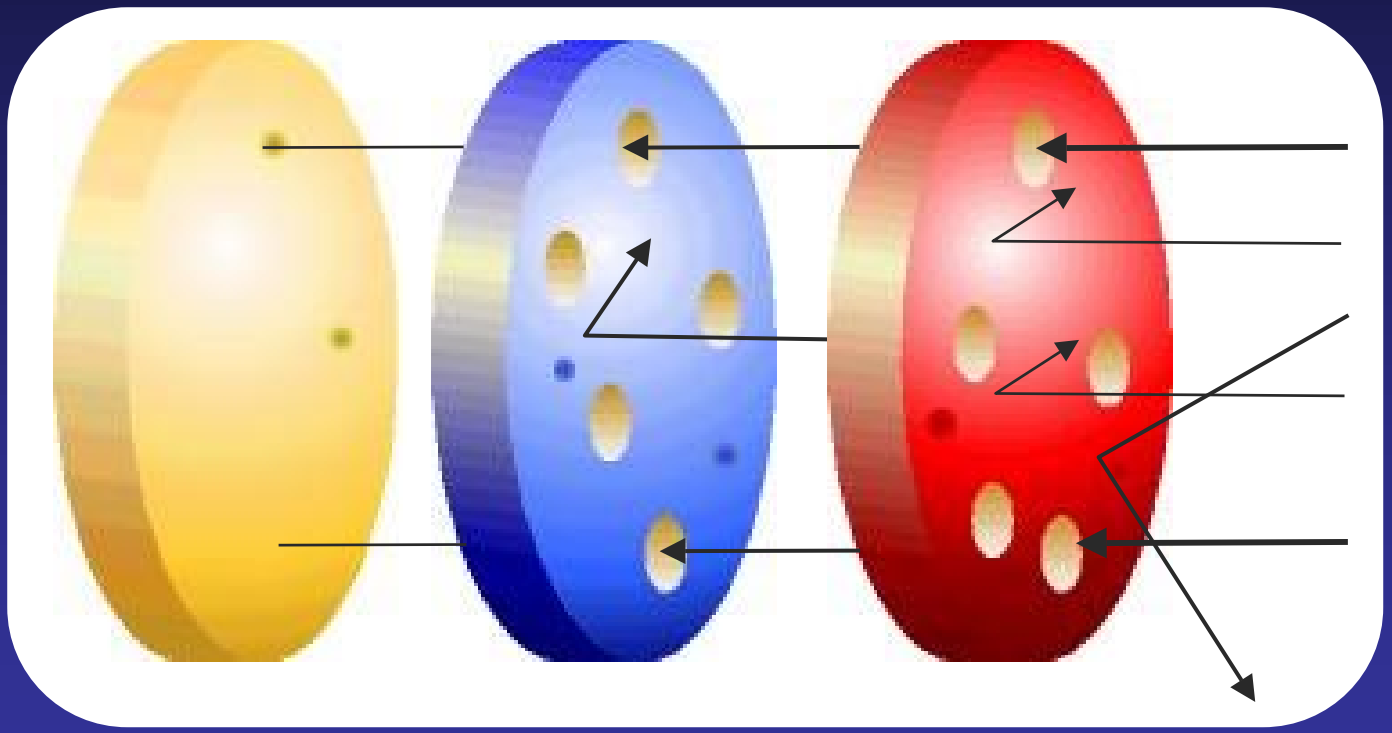
Inherent Information Survivability

Gary M. Koob
DARPA/ITO
gkoob@darpa.mil

ITO

Layered Defense

Tolerate Detect Prevent

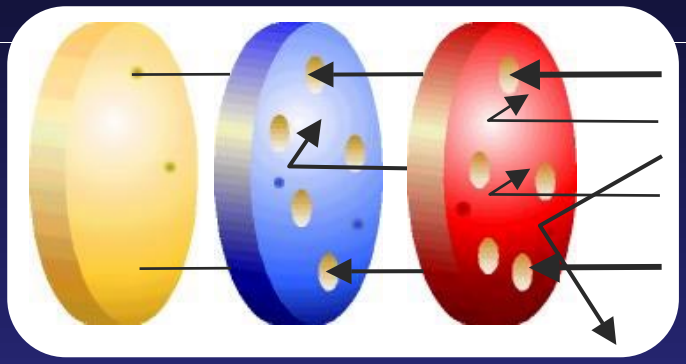


ITO

DARPA Strategy

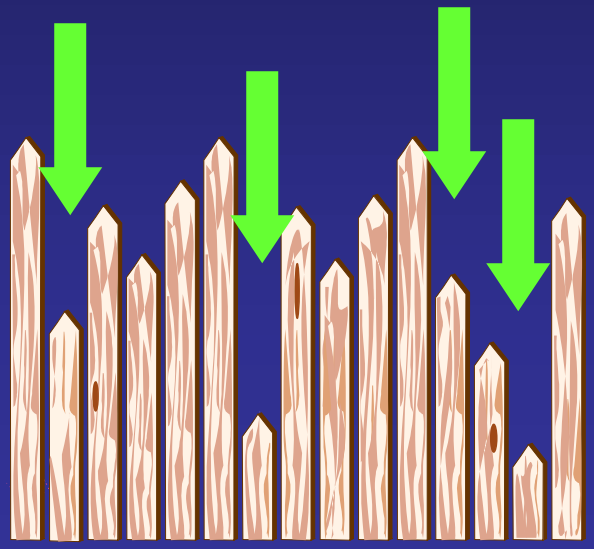
ITO

Address Critical Technology Gaps



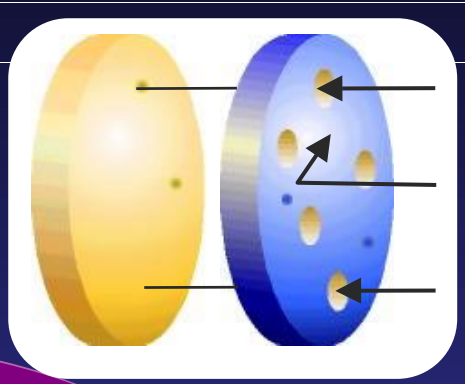
ISO

Integration for Balanced Protection

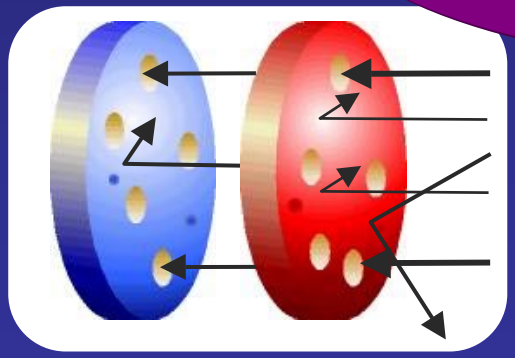


Roadmap

Inherent Survivability
1999-2003



ISO Info Assurance
1997-2000



Information Survivability
1995-1999

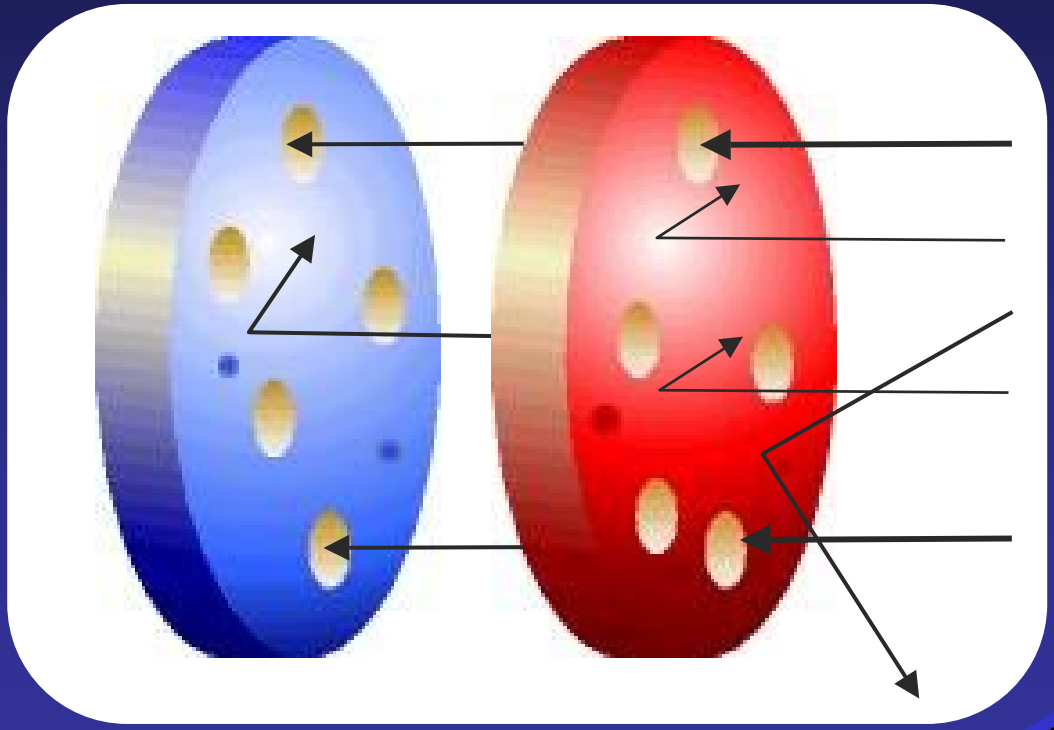
ITO

Accomplishments

Local Detection ***Strong Barriers***

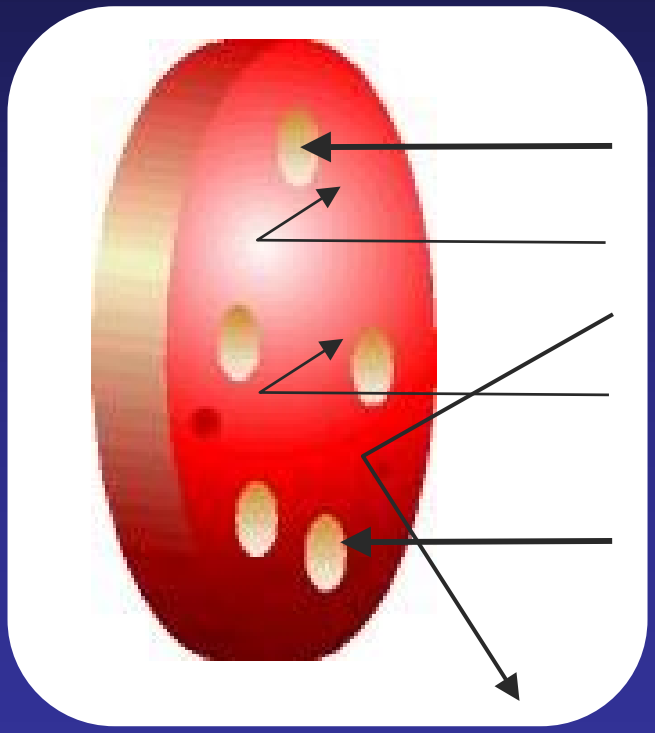
Information Survivability Program

1995-1999

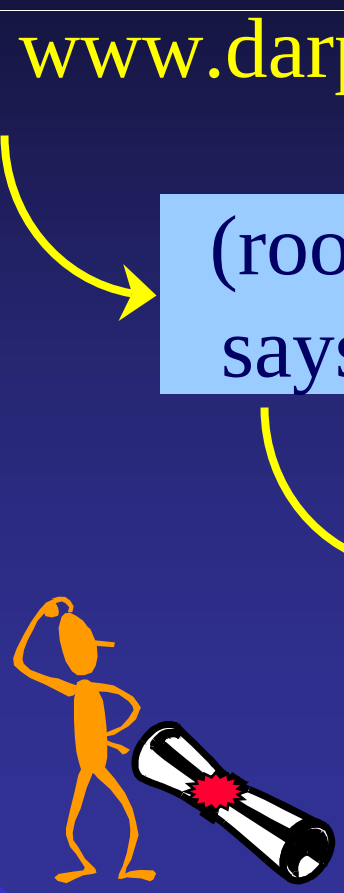


Strong Barriers

Develop strong barriers to penetration at all system levels

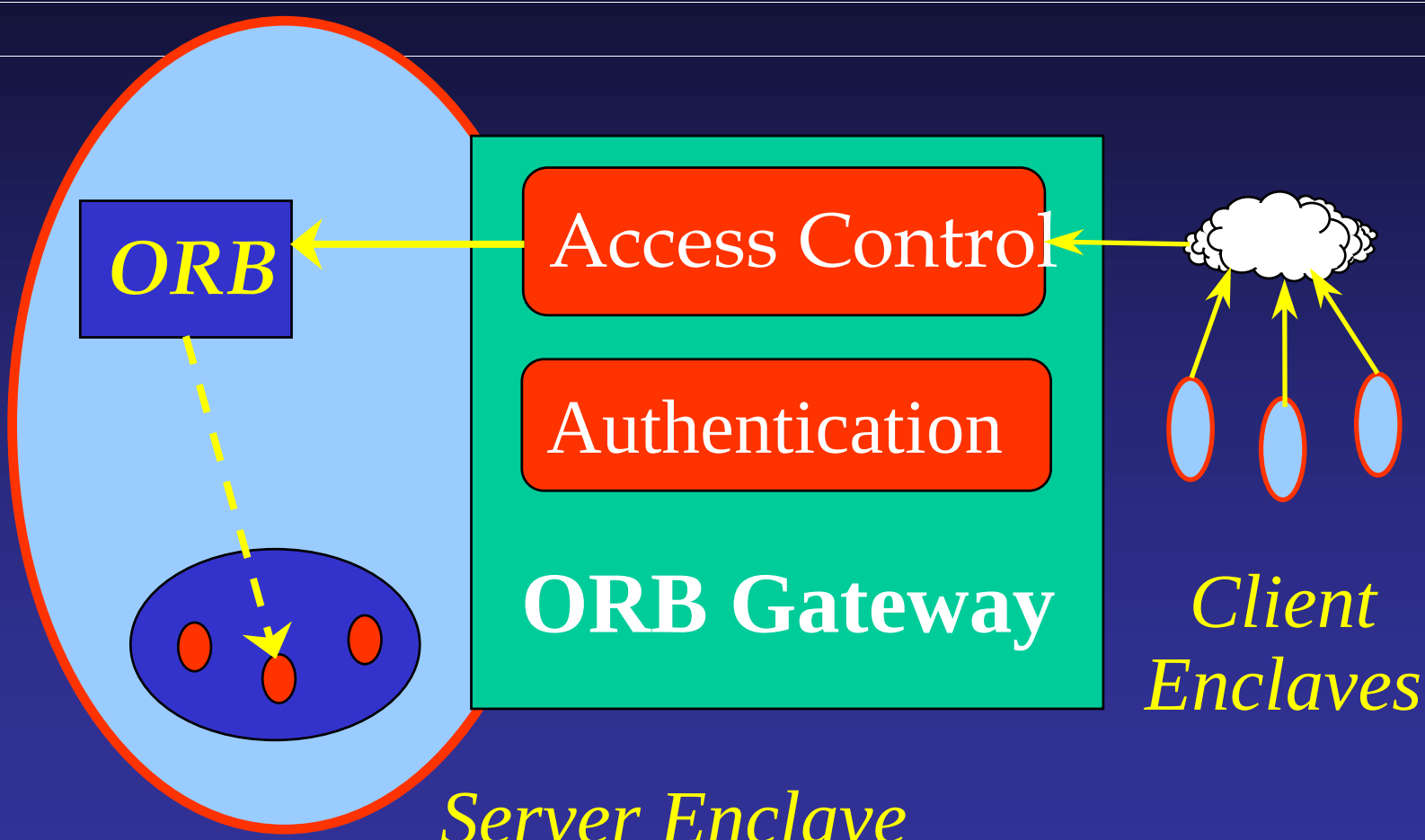


Network: DNS Security



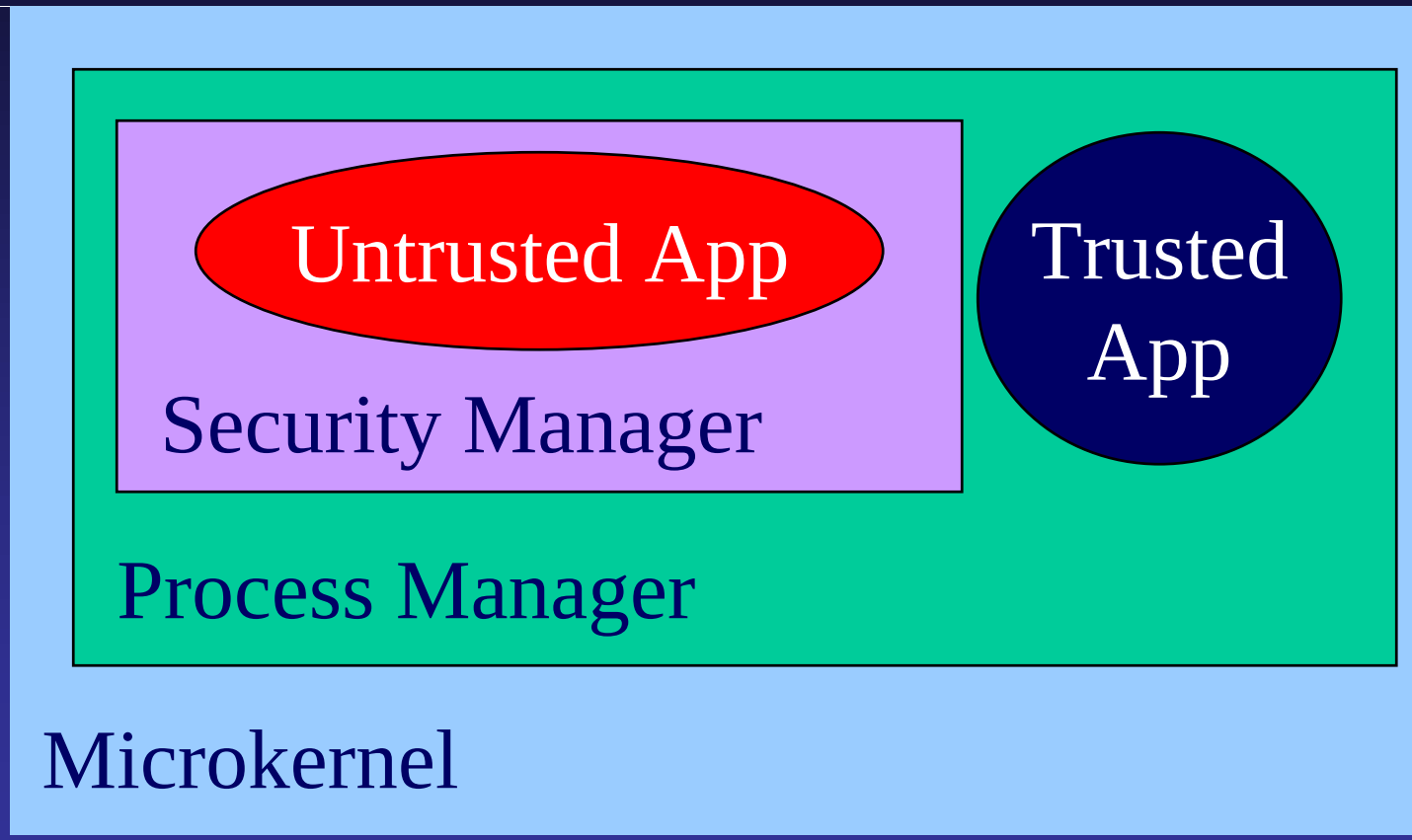
ITO

Middleware: CORBA



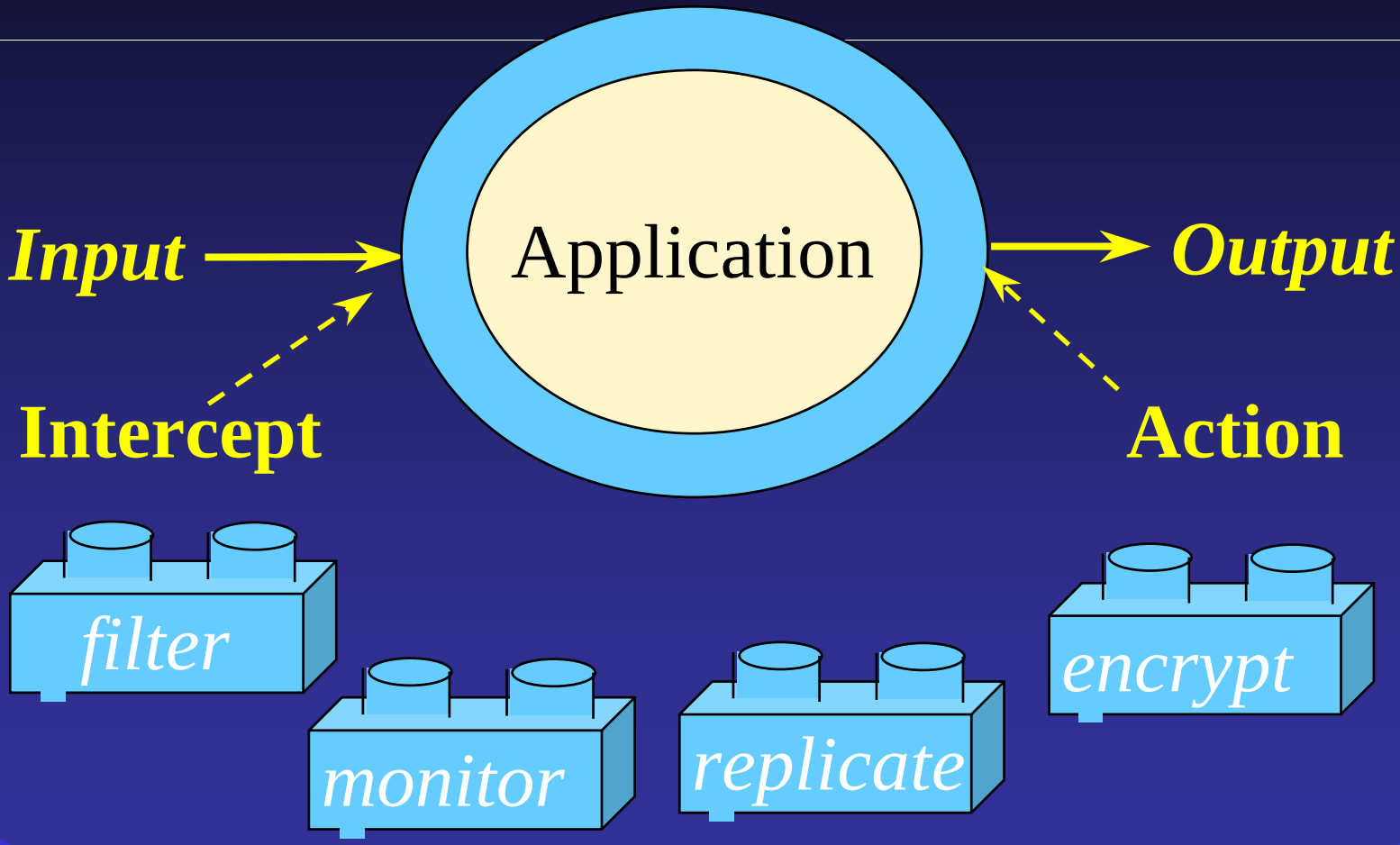
ITO

OS:Nested Processes



ITO

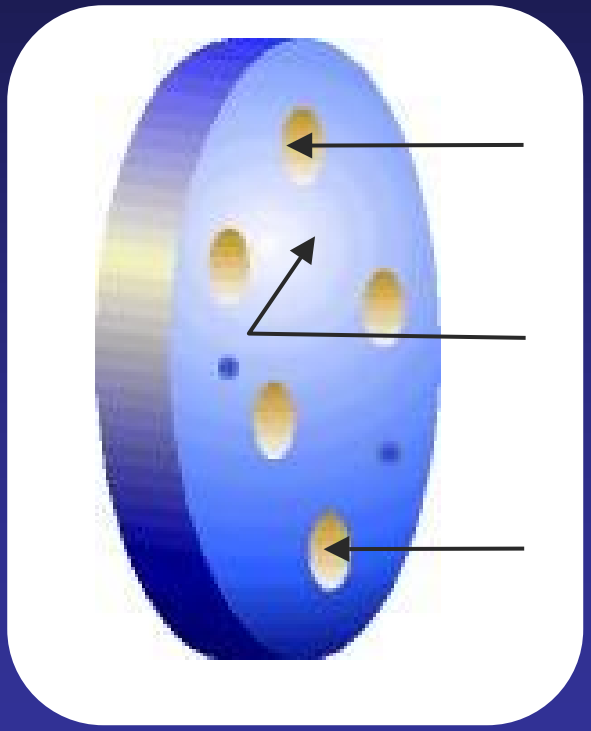
Application:Wrappers



ITO

Local Intrusion Detection

Detect attacks locally with high confidence and low false alarm rate

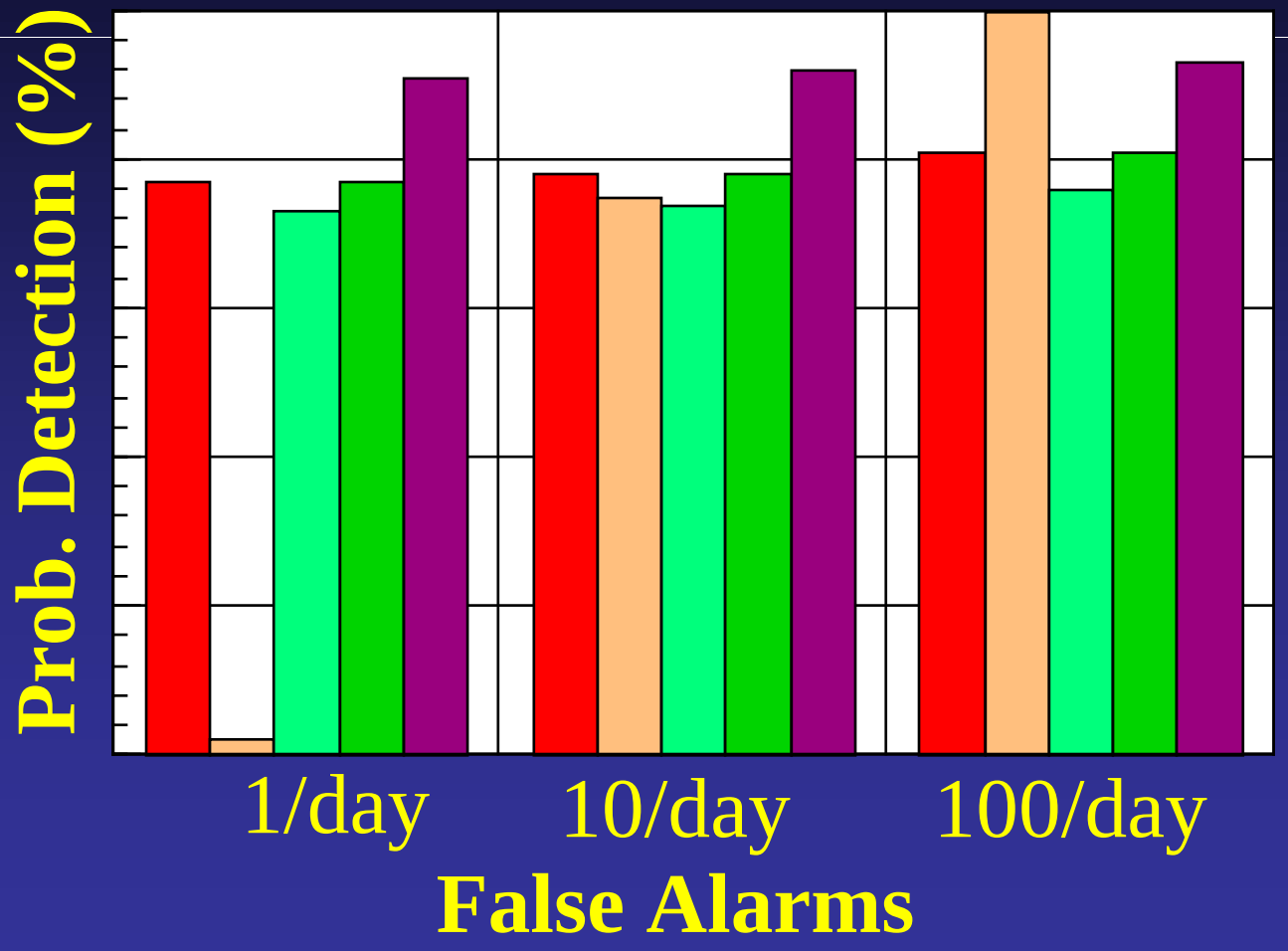


Intrusion Detection

- State-of-the-Practice
  - Pattern matching on known attacks
- Program focus
  - Statistical Anomaly Detection
  - Model-Based Profiles

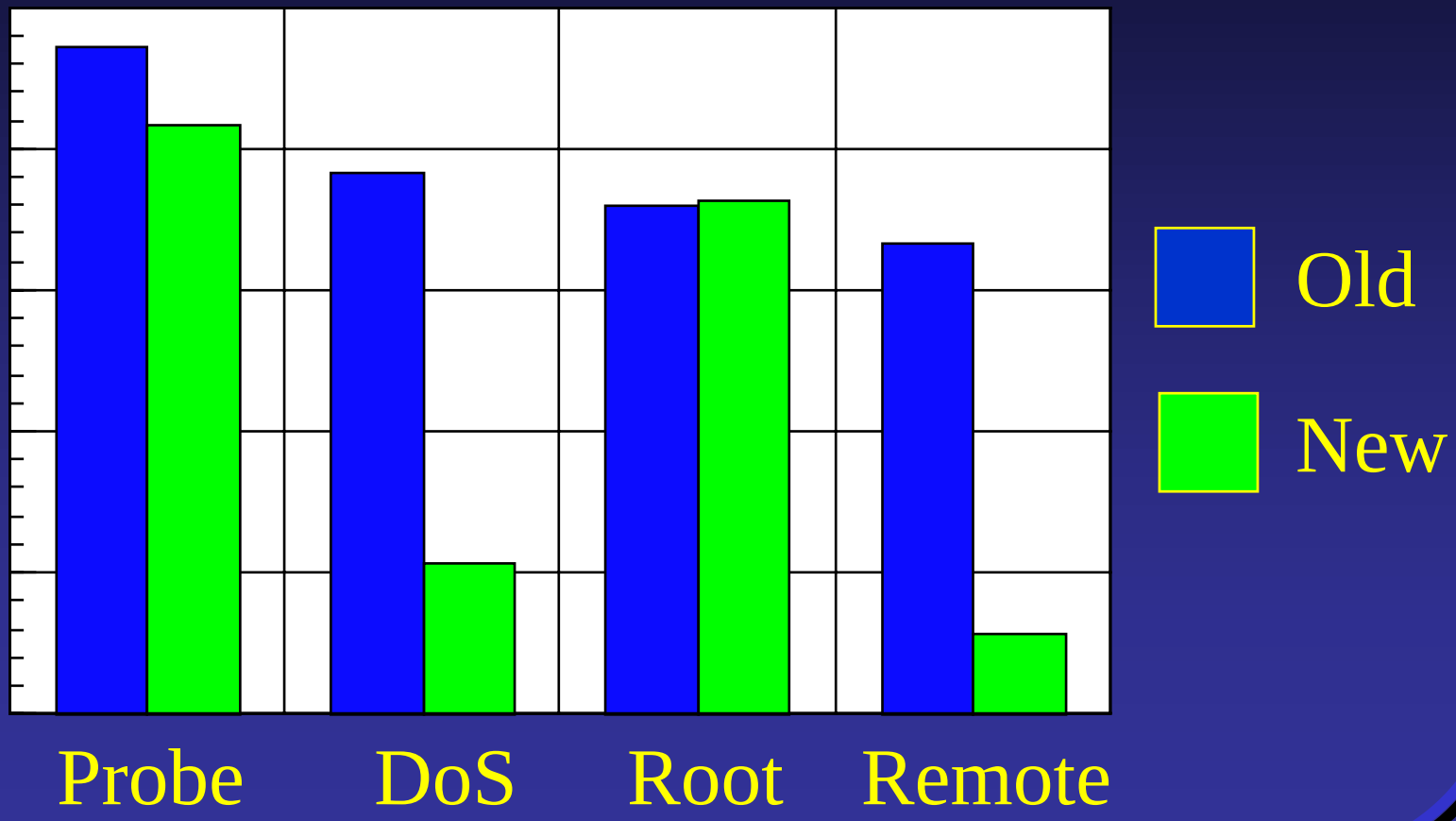
Detect Previously Unknown Attacks

Sample Results



ITO

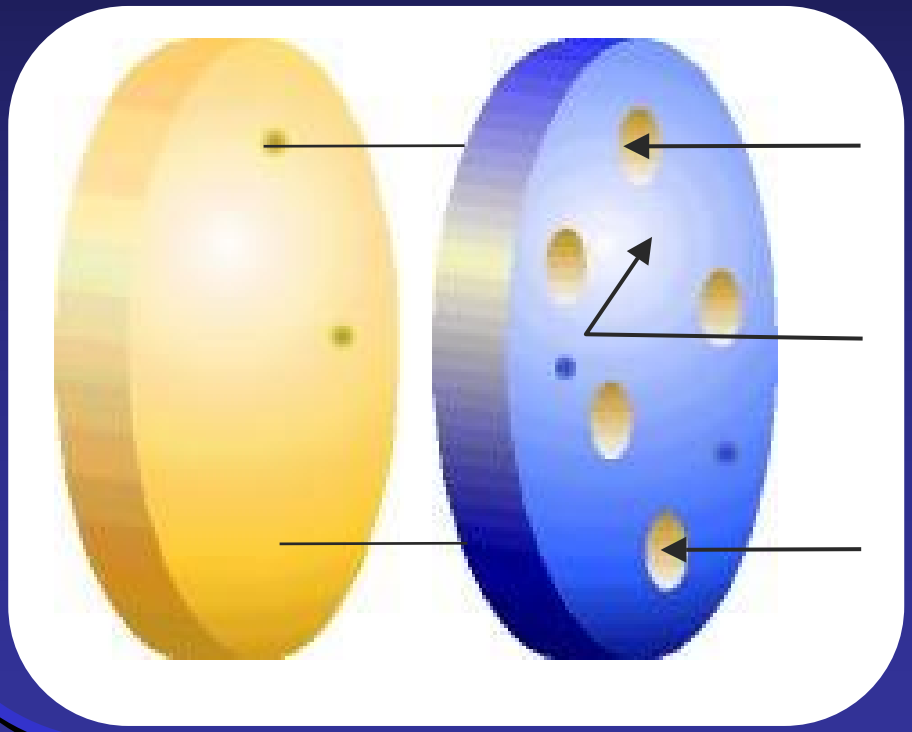
Old vs New Attacks



New Directions

Intrusion Tolerance

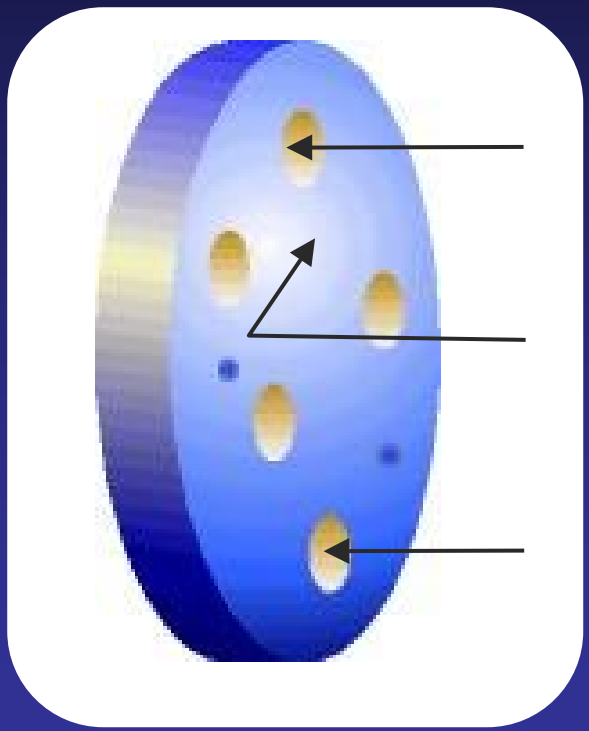
Global Detection



Inherent Survivability Program

1999-2003

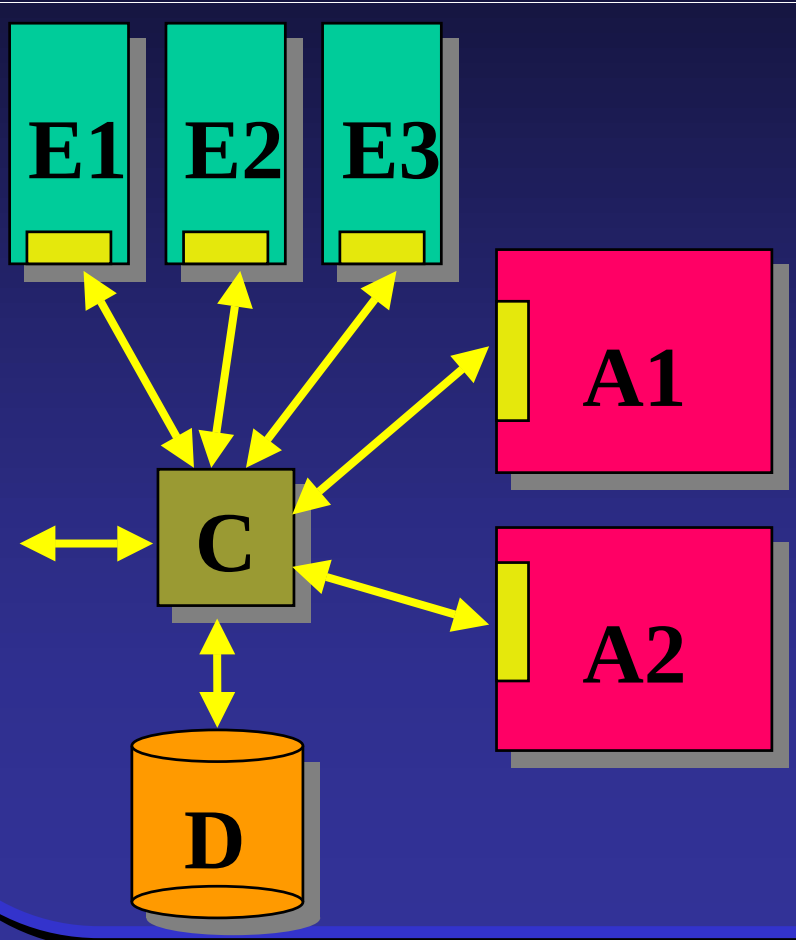
Global Detection



Distinguish events of elevated significance from those of only local interest

ITO

Common Intrusion Detection Framework



E Event Generator
A Event Analyzer
D Event Database
C Controller

Standard API

ITO

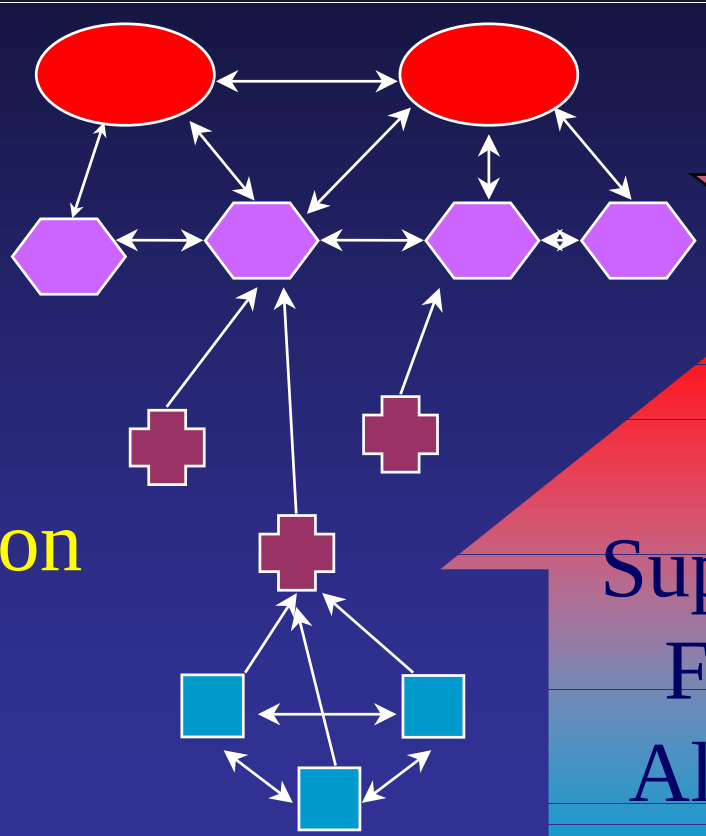
Intrusion Assessment

National

DoD

Organization

Local

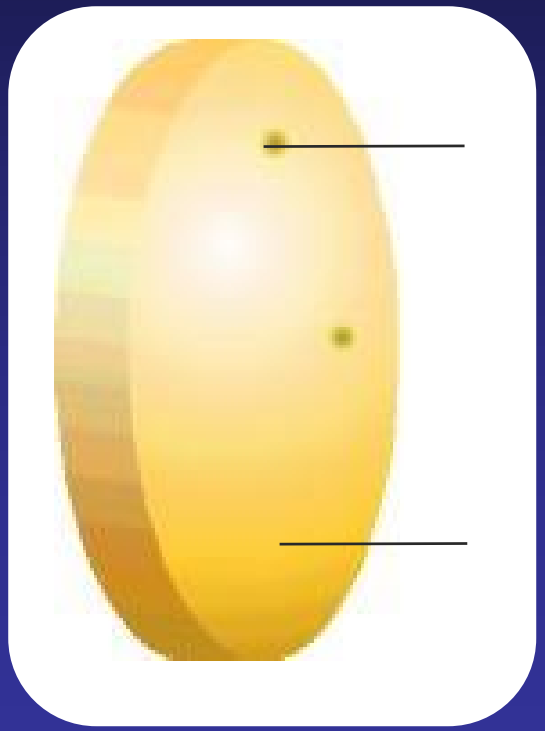


Global Context

Suppress False Alarms

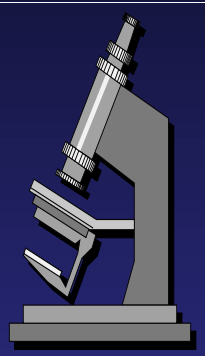
ITO

Intrusion Tolerant Systems



Maximize ability to continue critical operations following partial compromise

Data Integrity Marks

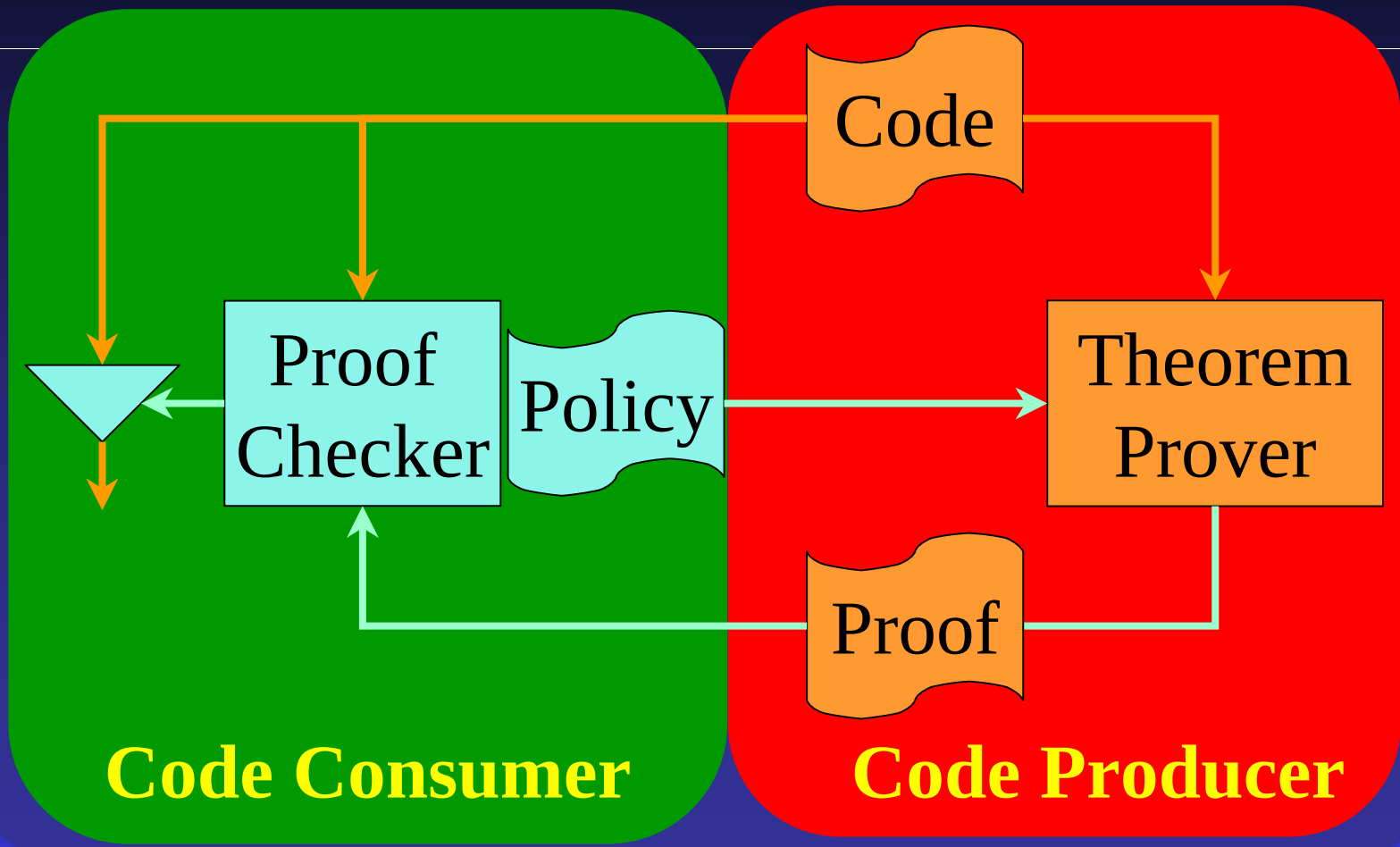


Wrapper:

- Verifies Marks
- Adds New One

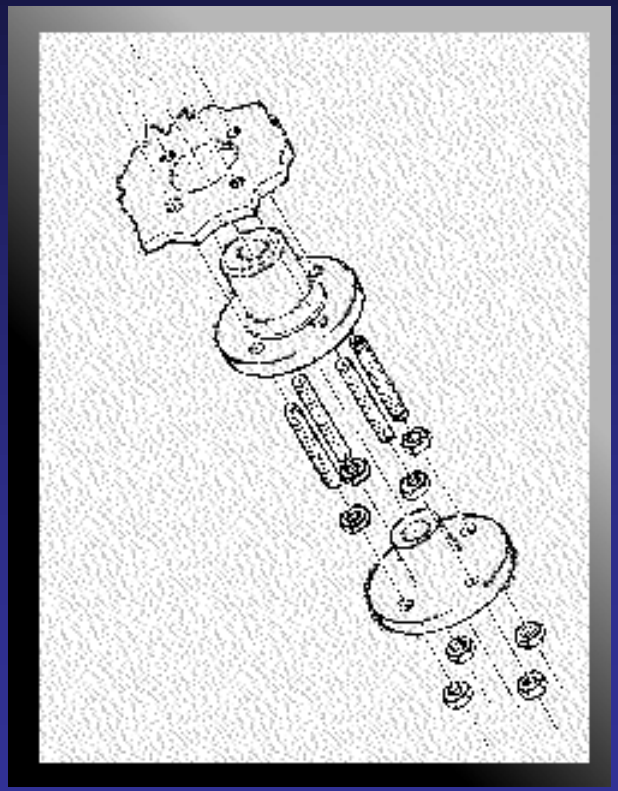
ITO

Proof Carrying Code



Tolerant Software

Analogy to Mechanical Parts



Tolerate:

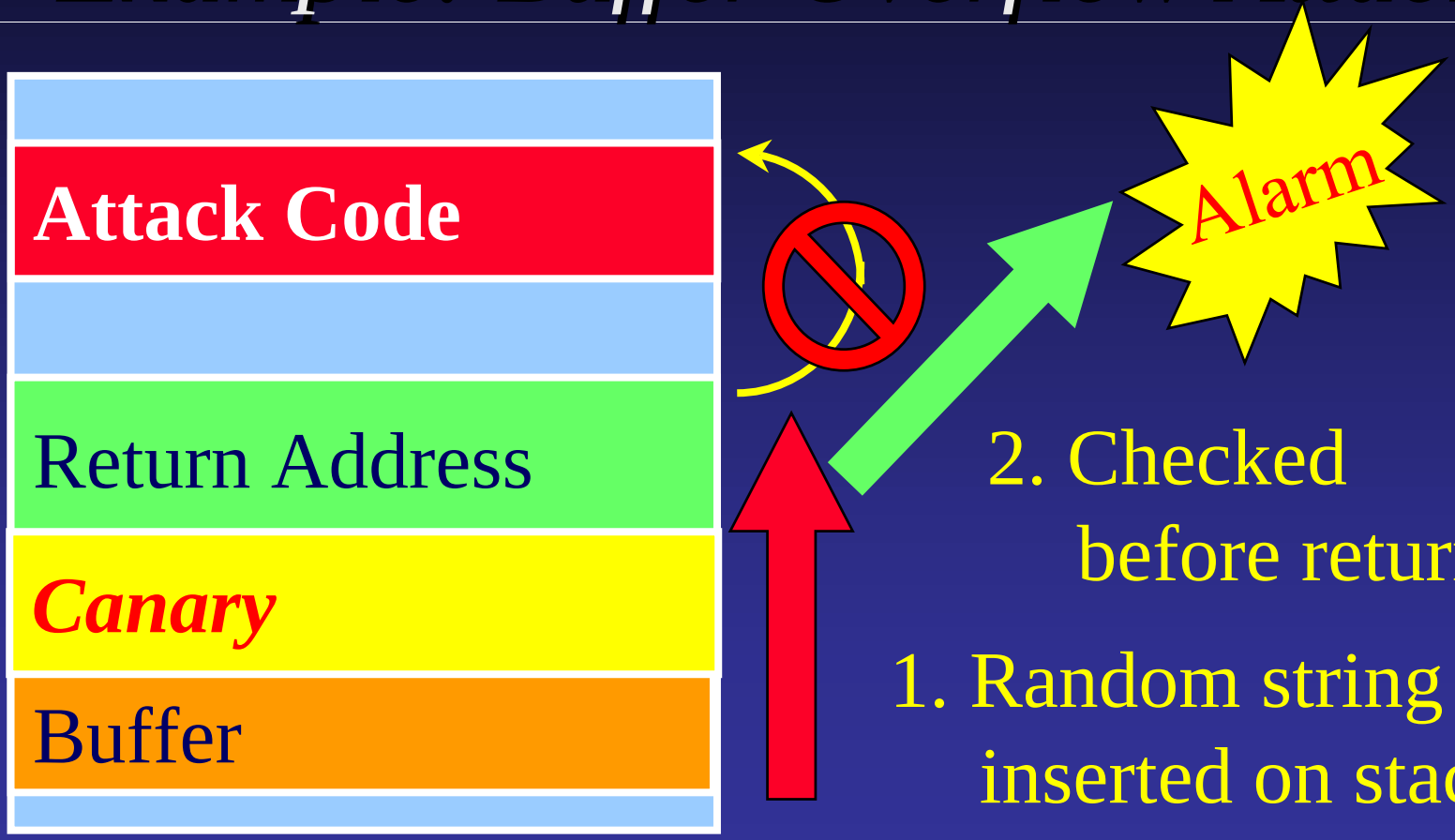
- Imprecision
- Completeness
- Latency

Ideas

- Active interfaces
- Probabilistic methods

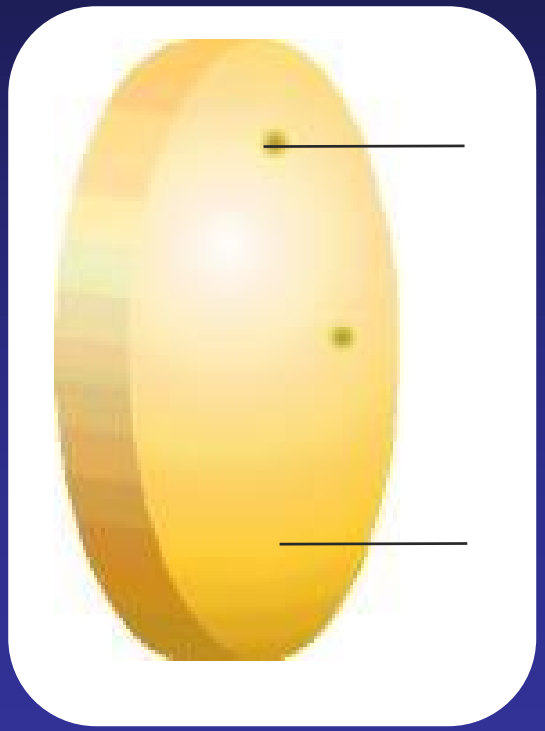
Artificial Diversity

Example: Buffer Overflow Attack



ITO

Intrusion Tolerant Networks



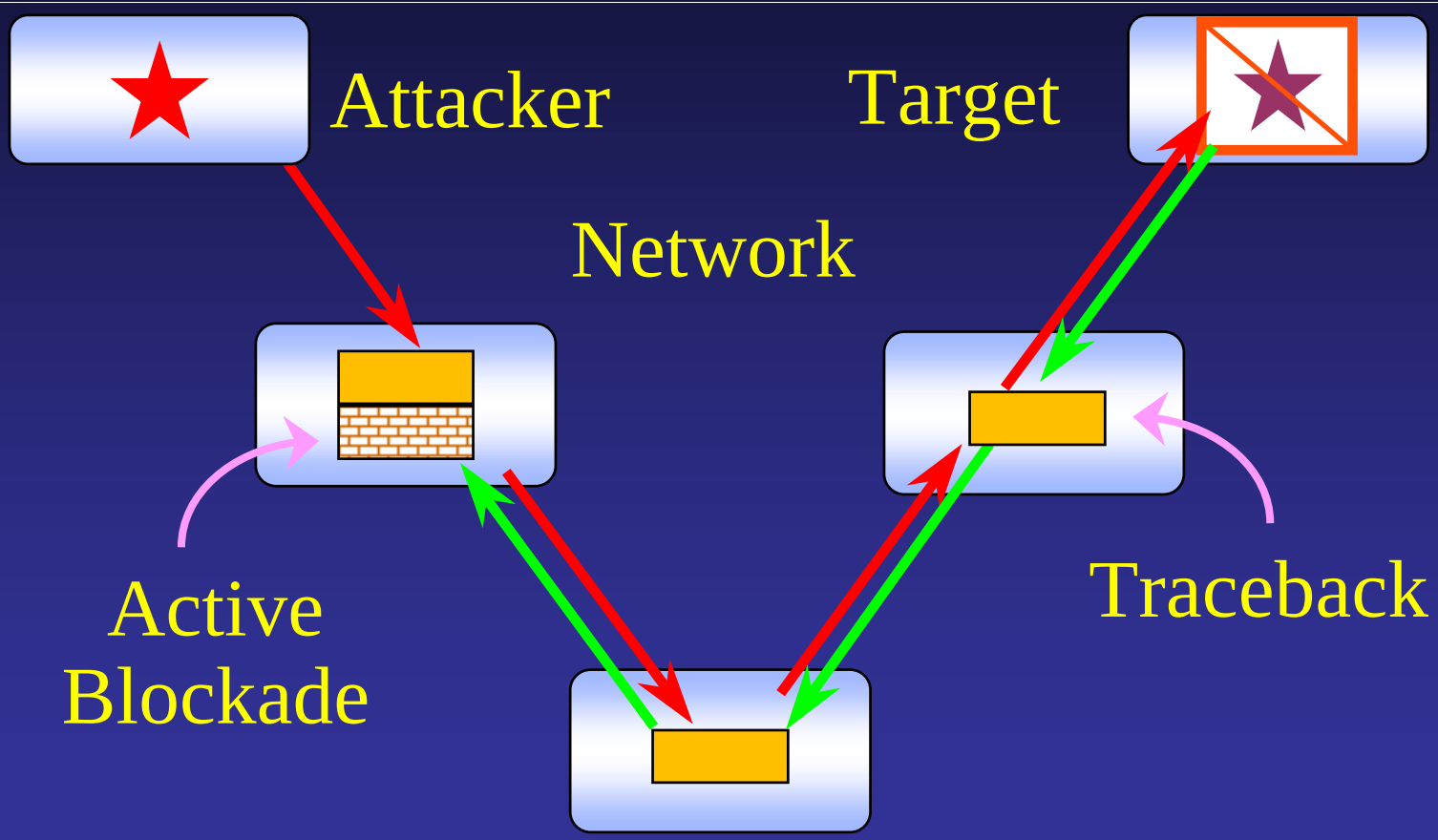
Maximize residual capacity of network infrastructure following partial compromise

Denying Denial-of-Service

Constrain attacker's resource consumption

- Market-Based Allocation
- Progress-Based Protocols

Active Net Response



Layered Defense

Tolerate **Detect** **Prevent**