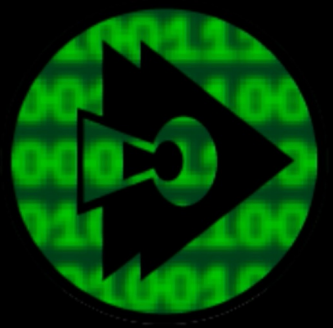
Enterprise Knights Insights



“Vulnerability Patterns for Authorized Code”

Scott Woolley, IBM Z Center for Secure Engineering

Enterprise Knights Insights

Scott Woolley, IBM Z Center for Secure Engineering

The Power of Authorized Code

APF

System Integrity Summary

It’s the property of a system that prevents the circumvention of security mechanisms

In z/OS, it’s the prevention of an unauthorized program from:

- Bypassing store or fetch protection
- Bypassing SAF/RACF protection
- Obtaining control in an authorized state

The APIs of Authorized Code

The upcoming vulnerability patterns are focused on

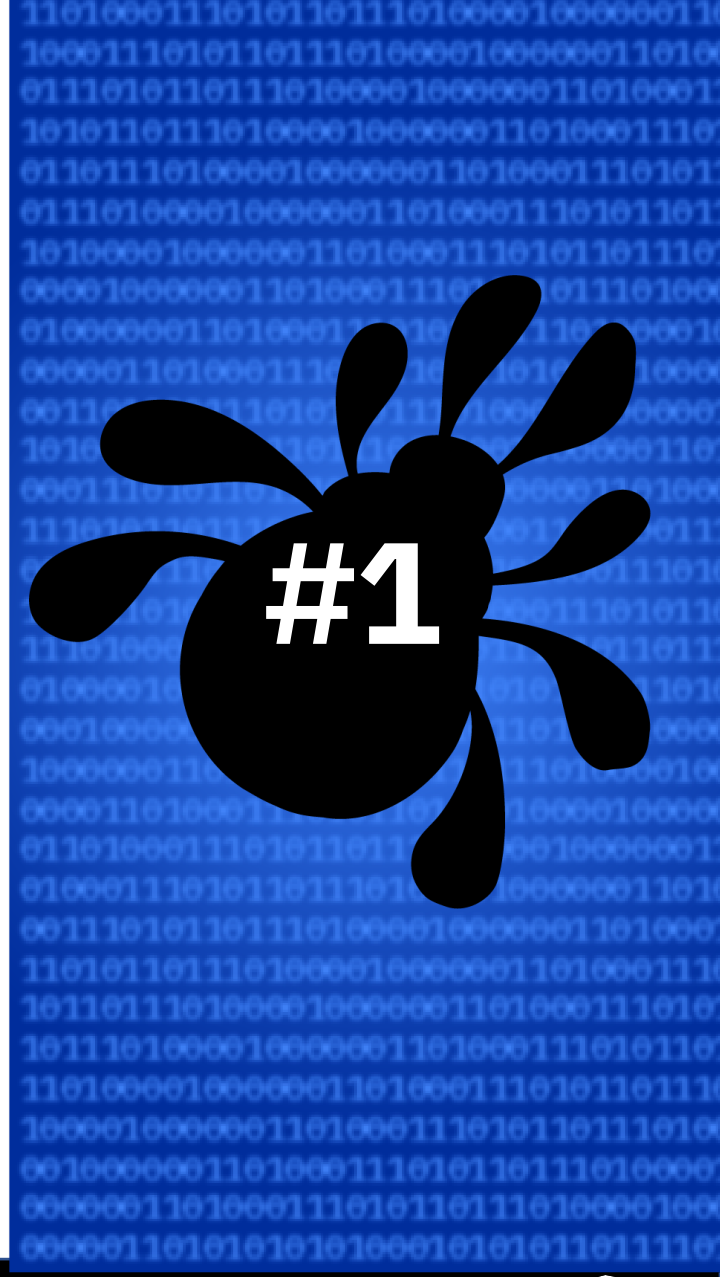
- Program Calls (PCs)
- Supervisor Calls (SVCs)

These APIs need to use special instructions such as

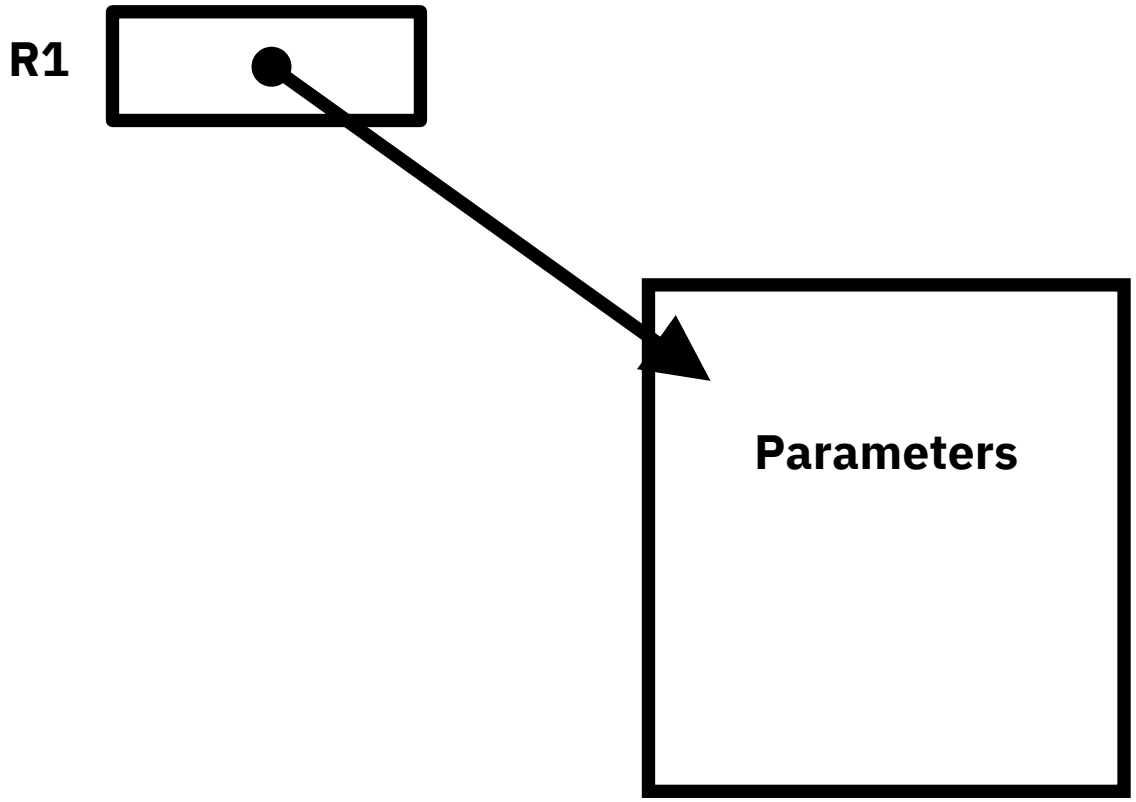
- MVCSK
- MVCDK

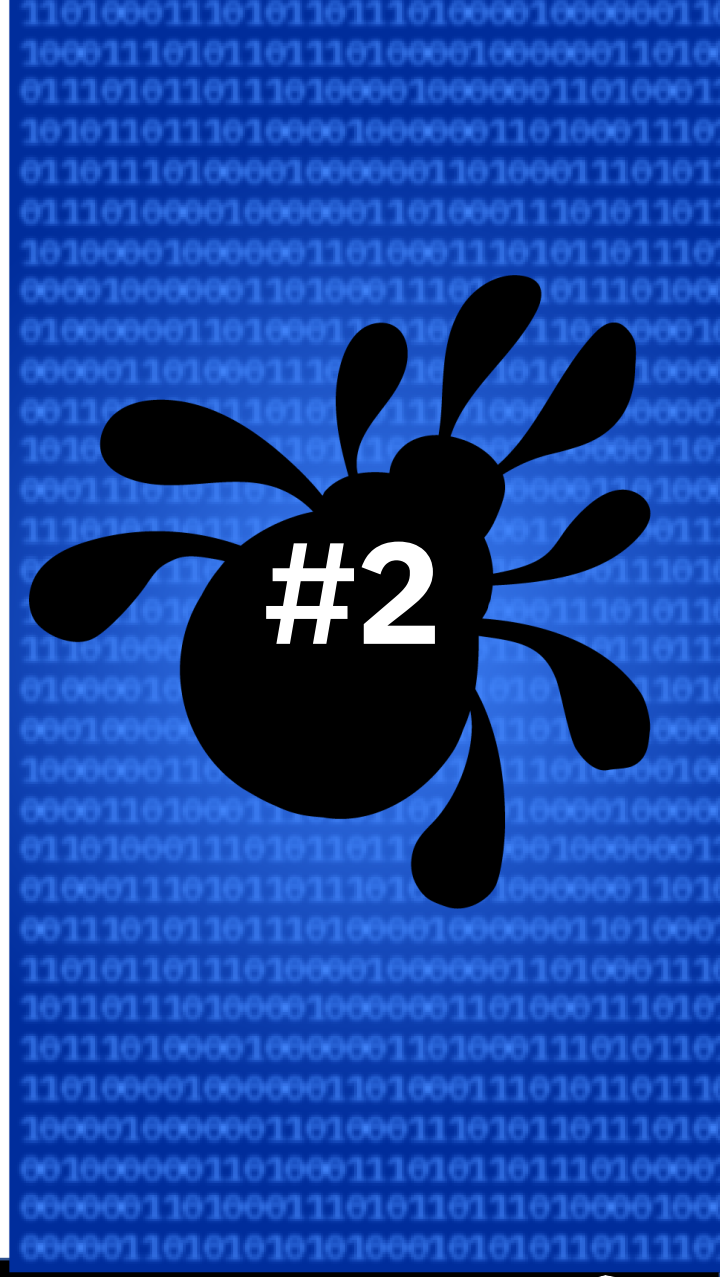
#1 - The Unintentionally Authorized PC

A critical keyword of the ETDEF service:
AKM (Authorization Key Mask)

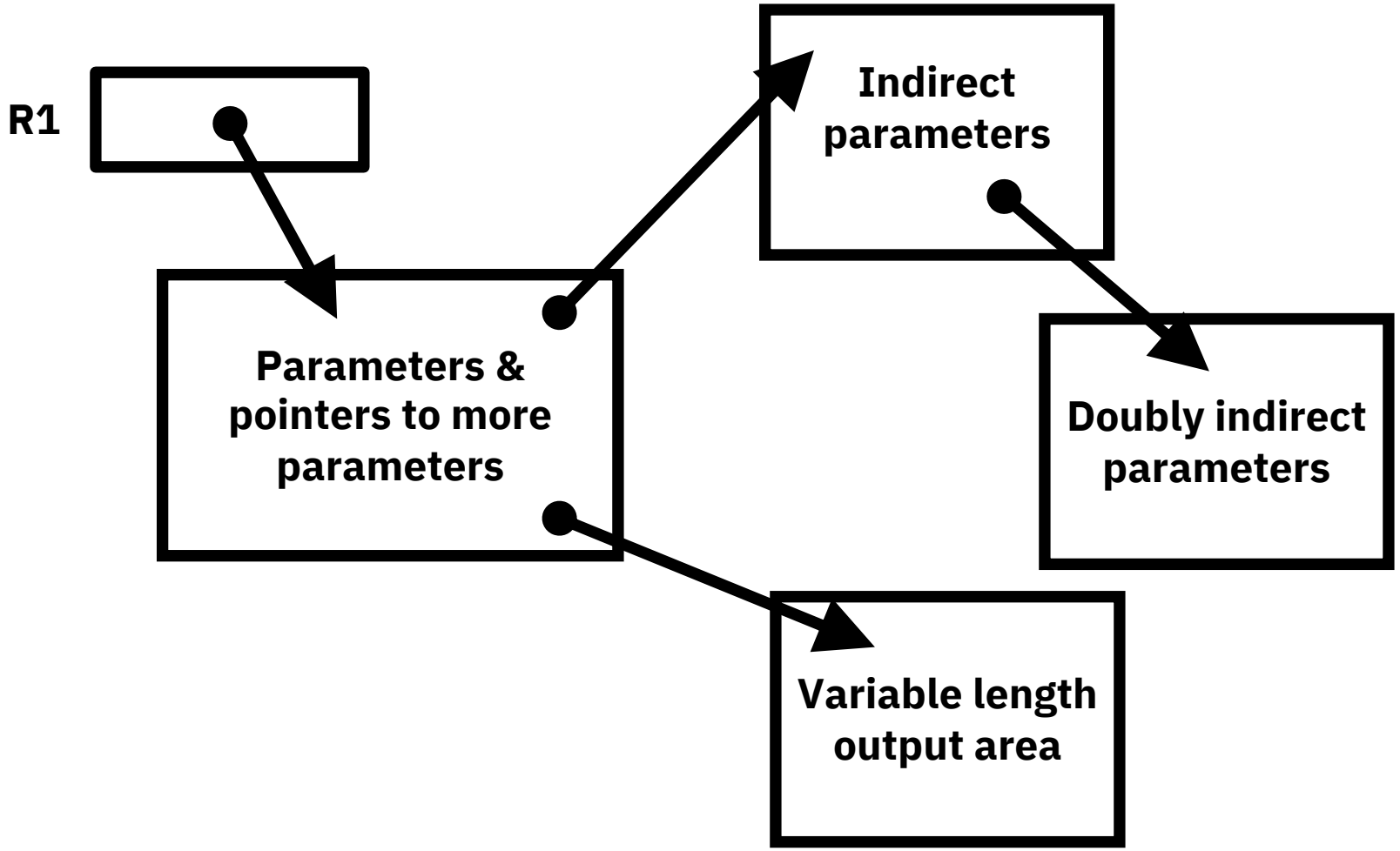


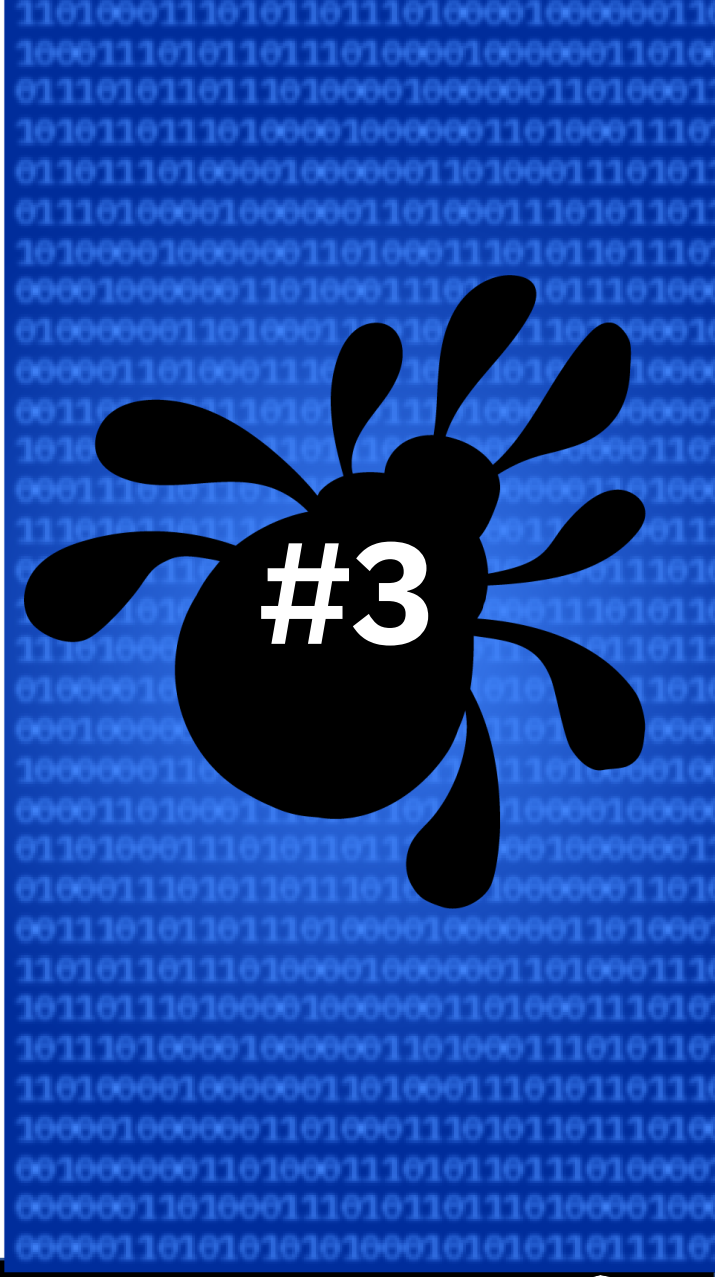
#2 – Generally Untrusted Registers



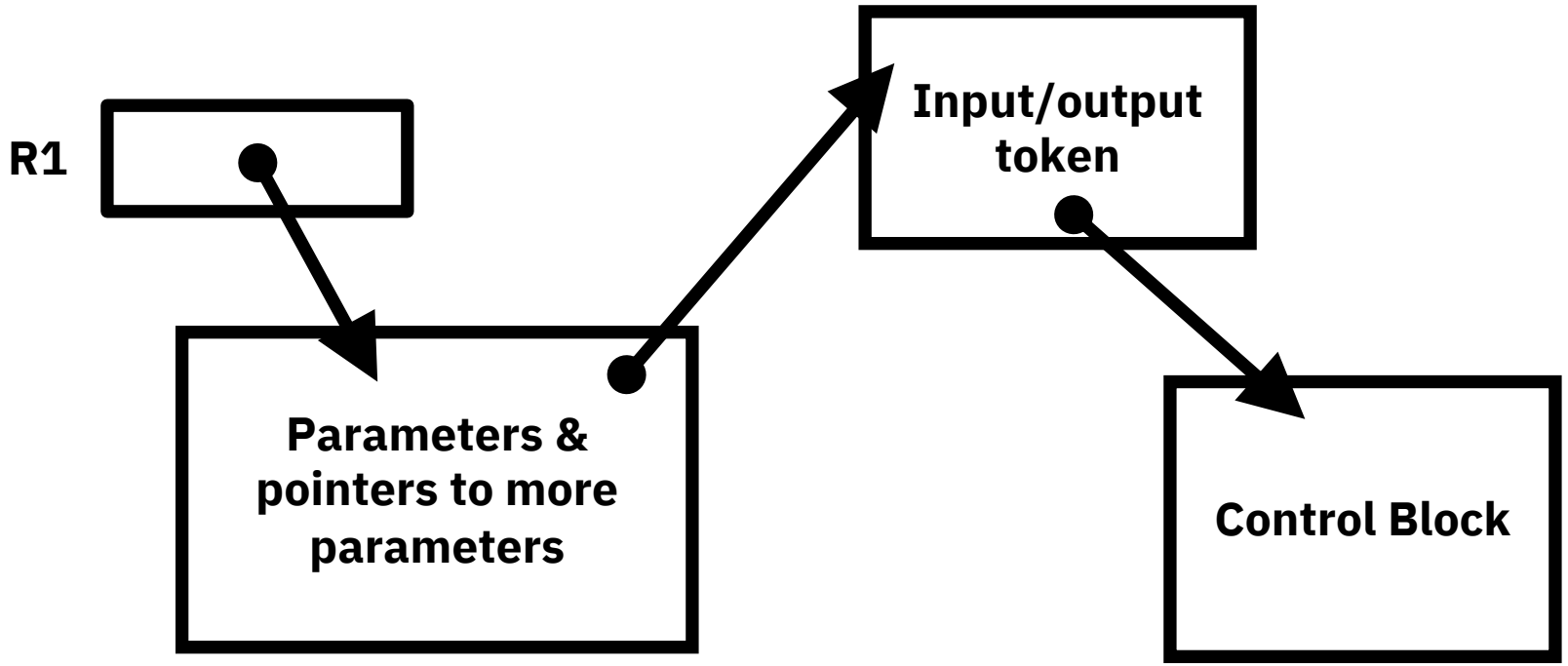


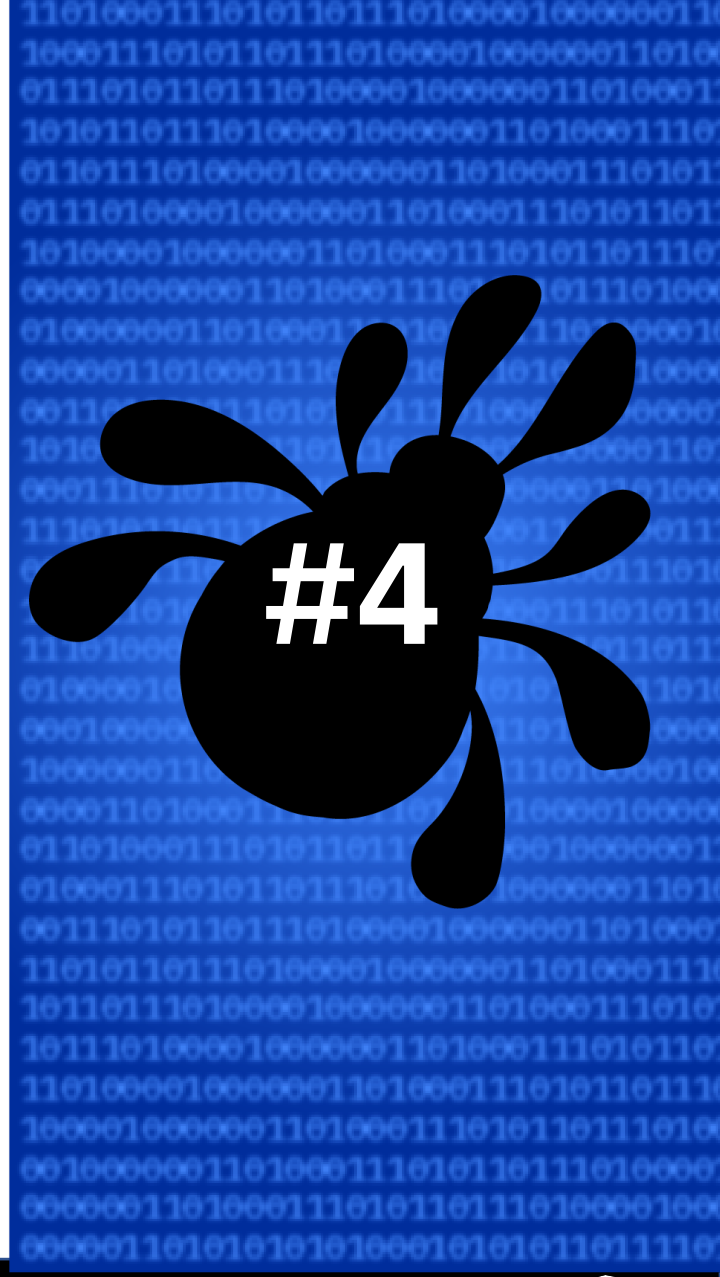
#3 –Untrusted Indirect Parameters



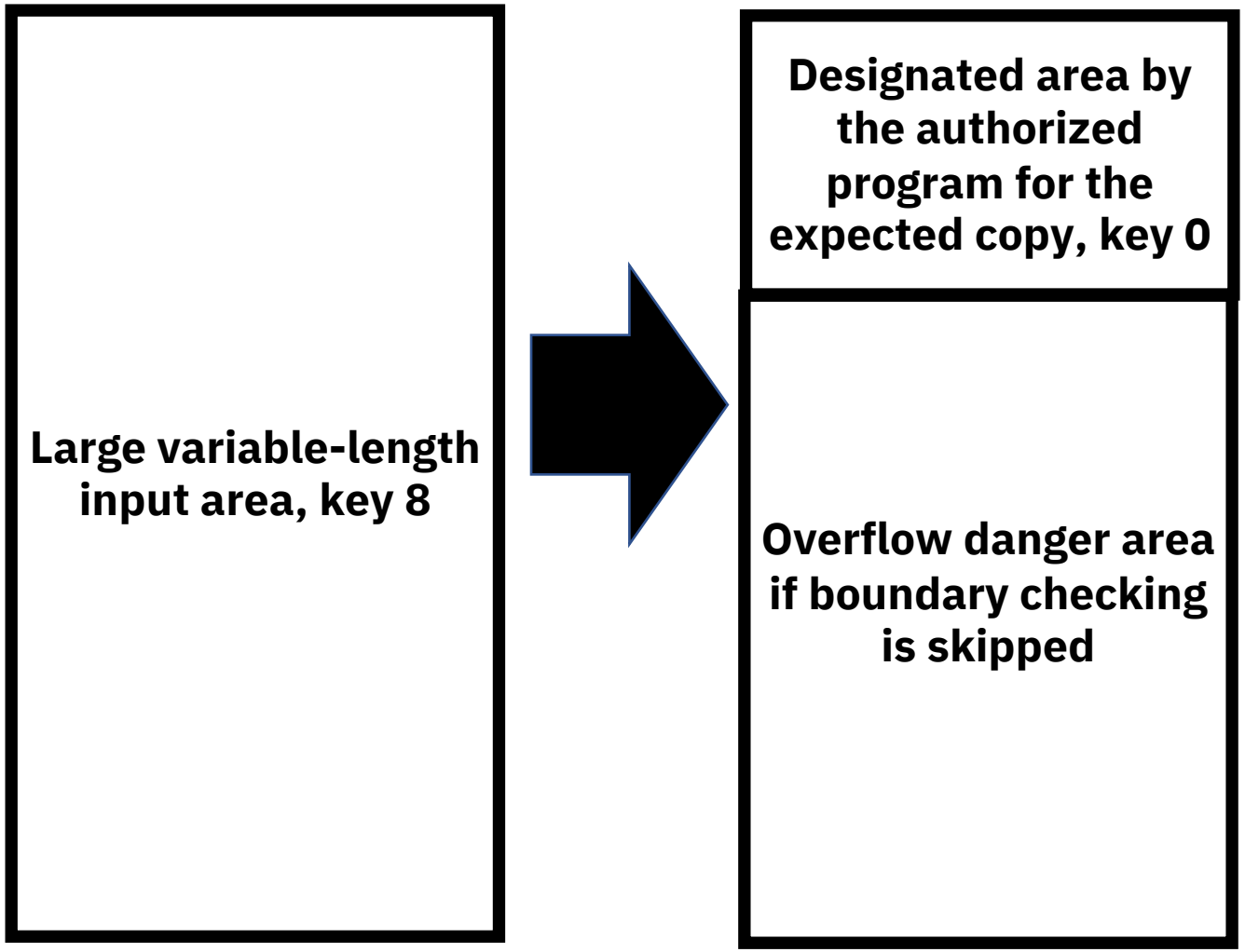


#4 – Control Block Masquerade





#5 – The Buffer Overflow

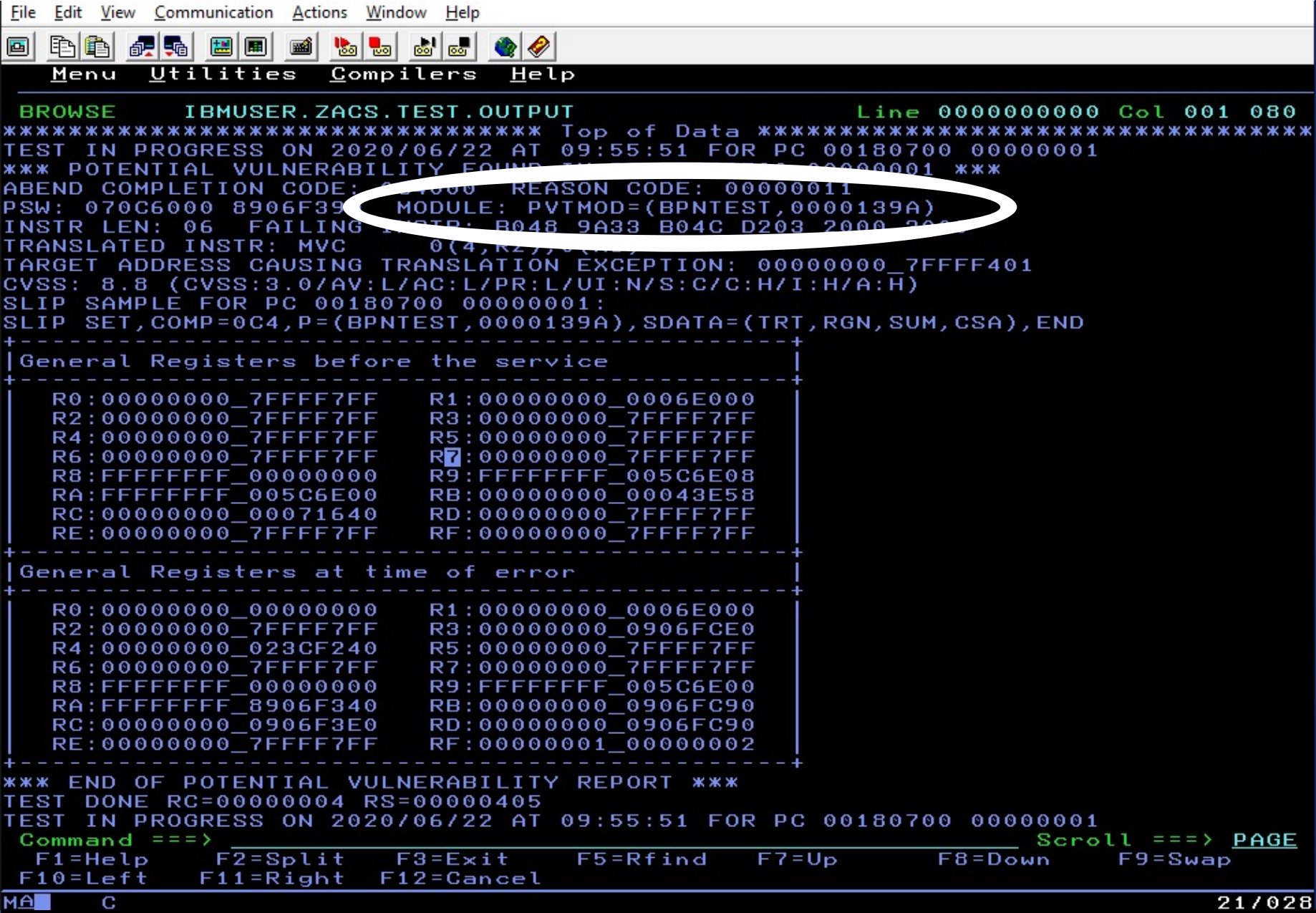


The IBM Z and LinuxONE Security Portal

IBM utilizes internal and external sources to uncover potential vulnerabilities. IBM Z offers a Security Portal that allows clients to stay informed about patch data, associated Common Vulnerability Scoring System (CVSS) ratings for new APARs and Security Notices to address highly publicized security concerns.
See more at: https://www.ibm.com/it-infrastructure/z/capabilities/system-integrity

The IBM z/OS Authorized Code Scanner

zACS



Enabling the feature

The **IBM z/OS Authorized Code Scanner (zACS)** dynamically scans the client's authorized code and provides diagnostic information for subsequent investigation as needed. Upon purchase or as part of a proof-of-concept agreement, it is activated via IFAPRDxx in parmlib:

```
PRODUCT OWNER('IBM CORP')
NAME('z/OS')
ID(5650-ZOS)
VERSION(*)
RELEASE(*)
MOD(*)
FEATURENAME('ZACS')
STATE(ENABLED)
```

Documentation can be found here: www.ibm.biz/zacskc2020

See URL:
https://www.ibm.com/legal/copytrade
for a list of trademarks

The Mike Kelly character, the Mock-Up Service Enterprises business, and associated events mentioned in this video are fictitious. Any resemblance to actual persons, living or dead, or actual events is purely coincidental. When a subject matter expert is introduced, the illustration does depict an actual person, and any message from that illustration is an audio recording of that person's voice. The information in this video is provided as is and without warranty of any kind. Following the instructions does not guarantee your system will be secure. You remain responsible for the security of your system.

The Enterprise Knights of IBM Z

A user group within the IBM Z and LinuxONE Community
providing insights to cyber security & resiliency

www.ibm.biz/ek-ibm-z