

Conventions for Software Facts

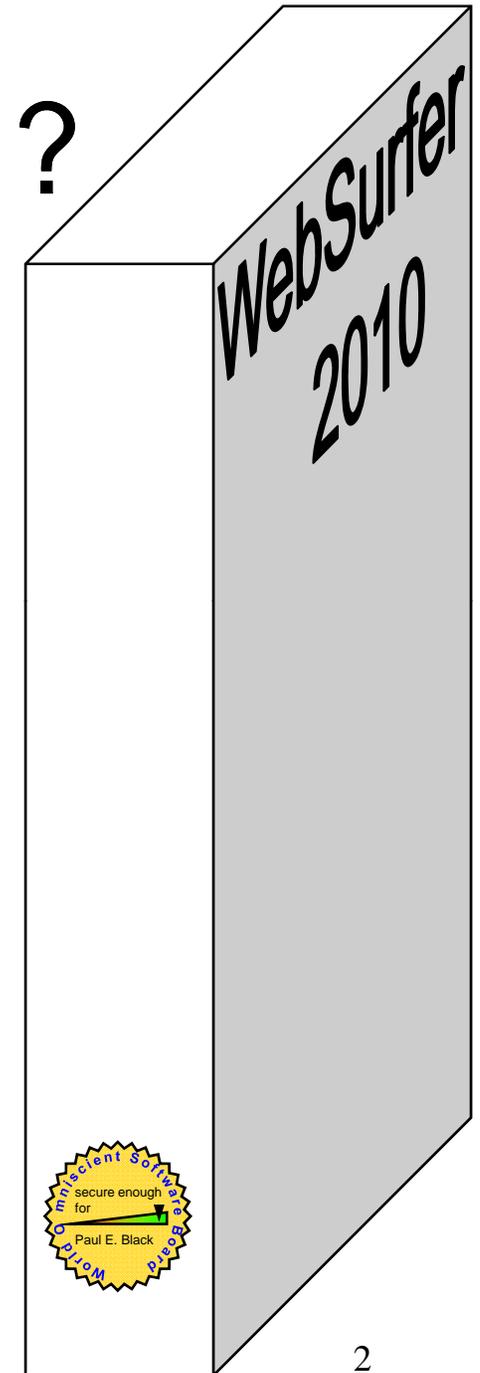
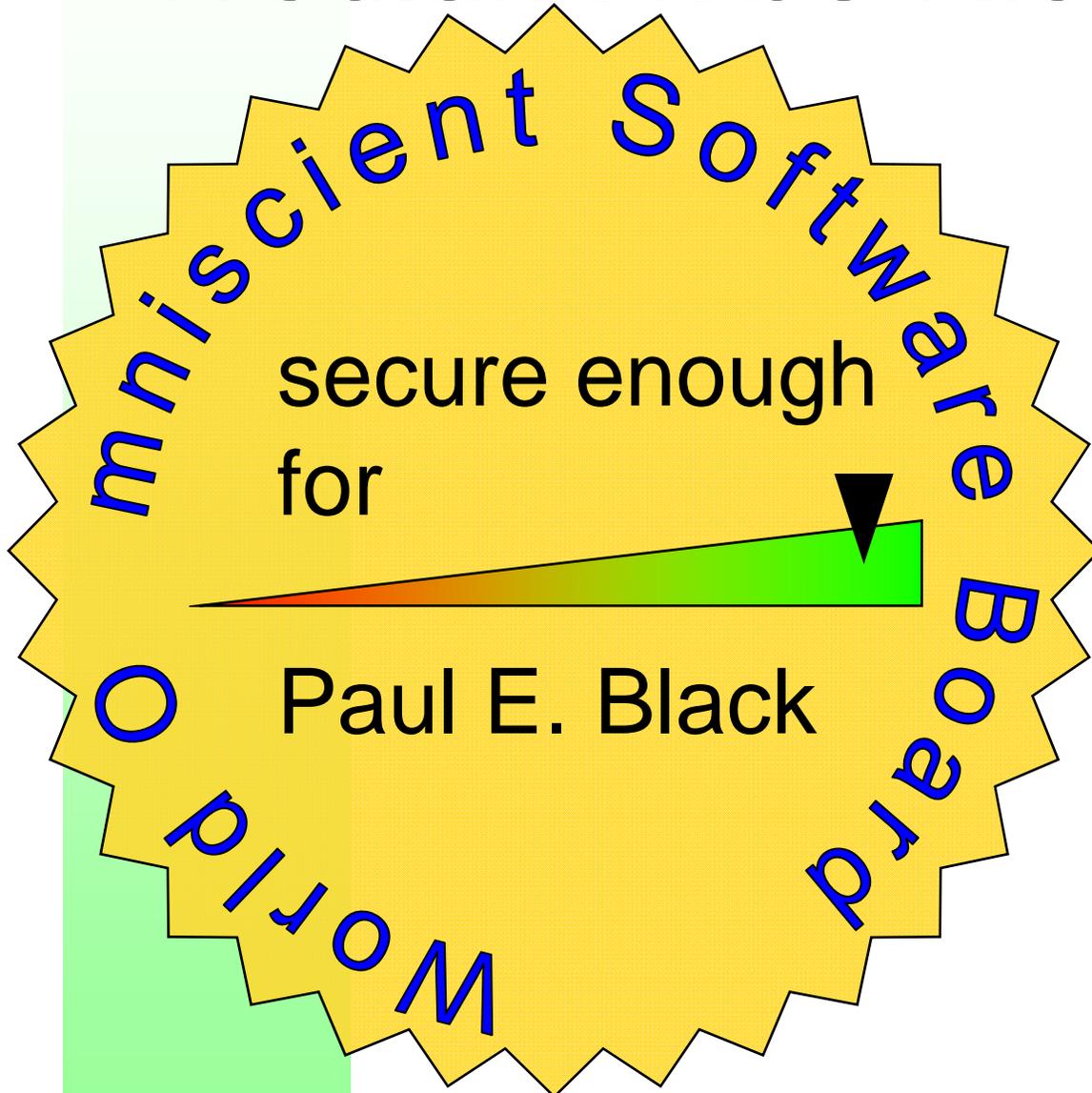
Paul E. Black

National Institute of Standards and Technology

<http://www.nist.gov/>

paul.black@nist.gov

Wouldn't it be Nice ...?



10 November 2008

NIST

National Institute of Standards and Technology • U.S. Department of Commerce

Paul E. Black

2

What are the Goals?

- **Inform “buy” decision**
 - Buy A vs. buy B
 - Buy vs. no buy
- **Convey secure settings**
 - E.g. for home computers
- **Feed risk or other assessment**
- **Lead to more secure software**

Audiences & Scope

1. **Naïve home users (my brother)**
 - **General applications (not OS or security-specific)**
2. **Small businesses (dentist, dry cleaner, accountant, plumber, restaurant)**
 - **General applications running on general purpose hardware (accounting package on a “PC”)**
3. **Integrators (incoming software is just one piece)**

What are Criteria for Facts?

- **First, do no harm**
- **Voluntary**
- **Uniform**
 - **May be different for different audiences**
- **Low impact for those doing “the right thing”**
- **Absolutely simple to produce or extract**
- **Based on science**
- **Not trivial or useless**

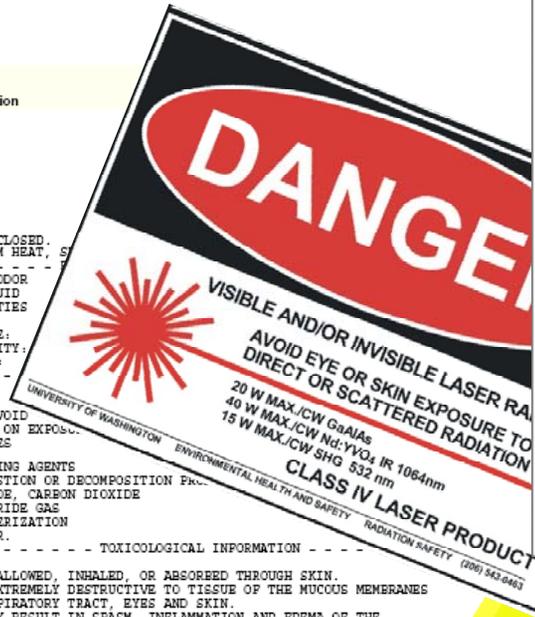
Many Information Models Exist

Product Number:335975
 Product Name:(+)-1-(9-Fluorenyl)ethyl chloroformate solution

James' Ben

Aldrich Chemical Co., Inc.
 1001 West St. Paul
 Milwaukee, WI 53233 USA
 Tel: 414-273-3850

SECTION 1. - - - - - APPEARANCE AND ODOR
 SECTION 2. - - - - - PHYSICAL PROPERTIES
 SECTION 3. - - - - - STABILITY
 SECTION 4. - - - - - TOXICOLOGICAL INFORMATION
 SECTION 5. - - - - - CHRONIC EFFECTS
 SECTION 6. - - - - - SECTION 7. - - - - - SECTION 8. - - - - - SECTION 9. - - - - - SECTION 10. - - - - - SECTION 11. - - - - - SECTION 12. - - - - - SECTION 13. - - - - - SECTION 14. - - - - - SECTION 15. - - - - -



Nutrition Facts	
Serving Size 1 cup (228g)	
Servings Per Container 2	
Amount Per Serving	% Daily Value*
Calories 250	Calories from Fat 110
Total Fat 12g	18%
Saturated Fat 3g	15%
Trans Fat 1.5g	
Cholesterol 30mg	10%
Sodium 470mg	20%
Total Carbohydrate 31g	10%
Dietary Fiber 0g	0%
Sugars 5g	
Protein 5g	
Vitamin A	4%
Vitamin C	2%
Calcium	20%
Iron	4%



Based on standard U.S. Government tests

ENERGYGUIDE

Use the Energy Use of this Water Heater with Others Before You Buy.

Uses Most Energy 422

Based on a 1998 U.S. Government national average cost of \$0.116 per therm for natural gas.

\$ 116

Based on energy use, your utility company uses it to compute your estimated yearly operating cost is:

No security problems found by methods that will be out of date by Apr 2009, but that doesn't mean you don't have security problems that we didn't find.

Possible Content: People/Process

- **People**

- Is there code accountability or responsibility assigned?
- Is there a trained, certified, or accredited application security “Software Engineer”?

- **Process**

- Secure coding practices followed
- Was a threat model defined?
- Are there requirements?
- Testing methodology
 - Black box, unit security testing, penetration testing, ...
- Tested on what platforms?
- Code reviewed? other than by developers? for security?
- Static analysis

Possible Content: Software Itself

- **Pedigree: amount from libraries, from Open Source, compiler**
- **Design: encryption, single points of failure, architecture signed off by app sec certified software engineer**
- **Provenance: protection of code in supply chain**
- **Traits: all communication over SSL, uses Internet or email**
- **Size: lines of code, function points, number of modules**
- **What and where are configuration files?**
- **% “banned” APIs, # “unforgivable vulnerabilities”**

Next Steps

- **Build a community**
- **Plan to put facts into practice**
- **Begin selecting from possibilities**

- **To participate, contact**
 - **Daniel G. Wolf**
 - **Software Assurance Consortium**

 - **Paul E. Black**
 - **NIST**

