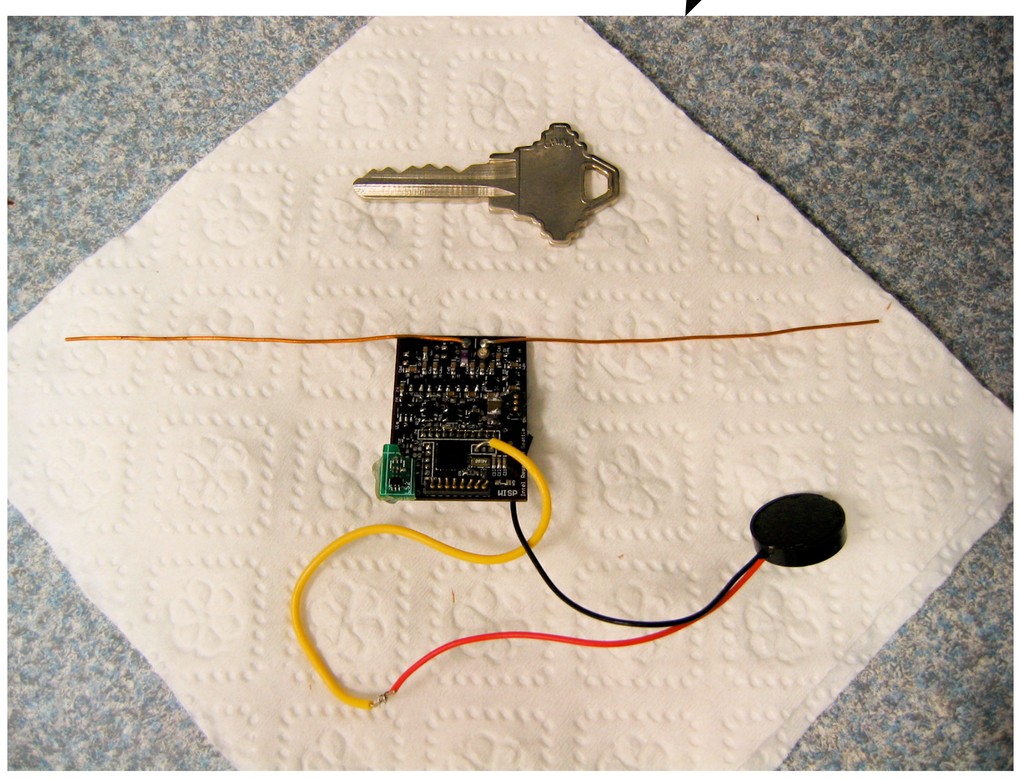
Our approach:

Passively-powered "gatekeeper" device **authenticates** external parties **before any battery power is used**.

Physical analogue: hire a bouncer.

Implementation:

WISP tag (MSP430, 256B RAM, EPC Class 1 Gen 1)
Added ~30 lines of C++ code
Simple challenge-response protocol (below)



Why this is interesting:

More battery power available for device functioning.
Longer battery lifetime.
Simple modification of existing devices.
Authentication for "free."
Also interesting because it's not perfect.

Open questions:

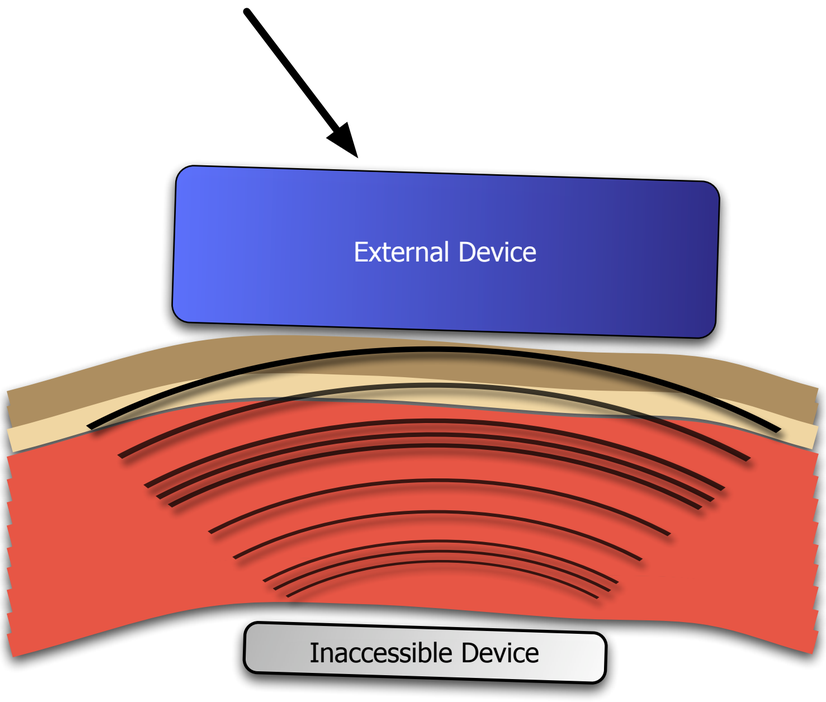
Key management?
How much computation can we squeeze out of the WISP?
Applications: best way to harvest power through various media?

Prototype ("WISPer")

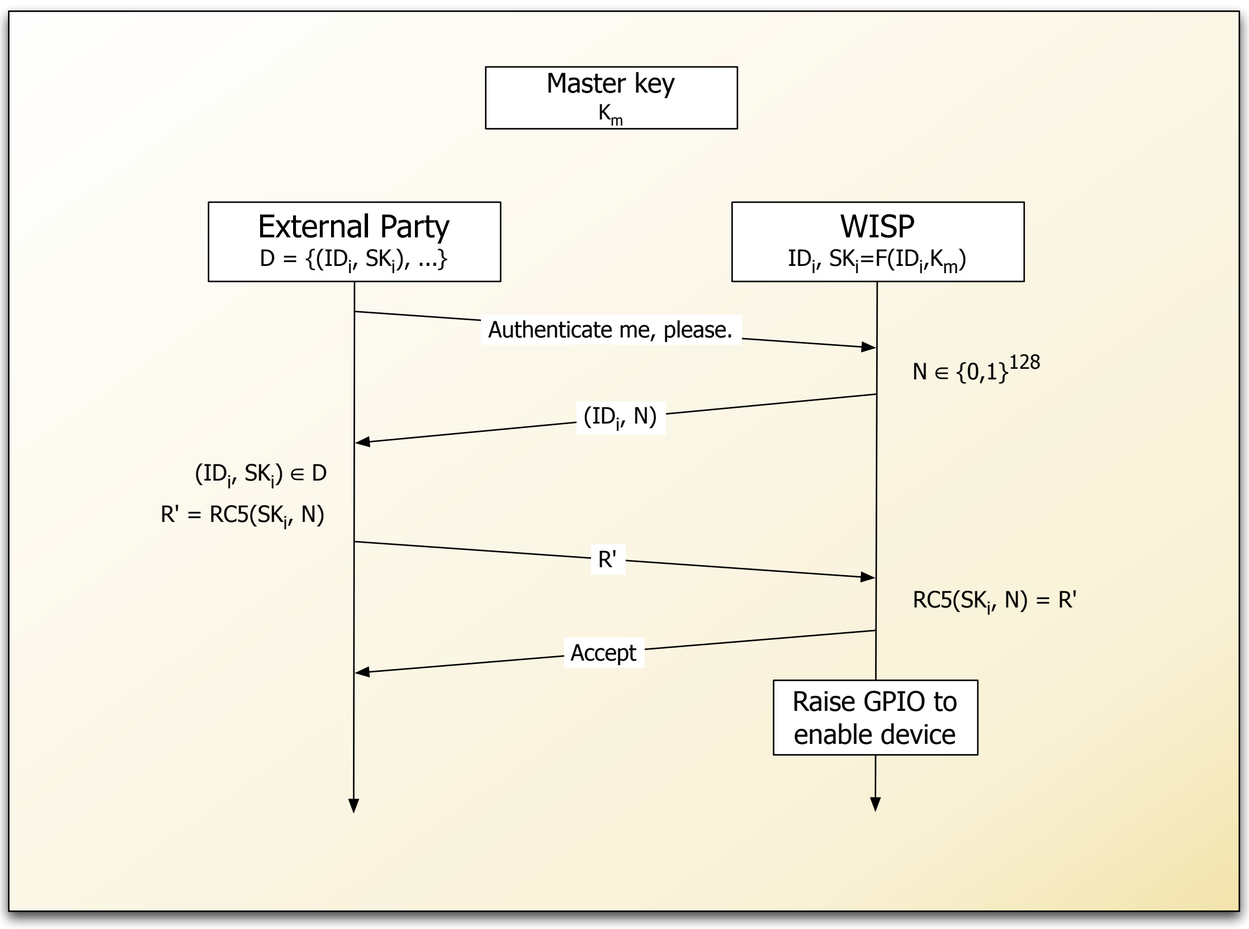
WISP beeps (piezobuzzer on GPIO) on successful authentication.
We have installed this device in *various inconvenient locations*.
Photo depicts WISP v1; newer WISP is smaller.

Future work:

Gather randomness from WISP SRAM (FERNS)?
Distance bounding (Drimer & Murdoch)?
Acoustic key exchange (certain circumstances).



A device that is inaccessible may have a private channel to external devices in the form of physical contact. A piezobuzzer produces acoustic waves (sound and vibration) that represent a modulated binary version of key material. This makes key distribution easier under those circumstances.



References:

"Maximalist cryptography and computation on the WISP UHF RFID tag." Conference on RFID Security, July 2007.
"Security and privacy for implantable medical devices." IEEE Pervasive Computing, Special Issue on Implantable Electronics, January 2008.
"Initial SRAM state as a fingerprint and source of true random numbers for RFID tags." Conference on RFID Security, July 2007.
"A wirelessly-powered platform for sensing and computation." 8th International Conference on Ubiquitous Computing (Ubicomp), September 2006.

Personnel:

Thomas S. Heydt-Benjamin (UMass, ETH Zurich)
Daniel Halperin (Washington)
Benjamin Ransford (UMass)
Shane S. Clark (UMass)
Kevin Fu (UMass)
Tadayoshi Kohno (Washington)