Photo Credit: thinkgeek.com

TARDIS

Time and Remanence Decay in SRAM to Implement Secure Protocols on Embedded Devices without Clocks

Amir Rahmati[1], Mastooreh Salajegheh[1], Dan Holcomb[2], Jacob Sorber[3],Wayne Burleson[1], Kevin Fu[1]

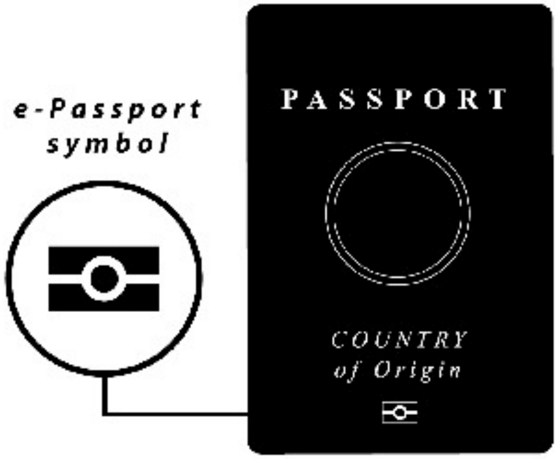
1 UMass Amherst 2 UC Berkeley, 3 Dartmouth College

This research is supported by NSF grants CNS-0831244, CNS-0845874, CNS-0923313, CNS-0964641, SRC task 1836.074, Gigascale Systems Research Center, and a Sloan Research Fellowship. Any opinions, findings, conclusions, and recommendations expressed in these materials are those of the authors and do not necessarily reflect the views of the sponsors. Portions of this work are patent pending.

Batteryless Devices

Transportation

Payment



Passports

Employee IDs

Photo Credit: digboston.com, mobileedgeblog.com, dhs.gov, vanntel.com

Batteryless Devices

Transportati

nt

Passports

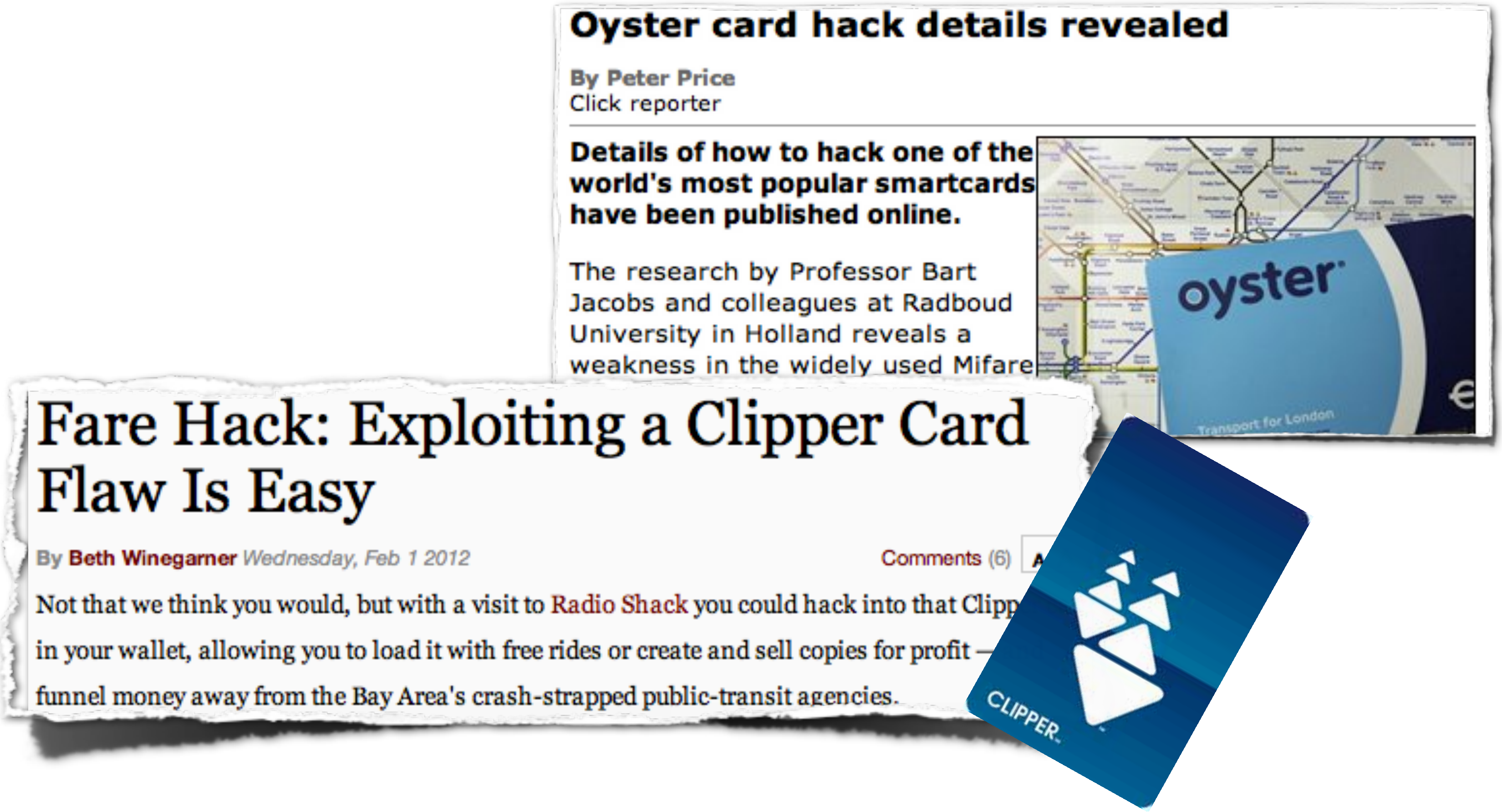
Employee IDs

Things in Common

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

Photo Credit: digboston.com, mobileedgeblog.com, dhs.gov, vanntel.com

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.

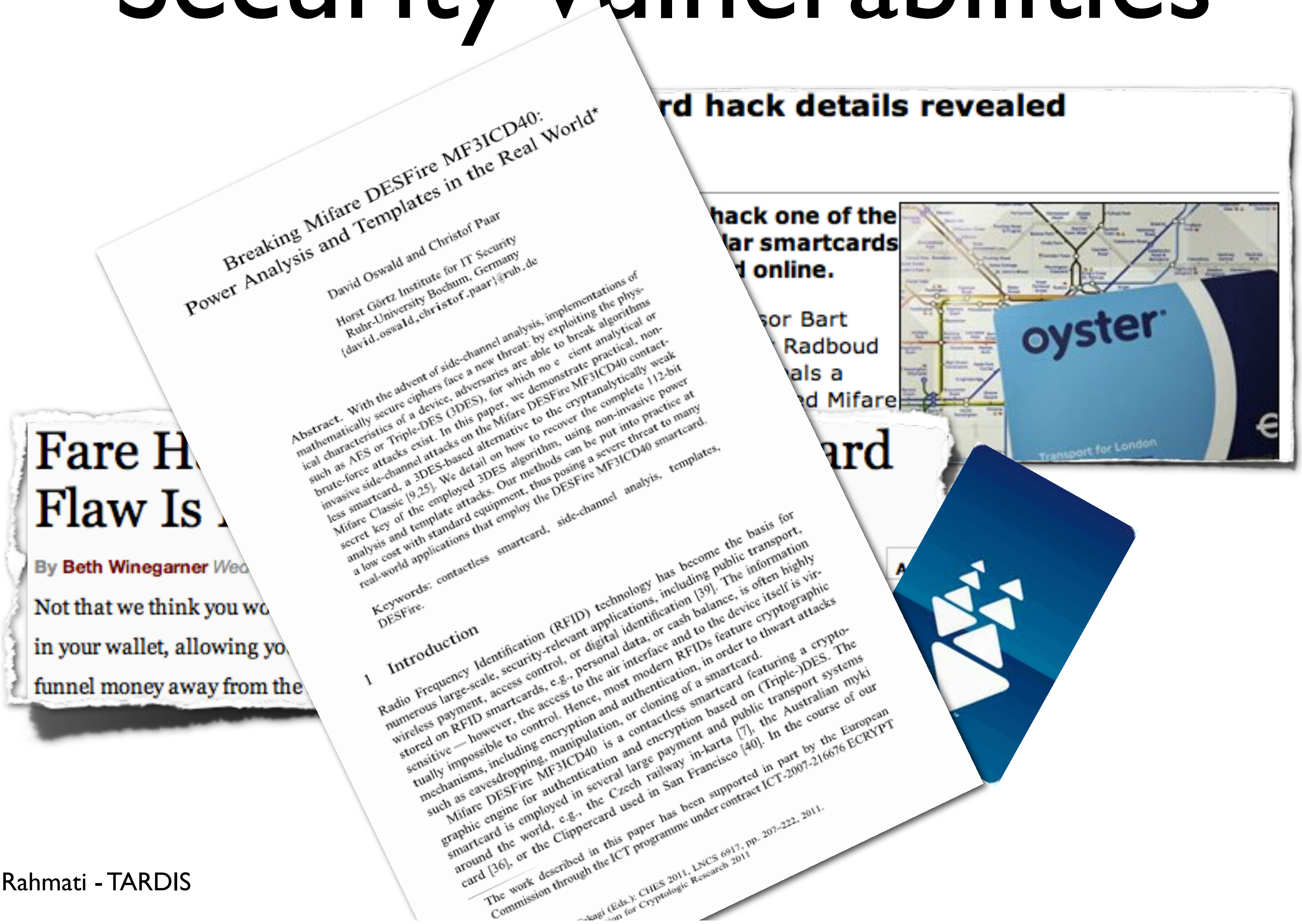
The research by Professor Bart Jacobs and colleagues at Radboud University in Holland reveals a weakness in the widely used Mifare

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 Clipp 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



rd hack details revealed

hack one of the
lar smartcards
d online.

sor Bart
Radboud
als a
d Mifare

Fare H
Flaw Is

ard

By Beth Winegarner Wed

Not that we think you wo
in your wallet, allowing yo
funnel money away from the

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 e cient 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 analyis, templates, DESFire.

1 Introduction

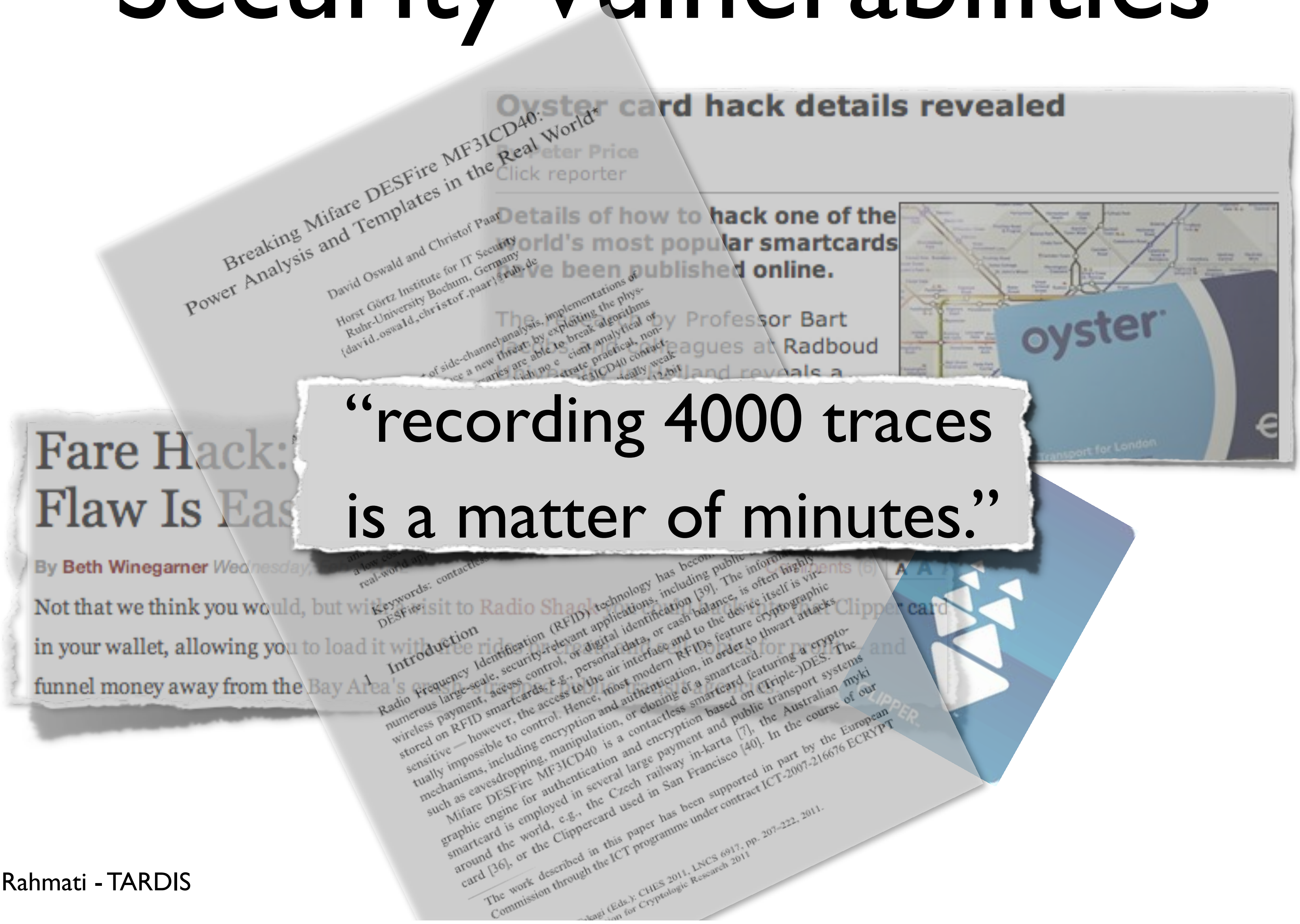
Radio Frequency Identification (RFID) technology has become the basis for numerous large-scale, security-relevant applications, including public transport, wireless payment, access control, or digital identification [39]. The information stored on RFID smartcards, e.g., personal data, or cash balance, 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 MF3ICD40 is a contactless smartcard featuring a cryptographic engine for authentication and encryption based on (Triple-)DES. The smartcard 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 Clippercard 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

kagi (Eds.): CHES 2011, LNCS 6917, pp. 207–222, 2011.
ion for Cryptologic Research 2011

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 ... by Professor Bart ... colleagues at Radboud ... Holland reveals a

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

Keywords: contactless ... DESFire

1 Introduction

Radio Frequency Identification (RFID) technology has become ... numerous large-scale, security-relevant applications, including public ... 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. The Mifare DESFire MF3ICD40 is a contactless smartcard featuring a cryptographic engine for authentication and encryption based on (Triple-)DES. The smartcard 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 Clippercard 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

...(Eds.): CHES 2011, LNCS 6917, pp. 207–222, 2011.
...for Cryptologic Research 2011

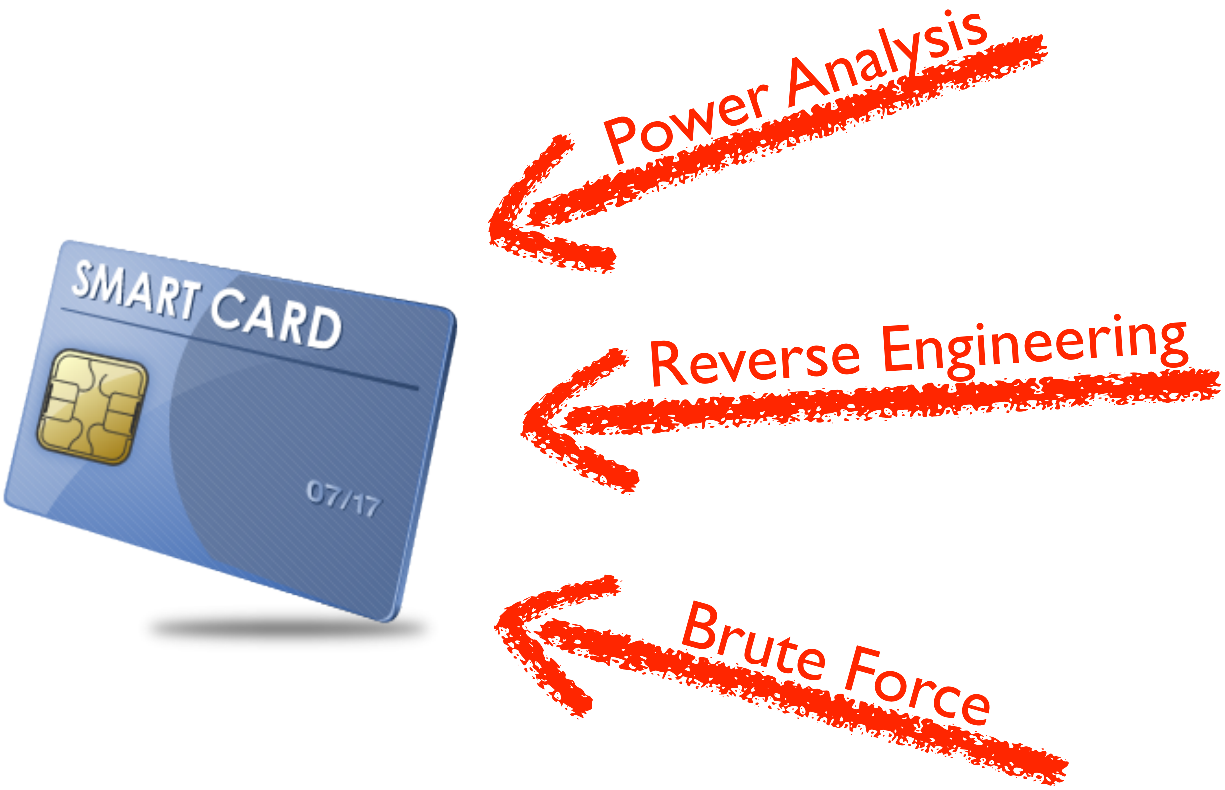
Fare Hack: ...
Flaw Is Eas...

By Beth Winegarner Wednesday, ...

Not that we think you would, but with a visit to Radio Shack ... Clipper card in your wallet, allowing you to load it with free rides ... for profit — and funnel money away from the Bay Area's ...

> “recording 4000 traces is a matter of minutes.”

Smart Card Threats



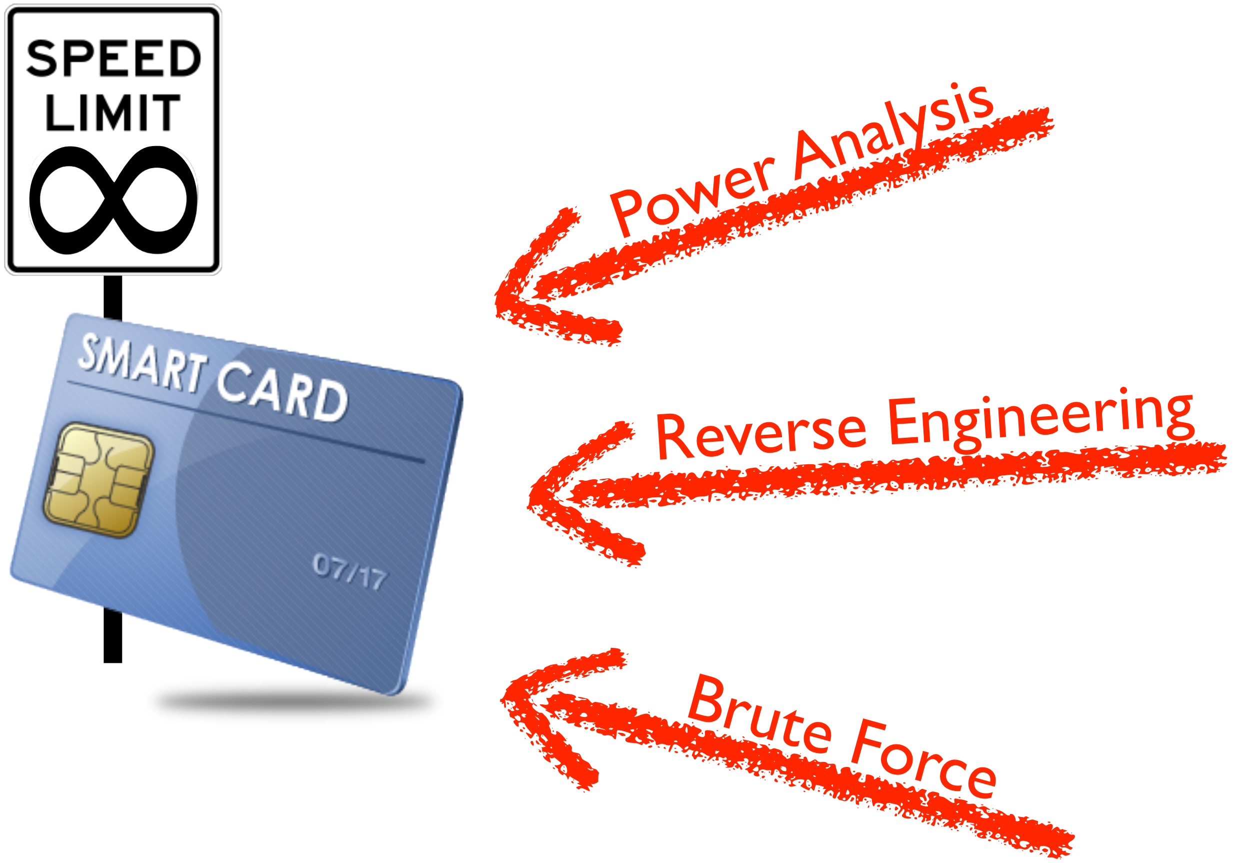
Power Analysis

Reverse Engineering

Brute Force

Photo Credit: 1and1soft.com

Smart Card Threats



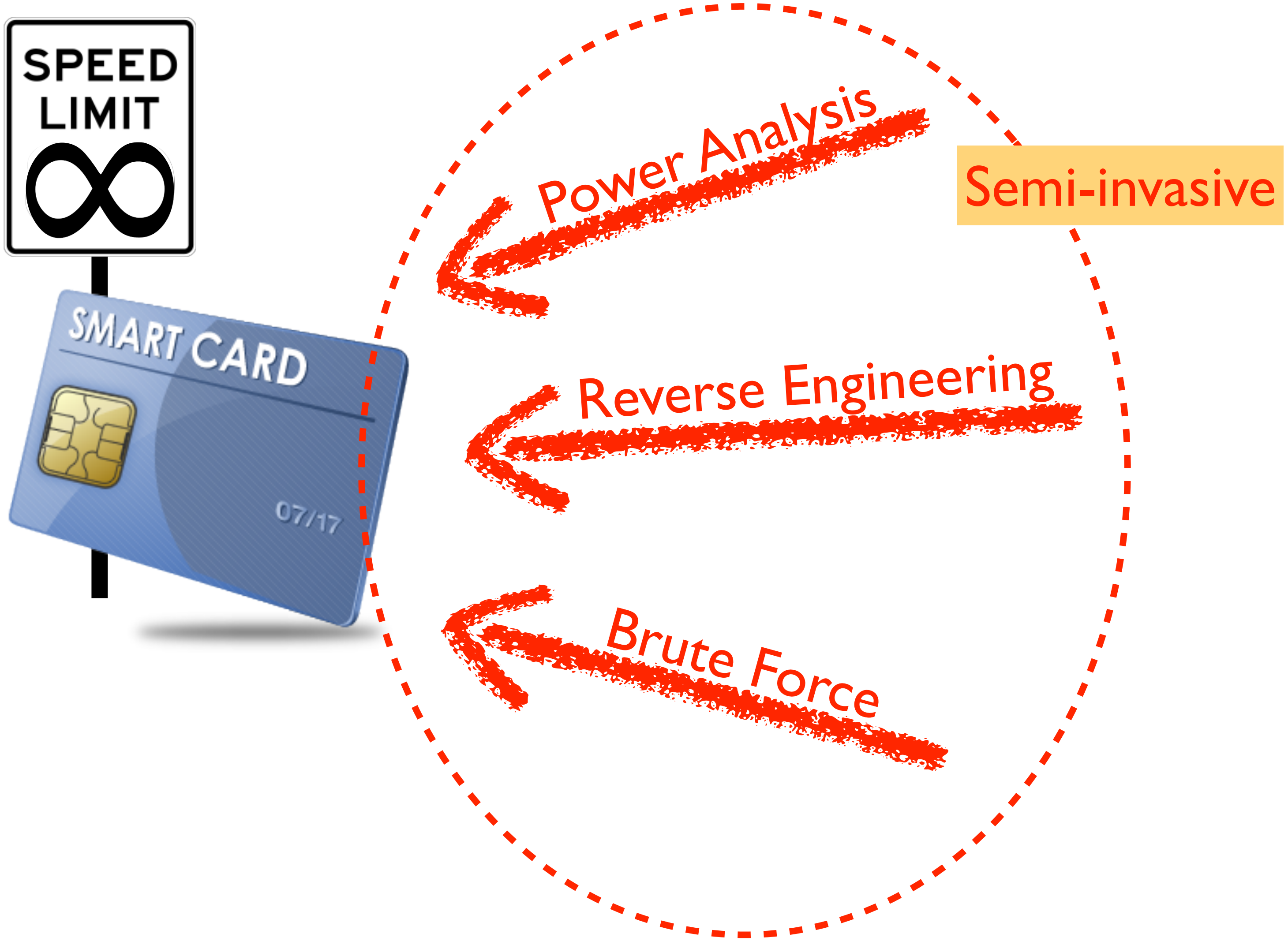
Power Analysis

Reverse Engineering

Brute Force

Photo Credit: 1and1soft.com

Smart Card Threats



Power Analysis

Semi-invasive

Reverse Engineering

Brute Force

Photo Credit: 1and1soft.com

Vulnerable to Brute Force Attacks

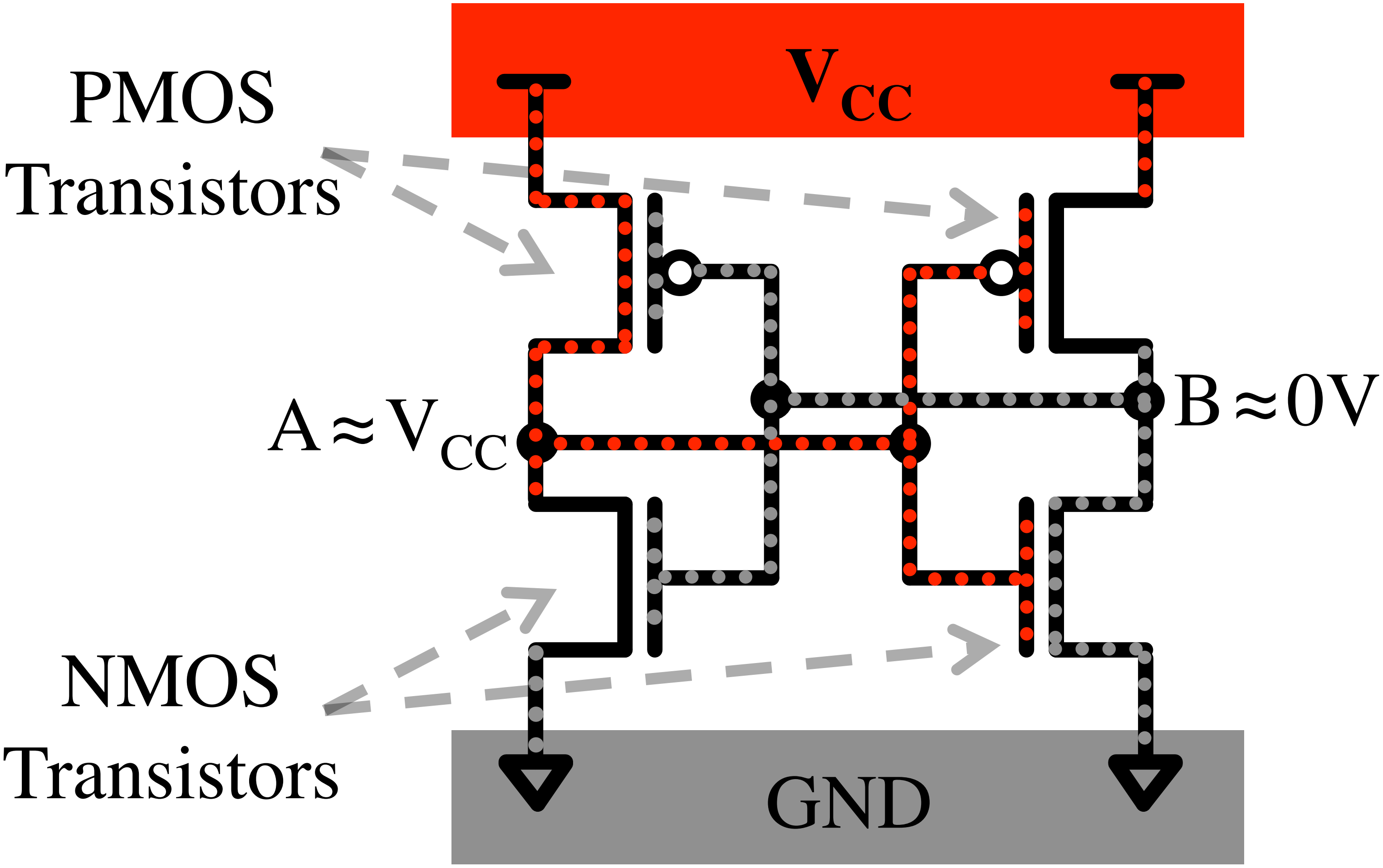
Device	#Queries	Time
UHF RFID Tags[Shamir'07]	200	2 Seconds
MIFARE Classic[Garcia'09]	1,500	16 Seconds
Digital Signal Transponder[Bono'05]	75,000	1 Hour
MIFARE DESFire[Paar'11]	250,000	7 Hours
GSM SIM Cards[Goldberg'99]	150,000	8 Hours

Photo Credit: thinkgeek.com

Our Contribution: TARDIS

A time-keeping technique based on SRAM decay

SRAM Remanence



PMOS Transistors

V_{CC}

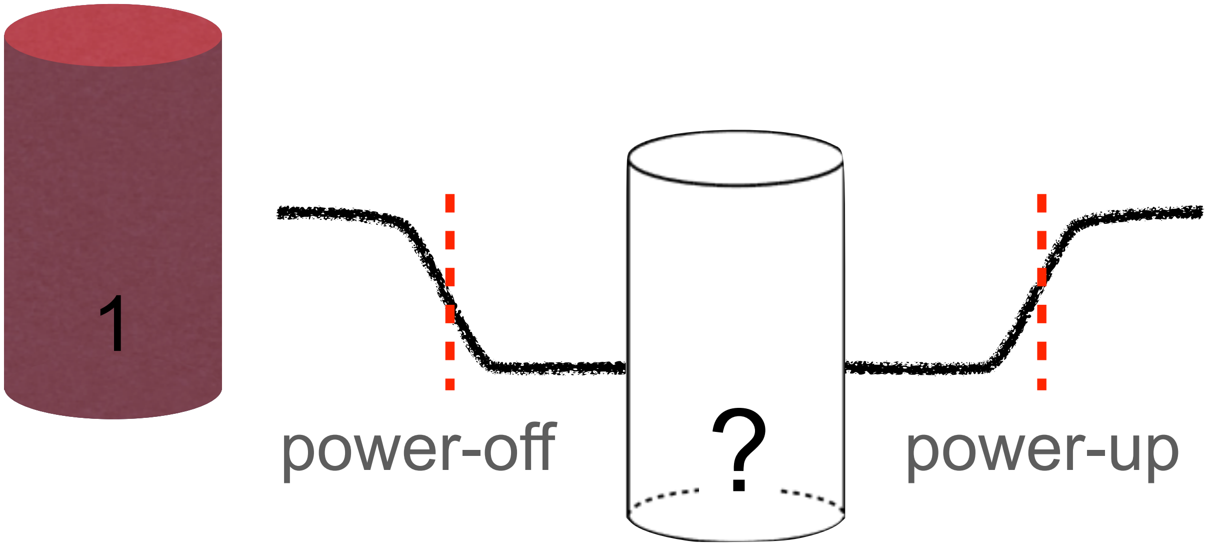
$A \approx V_{CC}$

$B \approx 0V$

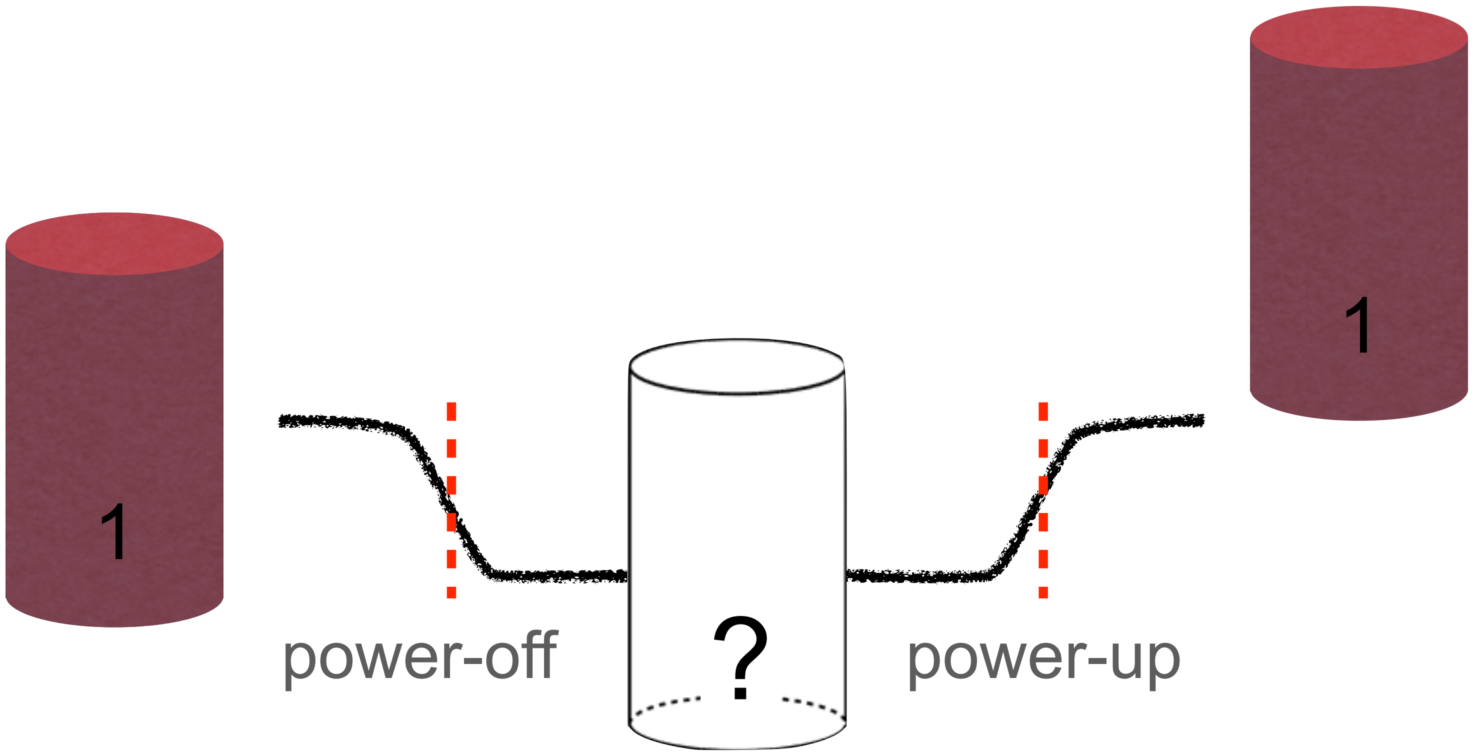
NMOS Transistors

GND

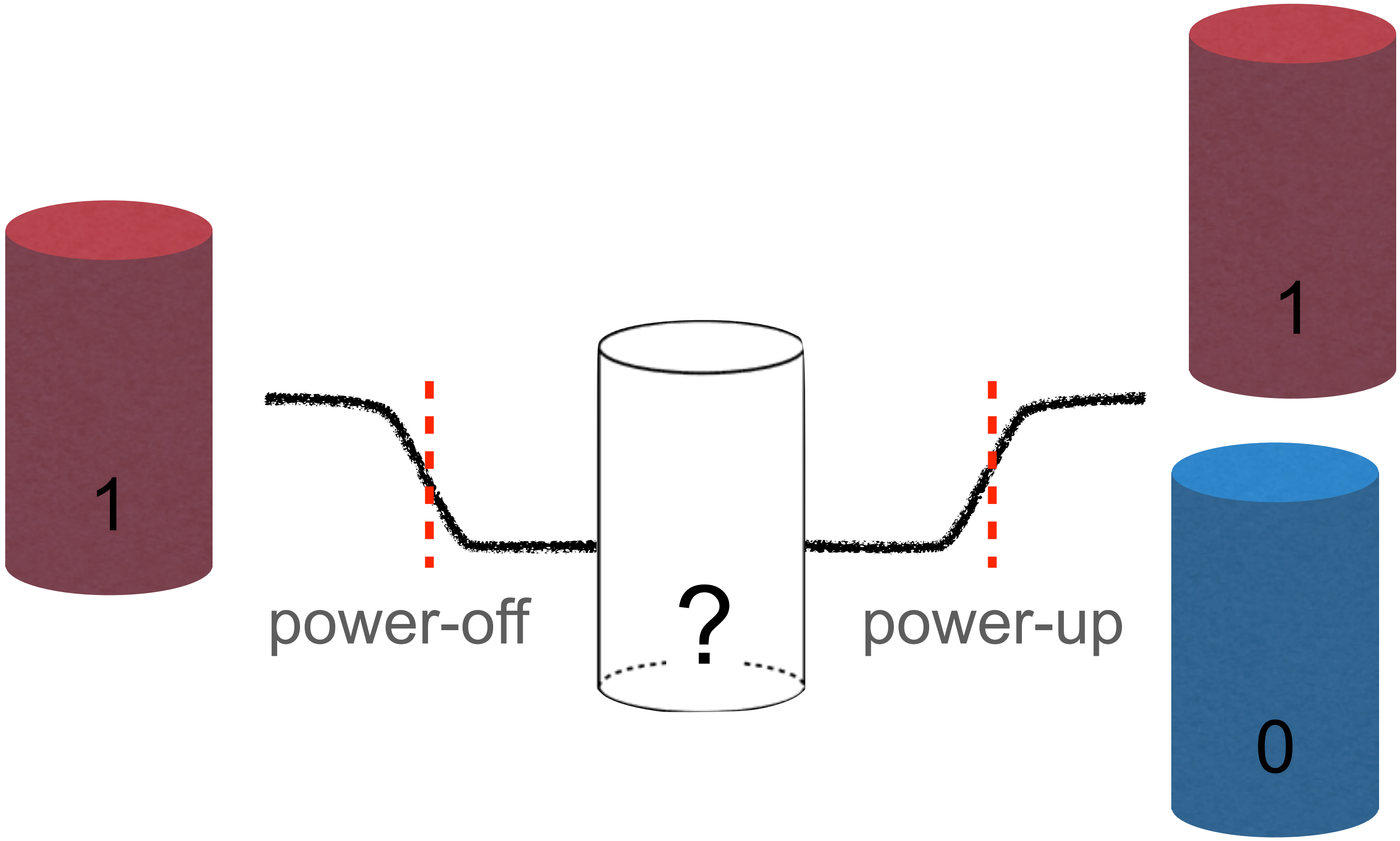
SRAM Remanence



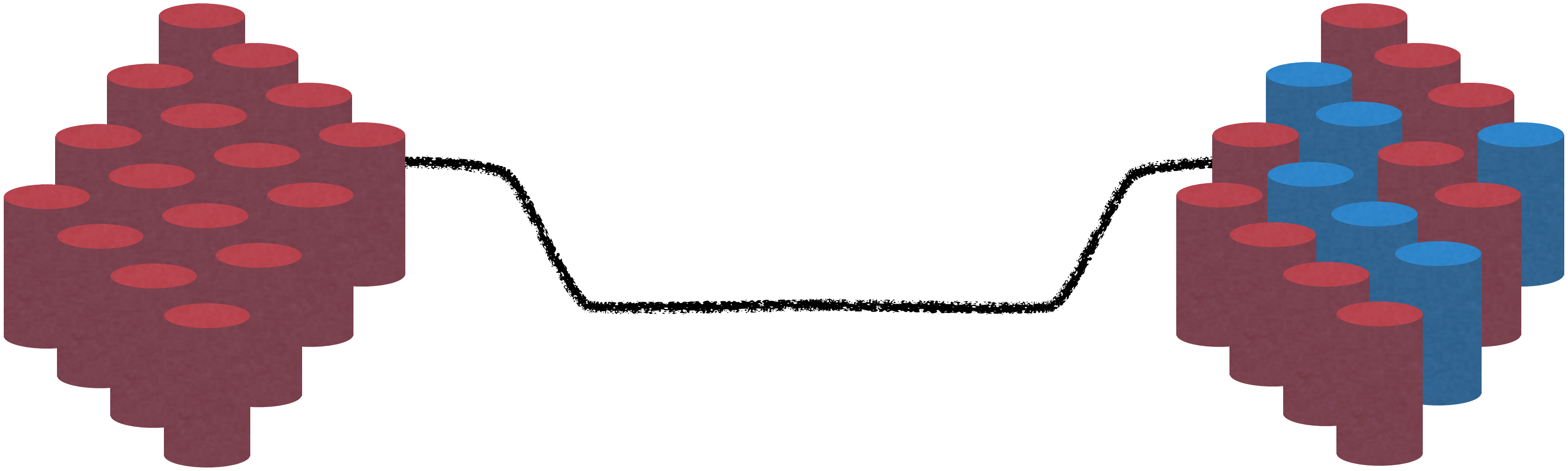
SRAM Remanence



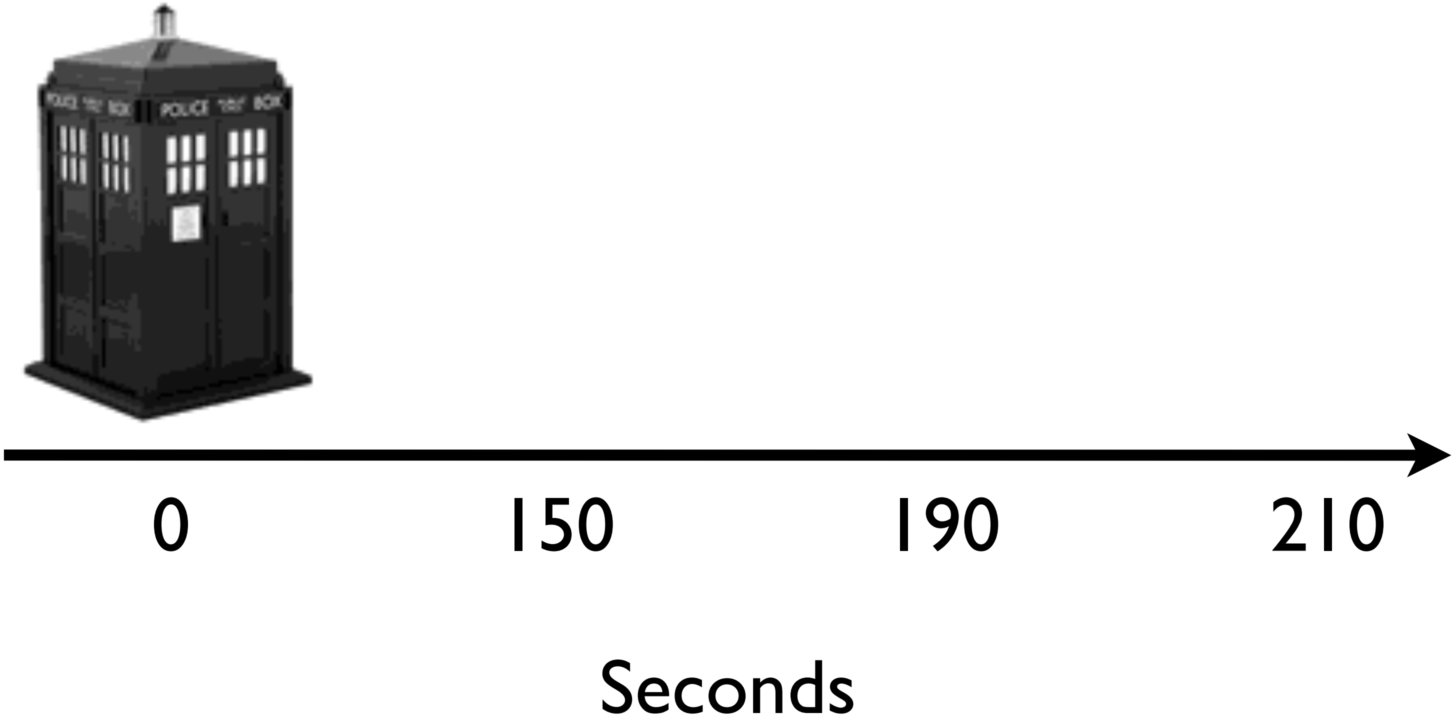
SRAM Remanence



SRAM Remanence



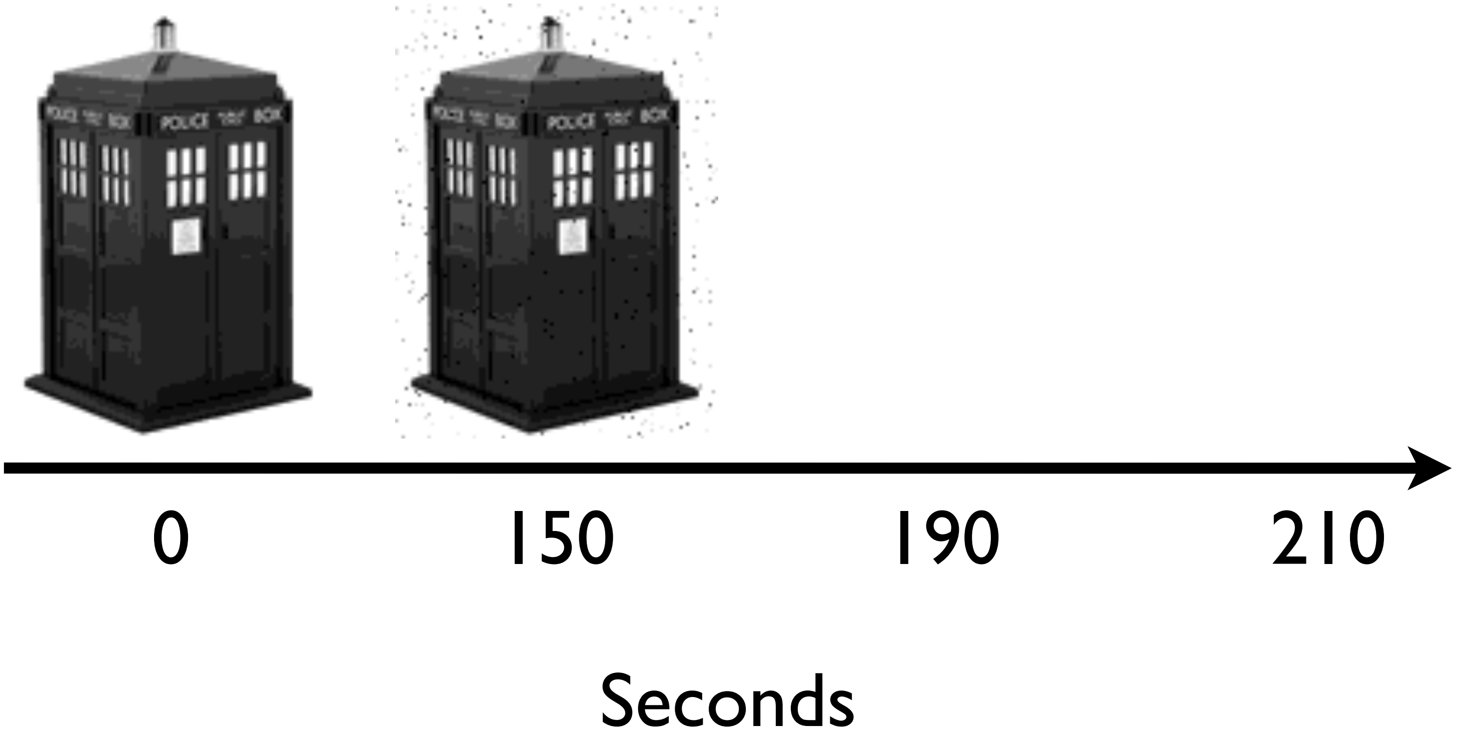
SRAM Remanence



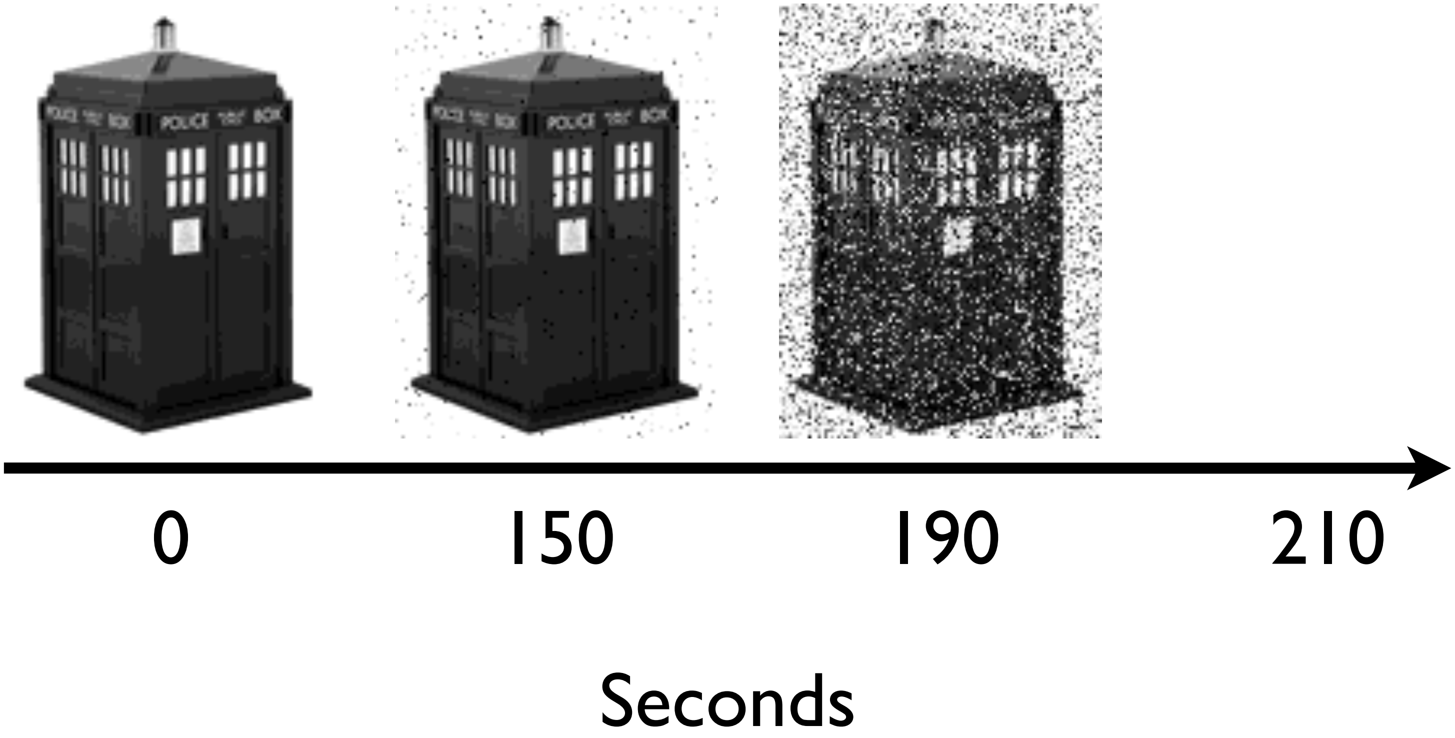
0 150 190 210

Seconds

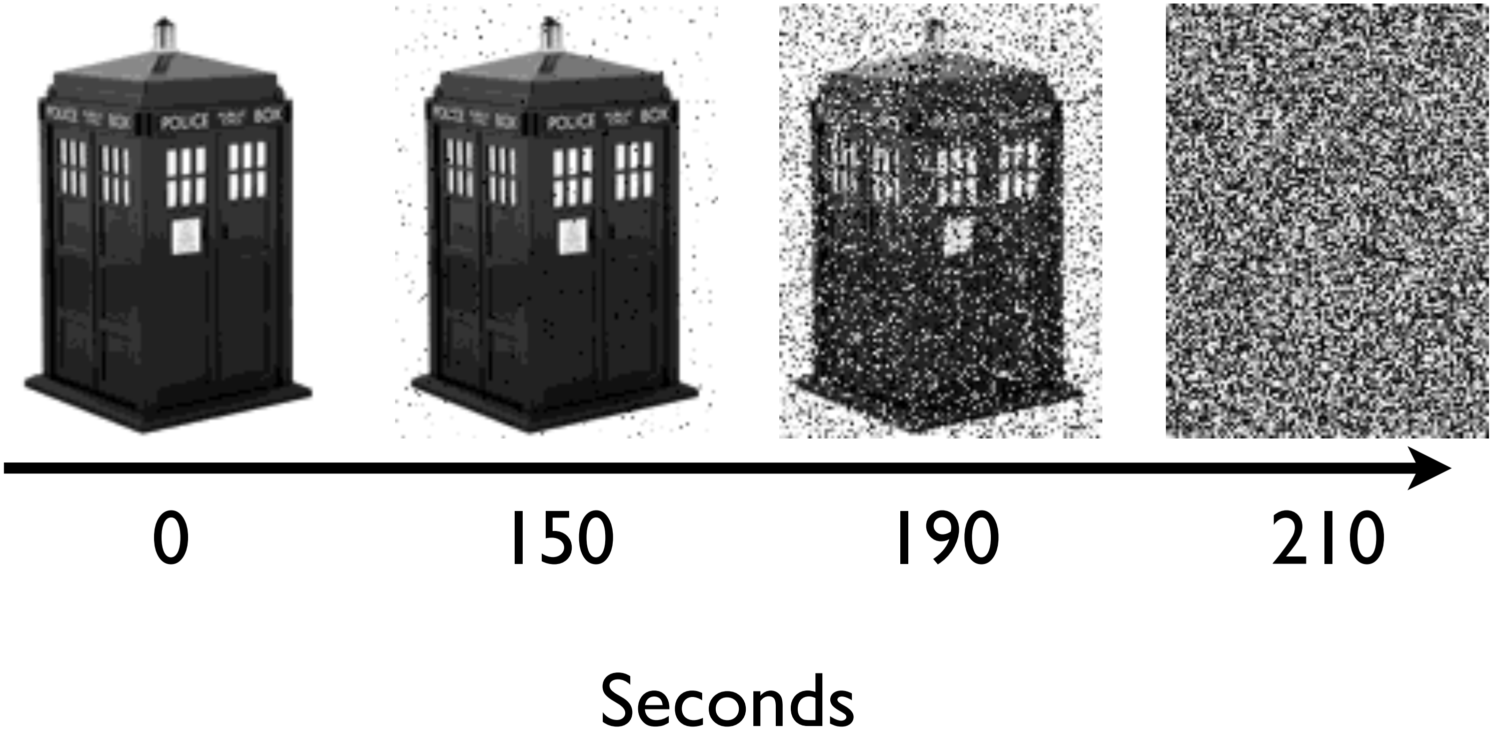
SRAM Remanence



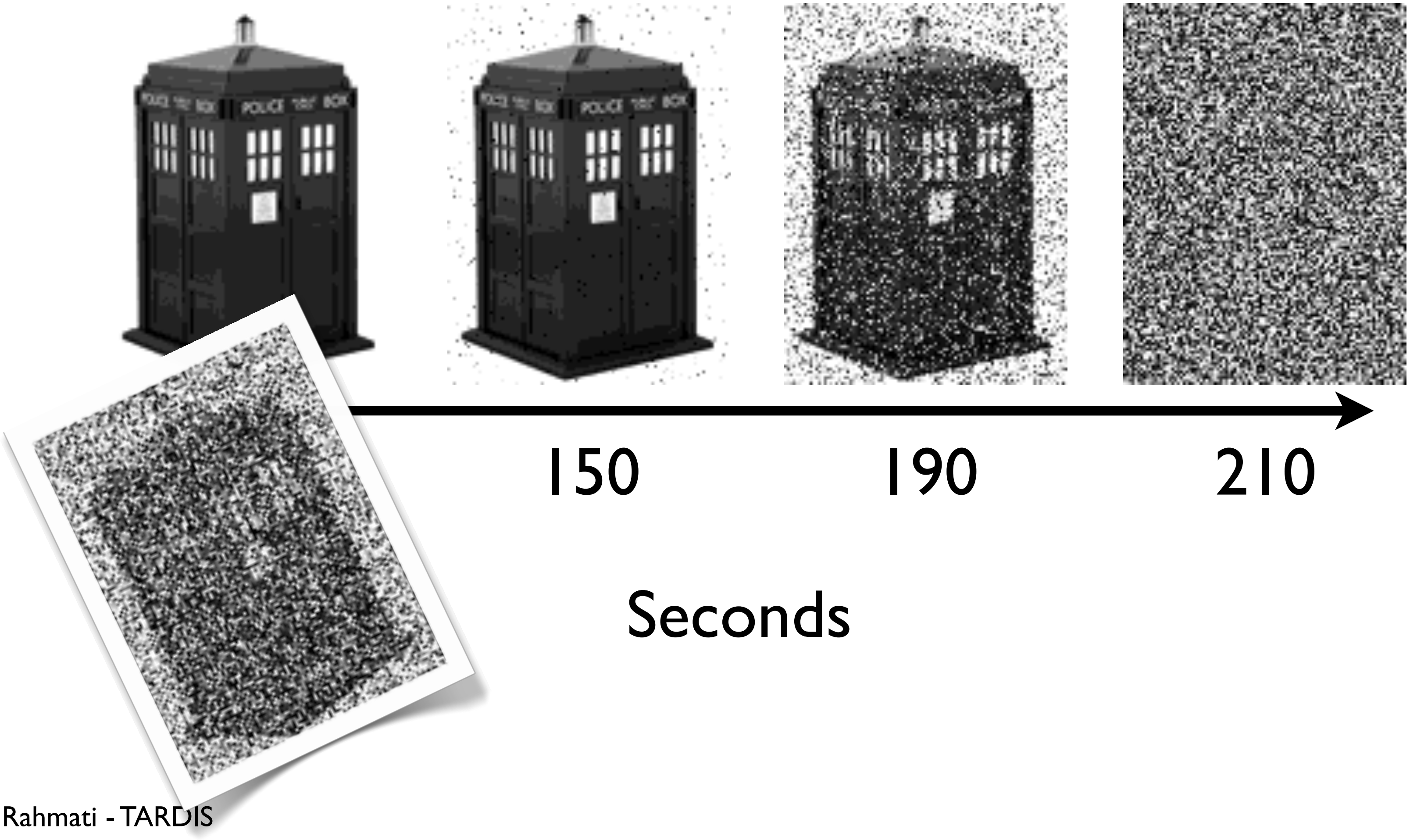
SRAM Remanence



SRAM Remanence



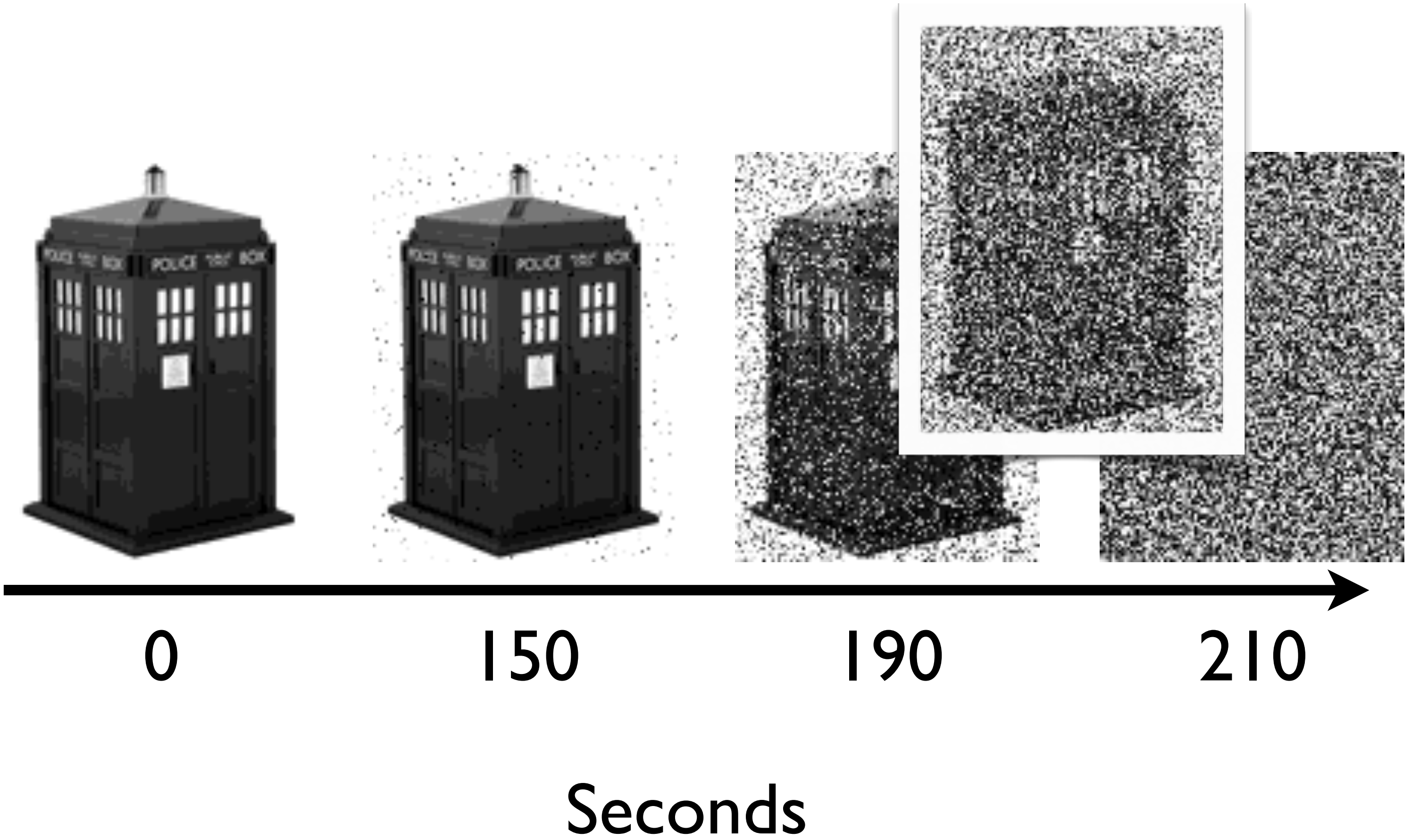
SRAM Remanence



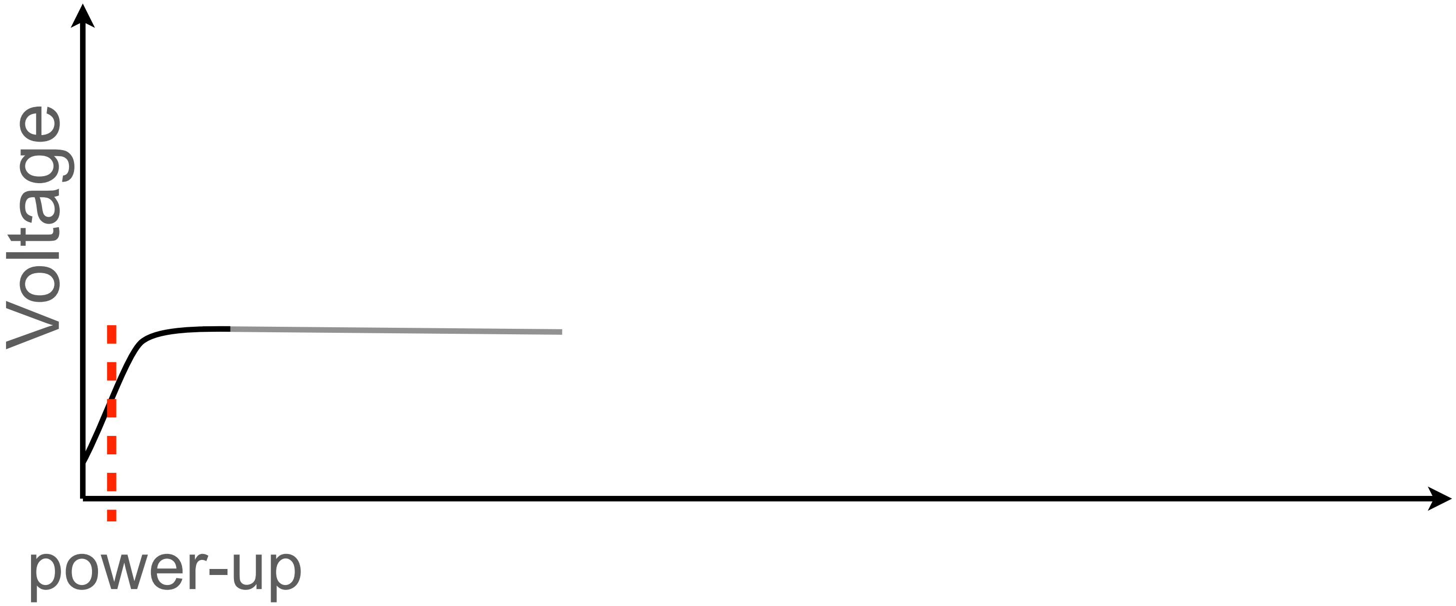
150 190 210

Seconds

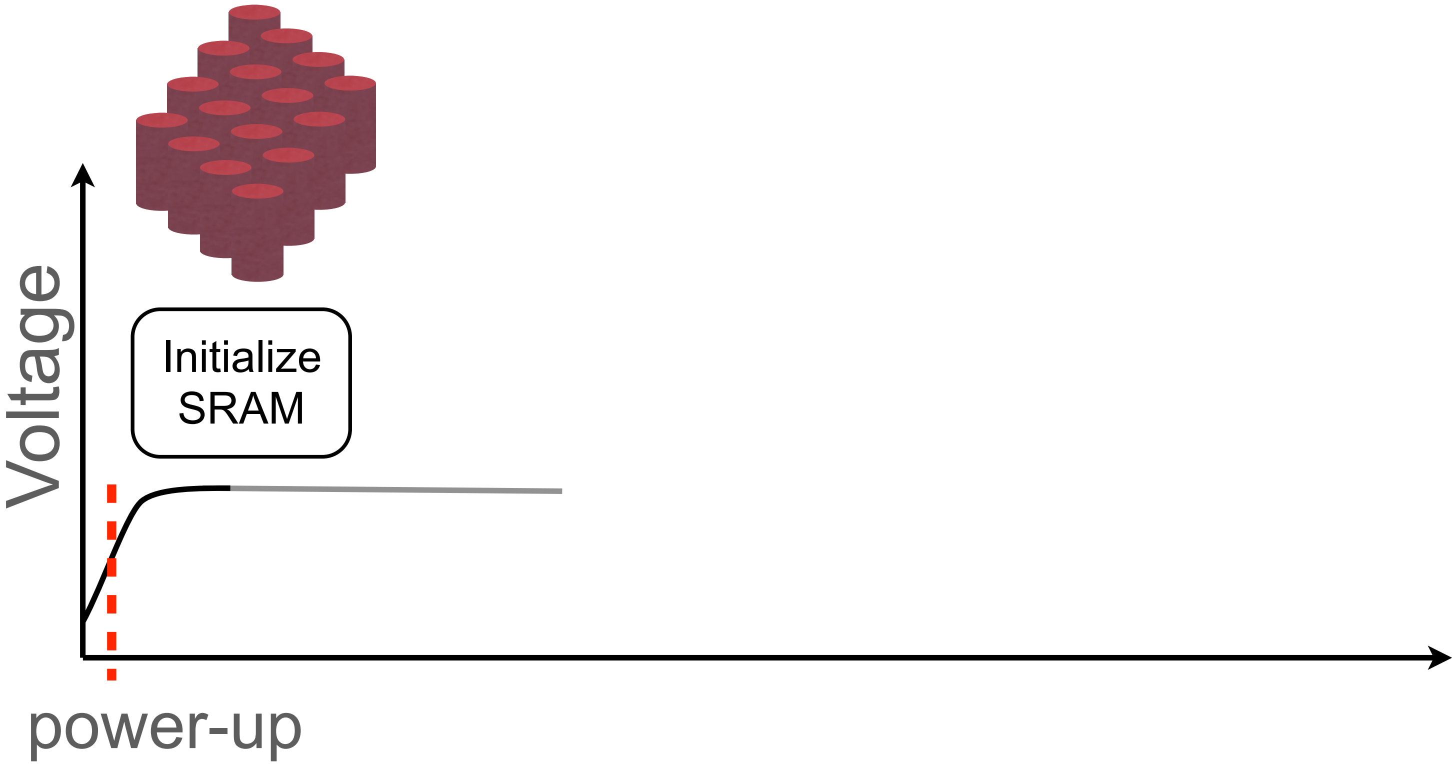
SRAM Remanence



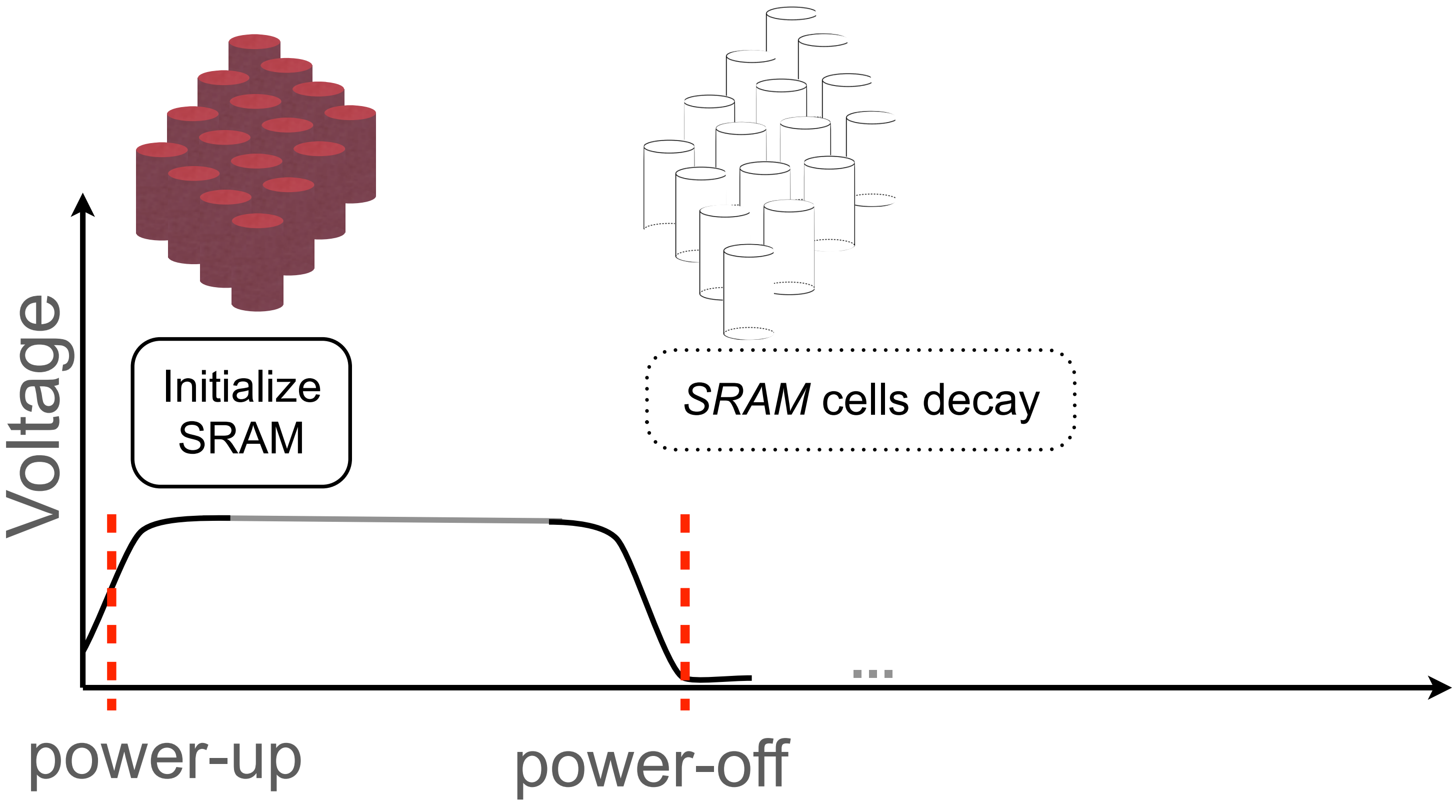
The TARDIS Algorithm



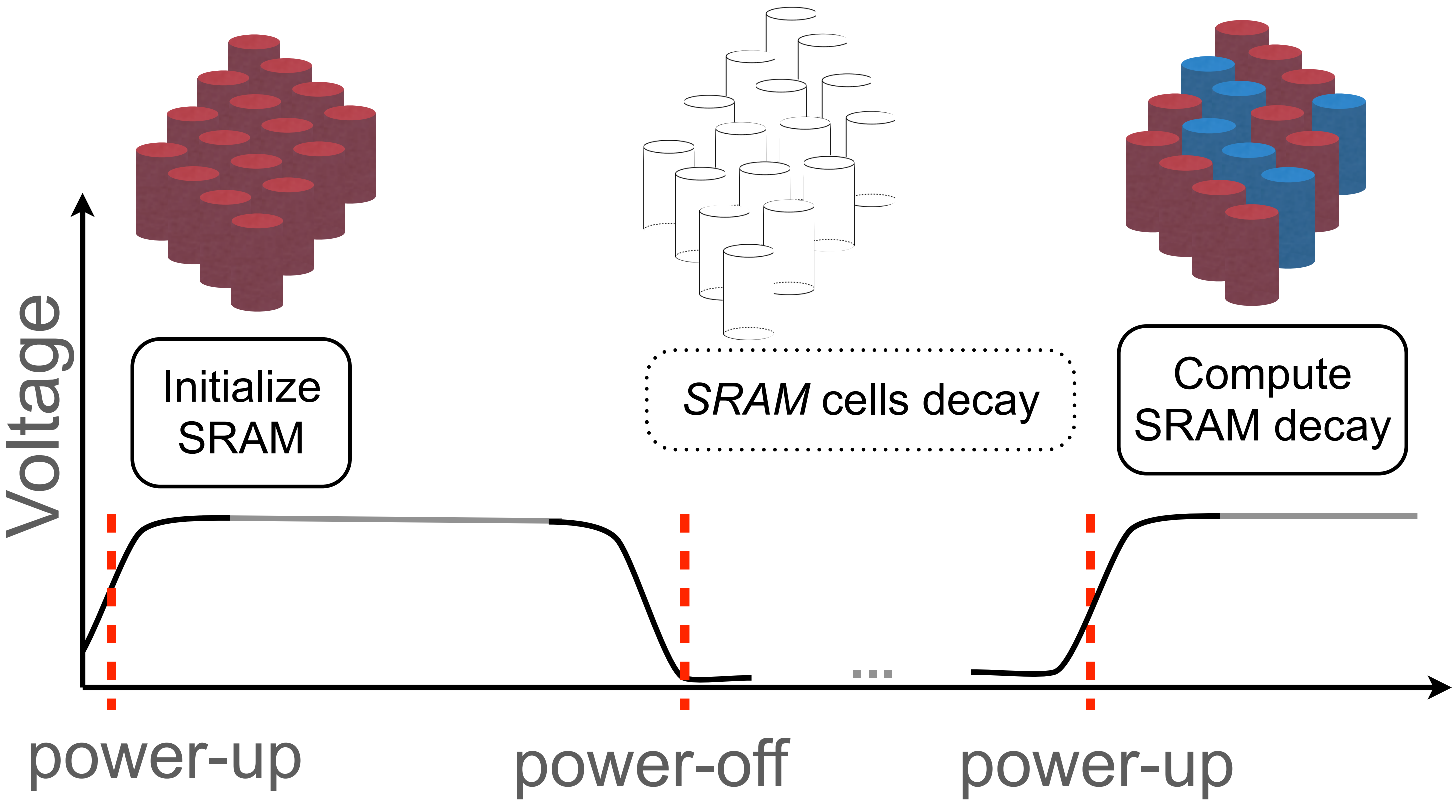
The TARDIS Algorithm



The TARDIS Algorithm



The TARDIS Algorithm



Initialize SRAM

SRAM cells decay

Compute SRAM decay

Voltage

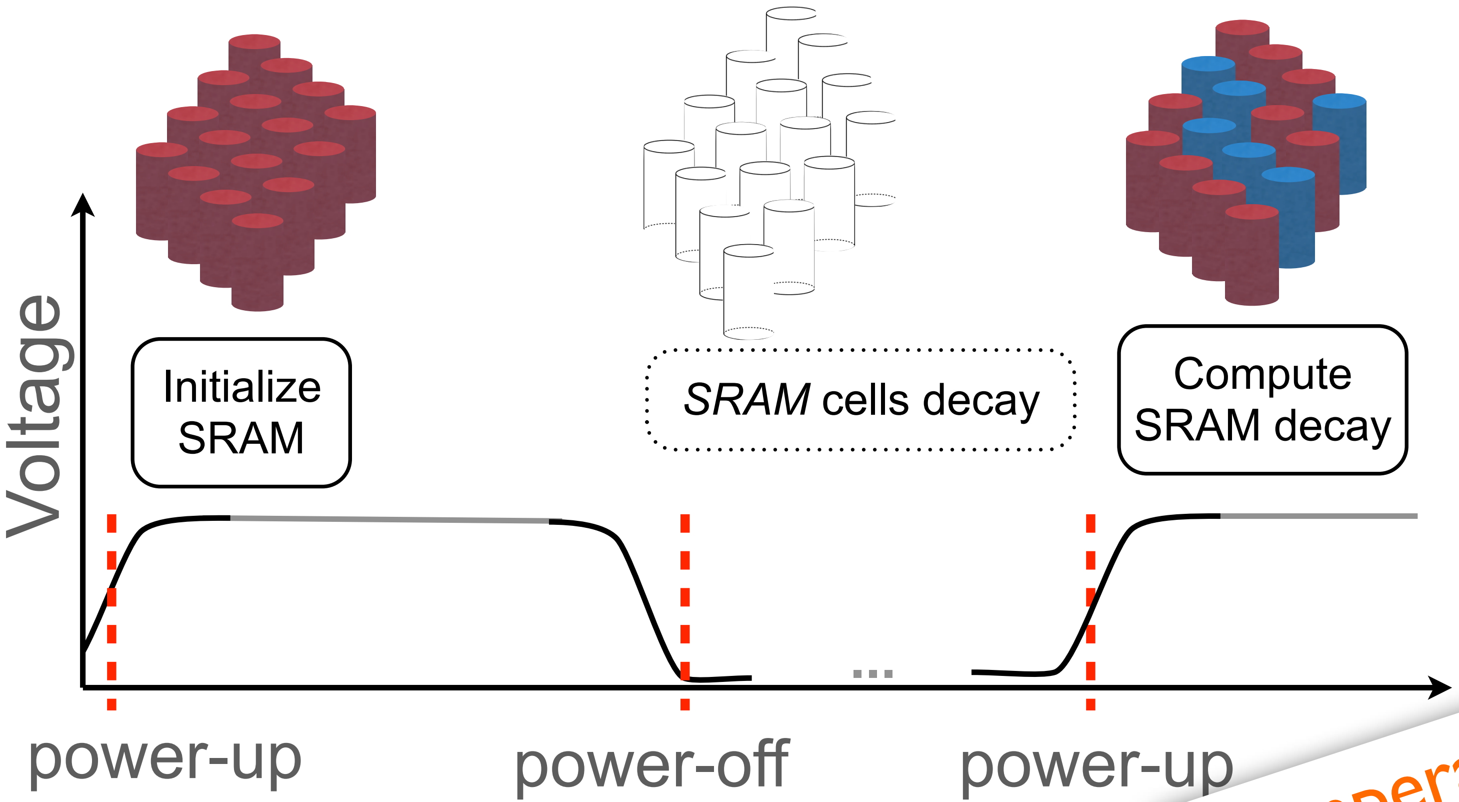
power-up

power-off

...

power-up

The TARDIS Algorithm



Temperature Later...

Factors Influencing SRAM Decay

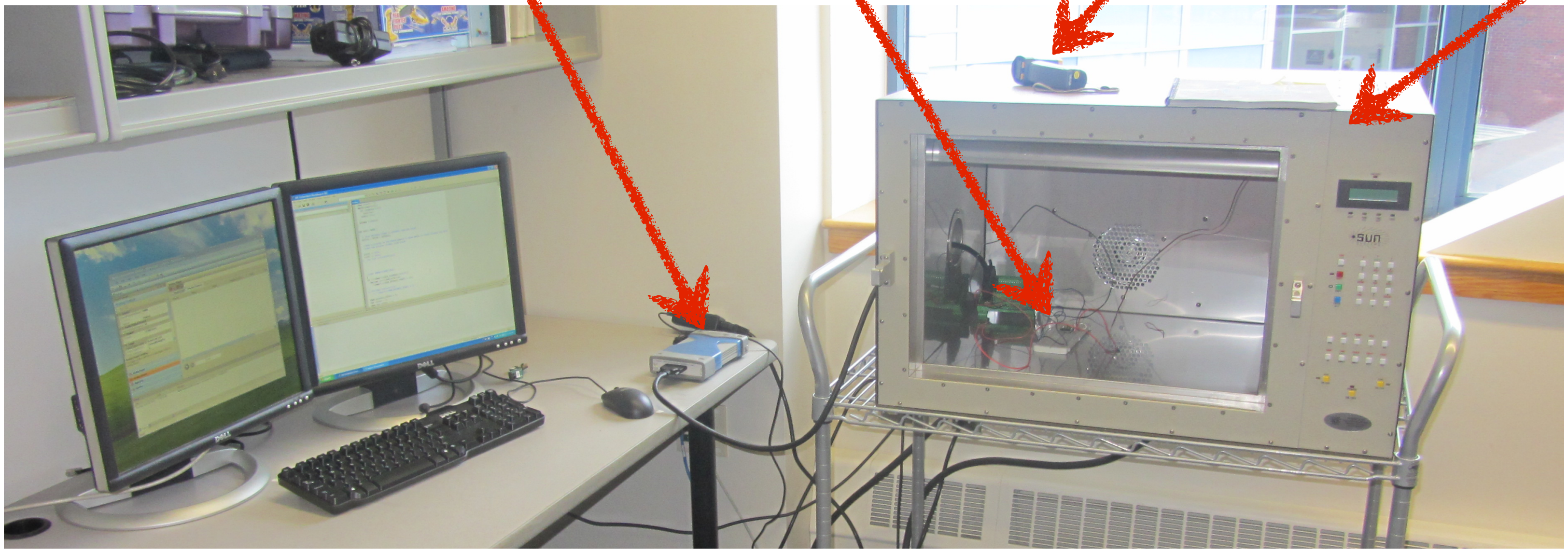
✓ SRAM Size

✓ Circuit Capacitance

✓ Temperature

✗ Chip Variation

Experimental Setup

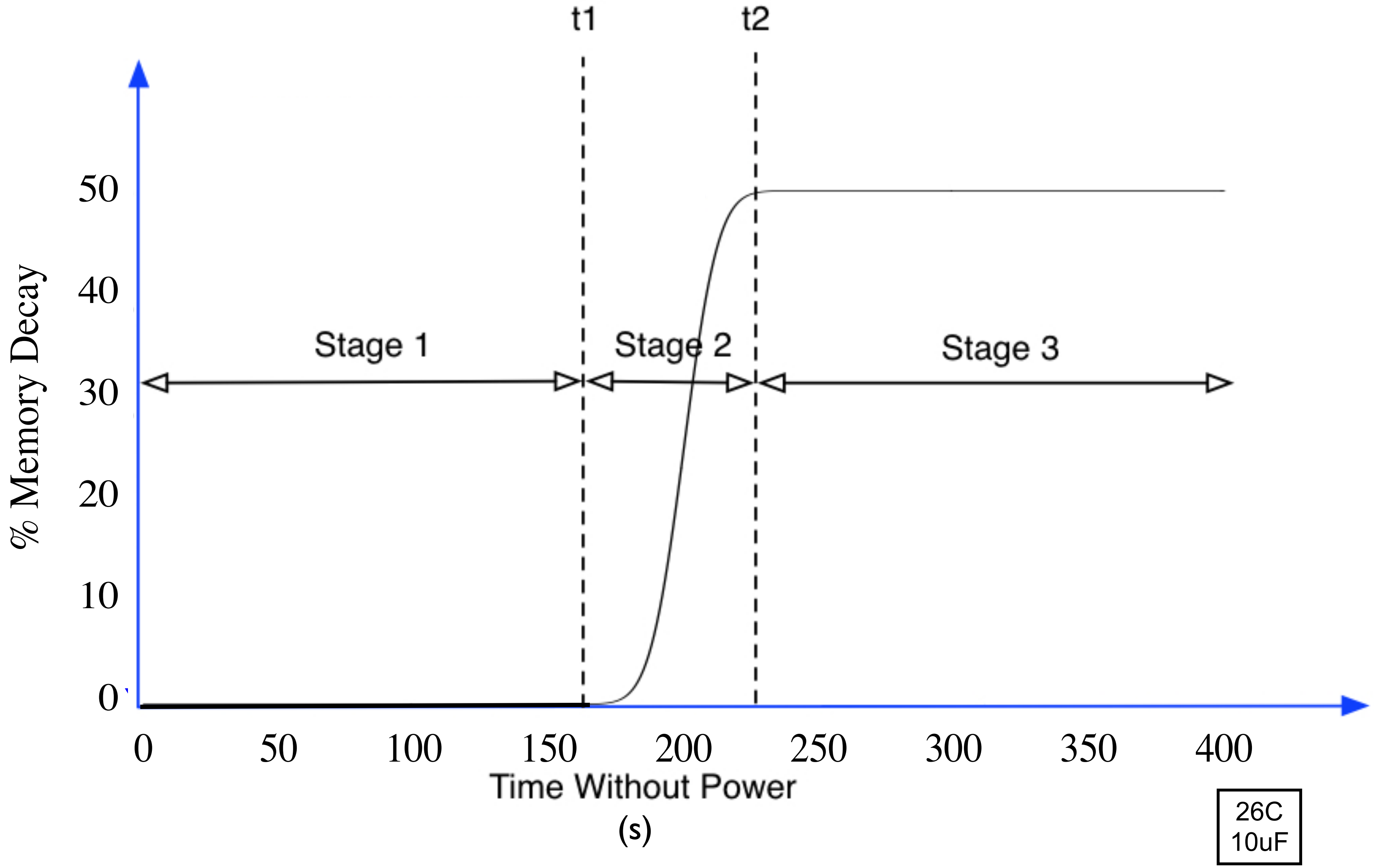


DAQ

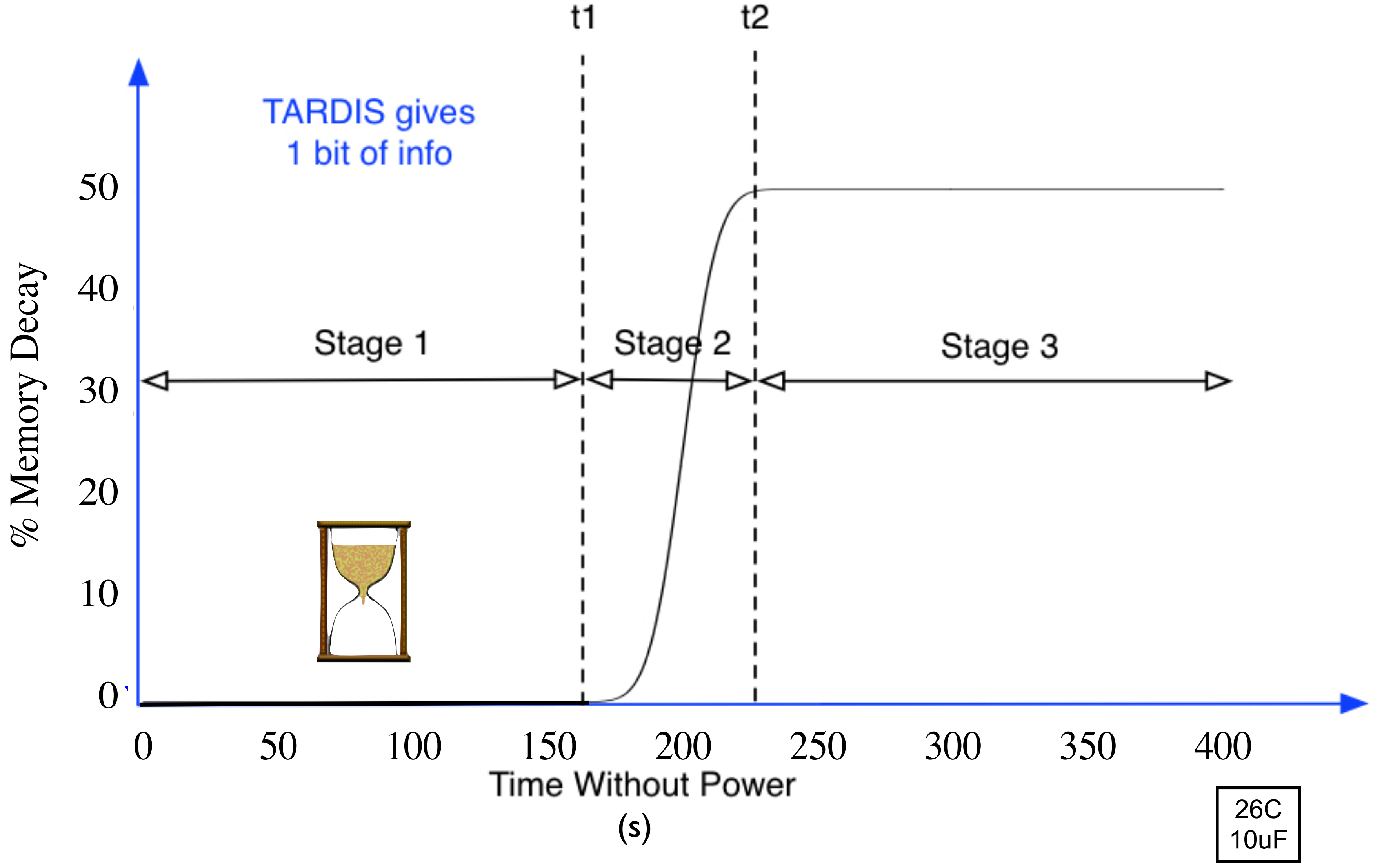
TI MSP430

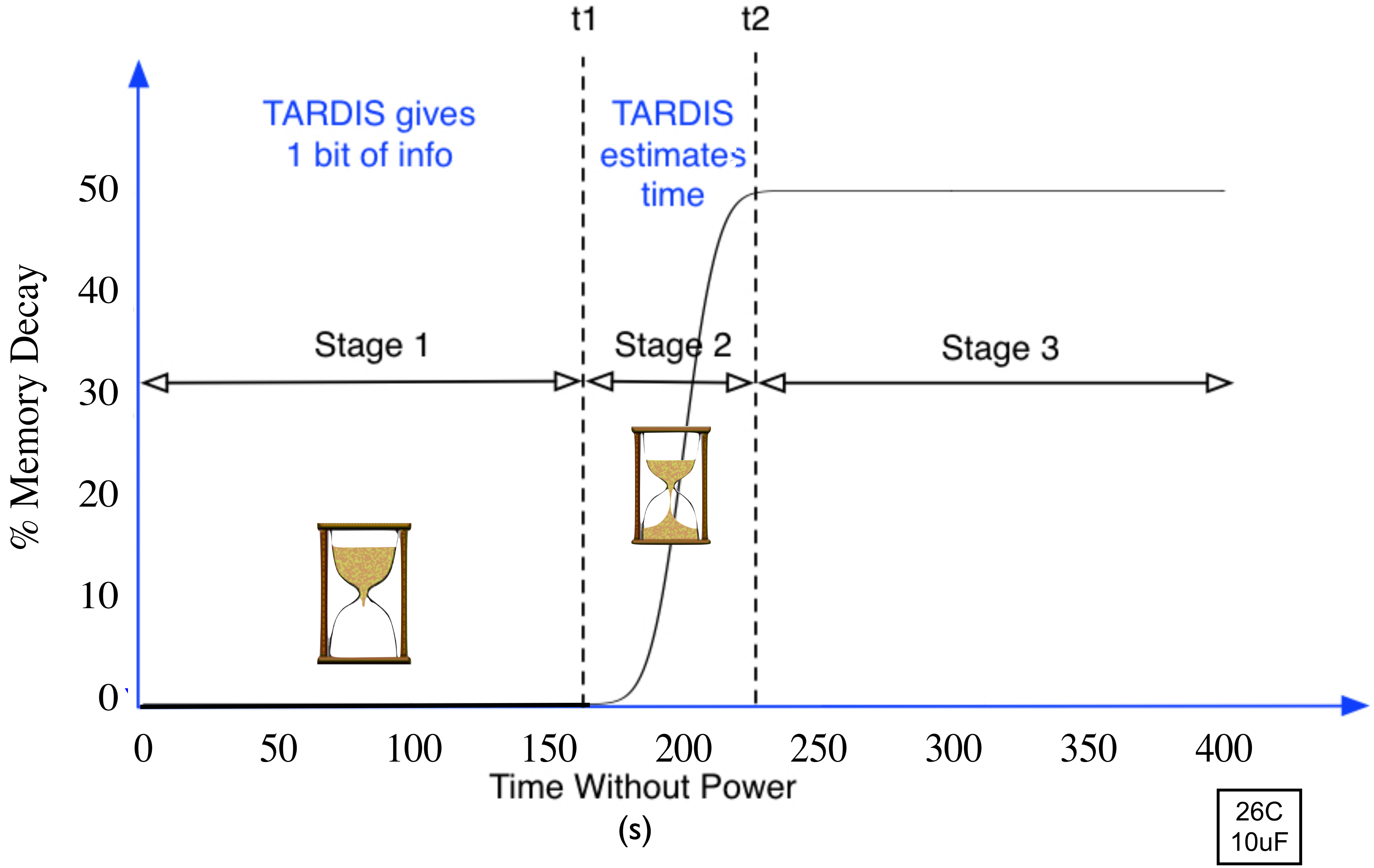
Thermometer

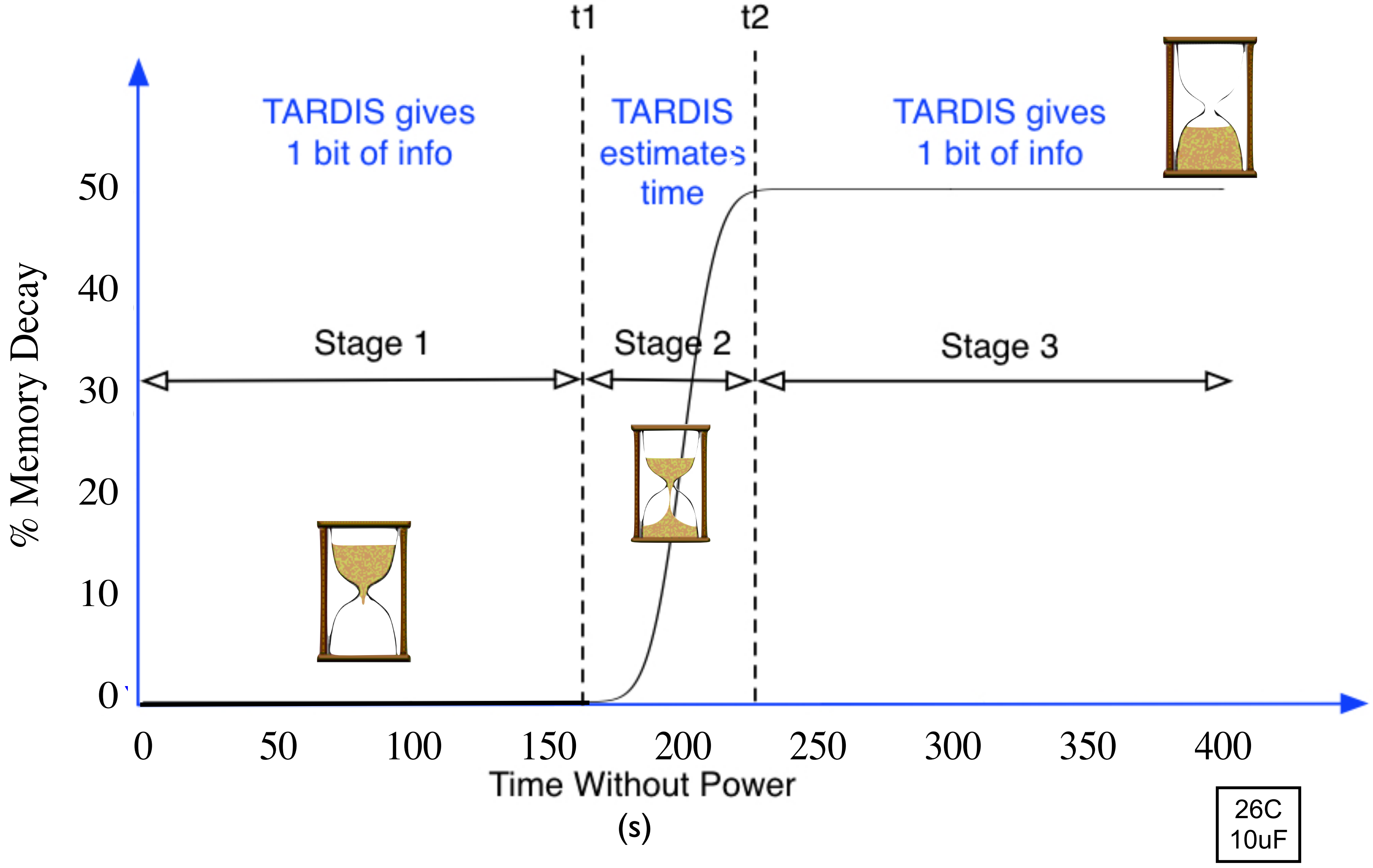
Thermal Chamber


t1
t2
% Memory Decay
50
40
30
20
10
0
Stage 1
Stage 2
Stage 3
0
50
100
150
200
250
300
350
400
Time Without Power
(s)

26C
10uF

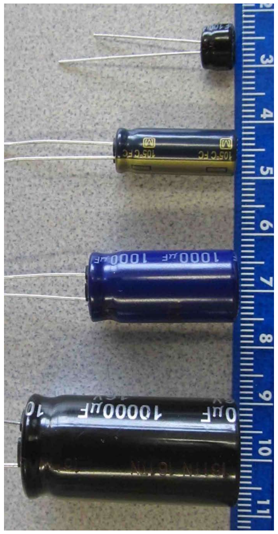

t1
t2
TARDIS gives
1 bit of info
50
40
30
20
10
0
% Memory Decay
Stage 1
Stage 2
Stage 3
0
50
100
150
200
250
300
350
400
Time Without Power
(s)
26C
10uF


t1
t2
TARDIS gives
1 bit of info
TARDIS
estimates
time
50
40
30
20
10
0
% Memory Decay
Stage 1
Stage 2
Stage 3
0
50
100
150
200
250
300
350
400
Time Without Power
(s)
26C
10uF

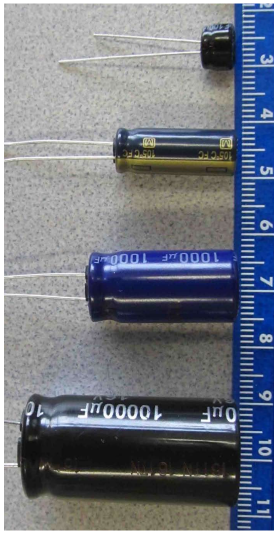

t1
t2
TARDIS gives 1 bit of info
TARDIS estimates time
TARDIS gives 1 bit of info
Stage 1
Stage 2
Stage 3
% Memory Decay
0
10
20
30
40
50
0
50
100
150
200
250
300
350
400
Time Without Power (s)
26C
10uF

Circuit Capacitnce

Capacitor Size	Expiration time	Scale
~0µF	2.1x10^{0}s	Seconds
10µF	2.25x10^{2}s	Minutes
100µF	1.98x10^{3}s	1/2 Hour
1000µF	2.12x10^{4}s	Hours
10000µF	>1.96x10^{5}s	Days



Circuit Capacitnce

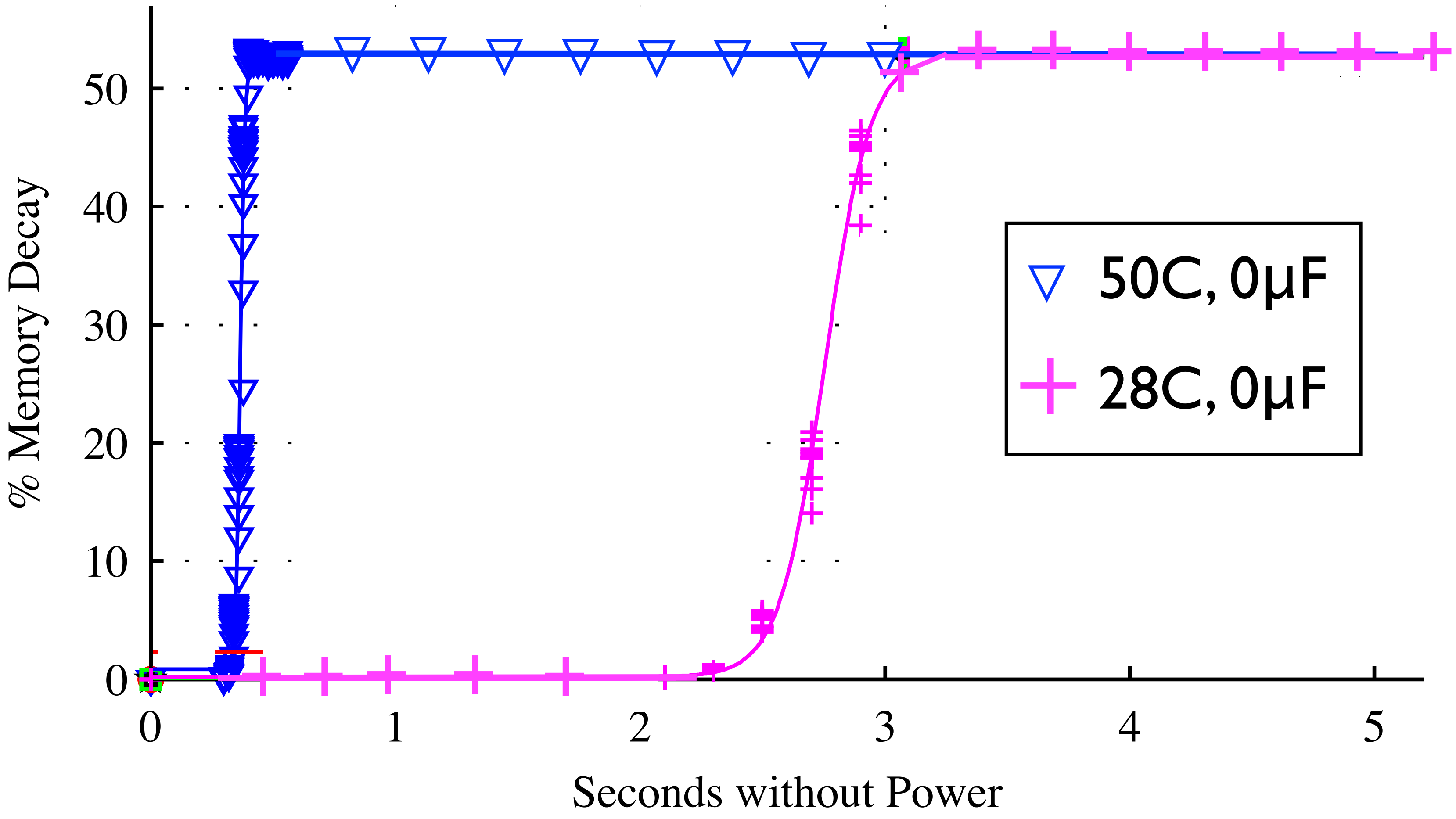


Capacitor Size	Expiration time	Scale
~0µF	$2.1x10^0s$	Seconds
10µF	$2.25x10^2s$	Minutes
100µF	$1.98x10^3s$	1/2 Hour
1000µF	$2.12x10^4s$	Hours
10000µF	$>1.96x10^5s$	Days

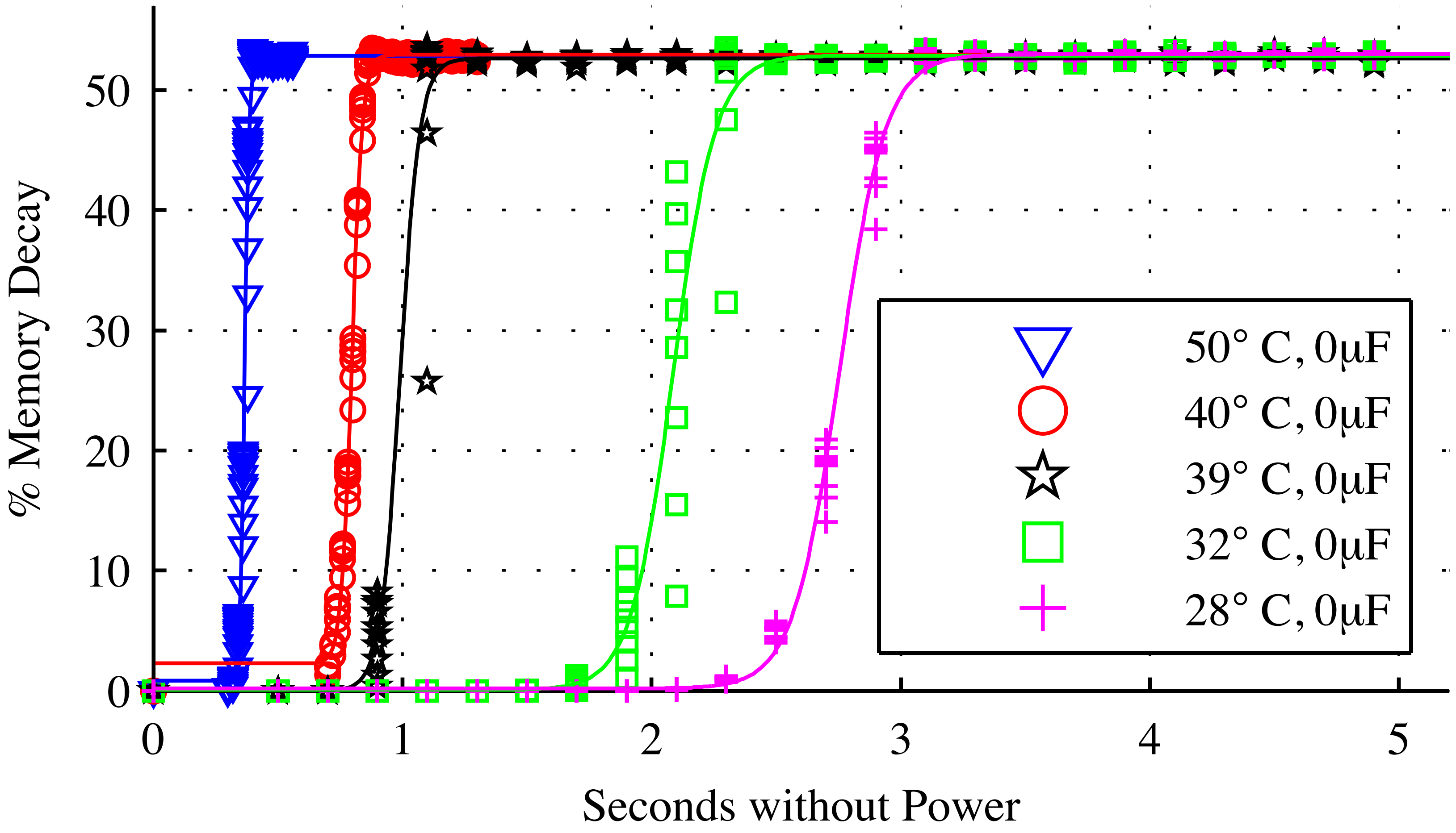
Smart Cards

Batteryless Sensor = 100,000µF

Temperature

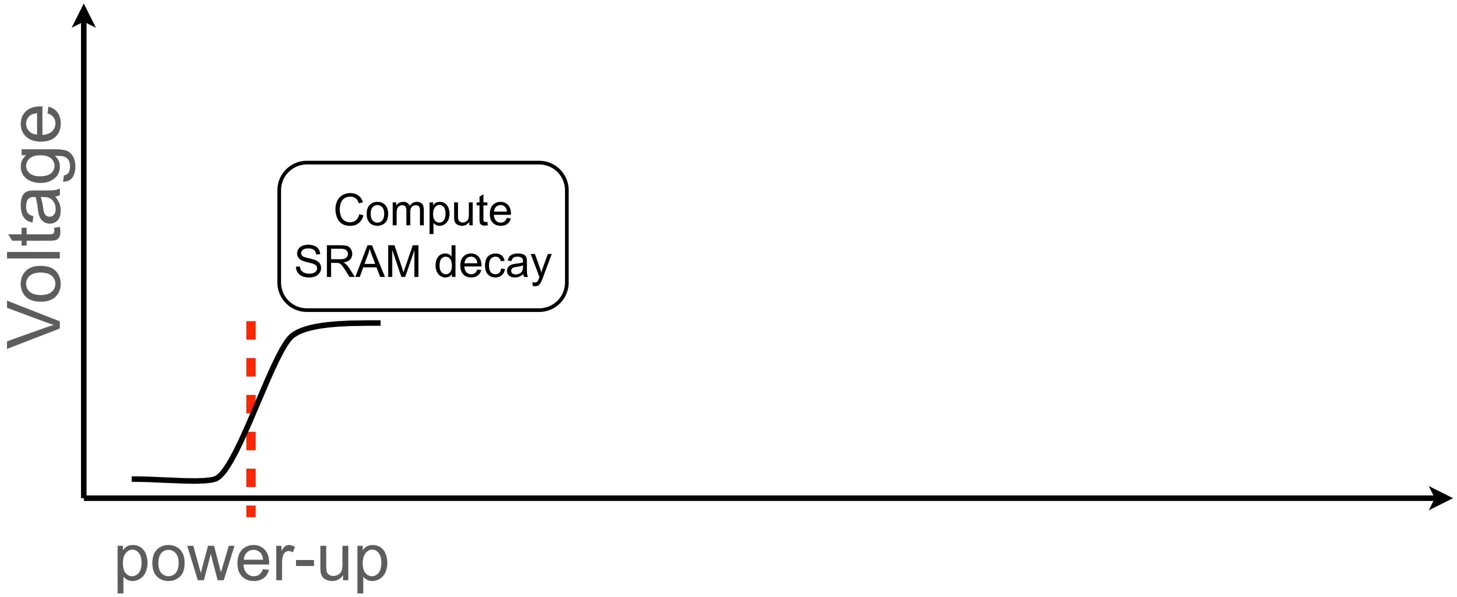


Temperature

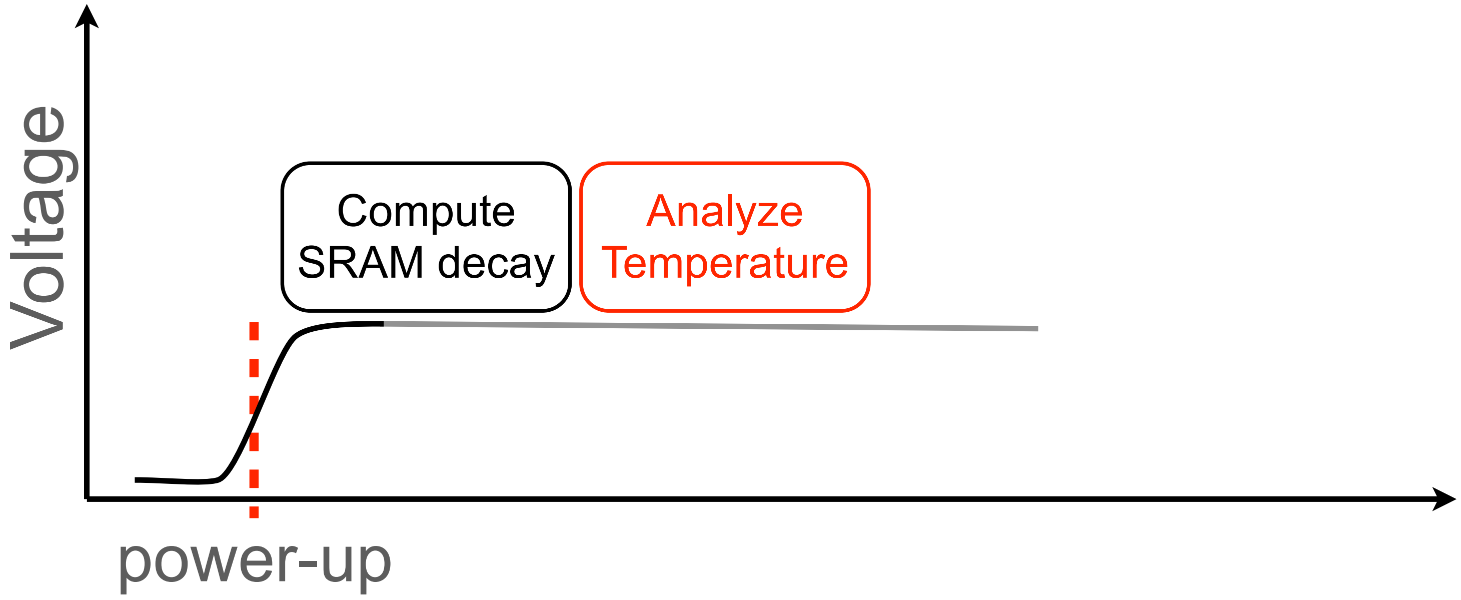


Compensate for Temperature

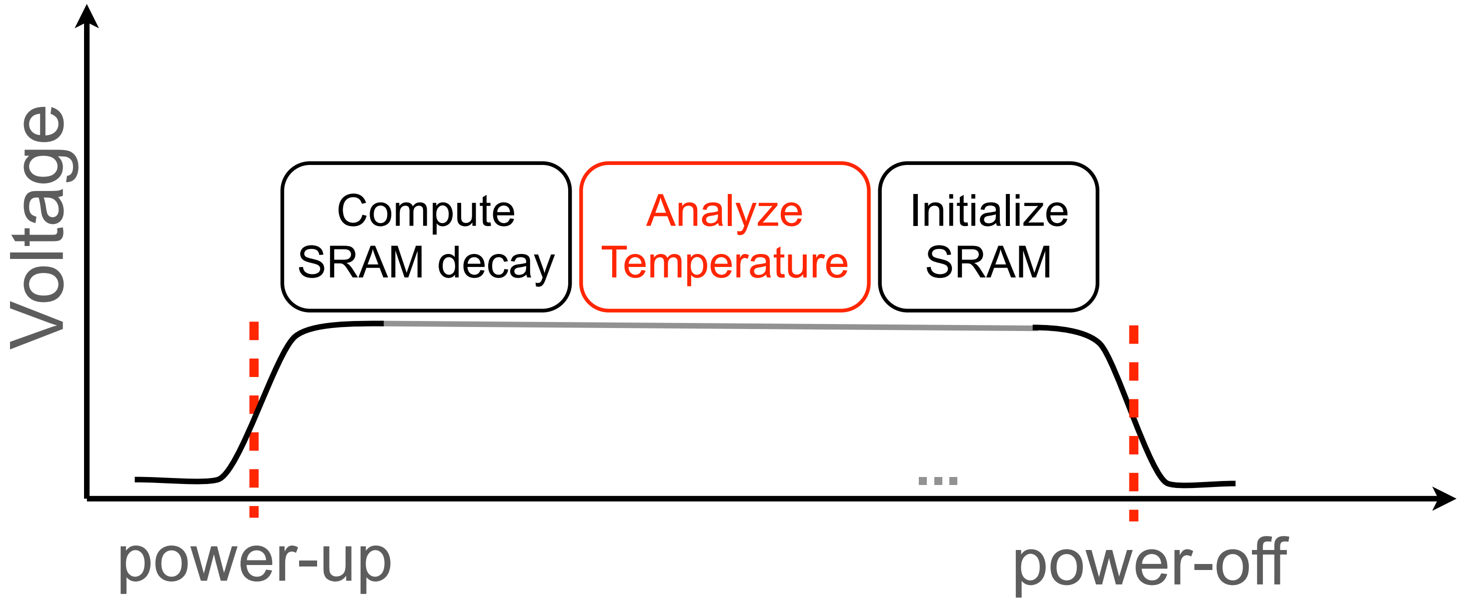
Compensate for Temperature



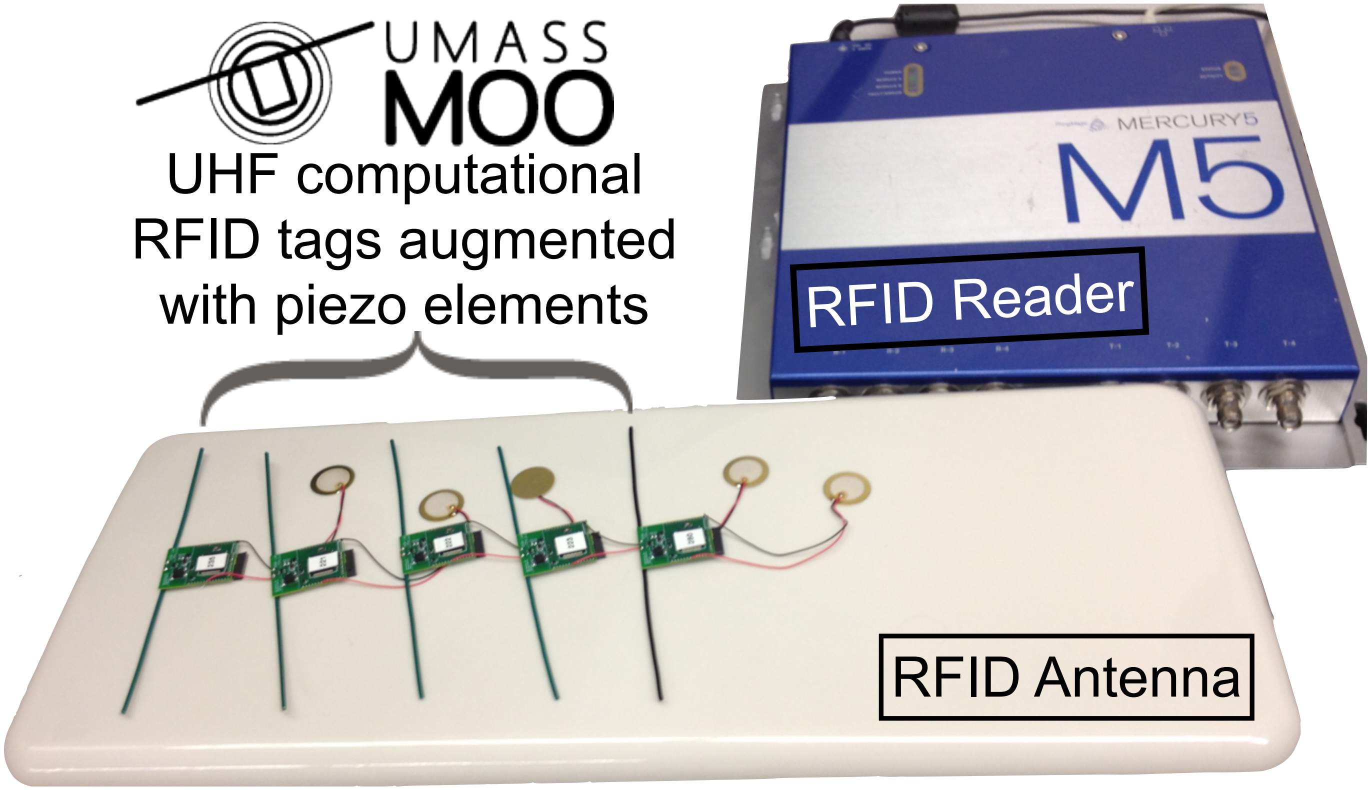
Compensate for Temperature



Compensate for Temperature

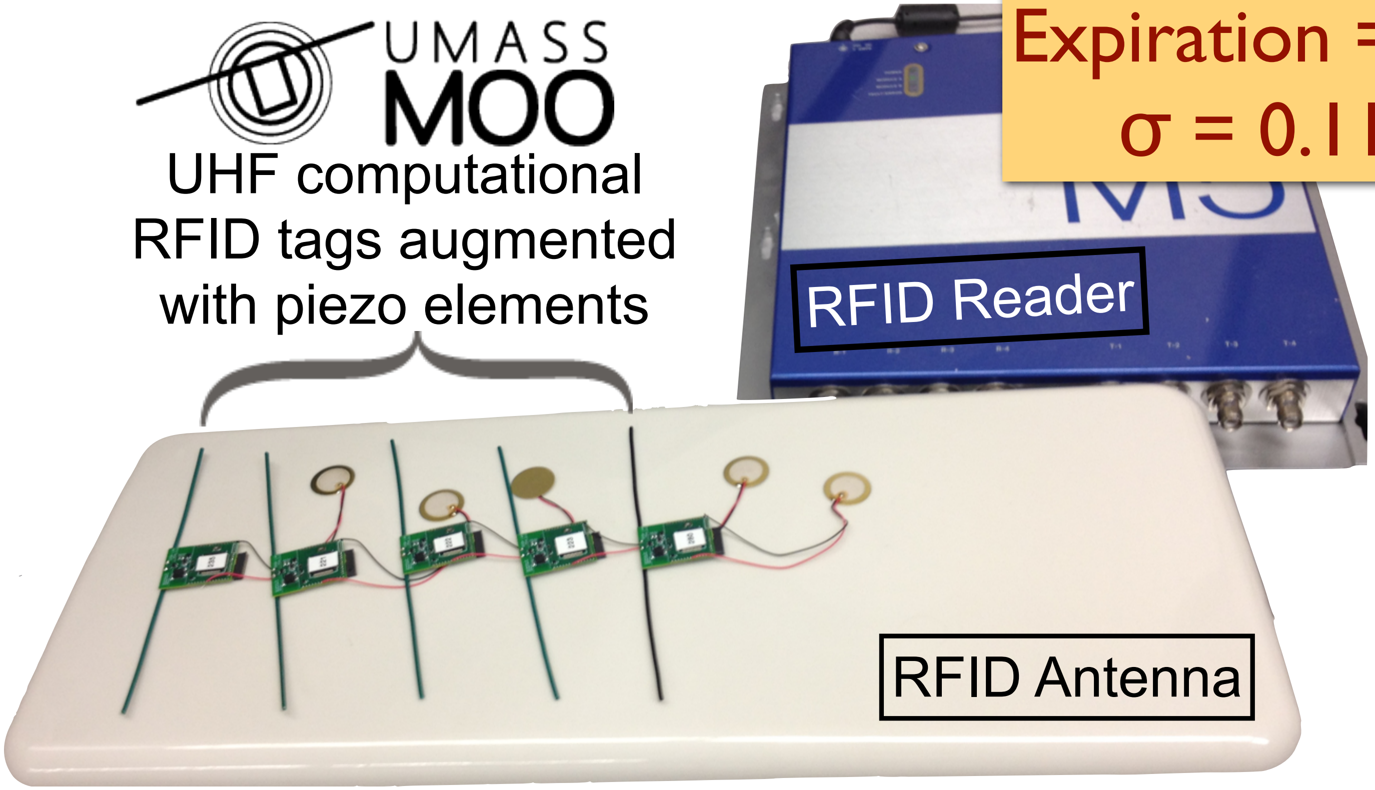


Implementation



UHF computational RFID tags augmented with piezo elements

Implementation



UMASS MOO

UHF computational RFID tags augmented with piezo elements

RFID Reader

RFID Antenna

Expiration = 12s

σ = 0.11s

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

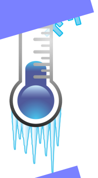
- Heating

Thermal Sensor

Attacking the TARDIS

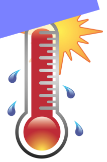
- Cooling

Thermal Sensor

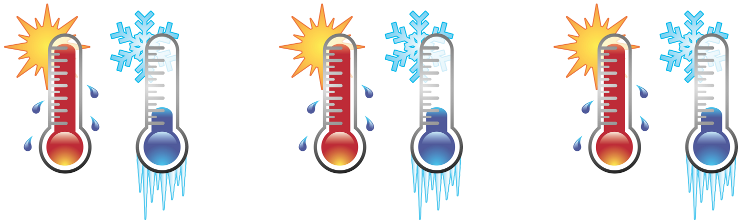


- Heating

Thermal Sensor



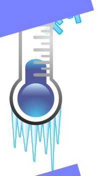
- Pulse



Attacking the TARDIS

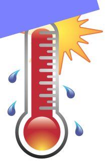
- Cooling

Thermal Sensor

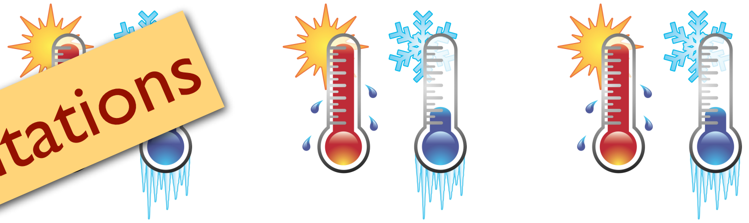


- Heating

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

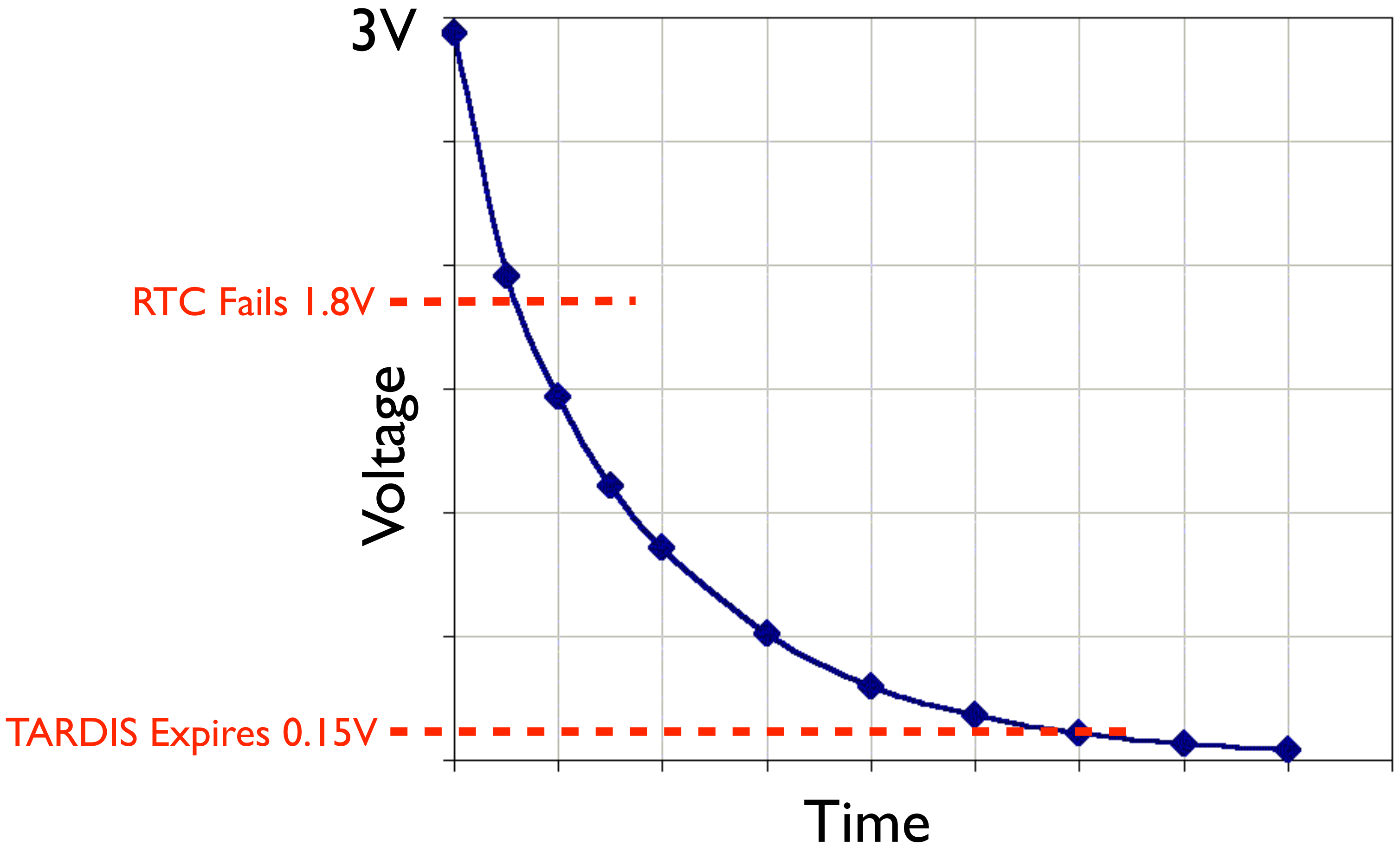
- uses memory decay to estimate time.
- makes brute force attacks orders of magnitude harder.
- is just software.
- uses remanence decay for good.

Photo Credit: thinkgeek.com

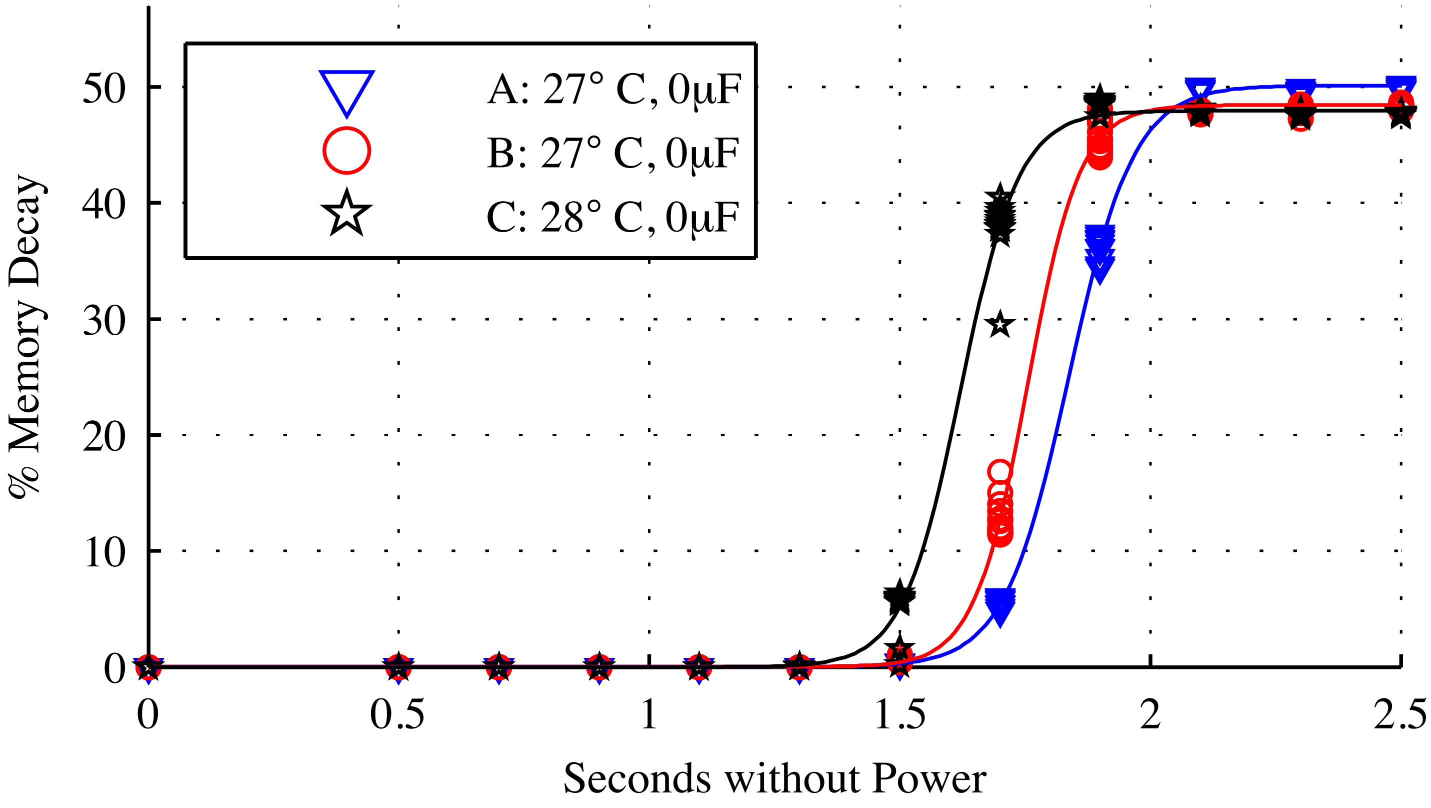
SPQR
LABORATORY

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

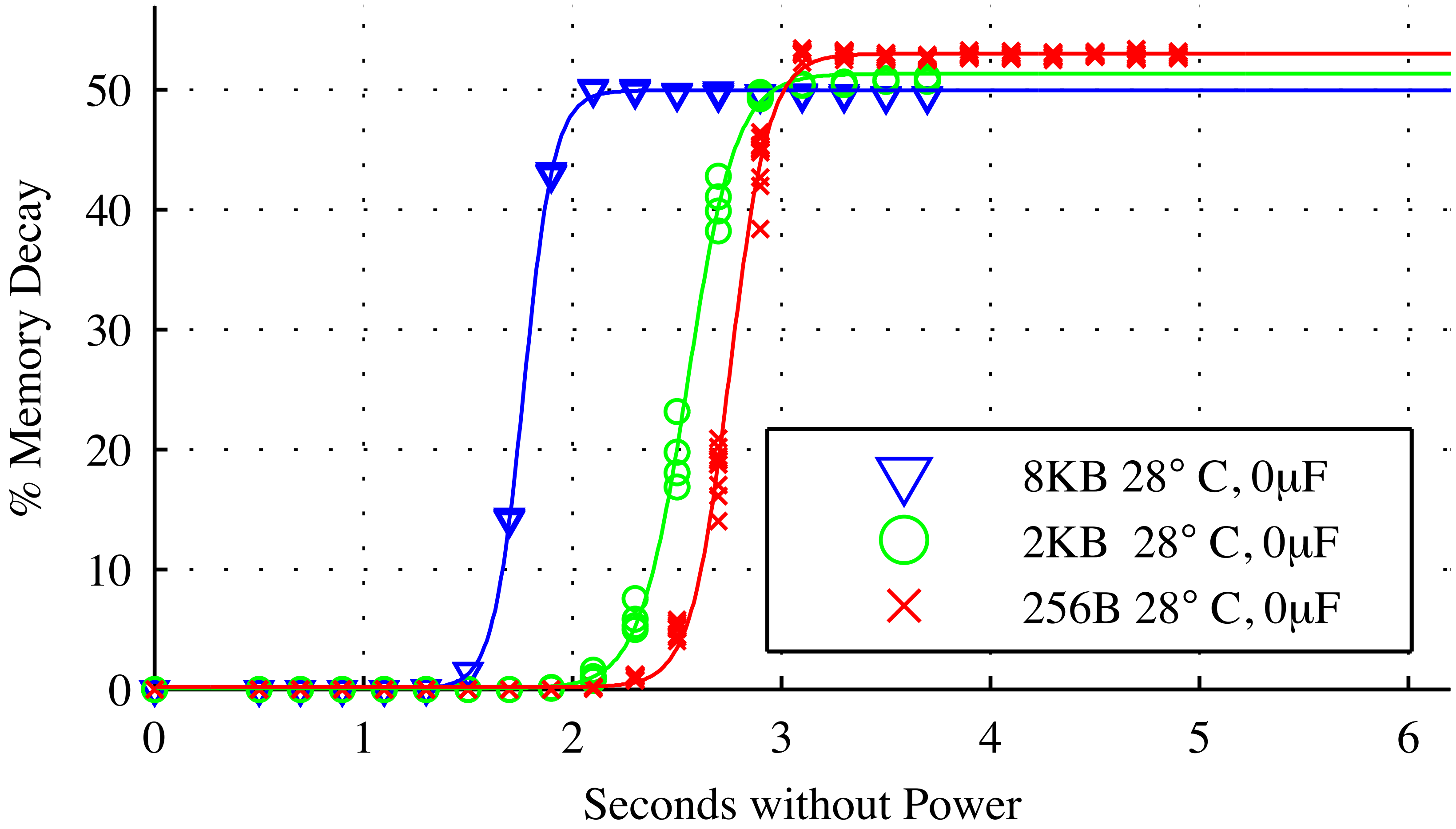
Capacitor Depletion



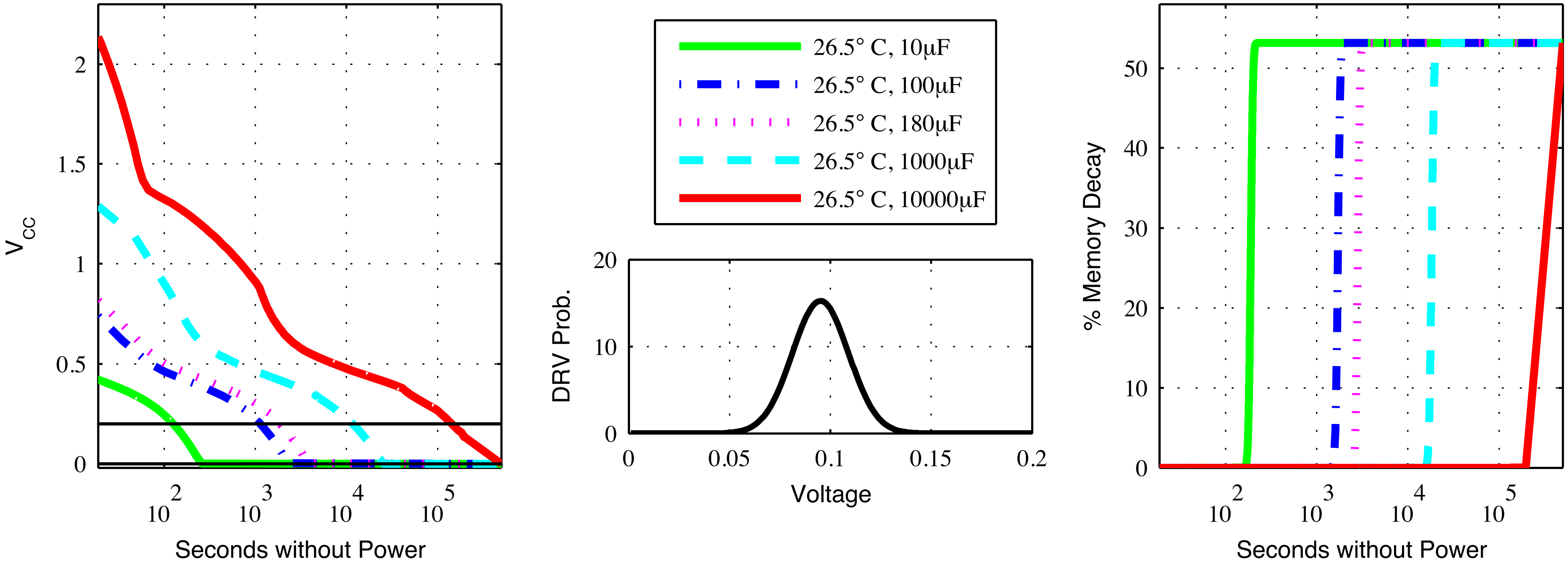
Chip Variation



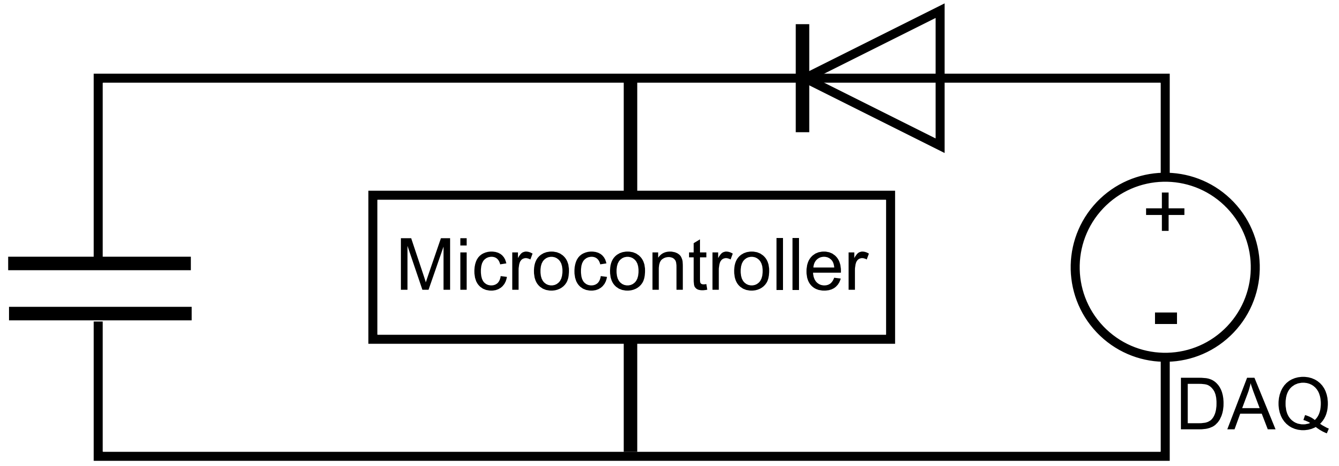
SRAM Size


% Memory Decay
0
10
20
30
40
50
0
1
2
3
4
5
6
Seconds without Power
▽ 8KB 28° C, 0μF
○ 2KB 28° C, 0μF
× 256B 28° C, 0μF

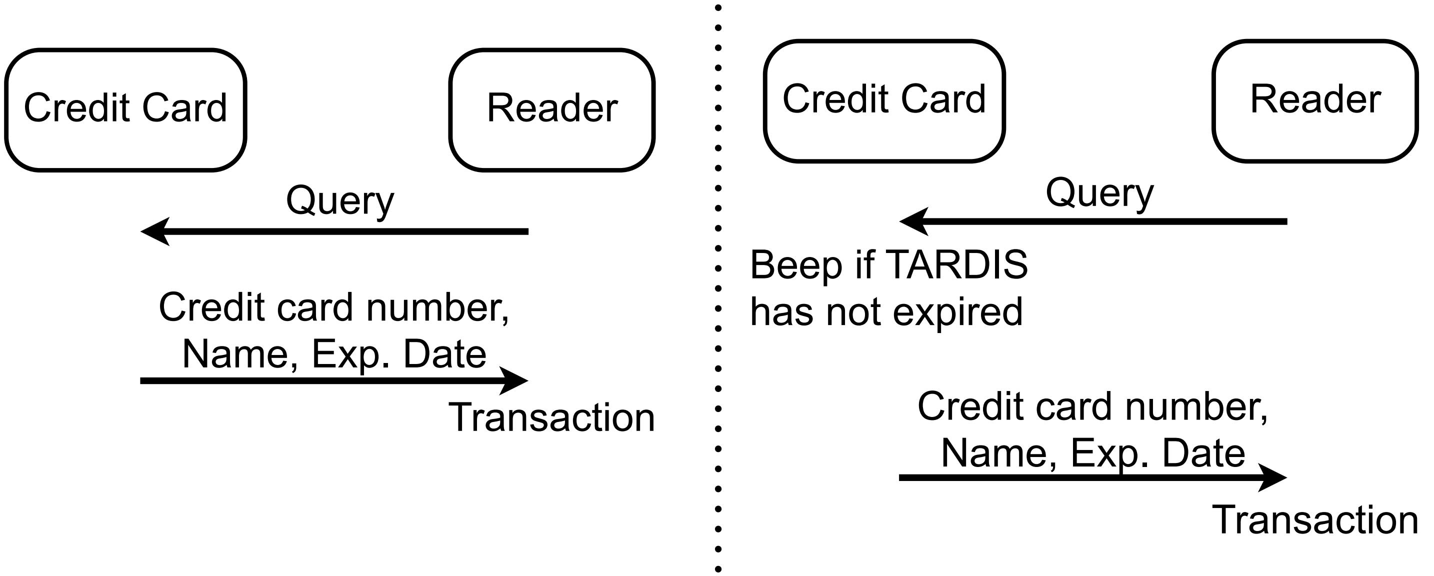
Capacitor Calculations



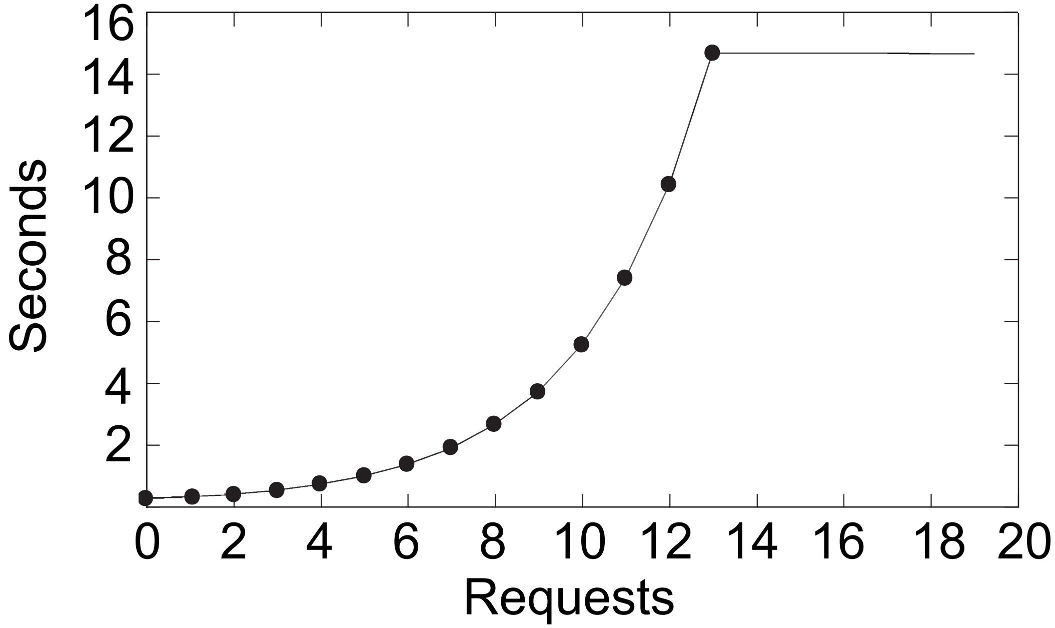
Our Circuit



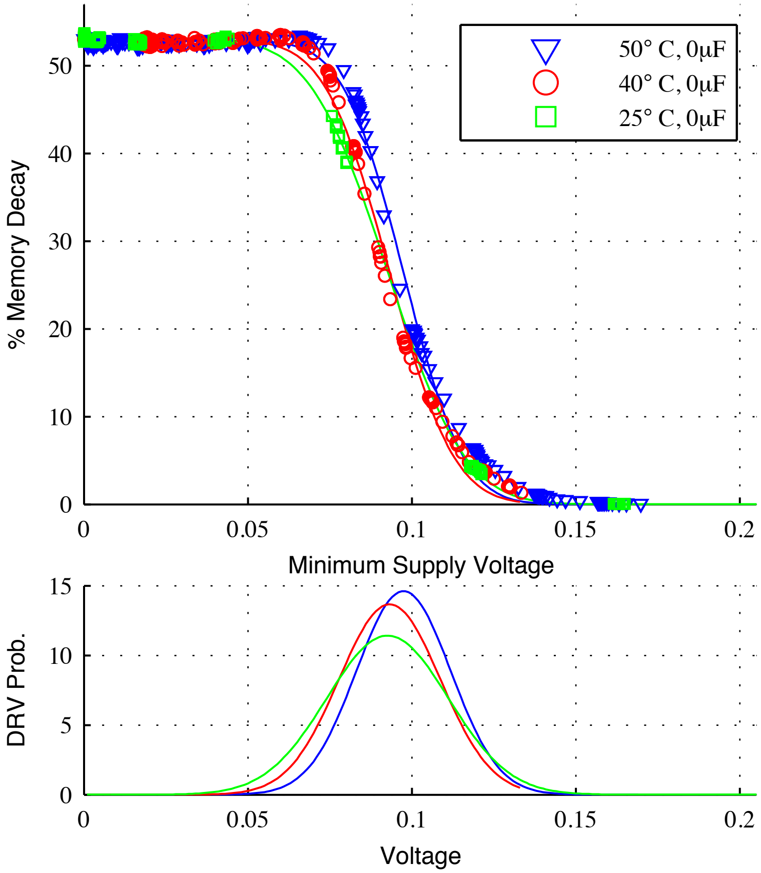
Squealing Cards


Credit Card
Reader
Query
Credit card number, Name, Exp. Date
Transaction
Credit Card
Reader
Query
Beep if TARDIS has not expired
Credit card number, Name, Exp. Date
Transaction

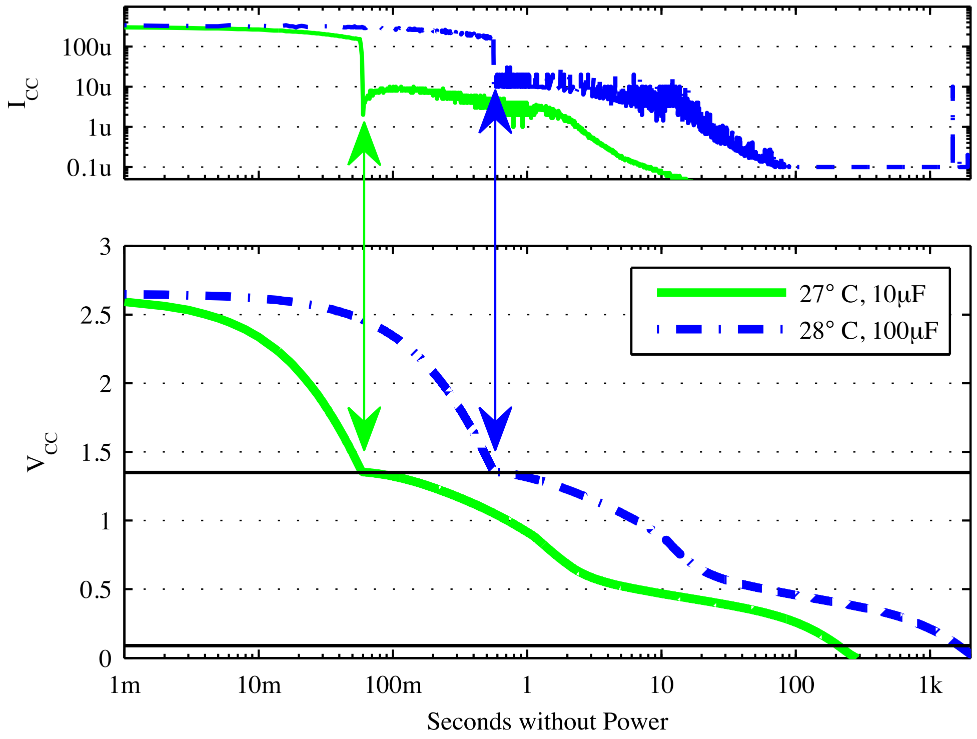
French Passports Counter



Remanence vs. Voltage

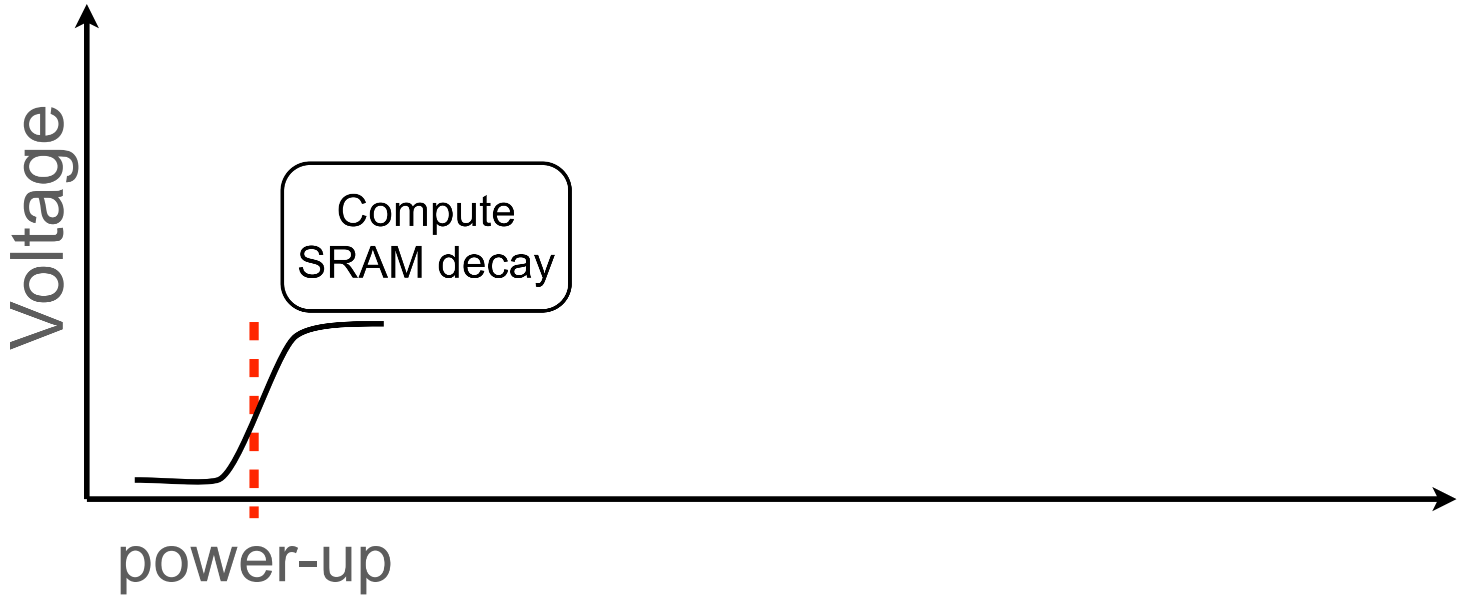


Voltage Regulators Effect



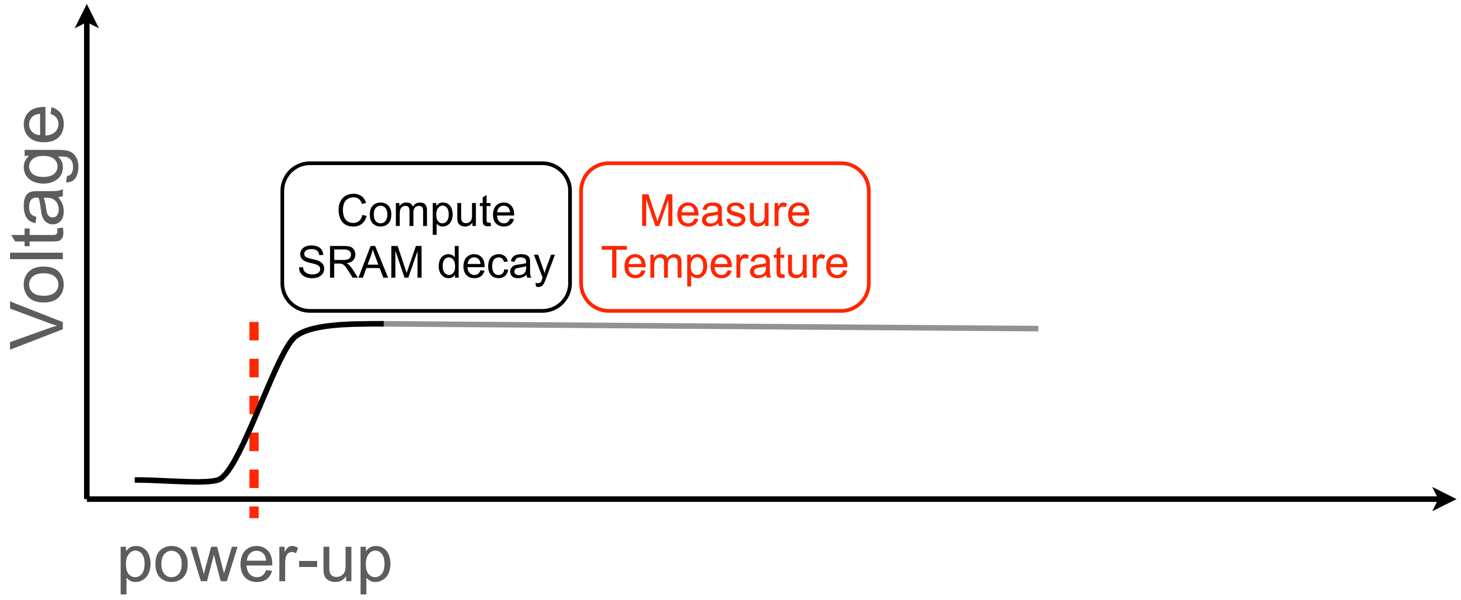
Compensate for Temperature

Compensate for Temperature

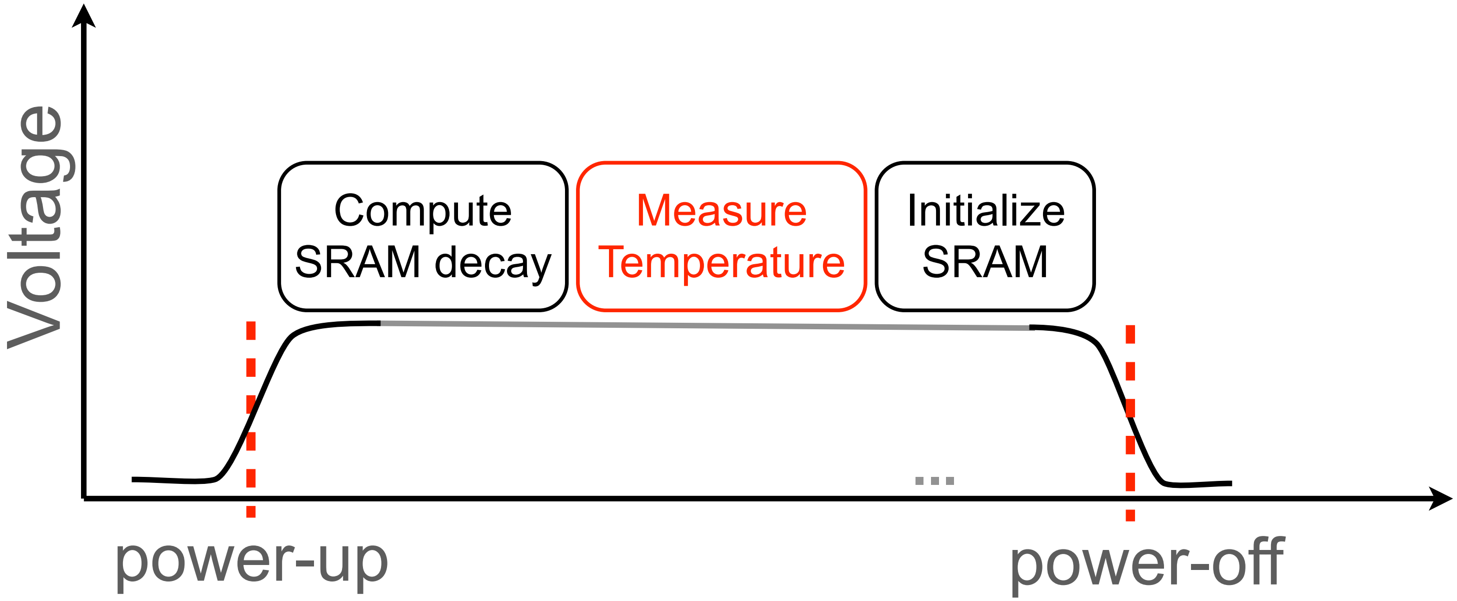


Compute SRAM decay

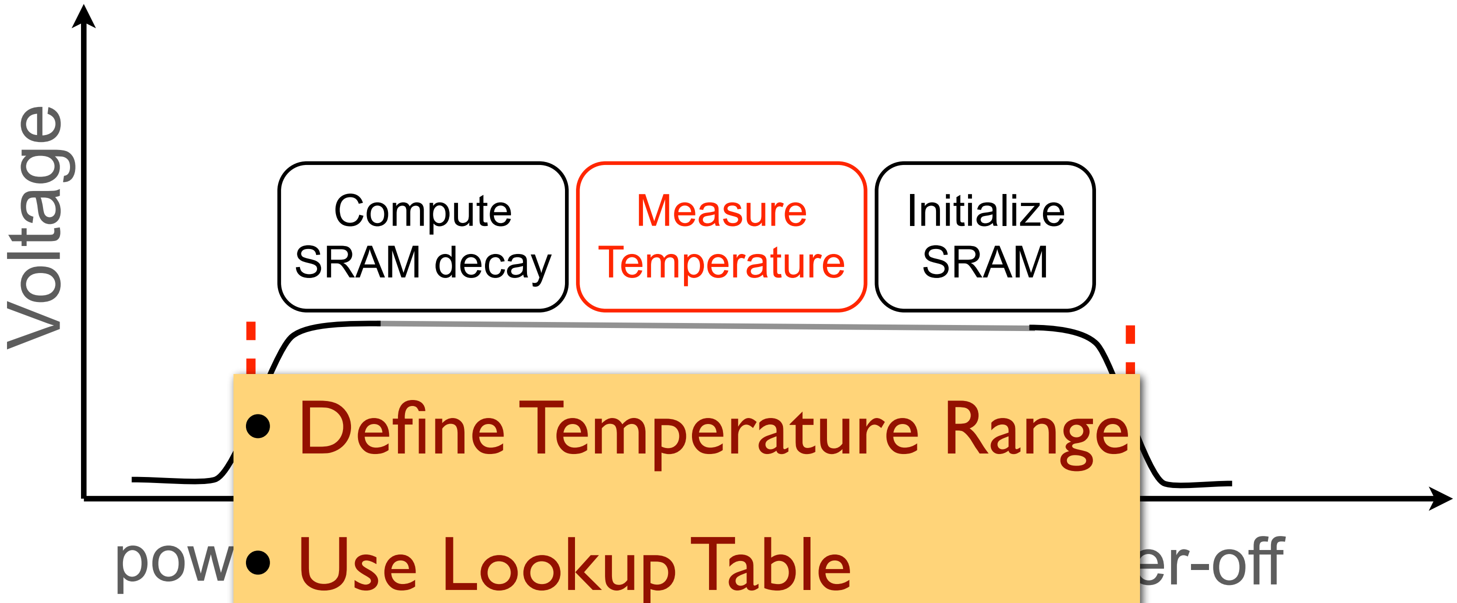
Compensate for Temperature



Compensate for Temperature



Compensate for Temperature



Voltage

Compute SRAM decay

Measure Temperature

Initialize SRAM

pow

er-off

- Define Temperature Range
- Use Lookup Table
- Polynominal Interpolation