# Report on Software Labels Panel

Paul E. Black

paul.black@nist.gov


# Background

- **Panel held at SIGAda, Oct 2010, Virginia**
- **Goals:**
  - **Inform “buy” decisions**
  - **Convey secure settings**
  - **Feed risk or assessments**
  - **Lead to more rugged software**
- **Being rugged is hard work. Labels help**
  - **encourage people to be rugged and**
  - **discourage ignorance, carelessness, or sloth.**

# Larry Wagoner

- **Labels get information from buyer to seller**
  - **Inform buyers' decisions**
  - **Differentiate products**
  - **Reward "good" products**
- **Labels come from**
  - **Regulation**
    - **Food, clothing, tobacco, EnergyGuide, MSDS**
  - **Vendor**
    - **MPAA, ICSA**
  - **Buyers & social media**
    - **eBay, Amazon, TripAdvisor, hotels.com**

# Dick Leslie

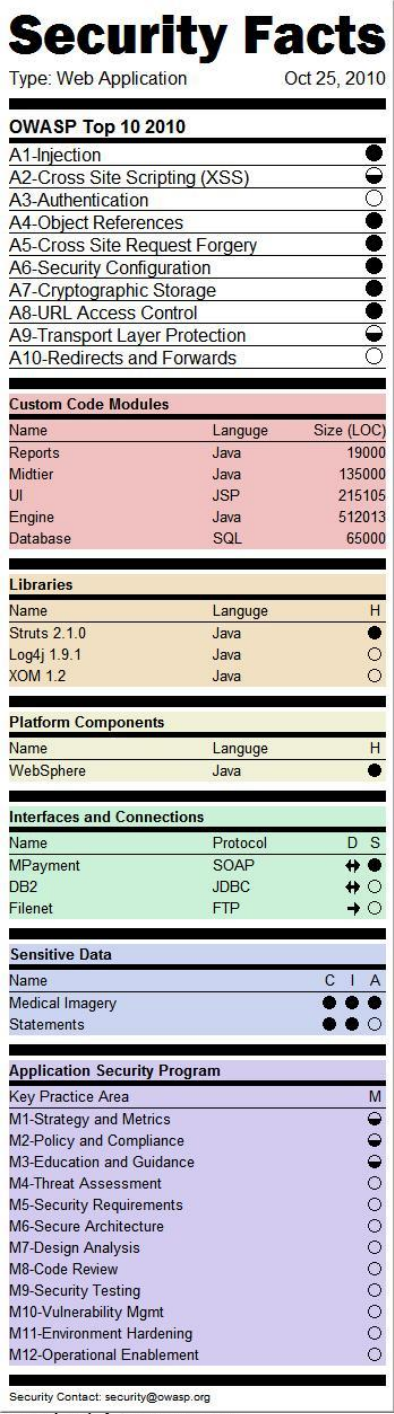
- **SCORE: Counselors to America's Small Businesses**

- **IT usually out-sourced - owner usually not aware of specifics and consequences**
- **Potential benefits: reduced liability, better customer relations, peace of mind!**
- **Essential ingredients:**
  - **Simplicity and integrity**
  - **Incentives, e.g. lower insurance rates**

# Jeff Williams

- **Competition drives food producers to voluntarily label their products' desirable attributes and to use third-party certifiers.**
- **Mandatory food labeling is more successful at filling information gaps than at addressing externalities.**

http://www.aspectsecurity.com/SecurityFacts/



**Security Facts**

Type: Web Application — Oct 25, 2010

**OWASP Top 10 2010**

| | |
|---|---|
| A1-Injection | ● |
| A2-Cross Site Scripting (XSS) | ◒ |
| A3-Authentication | ○ |
| A4-Object References | ● |
| A5-Cross Site Request Forgery | ● |
| A6-Security Configuration | ● |
| A7-Cryptographic Storage | ● |
| A8-URL Access Control | ● |
| A9-Transport Layer Protection | ◒ |
| A10-Redirects and Forwards | ○ |

**Custom Code Modules**

| Name | Languge | Size (LOC) |
|---|---|---|
| Reports | Java | 19000 |
| Midtier | Java | 135000 |
| UI | JSP | 215105 |
| Engine | Java | 512013 |
| Database | SQL | 65000 |

**Libraries**

| Name | Languge | H |
|---|---|---|
| Struts 2.1.0 | Java | ● |
| Log4j 1.9.1 | Java | ○ |
| XOM 1.2 | Java | ○ |

**Platform Components**

| Name | Languge | H |
|---|---|---|
| WebSphere | Java | ● |

**Interfaces and Connections**

| Name | Protocol | D | S |
|---|---|---|---|
| MPayment | SOAP | ↔ | ● |
| DB2 | JDBC | ↔ | ○ |
| Filenet | FTP | → | ○ |

**Sensitive Data**

| Name | C | I | A |
|---|---|---|---|
| Medical Imagery | ● | ● | ● |
| Statements | ● | ● | ○ |

**Application Security Program**

| Key Practice Area | M |
|---|---|
| M1-Strategy and Metrics | ◒ |
| M2-Policy and Compliance | ◒ |
| M3-Education and Guidance | ◒ |
| M4-Threat Assessment | ○ |
| M5-Security Requirements | ○ |
| M6-Secure Architecture | ○ |
| M7-Design Analysis | ○ |
| M8-Code Review | ○ |
| M9-Security Testing | ○ |
| M10-Vulnerability Mgmt | ○ |
| M11-Environment Hardening | ○ |
| M12-Operational Enablement | ○ |

Security Contact: security@owasp.org

# Simson L. Garfinkel

- **"The Pure Software Act"**


# Gary McGraw

- **Are we stuck on the *Track o' Doom*?**