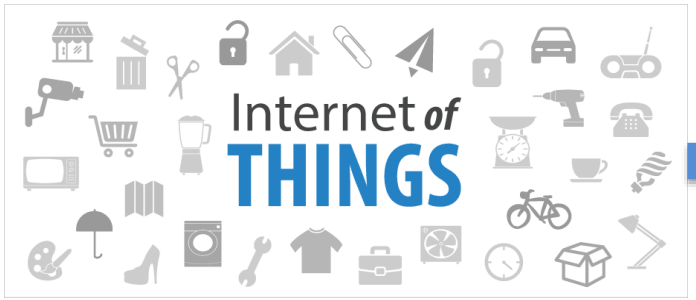
‘The Danger of Sleeping’, an Exploration of Security in Non-Volatile Processors

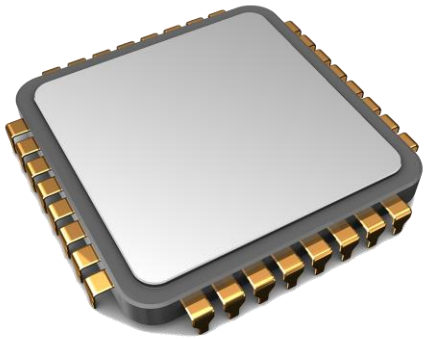
Patrick Cronin and **Chengmo Yang**
University of Delaware - Department of Electrical and Computer Engineering
Dongqin Zhou and Keni Qiu
Capitol Normal Univeristy – Information Engineering College
Xin Shi and Yongpan Liu
Tsinghua University – Department of Electronic Engineering

Outline



IoT Roadblocks

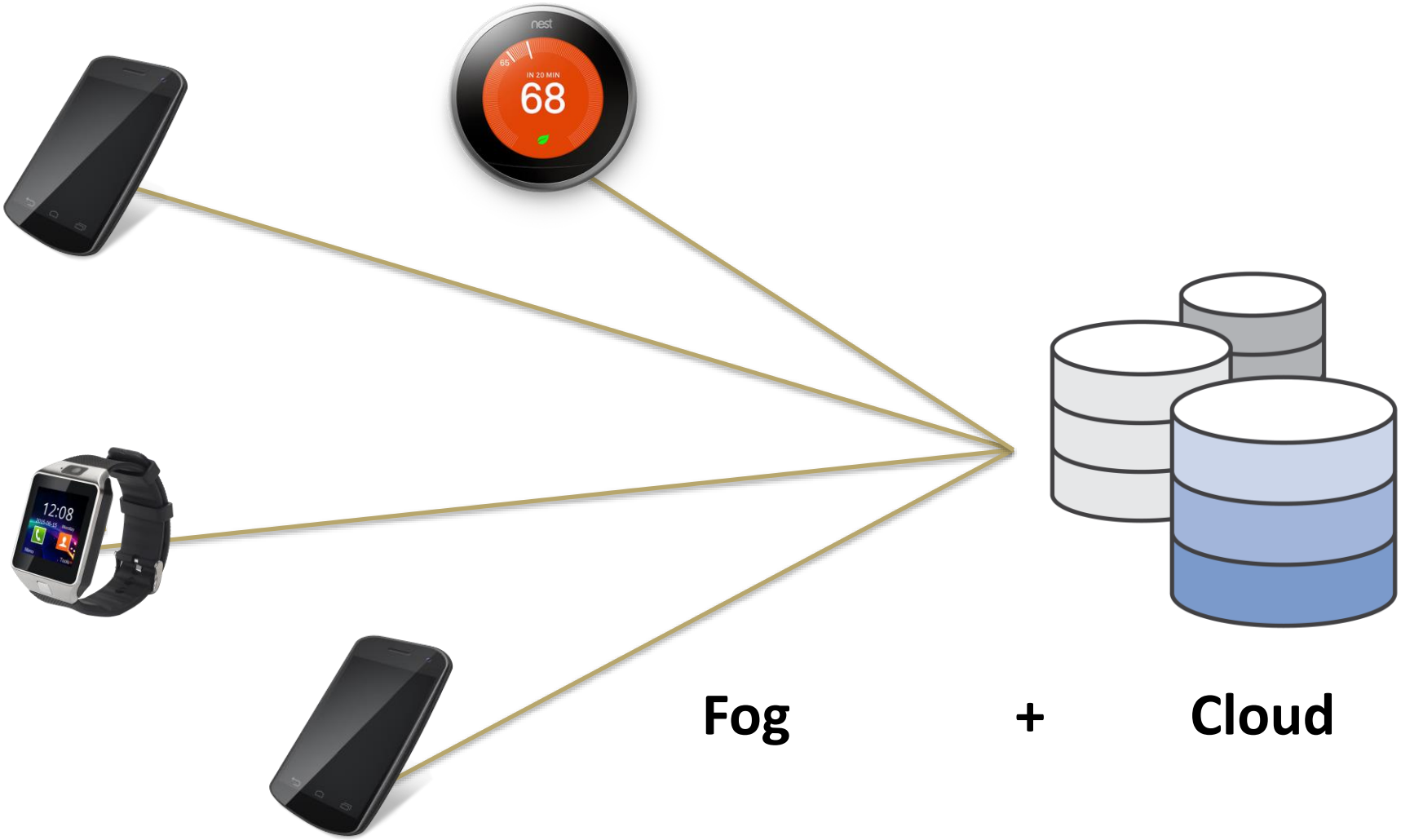
NVP Solutions



NVP Security Issues

NVP Security Solutions

Internet of Things



Fog + Cloud

Current Internet of Things Issues

Handhelds Require Batteries

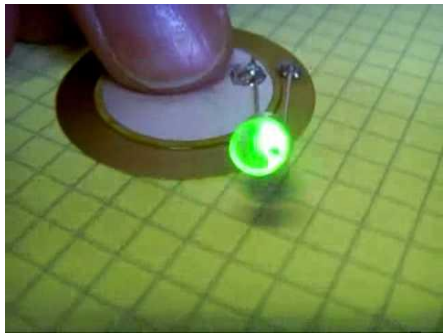
Too Bulky

Too Short of a Lifespan

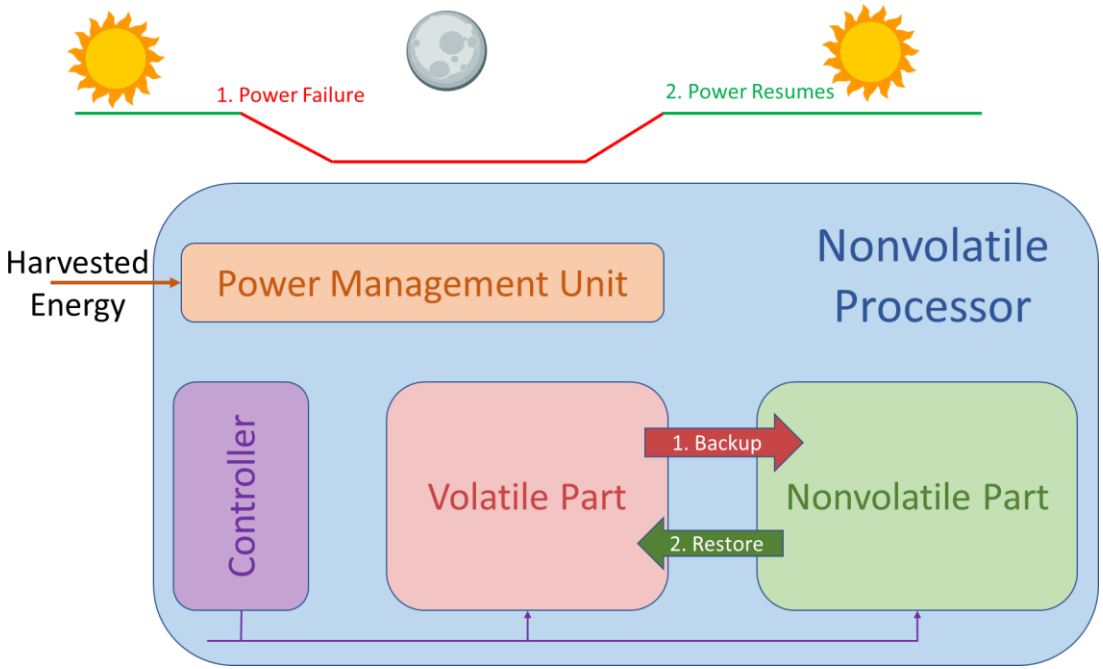
Non-Volatile Processors

Harvest energy from external source!

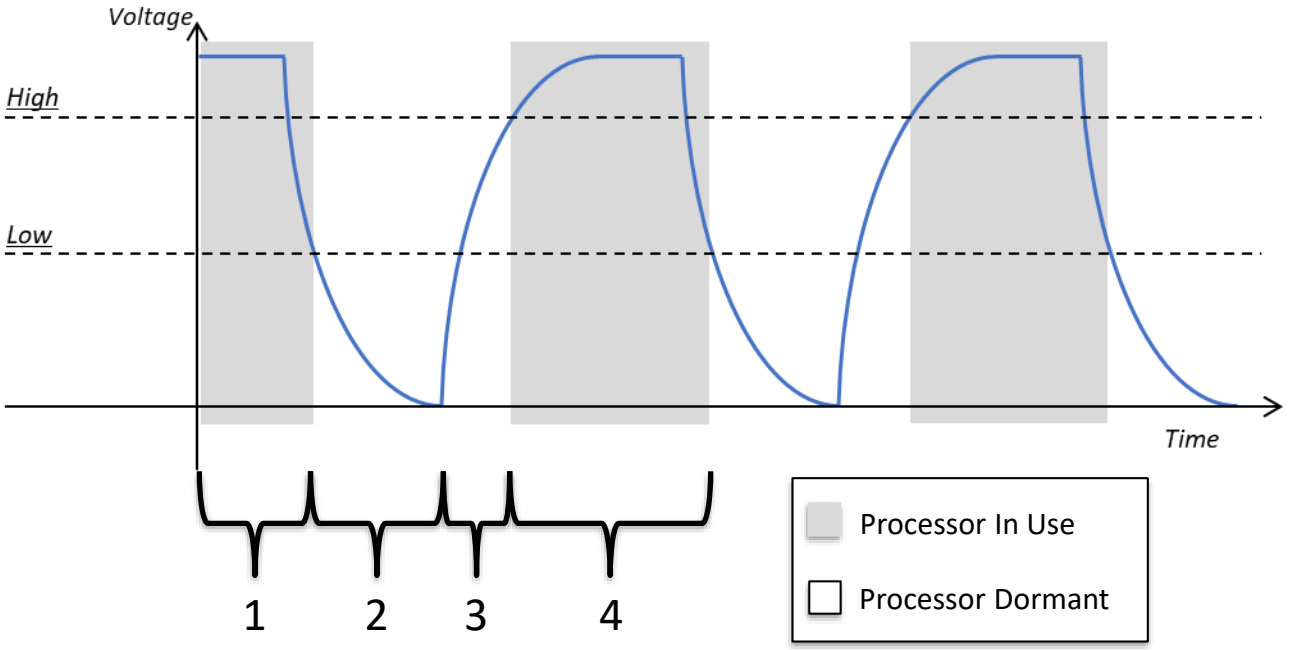
Piezoelectric



Solar



Non-Volatile Processors

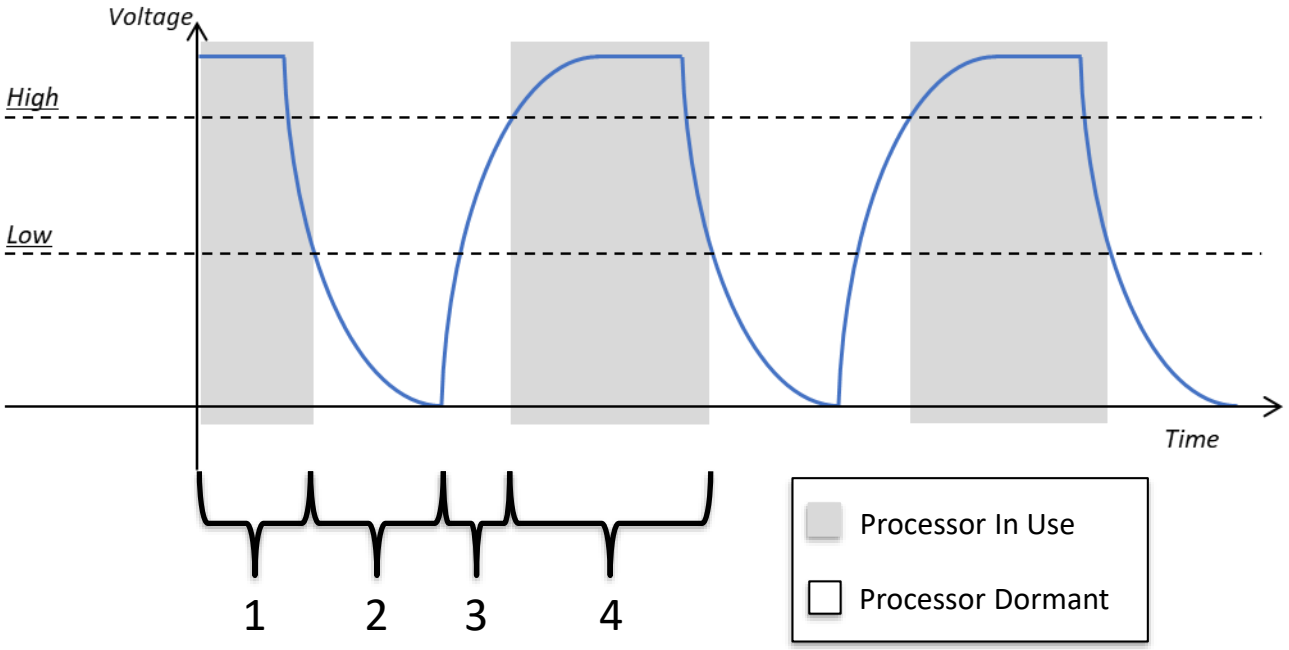


1. Processor in use and completing computations.
2. Upon reaching low energy threshold, NVP pauses to **checkpoint** and utilizes last of energy reserves.
3. Harvested energy begins to recharge capacitor.
4. Upon reaching high energy threshold, NVP **restores** from checkpoint and continues computation.

Volatile Processor

Nonvolatile Processor

Non-Volatile Processors

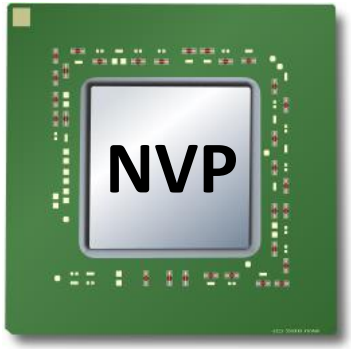


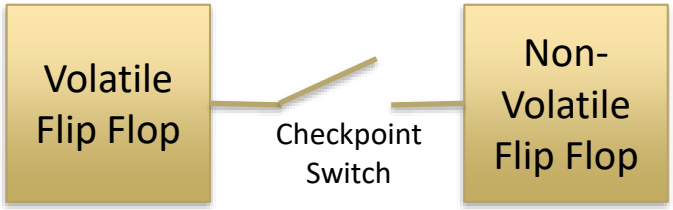
1. Processor in use and completing computations.
2. Upon reaching low energy threshold, NVP pauses to **checkpoint** and utilizes last of energy reserves.
3. Harvested energy begins to recharge capacitor.
4. Upon reaching high energy threshold, NVP **restores** from checkpoint and continues computation.

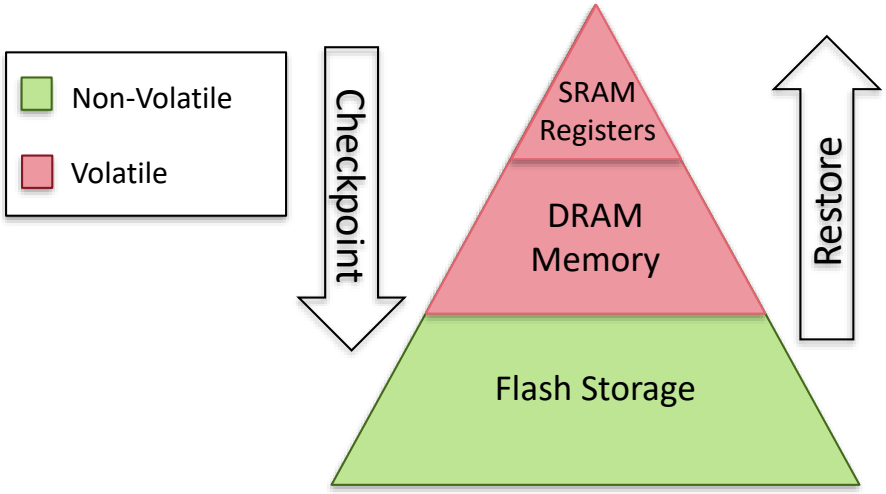
New Terms

- Checkpoint: saving internal **register** state when power approaches low
- Restore: recalling checkpointed data from **registers** when power returns

Non-Volatile Processor Checkpoints

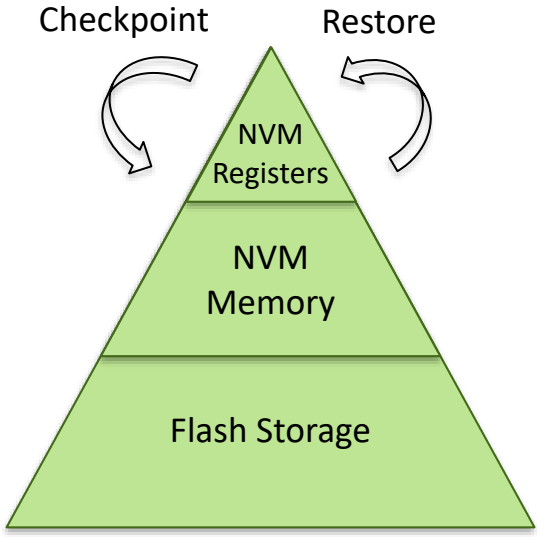






Volatile Processor

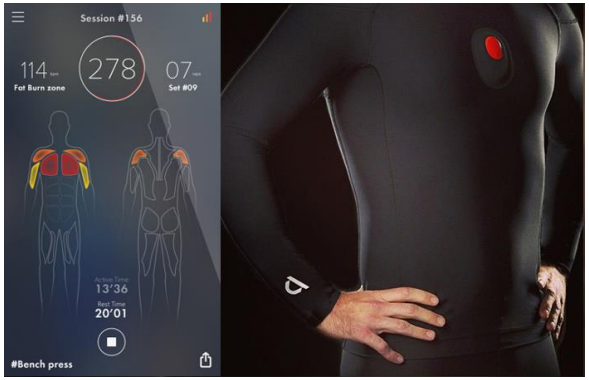
Slow!



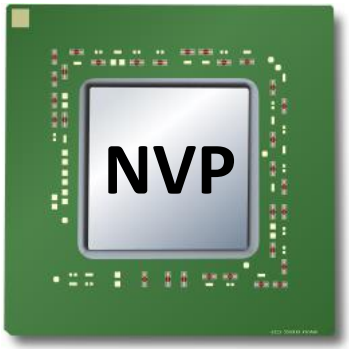
Non-Volatile Processor

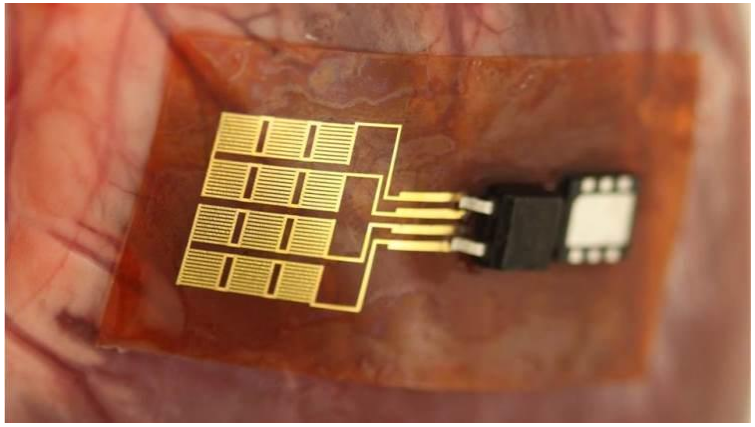
Fast!

Future IoT Applications



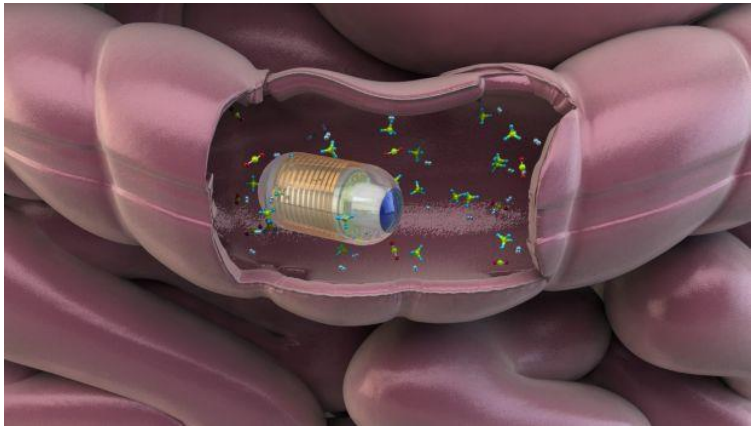
Smart Clothes



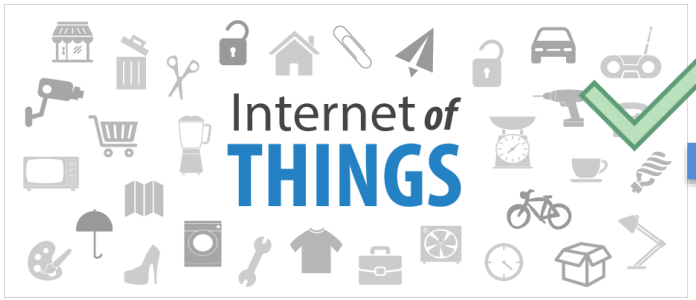


Internal Sensors

Battlefield Sensors

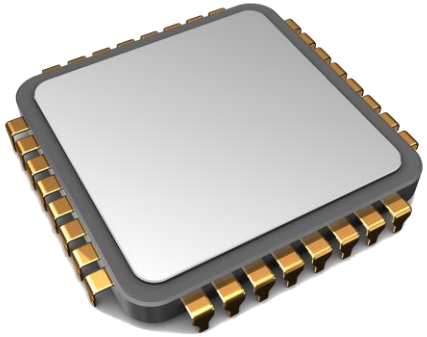


Outline



IoT Roadblocks

NVP Solutions



NVP Security Issues

NVP Security Solutions

Non-Volatile Registers	Availability	Register Rotation
Checkpoints	Confidentiality & Integrity	Secure Checkpointing
Voltage Manipulation	Integrity	Amnesia Avoidance

NVP Attacks – Register Wearout

Memory Technology	Volatile?	Endurance	Usage
Dynamic RAM	Y	$>10^{16}$ [1]	System Memory
Static RAM	Y	$>10^{16}$ [3]	Register File
Magnetoresistive RAM	N	$>10^{15}$ [4]	Register File
Ferroelectric RAM	N	10^{13} [3]	Register File
Phase Change Memory	N	10^{6}-10^{9} [1]	Main Memory
Resistive RAM	N	10^{6}-10^{12} [2]	Main Memory
Typical Flash Based SSD	N	10^{5} [3]	Main Memory

Current NVP generation → Magnetoresistive RAM

Previous NVP generation → Ferroelectric RAM

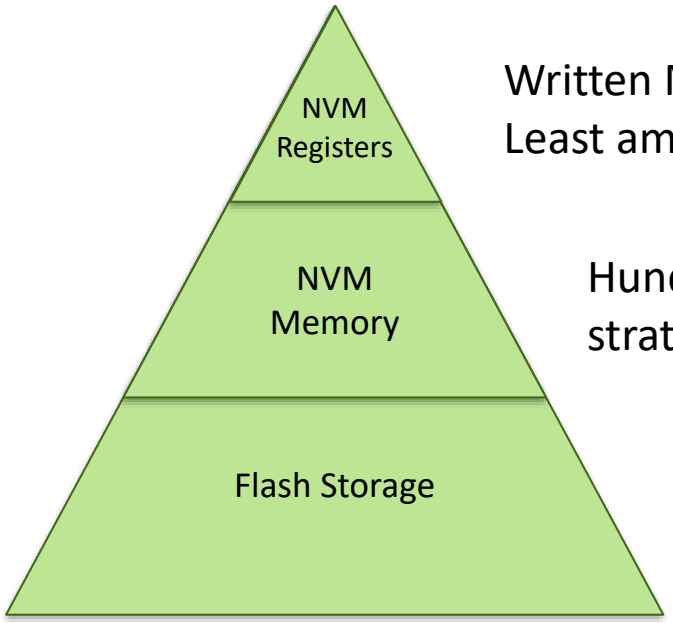
[1] Yu-Ming Chang, Pi-Cheng Hsiu, Yuan-Hao Chang, Chi-Hao Chen, Tei-Wei Kuo, and Cheng-Yuan Michael Wang. 2016. Improving PCM Endurance with a Constant-Cost Wear Leveling Design. *ACM Trans. Des. Autom. Electron. Syst.* (June 2016)

[2] J. Cong and B. Xiao, "FPGA-RPI: A novel FPGA architecture with RRAM-based programmable interconnects," TVLSI, vol. 22, Apr. 2014

[3] S. Evanczuk, "FRAM Ics Extend Endurance in Low-Power Applications", Apr. 2015

[4] M. Durlam *et al*., "Toggle MRAM: A highly-reliable Non-Volatile Memory," *2007 International Symposium on VLSI Technology, Systems and Applications (VLSI-TSA)*, 2007, pp. 1-2.

NVP Attacks – Register Wearout



Written Most Frequently!
Least amount of wear leveling flexibility!

Hundreds of wear leveling strategies already proposed!

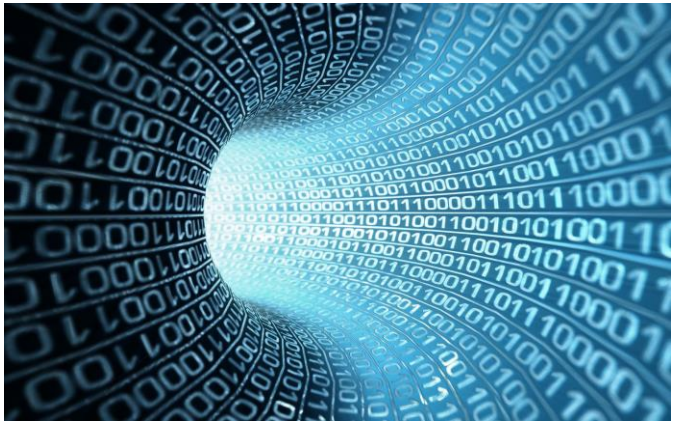
Wear leveling already supported in commercial products!

```
1   int main( int argc, const char* argv[] )
2   {
3     int flipper = 0xAAAAAAAA; //Variable to have bits flipped
4
5     while(true) {
6       flipper = flipper ^ 0xFFFFFFFF;  //Invert every single bit of variable
7     }
8
9   }
10
```

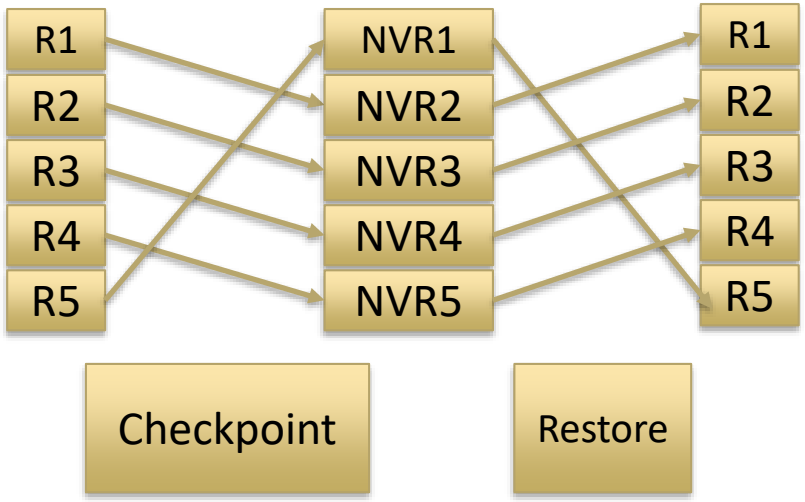
Countermeasure – Register Rotation

Software Solutions

Compiler-directed register rotation [1]



Hardware Solutions



Rotate FF to NVFF mapping on checkpoint
Need extra wires!

[1] C. Yang and M. Ruiz Varela, "Qualifying non-volatile register files for embedded systems through compiler-directed write minimization and balancing," *2015 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*, 2015.

New Feature	Compromises	Solution
Non-Volatile Registers	Availability	Register Rotation
Checkpoints	Confidentiality & Integrity	Secure Checkpointing
Voltage Manipulation	Integrity	Amnesia Avoidance

NVP Attacks – Checkpoint Exposure

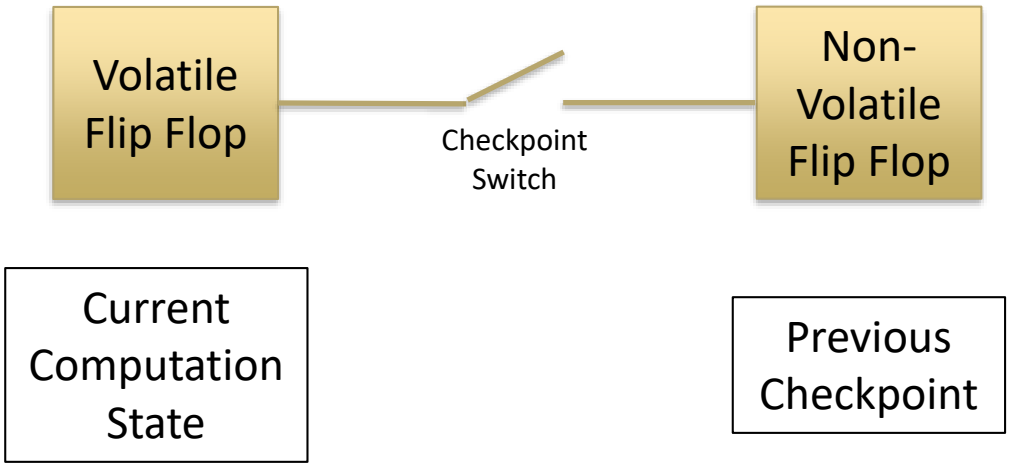
- Exposes Processor to Program Crashes
- Endangers Encryption

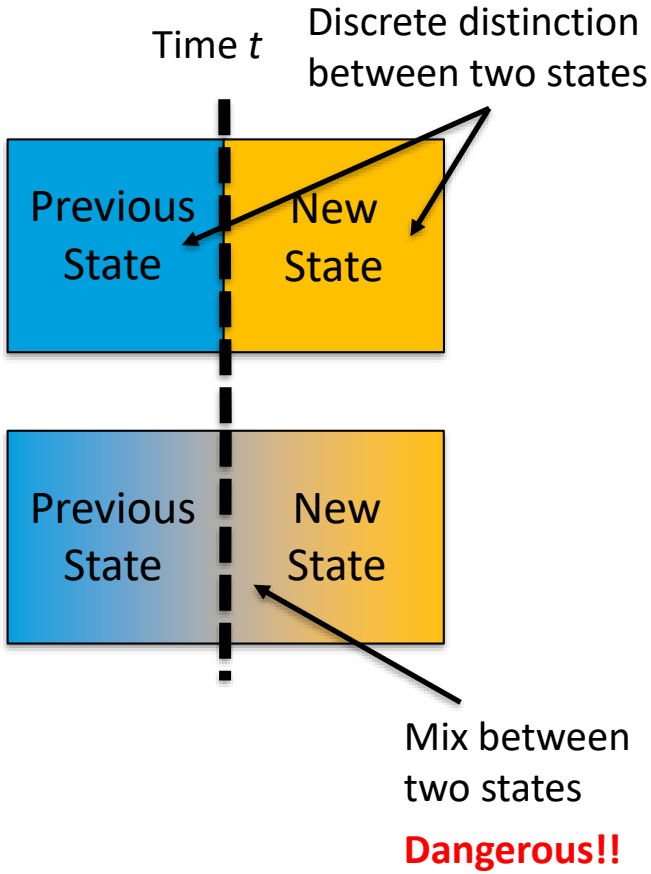
ENCRYPTION

NVP Attacks – Atomic Checkpoint

Ideally, deletion of previous checkpoint should happen **after** establishing current checkpoint.

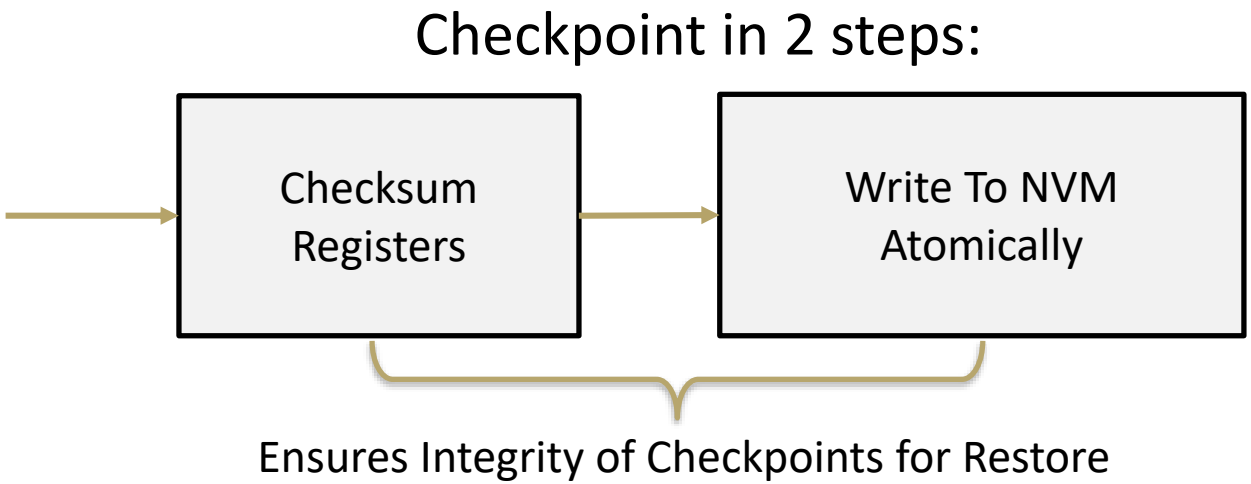
However, in NVP, the two events happen together.





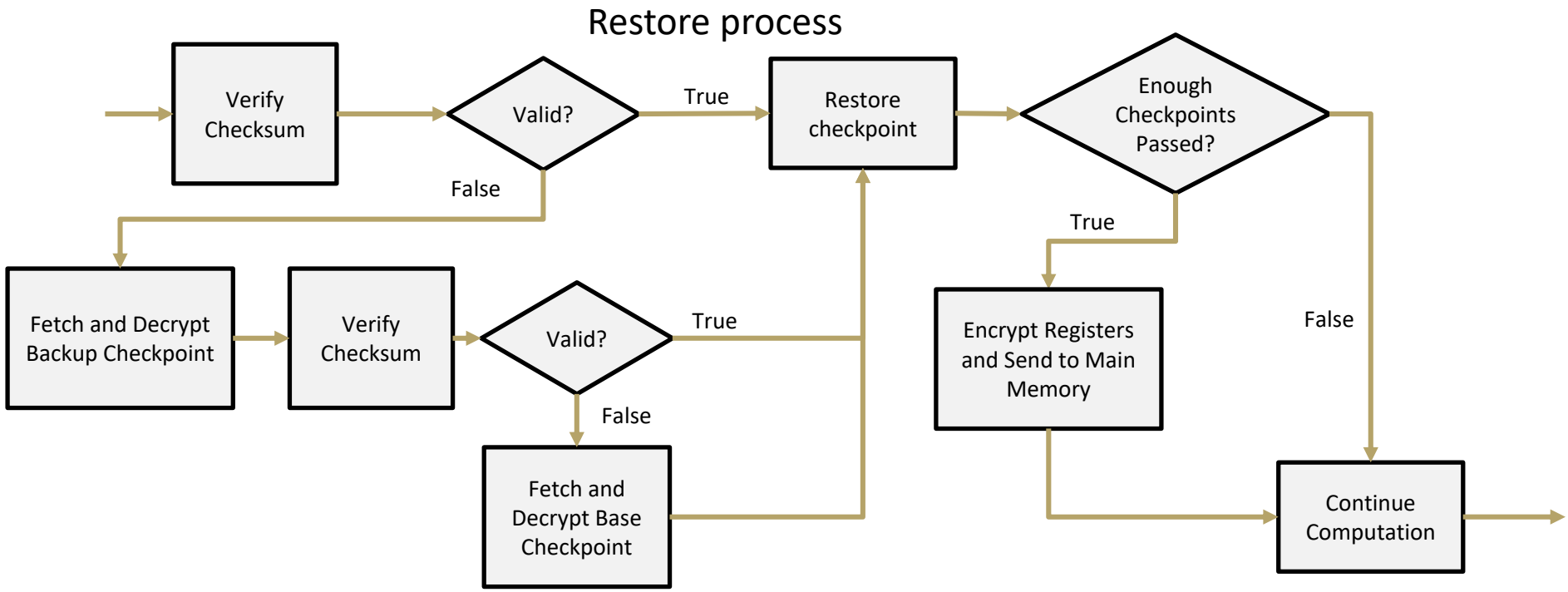
If there is a power issue, we can have mixed states!

Countermeasure – Secure Checkpointing



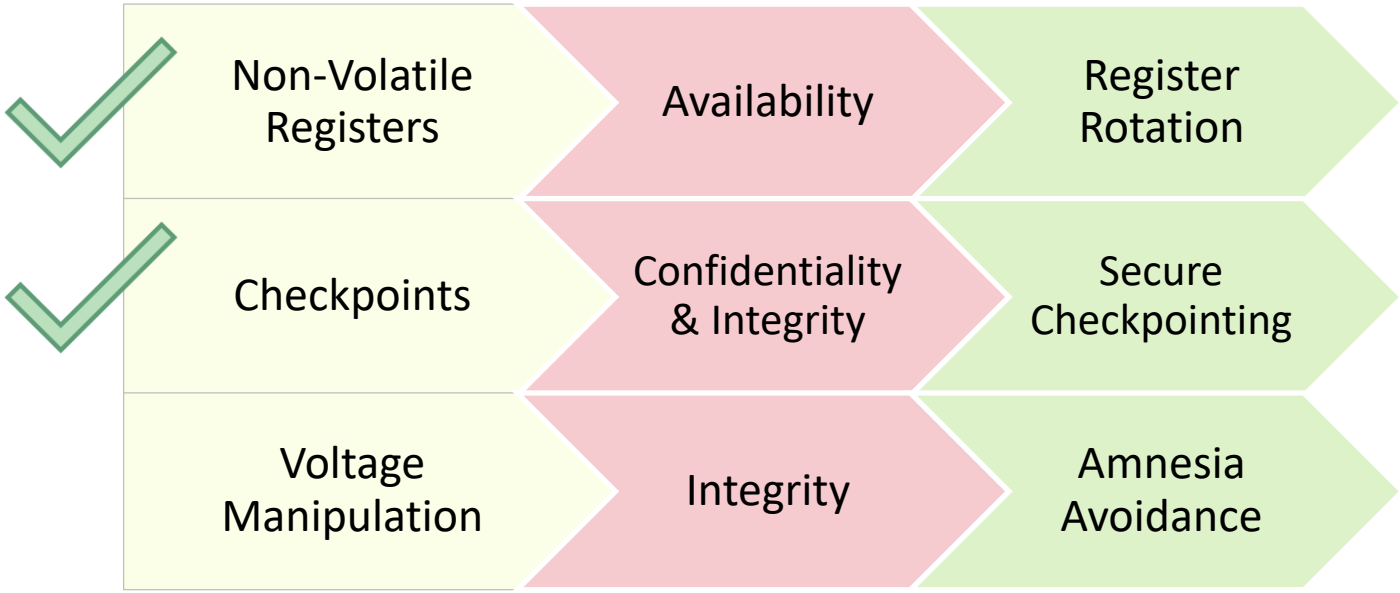
- Maintain three checkpoints
  - Current checkpoint
  - One among the last n checkpoints
  - Safe base state of device

Countermeasure – Secure Checkpointing



- Maintain three checkpoints
  - Current checkpoint
  - One among the last n checkpoints
  - Safe base state of device


New Feature
Compromises
Solution


Non-Volatile Registers
Availability
Register Rotation
Checkpoints
Confidentiality & Integrity
Secure Checkpointing
Voltage Manipulation
Integrity
Amnesia Avoidance

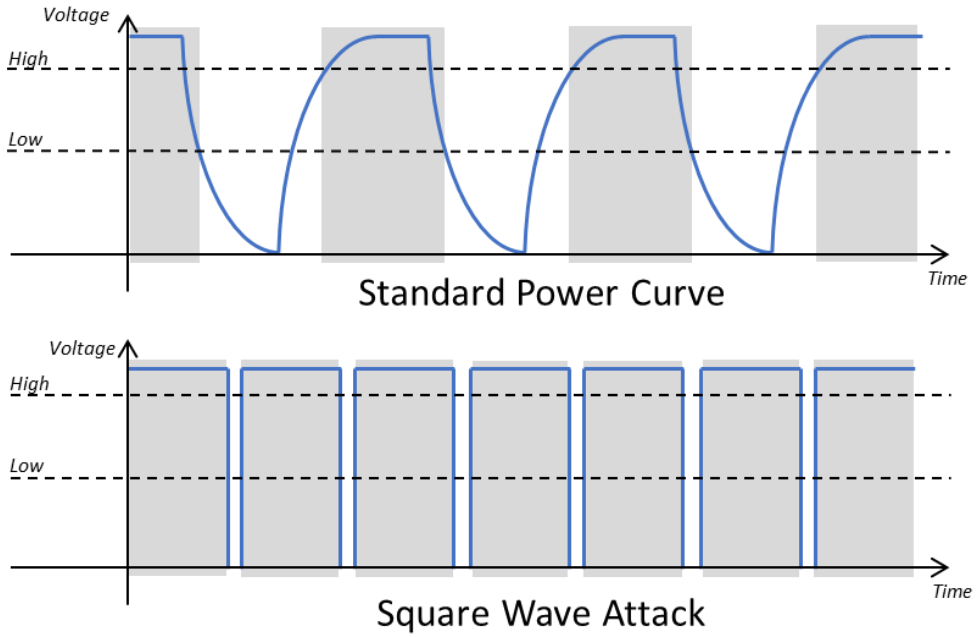
NVP Attacks – Voltage

ms-scale restore operations enable quick poweron

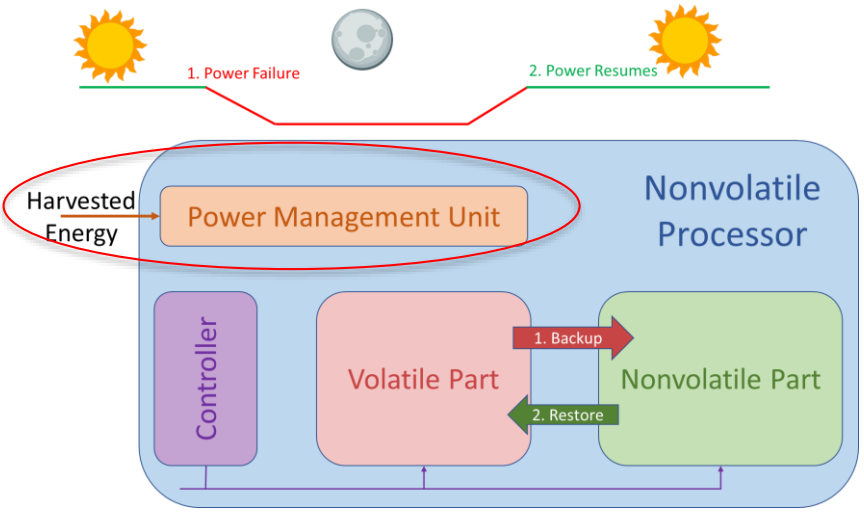
current NVP cannot keep track of time while off

Rate Limiting Attack!

Quick turn off causes current state to be forgotten without checkpointing progress. This vulnerability affects systems like password try rate limiting.

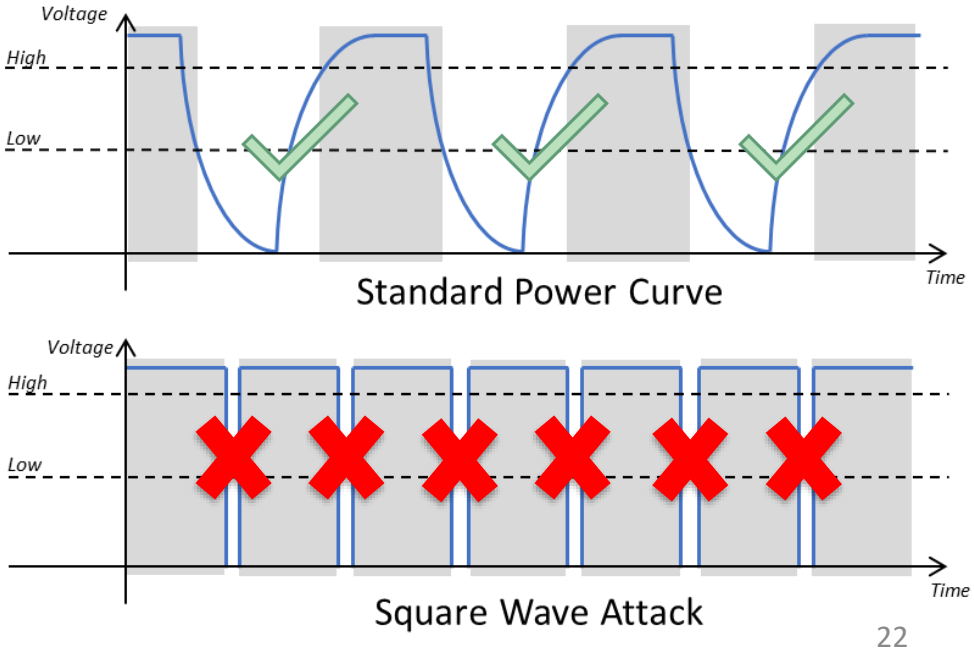


Countermeasure – Voltage Logging



Voltage logging enabled by ADC in PMU

Utilize voltage logging to keep system from acknowledging restart if it hasn't been charged correctly.



Conclusion and Further Research

Conclusion and Further Research

- Register Wearout Prevention
- Secure Checkpoint Implementations
- Secure Voltage Logging

Questions?