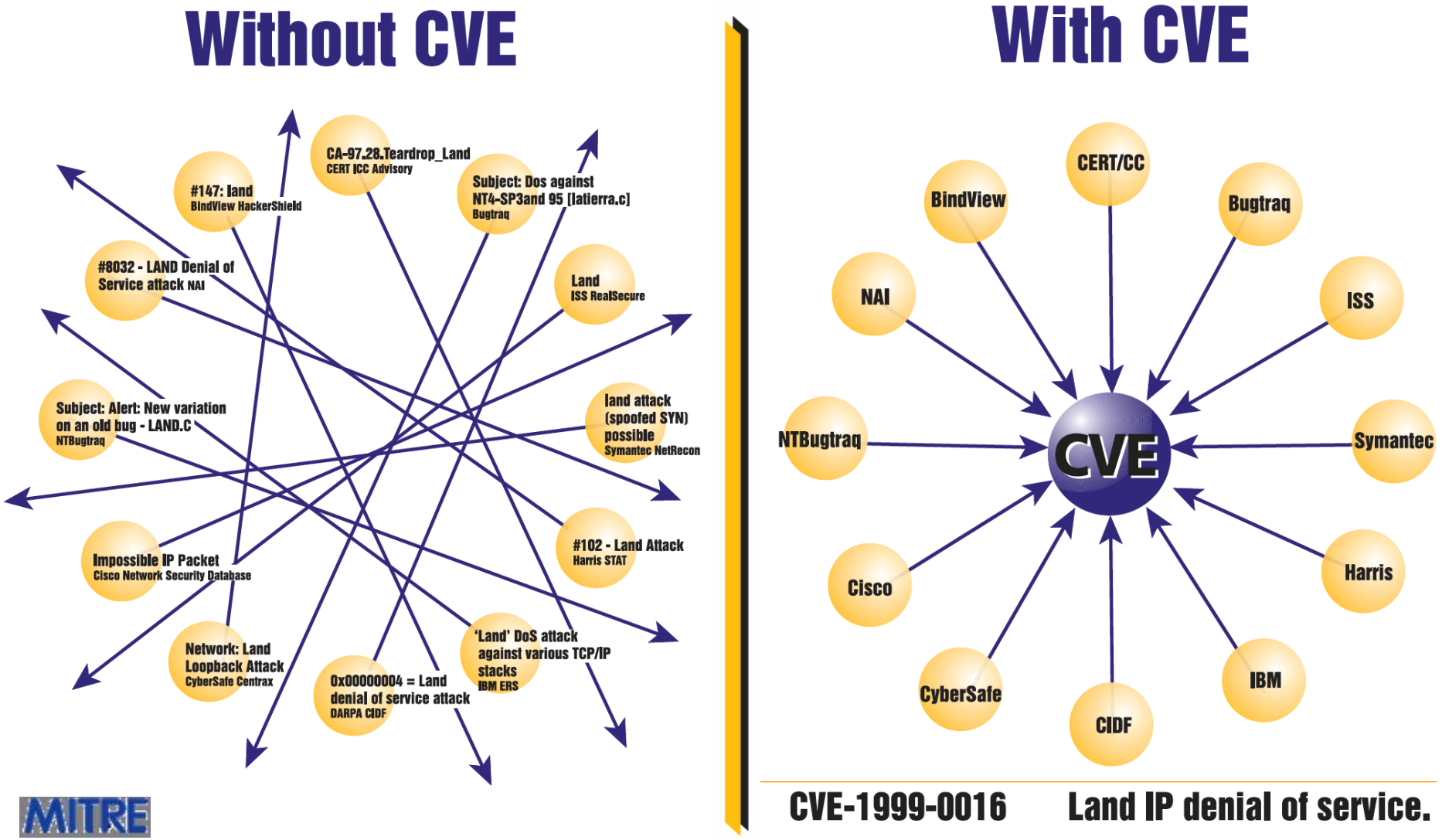
CVE & CCE Overview

David Mann, CVE Project Lead

“Seek simplicity, and distrust it.” - A. N. Whitehead

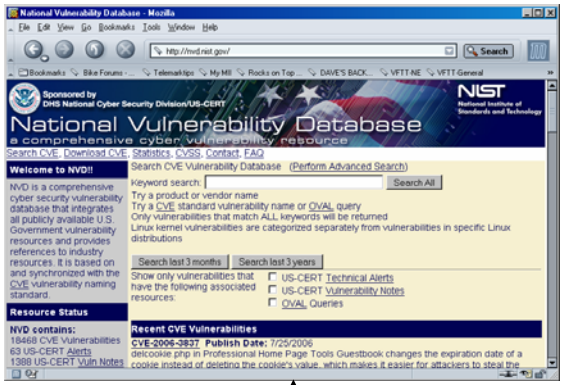
MITRE

The Problem and the CVE Solution: Windows NT Example



MITRE

CVE, NVD & Vulnerability Content



CVE

US-CERT
- Alerts
- Notes

Industry (ThreatGaurd)
- Vuln Checks (OVAL)
- Patch Checks (OVAL)

VENDORS (Red Hat)
- Vuln Comments
- Patch Checks (OVAL)

NIST
- Vuln Attributes
- CVSS Scores

- NVD as clearing house for:
  - All DHS/US-CERT vulnerability content
  - Vendor & Industry generated content
  - Executable OVAL checks
- Common identification enables correlation

Brief History of CVE

- 1999
  - Common Vulnerability Enumeration launched
  - Definition debate on Editorial Board
    - Vulnerability ≈ software flaw
    - Exposure ≈ configuration issue
  - Renamed Common Vulnerabilities & Exposures list
- 2000 – 2003
  - Vulnerability scanners dominate assessment market
  - CVE focuses on software flaws
- 2004
  - Growth in configuration audit market
  - Feasibility studies on enumerating configuration issues
- 2005
  - First CCE drafts produced (Windows and Solaris)
  - Solaris CCE working group meeting (Oct 2005)

2006 – Industry Validation Phase of CCE

- CCE Working Group formed
  - ArcSight, Configuresoft, Center for Internet Security, Citadell, eEye, nCircle, NIST, TriSixty, Microsoft, Sun, Symantec, ThreatGuard
  - MITRE Contact: Dave Mann, damann@mitre.org
- Windows Draft CCE List v2.1 released for public comment
  - Over 500 issues for W2K, XP & Win 2003
  - Cross references for
    - Center for Internet Security Benchmarks (W2K, XP, 2003)
    - DISA Stigs & GoldDisk (W2K, XP, 2003)
    - NSA Security Guide (XP)
    - NIST xp800-68 (XP)
    - Microsoft Security Guide (2003)
  - Download at: http://cce.mitre.org
- CCE Working Group meeting