We Need Assurance

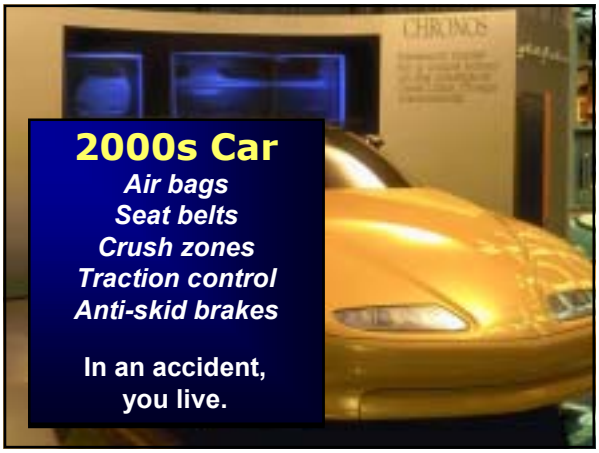
Brian D. Snow

Technical Director
Information Assurance Directorate
National Security Agency

1930s Car

Looks nice
Goes fast

But in an accident, you die.



2000s Car

Air bags
Seat belts
Crush zones
Traction control
Anti-skid brakes

In an accident, you live.

or

"It's ASSURANCE, Stupid"

Who will be the "Toyota" of the security industry?

Market share gained by reliability and quality!

Ten Years From Now

Buffer overflows will still exist in "secure" products

"Secure" operating systems will still crash when applications misbehave

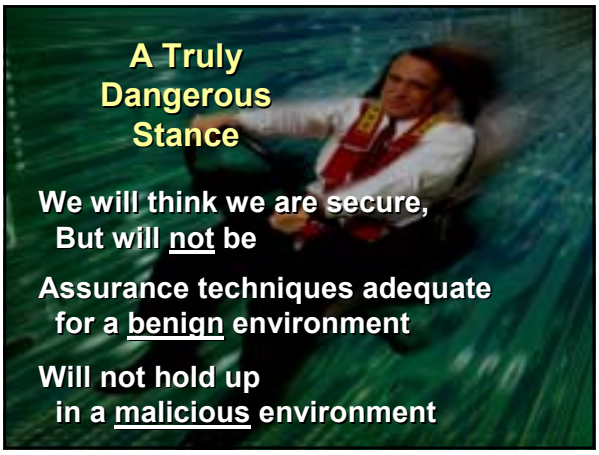
We will have:
Sufficient Functionality,
Plenty of performance,
But not enough ASSURANCE.

In The Next Five Years

We will counter many "hacker" attacks

But will not be safe from Nation States

National Security Agency



Assurance

- Confidence building activities that show
  - System possesses desired properties and only those properties
  - Functions are implemented correctly
- Assurance activities differ during
  - Manufacture
  - Delivery
  - Life cycle

National Security Agency

Assurance Provided Through:

- Structured design processes
- Documentation
- Testing

Six Major Areas:

Operating Systems
Software Modules
Hardware Features
Systems Engineering
Third Party Testing
Legal Constraints

Operating Systems

Digital Signature Check
prior to module execution

Self-Protective

Least-Privilege
type-enforcement, process-isolation

Enforce Security Policy

National Security Agency

Operating Systems

"Systems built without requirements cannot fail; They merely offer surprises. Usually unpleasant!"

Robert Morris

National Security Agency

Operating Systems

Operating System Security is the Foundation of System Security!

National Security Agency

Software Modules

- Well Documented
- Certified Development Environments
- Tested for
  - Boundary conditions
  - Invalid inputs
  - Improper sequences of commands
- Shown to meet Specification exactly, With no unexpected behaviors.

National Security Agency

Hardware Features

SmartCards
SmartBadges
Tokens
or other devices

to obtain
isolated processor and address space for assured operations

"An Island of Security"

National Security Agency

Systems Engineering

Using modules of unknown quality

- Partitioned Design
- "Blinded" Interfaces
- Mutual Suspicion
- Design Reviews for
  - -- Quality
  - -- Responsiveness to requirements
- Layered Defense

National Security Agency

Third Party Testing

NIAP Labs
Industry Consortia
Other

to obtain

Independent verification of vendor claims

Understandable By Users!

National Security Agency

Legal Constraints

"Due Diligence"

"Fitness-for-use" criteria

Liability

National Security Agency

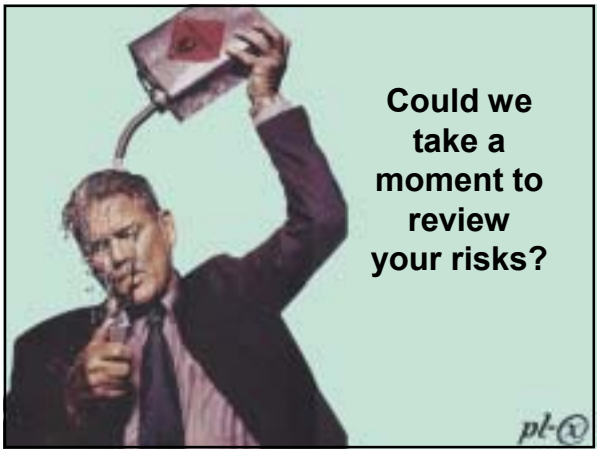
Summary

Most attacks result from failures of Assurance, not Function.

So We Need:

Focus on Using Assurance Technology in Products

National Security Agency



Brian D. Snow
Technical Director
Information Assurance Directorate
National Security Agency

b.snow@radium.ncsc.mil
(301) 688-8084