NVD International

John Banghart

NIST

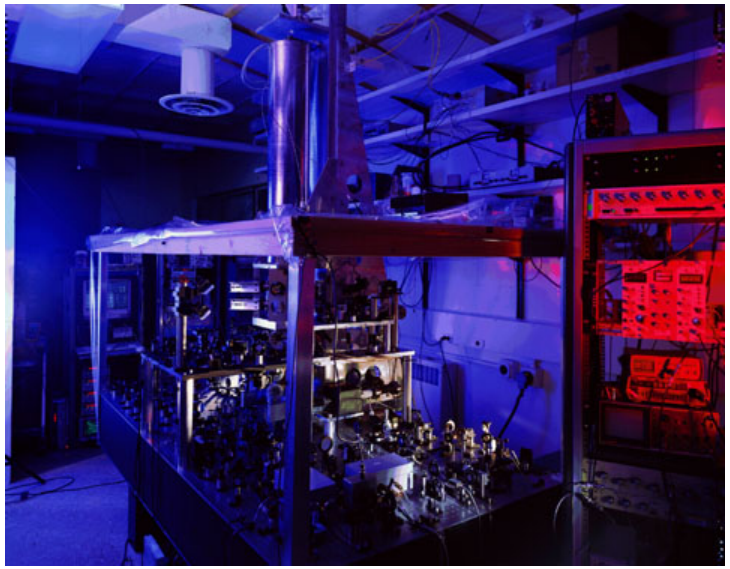
Agenda

- Shared Understanding
  - Acronym Soup
- Yesterday
  - Where have we been? Why did we do it?
- Today
  - How does it work?
- Tomorrow
  - The IVDA Proposal
  - Where do we want to go?

A Common Object

- English = “apple”
- French = “pomme”
- Spanish = “manzana”
- Russian = “яблоко”
- Japanese = “リンゴ”
- German = “apfel”

Telling Time



Standards

- Reference Data
  - Apple = *Malus domestica*
  - Atomic Time
- Communication
  - “I want to eat that apple”
  - “What time is it?”
- Measurement
  - How much does it weigh?
  - How much time has passed?

So What?

Acronym Soup

- **NVD**: National Vulnerability Database
- **NCP**: National Checklist Program
- **USGCB**: US Government Configuration Baseline
- **CVE**: Common Vulnerabilities and Exposures
- **CCE**: Common Configuration Enumeration
- **CPE**: Common Platform Enumeration
- **CVSS**: Common Vulnerability Scoring System
- **CCSS**: Common Configuration Scoring System
- **SCAP**: Security Content Automation Protocol

Yesterday

- Too many vulnerabilities, too many names

Operating System Vulnerability

Today: CVE

- Still too many vulnerabilities, now with less names

Operating System Vulnerability

CVE-2011-1234

Today: NVD

- How does it work?

Today: NVD/NCP

- 48,000+ vulnerabilities published (CVE +CVSS)
  - 16 added per day
- 35,000+ product identifiers (CPE)
  - Mapped to individual CVE's
- 36+ SCAP expressed checklists
  - USGCB
  - DISA STIG's
  - Others

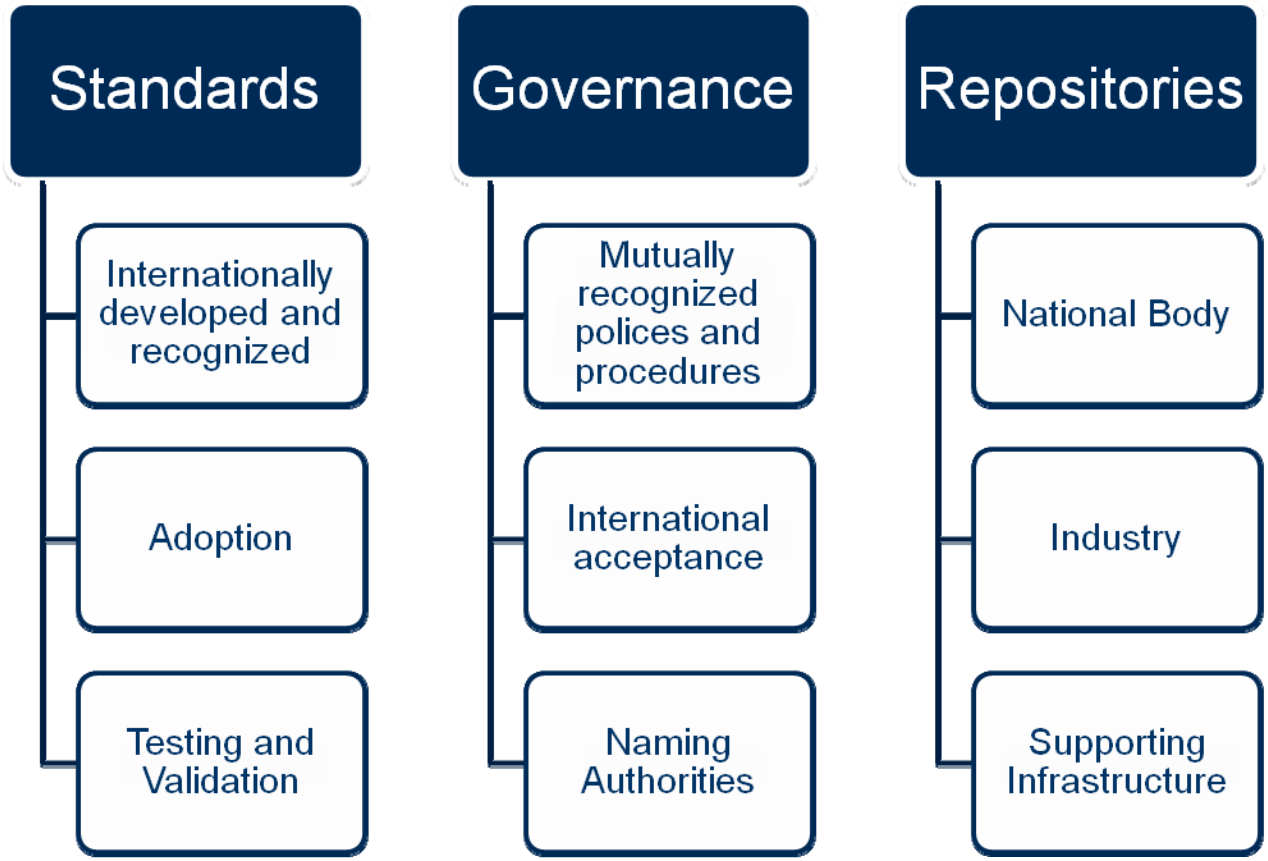
Tomorrow: IVDA

- International Vulnerability Database Alliance
  - Proposal from the *National Computer Network Intrusion Protection Center, GUCAS, Beijing China*
  - June, 2011 at the East-West Cyber Security Conference in London
- Summary
  - CVE and vulnerability databases are English-centric
  - CVE process is not open or well-defined
  - Insufficient ID's available per year
    - Currently 9,999

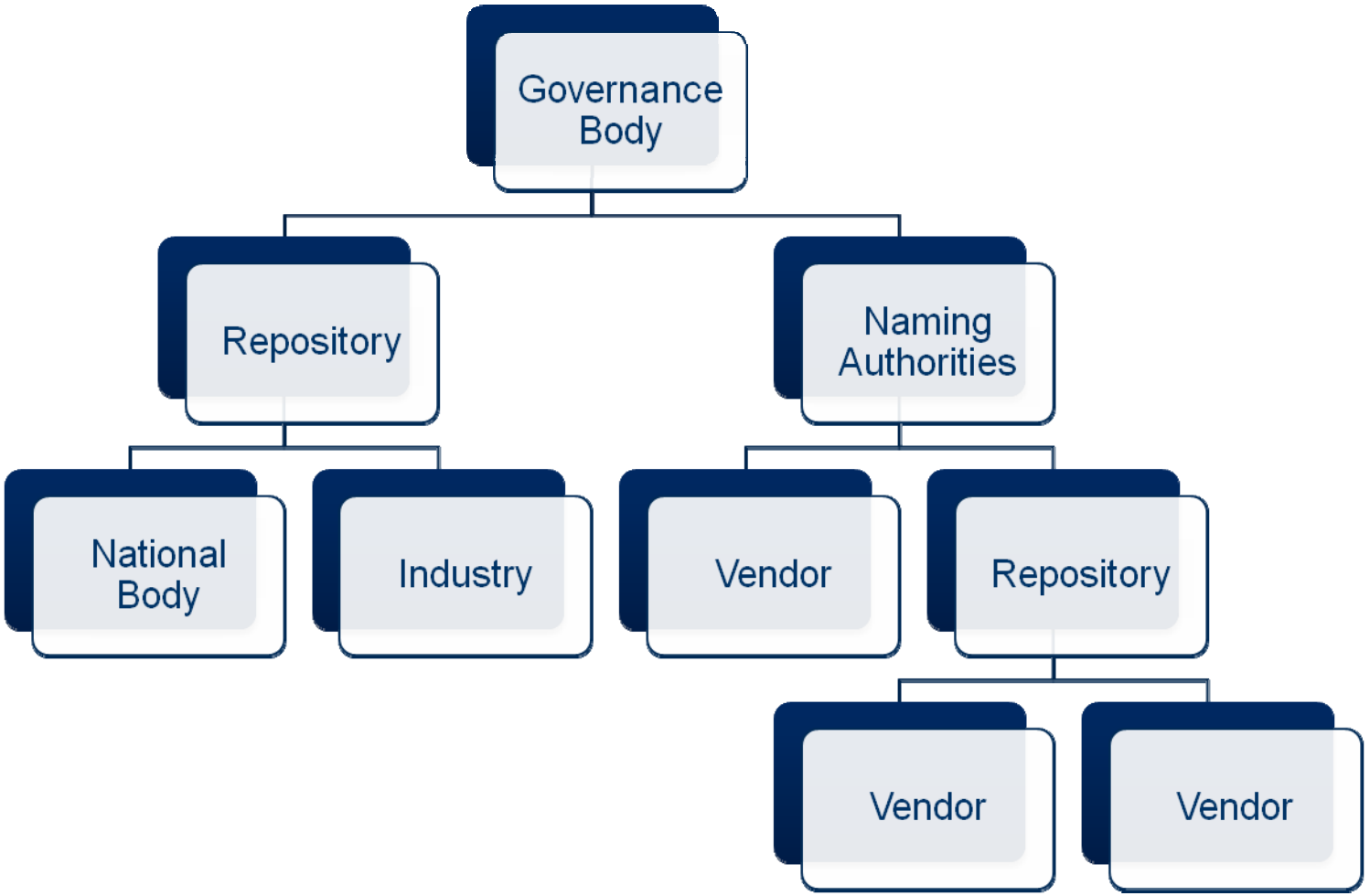
IVDA: Not so fast

- English language dependency
  - Most information is in English, but this is a resource and awareness/submission limitation, not a technical one
- Process is closed
  - Resource and language constraints, not technical ones.
- CVE must allow for more vulnerabilities per year
  - True; resolved by allowing more digits in the CVE identifier

Tomorrow: What do we need?



Tomorrow: Possible Structure



Tomorrow: Next Steps

- Coalition of the willing
  - Government, industry, standards developers
- Evolve CVE
  - More CVE IDs per year; refined process
- Internationalization
  - Standards
  - Governance
  - Localized Repositories
  - Infrastructure
- Other security automation data?

Conclusion

- Window of opportunity is open
  - Need to step through, or others will, resulting in the possibility of multiple standards
- We all face the same challenges
  - Cyber crime crosses borders
- If done right…
  - Improve global internet security
  - Set precedent and create structure for expansion into new information domains and information sharing

Questions / Feedback

John Banghart

National Institute of Standards and Technology (NIST)

john.banghart@nist.gov

(301) 975-8514