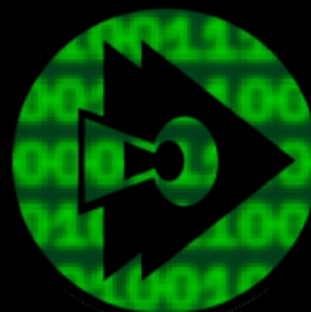


Enterprise Knights Insights



“Vulnerability Patterns for Authorized Code”

Scott Woolley, IBM Z Center for Secure Engineering

Copyright 2022 IBM Corporation

Enterprise Knights Insights



Scott Woolley, IBM Z Center for Secure Engineering

Copyright 2022 IBM Corporation

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

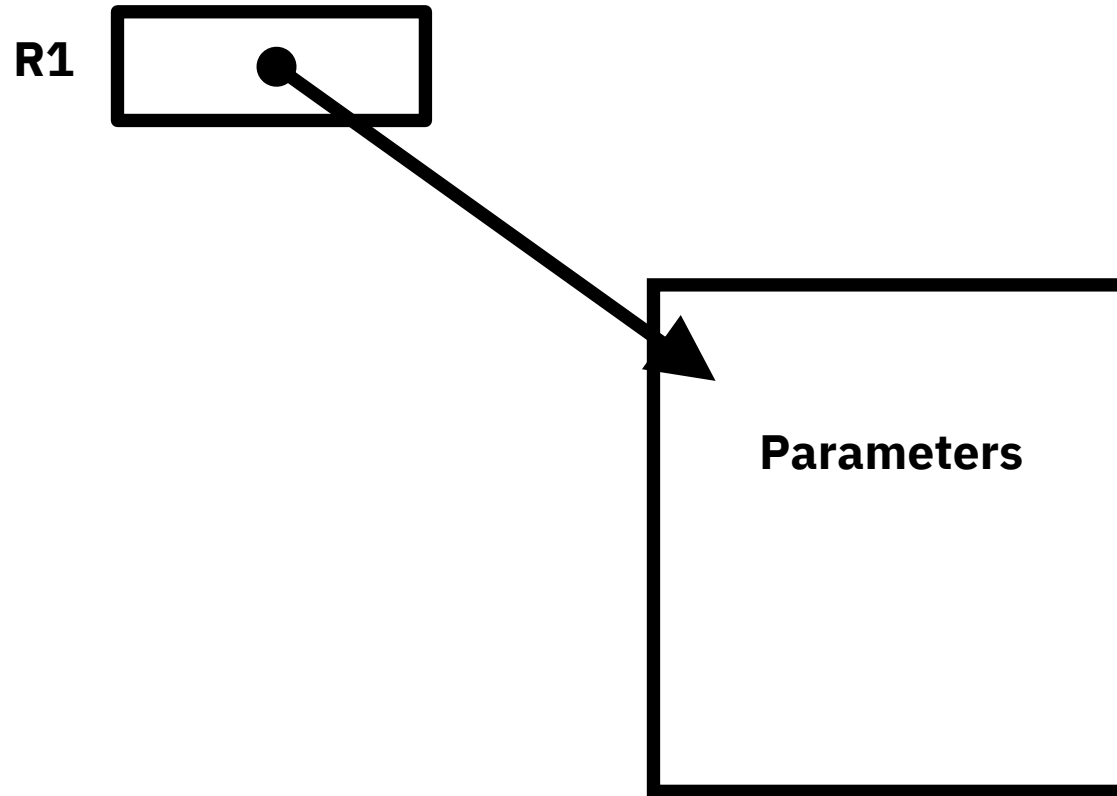


#1 - The Unintentionally Authorized PC

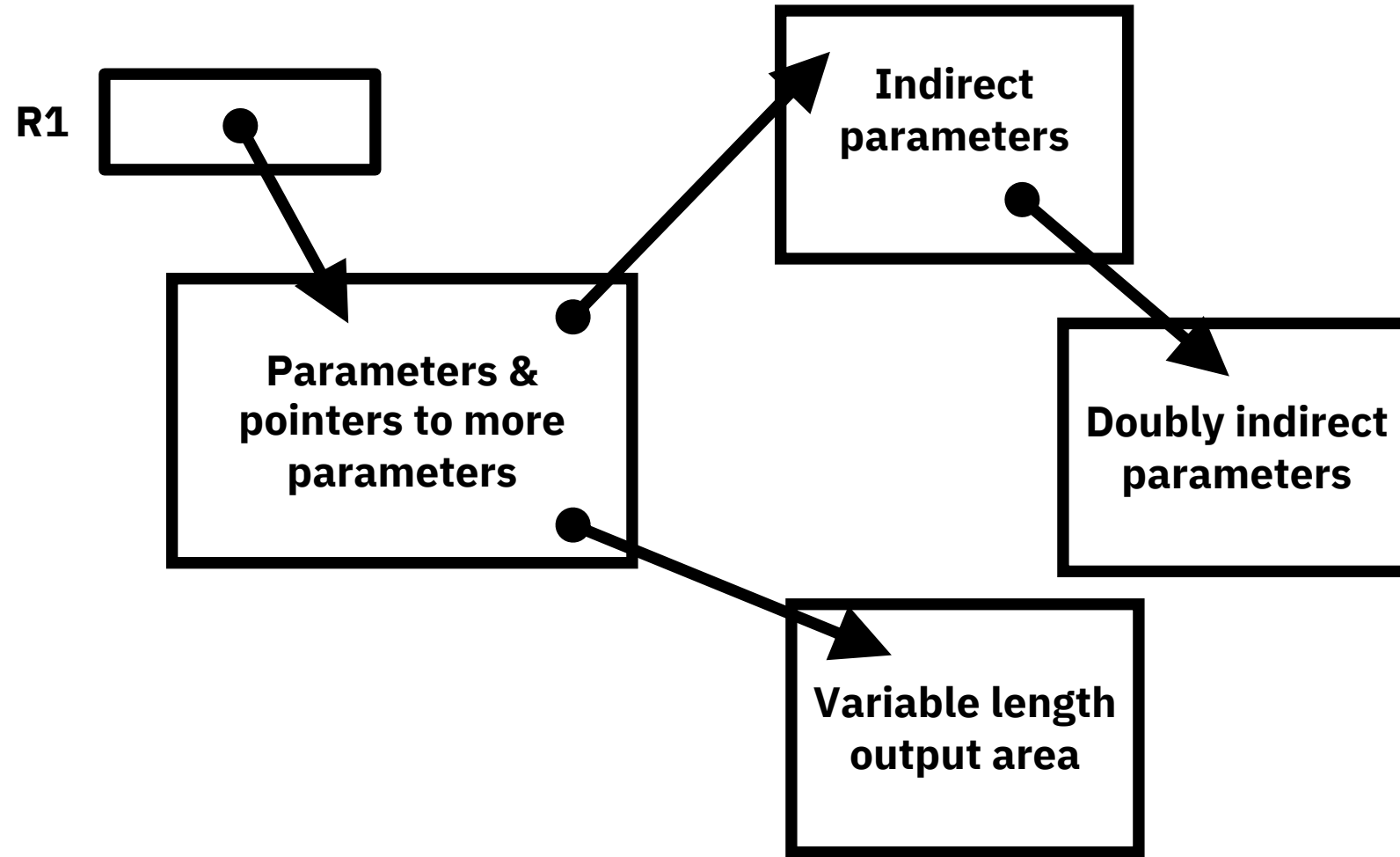
A critical keyword of the ETDEF service:
AKM (Authorization Key Mask)



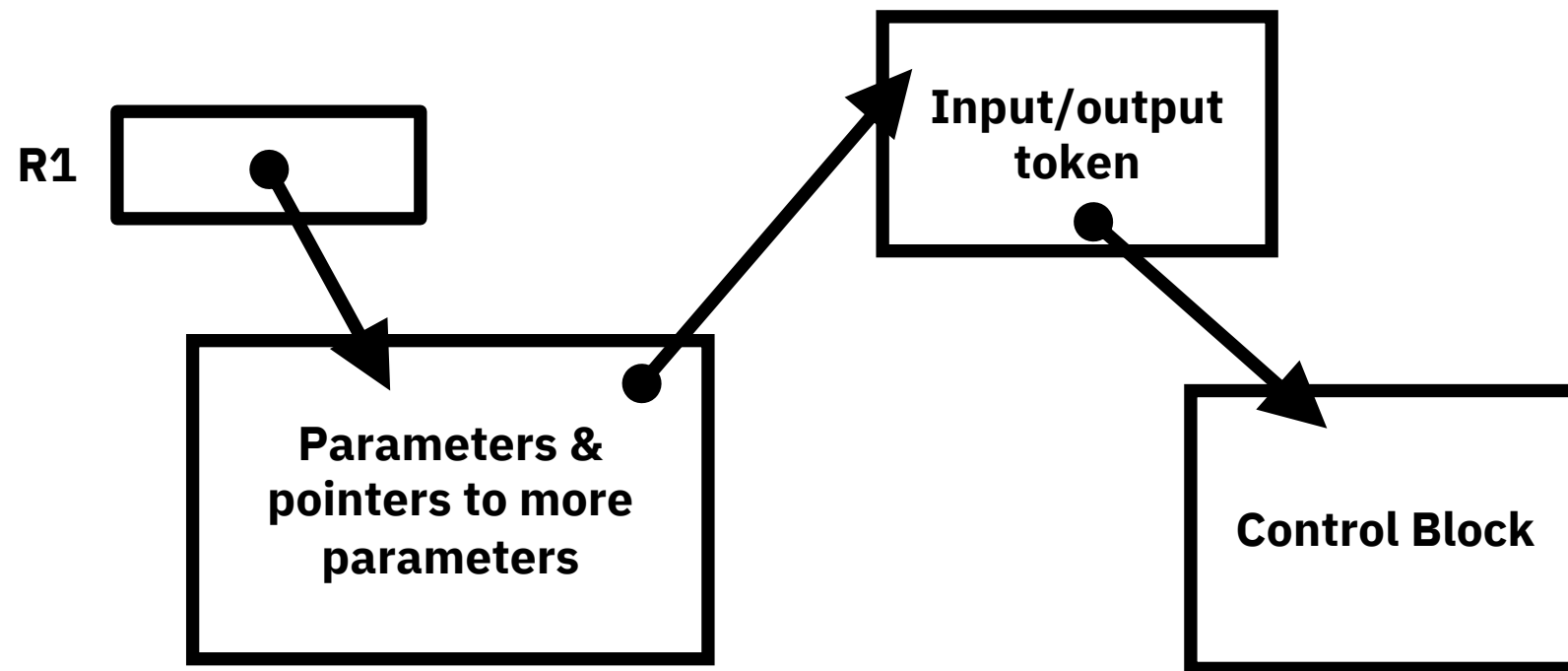
#2 – Generally Untrusted Registers



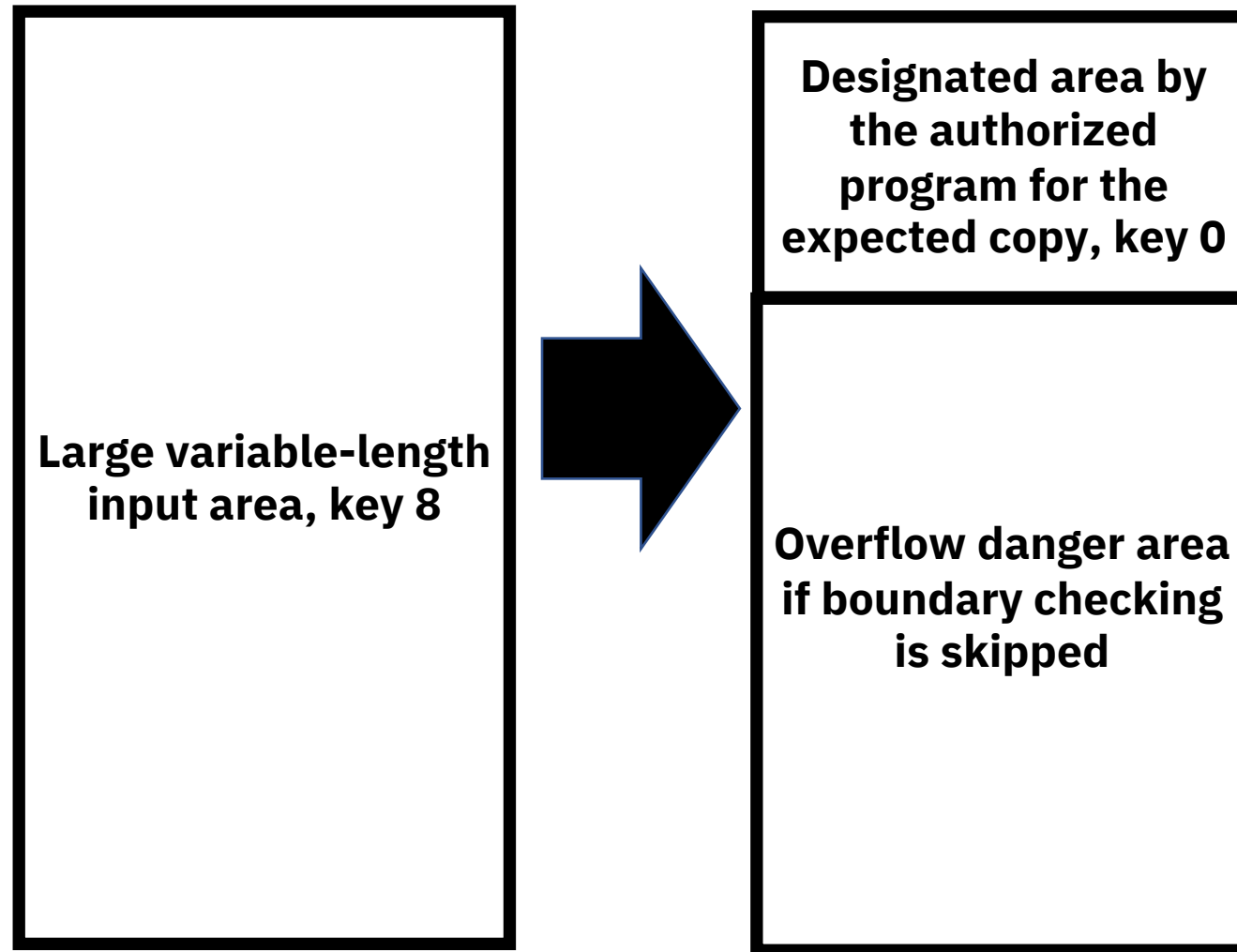
#3 –Untrusted Indirect Parameters



#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>



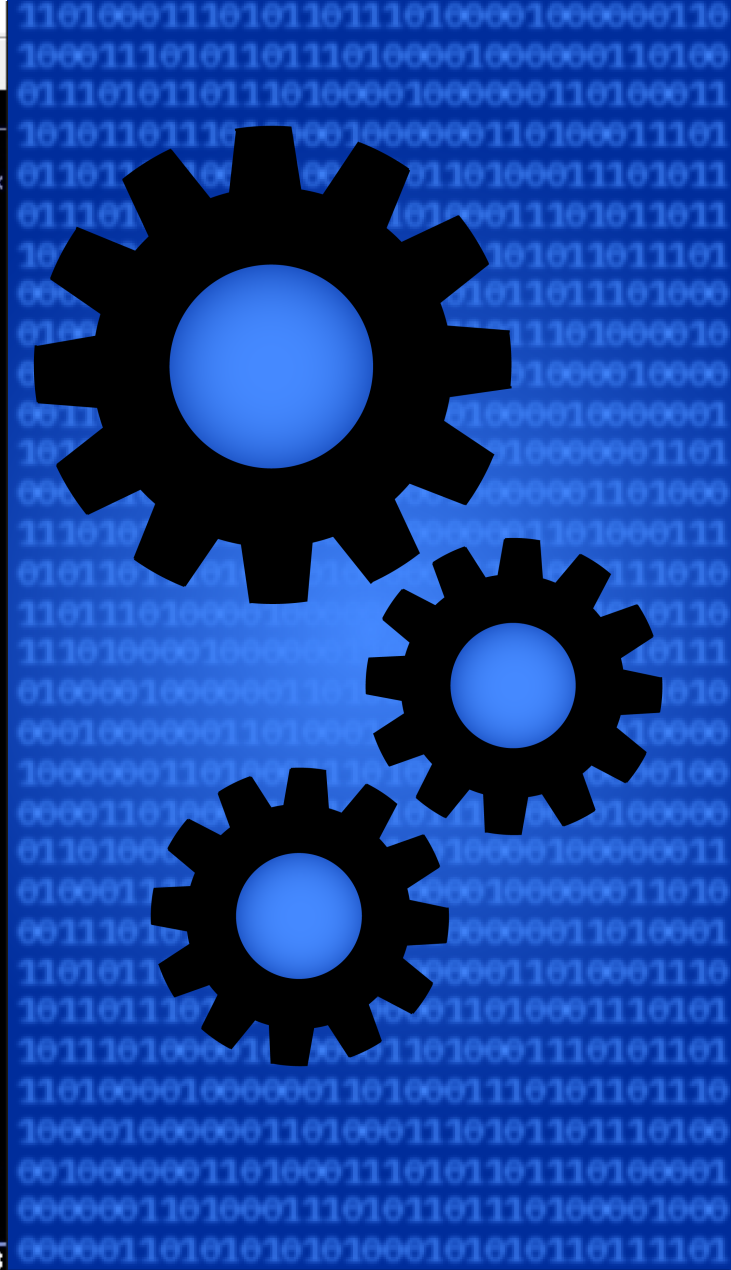
The IBM z/OS Authorized Code Scanner

ZACS



```
File Edit View Communication Actions Window Help
Menu Utilities Compilers Help

BROWSE IBMUSER.ZACS.TEST.OUTPUT Line 0000000000 Col 001 080
***** Top of Data *****
TEST IN PROGRESS ON 2020/06/22 AT 09:55:51 FOR PC 00180700 00000001
*** POTENTIAL VULNERABILITY FOUND ***
ABEND COMPLETION CODE: 00000000 REASON CODE: 00000011
PSW: 070C6000 8906F390 MODULE: PVTMOD=(BPNTST,0000139A)
INSTR LEN: 06 FAILING INSTR: B048 9A33 B04C D203 2000 3000
TRANSLATED INSTR: MVC 0(4,R2),R1
TARGET ADDRESS CAUSING TRANSLATION EXCEPTION: 00000000_7FFFF401
CVSS: 8.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)
SLIP SAMPLE FOR PC 00180700 00000001:
SLIP SET,COMP=0C4,P=(BPNTST,0000139A),SDATA=(TRT,RGN,SUM,CSA),END
+-----+
|General Registers before the service|
+-----+
R0:00000000_7FFFF7FF R1:00000000_0006E000
R2:00000000_7FFFF7FF R3:00000000_7FFFF7FF
R4:00000000_7FFFF7FF R5:00000000_7FFFF7FF
R6:00000000_7FFFF7FF R7:00000000_7FFFF7FF
R8:FFFFFFFF_00000000 R9:FFFFFFFF_005C6E08
RA:FFFFFFFF_005C6E00 RB:00000000_00043E58
RC:00000000_00071640 RD:00000000_7FFFF7FF
RE:00000000_7FFFF7FF RF:00000000_7FFFF7FF
+-----+
|General Registers at time of error|
+-----+
R0:00000000_00000000 R1:00000000_0006E000
R2:00000000_7FFFF7FF R3:00000000_0906FCE0
R4:00000000_023CF240 R5:00000000_7FFFF7FF
R6:00000000_7FFFF7FF R7:00000000_7FFFF7FF
R8:FFFFFFFF_00000000 R9:FFFFFFFF_005C6E00
RA:FFFFFFFF_8906F340 RB:00000000_0906FC90
RC:00000000_0906F3E0 RD:00000000_0906FC90
RE:00000000_7FFFF7FF RF:00000001_00000002
+-----+
*** END OF POTENTIAL VULNERABILITY REPORT ***
TEST DONE RC=00000004 RS=00000405
TEST IN PROGRESS ON 2020/06/22 AT 09:55:51 FOR PC 00180700 00000001
Command ==> Scroll ==> PAGE
F1=Help F2=Split F3=Exit F5=Rfind F7=Up F8=Down F9=Swap
F10=Left F11=Right F12=Cancel
```



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.

Copyright 2022 IBM Corporation

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

Copyright 2022 IBM Corporation