Why Building Trusted Computer Systems is our Only Hope

Robert Bigman
2BSecure
http://2bsecurellc.vpweb.com/
Rybbigs@GMail.com
Why Building Trusted Computer Systems is our Only Hope

**Agenda:**

* Why we Have Cyber Security Crises
* What is a Trusted Computer System
* A Very Quick History of Trusted Computing
* The Orange Book Legacy
* How Trusted Computing Lessons Addresses Today's Challenges
* A Recipe for the Future
Why Building Trusted Computer Systems is our Only Hope

Why we Have a Cyber Security Crises:

* Sophisticated hackers know that security vulnerabilities are always found inside untrusted firmware, O/S and application code
  * About 95% of the code inside today's systems is untrusted (and the number is only going up)
* Modern systems (including IOT) have no security model or attested trusted processes
* Firewalls, encryption, white-listing and threat intelligence address only symptoms of the crises
Why Building Trusted Computer Systems is our Only Hope

What is a **Trusted Computer System**:

* From Wikipedia: A system that is relied upon to a specified extent to enforce a specified security policy
* A system built to resist **Subversion**
* A system where **Trust** can be **Attested** and **Continuously Proven**
  * A system that possesses a **Small** and **Verifiable Reference Monitor**
  * A system that can **Securely Detect** and **Report** subversion
  * A system that enforces a **Mandatory Access Control** policy
  * A system programmed in a **Highly Typed** language
  * A system with a **Trusted** Supply/Update Channel
Why Building Trusted Computer Systems is our Only Hope

A Very Quick History of Trusted Computing:

* Willis Ware's warning – 1966
* Early efforts (Multics and CP-67) – 1967-1970
* Anderson/Schell's reference monitor/security kernel - 1972
* Mitre PDP 11/45, first trusted security kernel – 1977
* The Orange Book – 1983
* Sun MLS Trusted Solaris (B2)/ DEC VAX SVS (A1) - 1990
* GEMSOS MLS (A1) on an X86 platform - 1992
* Trusted computing dark ages – 1993-2003
* SELinux – 2003
* Trusted Computing Group TPM - 2008
Why Building Trusted Computer Systems is our Only Hope

- Multics:
Why Building Trusted Computer Systems is our Only Hope

• The Orange Book:
Why Building Trusted Computer Systems is our Only Hope

• Trusted Computing Time-Line
Why Building Trusted Computer Systems is our Only Hope

The Orange Book Legacy:

* Begin with a **Security Model**
* **Establish, Attest** and **Maintain O/S Trust** (in an “untrustable” environment)
* Ensure a **Small/Simple, Verifiable Reference Monitor**
* **Establish “Trustable”** system coding standards
* Establish **Mandatory Access Control** rules
* Ensure **Complete** mediation of rules
* Ensure “**Trustable**” event **Audit**
* **Establish “Trustable” Supply Chain**
Why Building Trusted Computer Systems is our Only Hope

How Trusted Computing Lessons Addresses Today's Challenges:

* A security model can establish security requirements from firmware up through application software (think Apple IOS)
* A security architecture can map all interactions between firmware, O/S and application software
* A “provable” security reference monitor can mediate all access decisions
* A programming standard can preclude code vulnerabilities
* A “trusted” security label can enforce access controls
* A protected kernel can report subversion/potential misuse
Why Building Trusted Computer Systems is our Only Hope

A Recipe for the Future:

* Time for a new public-private partnership
* Begin with the NIST cyber security framework
* Start with NIST Special Publication 800-160
* Include representatives from governments, vendors, user communities, academia, standards organizations and privacy advocates
* Publish a set of requirements for building/maintaining next generation trusted systems
* Hold a NSF/NIST sponsored competition (similar to the crypto. competition) to build operational models
* Establish a new CCR Arrangement program to test and rate systems based on requirements
Why Building Trusted Computer Systems is our Only Hope