DEPUTY FOR
MC COMMAND AND
MANAGEMENT SYSTEMS

MULTICS SECURITY EVALUATION

MULTICS SECURITY EVALUATION

INTRODUCTION

PROJECT ZARF

RECOMMENDATIONS/CONCLUSIONS

DISCUSSION

ERASA DURE

MC DEPUTY FOR COMMAND AND MANAGEMENT SYSTEMS	INTRO MULTICS SECURITY EVALUATION

MILITARY REQ - SECURE COMPUTER SYSTEM

PROJECT 6917 - TECHNOLOGY AVAIL

MULTICS - CANDIDATE

EVALUATION - MULTICS SECURITY

ZARF

AFSC / ESD

REQUIREMENT FOR
MILITARY SECURE SYSTEMS

MILITARY REQUIREMENT FOR SECURE COMPUTER SYSTEMS

DEDICATED SYSTEMS - SINGLE JOB - CLOSED ENVIRONMENT

MULTI-PROCESSING, MULTIUSER - OPEN ENVIRONMENT

SEVERAL LEVELS OF CLASSIFICATION - SIMULTANEOUS

UNCLASSIFIED USER - TOP SECRET USER

ADD ON SECURITY DESIGN - PROTECTS BENIGN USER

MULTI-LEVEL & NEED TO KNOW - NOT UNLIKE PRIVACY ISSUE

ZARF

AFSC / ESD

PROJECT 6917

AIR FORCE DATA SERVICE CENTER REQUIREMENT FOR SECURE MULTILEVEL USER ENVIRONMENT

COMPUTER SECURITY TECHNOLOGY PANEL - FINDINGS BY GROUP OF EXPERTS FROM UNIV, INDUSTRY & DOD

- CURRENT SYSTEMS - AD HOC DESIGN
- CURRENT SYSTEMS - PENETRATED - ERRORS TRAPDOORS
- TECHNOLOGY AVAILABLE TO SOLVE PROBLEM
- CERTIFICATION - ABSOLUTE NECESSITY

AFSC / ESD

CERTIFICATION / EXISTING SYSTEM

CERTIFICATION

- TIGER TEAMS - STUDENT - SHOW & TELL
- MALICIOUS USER - COVERT
- SECURE KERNEL - HARDWARE & SOFTWARE

EXISTING SYSTEMS SHOW PROMISE

- VIRTUAL MACHINE - IBM 370
- HARDWARE STATES & SEGMENTATION - PDP II/45
- RING STRUCTURE & VIRTUAL MEMORY - MULTICS

ZARF

AFSC / ESD

MULTICS / CANDIDATE

MULTICS - CANDIDATE SYSTEM - WHY THREE BRIEFINGS

RECOMMEND FOR AF DATA SERVICE CENTER

AVAILABLE - RADC / MIT

HONEYWELL - VENDOR

REPORT OF EFFORTS IS REQUIRED

CLAIMS FOR SECURITY - NEED TO UNDERSTAND PROBLEM

PROTECTED INFORMATION - SO FAR

AFSC/ ESD

PROJECT ZARF

PROJECT ZARF

UNDER P-6917 - SUPPORT AFDCS

USE ONLY WITH BENIGN USERS

WHAT'S IN A NAME -- ZARF

INVESTIGATION - MITRE TASKS RADC COMPUTER

SOFTWARE - HARDWARE - PROCEDURES

NEXT PRESENTATION - PURPOSE

NOT AN "IDES OF MARCH" ISSUE

UNDERSTAND WHAT MALICIOUS USER CAN DO

CARE WAS USED

ERASA DURE

AFSC / ESD

SECURITY VULNERABILITY ANALYSIS

PURPOSE

DEMONSTRATE WEAKNESS OF AD HOC APPROACH

AREAS

SOFTWARE - INTEGRITY OF CONTROLS

HARDWARE - ACCESS CHECKING

PROCEDURAL - SCRAMBLED PASSWORDS

APPROACH (LIMITED EFFORT)

ONE EXAMPLE IN EACH AREA -- IF POSSIBLE

POSTULATE WEAKNESS

EXPERIMENT ON RADC SITE

EXPLOITATION TECHNIQUES

CHANGE SDW ACCESS

CHANGE PROCESS ID

INSERT TRAPDOORS

ACCESS PASSWORDS

AFSC / ESD

SOFTWARE VULNERABILITY

AREAS CONSIDERED

- INSUFFICIENT ARGUMENT VALIDATION
  - TALLY GIVES MULTIPLE CASES
    FEBRUARY 1973
    FIXED AT MIT
- MASTER MODE TRANSFER
  - IN USER RING
    JUNE 1972 - 1 CRASH
- UNLOCKED STACK BASE
  - CONVENTION CHANGED AFTER DESIGN
    OCTOBER 1972 - 2 CRASHES
    DUMPS FOR ANALYSIS

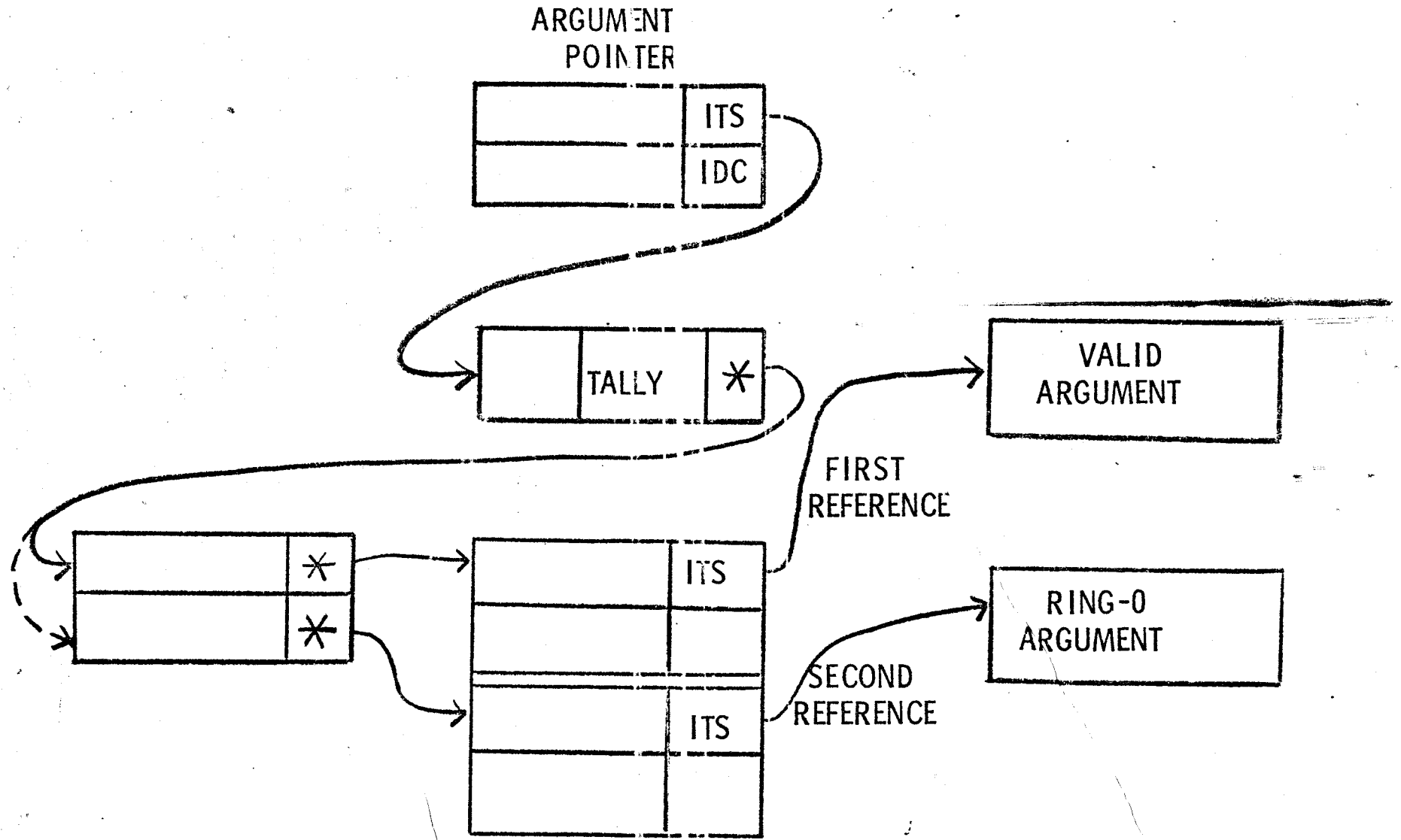
EXPLOITATION

- PATCH AND DUMP UTILITIES
  - CHANGE SDW ACCESS
- USE TO CHANGE PROCESS ID
  - COPY PASSWORD FILE (PNT)

ZARF

AFSC / ESD

INSUFFICIENT ARGUMENT VALIDATION



ERASA DURE

ZARF

AFSC / ESD

MASTER MODE TRANSFER

SET UP CONDITIONS:

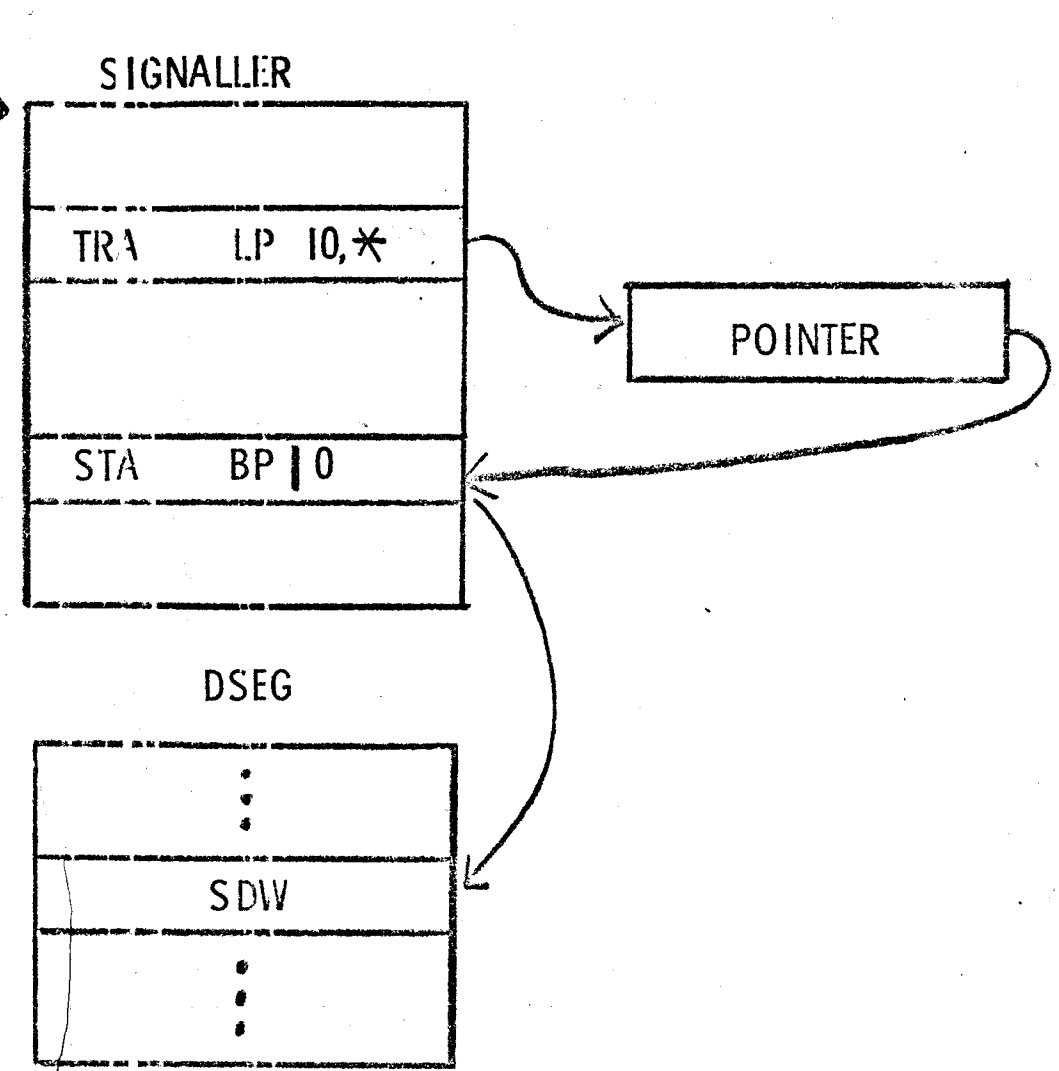
A - REG HAS SDW

INDEX REG 0 INVALID

LP ⟶ POINTER

POINTER ⟶ MM STORE

BP ⟶ SDW TO CHANGE



ERASA DURE

ZARF

AFSC/ESD	UNLOCKED STACK BASE (INITIATE)

ENTER

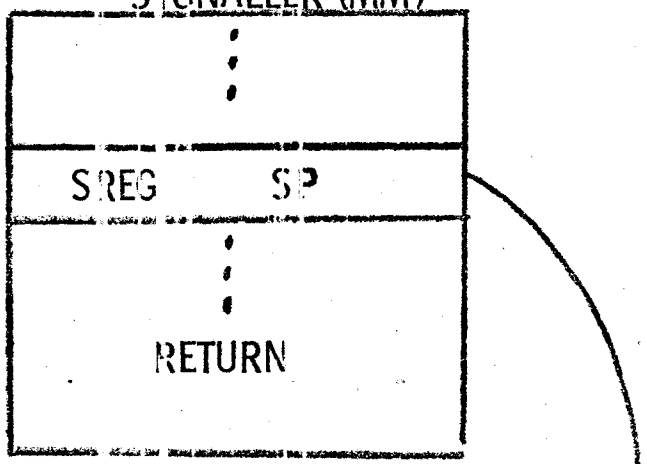
SIGNALLER (MM)

SET UP CONDITIONS:

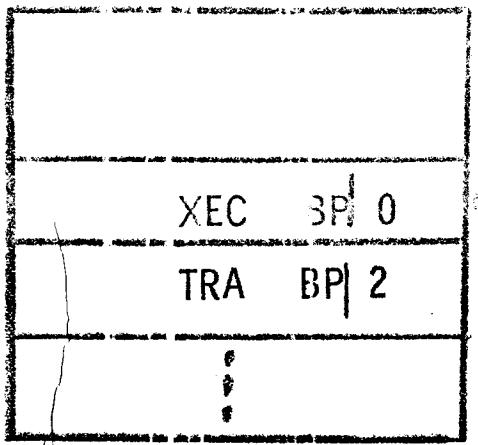
INDEX REG 0 INVALID

A-Q REG HAS XEC/TRA

SP → MM PROCEDURE



ESD.LINK (MM)



ERASA DURE

ZARF

AFSC / ESD	UNLOCKED STACK BASE (EXECUTE)

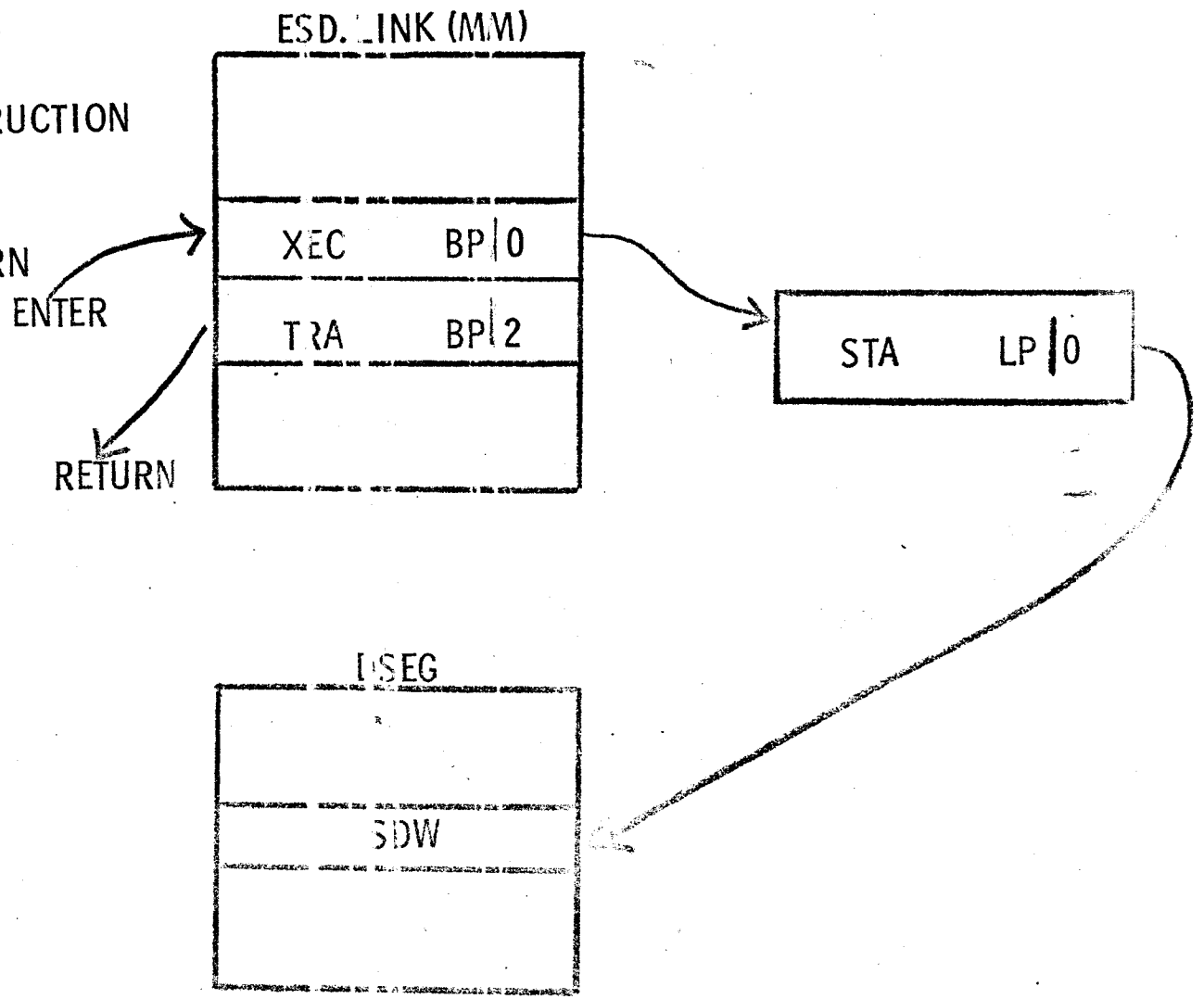
SET UP CONDITIONS:

BP |0 → INSTRUCTION

BP |2 → RETURN

A - REG HAS SDW

LP → SDW



ERASA DURE

ZARF

AFSC / ESD

HARDWARE VULNERABILITY

AREAS CONSIDERED

- NO RANDOM FAILURES DETECTED
  - SAMPLED EACH MINUTE
  - UNDOCUMENTED INSTRUCTION
- INCOMPLETE ACCESS CHECKING
  - EXECUTE INSTRUCTION BYPASSES
  - DECEMBER 1972

EXPLOITATION

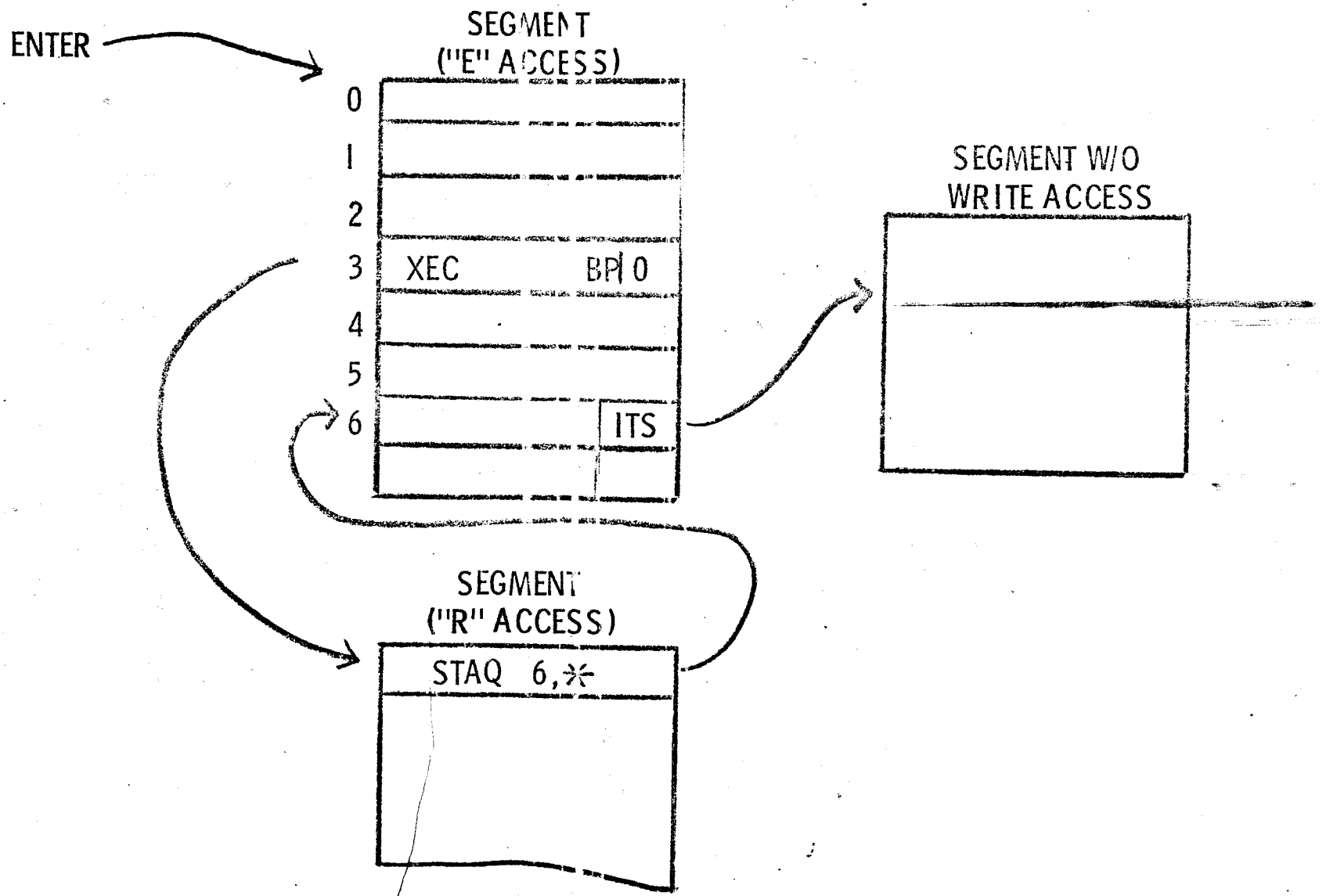
- DIRECT CHANGE OF PROCESS ID
  - CHANGE LIBRARY

ERASA DURE

ZARF

AFSC / ESD

HARDWARE ACCESS VIOLATION



ERASA DURE

ZARF

AFSC/ESD

PROCEDURAL VULNERABILITY

AREAS CONSIDERED

AUDITING INEFFECTIVE

DATES FORGED
PROCESS WITHOUT LOGIN

SYSTEM CONFIGURATION MODIFIABLE

ONCE PENETRATED, NO RECOVERY
OCTOBER 1972 (GIOC - CHECK)

SCRAMBLED PASSWORDS

0.04 SEC TO INVERT
NOVEMBER 1972

EXPLOITATION

PASSWORD LIST AND UPDATES

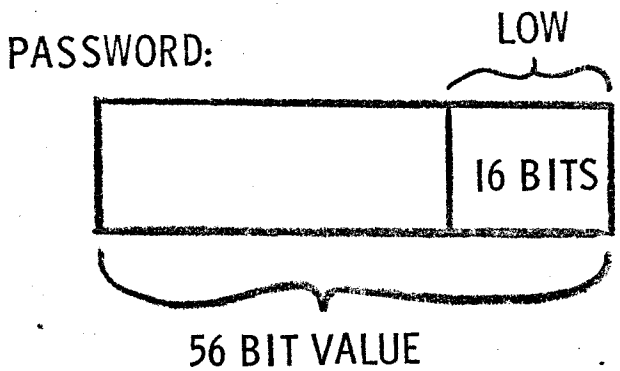
TRAP DOOR INSERTION

PRODUCTION, DISTRIBUTION, INSTALLATION
OBJECT CHANGES - INVISIBLE
SOURCE CHANGES - LASTING
KEY STRING TRIGGER - TTY
ESCAPE LIMITED SUBSYSTEM
COMPILERS, ETC.

ZARF

AFSC / ESD

PASSWORD INVERSION (SCRAMBLER)



C = (10**19) -1

MMOD ≡ "MARTIAN" MOD
(SAVE NORMALIZED 63 BITS)

M* ≡ "MARTIAN" MULTIPLY
(SAVE LOWER 72 BITS)

SCRAMBLED = MMOD (LOW M* VALUE, C)

NOTE THAT LOWER 16 BITS FORM A PERFECT SQUARE

"THE TRANSFORM IS SUPPOSED TO BE NON-INVERTIBLE.
I AM NOT SURE IT IS."

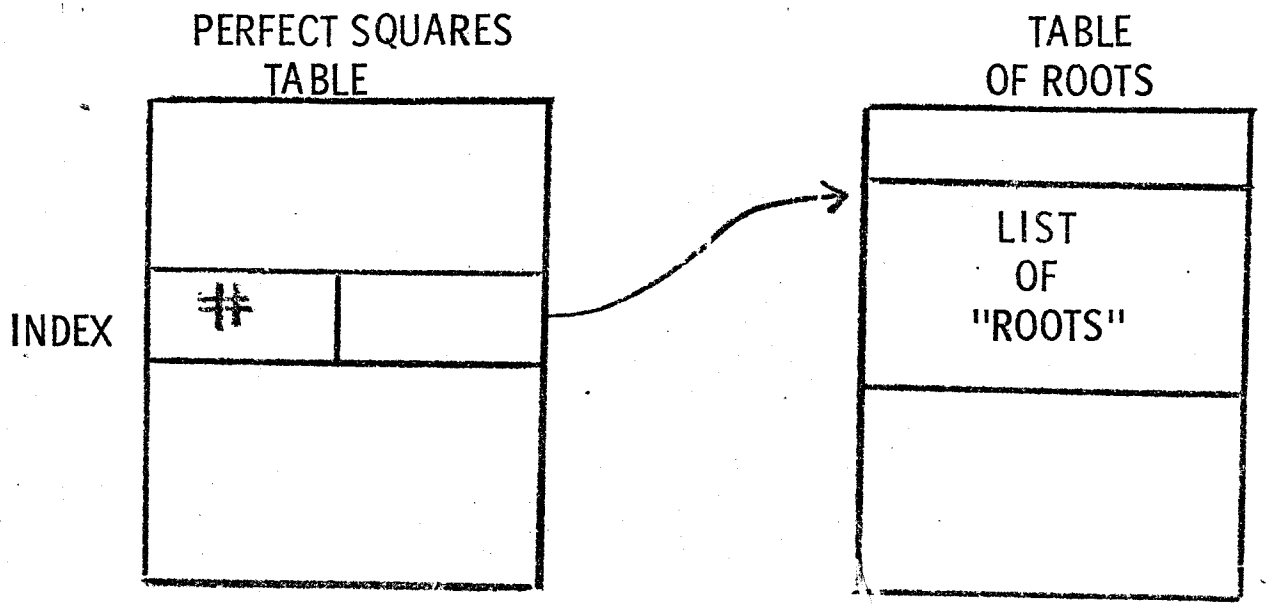
(REF: PL/I LISTING COMMENT)

ERASA DURE

ZARF

AFSC / ESD

PASSWORD INVERSION



INDEX = LOWER 16 BITS OF SCRAMBLED

SEARCH FOR "N" (< 256) SUCH THAT:
(N * C + SCRAMBLED) / ROOT = ROOT (LOWER 16 BIT)

PASSWORD

ERASA DURE

ZARF

AFSC / ESD

CONCLUSIONS

MINIMUM EFFORT GAVE EXAMPLES

- SOFTWARE
- HARDWARE
- PROCEDURE

STRONG CLAIMS NOT CURRENTLY WARRANTED

CARELESSNESS - NOT FUNDAMENTAL WEAKNESSES

SUPERVISOR TOO LARGE FOR CERTIFICATION

ERASA DURE

AFSC / ESD

RECOMMENDATIONS

- INCLUDE FLEXIBILITY FOR GOVERNMENT REQUIREMENTS
  - SEGMENT & PROCESS ATTRIBUTES
  - "HIGH WATER MARK" DESIRABLE
  - "TROJAN HORSE" PROTECTION DESIRABLE
- EARNEST REVIEW FOR VULNERABILITIES
  - NEEDED EVEN FOR BENIGN ENVIRONMENT
  - MULTICS STRUCTURE MAKES MEANINGFUL
    - REVIEW GATES & ARGUMENTS
    - INTERSEGMENT REFERENCES
    - IDENTIFY SECURITY SENSITIVITY
- FOR LONG TERM, RESTRUCTURE SUPERVISOR
  - ESSENTIAL FOR MALICIOUS USERS
  - APPLY FUNDAMENTAL PRINCIPLES
  - INCLUDE GOVERNMENT CERTIFICATION
- USE IMPROVED SCRAMBLER

MULTICS SECURITY

WHERE DO WE GO?

D72-1-696

- WHAT HAVE WE SEEN ?
- WHAT CAN THERE BE ?
- WHAT ARE THE STEPS ?

SOURCE
MITRE

MULTICS SECURITY

WHAT HAVE WE SEEN?

- IMPLEMENTATION ERRORS/OMISSIONS
  - HARDWARE
- MINOR AD HOC DESIGN -- MAJOR IMPACT
  - STACK POINTERS
  - ARGUMENT LISTS
- FEATURES AND SECURITY BLANKETS
  - PASSWORD SCRAMBLING
  - AUDITING

MULTICS SECURITY

WHAT HAVE WE SEEN?

- RELATION TO OTHER SYSTEMS
  - IF ITS TAKEN, ITS TAKEN
  - BUT SEEMS "MORE SECURE" THAN MOST

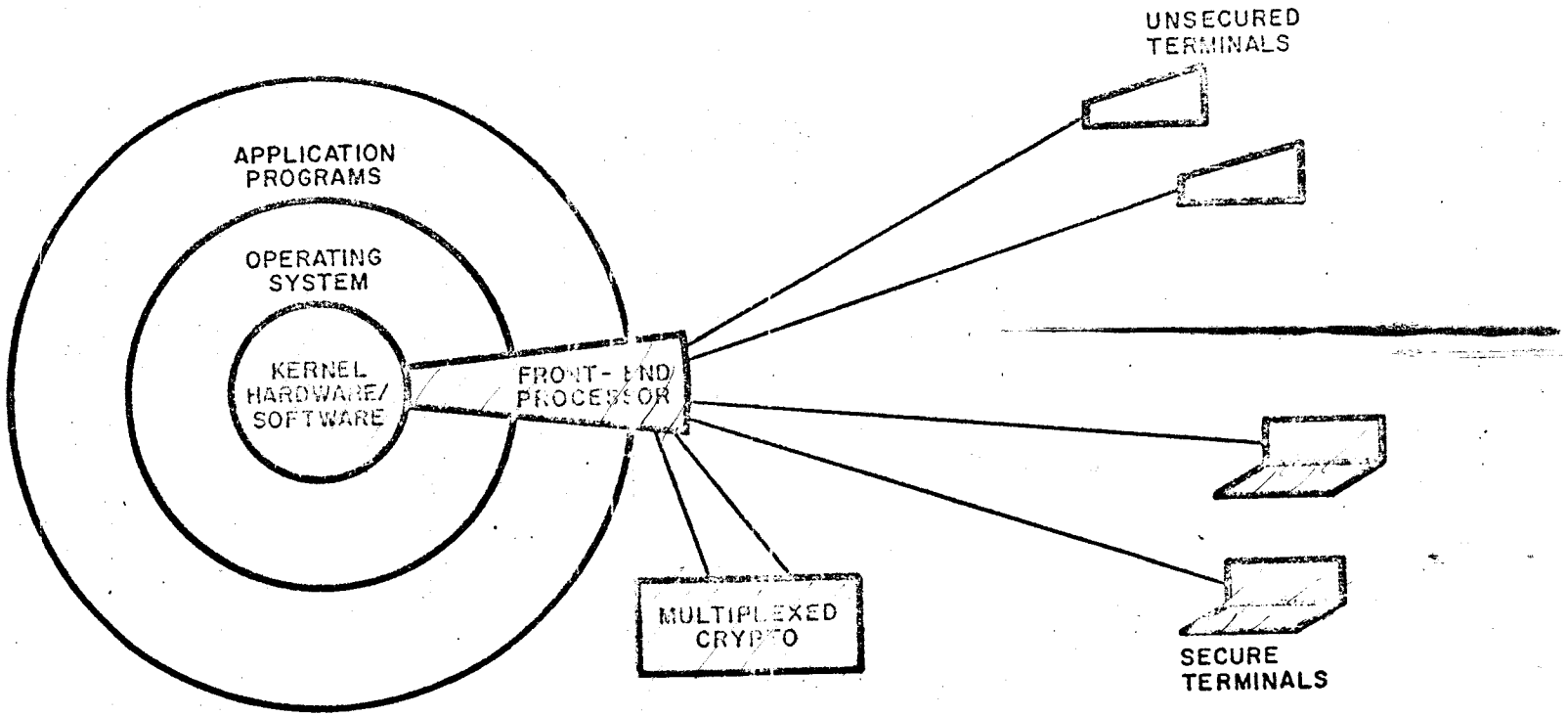
MULTICS SECURITY

WHAT CAN THERE BE?

D7[illegible]-699

- SECURE SYSTEM REQUIRES
  - INTEGRATED SECURITY CONCEPT
  - BASIS FOR SYSTEM ORGANIZATION
  - CORRECT SOFTWARE
  - APPROPRIATE HARDWARE

INTEGRATED SECURE COMPUTER
SYSTEM COMPONENTS



SECURITY - RELATED (CERTIFIED) ELEMENTS

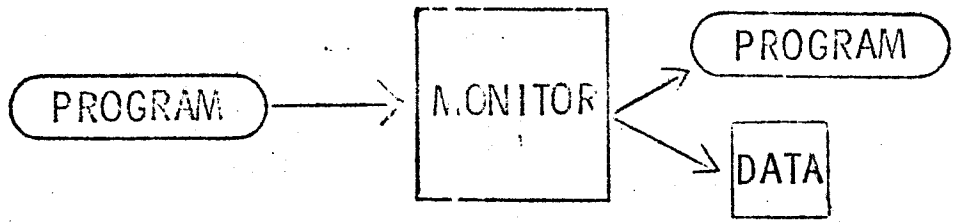
THE MITRE

COMPUTER SECURITY
R & D REQUIREMENTS

CENTRAL COMPUTER

PROJ.
VG. D72-V-553

- REFERENCE MONITOR PRINCIPLES
  - ACCESS CONTROLS TAMPERPROOF
  - ACCESS CONTROLS ALWAYS INVOKED
  - ACCESS CONTROLS SUBJECT TO EXHAUSTIVE TEST



DATE

MITRE FACILITY:

THE MITRE

COMPUTER SECURITY
R & D REQUIREMENTS

CENTRAL COMPUTER

PROJ.
VG. D72-V-612

CERTIFYING AND BUILDING A SECURE SYSTEM

- IDENTIFY
  - REFERENCE MONITOR REQUIREMENTS
  - SYSTEM BASE
  - PROCESS OPERATIONS
- MODEL
  - REFERENCE MONITOR
  - SYSTEM BY LAYERS
- IMPLEMENT KERNEL
  - STRUCTURED PROGRAMMING
  - PROOFS OF CORRECTNESS
- WRITE AND PUBLISH SPECIFICATIONS

THE MITRE

COMPUTER SECURITY
R & D REQUIREMENTS

CENTRAL COMPUTER

PROJ.
VG. D72-V-606

SYSTEM BASE

- SELECTED HARDWARE REQUIRED
- SEGMENTED VIRTUAL MEMORY WITH PER-SEGMENT ACCESS CONTROLS
  - UNIFORM PROGRAM ENVIRONMENT
  - MANAGEABLE LEVEL OF CONTROL
  - RAPID CHANGE OF PROTECTION ENVIRONMENT
- MULTIPLE EXECUTION STATES
  - ISOLATE KERNEL,
  - OPERATING SYSTEM,
  - USER PROGRAMS

MULTICS SECURITY — WHAT CAN THERE BE?

D72-V-700

- MULTICS VS. SECURE SYSTEM
  - HARDWARE APPEARS SUITABLE
  - CONCEPT OF SOFTWARE SOUND
  - BASIS FOR KERNEL, AND KERNEL IMPLEMENTATION REQUIRED

MULTICS SECURITY — WHAT ARE THE STEPS ?

D72-Y-701

- PROVIDE MULTICS ENHANCEMENTS
  - FIX THE DESIGN/IMPLEMENTATION PROBLEMS
  - ADD CLASSIFICATION AS AN EXPLICIT FACTOR
  - ISOLATE WEAK SPOTS (i/o) FROM USER
- OPERATE IN BENIGN LOW-RISK ENVIRONMENT

MULTICS SECURITY — WHAT ARE THE STEPS ?

D72-X-702

- DEVELOP "SECURE MULTICS"
  - MODEL
  - KERNEL
  - OPERATING SYSTEM
- APPLY AFDSC EXPERIENCE
  - USER INTERFACE
  - COMPATIBILITY REQUIREMENTS
  - FEATURES FOR SECURE ENVIRONMENT

SOURCE:
MITRE

MITRE FACILITY:

DATE

MULTICS SECURITY

CONCLUSION

D7_-V-703

- USE WITH CAUTION IN NEAR-TERM
- SUBMIT ROC TO DEVELOP OPEN SECURE SYSTEM THAT
  - APPLIES MULTICS INVESTMENT
  - EXPLOITS MULTICS EXPERIENCE
- APPLY TO WIDER COMMUNITY
  - AFDSC SYSTEMS
  - WWMCCS