Overview of Ferret Project

Timothy J. Smith
MCNC/RTI
Research Triangle Park, NC
tjsmith@mcnc.org
Ferret Project Presentation Outline

• Problem, objectives, method, accomplishments

• Background
  - Workflow
  - Event Characterization
  - Insider Threat Analysis
  - Policy Gap and Risk Analysis
  - Ferret Architecture
  - Ferret Metrics

• Example Scenarios

• Summary
• Ferret addresses insider attack on Manageability of high-value systems

• Oversight Groups
  - Peer group and immediate manager
  - Upper management
  - Inspectors, Auditors, Counter-Intelligence

• Spies
  - Robert Hanssen, spy at FBI for Russia, didn't play by the rules and was senior enough in management chain to avoid stricter scrutiny.
  - Anna Montez, spy at DIA for Cuba, only indication was from peer review of work.

• Automated policy compliance gives visibility and situational awareness to the management chain of activity.
• Identify and track misuse by authorized individuals of applications and services by automatic validation of compliance or variance from approved standard operating procedures in applications and processes

• Uses domain specific multi-sensor fusion of external observables of arbitrary workflows in structured and composable distributed systems (like document control systems) to produce strongly typed audit meta-data characterizing individual behaviors within a context

• Identify system and software failures and specification non-conformance that can lead to system or information compromise
• **Spy's Are Rare…**
  - Public information on details of intelligence information systems and the techniques to subvert them are rare
  - Frequently had disdain for established procedures
  - Colleagues did not report anomalous behavior
  - Spies are risk adverse, for obvious reasons
  - If we build a spy catcher, how would we test it?

• … **Fraud Is Not**
  - Ideas from fraud detection techniques employed by internal audit departments.
    • Stable production oriented processes.
    • Complex, arbitrary, business logic/rules.
    • Perspective of a possible financial crime.
    • Accounting is highly structured: system, procedures, and data.
Accomplishments to date

- **Workflow Audit Model (WAM) Language**
  - Flexible, adaptable way to describe audits of workflows
  - WAM Schema
  - WAM Language compiler and validating parser
  - Flexible API accessible to wide range of computer languages
  - Started process of specification standardization

- **Reference Implementation prototype**
  - Event Collection
  - Event Normalizer
  - Workflow audit analysis
  - Management console
  - Reporting module

- **Use in both formal specified & legacy systems**
  - Prototype anomaly detector (12m - Complete June 3^{rd})
  - 1st generation anomaly detector (18m – TBD December 2004)
A female ferret is called a “jill”
• Process
• Procedure
• Set of steps to accomplish a goal

• Workflow Domains
  - Content/Document Management
  - Asset or Resource management
  - Knowledge management
  - Issue and Bug tracking
  - Project management
  - Lifecycle management
  - Call center, CRM
  - ERP

• Trend to moving away from special purpose to generalized, flexible platforms.

• One way we can restate Ferret from negative form: Workflow Anomaly Detection to positive form: Policy and Procedure Compliance Validation

• Ferret is general purpose compliance checking, not special purpose.
Workflow Model Characterization

• Workflow Meta-Languages
  • PIF (Process Interchange Framework)
  • PSL (Process Specification Language)
  • GPSG (Generalized Process Structure Grammars)
  • Unified Modeling Language (UML)
• Business Process Expression Language (BPEL)
  • Defining the actions to be carried out in each possible state
  • Pre- and post-conditions of states
  • Transitions between states
  • Defining the sequencing of tasks / states
  • Defining automated states and states requiring user input

• Finite state machine
  – Σ with initial state of σ_i and final state σ_f
  – P with ρ_1, ρ_2, ρ_3, ..., ρ_n
  – E with e_1, e_2, e_3, ..., E_n
  – P1 = (e_{11}, e_{12}, e_{13}, ..., e_{1_n})
Event Characterization

Set of Events

Threshold

Anomaly

Normal

Threshold

Variance
Ferrets Sweet Spot

Event Variance

Anomaly

Set of Events

Threshold

Ferret

Normal

Threshold

Anomaly

Event Variance
Event Processing Chain

- Events
  - Ferret
    - Unclass
    - Other Rule-based IDS
    - Normal
  - Statistical IDS
    - Alerts
Metrics

- Anomaly Detection rate
- Observability
  - Can the system be observed by a third party?
- Auditability
  - Can the system be audited? Are there gaps?
  - Integrity: Is information reliable? Has it been tampered with?
  - Can you track usage by authorized individuals?
  - Does the audit contain too much information?
    - Useful in subverting the system
    - Sensitive information leakage
- Separation of Duty
  - Are multiple steps in process controlled by some identity? Same individual?
- Exception paths
- Audit computation cost reduction
  - Ratio of useful data for audit
Scenarios
Bridge the policy gap

- **High level security policy**
  - Keep secrets from our enemies
  - Share secrets with our friends
  - Know the difference between our friends and enemies

- **Low level security policy**
  - readme.txt should have 0640 filesystem permissions
  - network port 80 should be only opened by application apache.

- **Ferret occupies middle ground in security policy**
  - Between the executive level through the department level, human oriented security policies and the low level network or operating system level policies.
  - The middleground is the ability to express some structured standard operating security procedures (SOP) in terms of workflows in the digital domain.
  - Conformance to these SOP can be assessed automatically by Ferret.
Login prerequisites

• High level policy:
  - Use strong authentication for access control to sensitive facilities and systems

• Procedure
  - Use Photo ID Smart badge into building
    - Generate audit event
  - Use Photo ID Smart badge into secure rooms
    - Generate audit event
  - Badge/login to terminals
    - Generate audit event

• Workflow type: implicit resource management
Login prerequisites

• High level policy:
  - Use strong authentication for access control to sensitive facilities and systems

• Procedure
  • Use Photo ID Smart badge into building
    - Generate audit event
  • Use Photo ID Smart badge into secure rooms
    - Generate audit event
  • Badge/login to terminals
    - Generate audit event

• Workflow type: implicit resource management
• High level policy
  - Employees request vacation
  - Managers should have awareness of employees vacation status
• Cash register model for correcting mistakes
  - Manager can override, this prevents escalation of indication & warning.

• Additional procedures for unusual situations
  - Crisis causes folks to work extended hours
    • Manager would be warned of working outside normal hours.
    • Manager could authorize extended hours for those working during deadline or crisis.
    • AWOL would greatly escalate anomaly with that identity.

• Subsidiary: places a control at the lowest natural and proper place in management chain.
  - The correction/prevention of false alarms is integrated into natural business relationships.
  - Makes organization processes more visible to management.
• Web of compliance procedures

• Composable Audit System
  - Integrates information from unrelated existing COTS/GOTS systems
  - Decoupled, with read-only capability from audit sources.

• Ferret turns 2-factor authentication into n-factor authentication
  - If you pull the badge, everything dependent would be shutoff.
  - User provisioning without O/S and application support
  - Vacation, sick days, travel, normal hours workflows as login prerequisite conditions.
Security is mostly a superstition. It does not exist in nature. Life is either a daring adventure or nothing.
- Helen Keller