LINCOLN LABORATORY INTRUSION DETECTION RESEARCH

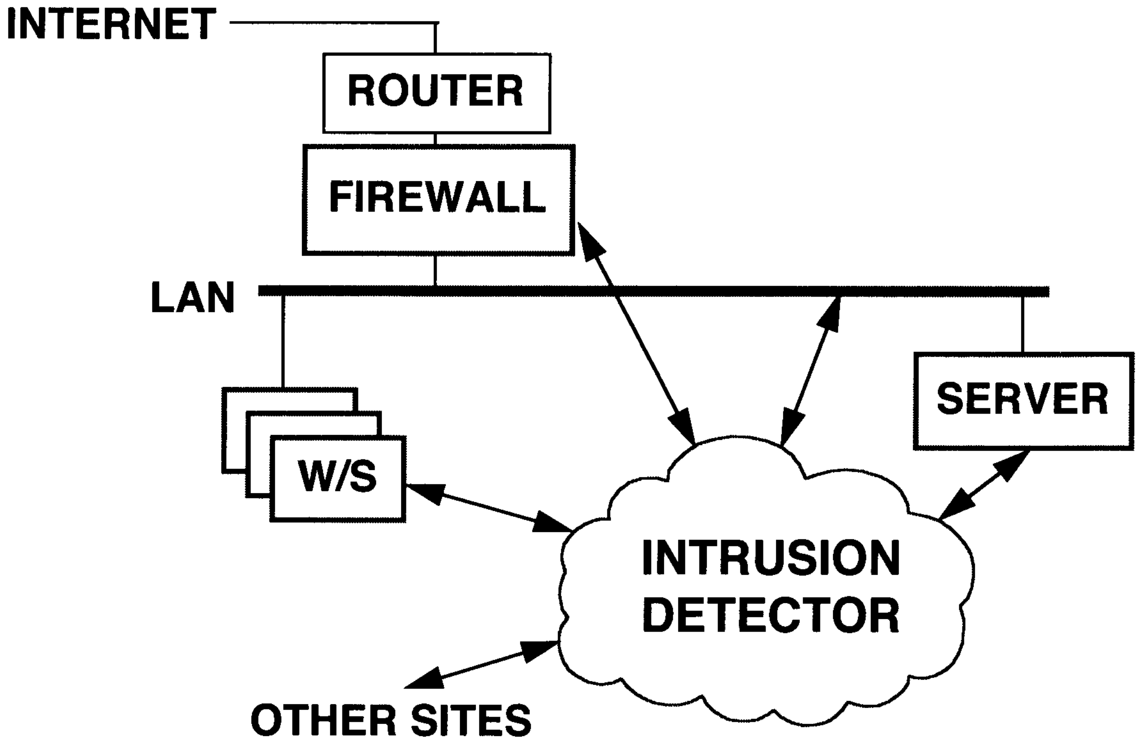
RICHARD P. LIPPMANN
617-981-2711 rpl@sst.ll.mit.edu

HAROLD M. HEGGESTAD
617-981-4014 hal@xn.ll.mit.edu

MIT LINCOLN LABORATORY
LEXINGTON, MA 02173

Presented at AFIWC
23 October 1996, San Antonio TX

A TEST AND EVALUATION ENVIRONMENT IS REQUIRED TO VERIFY THE PERFORMANCE OF INTRUSION DETECTION SYSTEMS



- •FEW OBJECTIVE COMPARISONS BETWEEN SYSTEMS
- •FEW OPERATIONAL PERFORMANCE ANALYSES
- •NO STANDARD COMPARISON METRICS
- •FEW STANDARD INTERFACES
- •FEW MODERN SYSTEMS IN OPERATIONAL USE

GOALS OF TEST AND EVALUATION WORK

- DEVISE OBJECTIVE APPROACH TO EVALUATE NEW INTRUSION DETECTION SYSTEMS
  - R&D RESULTS ARE DIVERSE AND INCOMMENSURABLE
  - HARD TO ASSESS SUITABILITY FOR DEPLOYMENT
- FOSTER INTEGRATION OF COMPLEMENTARY ID TECHNOLOGIES
  - IDENTIFY MUTUALLY SUPPORTIVE IDEAS
  - PERFORM EVALUATIONS AND ANALYSES
- EXPEDITE MIGRATION OF NEW TECHNOLOGIES INTO OPERATIONAL ID TOOLKITS
  - PROVIDE BRIDGE BETWEEN RESEARCH AND OPERATIONS
  - PERFORM TECHNOLOGY INSERTION AND DEMONSTRATION

APPROACH

- PERFORM UNBIASED COMPARISONS OF RESEARCH SYSTEMS
- DEVELOP AND APPLY STANDARD METRICS AND INTERFACES
- TEST IN REALISTIC GOVERNMENT APPLICATIONS WITH VARIED TYPES OF ATTACKS AND MISUSE MODELS
- CONTINUALLY INTERACT WITH THE RESEARCH COMMUNITY
- TRANSITION TO REALISTIC OPERATIONAL ENVIRONMENTS

TECHNICAL APPROACH

STEP 1: IMPLEMENT A TEST ENVIRONMENT

- ARCHITECTURE
- PERFORMANCE METRICS
- TEST DATA SET COLLECTION EXAMPLE
- OBTAIN BASELINE PERFORMANCE OF OPERATIONAL SYSTEM

STEP 2: TEST A SINGLE-SITE R&D SYSTEM

STEP 3: TEST ADDITIONAL SINGLE-SITE R&D SYSTEMS

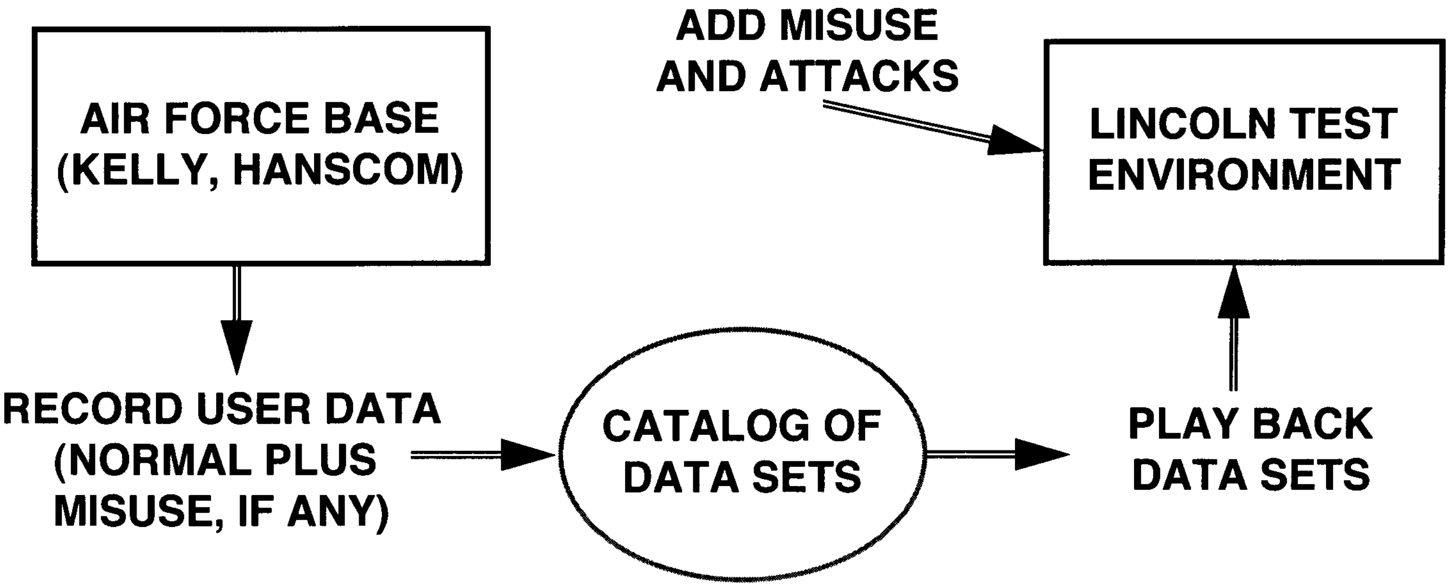
STEP 4: TEST MULTI-SITE R&D SYSTEMS

- •ONGOING:
  - FORM AND CHAIR A WORKING GROUP
  - TEST ADDITIONAL SYSTEMS
- •LONGER-TERM GOALS:
  - INSTALL R&D PRODUCTS IN GOVERNMENT APPLICATIONS
  - TRANSITION THE TEST AND EVALUATION ENVIRONMENT TO AN OPERATIONAL NATIONAL ASSET

TECHNICAL APPROACH, STEP 1: IMPLEMENT A BASELINE TEST ENVIRONMENT USING CURRENT TECHNOLOGY

- CREATE A TEST ENVIRONMENT AT LINCOLN LABORATORY
- USE AN EXISTING INTRUSION DETECTION TOOL (ASIM)
- BRING UP ASIM IN THE TEST ENVIRONMENT
  - EXPERIMENT WITH ITS FUNCTIONS AND CONTROLS
  - FIX ANY INTERFACING PROBLEMS
- APPLY RECORDED DATA FROM OPERATIONAL SITE
- DEVELOP AND APPLY ATTACK AND MISUSE MODELS
- EVALUATE BASELINE PERFORMANCE

DATA COLLECTION FROM OPERATIONAL AIR FORCE BASES



AIR FORCE BASE (KELLY, HANSCOM)

RECORD USER DATA (NORMAL PLUS MISUSE, IF ANY)

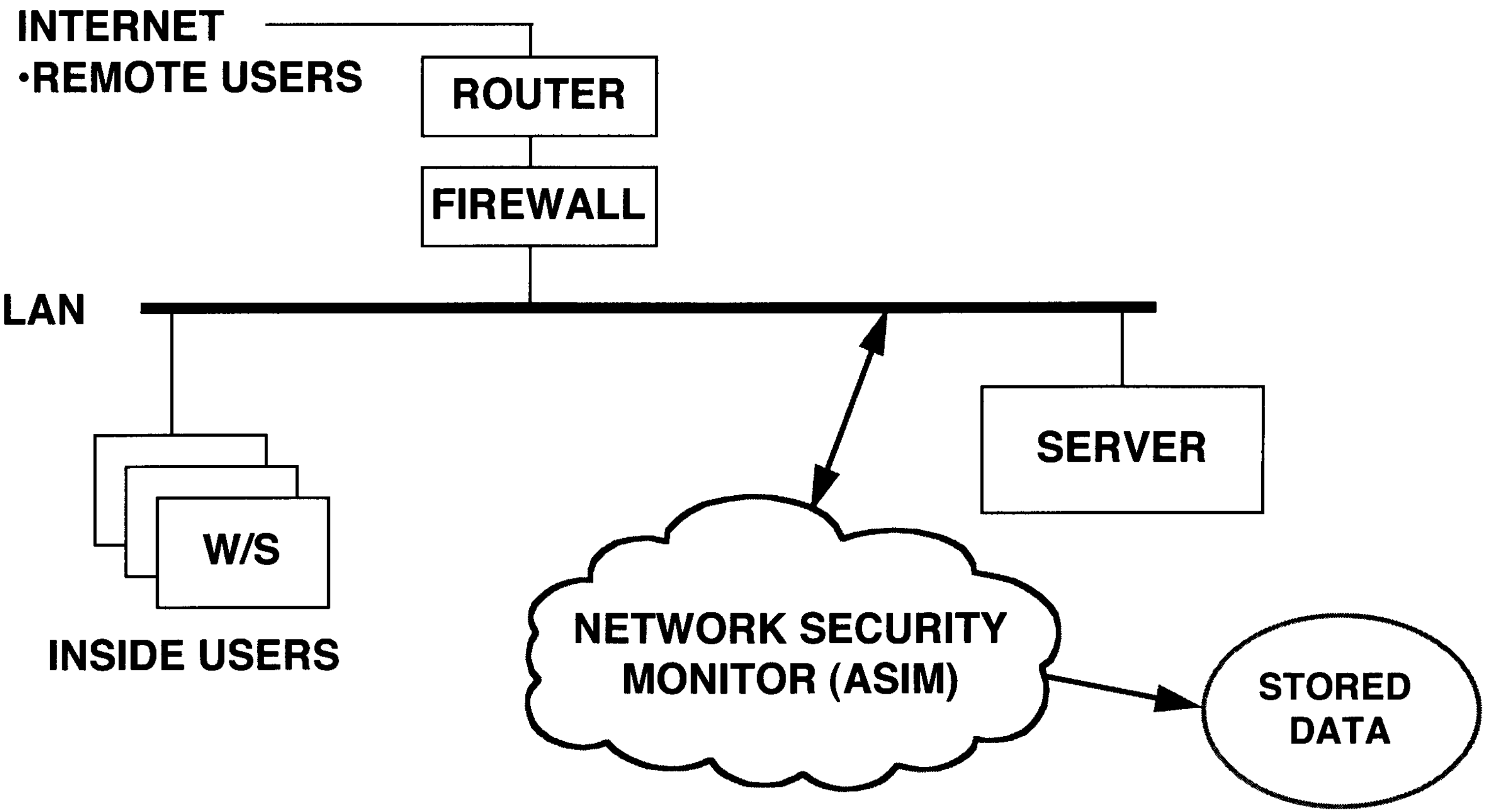
CATALOG OF DATA SETS

PLAY BACK DATA SETS

ADD MISUSE AND ATTACKS

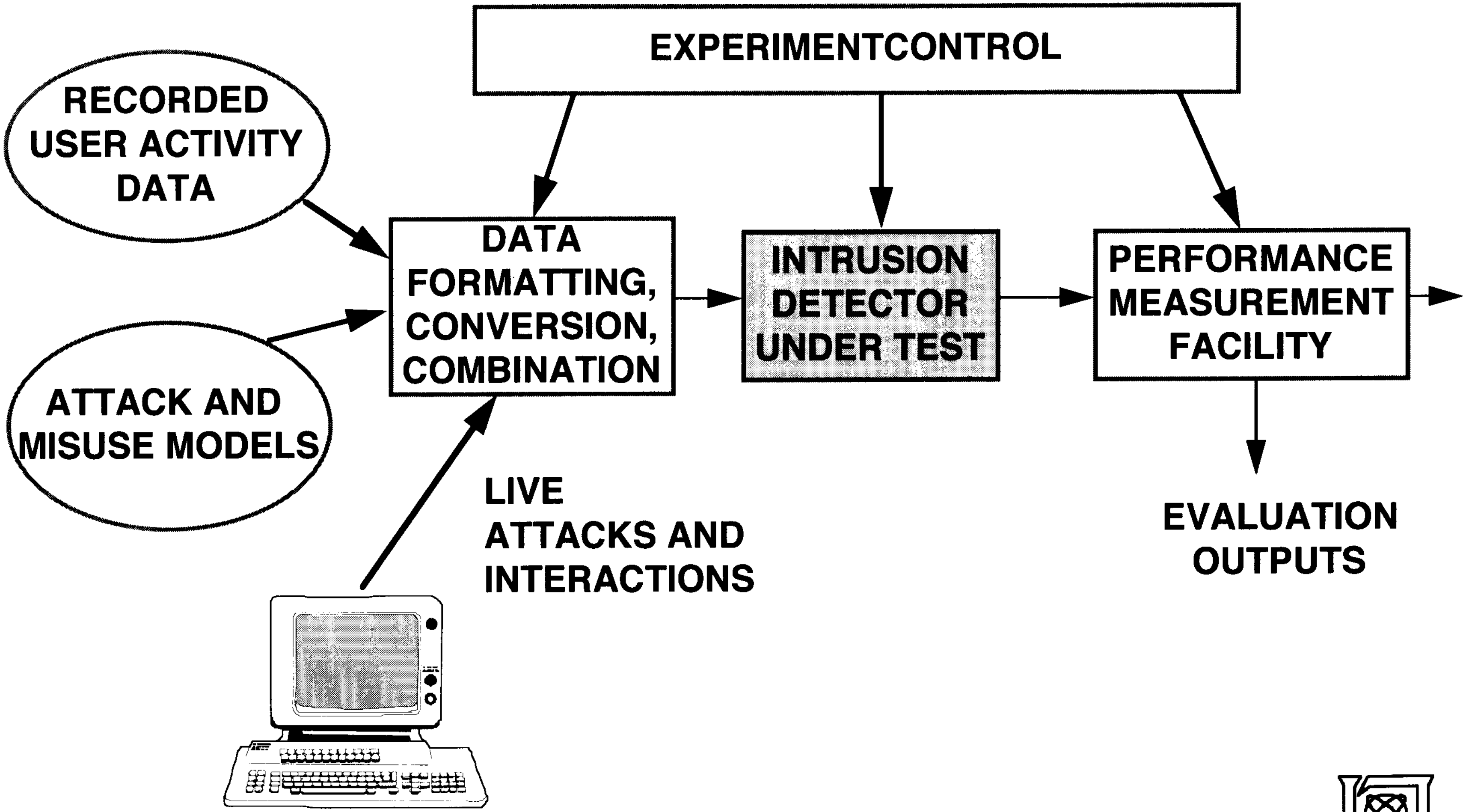
LINCOLN TEST ENVIRONMENT

ASIM INTRUSION DETECTION ENVIRONMENT ON AIR FORCE BASES



- •ASIM EXAMINES ALL TCP/IP PACKETS FROM LOCAL TO REMOTE SITES
- •STORES PACKET INFORMATION AND CONTENTS

LOCAL LINCOLN/ROME TEST ENVIRONMENT



EXPERIMENTCONTROL

RECORDED USER ACTIVITY DATA

ATTACK AND MISUSE MODELS

DATA FORMATTING, CONVERSION, COMBINATION

INTRUSION DETECTOR UNDER TEST

PERFORMANCE MEASUREMENT FACILITY

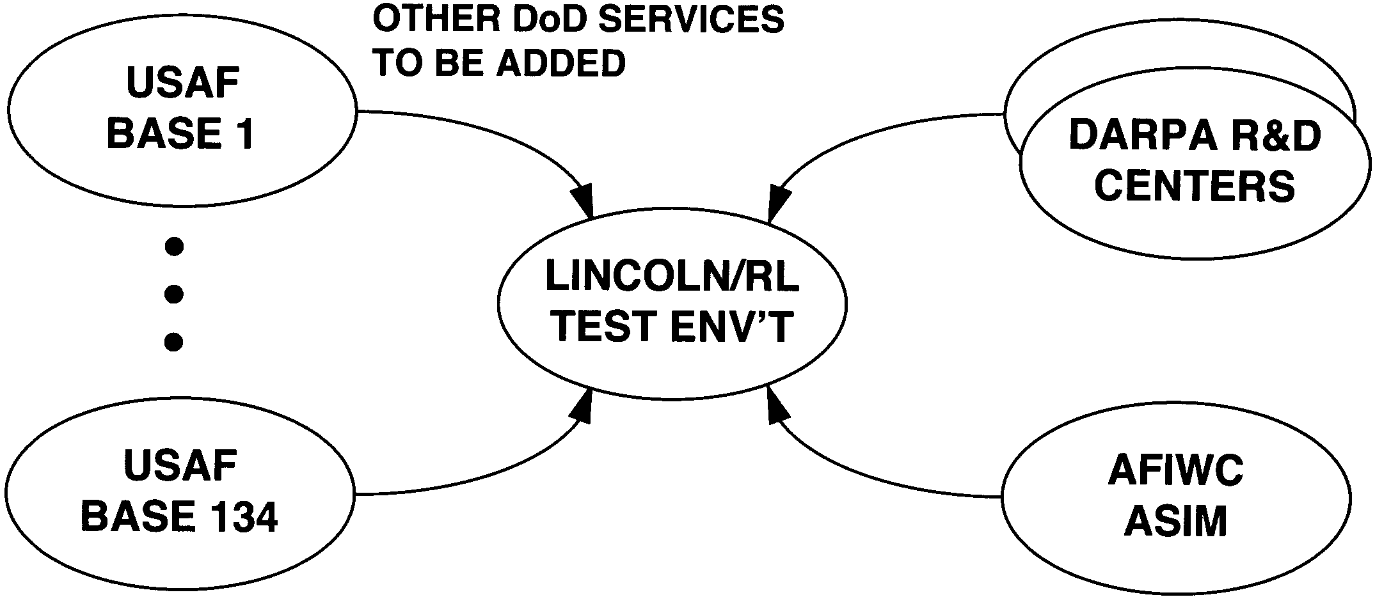
LIVE ATTACKS AND INTERACTIONS

EVALUATION OUTPUTS

ATTACK AND MISUSE MODELS

- SOURCES OF ATTACKS
  - INCIDENTAL EVENTS IN NORMAL DATA
  - COMPUTER SECURITY ASSESSMENT TEAMS
  - DARPA R&D CONTRACTORS
  - RESEARCH AND COMMERCIAL SCANNERS (COPS, SATAN, Internet Security Systems Internet Scanner)
- GENERATING NEW ATTACKS
  - NEW REAL ATTACKS CAN BE ADDED DURING PROGRAM
  - PRESENT HISTORICAL SEQUENCE (CERT Advisories) OF ATTACKS, DISABLE ATTACK-SPECIFIC RULES
- SOURCES OF MISUSE
  - AIR FORCE MONITORS AND SYSTEM ADMINISTRATORS
  - SIMPLE BASELINE (Swap Users, Move Users Between Groups)

TEST ENVIRONMENT AND DATA SOURCE RELATIONSHIPS



- NORMAL OPERATION
- INCIDENTAL ATTACKS AND FAULTS
- EXERCISES
- RED TEAM ATTACKS

DATA BASE ISSUES

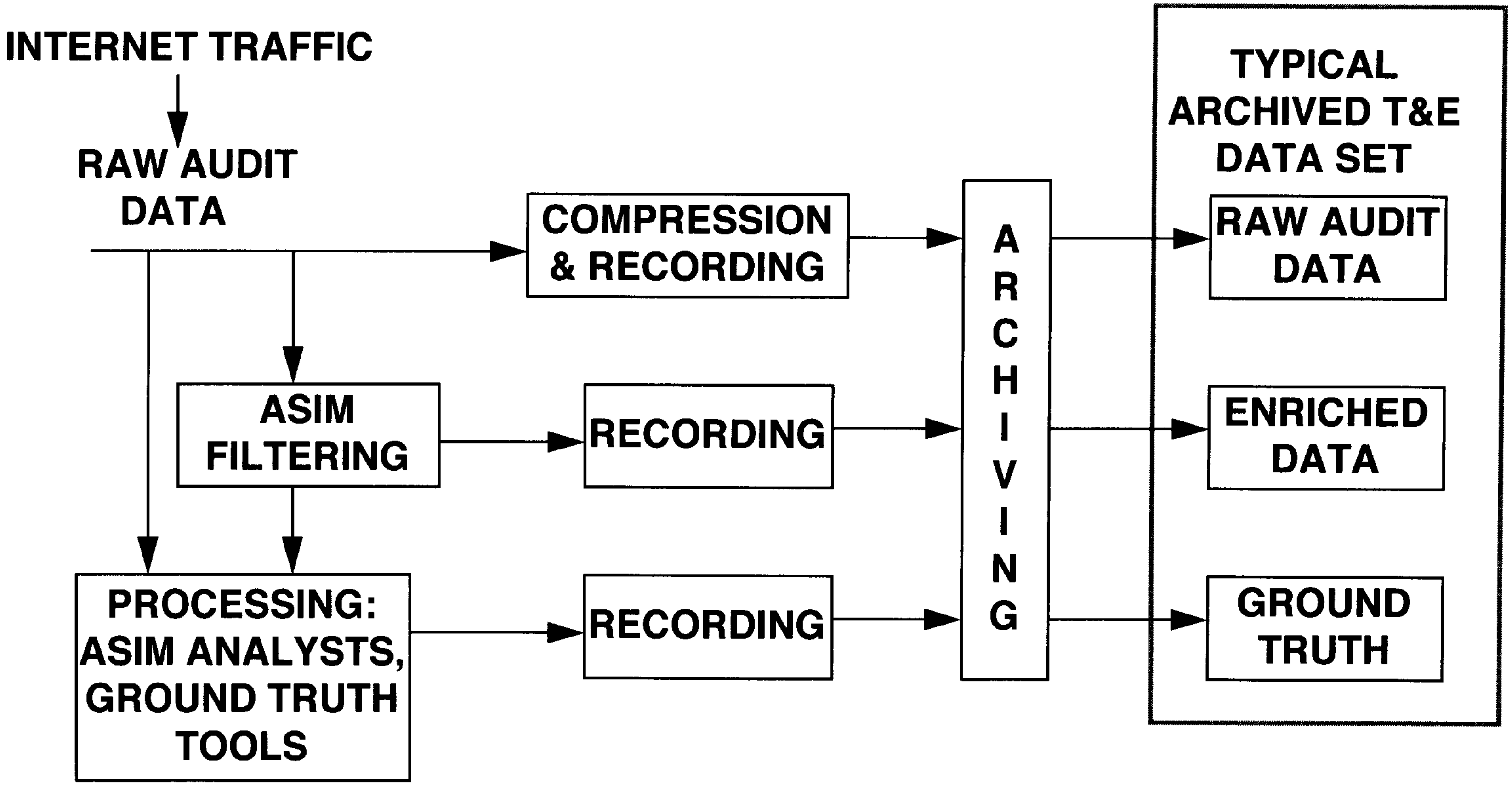
- VALIDITY OF SAMPLING (Location, Date/Time, Activities, System, System Load, System Configuration)
- OBTAINING GROUND TRUTH (Are Attacks or Misuse Hidden in the Data?)
- SELECTING TRAINING AND TEST DATA
- STATISTICAL SIGNIFICANCE OF RESULTS (Attacks and Misuse are Infrequent)
- TYPES AND FREQUENCY OF OCCURRENCE OF ATTACKS

POTENTIAL PERFORMANCE METRICS

- DETECTION PROBABILITY AND FALSE ALARM RATE (KNOWN AND NEW ATTACKS)
- RESOURCE UTILIZATION BY DETECTOR
  - CPU, MEMORY, FILE SIZE, NETWORK LOAD
- LATENCY OF DETECTION
- VALIDITY OF DIAGNOSES AND RECOMMENDED ACTIONS

- EASE OF EXTENSION TO DETECT NEW ATTACKS
- PORTABILITY, EASE AND COST OF INSTALLATION
- QUALITY OF TOOLS FOR INFORMATION REPRESENTATION AND EVALUATION
- WORKLOAD AND EFFICIENCY LEVERAGE

TEST DATA SET COLLECTION EXAMPLE: AIR FORCE SITE MONITORED BY ASIM



rpl 10/23/96 18

TECHNICAL APPROACH

STEP 1: IMPLEMENT A TEST ENVIRONMENT

- ARCHITECTURE
- PERFORMANCE METRICS
- TEST DATA SET COLLECTION EXAMPLE
- OBTAIN BASELINE PERFORMANCE OF OPERATIONAL SYSTEM

→ STEP 2: TEST A SINGLE-SITE R&D SYSTEM

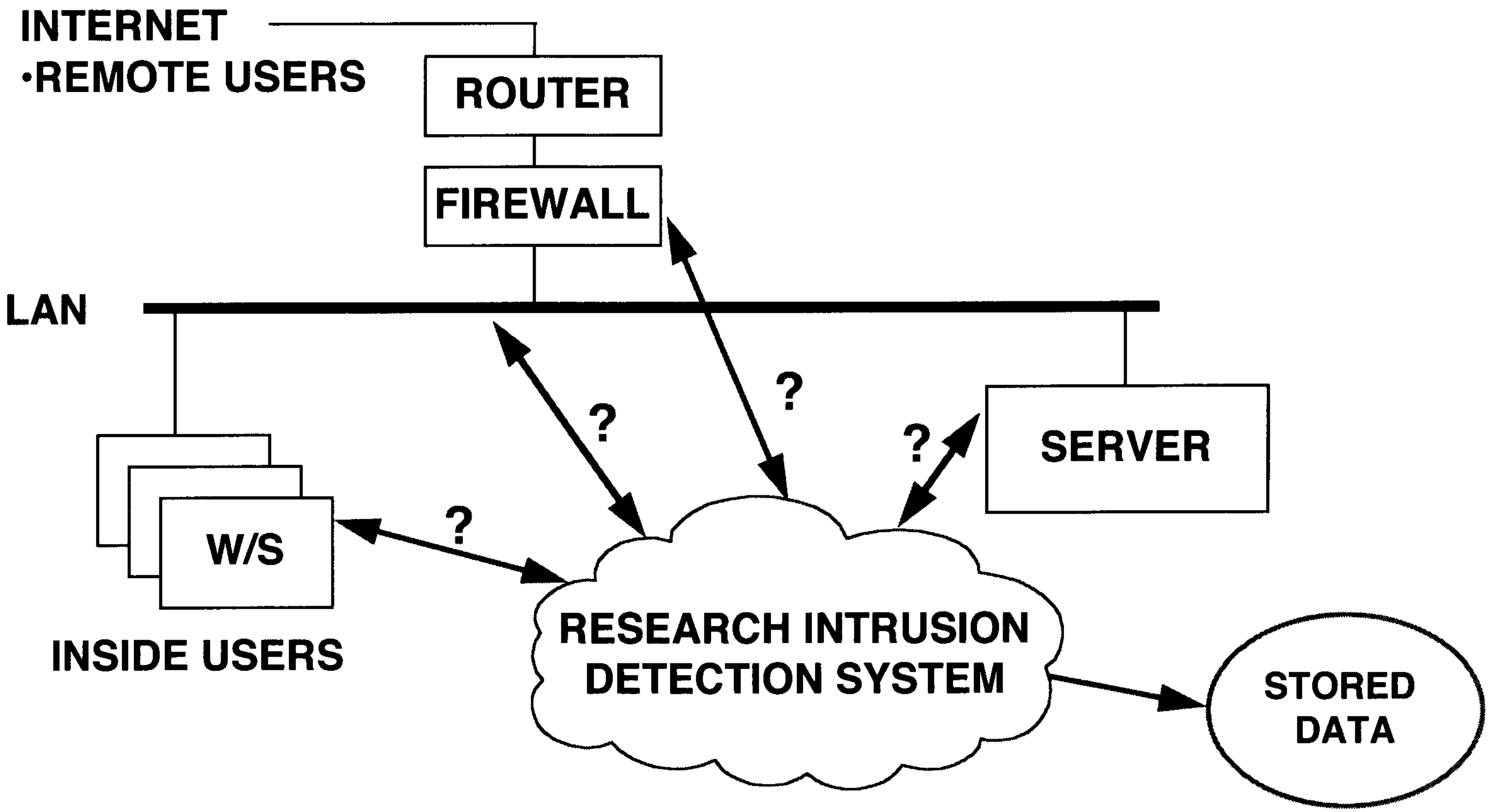
STEP 3: TEST ADDITIONAL SINGLE-SITE R&D SYSTEMS

STEP 4: TEST MULTI-SITE R&D SYSTEMS

TECHNICAL APPROACH, STEP 2: TEST AN INTRUSION DETECTION R&D PRODUCT

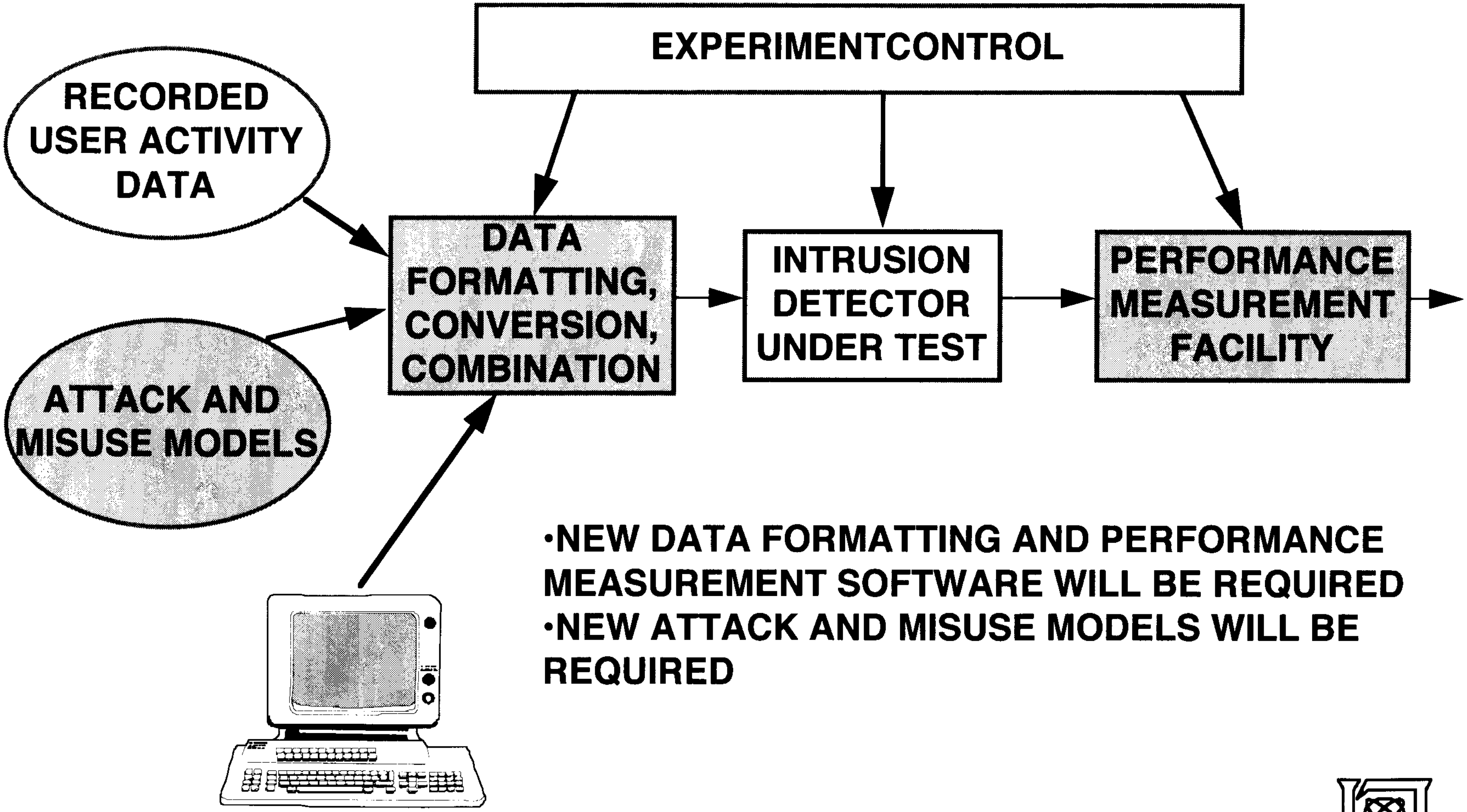
- SELECT A SUITABLE SYSTEM FROM THE R&D COMMUNITY
- CUSTOMIZE FACILITIES IN THE LOCAL TEST ENVIRONMENT
  - DATA FORMATTING
  - PERFORMANCE MEASUREMENT
- MODIFY AF BASE DATA COLLECTION AS NECESSARY
- BRING UP THE SYSTEM TO BE TESTED AT LINCOLN
  - EXPERIMENT WITH ITS FUNCTIONS AND CONTROLS
  - FIX ANY INTERFACING PROBLEMS
- APPLY RECORDED DATA FROM OPERATIONAL SITE
- APPLY ATTACKS AND VARIOUS MISUSE MODELS
- EVALUATE PERFORMANCE AND COMPARE TO BASELINE

INSTALLING A RESEARCH INTRUSION DETECTION SYSTEM ON AIR FORCE BASES



- NEW SOFTWARE WILL HAVE TO BE INSTALLED IN WORKSTATIONS, FIREWALL, AND/OR SERVERS TO OBTAIN DATA

STEP 2 EXTENSIONS REQUIRED FOR LOCAL LINCOLN/ROME TEST ENVIRONMENT


EXPERIMENTCONTROL
RECORDED USER ACTIVITY DATA
ATTACK AND MISUSE MODELS
DATA FORMATTING, CONVERSION, COMBINATION
INTRUSION DETECTOR UNDER TEST
PERFORMANCE MEASUREMENT FACILITY

- •NEW DATA FORMATTING AND PERFORMANCE MEASUREMENT SOFTWARE WILL BE REQUIRED
- •NEW ATTACK AND MISUSE MODELS WILL BE REQUIRED

TECHNICAL APPROACH

STEP 1: IMPLEMENT A TEST ENVIRONMENT

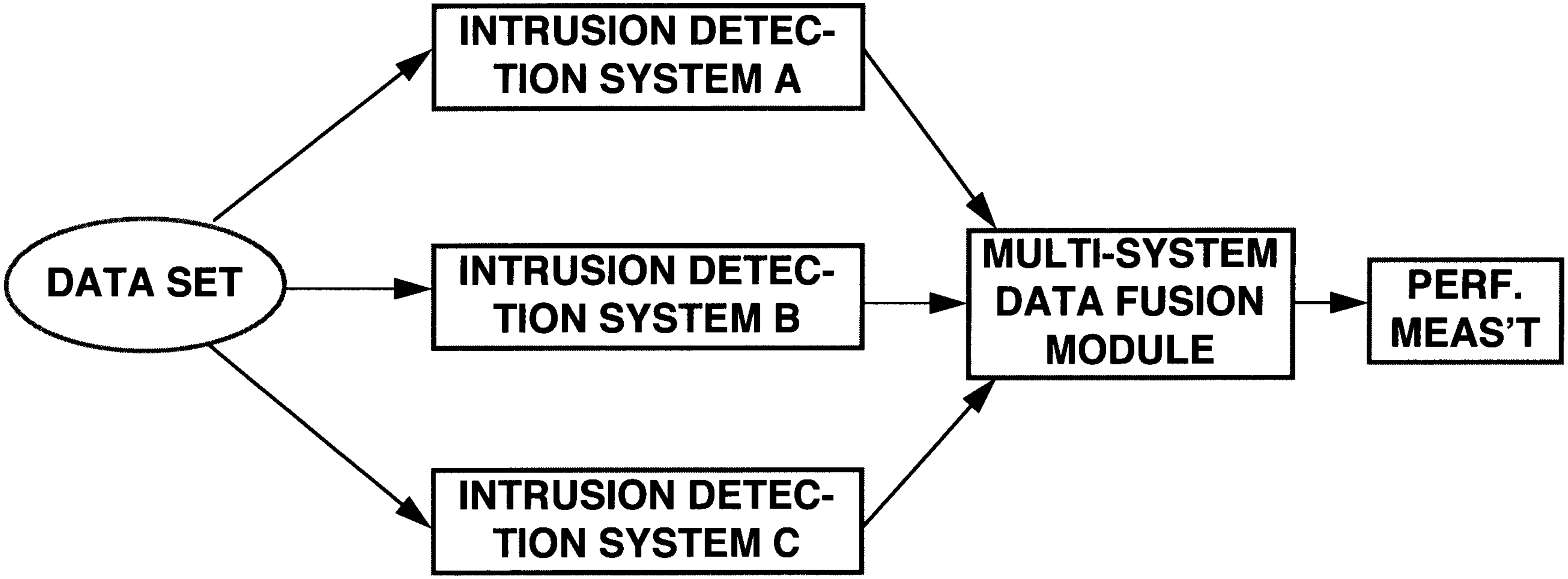
- ARCHITECTURE
- PERFORMANCE METRICS
- TEST DATA SET COLLECTION EXAMPLE
- OBTAIN BASELINE PERFORMANCE OF OPERATIONAL SYSTEM

STEP 2: TEST A SINGLE-SITE R&D SYSTEM

→ STEP 3: TEST ADDITIONAL SINGLE-SITE R&D SYSTEMS

STEP 4: TEST MULTI-SITE R&D SYSTEMS

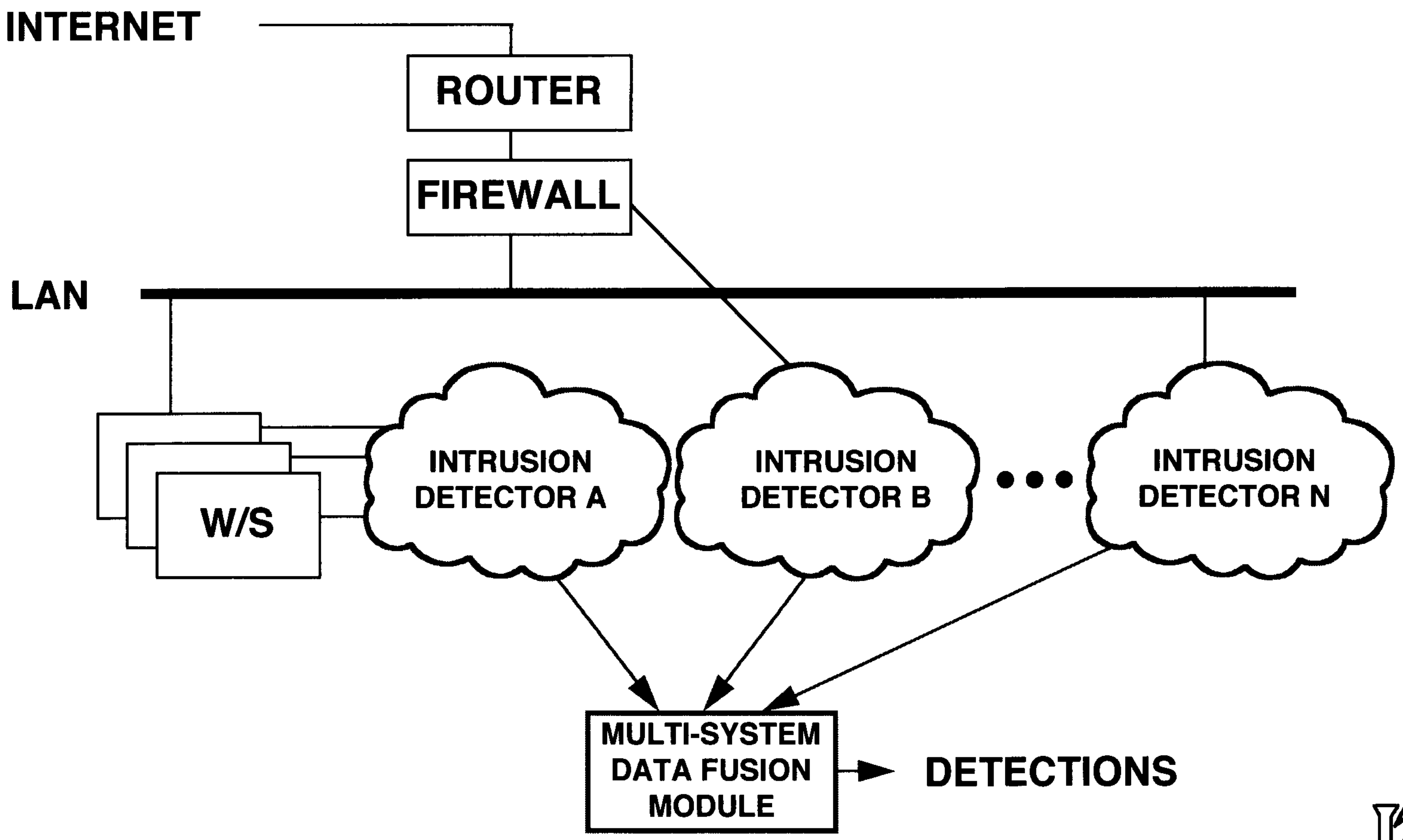
TECHNICAL APPROACH, STEP 3: TEST ENVIRONMENT FOR COMBINATIONS OF INTRUSION DETECTION SYSTEMS


DATA SET
INTRUSION DETECTION SYSTEM A
INTRUSION DETECTION SYSTEM B
INTRUSION DETECTION SYSTEM C
MULTI-SYSTEM DATA FUSION MODULE
PERF. MEAS'T

GOALS:

- COMPARE APPROACHES ON IDENTICAL DATA SETS
- FIND MOST EFFECTIVE DETECTION INPUT MEASURES AND ALGORITHMS
- COMBINE TO PROVIDE IMPROVED PERFORMANCE AT LOWER OPERATIONS COST

INTEGRATED INTRUSION DETECTION SYSTEM ENVIRONMENT (FOR STEP 3)



TECHNICAL APPROACH

STEP 1: IMPLEMENT A TEST ENVIRONMENT

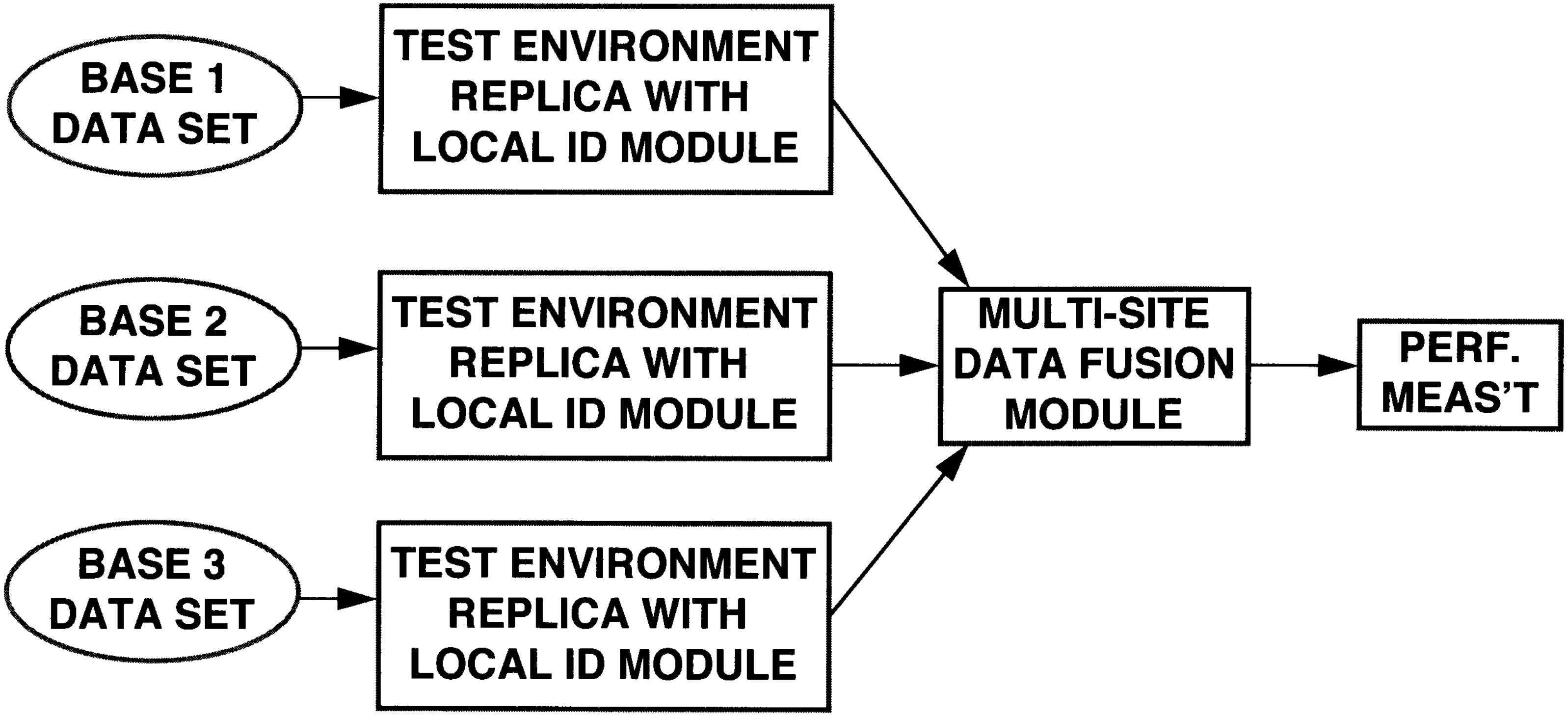
- ARCHITECTURE
- PERFORMANCE METRICS
- TEST DATA SET COLLECTION EXAMPLE
- OBTAIN BASELINE PERFORMANCE OF OPERATIONAL SYSTEM

STEP 2: TEST A SINGLE-SITE R&D SYSTEM

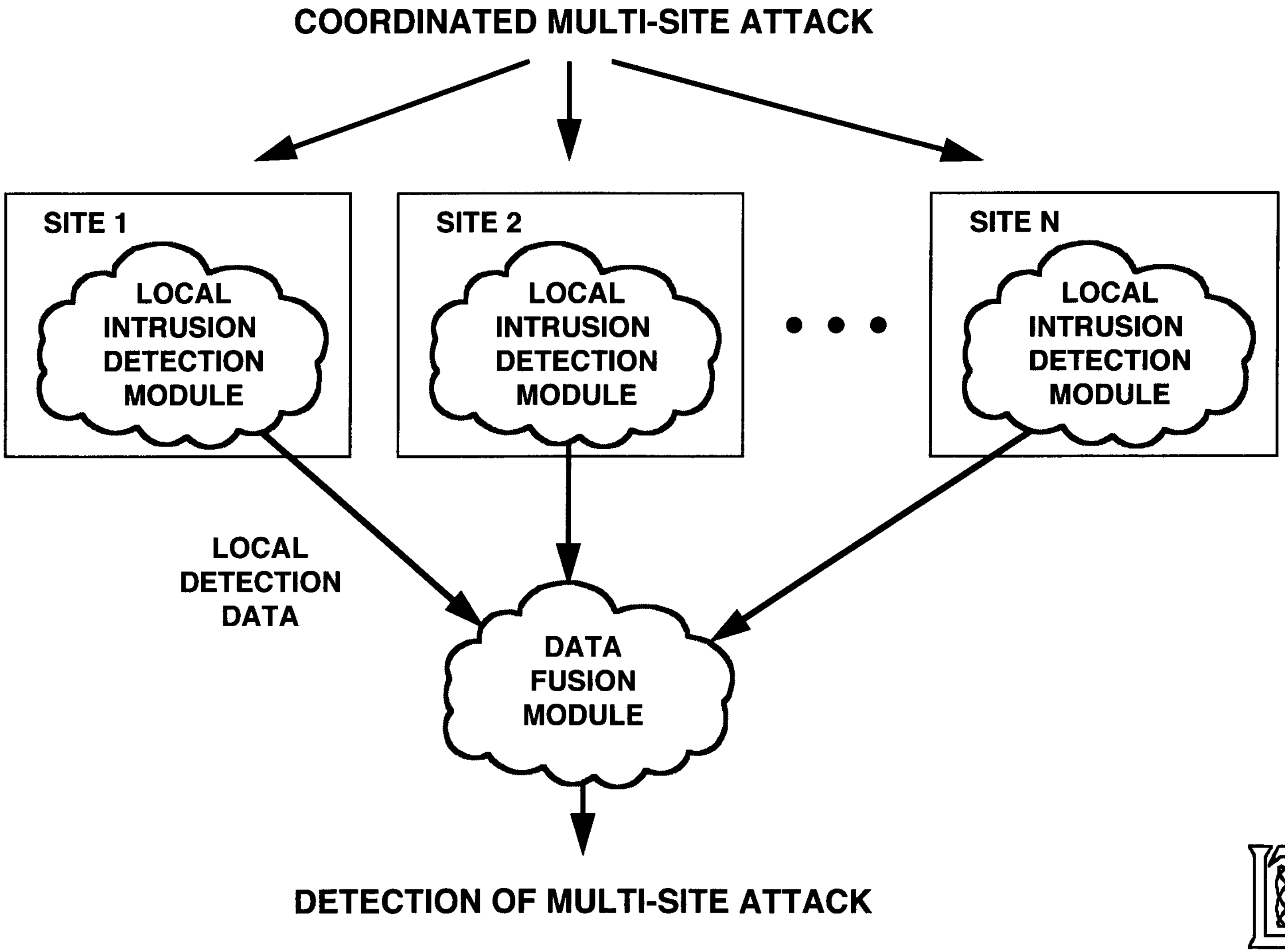
STEP 3: TEST ADDITIONAL SINGLE-SITE R&D SYSTEMS

→ **STEP 4: TEST MULTI-SITE R&D SYSTEMS**

TECHNICAL APPROACH, STEP 4: TEST ENVIRONMENT FOR MULTI-SITE INTRUSION DETECTION SYSTEMS


BASE 1 DATA SET
TEST ENVIRONMENT REPLICA WITH LOCAL ID MODULE
BASE 2 DATA SET
TEST ENVIRONMENT REPLICA WITH LOCAL ID MODULE
BASE 3 DATA SET
TEST ENVIRONMENT REPLICA WITH LOCAL ID MODULE
MULTI-SITE DATA FUSION MODULE
PERF. MEAS'T

MULTI-SITE ATTACK ENVIRONMENT (FOR STEP 4)



COORDINATED MULTI-SITE ATTACK

SITE 1

LOCAL INTRUSION DETECTION MODULE

SITE 2

LOCAL INTRUSION DETECTION MODULE

• • •

SITE N

LOCAL INTRUSION DETECTION MODULE

LOCAL DETECTION DATA

DATA FUSION MODULE

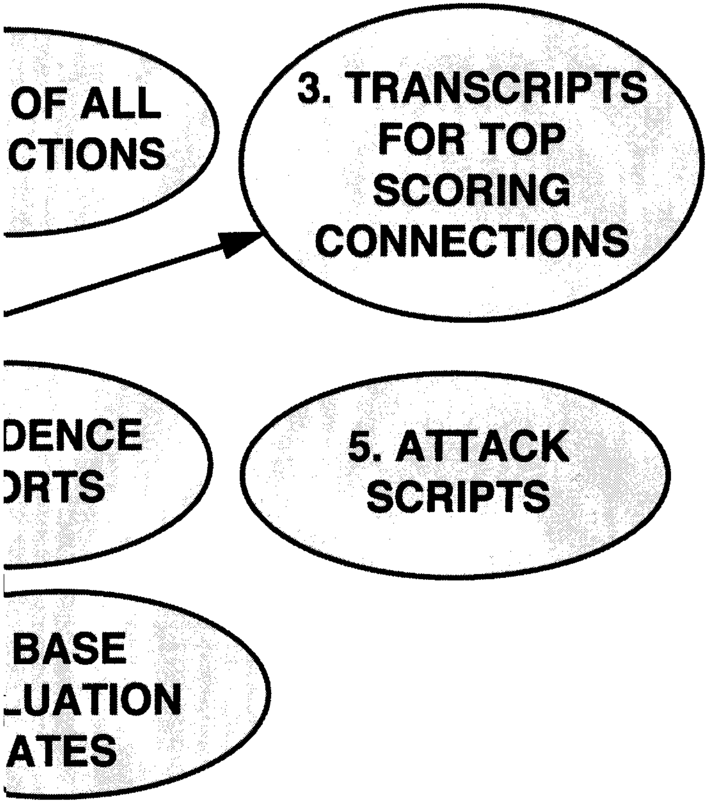
DETECTION OF MULTI-SITE ATTACK

A LARGE REAL CONNECTION DATA BASE IS REQUIRED TO EVALUATE ASIM (NSM)

- SELECT A FEW REPRESENTATIVE BASES (e.g. Wright Patterson, Hanscom, ...)
- OBTAIN SIX MONTHS OF DATA
  - RAW SNIFFED PACKET LOGS STORED ON BASE
  - CONNECTION SCORES STORED AT AFIWC
  - HIGH-SCORING CONNECTION TRANSCRIPTS STORED AT AFIWC
  - INCIDENTREPORTS ISSUED FROM AFIWC
  - INFORMATION ABOUT RED-TEAM AND BASE EVALUATION ACTIVITIES
- STORE DATA AT LINCOLN TO PLAY BACK AND EVALUATE INTRUSION DETECTION SYSTEMS
  - USE ON LOCAL NET WITH NO EXTERNAL CONNECTIONS
  - INSIDE BUILDING THAT REQUIRES CLEARANCE TO ENTER

OR TEST AND
MENT

C (San Antonio)



OF ALL
CTIONS

3. TRANSCRIPTS
FOR TOP
SCORING
CONNECTIONS

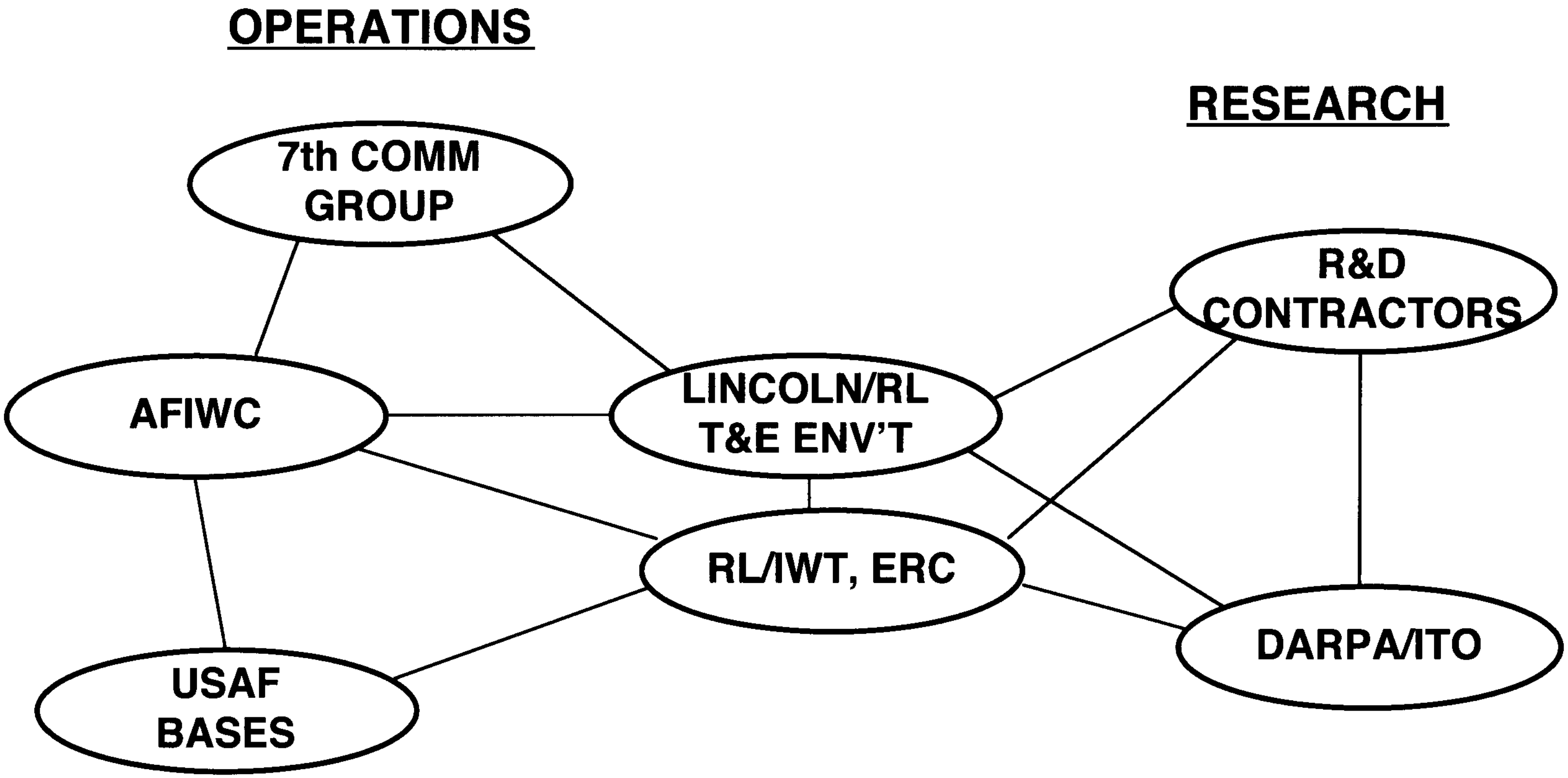
DENCE
ORTS

5. ATTACK
SCRIPTS

BASE
LUATION
ATES

D USED TO
ND ALSO OTHER

KEY PARTICIPANTS



NEAR-TERM ACTIVITIES

- PROCEED WITH TECHNICAL APPROACH, STEP 1
  - IMPLEMENT THE TEST ENVIRONMENT FOR ASIM
  - COLLECT DATA SETS AND GROUND TRUTH
  - GENERATE MISUSE AND ATTACK MODELS
  - PERFORM EVALUATIONS
- PROVIDE UPDATES TO THE R&D COMMUNITY
  - TWO-WAY FLOW OF ADVICE AND PROGRESS REPORTS
  - ANALYSIS AND EVALUATION REPORTS
  - PLANNING OF STEP 2 AND BEYOND
- FORM AND CHAIR A WORKING GROUP
  - DEFINE TEST AND EVALUATION METHODOLOGY
  - DEFINE THE TEST ENVIRONMENT AND PERFORMANCE METRICS

SUMMARY OF TEST EVALUATION WORK

- LINCOLN AND ROME LABORATORIES ARE DEVELOPING AN ENVIRONMENT TO EVALUATE INTRUSION DETECTION SYSTEMS
  - UNBIASED EVALUATION
  - MODEL ACTUAL GOVERNMENT OPERATIONS
  - ACTUAL ATTACK AND MISUSE MODELS
  - OBJECTIVE EVALUATIONS
- INITIAL BASELINE WORK WILL USE ASIM SOFTWARE
- RESEARCH SYSTEMS WILL THEN BE EVALUATED