Domain Name System (DNS) Attack Demonstration

Russ Mundy

Principal Networking Scientist

SPARTA, Inc.

7110 Samuel Morse Dr.

Columbia, MD. 21046

mundy@sparta.com

http://www.dnssec-deployment.org

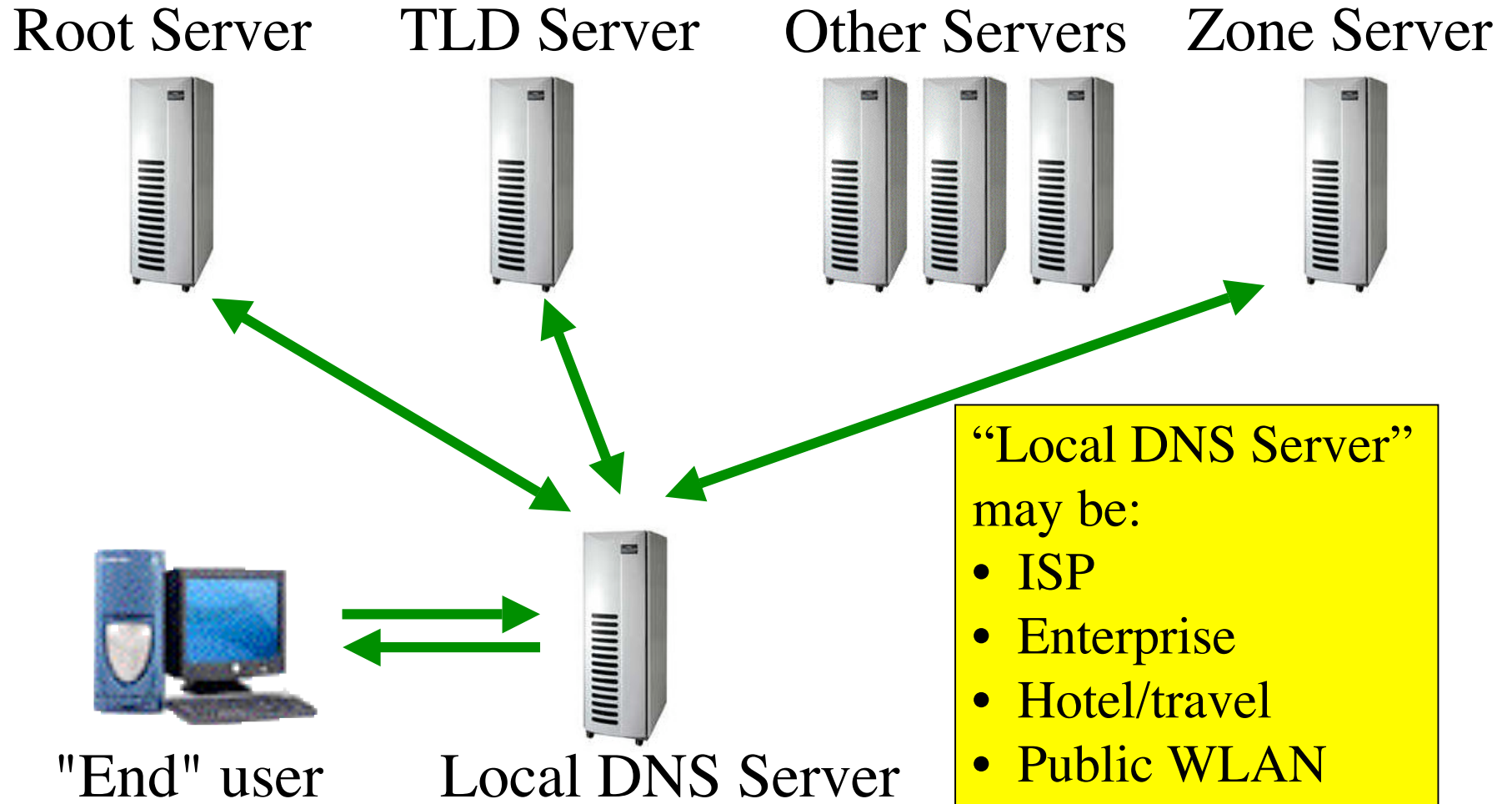http://www.dnssec-tools.org

December 7, 2006

Domain Name System Background

- Essentially all Internet users use the DNS

- Most people trust the DNS

  - They expect to be connected to the site they enter into their application

    - e.g. when entering www.dnssec-deployment.org, they expect to go directly to www. dnssec-deployment.org

  - Unfortunately, this is not always the case

    - DNS attacks provide basis for attacking applications

- Demonstration is only one type of attack based on DNS

Nov 30, 2005

mundy@sparta.com
www.dnssec-deployment.org
www.dnssec-tools.org

2

DNS Name Resolution

Root Server   TLD Server   Other Servers   Zone Server

"End" user   Local DNS Server

"Local DNS Server" may be:
- ISP
- Enterprise
- Hotel/travel
- Public WLAN

Nov 30, 2005

mundy@sparta.com
www.dnssec-deployment.org
www.dnssec-tools.org

3

User DNS Attack Demo

Existing DNS Usage

Easy to observe UDP DNS query sent to well known server on well known port.

www.dnssec-deployment.org A?

www.dnssec-deployment.org

www. dnssec-deployment.org A 63.241.136.206
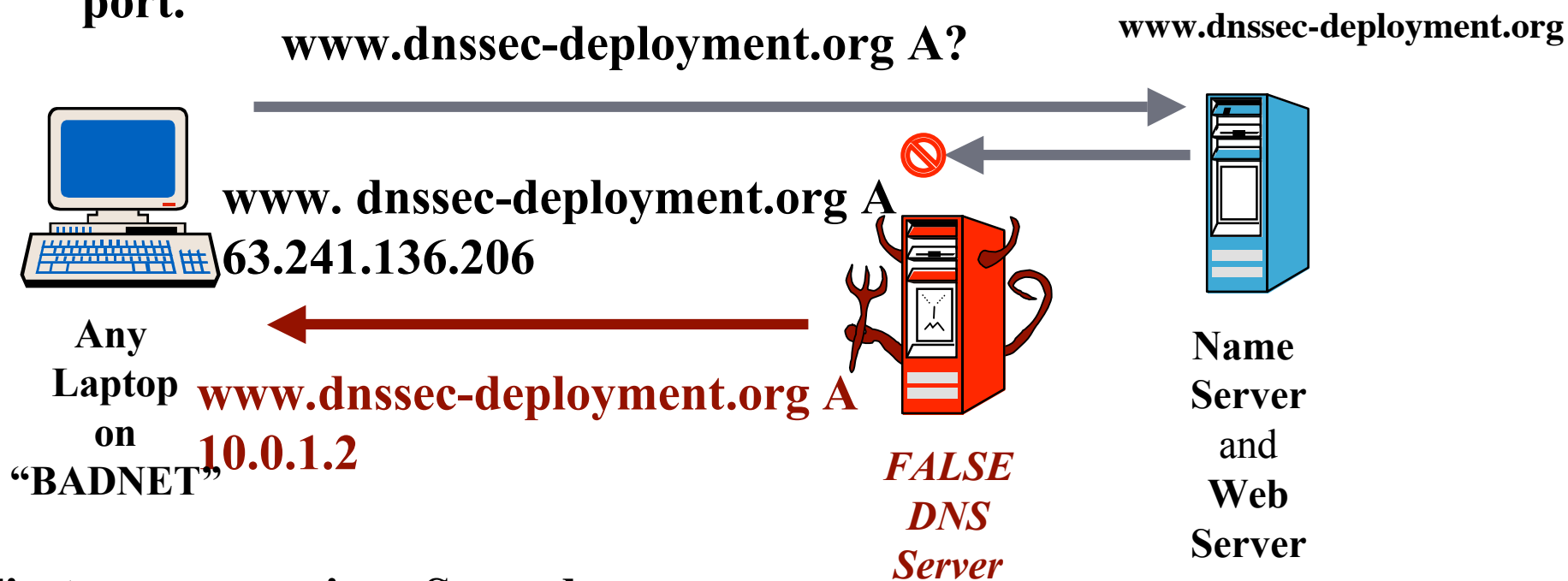
Any Laptop on "BADNET"

Name Server and Web Server
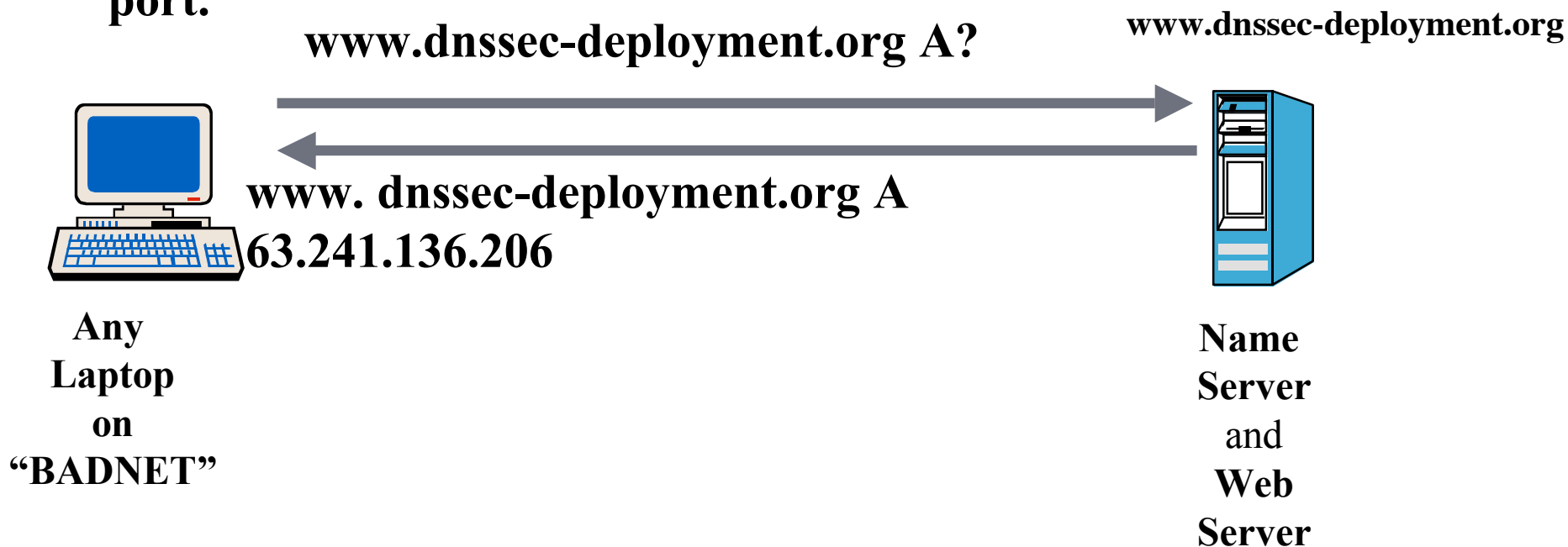
User DNS Attack Demo (cont)

Existing DNS Usage

Easy to observe UDP DNS query sent to well known server on well known port.

www.dnssec-deployment.org A?

www.dnssec-deployment.org

www. dnssec-deployment.org A 63.241.136.206

Any Laptop on "BADNET"

www.dnssec-deployment.org A 10.0.1.2

FALSE DNS Server

Name Server and Web Server

First response wins. Second response is silently dropped on the floor.

mundy@sparta.com
www.dnssec-deployment.org
www.dnssec-tools.org

QUESTIONS????

Questions, comments and other feedback can be sent to
mundy@sparta.com