

# Requirements for a Secure Information Infrastructure

Matt Curtin

September 18, 2002  
Dayton InfraGard

# Meta: Purpose

The purpose of this discussion is to stimulate thinking and intelligent discussion of this problem. I profusely apologize in advance to anyone on whose toes I do not step.

# Objectives of information infrastructure security (INFOINFRASEC)

Infrastructure must be reliable, able to support an information society.

- Availability
- Security
- Reliability

. . . Trustworthy.

# Current INFOINFRASEC Proposals

- Expanded police powers
- Fewer “administrative hurdles” (like warrants)
- Cryptography restrictions (“You’d think differently if al-Qaeda were using crypto.”)

# Current Direction Toward Centralization

- Strengthening law enforcement
- Getting lazy—“not my problem”

# The Net Must Remain Free

“Freedom itself was attacked.”

—President George W. Bush, September 11, 2001

“Securing the infrastructure” must not finish a job started by terrorism.

# Why It's Your Problem

Someone else can only protect you perfectly when he is:

- Omniscient
- Omnipotent
- Benevolent

# Public Servants Can Be Strengthened

- We can give them greater information, but their ability to process it will prevent them from achieving omniscience.
- We can give them greater power, but their humanity will prevent them from achieving omnipotence.
- Human history suggests that benevolence is, at best, rare.

## Strengthening Ad Absurdium

You might well enable a malevolent totalitarian regime, acting with imperfect information, imperfectly achieving its objectives.

## Moral of the Story

Omnipotent law enforcement is not only unworkable from a practical standpoint, but provides an avenue of attack against the “protected.”

# What If This Guy Were Working for al-Qaeda?



# The Founders Understood Power

*Power must never be trusted without a check.*

—John Adams, American Patriot, Second U.S.  
President

# Good Public Policy vs. Good Private Policy

- Optimization for a society that values liberty places certain limits on the ability to investigate and to prosecute possible crimes.
- Private networks don't exist to support free society. Adding policy and enforcing policy on the private networks is entirely reasonable.

# Scope

No one can protect it all; we each need to protect our own territory, and to cooperate with each other to protect it all.

Corollary: Law enforcement really is your friend, but must be peers, defenders of the public space, just as we in the private sector are defenders of private space.

# INFOSEC Principles

Information security isn't a "new" problem.  
Saltzer-Schroeder INFOSEC principles are just as applicable today as they were when proposed in 1975.

# Economy of Mechanism

*Pluralitas non est ponenda sine neccesitate*

—Occam

Everything should be as simple as possible, but no simpler.

—Einstein

## Fail-Safe Defaults

What happens *when*—not “if”—the system fails?

Bank vault power failure. Unlock and open door with remaining power, or close and lock door? (Both have issues; one leaves money unlocked, the other might trap someone inside.)

## Complete Mediation

No direct access. Working through a mediator provides a convenient point for access controls. (Also can provide audit trail.)

# Open Design

Transparency in design goes back even further than Saltzer-Schroeder; it has been the rule in crypto since the nineteenth century. (Military doesn't generally agree.)

Open source implementations take this one step further. Open design and open source are different (but related) issues.

## Separation of Privilege

The ability to perform one function should not imply the ability to do another.

Imagine being able to allow clerical staff to copy sensitive documents for people with the credentials to read them, without granting clerical staff the ability to read those documents. This would be a good example of separation of privilege.

# Least Privilege

You get no more rights than you need to fulfill your role.

When combined with Separation of Privilege, provides a powerful means of reducing potential areas for exploit.

# Least Common Mechanism

An operating systems example: userland programs, libraries, and kernels. Where to put the code?

## Psychological Acceptability

People are a part of the system. If they can't deal with it, they'll work around it. They'll break policy and cause other problems that undermine the security of the system.

Two nuclear scientists at Los Alamos leaked critical components of nuclear weapons to the Soviets. No amount of security can stop key insiders from harming you.

# Work Factor

Understand how much work it will take for the attack to work.

- e.g., safe ratings

# Compromise Recording

When all else fails, at least be sure to indicate that a breakin has occurred, and hopefully to preserve evidence that can be used for prosecution or litigation.

# INFOINFRASEC Requirements

- Robustness: rebuts attacks against infrastructure itself.
- Baseline policy optimized for liberty.
- Implementation of baseline in public spaces.

## INFOINFRASEC Requirements, 2

- Layer additional policy atop the baseline as needed to meet requirements of each zone. (Identification, authentication, confidentiality, integrity, etc.)
- Decentralization: control of one's own zone.
- Facilitation of cooperation among zones.

## INFOINFRASEC Requirements, 3

- “Trust but verify.” We need a way to verify that people with whom we interact are authorized agents.

Large problem right now; e.g., NIPC alerts and other information are hard to verify (no digital signatures).

## In a Nutshell

The Information Infrastructure will be safe only when it continues to work, even when the inevitable happens:

- Computer systems fail
- People do the wrong thing

# Contact

Matt Curtin

Interhack

5 E Long St Ste 1101

Columbus OH 43215

+1 614 545 HACK

<http://web.interhack.com/>