Discussion Points from Session II

Carl Landwehr, Rapporteur

Session 2 . Risks and Defenses

Two talks on techniques:

Building Survivable Services Using Redundancy and Adaptation

Richard D. Schlichting, AT&T Research, Florham Park, NJ, USA

Assuring the Safety of Opening Email Attachments

Bob Balzer, Teknowledge, USA

One talk on concepts/terminology:

Dependability Concepts for Malicious Faults

David Powell, LAAS-CNRS

One talk on problems/requirements

Information Infrastructure Interdependencies: Systemic Risk Issues

Marc Wilikens, JRC, Ispra, Italy

Capsule Summaries - 1/2

Building Survivable Services Using Redundancy and Adaptation

- Cactus package supports adaptive use of different encryption protocols via microprotocols
- Could be a basis for experimental evaluation of security / performance trade-offs
- Logic for assessing strength of adaptive system is lacking

Safely Executing (Possibly) Malicious Code (Within COTS Products)

- Wrapper technology for Windows platforms continues to mature
- Have added "contain" mode via virtualization of some resources
- Could soon be of practical use for confining potentially malicious code, as well as e-mail attachments

Capsule Summaries - 2/2

Dependability concepts for malicious faults

- Develop conceptual model unifying NSA glossary of intrusion detection and security terms with dependability concepts
- Seems successful at elucidating concepts, shedding light on relationships

Information Infrastructure Interdependencies

- Infrastructures are increasingly complex
- Interdependencies are increasing
- Privacy a concern

Potential Discussion Points

- How real is the risk?

  Cyber-Attacks by Al Qaeda Feared
  Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say

  By Barton Gellmanm Washington Post Staff Writerm **Thursday, June 27, 2002**; Page A01

- Need for vulnerability models at the different layers of the II
- How to study potential instabilities, esp. across different infrastructures?
- How to construct designs / control system evolution in ways that provide strong assurance of damage confinement?
  - Insurance will cover damage from locally caused outage, not remote
- How to validate infrastructure models/simulations?