DARPATECH 2000

ISO

Information Assurance & Survivability

Brian Witten

Information Systems Office

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	9/21/2000	Briefing 9/21/2000

4. TITLE AND SUBTITLE
Information Assurance & Survivability

5. FUNDING NUMBERS

6. AUTHOR(S)
Witten, Brian

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

DARPATECH 2000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

IATAC
3190 Fairview Park Drive
Falls Church, VA 22042

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

14. SUBJECT TERMS
IATAC Collection, information assurance, warfighter, malicious code, mobile agents

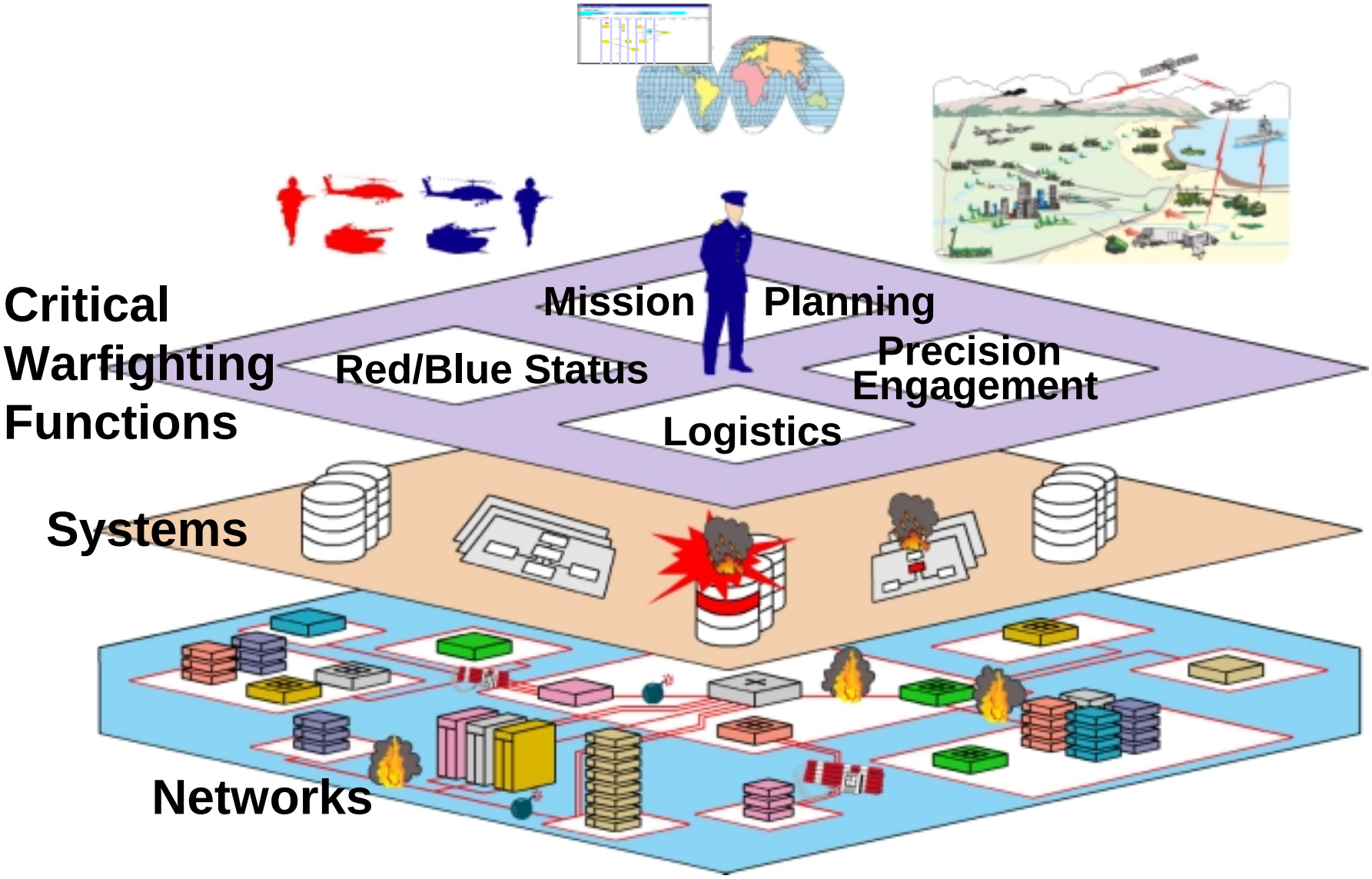
15. NUMBER OF PAGES
11

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

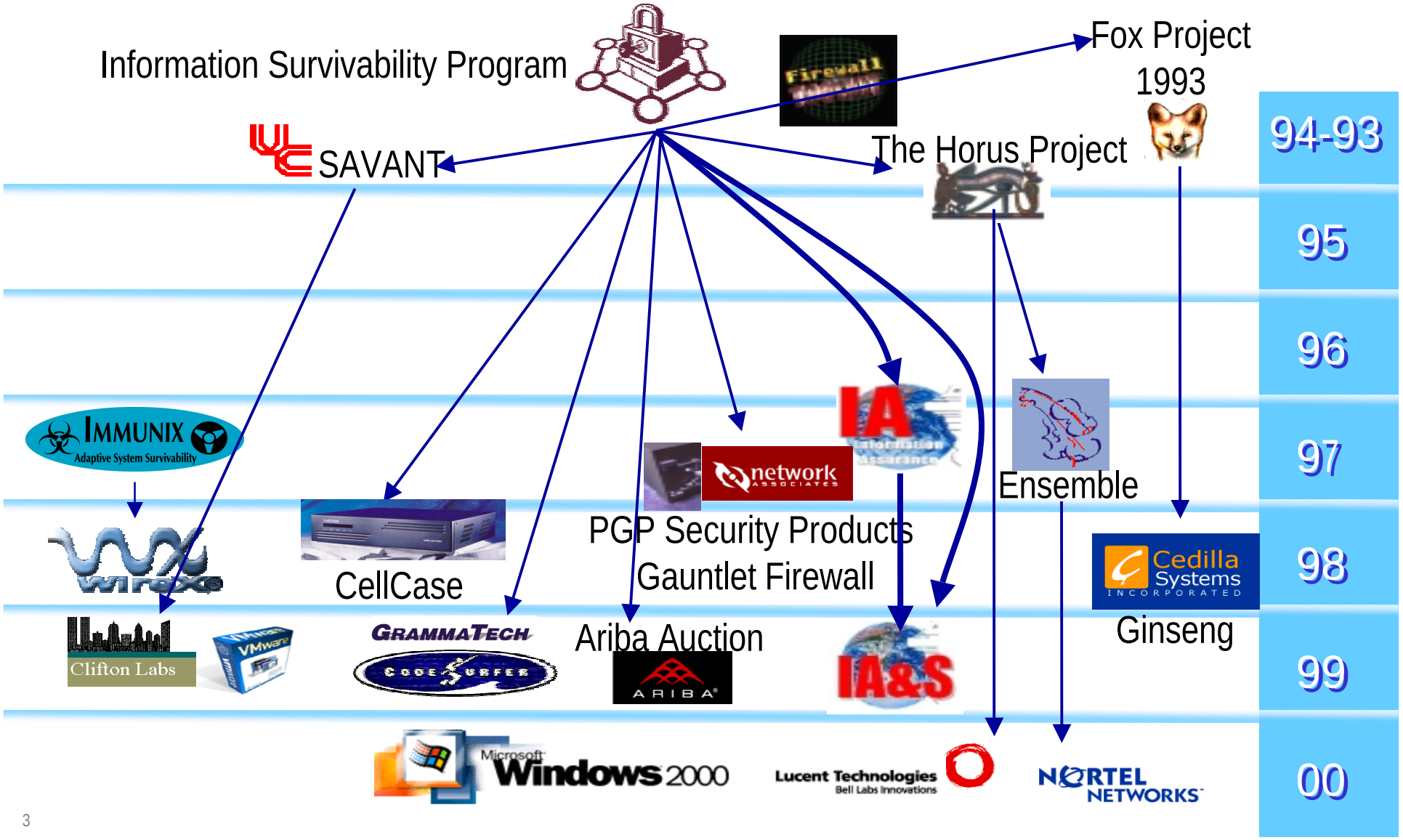
DARPATECH 2000 ISO

Can we trust the data we are fighting on?



History of Innovations

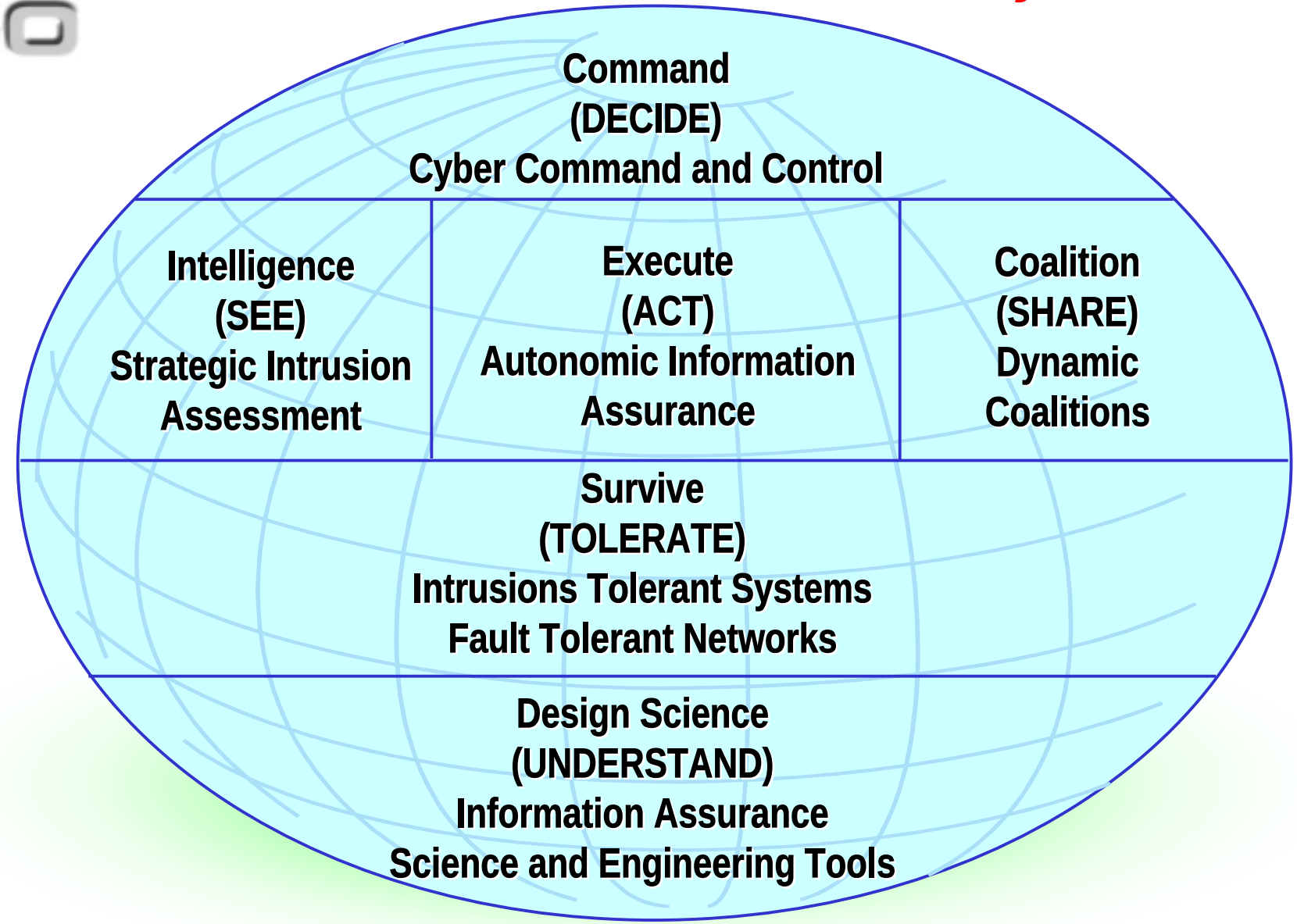
IS Conference Proceedings - http://schafercorp-ballston.com/discex



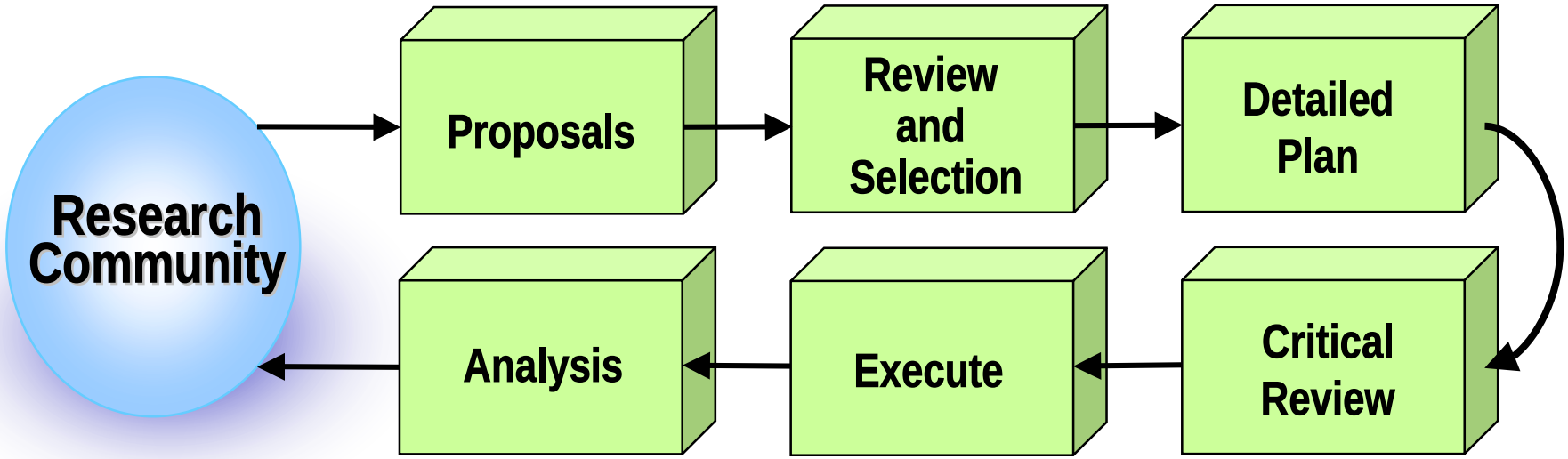

Long Road Ahead
Auto Forensics
Cyber Strategy
Autonomic Response
Course of Action Projection
Insider Attacks
Intrusion Assessment
IA Sensors
Adaptive Survivable Network Infrastructures
Adaptive Survivable Architectures
?
?
Malicious Code
Cyber Sensor Exploitation
Intrusion Detection
Protective Mechanisms
Crypto
Dynamic Policy
Situational Understanding
Composable Trust
Policy
Physical Security
Dynamic Coalition
Modeling/ Simulation
Lifecycle Attacks
Formalized Design & Assessment
Multi-Level Security
?

DARPATECH 2003
ISO

Objectives



Approach: Scientific Experimentation



Grand Hypotheses:

- Layered Defense
- Dynamic Defense
- Assurance Methodology
- Automated Response
- Automated Decision Support

Types of Experiments:

- Field Experiments
- Red Team Lab Exercise
- Laboratory Experiments
- Interdisciplinary White-Boarding
- Component Specific Testing

DARPATECH 2003

ISO

Contact

Autonomic Information Assurance…… **Brian Witten**
Dynamic response bwitten@darpa.mil

Cyber Command & Control……. **Catherine McCollum**
Human directed strategy cmccollum@darpa.mil

Dynamic Coalitions…….. **Doug Maughan**
Coalition policy mechanisms dmaughan@darpa.mil

Fault Tolerant Networks……. **Doug Maughan**
Tolerant mechanisms dmaughan@darpa.mil

IA Science & Engineering Tools……. **Michael Skroch**
Design tools & models mskroch@darpa.mil

Information Assurance…… **Michael Skroch**
Composable trust mskroch@darpa.mil

Intrusion Tolerant Systems…….. **Jay Lala**
Tolerant systems jlala@darpa.mil

Strategic Intrusion Assessment…….. **Catherine McCollum**
Attack recognition & correlation cmccollum@darpa.mil

Cyber Sensor Grid……. Catherine McCollum

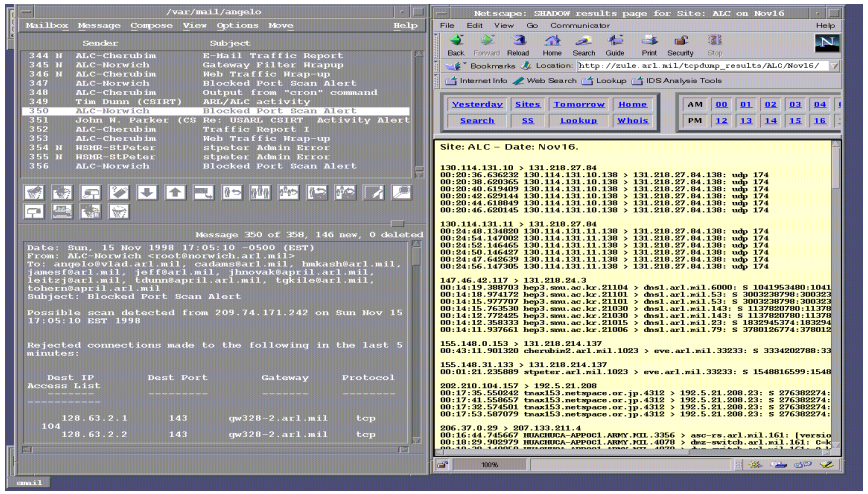
Malicious Code Mitigation…….. Michael Skroch

Reliable Mobile Agents…….. Brian Witten

Secure Operating Systems…….. Doug Maughan

Security of High Speed Networks…… Doug Maughan

New Focus: Cyber Sensor Grid



Sniffer data

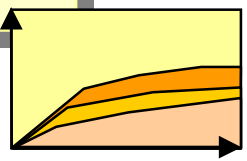
```
% ls -l

header,79,2,fork(2),,Sun Oct 03 21:57:43 1999, + 510000000 msec
argument,0,0x1b7,child PID
subject,aheberle,aheberle,staff,aheberle,staff,408,407,24 6 han
return,success,0

header,107,2,execve(2),,Sun Oct 03 21:57:43 1999, + 510000000 msec
path,/usr/bin/ls
attribute,100555,bin,bin,26738688,427674,0
subject,aheberle,aheberle,staff,aheberle,staff,439,407,24 6 han
return,success,0
   •
   •
   •
header,121,2,lstat(2),,Sun Oct 03 21:57:43 1999, + 510000000 msec
path,/export/home/aheberle/foo
attribute,100000,aheberle,staff,26738688,139738,0
subject,aheberle,aheberle,staff,aheberle,staff,439,407,24 6 han
return,success,0
```

Process ID 0x1b7 = 439

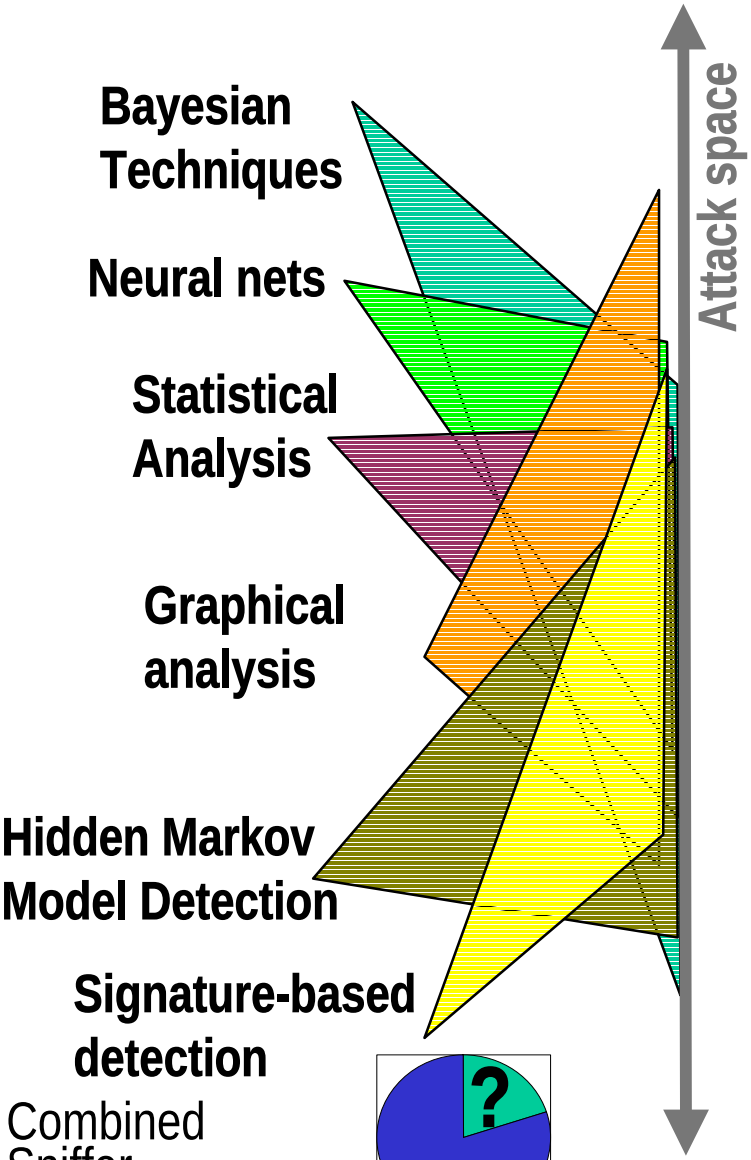
Execute `ls`

Stat `foo`

Audit data



Combined Sniffer Audit



New Focus: Malicious Code Mitigation

Complicating factors:
- More COTS
- Increasing use and reliance on systems
- Increasing connectivity

Strategy:
- Detect & Expunge "On the Fly"
- New Architectural Concepts
- Address Policy Language Lag

New Focus: Reliable Mobile Agents

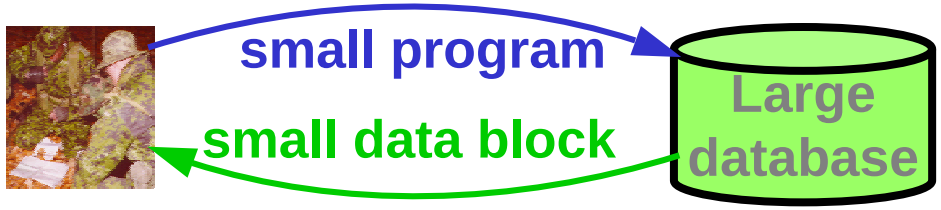
Mobile Agents are:

Programs that can migrate from machine to machine under their own control.

Code mobility…

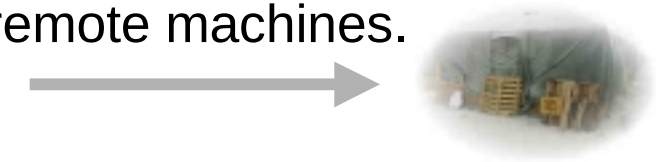
Functionally enhances:

1. **Efficiency**



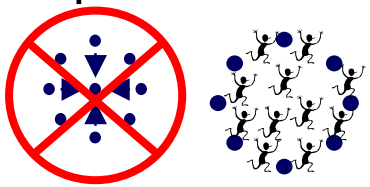
2. **Disconnected operations**
   (e.g.. wireless networks)

3. **Flexibility**
   Install new functionality on remote machines.



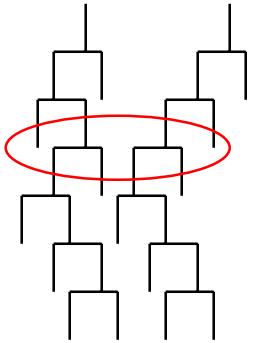
Presents Survivability Opportunities:

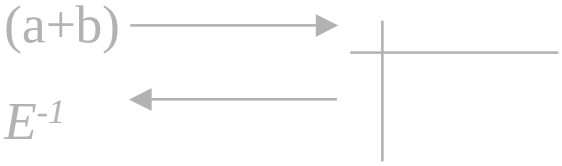
1. **Availability**
   No central failure point.



2. **Integrity**
   Fluidly reinforce execution traces.

3. **Confidentiality**
   Code fragmentation.
   Mobile cryptography.





DARPATECH 2000

ISO

Conclusions:

- **National Level Problem**
- **DARPA "high-risk"/ "high-reward" focus**

New Focus Areas:

- **Cyber Sensor Grid**
- **Malicious Code Mitigation**
- **Reliable Mobile Agents**

Proven Success:

- **ARPANET**
- **Firewall Toolkit**

Waiting Gold:

- **Secure Domain Name Service**
- **Internet Protocol Security (IPSEC)**
- **Secure Border Gateway Protocol**
- **Next Generation Intrusion Detection**

More to Come:

- **Denying Denial-of-Service**
- **Self-Healing Systems**
- **Proof Carrying Code**
- **Trace Back**
- **Dynamic Defense**
- **Metrics & Science Based Design**

IA&S Information – www.darpa.mil