



TARDIS

Time and **R**emanence **D**ecay in **S**RAM
to Implement Secure Protocols on
Embedded Devices without Clocks

Amir Rahmati¹, Mastrooreh Salajegheh¹, Dan Holcomb²,
Jacob Sorber³, Wayne Burleson¹, Kevin Fu¹

¹ UMass Amherst ² UC Berkeley, ³ Dartmouth College



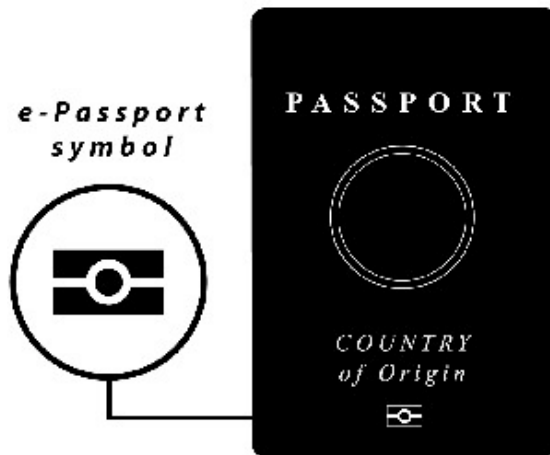
Batteryless Devices



Transportation



Payment



Passports



Employee IDs

Batteryless Devices



Transportation



Things in Common

- No long running clocks
- Adversary controls power & time
- Hold secrets

e-Passport symbol



Passports



Employee IDs

Security Vulnerabilities

Oyster card hack details revealed

By Peter Price
Click reporter

Details of how to hack one of the world's most popular smartcards have been published online.

The research by Professor Bart Jacobs and colleagues at Radboud University in Holland reveals a weakness in the widely used Mifare



Fare Hack: Exploiting a Clipper Card Flaw Is Easy

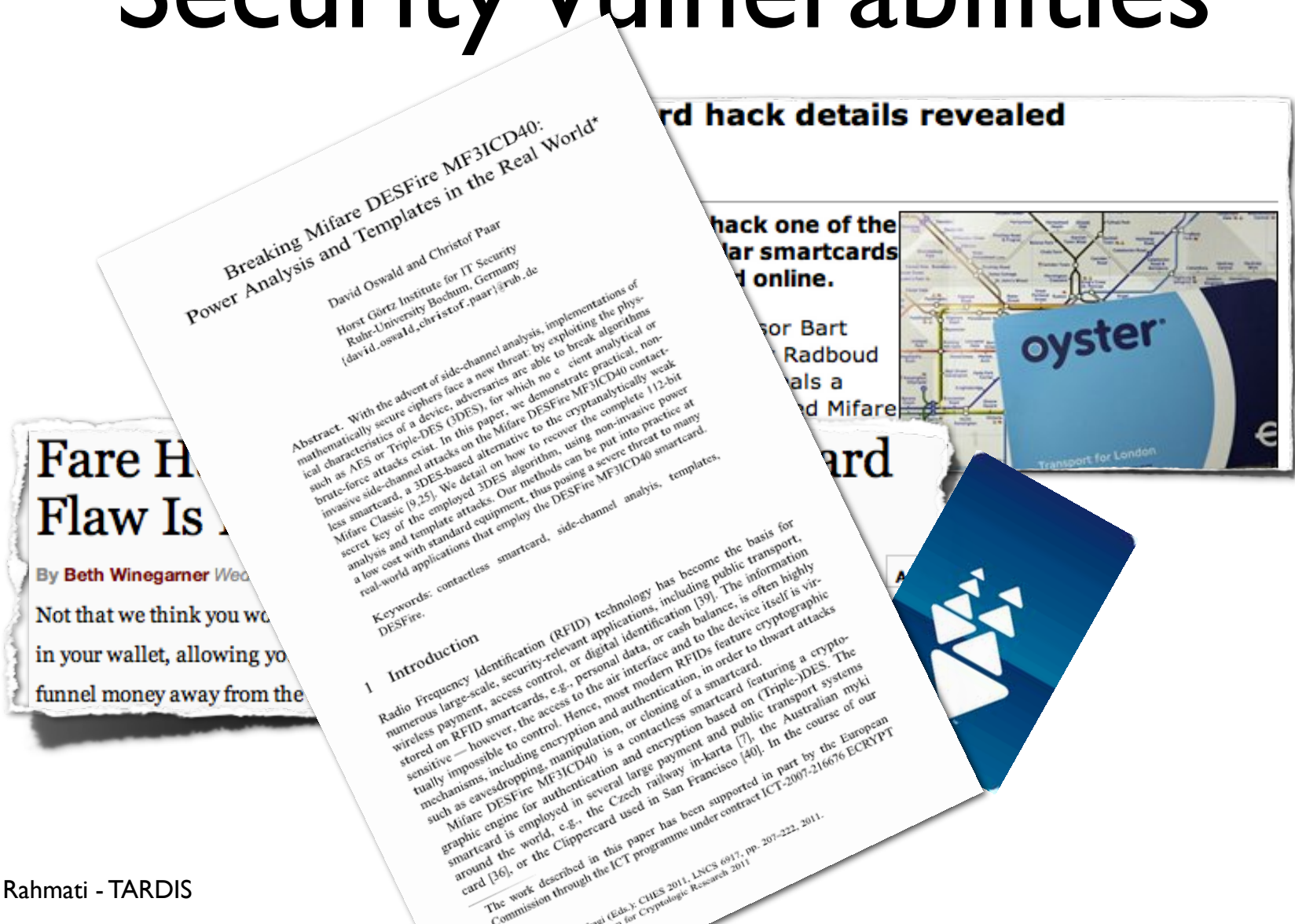
By Beth Winegarner Wednesday, Feb 1 2012

Comments (6)

Not that we think you would, but with a visit to [Radio Shack](#) you could hack into that Clipper in your wallet, allowing you to load it with free rides or create and sell copies for profit — funnel money away from the Bay Area's crash-strapped public-transit agencies.



Security Vulnerabilities



Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World*

David Oswald and Christof Paar
Horst Görtz Institute for IT Security
Ruhr-University Bochum, Germany
(david.oswald, christof.paar}@rub.de

Abstract. With the advent of side-channel analysis, implementations of mathematically secure ciphers face a new threat: by exploiting the physical characteristics of a device, adversaries are able to break algorithms such as AES or Triple-DES (3DES), for which no efficient analytical or brute-force attacks exist. In this paper, we demonstrate practical, non-invasive side-channel attacks on the Mifare DESFire MF3ICD40 contactless smartcard, a 3DES-based alternative to the cryptanalytically weak Mifare Classic (9,25). We detail on how to recover the complete 112-bit secret key of the employed 3DES algorithm, using non-invasive power analysis and template attacks. Our methods can be put into practice at a low cost with standard equipment, thus posing a severe threat to many real-world applications that employ the DESFire MF3ICD40 smartcard.

Keywords: contactless smartcard, side-channel analysis, templates, DESFire.

1 Introduction

Radio Frequency Identification (RFID) technology has become the basis for numerous large-scale, security-relevant applications, including public transport, wireless payment, access control, or digital identification [39]. The information stored on RFID smartcards, e.g., personal data, or cash balance, is often highly sensitive — however, the access to the air interface and to the device itself is virtually impossible to control. Hence, most modern RFIDs feature cryptographic mechanisms, including encryption and authentication, in order to thwart attacks such as eavesdropping, manipulation, or cloning of a smartcard. Mifare DESFire for authentication and encryption based on (Triple-)DES. The smartcard engine is employed in several large payment and public transport systems around the world, e.g., the Czech railway in-karta [7], the Australian myki card [36], or the Clipperecard used in San Francisco [40]. In the course of our

The work described in this paper has been supported in part by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT

Security Vulnerabilities



Smart Card Threats

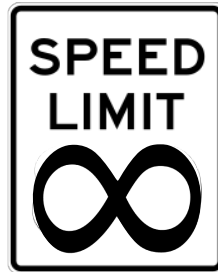


Power Analysis

Reverse Engineering

Brute Force

Smart Card Threats

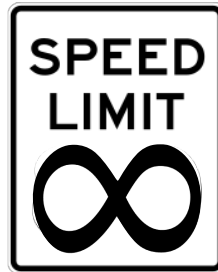


Power Analysis

Reverse Engineering

Brute Force

Smart Card Threats



Power Analysis

Semi-invasive

Reverse Engineering

Brute Force

Vulnerable to Brute Force Attacks

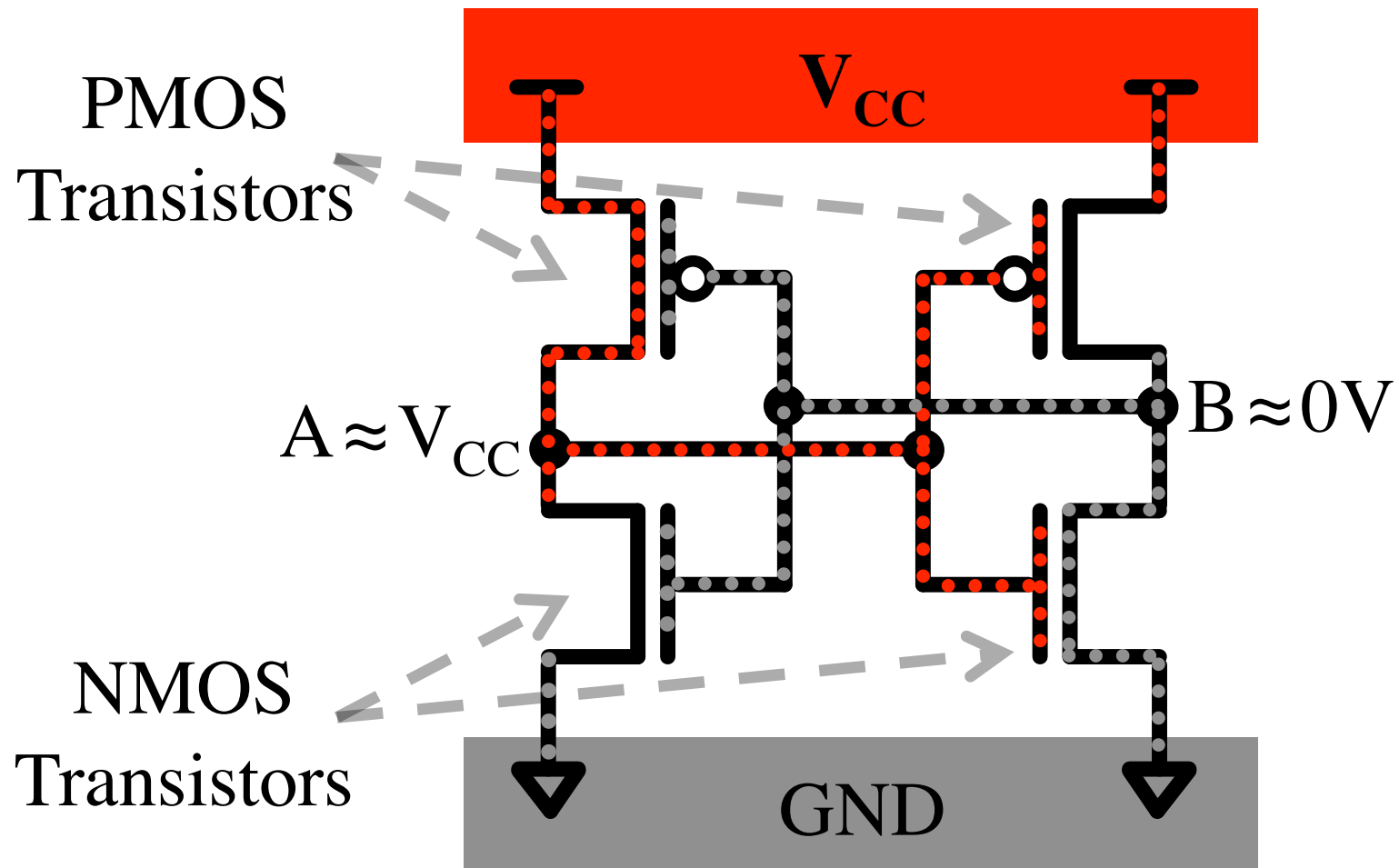
Device	#Queries	Time
UHF RFID Tags[Shamir'07]	200	2 Seconds
MIFARE Classic[Garcia'09]	1,500	16 Seconds
Digital Signal Transponder[Bono'05]	75,000	1 Hour
MIFARE DESFire[Paar'11]	250,000	7 Hours
GSM SIM Cards[Goldberg'99]	150,000	8 Hours



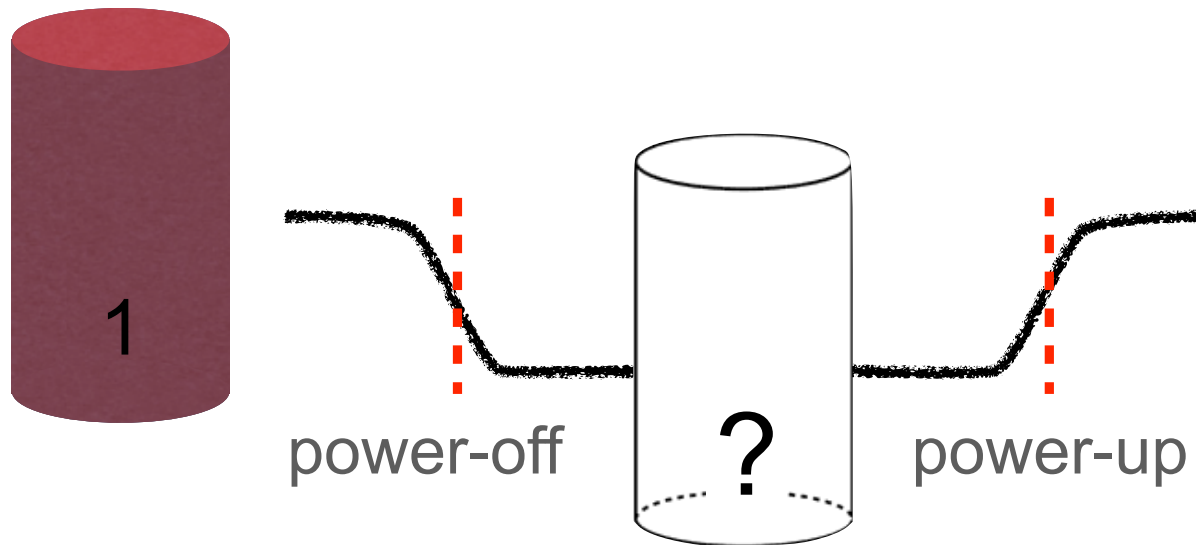
Our Contribution: TARDIS

A time-keeping technique based on SRAM decay

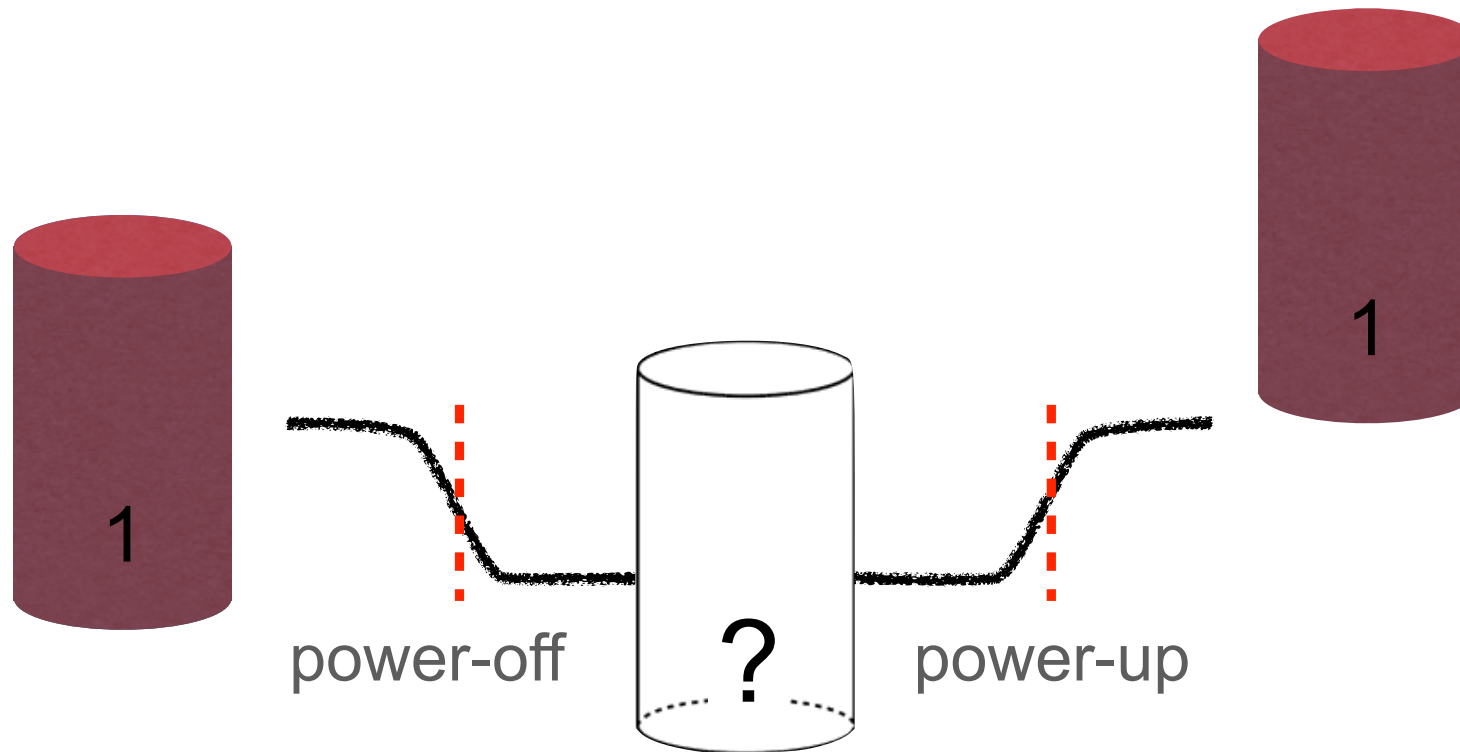
SRAM Remanence



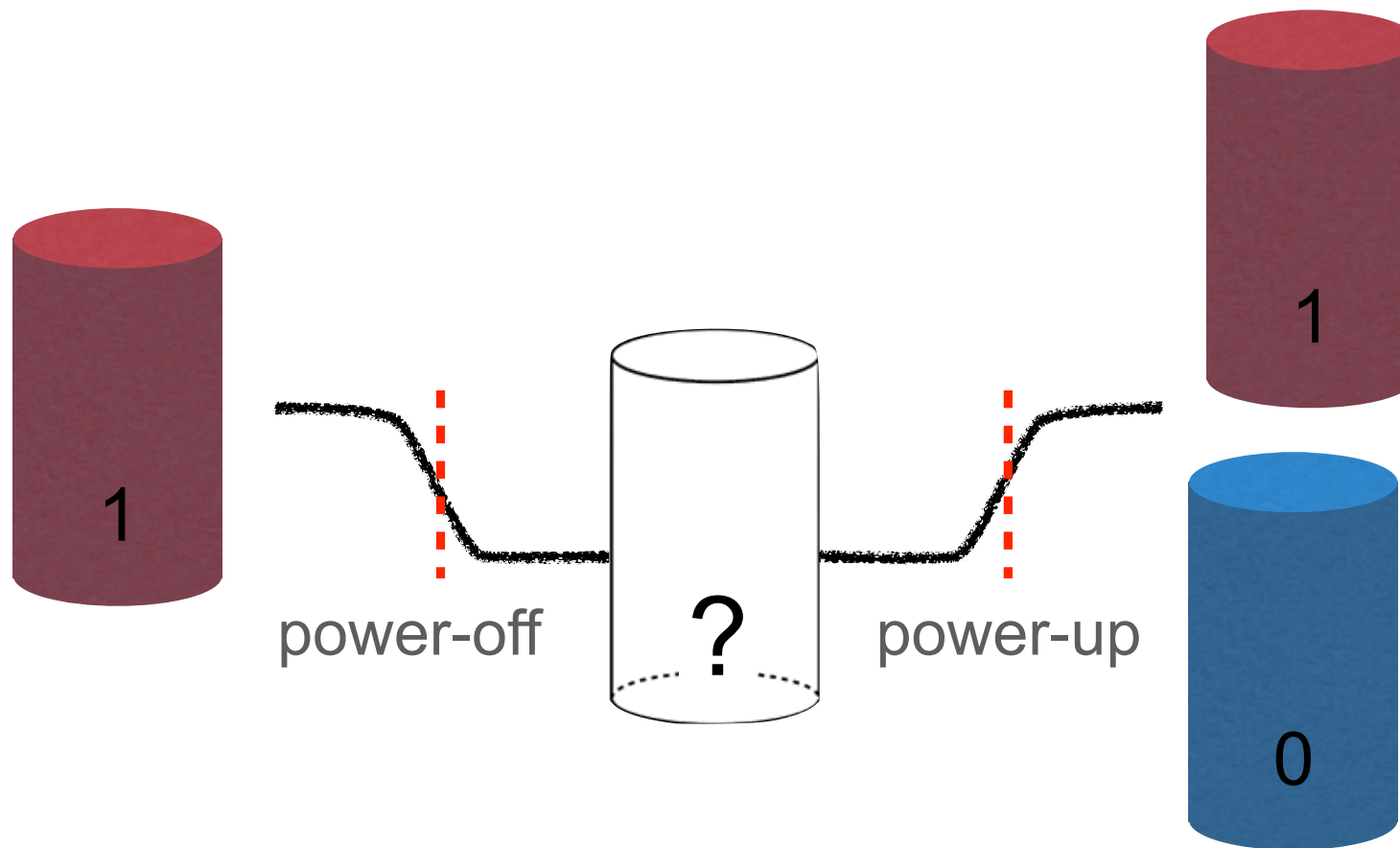
SRAM Remanence



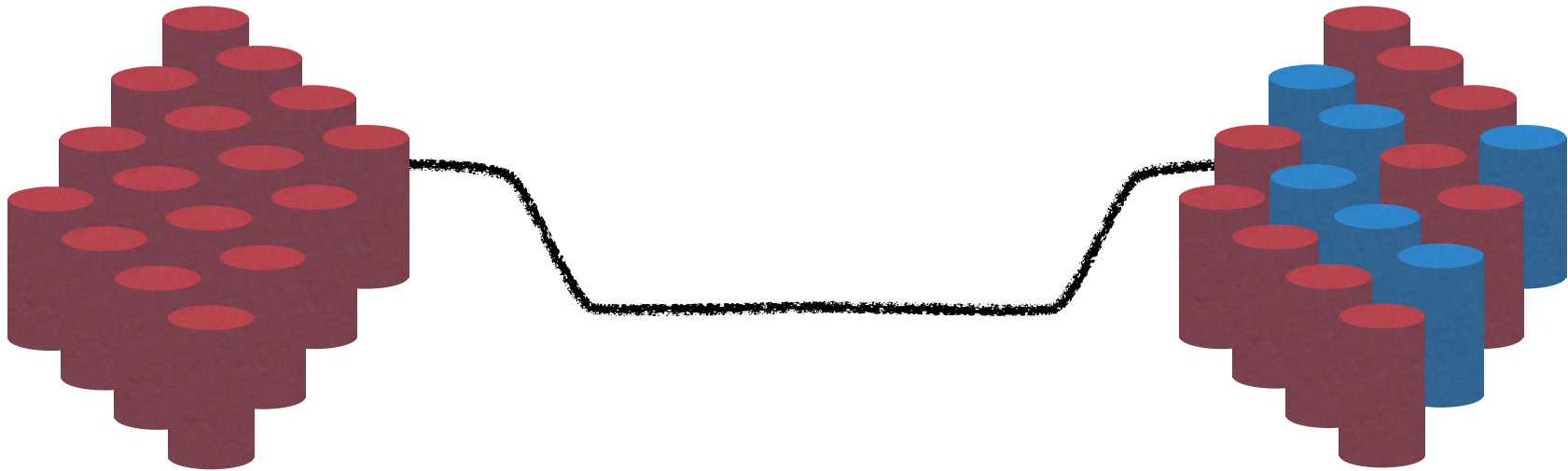
SRAM Remanence



SRAM Remanence



SRAM Remanence



SRAM Remanence



0

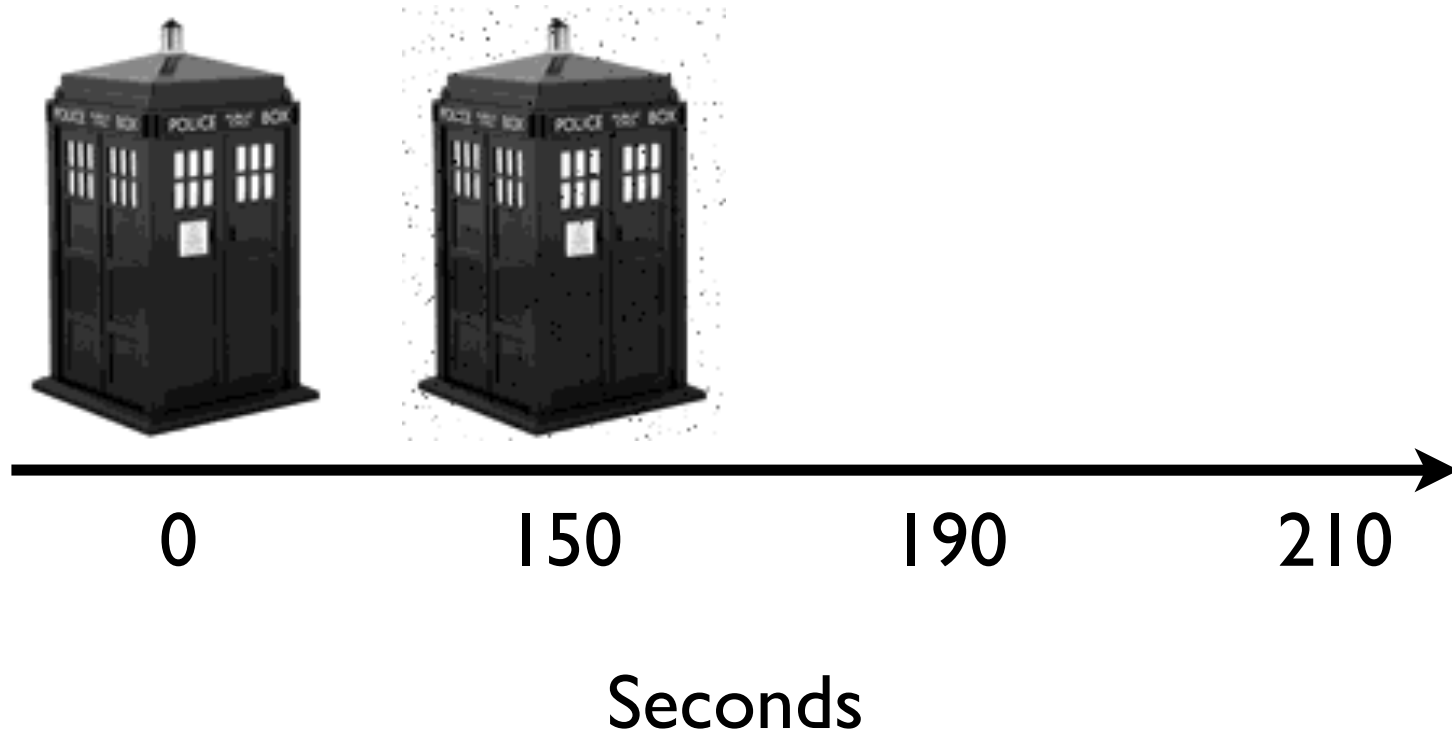
150

190

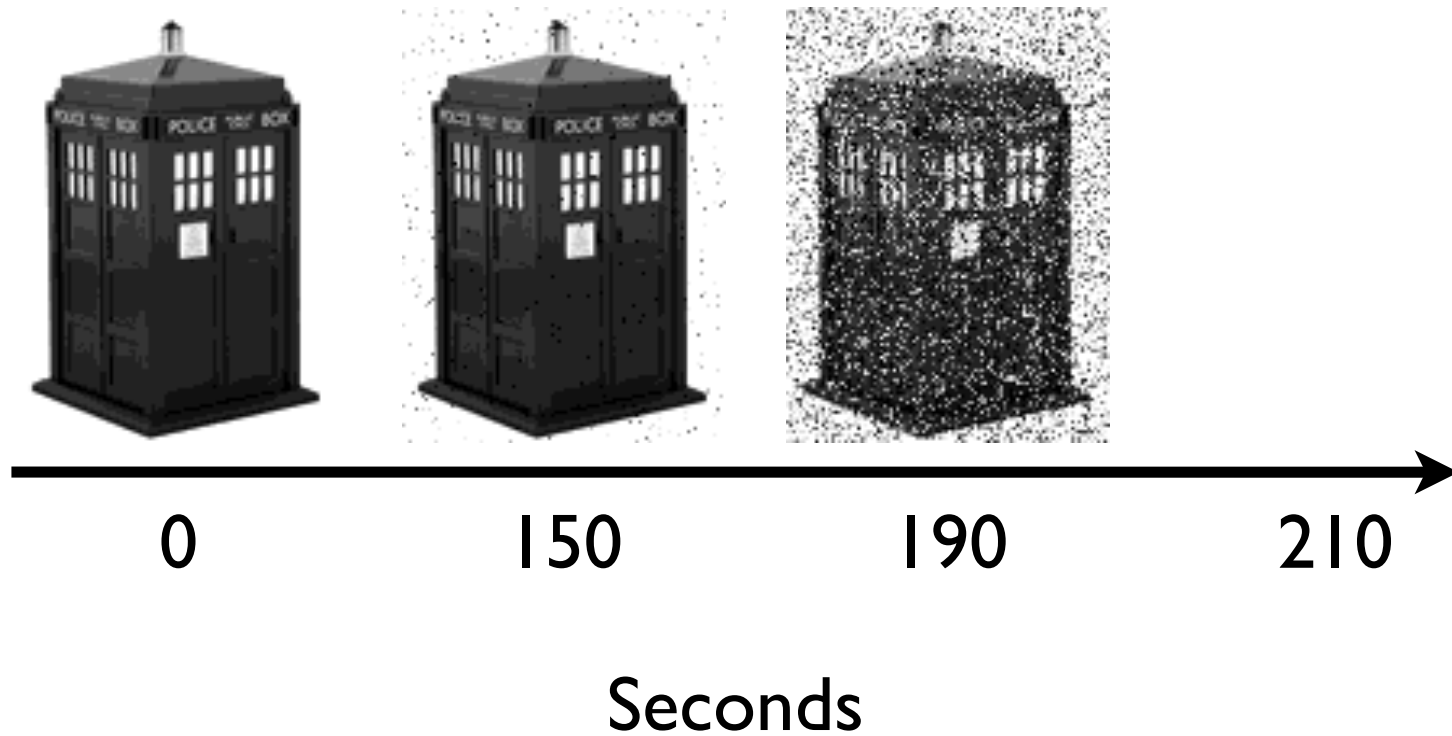
210

Seconds

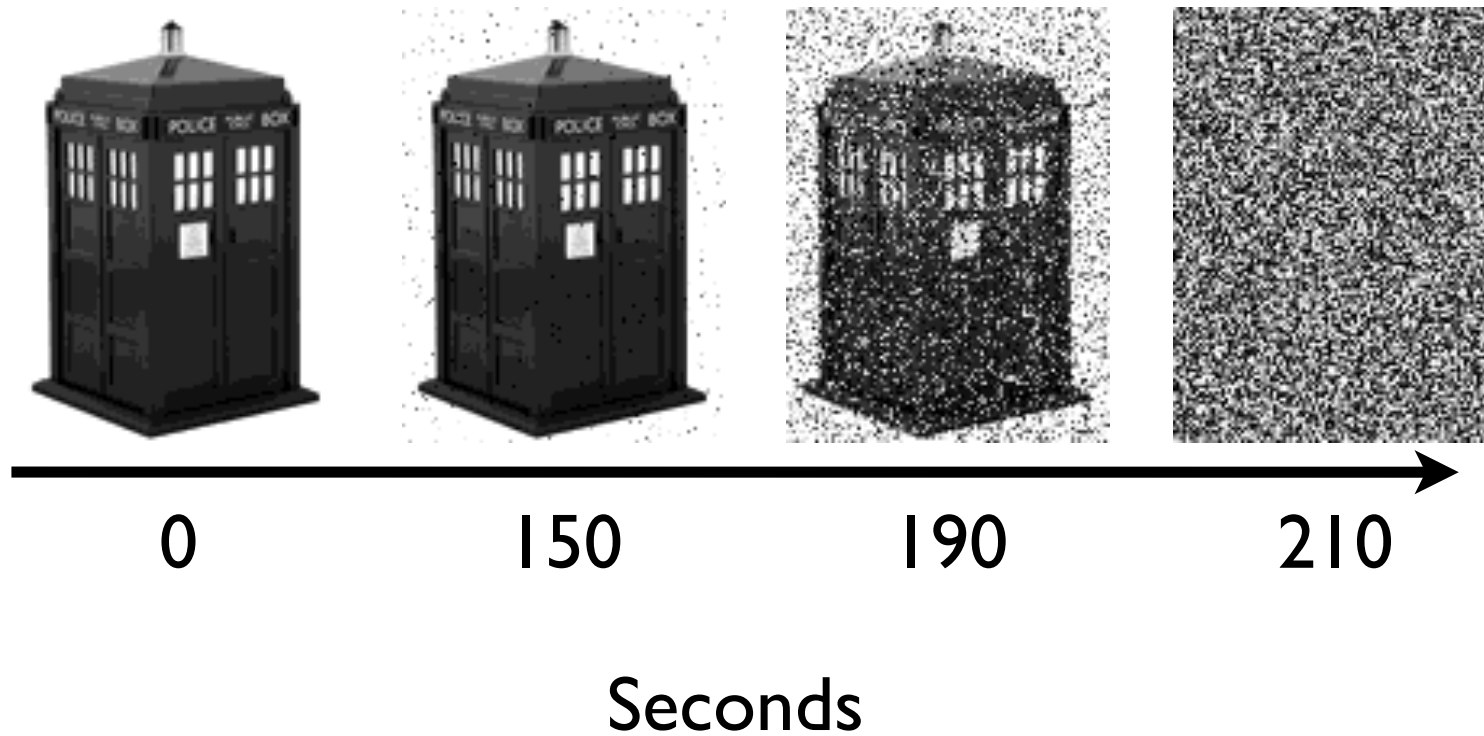
SRAM Remanence



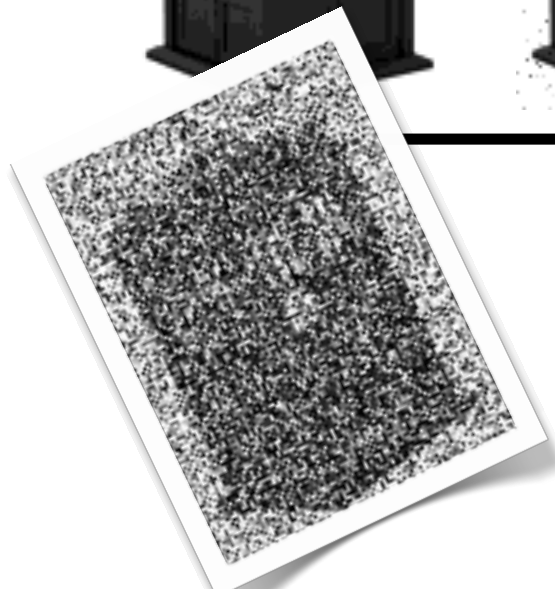
SRAM Remanence



SRAM Remanence



SRAM Remanence



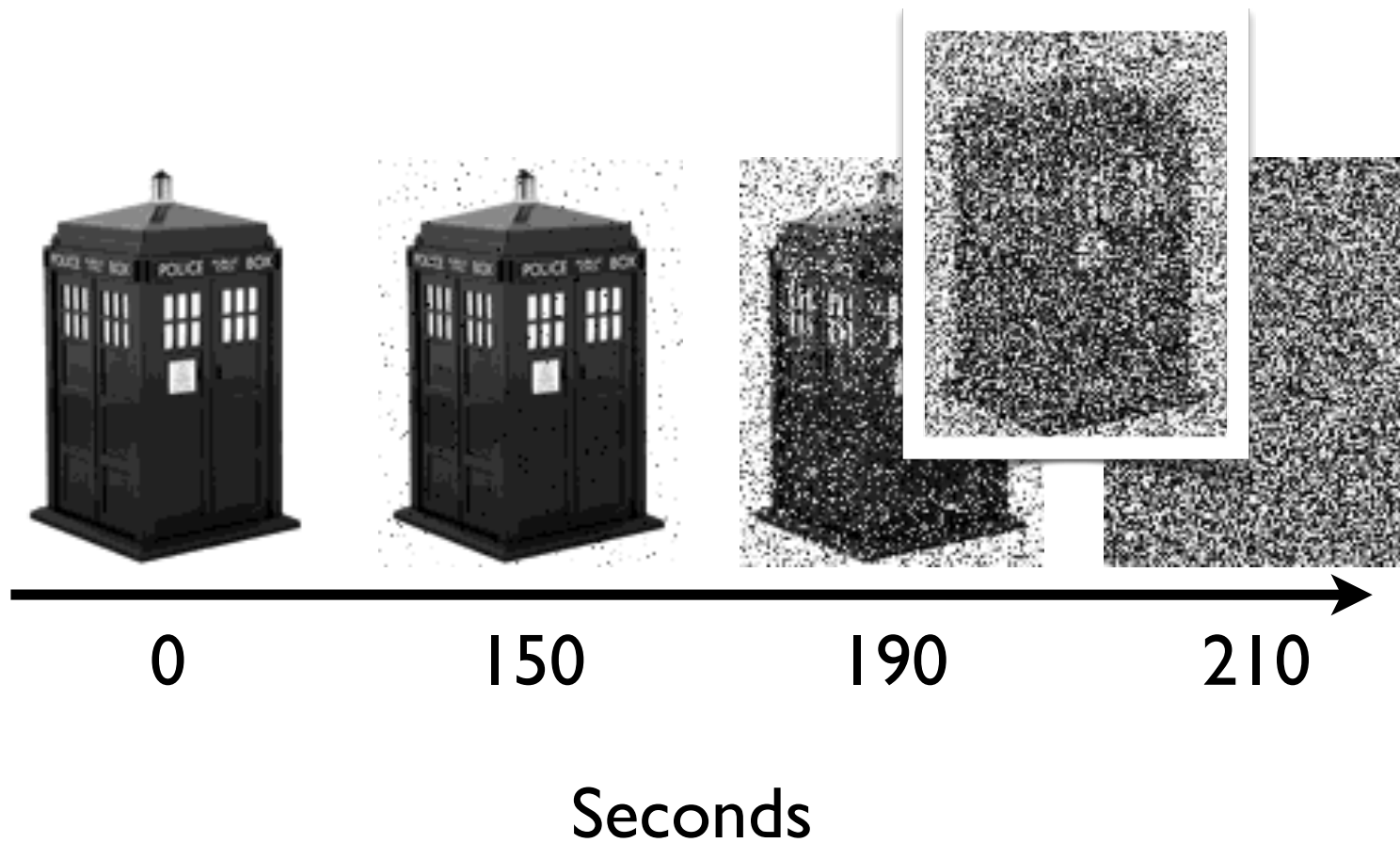
150

190

210

Seconds

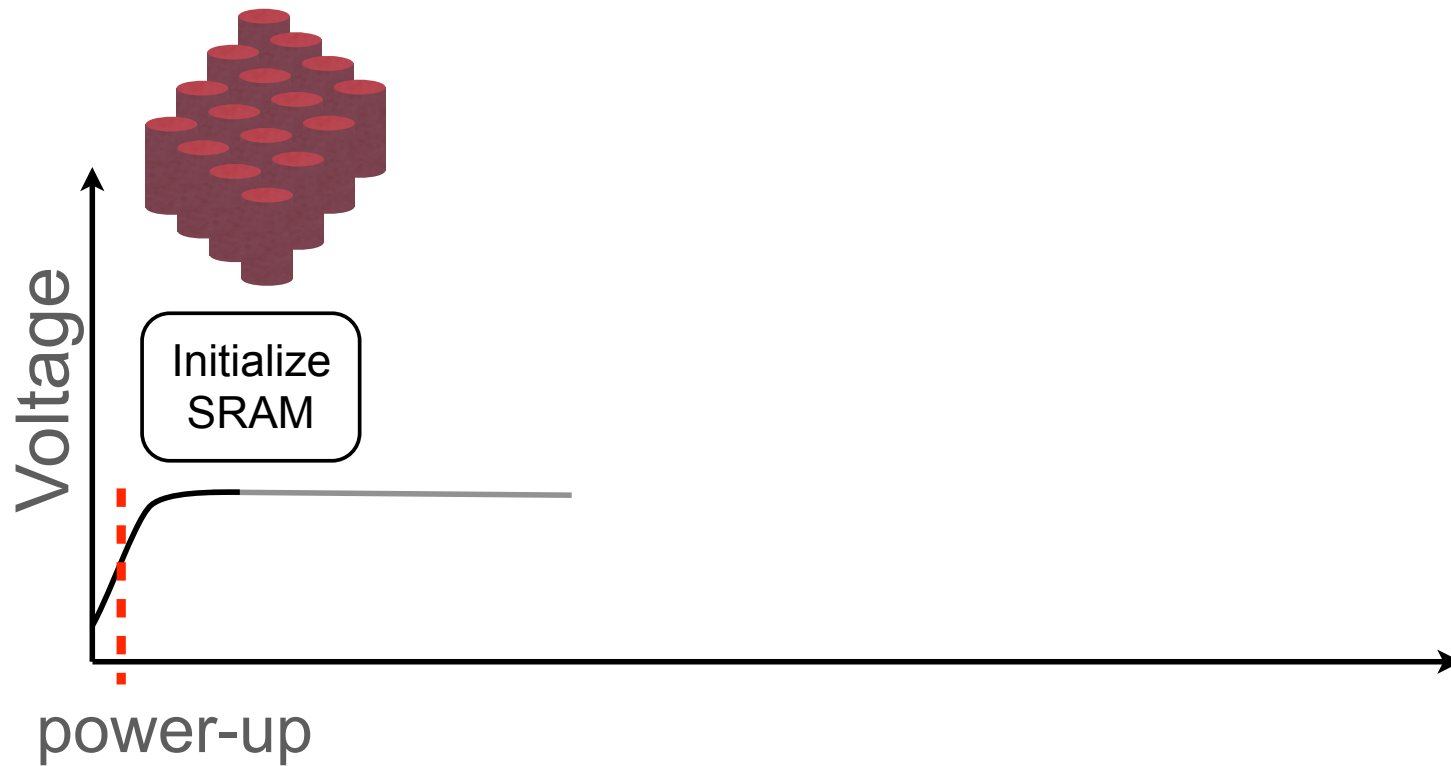
SRAM Remanence



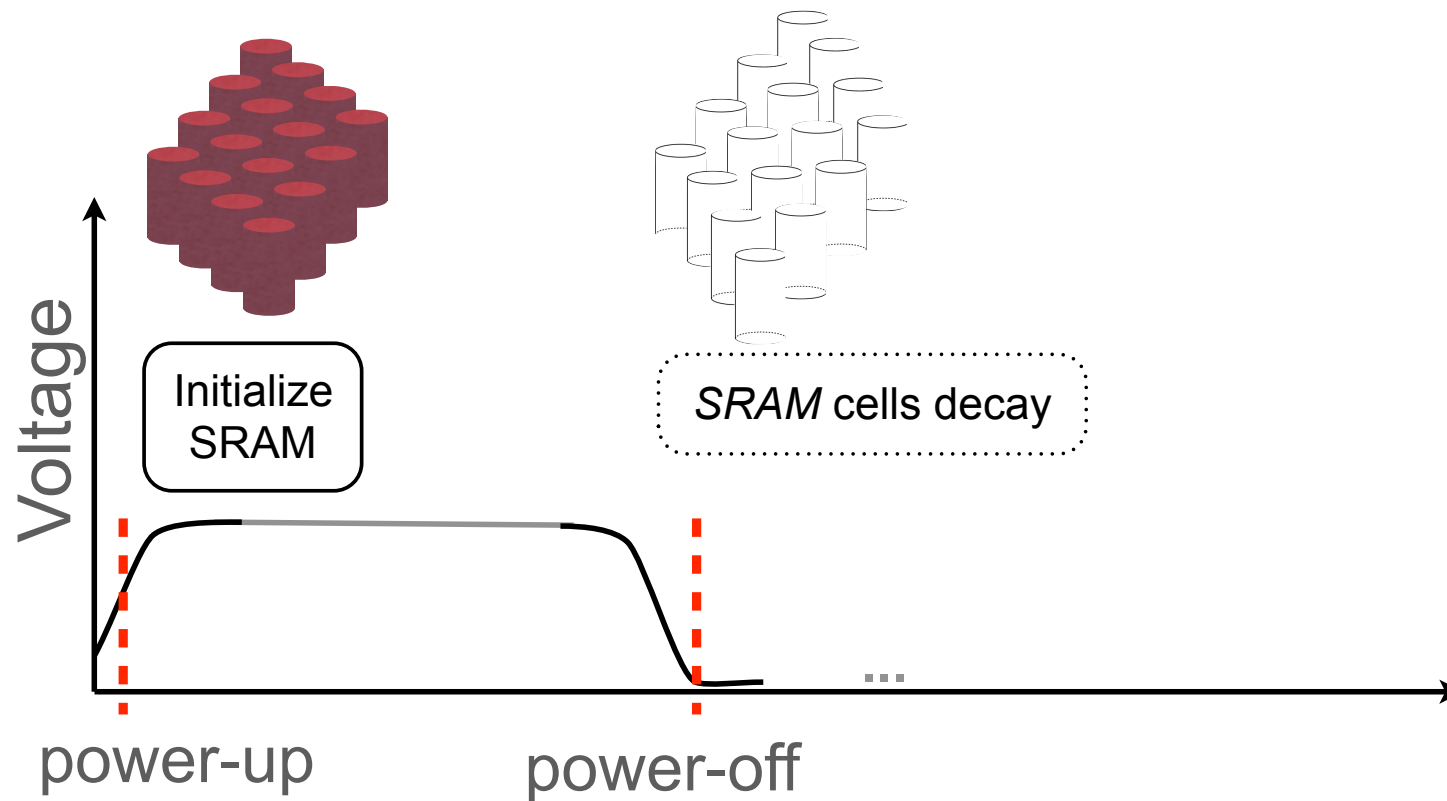
The TARDIS Algorithm



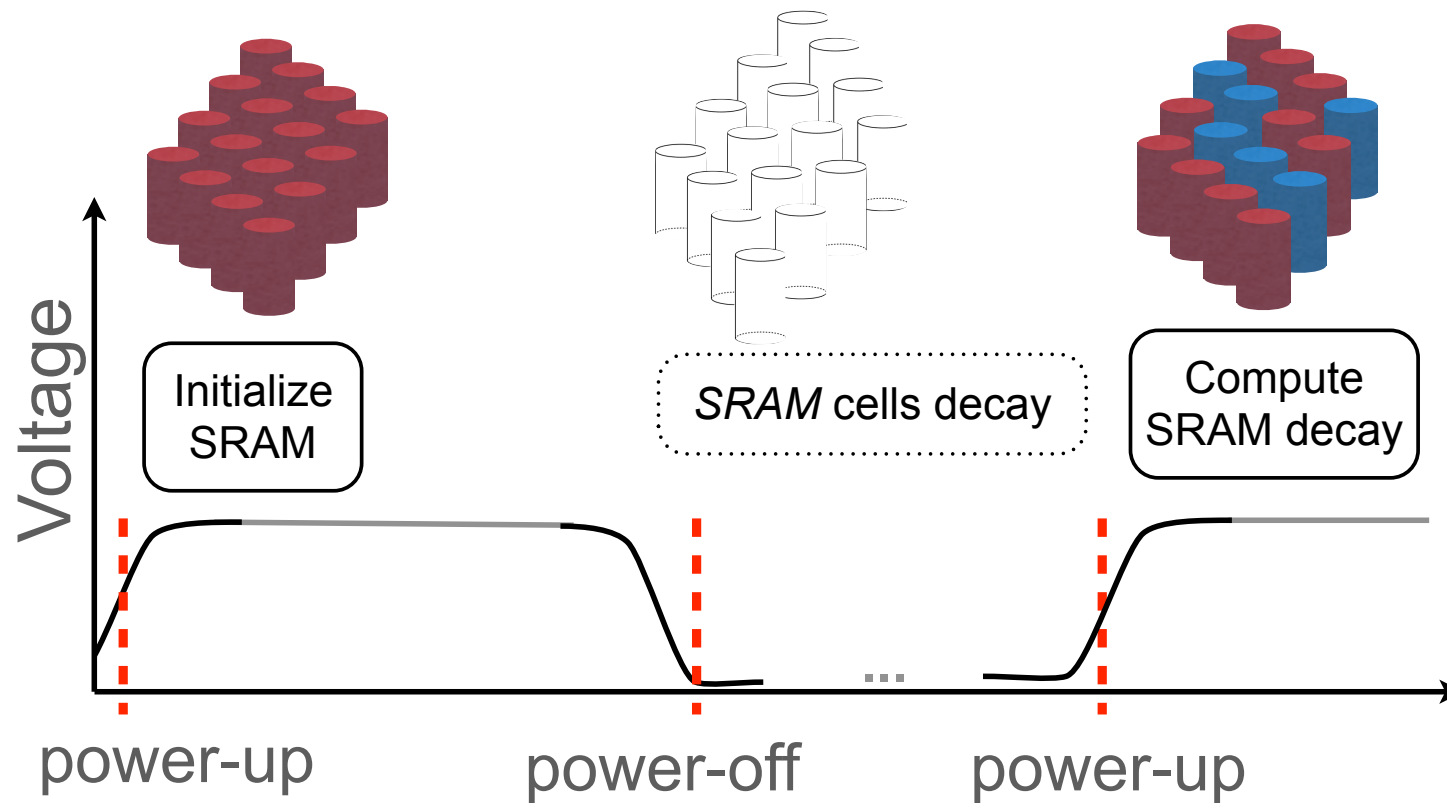
The TARDIS Algorithm



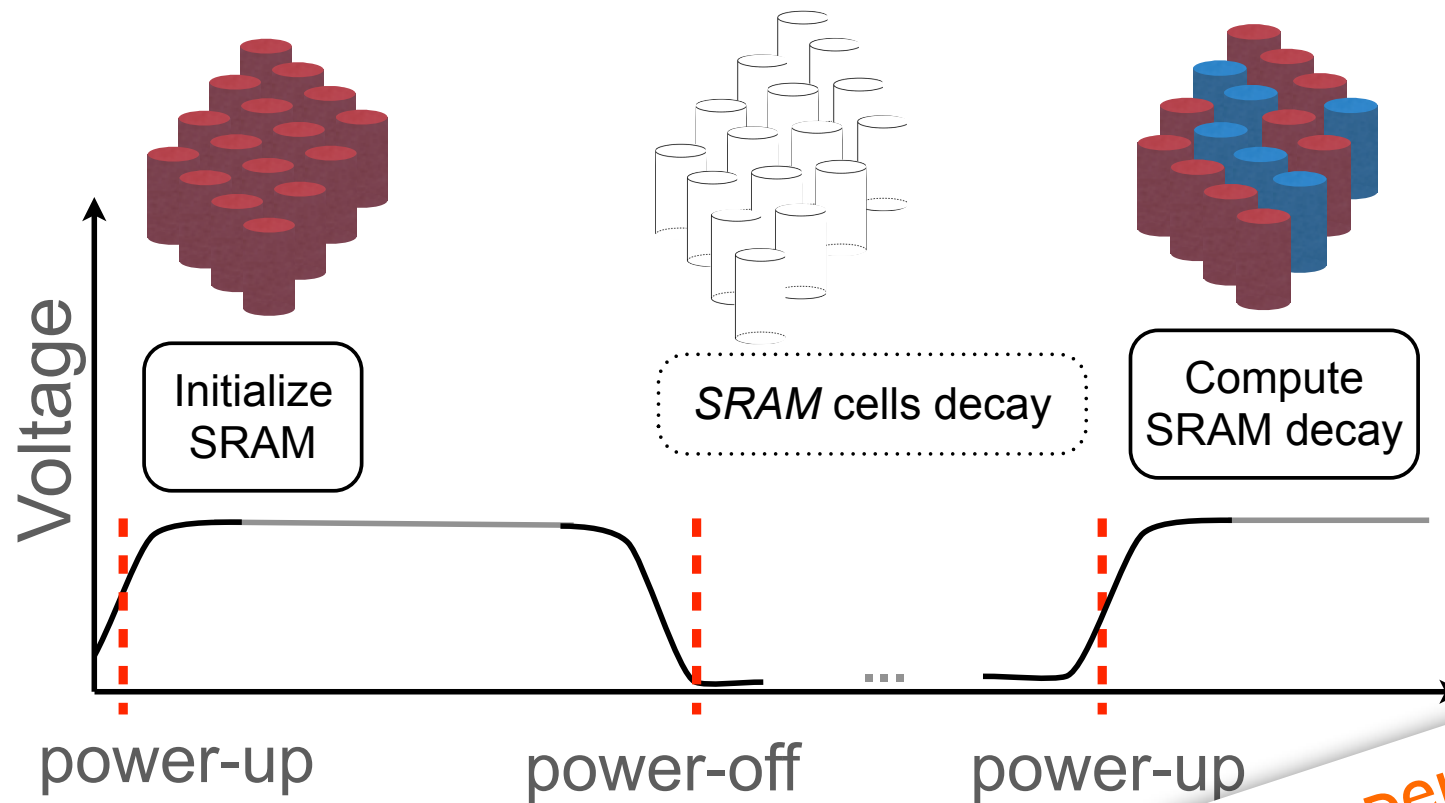
The TARDIS Algorithm



The TARDIS Algorithm



The TARDIS Algorithm

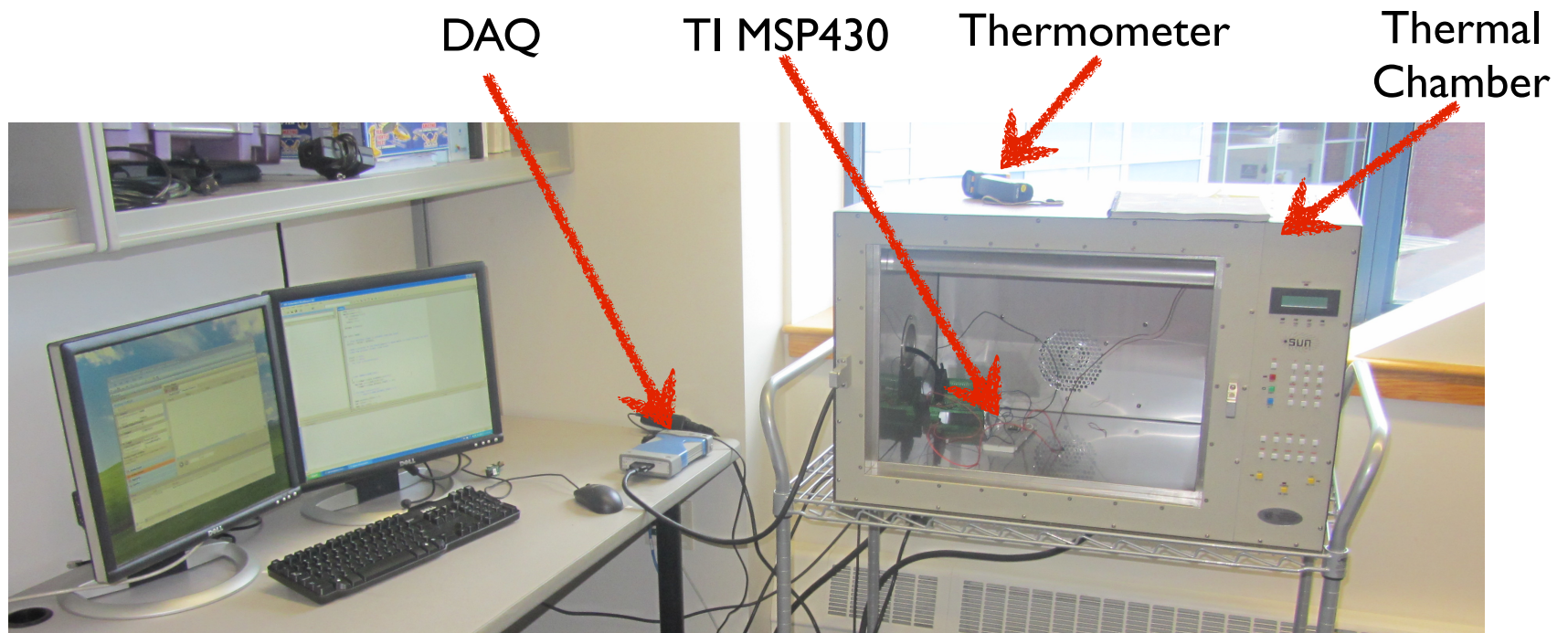


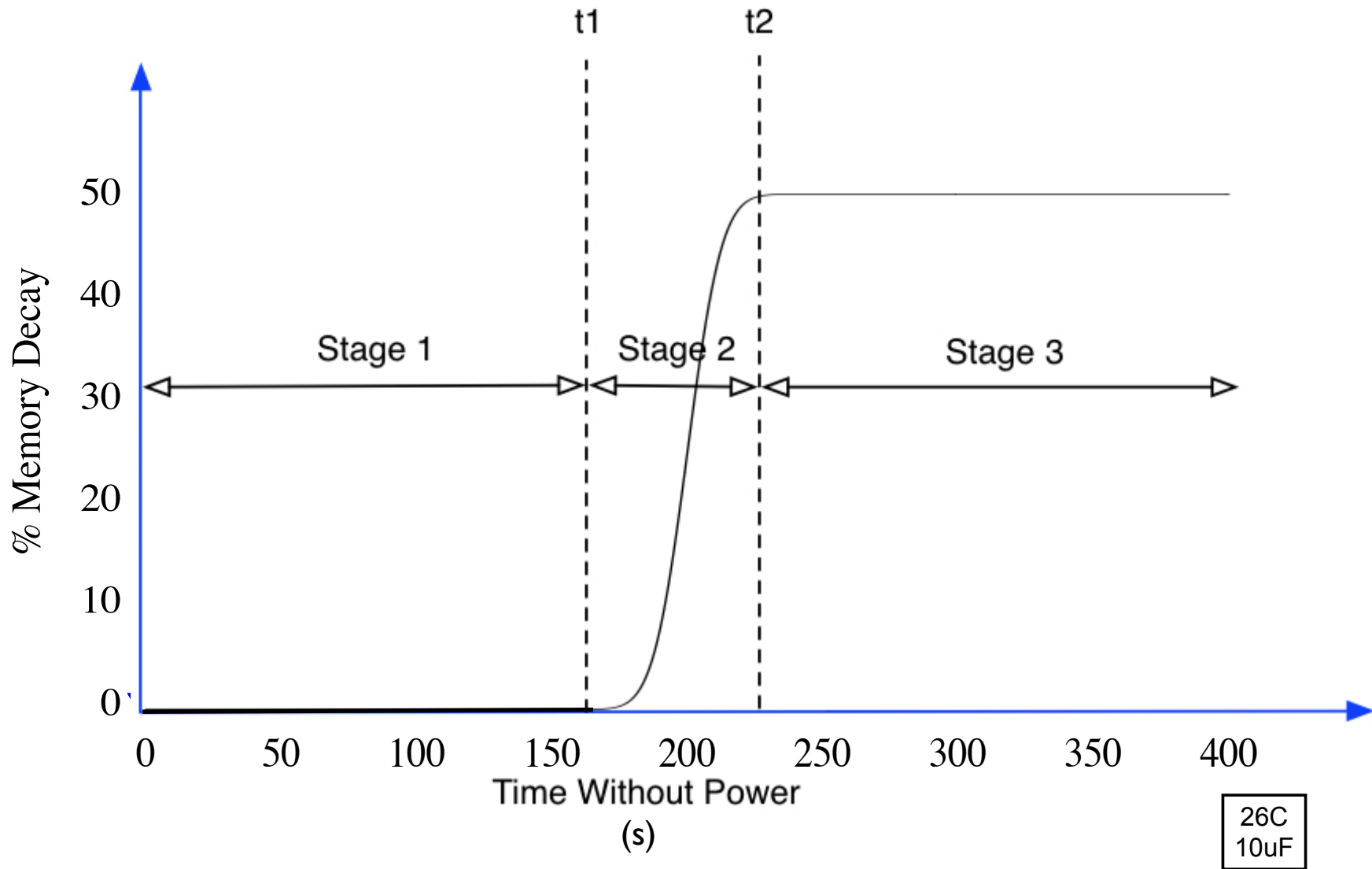
Temperature
Later...

Factors Influencing SRAM Decay

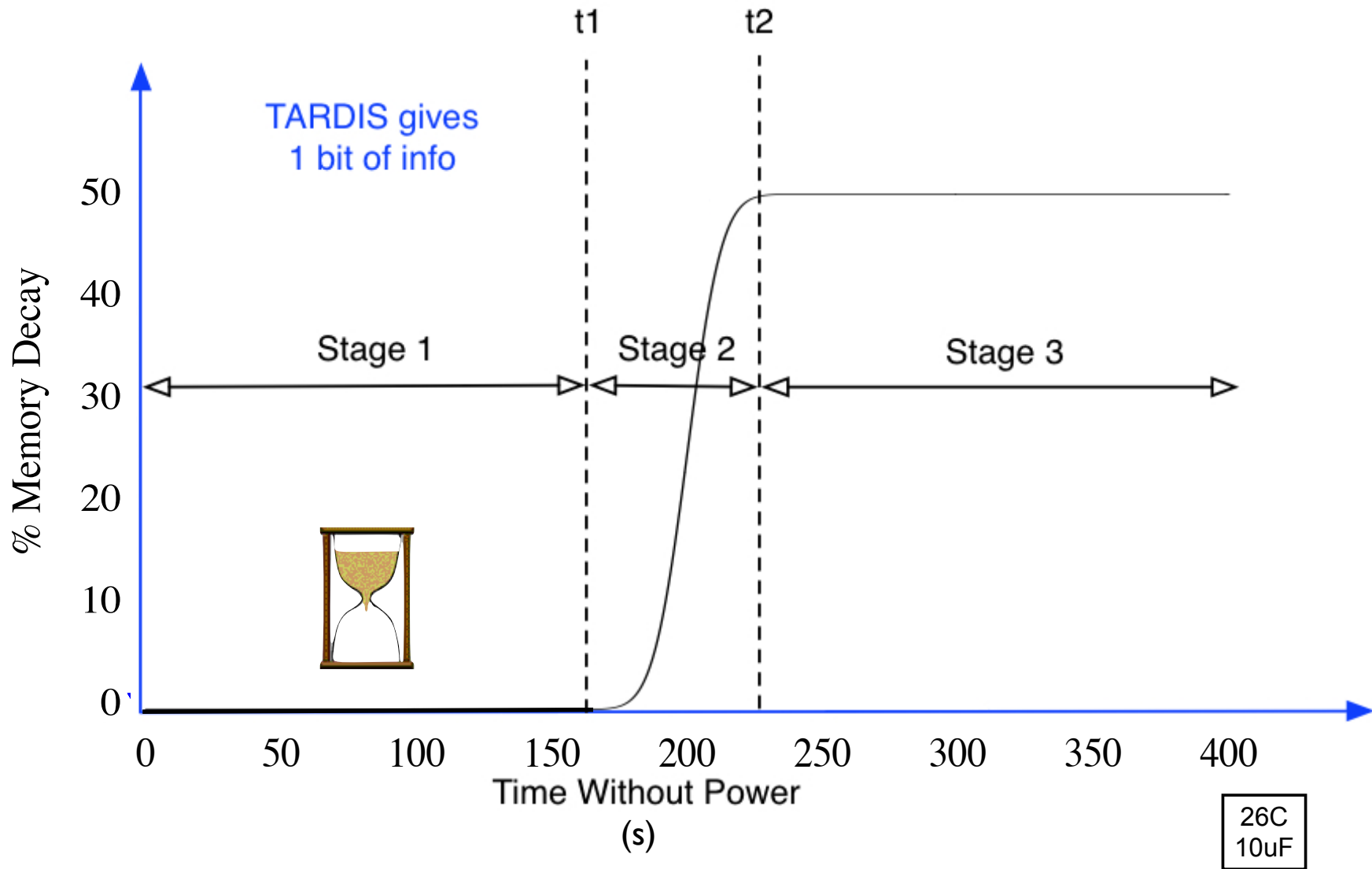
- ✓ SRAM Size
- ✓ Circuit Capacitance
- ✓ Temperature
- ✗ Chip Variation

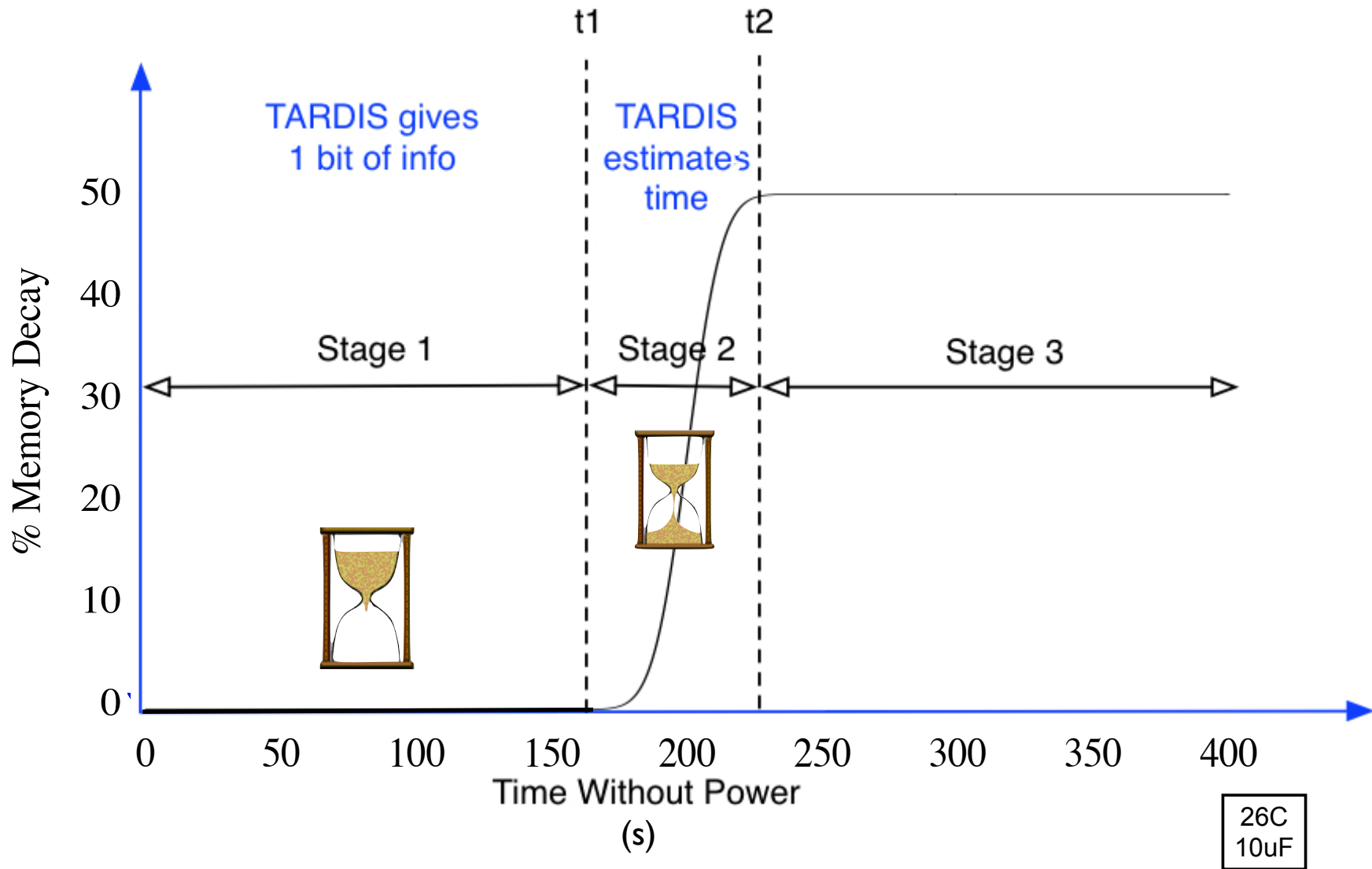
Experimental Setup

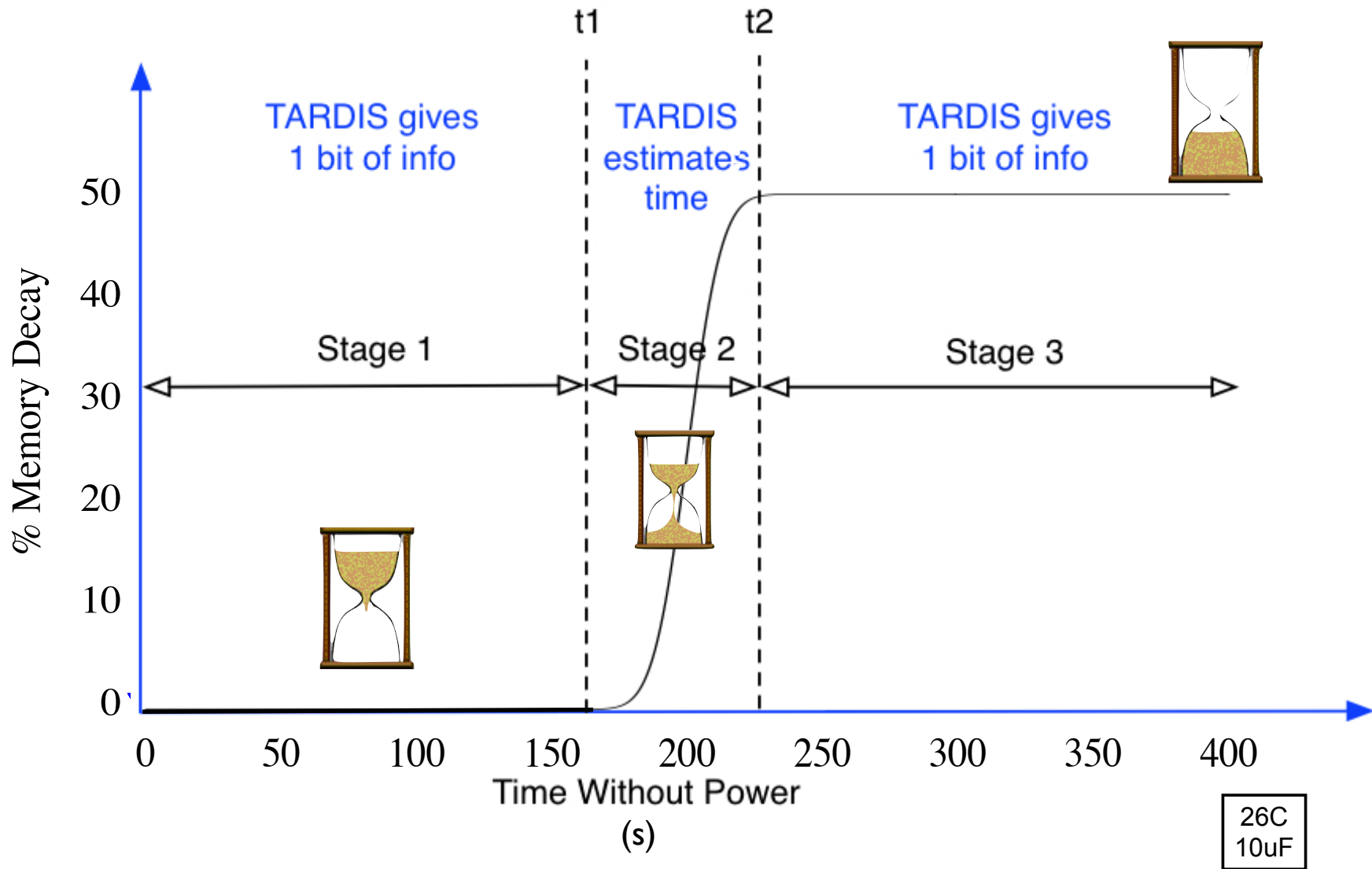




26C
10uF







Circuit Capacitance



Capacitor Size	Expiration time	Scale
$\sim 0\mu\text{F}$	$2.1 \times 10^0 \text{s}$	Seconds
$10\mu\text{F}$	$2.25 \times 10^2 \text{s}$	Minutes
$100\mu\text{F}$	$1.98 \times 10^3 \text{s}$	1/2 Hour
$1000\mu\text{F}$	$2.12 \times 10^4 \text{s}$	Hours
$10000\mu\text{F}$	$> 1.96 \times 10^5 \text{s}$	Days

Circuit Capacitance

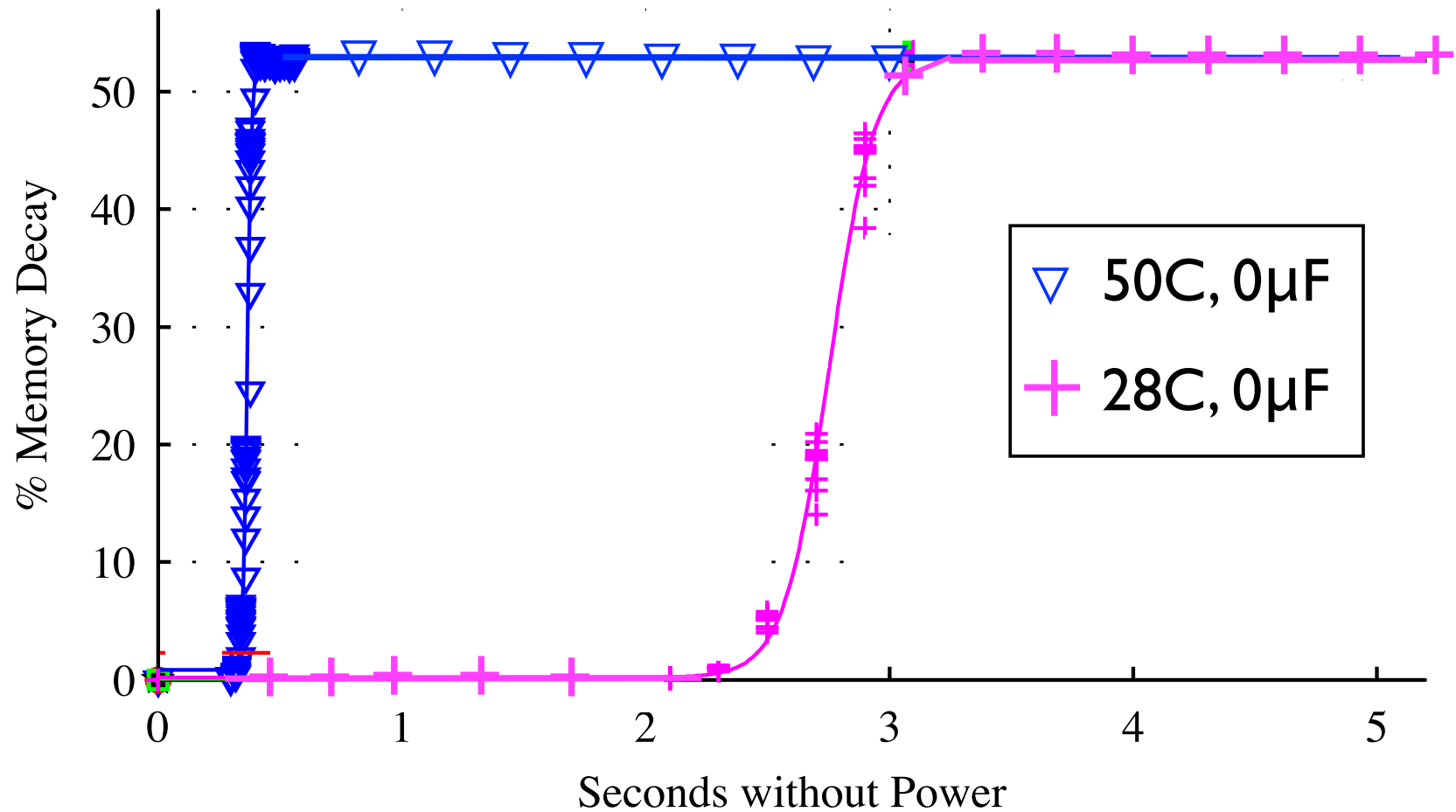
Capacitor Size	Expiration time	Scale
$\sim 0\mu\text{F}$	$2.1 \times 10^0 \text{s}$	Seconds
$10\mu\text{F}$	$2.25 \times 10^2 \text{s}$	Minutes
$100\mu\text{F}$	$1.98 \times 10^3 \text{s}$	1/2 Hour
$1000\mu\text{F}$	$2.12 \times 10^4 \text{s}$	Hours
$10000\mu\text{F}$	$> 1.96 \times 10^5 \text{s}$	Days

Smart Cards

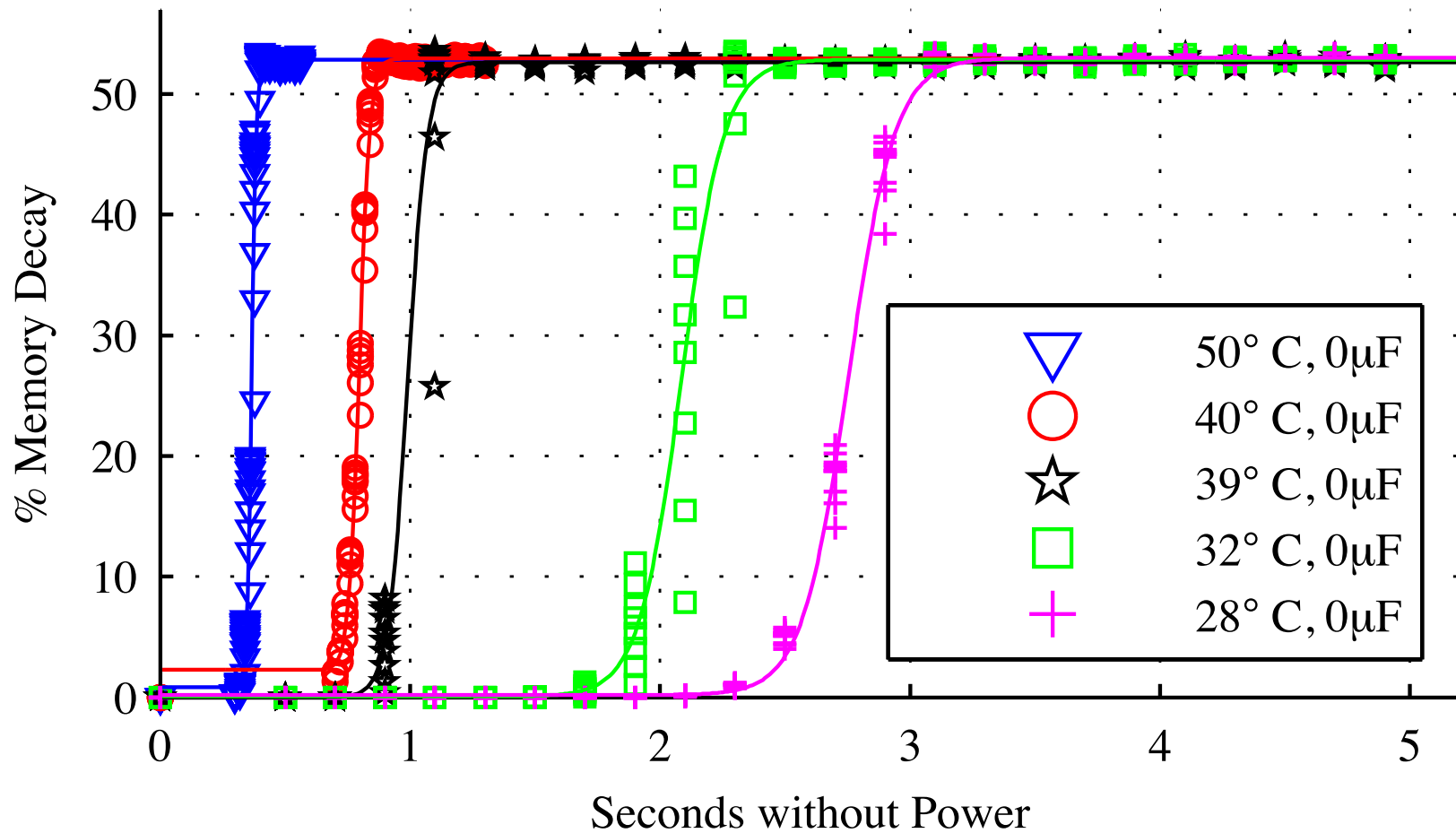


Batteryless Sensor = 100,000 μF

Temperature



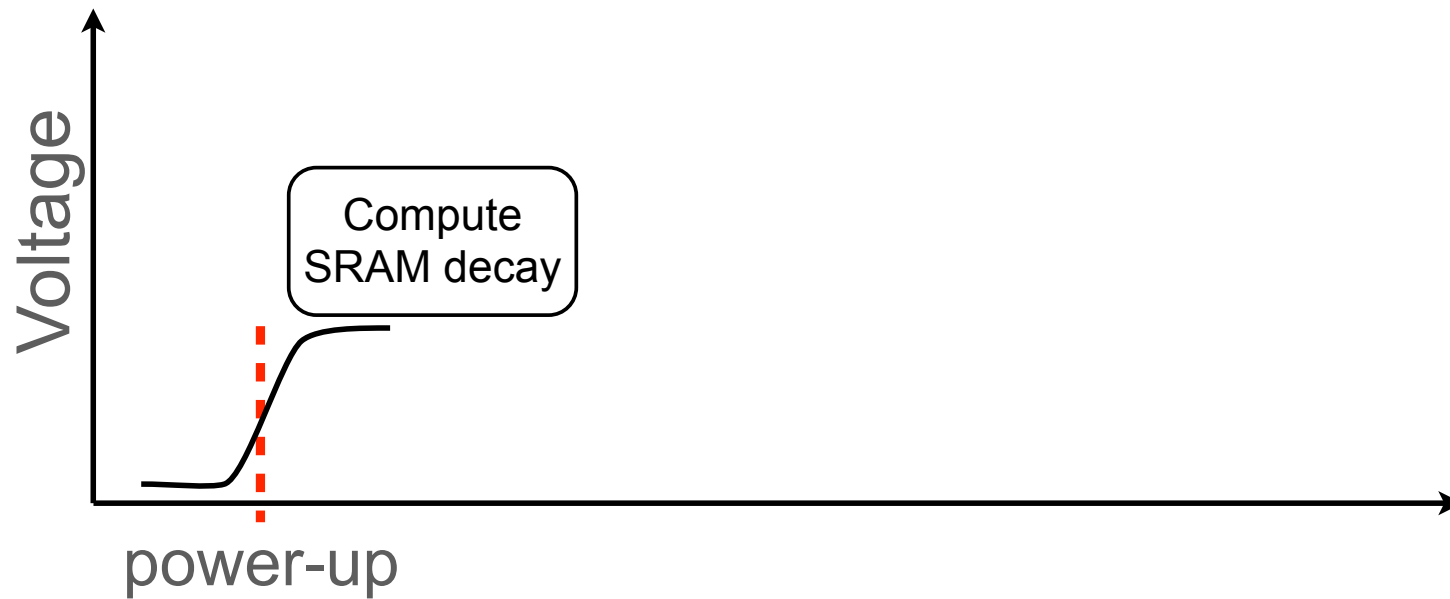
Temperature



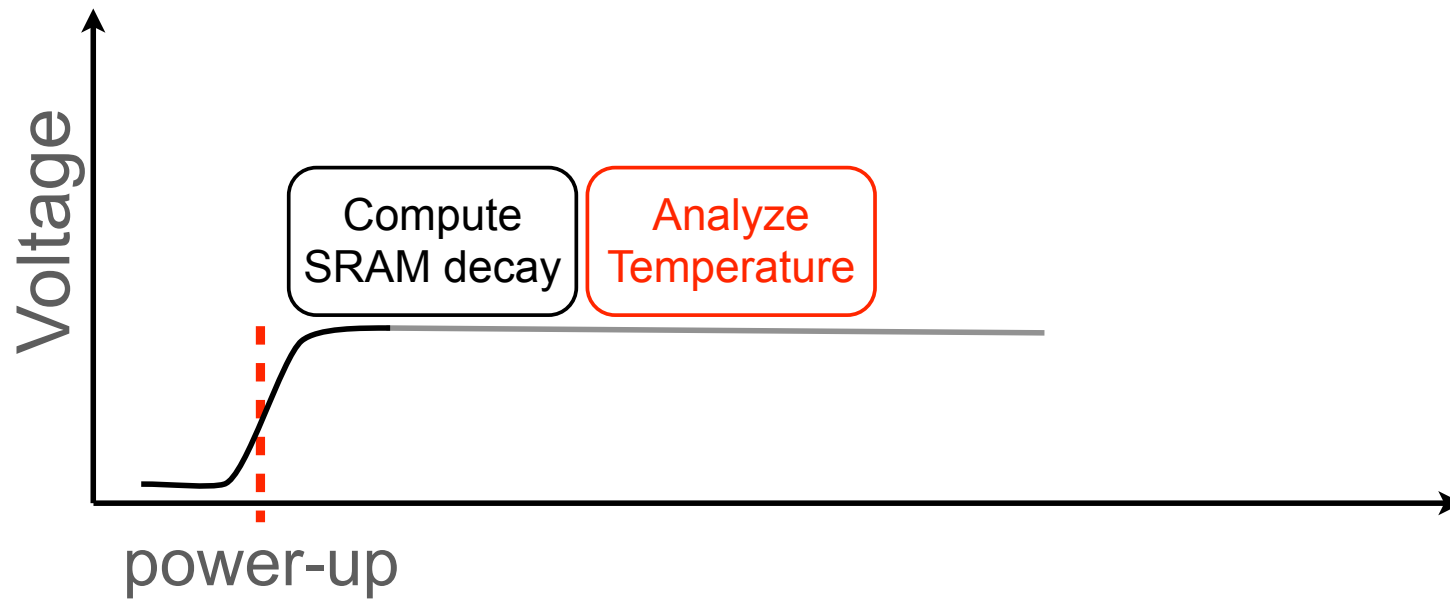
Compensate for Temperature



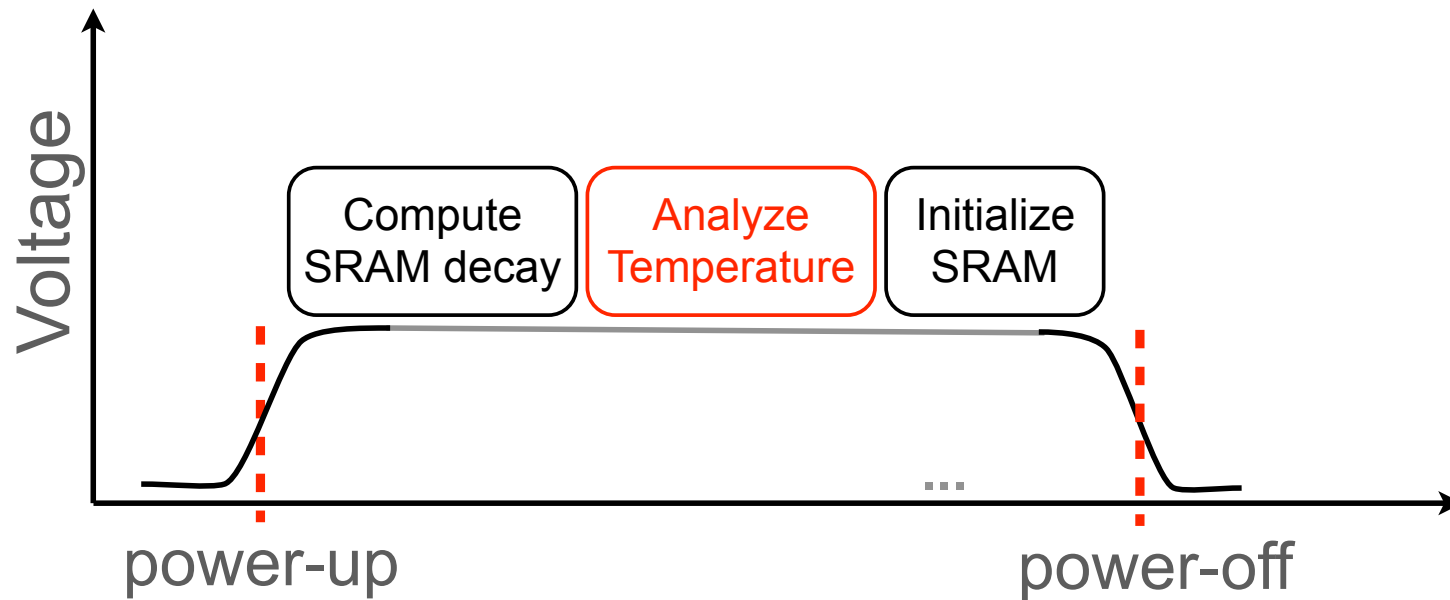
Compensate for Temperature



Compensate for Temperature

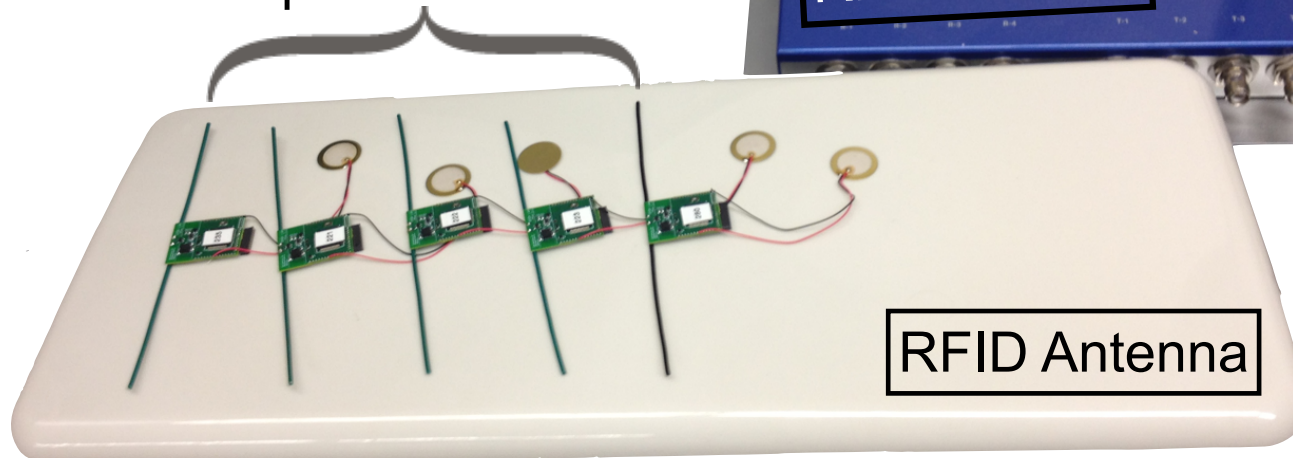


Compensate for Temperature



Implementation

 **UMASS
MOO**
UHF computational
RFID tags augmented
with piezo elements



Implementation

 **UMASS
MOO**
UHF computational
RFID tags augmented
with piezo elements

Expiration = 12s
 $\sigma = 0.11s$

RFID Reader

RFID Antenna

The Effect of TARDIS*

Device	#Queries	Time
UHF RFID Tags[Shamir'07]	200	2 Seconds
MIFARE Classic[Garcia'09]	1,500	16 Seconds
Digital Signal Transponder[Bono'05]	75,000	1 Hour
MIFARE DESFire[Paar'11]	250,000	7 Hours
GSM SIM Cards[Goldberg'99]	150,000	8 Hours

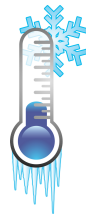
The Effect of TARDIS*

Device	#Queries	W/O TARDIS	W/ TARDIS
UHF RFID Tags	200	2 Seconds	40 Minutes
MIFARE Classic	1,500	16 Seconds	5 Hours
Digital Signal Transponder	75,000	1 Hour	10 Day
MIFARE DESFire	250,000	7 Hours	35 Days
GSM SIM Cards	150,000	8 Hours	21 Days

* Assuming a 12 seconds TARDIS

Attacking the TARDIS



- Cooling





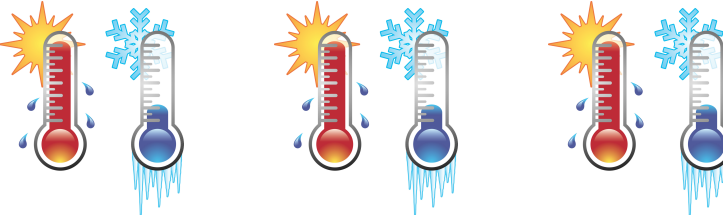
- Heating



Attacking the TARDIS

- Cooling Thermal Sensor 
- Heating Thermal Sensor 

Attacking the TARDIS

- Cooling  Thermal Sensor
- Heating  Thermal Sensor
- Pulse 

Attacking the TARDIS

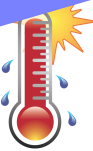
- Cooling

Thermal Sensor



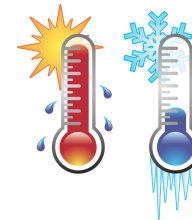
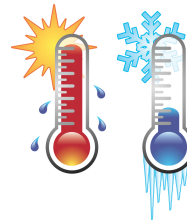
- Heating

Thermal Sensor



- Pulse

Physical Limitations



Attacking the TARDIS

- Cooling

Thermal Sensor



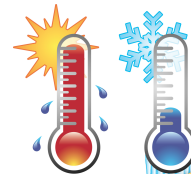
- Heating

Thermal Sensor



- Pulse

Physical Limitations



Thermal Fuse

Other Applications

- **Time out** in authentication protocols
- **Temporary ownership (Resurrecting Duckling)**
- RTC replacement in low-power sensors
- E-passports [Avoine'08]
- Time released cryptography [May'93,Rivest'96,May'01]

Related Work

Data Remanence in Volatile Memory

- Data retention in SRAM [Gutmann'01,Skorobogatov'02]
- FERNS [Holcomb'07]
- DRAM cold boot attack [Halderman'08]
- Background to data retention [Flautner'02]
- First proposed attacks [Anderson'96]
- SRAM attack [Taun'07]

Related Work

Reliable Time

- Lamport Clock [Lamport'78]
- Use Multiple Sources of Time [Rousseau'01]

Conclusion



uses memory decay to estimate time.



makes brute force attacks orders of magnitude harder.



is just software.



uses remanence decay for good.

Photo Credit: thinkgeek.com

SPQR
LABORATORY

<https://spqr.cs.umass.edu/tardis/>

