Frustrating an Adversary

* Prevent successful targeting of organization resources
* Host-based and Network-based measures
* Reduce the space of attacks that can succeed
* Can reduce only so far
* Goal is practical level of reduction

Asymmetry: Three cases of dependability:

* Sum of efforts
* Weakest link
* Best effort

Minimization:

* Reduce cross-service vulnerabilities
* Reduce unfamiliar or unknown services
* Blacklist or Whitelist

Host Hardening

Network Devices

* Minimize permitted traffic on organization network
* Several options (often combined in single devices)
* Access Control

Network Architectures

* Physical and logical connections
* Public spaces and private spaces

Verifiable Security

* Beyond scope of conventional operating systems:
* security as primary design goal
* Operational formal model of security