Current Research at NCSTATE

- **Motivation:**
  - We need systems that comply with relevant organizational policies, legislation and standards.

- **Approach:**
  - Approximate the semantics of a subset of NL that corresponds to a machine-enforceable context-free grammar.

- **Developments:**
  - Semantic Parameterization, a process to reduce complexity in NL statements while minimizing information loss.
  - KTL, a context-free grammar to encode and query policy statements (restated using semantic parameterization).
SPARCLE: Policy Authoring Workbench at IBM

- **Motivation:**
  - Enable privacy policy authors to quickly and accurately specify policies governing information use and disclosure.
  - Generate machine-enforceable rules from structured policy.

- **Approach:** Two primary interfaces,
  - 1) Semi-structured, captures natural language rules.
  - 2) Structured, captures 5 information types: user, action, data, purpose, condition.

- **Challenge:**
  - Can SPARCLE generalize to security policies?

Can SPARCLE generalize to security policies?

- **Begin by examining organizational security policies.**
  - What are the important elements conveyed in OSPs?
  - To whom are these elements relevant?
  - How do these people interact with these elements?
  - How do regulations and standards relate to OSPs?

- **Approach:**
  - Interviews with IBM personnel with security experience.
  - Analyze best-of-breed organizational security policies.
Interviews

- Interviews with three IBM experts regarding:
  - MLS and security compliance standards.
  - System security policies including SELinux.
  - Security policy development/ ownership.

- Two often opposing views: system security must be:
  - Formally sound and complete.
  - Usable and driven by workflows.

- The specification of security policies to-date is:
  - Fairly ad-hoc, vulnerability-driven.
  - Generally limited to business-unit and rarely organization-wide.

Analyzing Security Policy Documents

- Acquired best-of-breed OSP documents in three domains:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Finance</th>
<th>Government</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size (Pages)</td>
<td>400</td>
<td>457</td>
<td>453</td>
</tr>
</tbody>
</table>

- Document topics cover broad areas including:
  - Authentication
  - Authorization
  - Confidentiality & Integrity
  - Availability
  - Auditing & Traceability
  - Backup & Recovery
  - Risk Assessment
  - Security Classification
Overview: OSP Composition

<table>
<thead>
<tr>
<th>Definitions and References</th>
<th>~15%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsibilities: What people do.</td>
<td>~55%</td>
</tr>
<tr>
<td>Requirements: What systems do.</td>
<td>~30%</td>
</tr>
</tbody>
</table>

Note: Analysis covers only 10.8% of the entire OSP analyzed.

- **Types of Responsibilities**
  - Classification
  - Notification
  - Review/ Audit
  - Documentation

- **Types of Requirements**
  - Configuration
  - Access Control
  - Constraints

Definitions

- **For security terminology:**
  - In **Public Key Infrastructure** (PKI), one key is kept private while the other, the public key, can be generally known and even published and circulated.
  - In authentication, **unique identifiers** include: something a person *is* (fingerprint, voice), something a person *has* (smart card), something a person *knows* (reusable password).

- **For elements in responsibility/ requirement descriptions:**
  - **Time limits** for applying security patches are specified in the IT security patch publication and commence from the publication date.
Personnel Responsibilities

- **Classification:**
  - Application owners must identify criteria for permitted business needs.
  - Administrators must classify vulnerabilities by risk: low, medium, high.

- **Notification:**
  - Notify the system administrator of the security incident and report: the time of discovery, resources affected, discontinuity of service.

- **Review/ Audit:**
  - Security components must be annually reviewed for effectiveness.

- **Documentation:**
  - Evidence from user revalidation process is retained for one year.

System Requirements

- **Configuration:**
  - Anti-virus software must be installed and updated regularly.
  - All mandatory access control options are set in accordance with platform specifications.

- **Access Control Rule:**
  - General users may not update operating system resources.

- **Constraints:**
  - All mail servers must have port-level encryption using SSL.
  - All passwords must have a minimum 8 character length.
  - The minimum key length required for RSA encryption is 1024-bit.
Platform-specific Policies

- System policies are individually developed for...
  - Operating systems (MS Windows, AIX, Linux)
  - Applications and services (apache, mail, samba, ssh)
  - Network routers and firewalls
- System policies are implemented by...
  - Installing libraries, modifying compilation directives, recompiling components.
  - Modifying runtime configuration files.
  - Updating database tables.
  - Executing programs with specific arguments.
  - Users interacting with unscripted administrative tools.

Bridging the Gap

- Three degrees of policy abstraction:
  - Goals – describe high-level objectives to be achieved independent of people. Goals justify implementations.
  - Responsibilities – require personnel to implement processes to achieve goals.
  - Requirements – describe what systems do to support processes to achieve goals.
- These elements are owned and implemented by different stakeholders: lawyers, managers, analysts, system developers and administrators.
- Traceability between corresponding policy elements and individuals is a significant challenge.
Connecting OSPs to System Policies: The How and Why?

- Reusable passwords must not be transmitted over a network in clear-text form.

  Why?

  How?

- Mail applications must use TLS for encrypted communications.

  Why?

  How?

  - Install OpenSSL libraries.
  - Compile Sendmail with TLS support.
  - Configure Sendmail for TLS support.
  - Generate X.509 Certificates for Sendmail.

Influences from Law, Regulations, and Standards.

<table>
<thead>
<tr>
<th>Laws and Regulations</th>
<th>Security Policy Scopes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Program</td>
</tr>
<tr>
<td>FISMA</td>
<td>✓</td>
</tr>
<tr>
<td>SOX</td>
<td>✓</td>
</tr>
<tr>
<td>GLBA</td>
<td>✓</td>
</tr>
<tr>
<td>HIPAA</td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standards</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 15408/CC</td>
<td>✓</td>
</tr>
<tr>
<td>ISO 17799</td>
<td>✓</td>
</tr>
<tr>
<td>NIST 800-12</td>
<td>✓</td>
</tr>
<tr>
<td>NIST 800-27</td>
<td>✓</td>
</tr>
</tbody>
</table>
Final Observations

- **Security is expensive.**
  - Requirements establish baseline or minimal security.
  - Increased flexibility through guidelines or recommendations lower costs and enable workflow but increase risk to known vulnerabilities.
    - Security should be commensurate with risk.
  - Legacy systems dictate policies to administrators.

- **Security has multiple viewpoints.**
  - Different motivations for stakeholder compliance.
  - Different strategies for implementing security goals.

- **Security must be dynamic.**

Publications


- In the Fall, expect to see access control rules (that meet RBAC specification) derived from the HIPAA Privacy Rule.