TARDIS

Implementing Secure Protocols on Embedded Devices without Clocks

Amir Rahmati, Mastooreh Salajegheh, Dan Holcomb[1], Jacob Sorber[2], Wayne Burleson, Kevin Fu

1 UC Berkeley 2 Dartmouth Collage

The Problem

Slow Brute Force attacks on batteryless devices

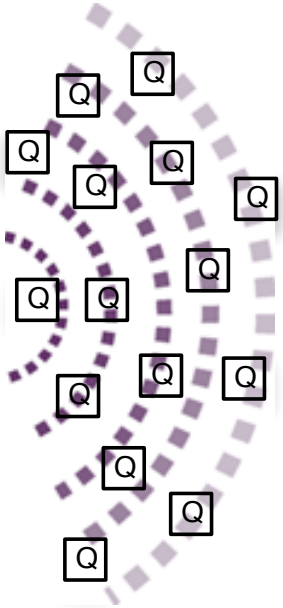
E-Passports

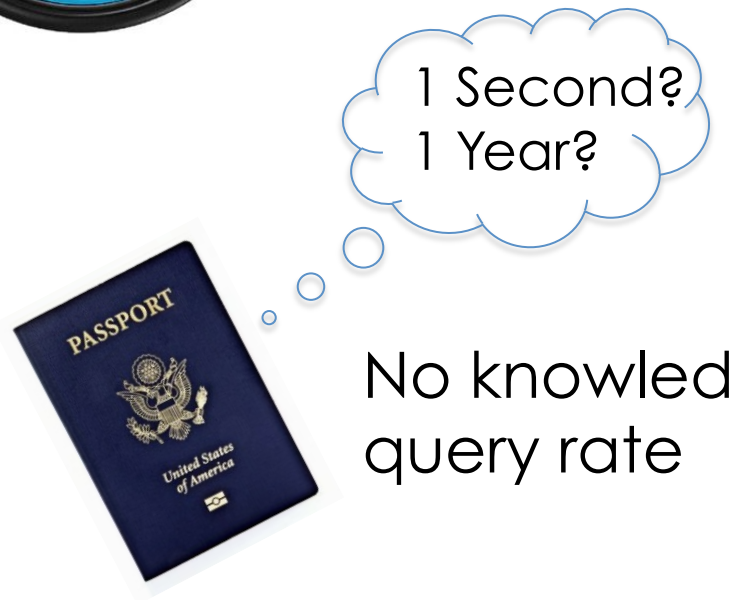
Smartcards

Garcia et al., Oakland'09
Kasper et al., ISSE'11

Clocks Need Power

No Notion of Time





No knowledge about the query rate

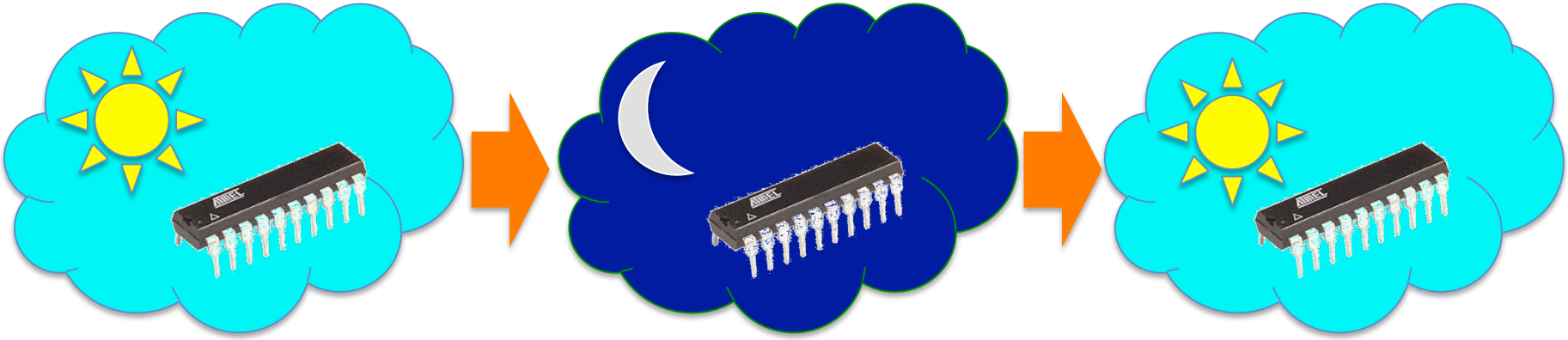
Our Solution

Use decay in SRAM to derive a notion of time

1	1	1	1	1

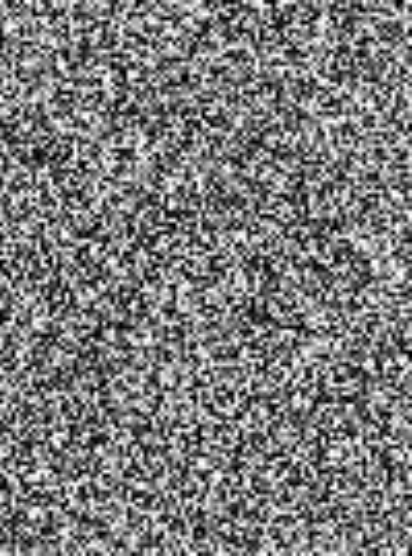
x	x	x	x	x

1	1	0	1	0



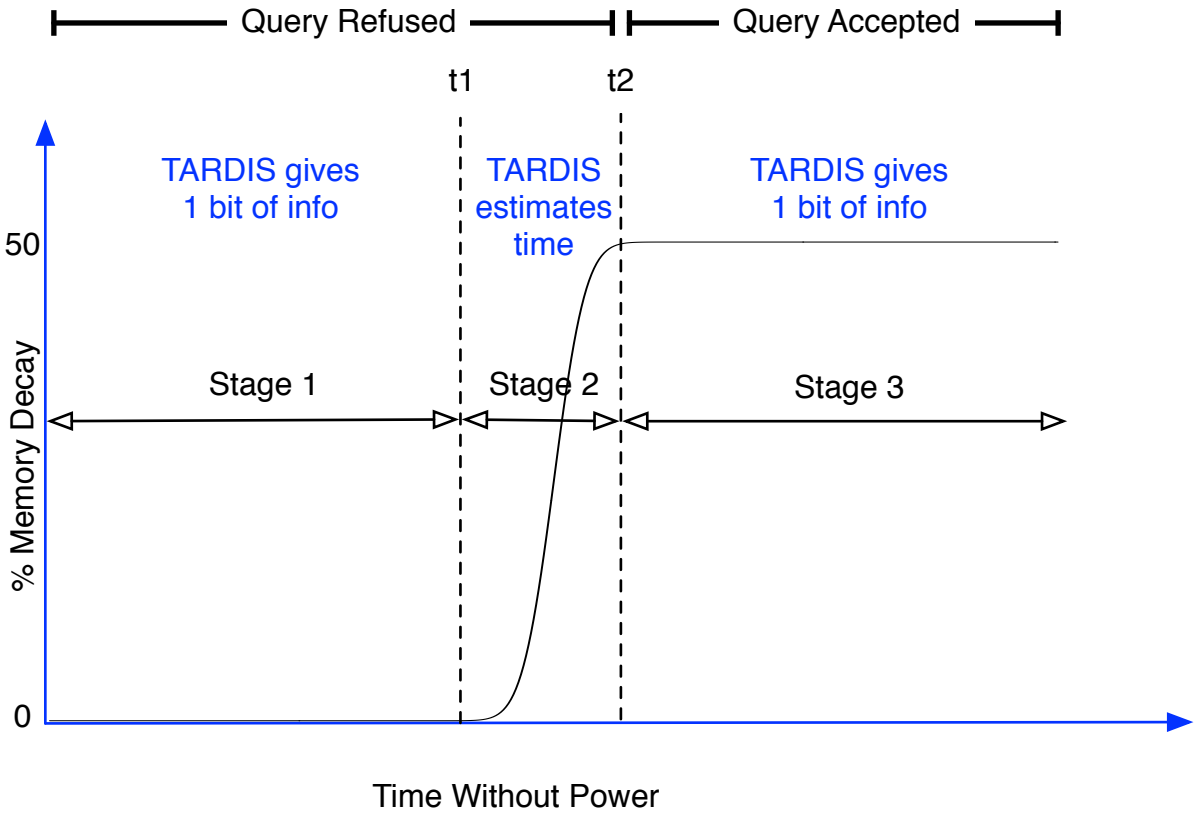
Halderman et al., Cold boot attacks, USENIX Sec'08

Gutmann, Secure deletion, USENIX Sec'96



How it works

Three Stages of Decay



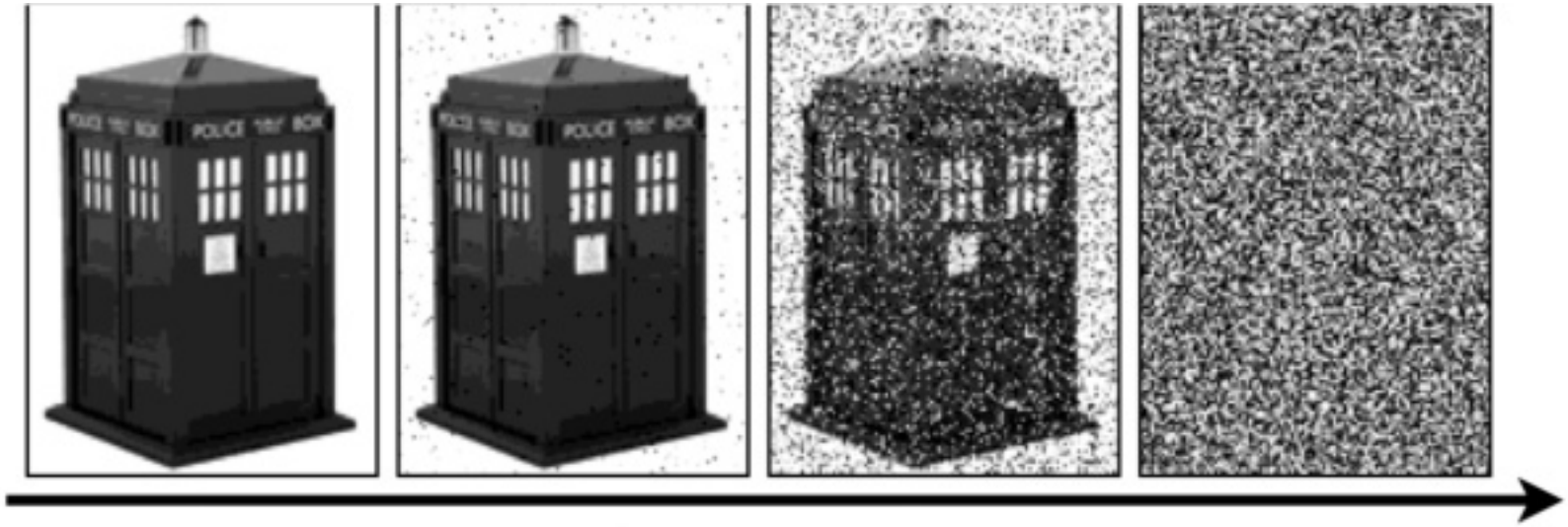
Factors affecting stage lengths:

- Circuit specifications
- Capacitance
- Temperature

Stages can range from seconds to hours

What about a thermal attacks?

TARDIS: Time And Remanence Decay In SRAM



SPQR LABORATORY

Materializing in USENIX Security 2012
https://spqr.cs.umass.edu/tardis/

Holcomb RFID Sec'07, IEEE Trans'09