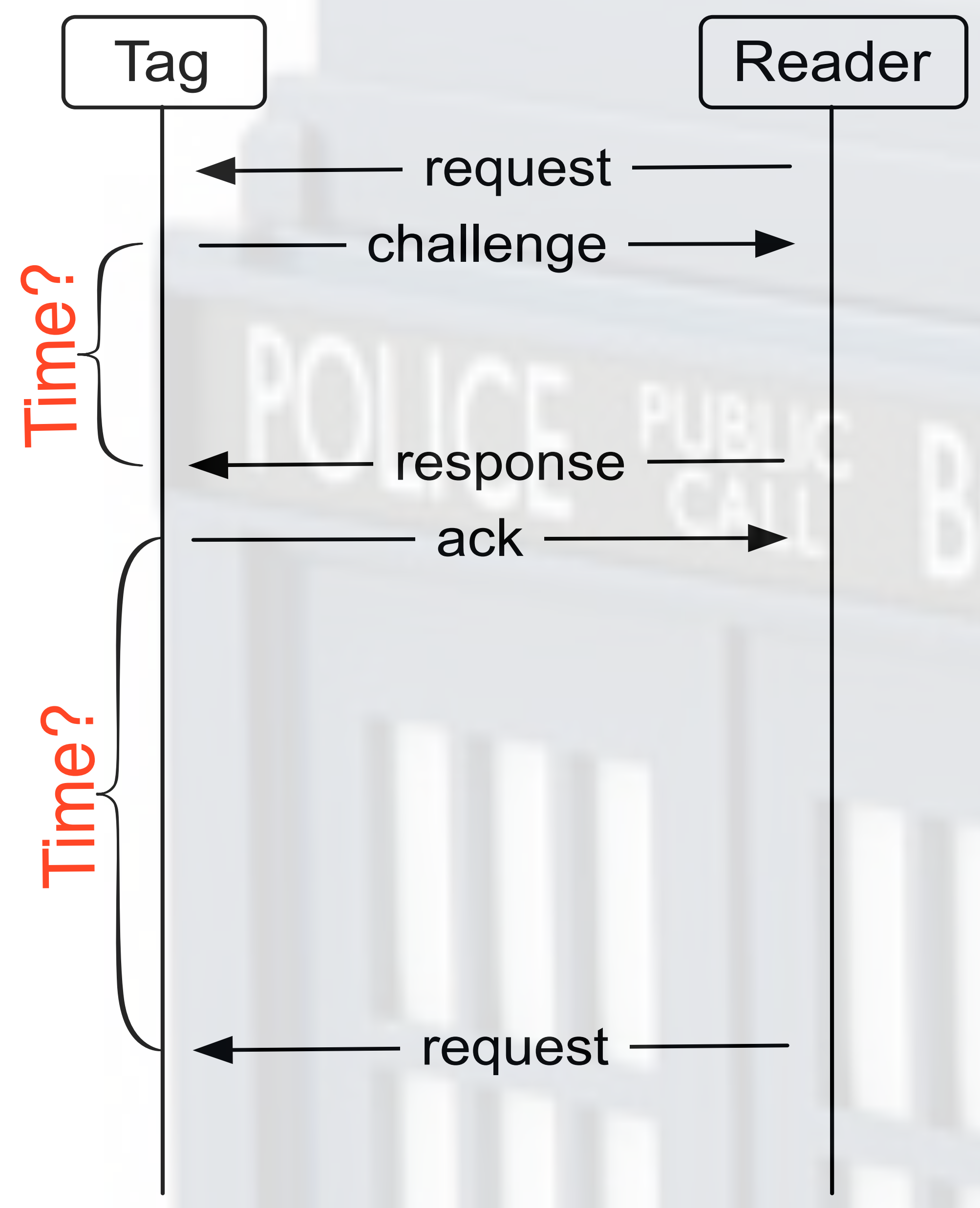
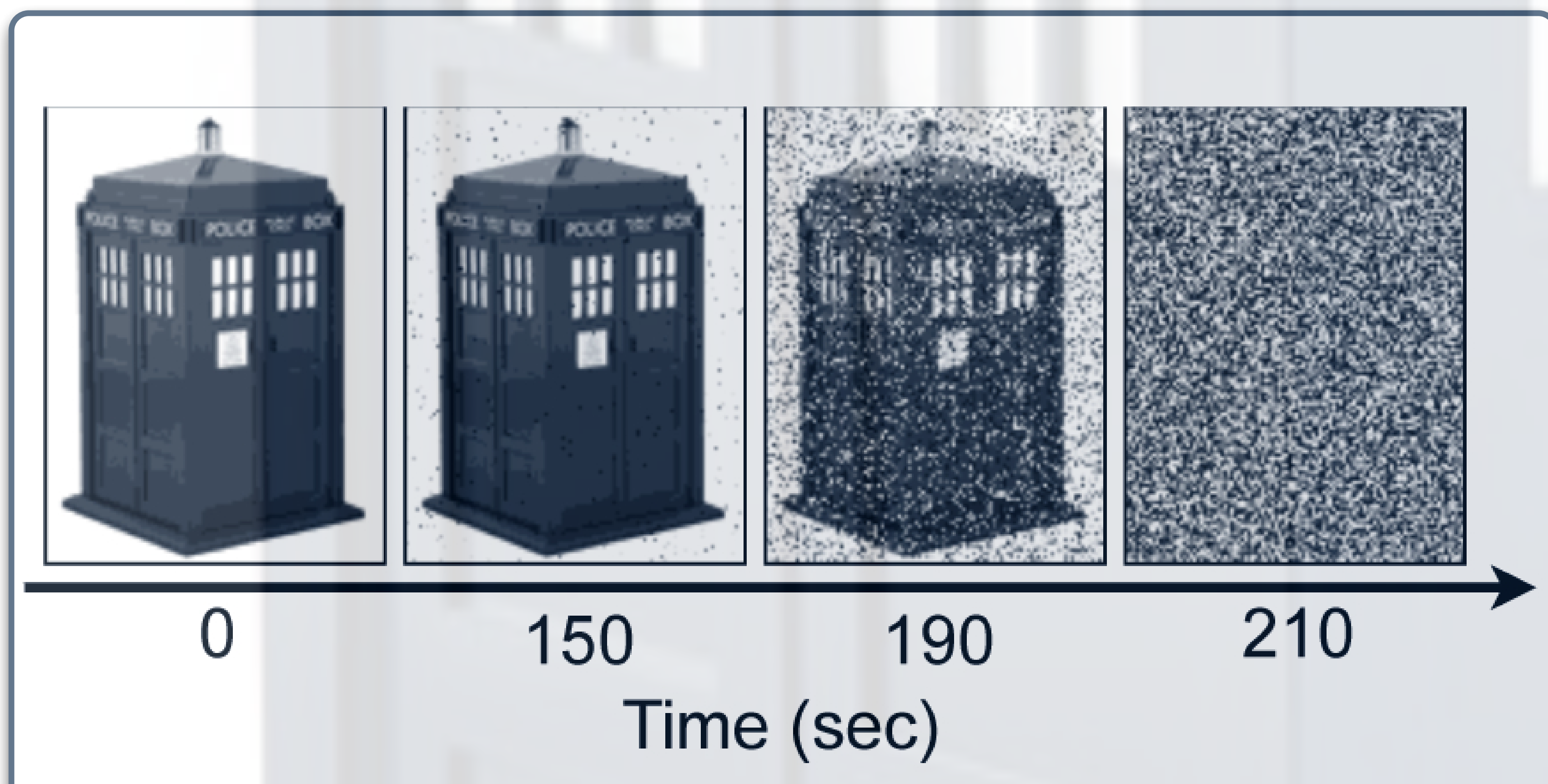
TARDIS (Time and Remanence Decay In SRAM): Secure Time Keeping For Embedded Devices Without Clocks

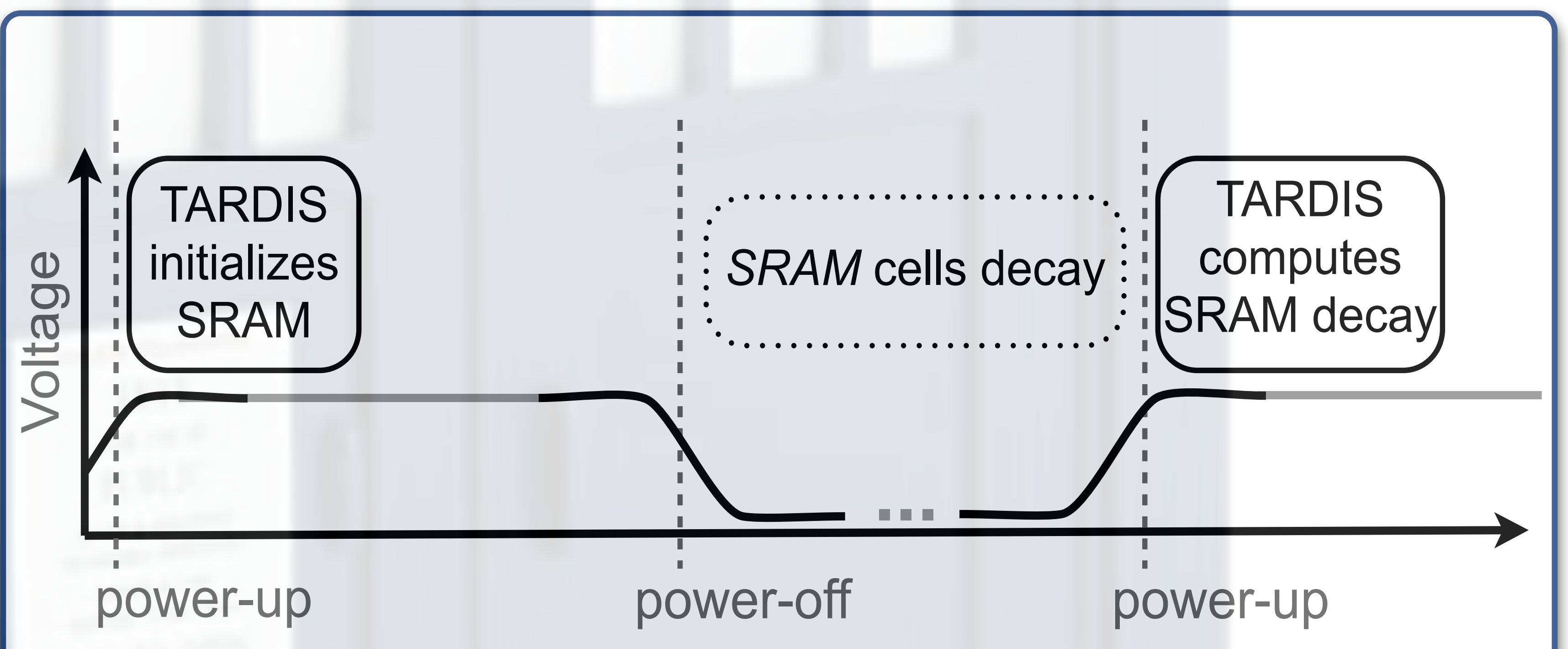
Amir Rahmati UMass Amherst | **Mastooreh Salajegheh** UMass Amherst | **Daniel Holcomb** UC Berkeley | **Jacob Sorber** Dartmouth College | **Wayne Burleson** UMass Amherst | **Kevin Fu** UMass Amherst



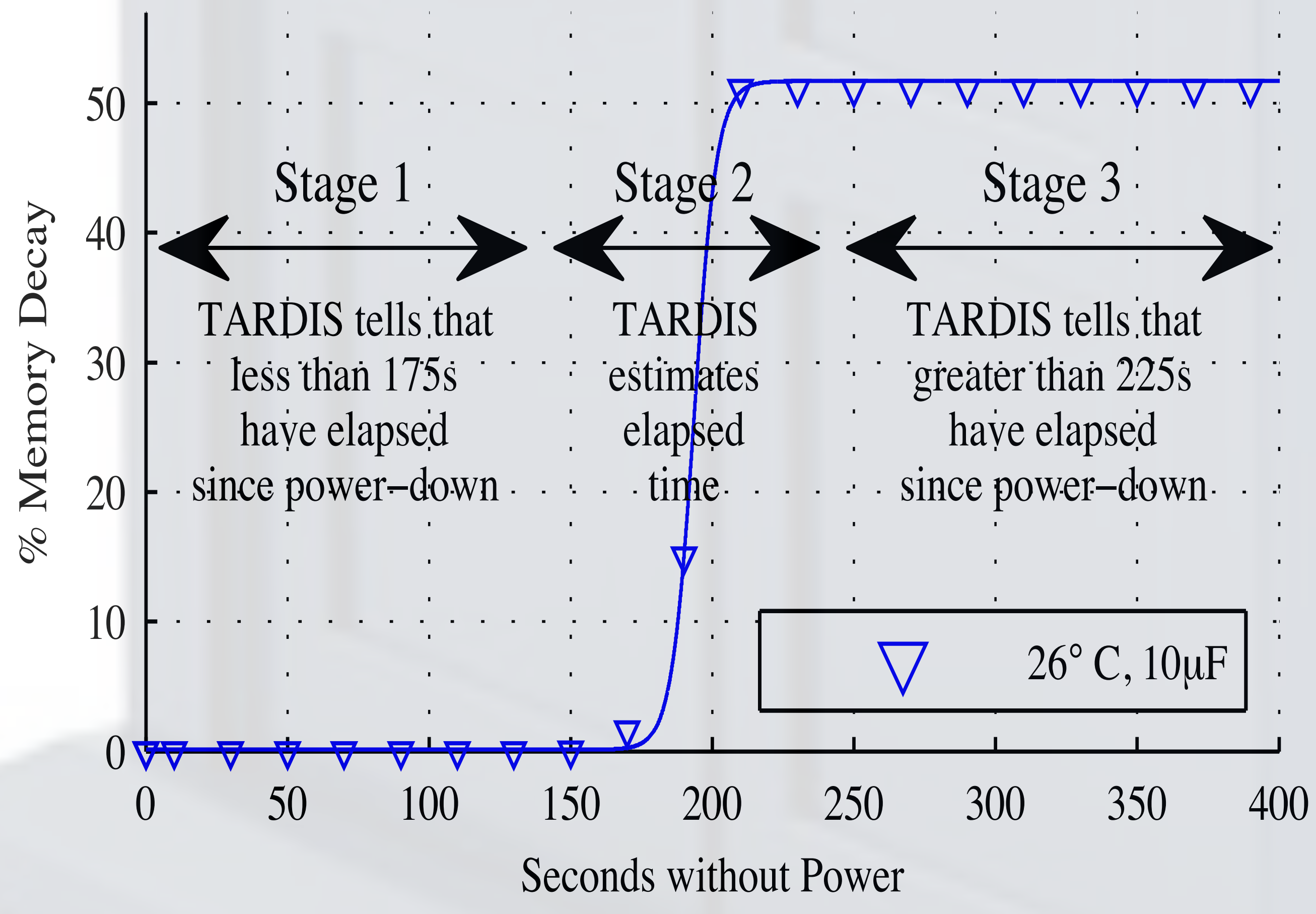
- Smart cards, RFID tags and other intermittently powered devices do not have a notion of time across power ups.
- Lack of a trustworthy clock makes it difficult to implement security protocols.
- Any solution must consider legacy hardware and implementations costs.



SRAM is a **volatile memory** that loses data in the absence of power. This **loss of data is gradual** and depends on the *circuit's specifications, capacitance*, and *temperature*. TARDIS derives a **notion of time** from the gradual data loss.



TARDIS works by first **initializing a portion of SRAM to 1's**. After a power loss, TARDIS **reads the SRAM** and will use the **decay percentage** (ratio of flipped bits) and the reading from the **temperature** sensors present in these devices to maintain a sense of time elapsed.



Estimated power loss duration on a TI MSP430F2131

Time frames can be tweaked based on cap size from few seconds to hours

Applications

- Preventing brute force attacks:

Platform	# Queries
Mifare Classic	>1500
Mifare DESfire	250,000
UHF RFID tags	200
TI DST	~75,000
GSM SIM Card	150,000

- Allowing time-out in security protocols
- Preventing Passback and Double Reads
- Implementing E-coupons

Supported by NSF Grants CNS-0831244, CNS-0923313
Any opinions, findings, and conclusions or recommendations expressed in these materials are those of the authors and do not necessarily reflect the views of the sponsors.

SPQR LABORATORY https://spqr.cs.umass.edu