ROME LABORATORY

COMPUTER SECURITY

PRESENTED BY
MR JOSEPH GIORDANO
RL/C3AB
(315) 330-3681
Form SF298 Citation Data

<table>
<thead>
<tr>
<th>Report Date</th>
<th>Report Type</th>
<th>Dates Covered (from... to)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11101993</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title and Subtitle</th>
<th>Contract or Grant Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rome Laboratory Computer Security</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authors</th>
<th>Project Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Task Number</td>
</tr>
<tr>
<td></td>
<td>Work Unit Number</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Performing Organization Name(s) and Address(es)</th>
<th>Performing Organization Number(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rome Laboratory</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sponsoring/Monitoring Agency Name(s) and Address(es)</th>
<th>Monitoring Agency Acronym</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distribution/Availability Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved for public release, distribution unlimited</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supplementary Notes</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Abstract</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Subject Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;IATAC COLLECTION&quot;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Document Classification</th>
<th>Classification of SF298</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
<td>unclassified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Classification of Abstract</th>
</tr>
</thead>
<tbody>
<tr>
<td>unclassified</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
</tr>
</tbody>
</table>
# Rome Laboratory Computer Security

**1. AGENCY USE ONLY (Leave blank)**

**2. REPORT DATE**

10/1/95

**3. REPORT TYPE AND DATES COVERED**

Briefing

**4. TITLE AND SUBTITLE**

Rome Laboratory Computer Security

**5. FUNDING NUMBERS**

**6. AUTHOR(S)**

Joseph Giordano

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

**11. SUPPLEMENTARY NOTES**

**12a. DISTRIBUTION / AVAILABILITY STATEMENT**

A

**12b. DISTRIBUTION CODE**

**13. ABSTRACT (Maximum 200 Words)**

The objective of this presentation is to develop & demonstrate the tools & technology necessary to realize trusted C3I systems in Air Force & DoD applications, and to emphasize use of formal Verification to assure Security/Trust Mechanism Satisfies Formal Security/Trust Policy Model.

**14. SUBJECT TERMS**

IA

**15. NUMBER OF PAGES**

**16. PRICE CODE**

**17. SECURITY CLASSIFICATION OF REPORT**

Unclassified

**18. SECURITY CLASSIFICATION OF THIS PAGE**

UNCLASSIFIED

**19. SECURITY CLASSIFICATION OF ABSTRACT**

UNCLASSIFIED

**20. LIMITATION OF ABSTRACT**

None
COMPUTER SECURITY

OBJECTIVE: TO DEVELOP & DEMONSTRATE THE TOOLS & TECHNOLOGY NECESSARY TO REALIZE TRUSTED C3I SYSTEMS IN AIR FORCE & DOD APPLICATIONS

APPROACH: EMPHASIZE USE OF FORMAL VERIFICATION TO ASSURE SECURITY/TRUST MECHANISM SATISFIES FORMAL SECURITY/TRUST POLICY MODEL
MULTI LEVEL SECURE C2 SYSTEMS
# Technology Status

<table>
<thead>
<tr>
<th>Policy</th>
<th>State-of-the-Art</th>
<th>Deficiencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Operating System</td>
<td>Integrity</td>
</tr>
<tr>
<td></td>
<td>Guards</td>
<td>Assured Service</td>
</tr>
<tr>
<td></td>
<td>Multinet Gateway</td>
<td></td>
</tr>
<tr>
<td>Verification</td>
<td>Testing</td>
<td>Distributed Systems</td>
</tr>
<tr>
<td></td>
<td>Penetration</td>
<td>Database Mgmt Sys</td>
</tr>
<tr>
<td></td>
<td>Design Verification</td>
<td>Parallel Processing</td>
</tr>
<tr>
<td>Certification</td>
<td>Ad Hoc Process</td>
<td>Code Verification</td>
</tr>
<tr>
<td></td>
<td>Labor Intensive</td>
<td>Trusted Compilers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trusted Hardware</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software Engineering</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Standardized Process</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automated Tools</td>
</tr>
</tbody>
</table>
COMPUTER SECURITY AREAS OF INTEREST

- SECURITY PROPERTIES MODELING
- SECURE DISTRIBUTED SYSTEMS
- MULTILEVEL SECURE DBMS
- FORMAL VERIFICATION
- CERTIFICATION TECHNOLOGY
SECURITY PROPERTIES MODELING

ROMULUS

- Established concept of "hook-up" security
- Implemented secure system development environment on Sun workstation
- Populate environment with generic models of secure system components
- Extend environment to address: data integrity, assured service

FORMAL MODELS

- Database integrity
- Assured service for distributed systems
- Database aggregation
- Distributed systems integrity
TO-BOTTOM VERIFICATION

FUNCTIONAL REQUIREMENTS

FORMAL SECURITY MODEL

DESIGN VERIFICATION

SECURITY POLICY
- ACCESS CONTROL
- DATA/PROCESS INTEGRITY
- DENIAL OF SERVICE

FORMAL TOP-LEVEL SPECIFICATION

DESIGN VERIFICATION

LOWER LEVEL FORMAL SPECIFICATIONS

CODE VERIFICATION

FORMAL ASSURANCE

SOURCE CODE

TRUSTED SECURITY MECHANISM
WHAT IS ROMULUS?

ROMULUS IS A WORKSTATION-BASED, TRUSTED SYSTEM DESIGN ENVIRONMENT TO MODEL, ANALYZE, & VERIFY THE SECURITY PROPERTIES OF TRUSTED, DISTRIBUTED COMPUTER SYSTEMS.
COMPONENTS OF ROMULUS

MODELS LIBRARY

GRAPHICAL SPECIFICATION

SPECIFICATION LANGUAGE

THEOREM PROVER

FLOW ANALYZER
SYSTEM DESIGN WITH ROMULUS
ROMULUS EXTENSIONS

- REQUIREMENTS TOOL INTEGRATION
- ROMULUS/PENELOPE INTEGRATION
- ENHANCED MODELING SUPPORT
ARCHITECTURES

LAYERED (CRONUS)
KERNELIZED (MACH)
REAL-TIME (ALPHA)

SEC
DIST
SYS

POLICY MODELS

CONFIDENTIALITY
INTEGRITY
ASSURED SERVICE

EXPERIMENTS

DATABASE SUPPORT
ARCHITECTURES INTEROPERABILITY
SURVIVABILITY

COMPONENTS

TACTICAL INFOSEC WORKSTATION
MLS DISTRIBUTED OPERATING SYSTEM

TRUSTED DISTRIBUTED COMPUTING ENVIRONMENT

HOST COMPUTER

HOST COMPUTER

HOST COMPUTER

MLS NETWORK

MANDATORY ACCESS CONTROLS

AUTHENTICATION MANAGER

AUDITOR

PROCESS MANAGER

DISCRETIONARY ACCESS CONTROLS

FILE MANAGER

UNTRUSTED APPLICATIONS

MLS APPLICATIONS
THETA PROGRAM-HISTORY

- ROME LAB SUPPORT FROM 1985
- CONCEPT EXPLORATION PHASE ("PHASE I"):  
  - BBN/ORA, 1985-47  
  - STUDY DISTRIBUTED SECURITY; FORMULATE POLICY  
  - DESIGN A SECURE DISTRIBUTED OS  
  - CARRY OUT AI-LEVEL VERIFICATION FOR ASSURANCE
- DEMONSTRATION/VALIDATION PHASE ("PHASE II"):  
  - ORA/BBN, 1988-92  
  - DETAILED DESIGN & POLICY BASED ON PHASE I WORK  
  - IMPLEMENT PROTOTYPE  
  - B3-LEVEL DESIGN & ASSURANCE
THETA/TRUSTED DBMS INTEGRATION

TRUSTED DISTRIBUTED COMPUTING ENVIRONMENT

MLS NETWORK

USER'S QUERY

INTERFACE

QUERY HANDLER

AIRCRAFT
- C-5A
- C-130
- C-17
- KC-135

BASES
- SCOTT
- TRAVIS
- McGUIRE
- HICKAM

SPARES
- XXXX
- YYYY
- ZZZZ
Next-generation DBMS
Intelligent Databases
Data + Rules + Knowledge
Object-oriented programming
Security Policy, formal model

Data Views
MLS Relational Data Model
Targeted to A1
Two security policies address:
- Mandatory/Discretionary Integrity
- Rule-based classification constraints
- Polyninstantiation
- Formal models, FTLS, and demonstration
- SCTC Lock & Gemini GEMSOS

MLS Data Management
Secure Distributed DBMS
Client-server
Distributed homogeneous
Distributed heterogeneous
Federated

Aggregation of Data
Expert systems
Mathematical models
Integration of audit & intrusion detection
TRUSTED DATABASE FRONT-END

OBJECTIVE:

• DEVELOP & DEMONSTRATE TRUSTED DBMS FRONT-END CAPABILITIES TO SUPPORT
  -- MULTILEVEL WORKSTATION INTERFACE
  -- MULTILEVEL OUTPUT TECHNOLOGY
  -- PRESENTATION TECHNOLOGY
  -- WINDOWING
  -- TRUSTED DATA LABELS

PROGRAM REQUIREMENTS:

• BUILD TO AT LEAST CLASS B2
• TRUSTED SUBJECT APPROACH
• CLIENT-SERVER ARCHITECTURE
SUN 3/60 WORKSTATION WITH TEMPLATE BASED SCREEN EDITOR
SPECIFICATION LANGUAGE BASED ON LARCH & ANNA
PHASE I (FY89): PASCAL-LIKE FEATURES
   WITH EXCEPTIONS
PHASE II (FY92): REUSABLE LIBRARIES
PHASE III (FY95): CONCURRENCY

Design & implement a verification environment
from ADA spec to hardware chip
Uses executable specification language
Emphasis to date:
TRUSTED COMPILER
RISC PROCESSOR VERIFICATION
APPLICATION:
TRUSTED ADA COMPILER
SD1 CHIP VERIFICATION (RH32)

Establish theoretical foundations
Implement prototype environment to establish feasibility (based on C)
Demonstrate via SD1 weapons assignment algorithm
Incorporate into ADA verification environment

Evaluate existing methodologies
Develop midterm requirements
Research long term verification issues
CERTIFICATION TECHNOLOGY

OBJECTIVE:
DEVELOP A METHODOLOGY & PROVIDE A SET OF TOOLS & TECHNIQUES TO SUPPORT THE SECURITY SYSTEM ACCREDITATION/EVALUATION PROCESS & TO AID THE DETERMINATION OF THE DEGREE OF SECURITY PROVIDED BY AUTOMATED INFORMATION SYSTEMS

APPROACH:
• DEFINITIZE EXISTING CERTIFICATION PROCESS
• TAILOR PROCESS TO AIR FORCE NEEDS
• IDENTIFY AREAS AMENABLE TO AUTOMATION
• SURVEY EXISTING TOOLS/TECHNIQUES TO DETERMINE APPLICABILITY TO AIR FORCE SECURITY CERTIFICATION PROCESS
• DEVELOP A METHODOLOGY & NEW TOOLS & TECHNIQUES TO SUPPORT SYSTEM CERTIFICATION & LIFE CYCLE MANAGEMENT
## Projected FY93 New Starts

<table>
<thead>
<tr>
<th>EFFORT TITLE</th>
<th>POINT OF CONTACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Database Front-End</td>
<td>Joseph Giordano/x2805</td>
</tr>
<tr>
<td>Theta/Trusted DBMS Integration</td>
<td>Emilie J. Siarkiewicz/x3241</td>
</tr>
<tr>
<td>Romulus Extensions</td>
<td>John C. Faust/x3241</td>
</tr>
</tbody>
</table>