New Realities

Modern Societies are critically dependent on computing and telecommunications

Same Terms → New Meanings

- WMD
  - Weapons of Mass Disruption
- Proliferation
  - Connected devices and software
- Critical Infrastructure Protection
  - Protecting the Internet and devices attached to it
The Dream

FBI

Field Personnel

CIA

Analyst

Staff

State Department

Embassy Staff

Staff

Coast Guard

Staff

State Licensing Bodies

Customs INS

Secure, private, reliable, and granular data interoperability across organizational boundaries at the edge of the network
...but this can not happen until computer systems are trustworthy...
High Confidence Systems

- Security
- Privacy
- Reliability

TRUST
Hardware Securing Software

Chain Of Trust

- Applications
- DRM/Crypto
- Identity
- OS
- Virtualization/Hypervisor
- Trusted Hardware
Identity

Identity for:
- Trust
- Access

Identity for Machines

Identity for People

Identity for Programs
Privacy

- No privacy without security
- Global information flows forcing a rethink of Privacy
- Role-based access control:

**Role: ADMINISTRATOR**
access: All Access

**Role: ACCOUNTANT**
access: Restricted To Financial Information

**Role: DOCTOR**
access: Restricted To Medical Information
Parallel features are worked out by teams of wizards most people just do what they’re told – Microsoft Engineer
Complexity

Complexity of developing, testing, and supporting large scale software systems continues to escalate.

Today's Software Development Process (Large Projects):
Only 13% of projects are on time!

Source:
- Capers Jones, Estimating Software Costs, pg. 140
- Capers Jones, Patterns of Software Systems Failure & Success
Going Forward

Dealing effectively with concurrency and complexity to build reliability

- Loosely-coupled
- Asynchronous
- Concurrent
- Composable
- Decentralized
- Resilient Systems

Concurrent Complexity

Verifiable composability + Protocol-oriented programming
We (the DoD) need to pay a great deal more attention to supporting peer-to-peer relationships and information exchanges that transcend individual systems and organizations. Doing these things will empower the edge of the organization and enable us to change the way we approach everything we do.

John Stenbit – Power to the Edge (Forward)
NGSCB + DRM: Intermediate Vision

Beyond ACLs

Content is protected from unauthorized users or applications

DRM (strengthened by NGSCB) establishes rights and allows content to be viewed

Guard between networks ensures data is protected by DRM

User creates DRM protected content on NGSCB machine

Guard required because hardware runs both DRM aware and non-DRM aware applications
NGSCB + DRM: Long-Term Vision

Content is protected from unauthorized users

DRM (strengthened by NGSCB) establishes rights and allows content to be viewed

Data automatically protected at the moment of creation via DRM and NGSCB

A chain of trust is established via a powerful, flexible DRM system, secured with NGSCB
It Gets Better From Here

*Today*: complex software auditing and air gaps

*Tomorrow*...

Secure, private, reliable, and granular data interoperability across organizational boundaries at the edge of the network
discussion