Dependability: Information Assurance Research Agenda

Jaynarayan H. Lala

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

January 6, 2002

After September 11, 2001

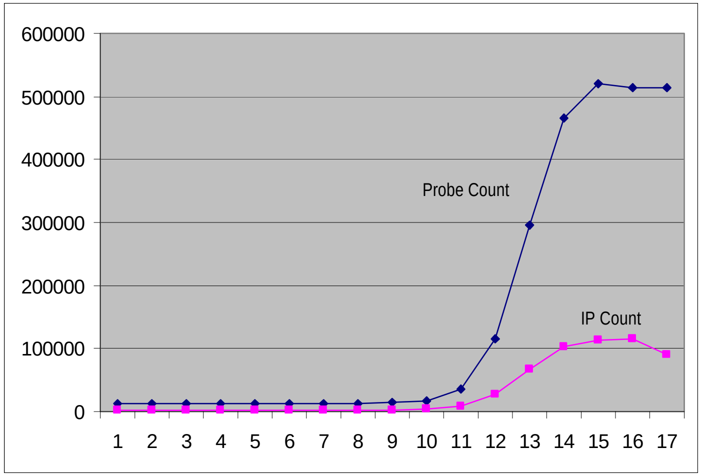
What was only imaginable is now a reality.

What was inconceivable can now be imagined.

Cyber Attacks

Reality

- **Code Red Worm***
  - –Code Red I - July 17, 2001
  - –Code Red II - August 4, 2001
  - –Propagates through networks without user intervention. Exploits vulnerability in Microsoft's IIS Web Server software (specifically, buffer overflow)
  - –Performed a DOS attack against www.whitehouse.gov.
  - –Relatively benign payload. Defaces web sites.
  - –Infected 250,000 systems in 9 hours; 975,000 total



*GAO Report GAO-01-1073T of 29 August 2001

Imaginable

- **Andy Warhol Worm**
  - –Spreads throughout internet in 15 minutes
  - –Malicious payload, such as the Nimda virus
    - –Provides remote attackers "Administrator" privileges and access to entire file system

Or

- **Flash Worm**
  - –Spreads throughout internet almost instantaneously
  - –Malicious Payload

SecDef Guidance

“The surprises we will encounter a decade from now will very likely be different from the one that struck us on Sept. 11. To deal with those future surprises, we must move rapidly now to improve our ability to protect U.S. information systems…..”

- *Donald H. Rumsfeld*

Washington Post Op-Ed Column,Thursday, November 1, 2001

Cyber Czar Guidance

These days Clarke spends his time worrying about America's computer systems, about what he calls a "digital Pearl Harbor."

"There are a countless number of bad scenarios," Richard Clarke said in an interview.

“New Cyberspace Czar Pushes for Tighter Online Security”

By Ariana Eunjung Cha,

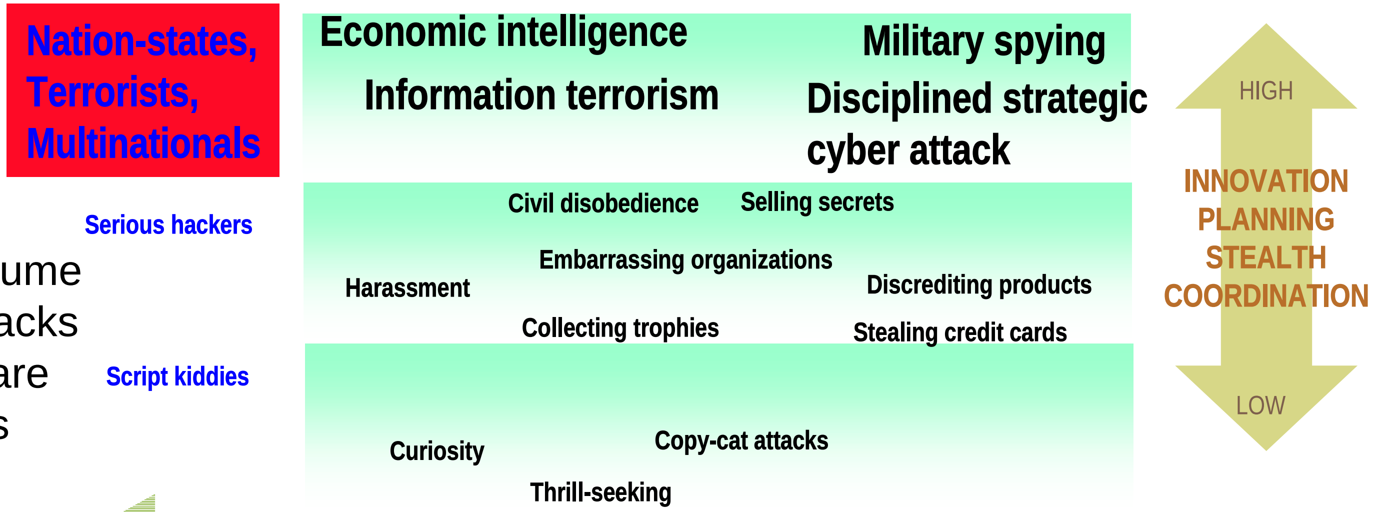
Washington Post Staff Writer

Sunday, November 4, 2001

Defending Against Most Serious Attacks

The Daily Peacetime Problem

- Overwhelming volume of harassment attacks
- Can’t tell if some are serious IW attacks



Nation-states, Terrorists, Multinationals

Serious hackers

Script kiddies

Economic intelligence

Military spying

Information terrorism

Disciplined strategic cyber attack

Civil disobedience

Selling secrets

Embarrassing organizations

Harassment

Discrediting products

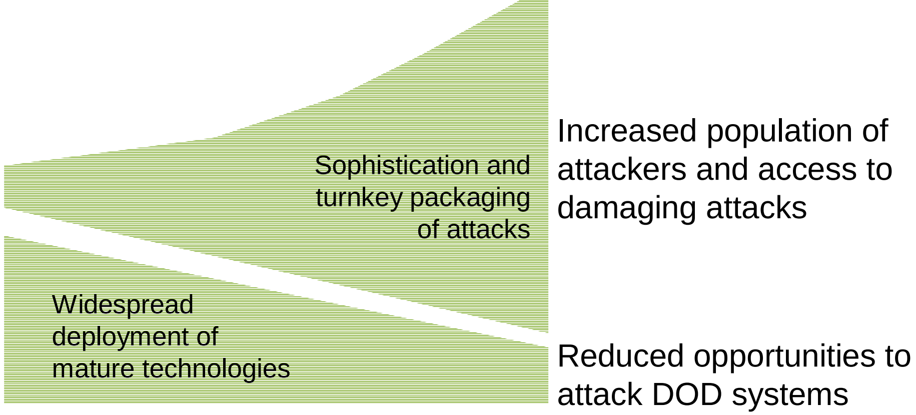
Collecting trophies

Stealing credit cards

Curiosity

Copy-cat attacks

Thrill-seeking



Sophistication and turnkey packaging of attacks

Increased population of attackers and access to damaging attacks

Widespread deployment of mature technologies

Reduced opportunities to attack DOD systems

The Critical IW Attack Problem

- Still face high volume of harassment attacks
- Nation-state-level threats may use harassment attacks as cover, diversion, or disguise
- Determination and attribution of IW attacks is critical

Information Assurance Attributes*

- Integrity
  - Maintain data and program integrity in the face of intrusions and malicious faults.
- Availability
  - Counter Denial-of-Service attacks and maintain high system availability.
- Confidentiality
  - Prevent unauthorized disclosure of information.
- Authentication
  - Prevent unauthorized access.
- Non-repudiation
  - Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender’s identity, so that neither can later deny having processed the data.

* Joint Pub 3-13 “Joint Doctrine for Information Operations”

Goals vs Impairments

		Integrity	Availability	Confidentiality	Authentication	Non-repudiation
Malicious Code	NIMDA					
	ILoveYou					
	nakedwife					
	Moonlight Maze					
	AnnaKournikova					
DOS	Code Red					
	Trinoo					
	Stachaldracht					
	Trinity					
	Morris Worm					
	smurf					
Insider Attack	Misuse					
	Exfiltration					
	Theft					
	Sabotage					
Novel Attacks						
Accidental Faults, Errors, Failures						

DARPA Information Assurance Philosophy

Premise: The number and sophistication of cyber attacks is increasing – some of these attacks will succeed

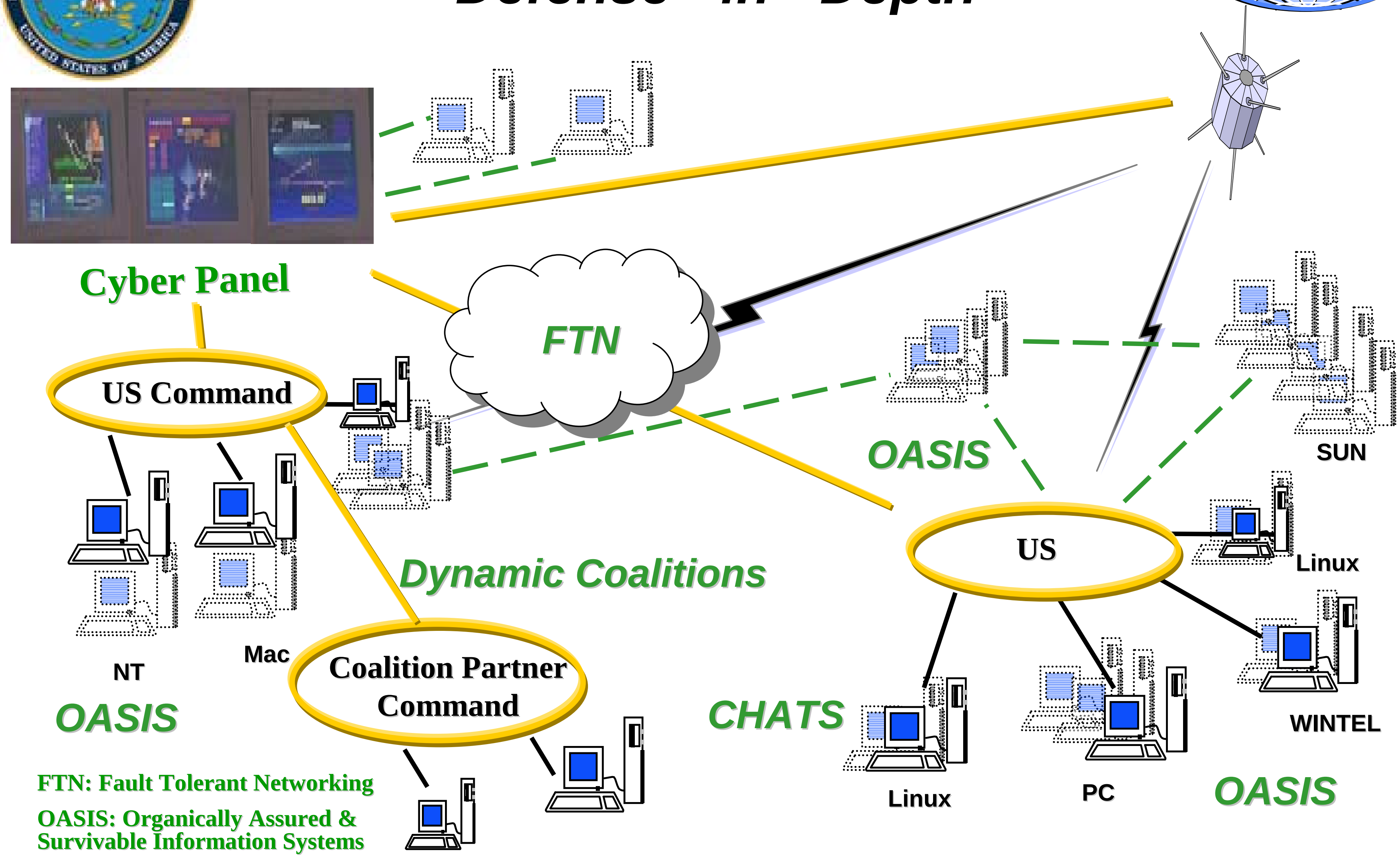
DARPA Philosophy: Operate through attacks by using a layered defense-in-depth concept

- Accept some degradation
- Protect most valuable assets
- Provide commanders a mechanism to visualize attacks

DARPA Approach:

- Continuously test new solutions
- Speed transition of technologies to DoD users

DARPA Information Assurance
Defense - in - Depth



FTN: Fault Tolerant Networking

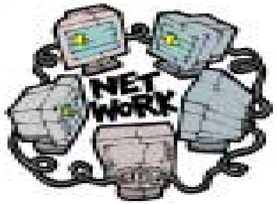
OASIS: Organically Assured & Survivable Information Systems

CHATS: Composable High Assurance Trusted Systems

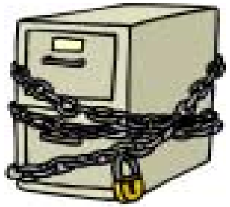
State-of-Practice (1st & 2nd Generation Security Technologies)

- Prevention mechanisms for basic protection (1GS)
- Firewalls, intrusion detection, biometrics and commercial cryptography (2GS)
- NMCI program is scaling up 1GS/2GS to ~10^5 users/seats
- Emerging technologies: wrappers, alert correlation

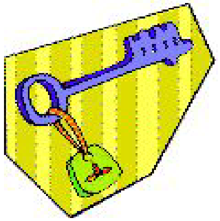
Cryptography



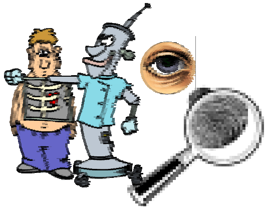
Trusted Computing Base



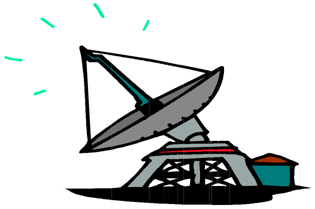
Access Control & Physical Security



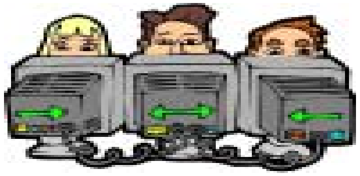
PKI



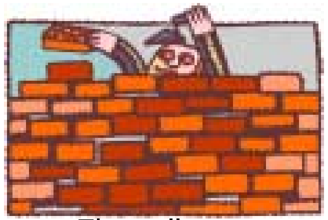
Biometrics



Intrusion Detection Systems



VPNs



Firewalls

State-of-Practice (1)

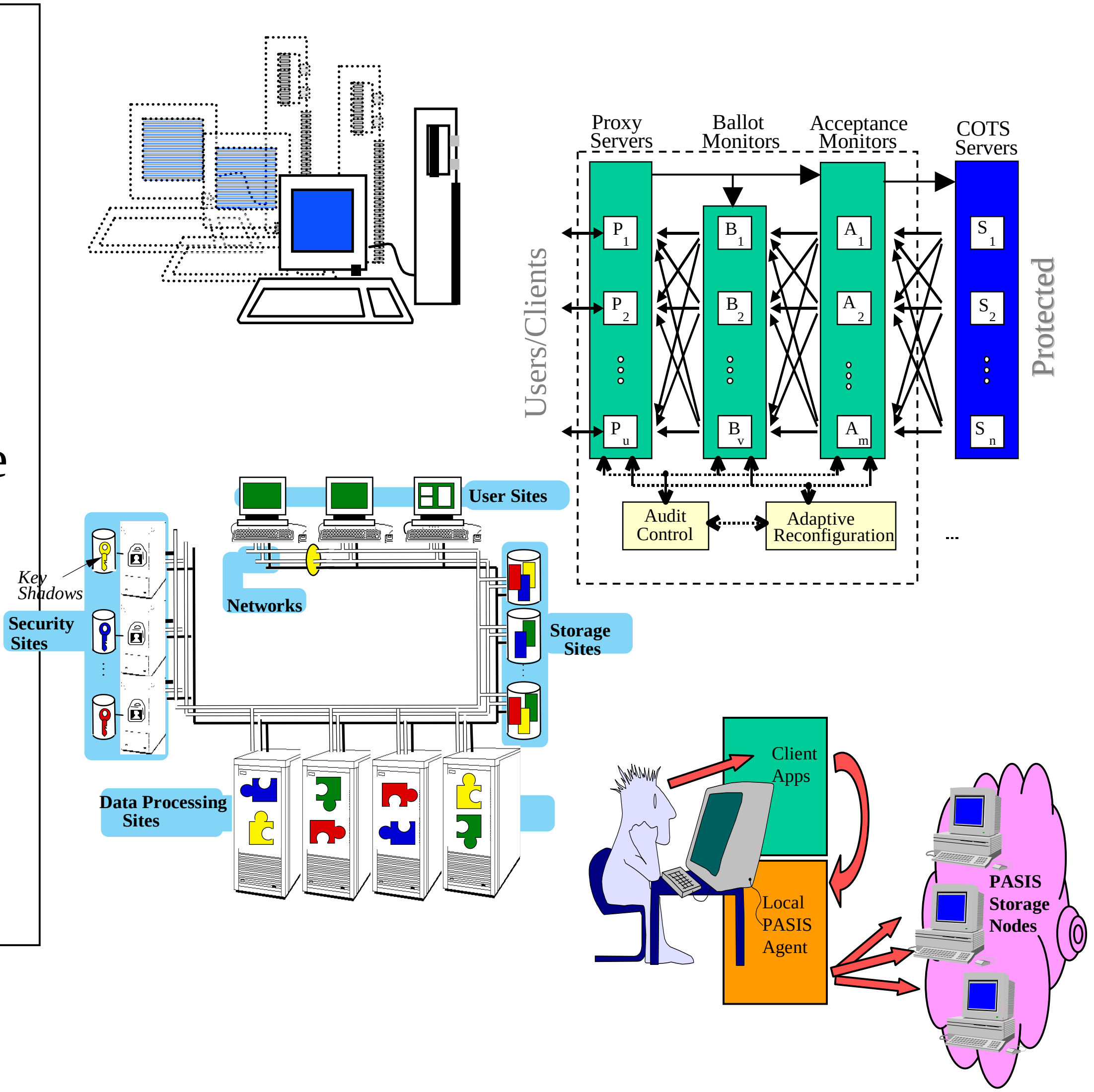
- Systems do not continue operating through most attacks unless isolated, custom-built using trusted computing components, and protected with access control.
- Data can be corrupted, information ex-filtrated, user services interrupted and mission capabilities impaired during an attack .
  - 2GS technologies cannot keep intruders at bay
  - Most attacks are not even detected until after damage is done
- Systems are disconnected from networks and/or shut down to cope with attacks.
- Mission commanders do not know how well systems will cope with a cyber attack.
  - Neither do system designers because the scientific and engineering basis for it is weakly understood and developed

State-of-Practice (2)

- Following an attack, tedious and manual data and code reconstruction must take place and vulnerabilities identified and patched.
- Systems are unavailable to mission commander during the manual restoration process.
- Following manual restoration, systems are still vulnerable to unidentified weaknesses, known-but-unpatched vulnerabilities, and misconfigurations.
- System administrators do not have the time and/or expertise to keep up with all the patches.

State-of-the-Art (3GS Technologies)

- Avoid single points of failure
- Design for graceful degradation
- Exploit diversity to increase the attacker's work factor
- Disperse and obscure sensitive data
- Make systems self-monitoring
- Make systems dynamic and unpredictable
- Deceive attackers



State-of-Art (1)

- Fundamental concepts to construct intrusion-tolerant architectures will have been explored by end of OASIS program.
- It should be feasible to design systems that can maintain data integrity, confidentiality, and un-interrupted user services for a limited period during an attack.

State-of-Art (2)

- But to build an exemplar intrusion-tolerant system, additional research & development is still needed.
- Architecture and System Engineering Issues
  - Integration of defense-in-depth layers to achieve intrusion-tolerance (avoidance, prevention, detection/diagnosis, isolation, recovery, reconfiguration, response)
  - How to cover goals/impairment matrix at minimum cost
  - Synergy between individual solutions, both, positive and negative
- Validation Issues
  - Characterization of cyber-survivability, (survival time and functionality) vs. attack space/vulnerability coverage vs. cost
- Operational Issues
  - Concept of operations for deploying intrusion-tolerant systems

Looking Ahead (1)

- **Intrusion Tolerant Architectures (Networked Applications and Embedded Systems)**
  - Integration of defense-in-depth layers to achieve intrusion-tolerance (avoidance, prevention, detection/diagnosis, isolation, recovery, reconfiguration, response)
  - Adapt security posture to changing threat conditions and adjust performance and functionality

Looking Ahead (2)

- **Self-Healing Systems**
  - – Restore system capabilities to full functionality following an event
  - – Autonomously reassess success and failure of all actions before, during and after an event
  - – Autonomously incorporate lessons learned into all system aspects including architecture, operational procedures, and user interfaces

Looking Ahead (3)

- **Theory of Information Assurance**
  - Development of taxonomy of vulnerabilities and attacks
  - Methods to characterize cyber threats
  - Assessment methodologies to characterize cyber-survivability, (assurance attributes, survival time, functionality, etc.) vs. attack space/vulnerability coverage vs. cost
  - Techniques to optimize information assurance attributes (integrity, availability and confidentiality) at minimum cost