DANE Secured E-Mail Demonstration

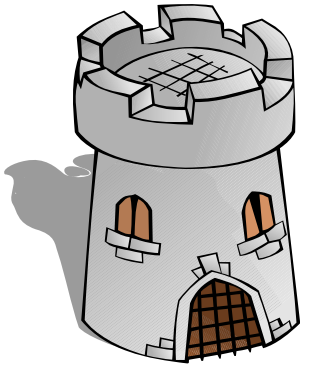
Wes Hardaker
Parsons
<wes.hardaker@parsons.com>

Overview

- My Background
- In scope topics
- Securing E-Mail Requirements
- Implementing Each Requirement

My Background

- Part of the Network Security Research Group
  - A small division within PARSONS
  - Experts on and evangalists for security protocols
- My DNS history
  - Multiple DNS RFCs:
    - 4509, 6168, 7477, **7671, 7672**
  - DNSSEC-Tools development
  - DNS-Sentinel
    - DNS/DNSSEC monitoring service



DNS-Sentinel

DNSSEC-Tools

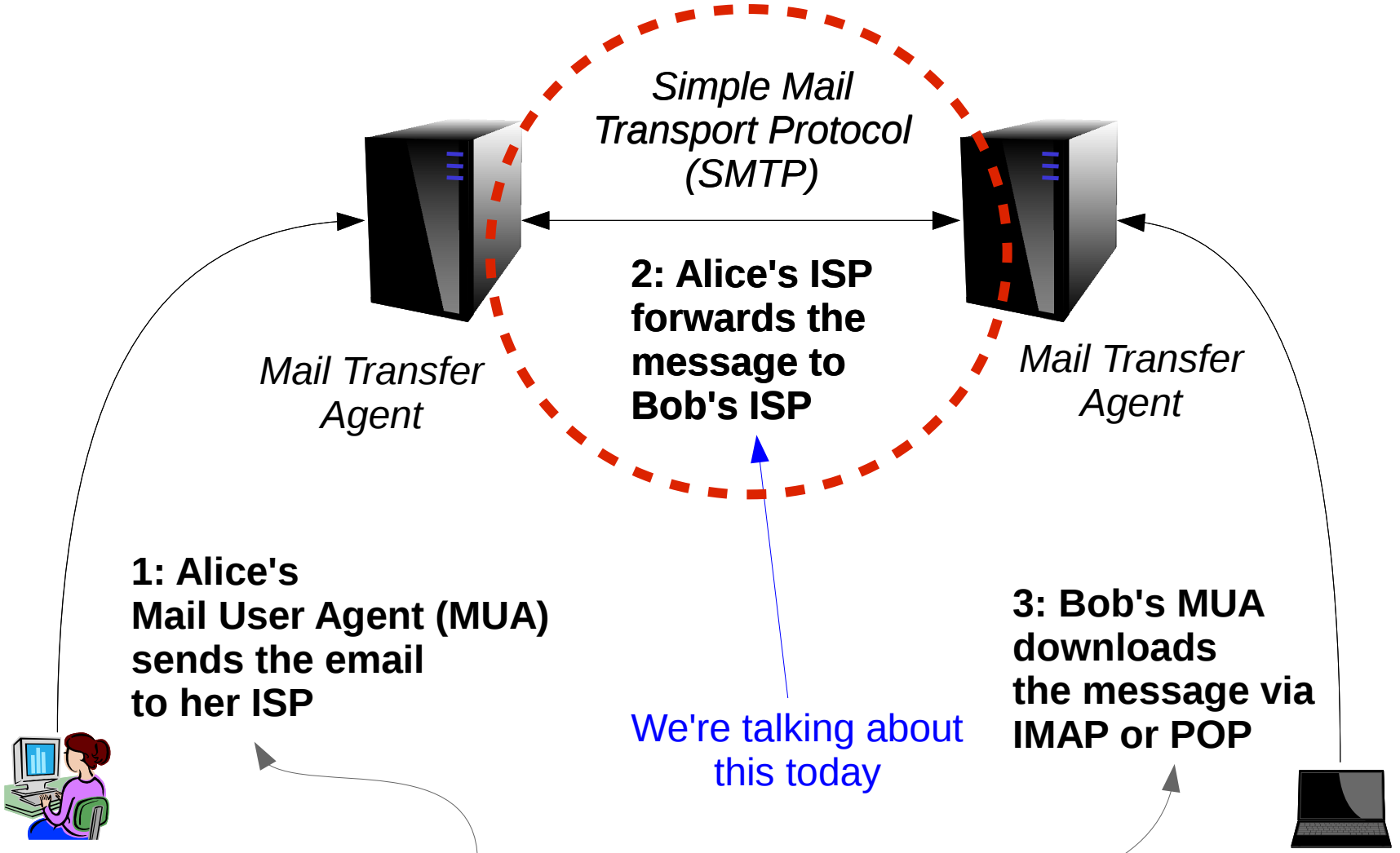
What I am covering

- How to set up secure E-Mail with DANE

What I am not covering

- How DNSSEC and DANE work
  - See my slides from ICANN 53 / Buenos Aires
  - My YouTube “Tutorial on DANE and DNSSEC” video:
    - https://www.youtube.com/watch?v=BhvU19RJrPY
- Securing E-Mail clients to their ISP
  - IE: We're not discussing POP, IMAP, etc.
  - Today: server to server (ISP to ISP)

Server-to-Server Email



Requirements for *Receiving* Secure E-Mail

Receiving Secure E-Mail

- Be found by the distant server DNSSEC
- Accept an authenticated connection DANE
- Accept an encrypted connection DANE

- Your DNS zone must be DNSSEC signed
- Your DNS zone must include a DANE record

Receiving Secure Mail with Postfix
(regardless of DANE usage)

- Create a certificate to use:

```
openssl req -new -newkey rsa:2048 -days 365
-nodes -x509 -keyout server.pem -out
server.pem
```

- Tell postfix to use it:

```
smtpd_tls_key_file  = /etc/postfix/server.pem
smtpd_tls_cert_file = /etc/postfix/server.pem
smtpd_tls_security_level = may
```

DNS Records for our test zone

- In the DNSSEC-Tools.org zone, I created:
  - dane.dnssec-tools.org:
    - `dane IN 60 A 192.0.2.1`
    - `dane IN 60 MX 10 dane.dnssec-tools.org.`
    - `_25._tcp.dane IN 60 TLSA 3 1 1 e8d145d7df0b269d19a5107e489419e0445df7d3c256e0ec24a2a23ff25d249c`
  - And DNSSEC signed it!
    - `dane.dnssec-tools.org. 60 IN RRSIG A`

      `5 3 60 20151113185506 20151014175506`

      `3147 dnssec-tools.org.`

      `UY3+UB7GyO/eaNsf5fFTbTBx9G6R......`

CRITICAL

- When you update your mail server certificate
  - You **must** update your TLSA record to match!
- You **must** continue to resign your zone
- You **should** monitor your services:
  - DNS/DNSSEC health checks
  - DANE records match the mail server certificate
  - Have it yell loudly when broken!!

Test It!

- https://dane.sys4.de/
  - A fantastic SMTP/DANE/DNSSEC testing utility
  - Checks if:
    - Your zone is properly signed
    - Your zone contains TLSA records
    - Your SMTP TLS certificate matches your DANE records
    - For each server!

Requirements for *Sending* Secure E-Mail

Sending Secure E-MAIL Requirements

- DNS Software that verifies DNSSEC records
  - **EVERY** lookup from start to finish must be verified
  - MX records
  - Address records
  - DNSSEC signatures and chain records
- Mail server software that verifies DANE records
  - Collects DNSSEC validated TLSA records
  - Certificates must match these TLSA records

Configuring Postfix

- Needed deployment architecture:
  - DNSSEC Validating Resolver
  - Postifx 2.11 or better
  - **Running on the same host**

- Needed configuration:

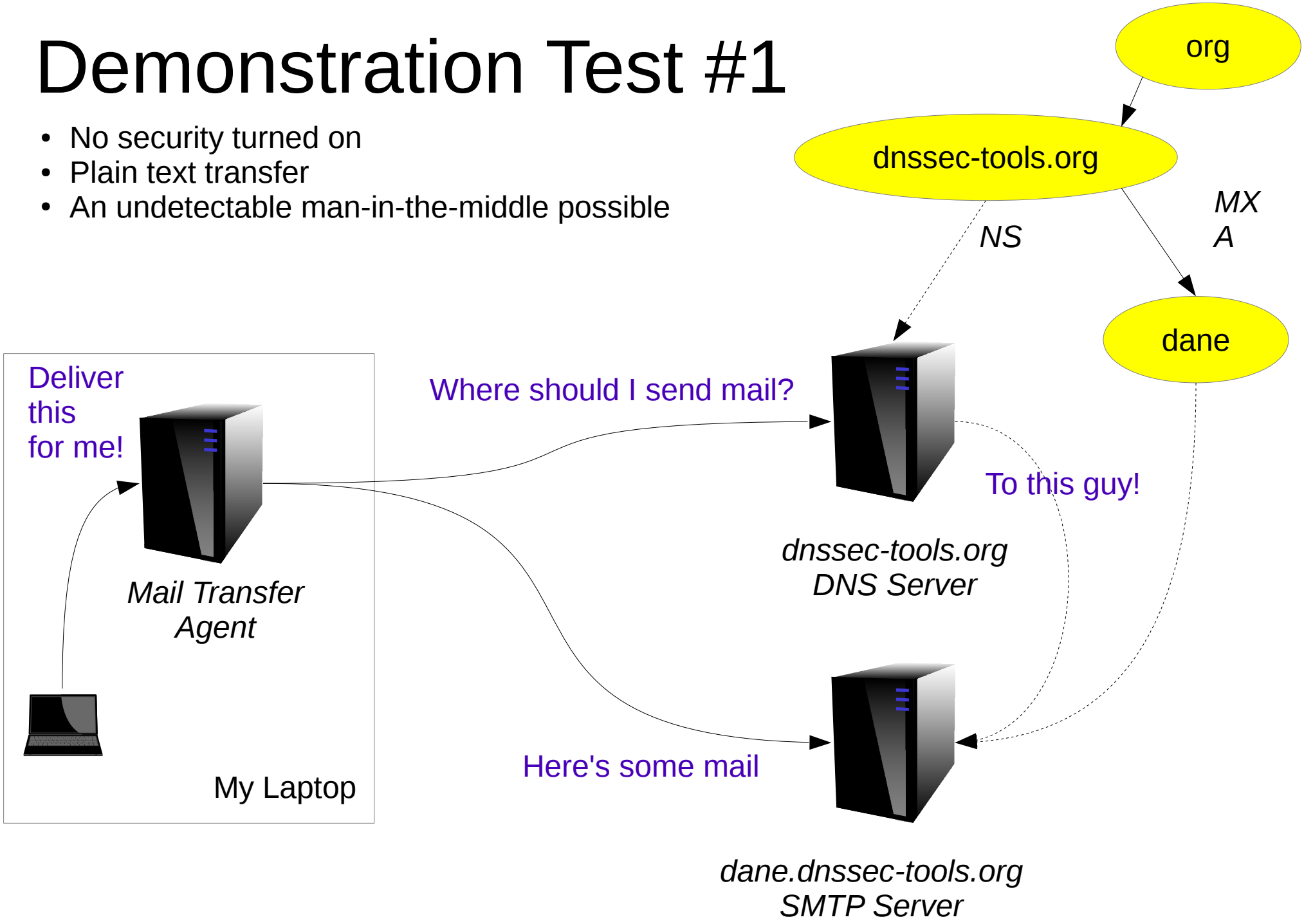
```
smtp_tls_security_level    = dane
smtp_dns_support_level   = dnssec
```

Demonstration

- Sending via an insecure mail server
- Sending to a DANE secured address
- Sending to a DANE failing address
- Sending to a domain with two MX records
  - (with the first being broken)

Demonstration Test #1

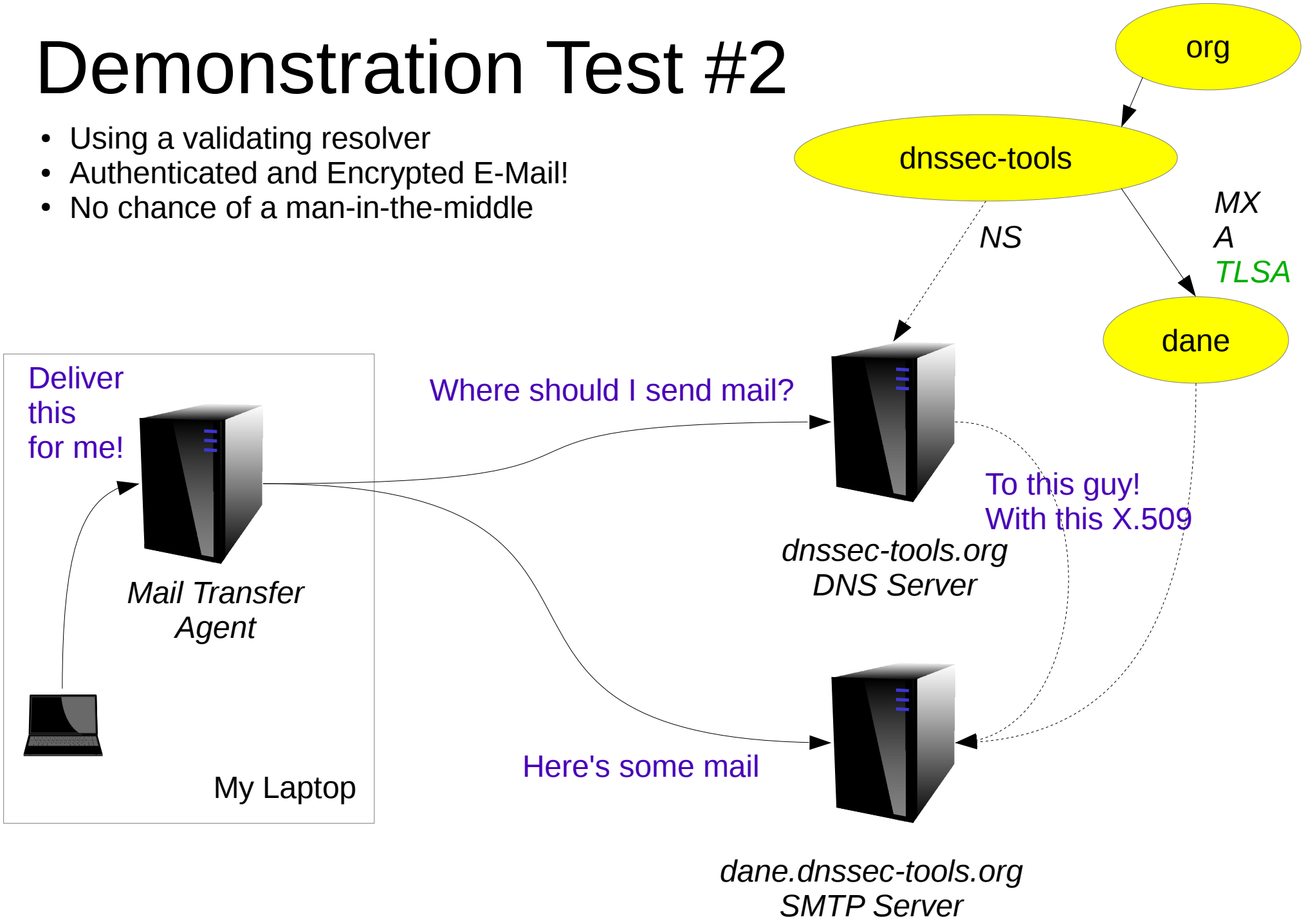
- No security turned on
- Plain text transfer
- An undetectable man-in-the-middle possible



wes.hardaker@parsons.com

Demonstration Test #2

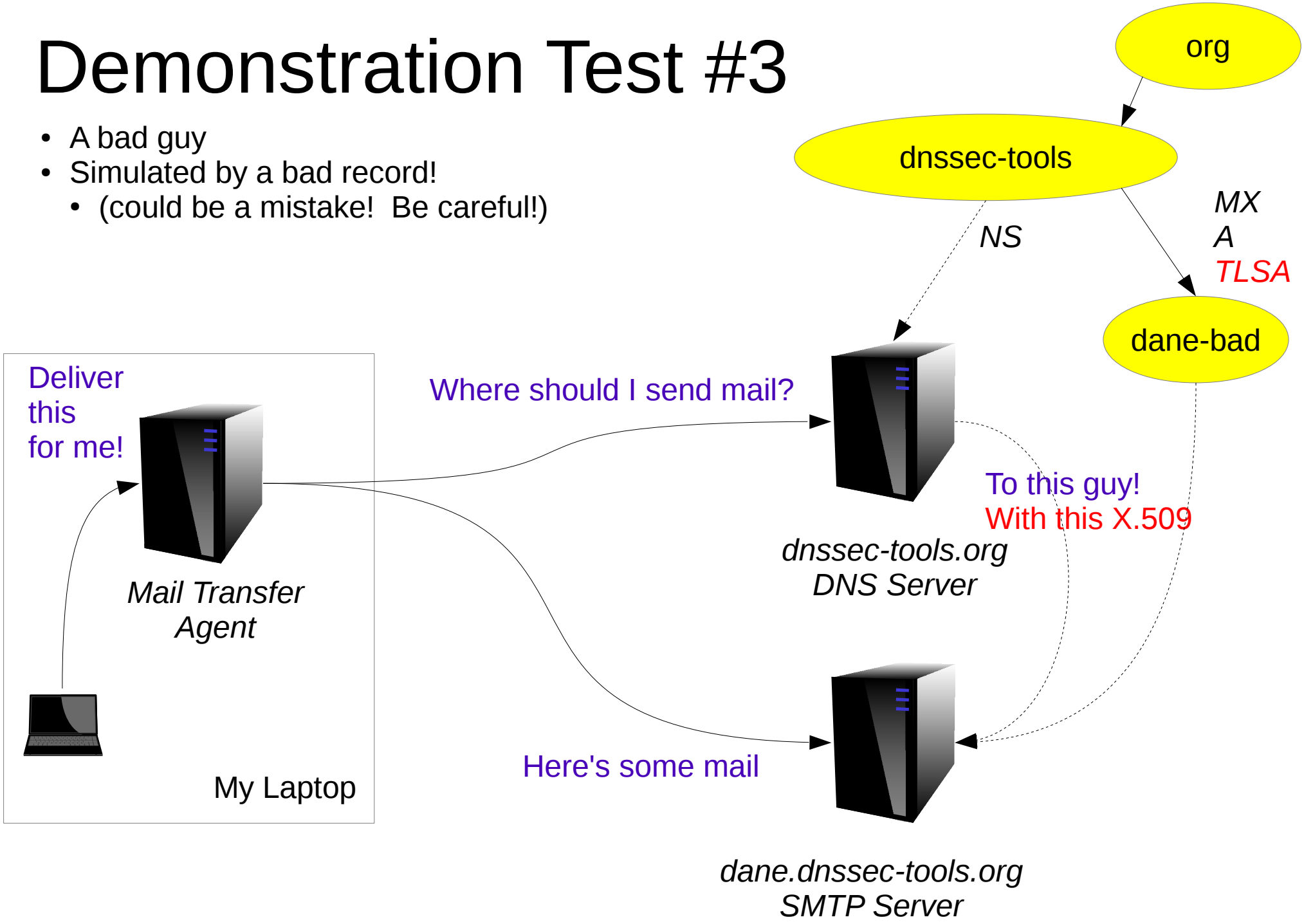
- Using a validating resolver
- Authenticated and Encrypted E-Mail!
- No chance of a man-in-the-middle



wes.hardaker@parsons.com

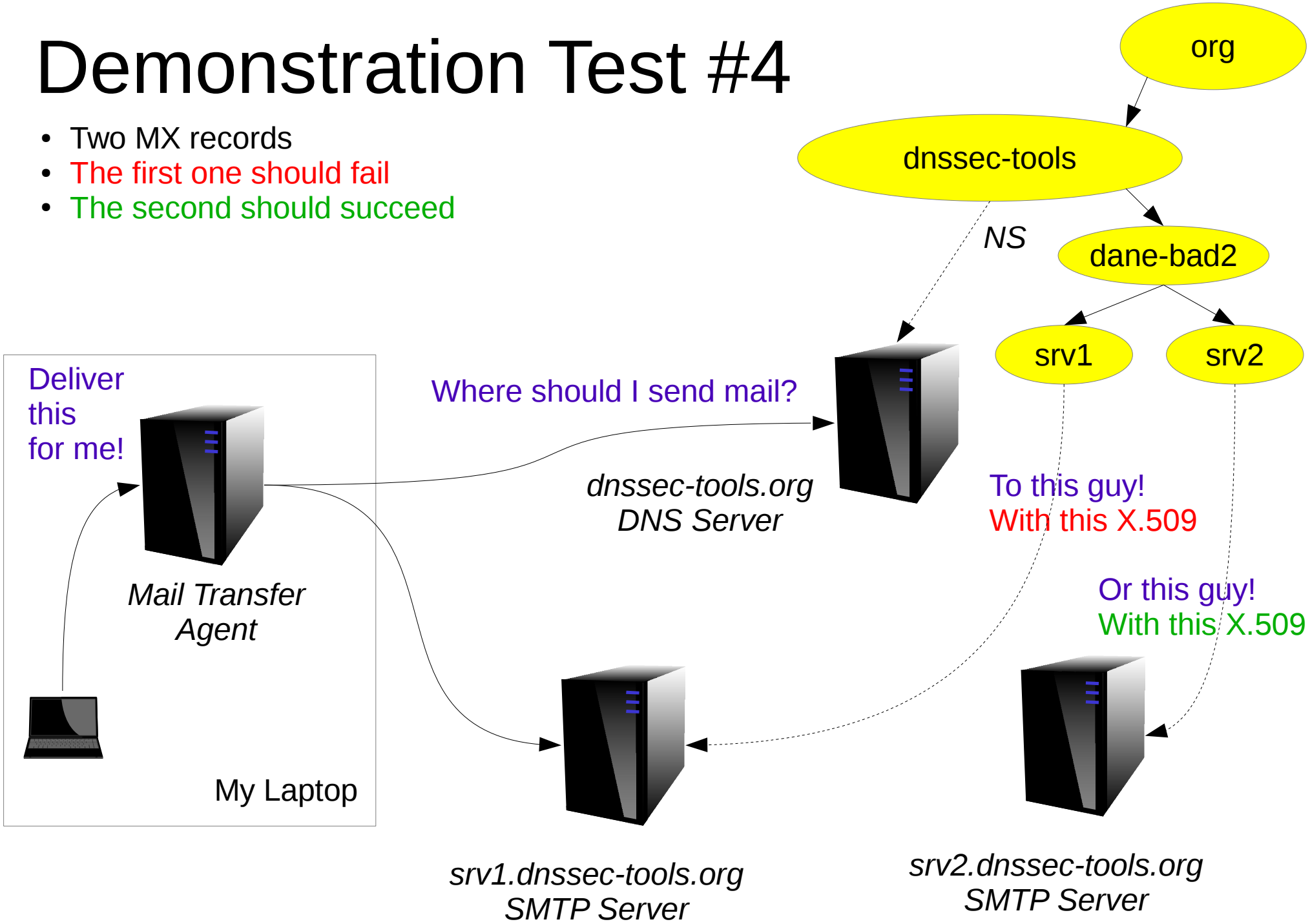
Demonstration Test #3

- A bad guy
- Simulated by a bad record!
  - (could be a mistake! Be careful!)



Demonstration Test #4

- Two MX records
- The first one should fail
- The second should succeed



Come On Out And Play

28,000 Domains with DANE/SMTP enabled!

And the RFC has only been out for a week!

Questions?

wes.hardaker@parsons.com

Extra Slides

Available Software

- DNSSEC Compliant Name Servers
  - Most recent releases of just about everything
  - (no excuses here)

- Mail Software
  - Postfix 2.11 or higher
  - EXIM 4.85 or higher

Try looking up the data!

- Using a DNSSEC compliant resolver:
  - dig dane.dnssec-tools.org MX
  - dig dane.dnssec-tools.org A
  - dig _25._tcp.dane.dnssec-tools.org TLSA
  - dig +dnssec dane.dnssec-tools.org MX

Resources

- RFC6698 DANE
- RFC7218 DANE Acronyms
- RFC7672 SMTP
- RFC7671 DANE Guidance
- http://www.dnssec-tools.org/
- http://postfix.org/