

Information Assurance & Survivability



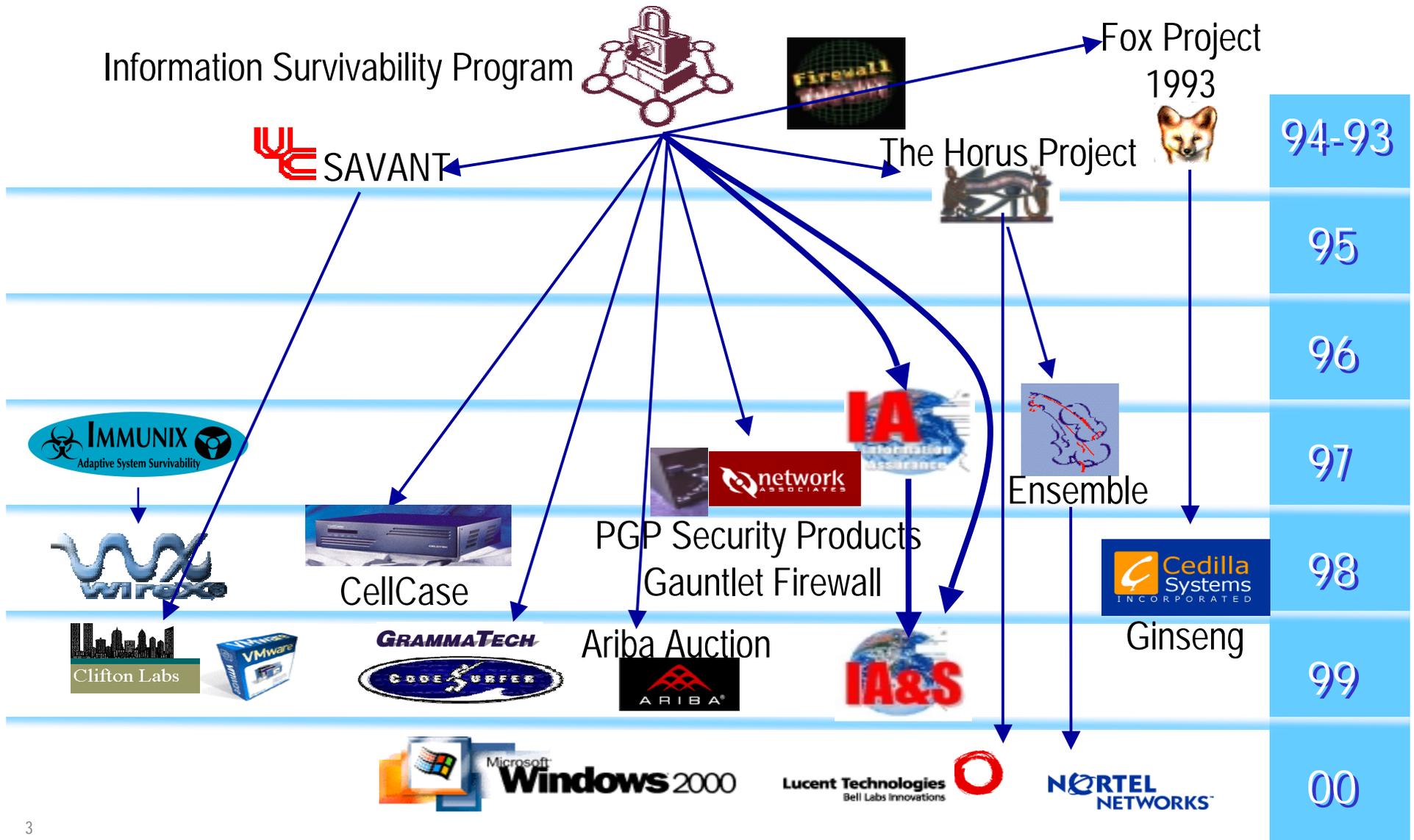
Brian Witten
Information Systems Office

Can we trust the data we are fighting on?



History of Innovations

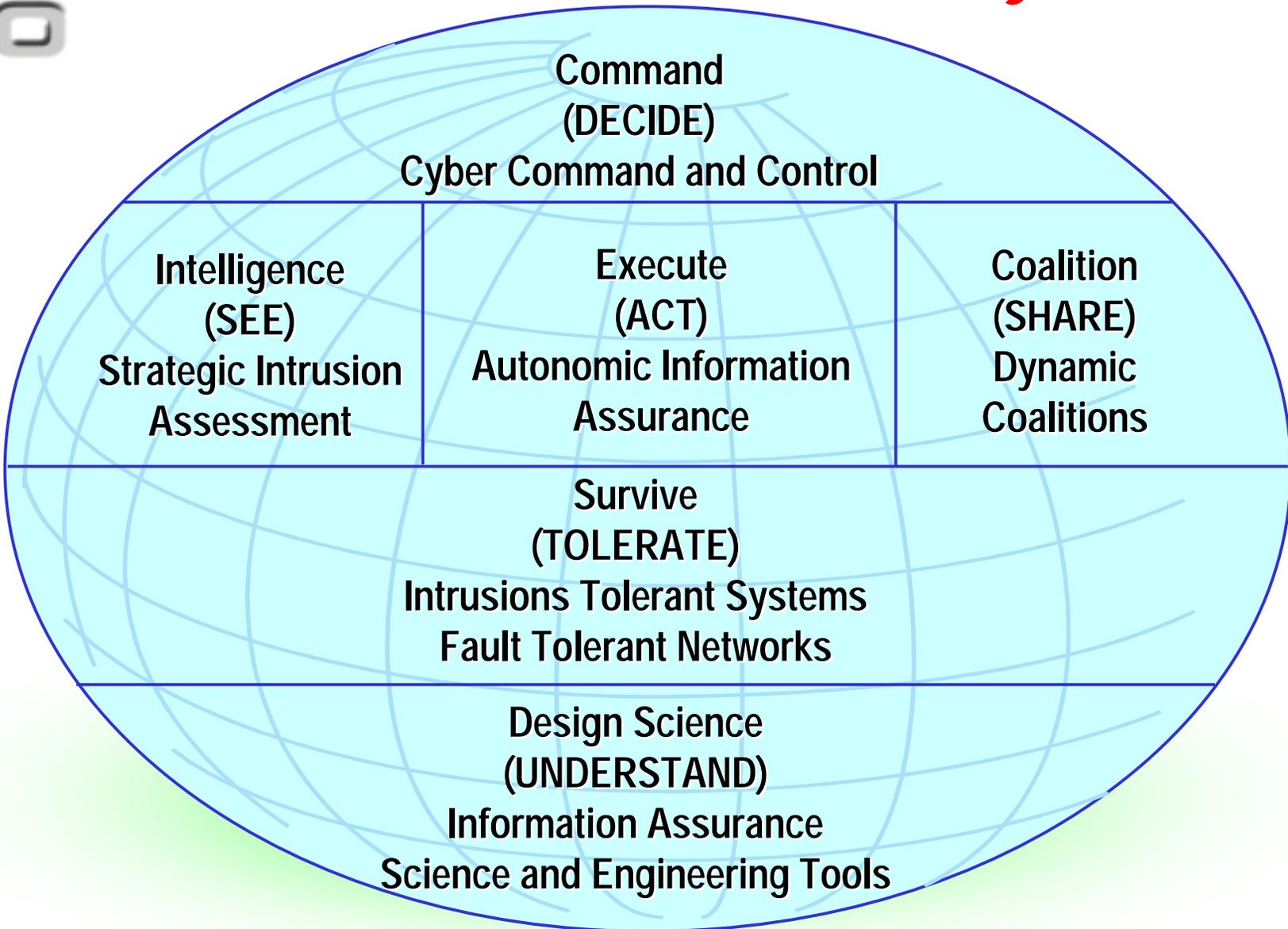
IS Conference Proceedings - <http://schafercorp-ballston.com/discex>



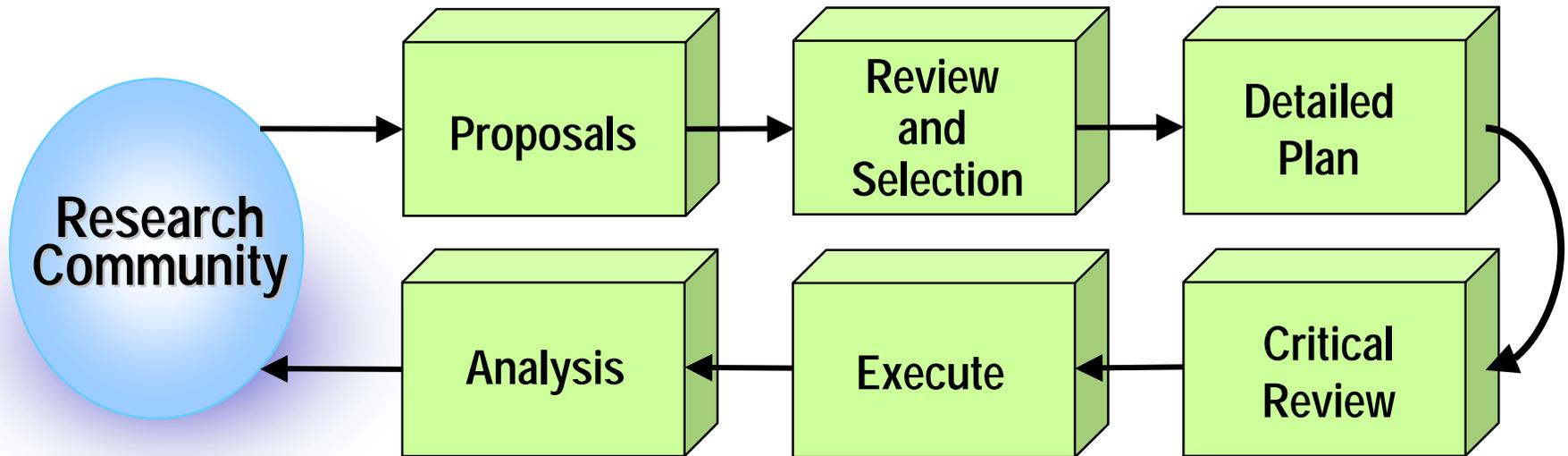
Long Road Ahead



Objectives



Approach: Scientific Experimentation



Grand Hypotheses:

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

Types of Experiments:

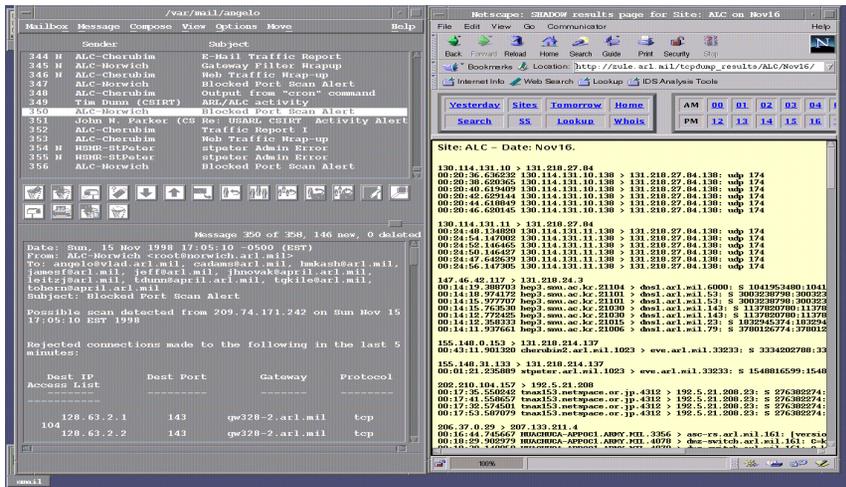
- Field Experiments
- Red Team Lab Exercise
- Laboratory Experiments
- Interdisciplinary White-Boarding
- Component Specific Testing



Contact

Autonomic Information Assurance..... Dynamic response	Brian Witten bwitten@darpa.mil
Cyber Command & Control..... Human directed strategy	Catherine McCollum cmccollum@darpa.mil
Dynamic Coalitions..... Coalition policy mechanisms	Doug Maughan dmaughan@darpa.mil
Fault Tolerant Networks..... Tolerant mechanisms	Doug Maughan dmaughan@darpa.mil
IA Science & Engineering Tools..... Design tools & models	Michael Skroch mskroch@darpa.mil
Information Assurance..... Composable trust	Michael Skroch mskroch@darpa.mil
Intrusion Tolerant Systems..... Tolerant systems	Jay Lala jlala@darpa.mil
Strategic Intrusion Assessment..... Attack recognition & correlation	Catherine McCollum 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,(0x1b7),child PID
Process ID
0x1b7 = 439
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
Execute ls
subject,aheberle,aheberle,staff,aheberle,staff,439,407,24 6 han
return,success,0
.
.
header,121,2,lsstat(2),Sun Oct 03 21:57:43 1999, + 510000000 msec
path,/export/home/aheberle/foo
attribute,100000,aheberle,staff,26738688,139738,0
Stat foo
subject,aheberle,aheberle,staff,aheberle,staff,439,407,24 6 han
return,success,0
    
```

Audit data



Combined Sniffer Audit

Bayesian Techniques

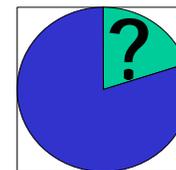
Neural nets

Statistical Analysis

Graphical analysis

Hidden Markov Model Detection

Signature-based detection



Attack space

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

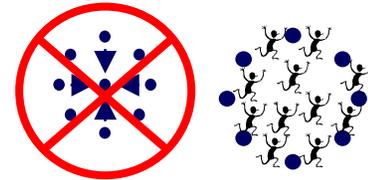
Install new functionality on remote machines.



Presents Survivability Opportunities:

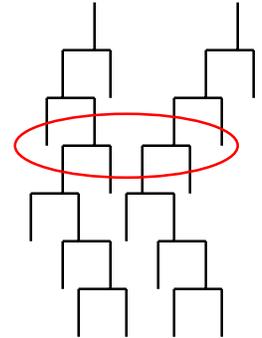
1. Availability

No central failure point.



2. Integrity

Fluidly reinforce execution traces.



3. Confidentiality

Code fragmentation.
Mobile cryptography.



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