Systems and Internet Infrastructure Security

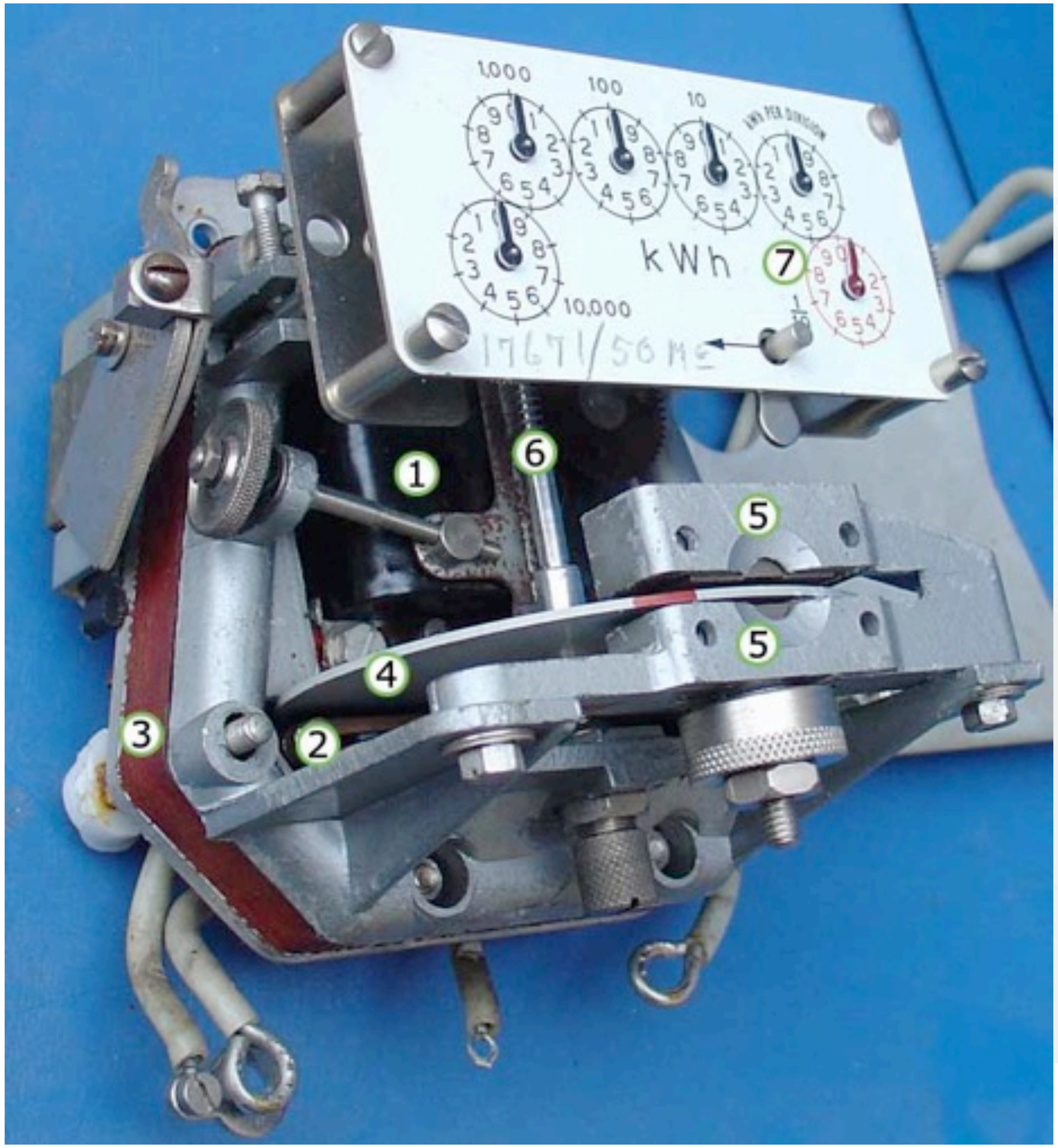
Network and Security Research Center
Department of Computer Science and Engineering
Pennsylvania State University, University Park PA

Embedded Firmware Diversity for Smart Electric Meters

Stephen McLaughlin, Dmitry Podkuiko, Adam Delozier, Sergei Miadzvezhanka, and Patrick McDaniel

Tuesday, August 10, 2010

Smart Meters



Electromechanical

Smart Meter

3 Concerns

Fraud - Hacking meters to reduce energy bill

Privacy - Using detailed load profiles to determine behavior

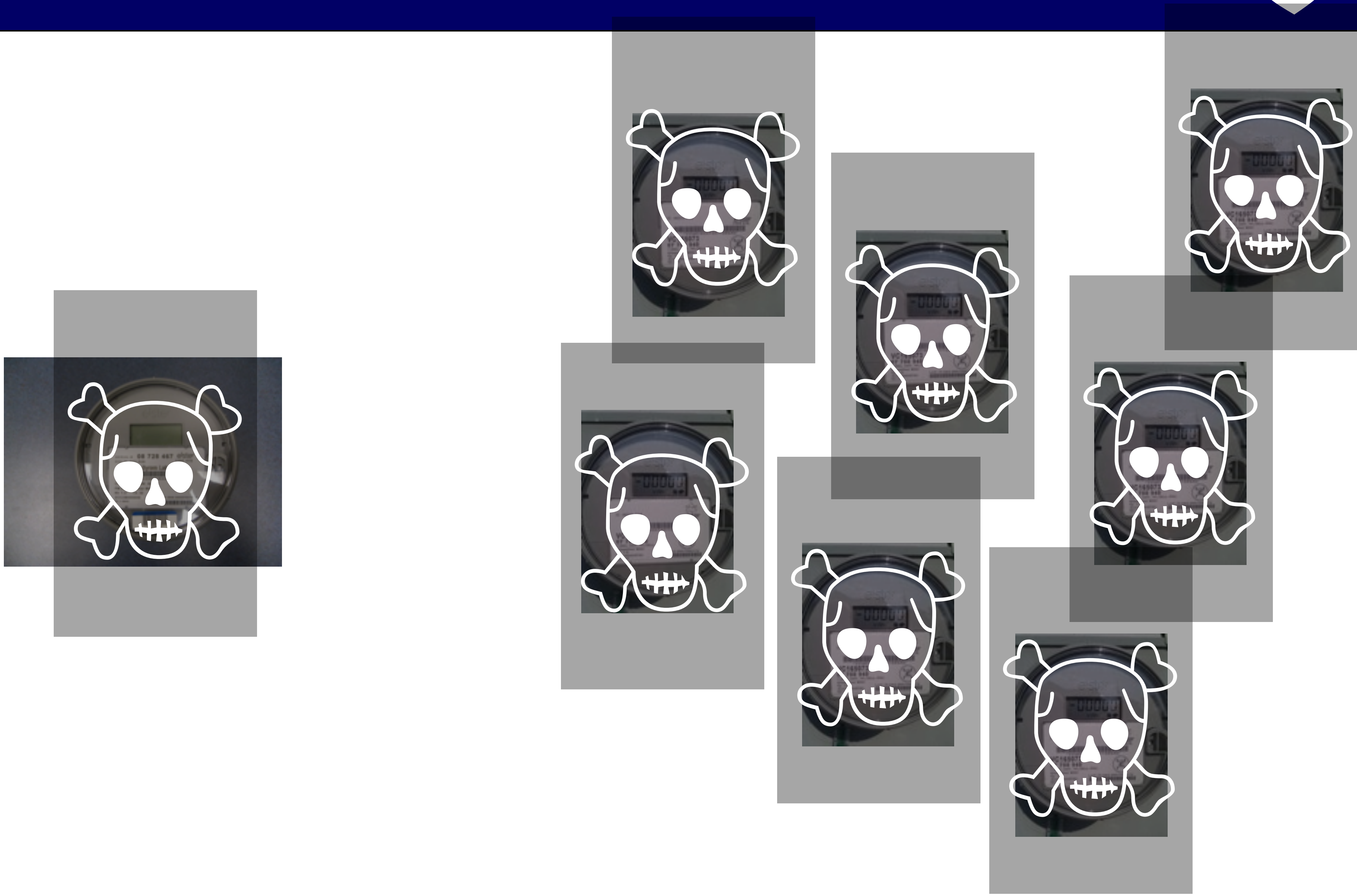
Blackout - Exploiting large numbers of meters and cutting power

The Problem of Meter Monocultures

The Problem of Meter Monocultures

The Problem of Meter Monocultures

The Problem of Meter Monocultures



A Known Mitigation: Diversity

Software Diversity: *Uniqueness added to the implementation, but not interfaces of a program.*

Caveat: Uniqueness must depend on good randomness

Limitations of Embedded Systems

Diversity Technique	Limitation
Address Space Layout Randomization	No MMU
Software Fault Isolation	No protected supervisor mode
Non-Executable Stacks	No NX bit
Stack Cookies	Check code not segmented
Address Encryption	Works, but failed exploits can cause random errors

Firmware Type	Processor Type	MMU	Privileged Mode	NX Bit	RAM
Repeater Controller	Renesas M16C	No	No	No	20KB
Wireless Mesh	Renesas H8S	No	No	No	N/A
Embedded TCP/IP	Lantronix DSTni-EX 186	No	No	No	256KB
Gateway Controller	Intel i386EX	Yes	Yes	No	8MB

More Embedded Challenges

- Diversity scheme hardness depends on secret size, which is related to machine word size.

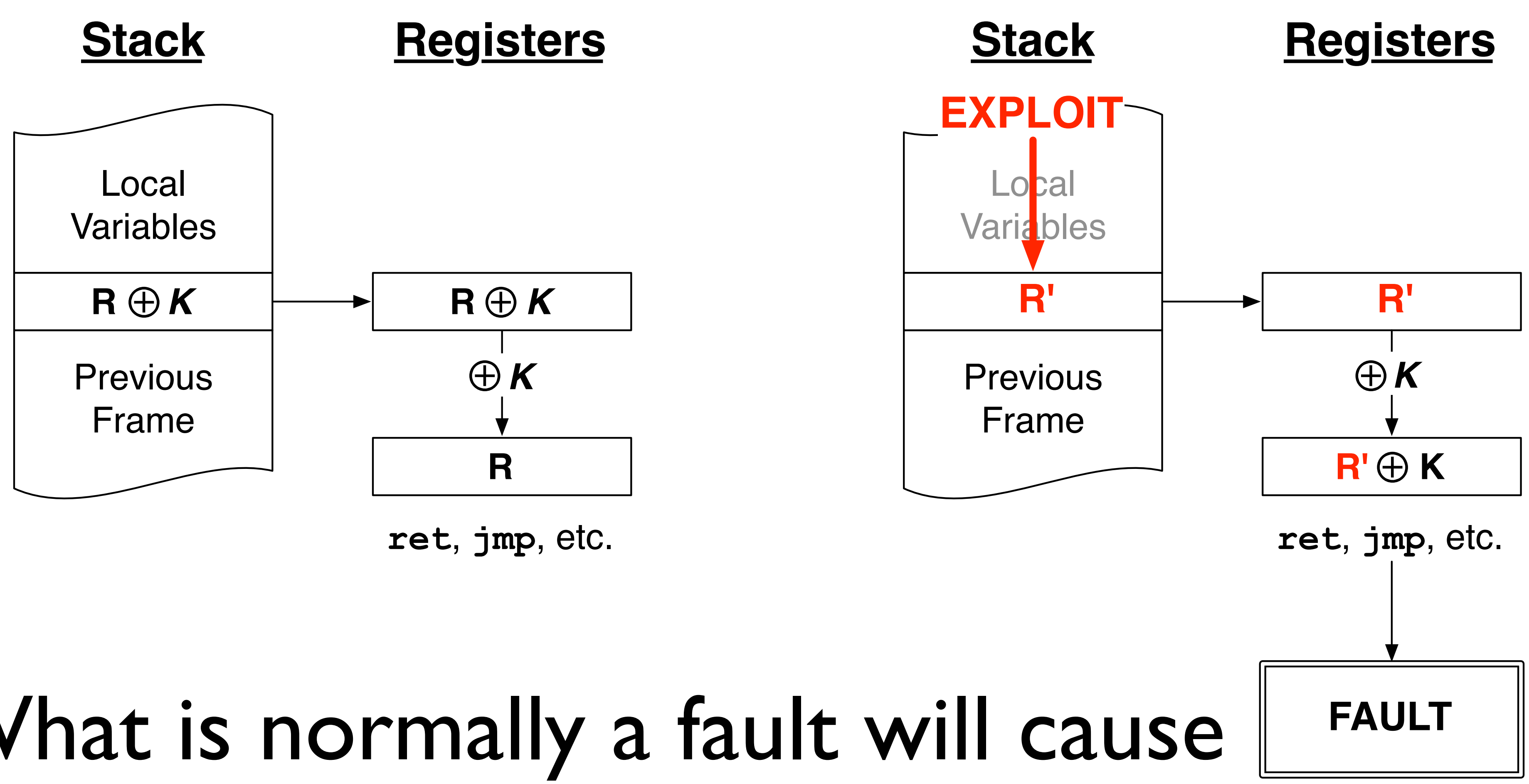
- Smart meter components range from 32- down to 8-bit MCUs.

- This will affect the layout of some data structures in 8- and 16-bit systems, where multiple machine words will be needed to store the diversified value.

Address Encryption

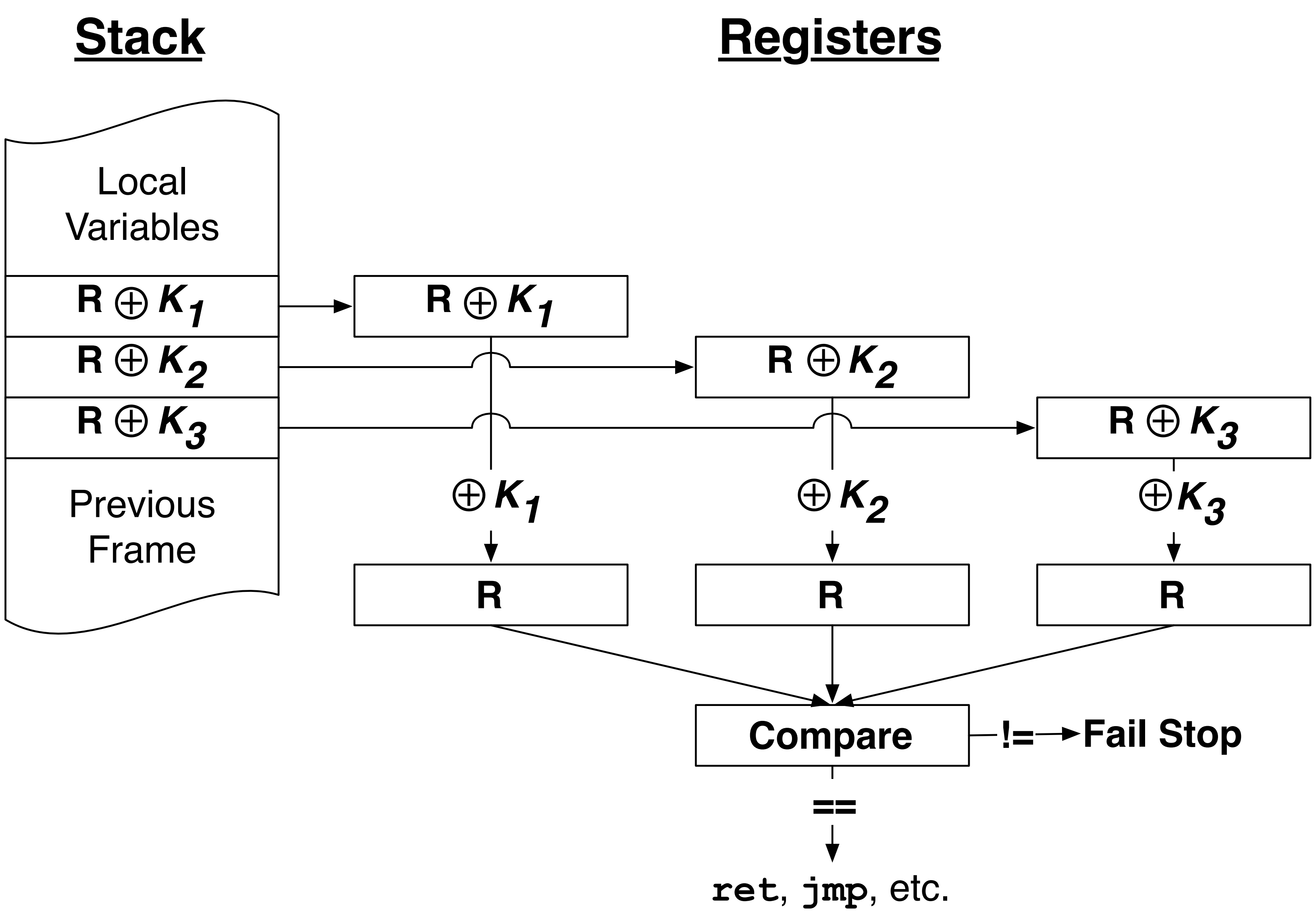
Normal Dereference

Exploit Dereference



What is normally a fault will cause unpredictable errors in embedded architectures with single, real-mode address spaces.

Redundant Address Encryption



For three keys on a 16 bit MCU:

- 2^{48} probes to compromise
- 2^{32} probes to random error

A 15,000 node deployment that is rate limited to 3 request/second for each meter requires approx. 10 years to fully compromise when using three keys.

Binary Instrumentation

- Feasible for embedded smart meters:
  - Statically linked code
  - Explicit call and return instructions
  - Loose performance constraints
- Code size must be minimized!

Original function call:

```
push  A                  ; Save address
jmp   B                  ; Perform branch
```

Instrumented function call:

```
mov   D [key1_addr]  ; D = K_1
mov   C A            ; C = A
xor   C D            ; C = C XOR D
push  C              ; Save encrypted address
mov   D [key2_addr]  ; D = K_2
mov   C A            ;
xor   C D            ; Second redundant encryption
push  C              ;
mov   D [key3_addr]  ; D = K_3
mov   C A            ;
xor   C D            ; Third redundant encryption
push  C              ;
jmp   B              ; Perform branch
```

Meter Configuration

PENNSTATE 1855

Challenges / Updates

Deployment – Endpoint

- Electric meter supply chain secured
- 138 curb meters set with incorrect programming
- Early indication that 900 MHz may trip customer GFI
- Bakersfield substation bank work is requiring meter redeployment of about 29,000 endpoints

Risks	Impact
Implementation of new technology does not perform as intended. Key drivers: IT systems do not scale to meet volumes, Equipment fails at a higher rate than anticipated	Billing errors, customer complaints, inability to meet endpoint deployment goals

The project has been using interfaces which have not completed testing (60, 50, 104, 66, 67) to enable AMS Ops to discover and initialize installed meters. The conversion approach for the MDMS needs to be revisited to determine if the right approach is to "initialize" the MEM go live weekend, or use ORT to enable "cut-over".

PG&E

Summary

- Meter monocultures
  - Highly exposed nodes
  - Hard to configure
  - Same pandemic problem as other monocultures
- Diversity
  - Well understood exploit mitigation
  - Significantly slows large scale exploit attempts
  - Embedded diversity schemes will present their own challenges while facing less stringent performance requirements than traditional diversity techniques

Thank You

Seed Questions

• Are there suggestions for approaches besides diversity for mitigating large-scale meter exploitation?

• How could we reduce meter TCB, thus reducing the amount of code that needs to be diversified?

• Should we build redundant address encryption or explore additional diversity techniques?

http://www.cse.psu.edu/~smclaugh

http://siis.cse.psu.edu

Performance Considerations