Carnegie Mellon
Software Engineering Institute

CERT
Coordination
Center

Top Level Domain Security Checklist

Presented by Martin Lindner

CERT® Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

The CERT Coordination Center is part of the Software Engineering Institute. The Software Engineering Institute is sponsored by the U.S. Department of Defense.
© 2001 by Carnegie Mellon University
some images copyright www.arttoday.com and www.clipartcity.com

Focus of Presentation

- This presentation is focusing on proper configuration and deployment of TLD name servers.
- This presentation does not address physical security, hardening of operating systems or data integrity between registrars and registries.

© 2001 by Carnegie Mellon University

Security Checklist for Top Level Domains

- ✓ Software version
- ✓ Recursion
- ✓ SOA records
- ✓ Consistent NS records
- ✓ Authoritative answers
- ✓ Restricted zone transfers
- ✓ Name servers on multiple networks

© 2001 by Carnegie Mellon University

Software version

- ✓ Does the name server software have known vulnerabilities?
- ✓ Is someone monitoring for new threats and vulnerabilities?
  - CERT/CC Advisories
  - Vendor Advisories
  - Public news groups and mailing lists

© 2001 by Carnegie Mellon University

Recursion

- ✓ **Do the name servers use recursion?**
  - **Recursion leaves name servers vulnerable to cache poisoning.**

© 2001 by Carnegie Mellon University

SOA records

- ✓ Do the name servers have a Start of Authority (SOA) record for the TLD?

© 2001 by Carnegie Mellon University

Consistence NS records

- ✓ Do all the name servers listed in the root answer authoritative for the TLD?
  - Lame Delegations
- ✓ Do the name servers' NS records match the NS records offered by the root?

© 2001 by Carnegie Mellon University

Authoritative answers

- ✓ Do the name servers give authoritative answers?

© 2001 by Carnegie Mellon University

Restricted Zone Transfers

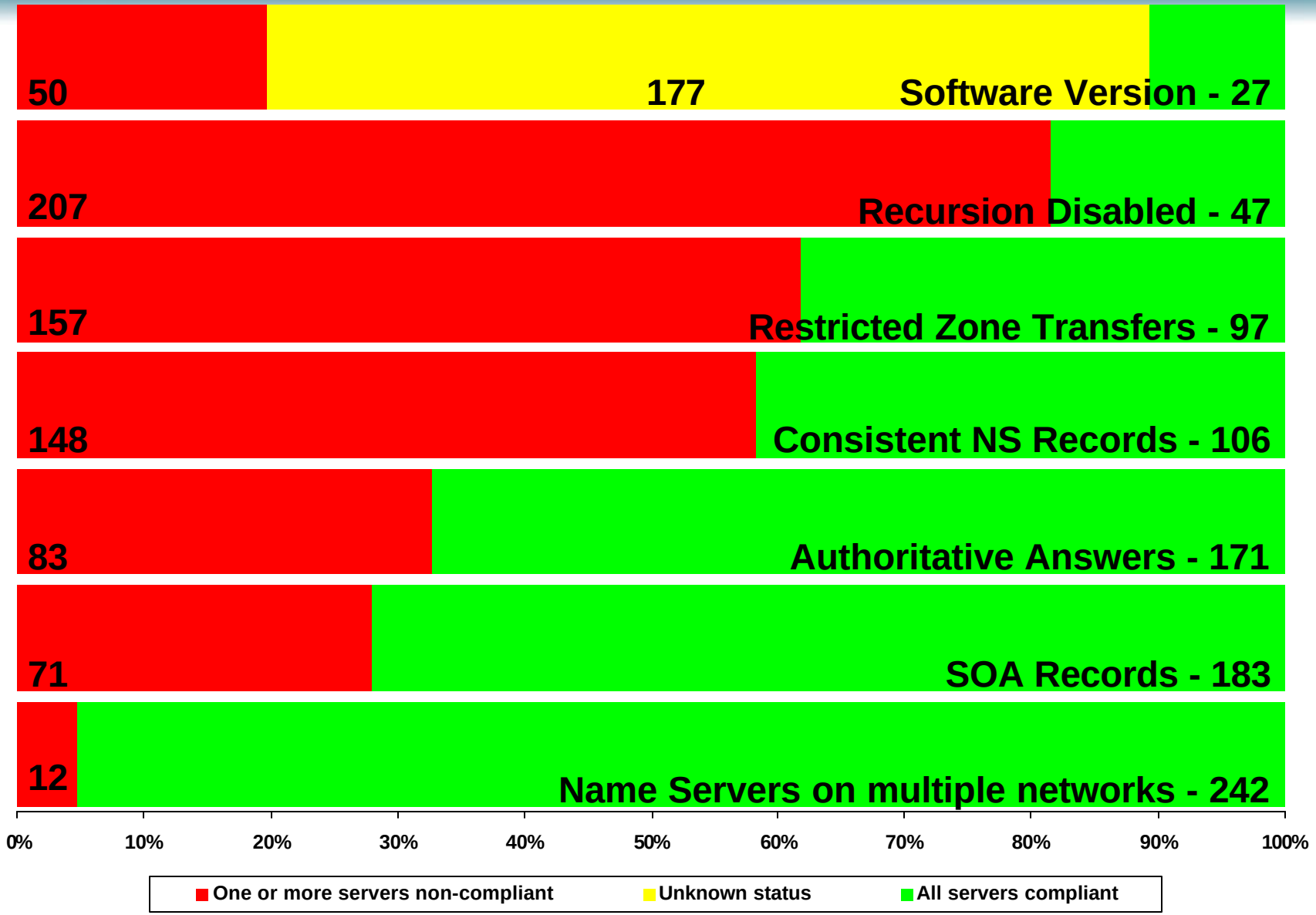
- ✓ **Do the name servers restrict zone transfers to authorized parties?**

© 2001 by Carnegie Mellon University

DNS on multiple networks

- ✓ **Are name servers distributed across multiple networks?**
  - **Different networks**
  - **Multiple upstream providers**

© 2001 by Carnegie Mellon University



© 2001 by Carnegie Mellon University

CERT® Contact Information

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890
USA

Hotline: +1 412 268 7090 CERT personnel answer 8:00 a.m. — 5:00 p.m. EST(GMT-5) / EDT(GMT-4), and are on call for emergencies during other hours.

Fax: +1 412 268 6989

Web: http://www.cert.org/

Email: cert@cert.org

© 2001 by Carnegie Mellon University