Opportunistic SMTP Security

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

Overview

- E-Mail Overview
- Where E-Mail Can Go Wrong
- Securing E-Mail Requires DNSSEC
- Securing SMTP Using DNSSEC and DANE

Scenario

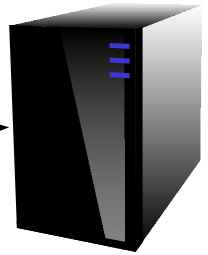
- Alice  needs to send mail to Bob 

- Alice has an ISP 

- Bob has an ISP 

wes.hardaker@parsons.com

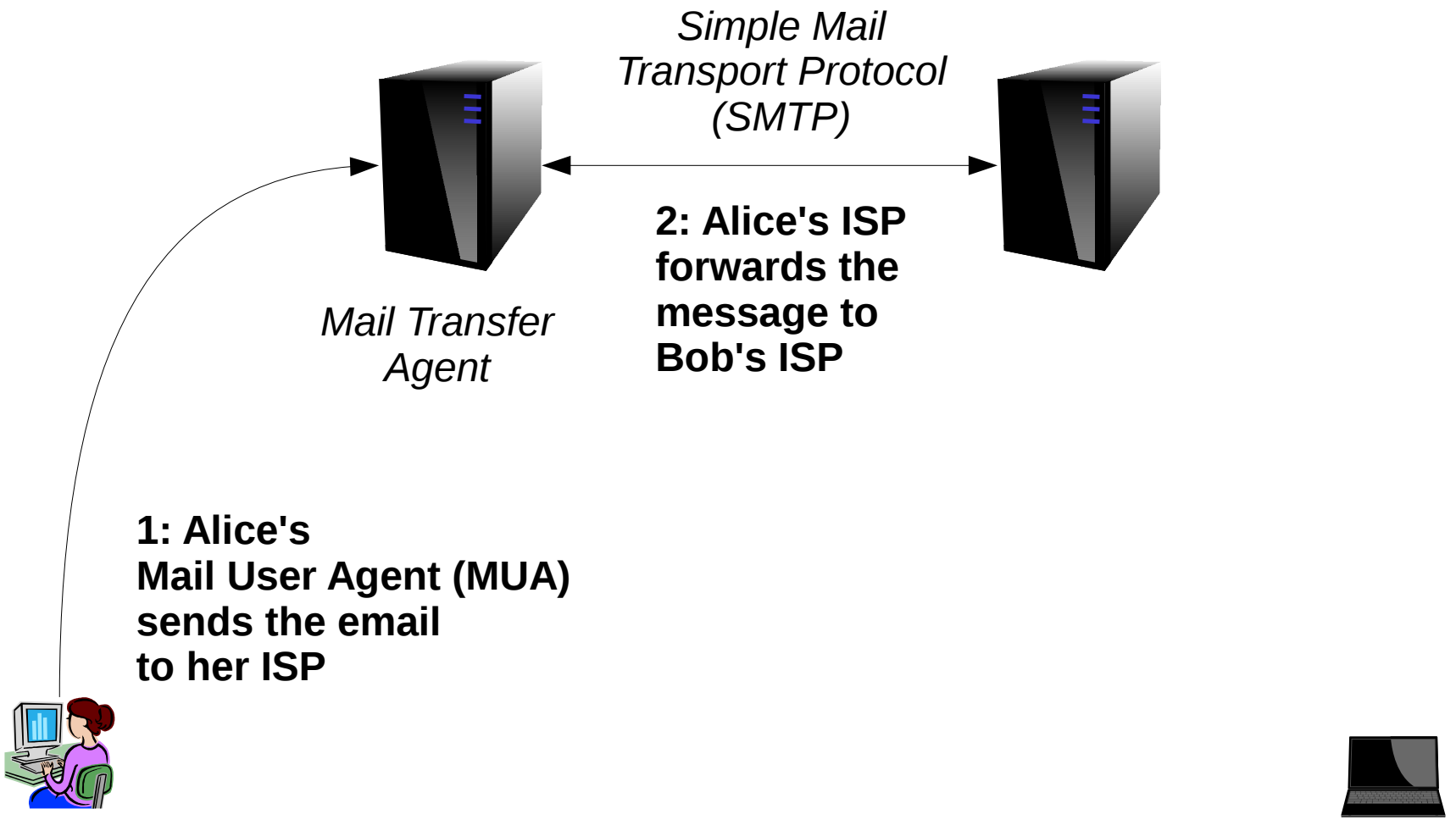
Server-to-Server Email



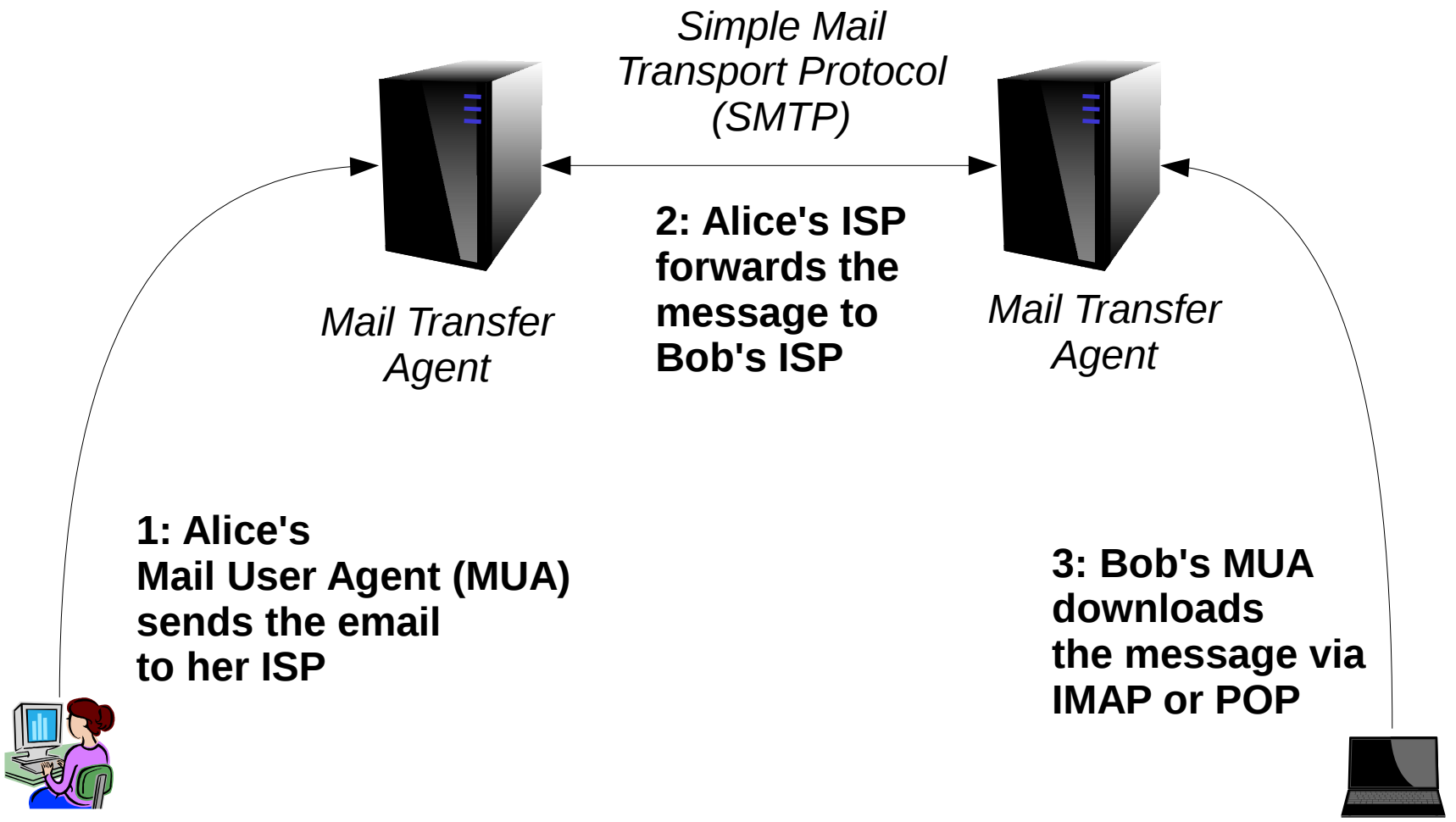
Mail Transfer Agent

1: Alice's Mail User Agent (MUA) sends the email to her ISP

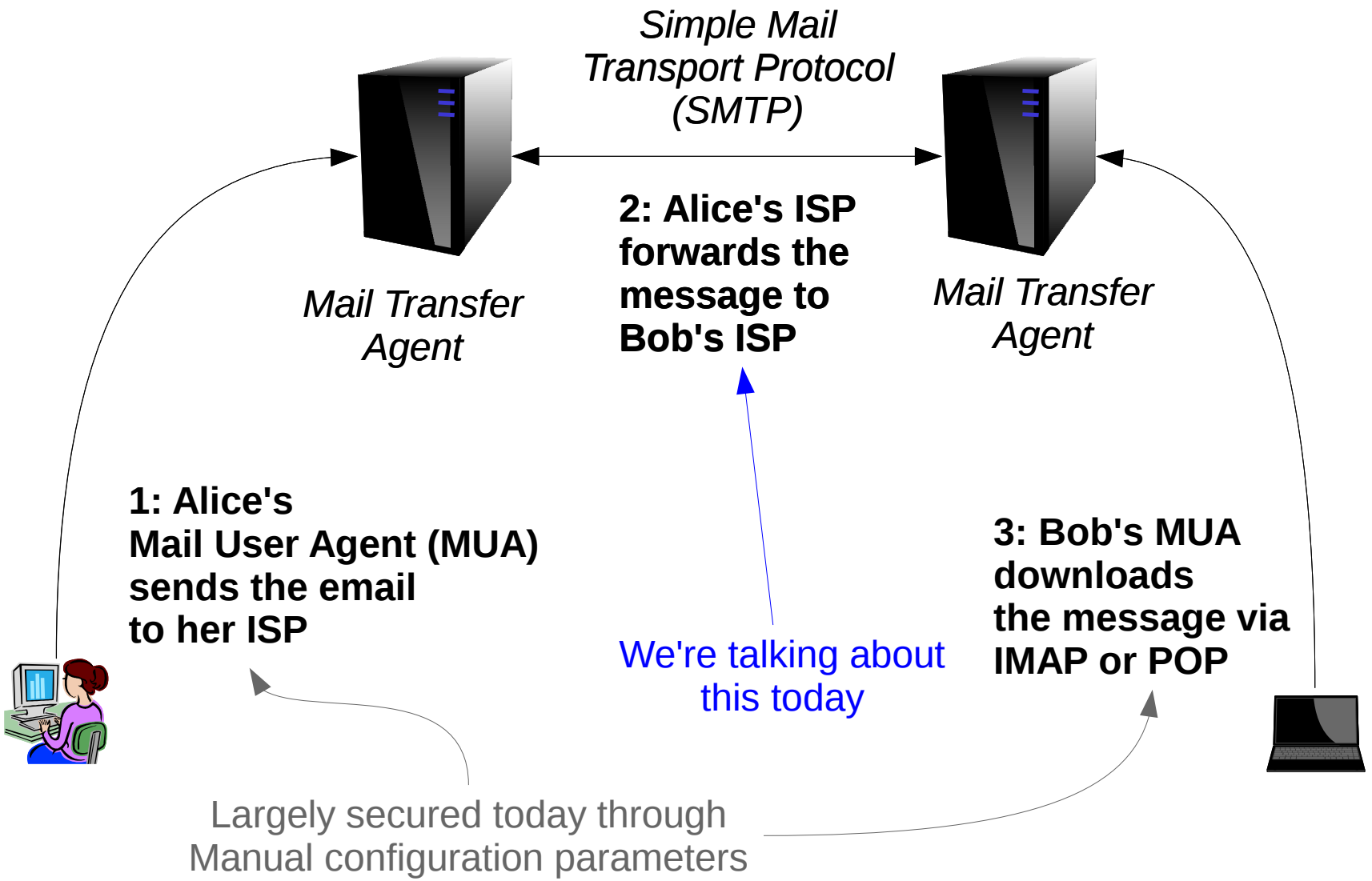
Server-to-Server Email



Server-to-Server Email



Server-to-Server Email

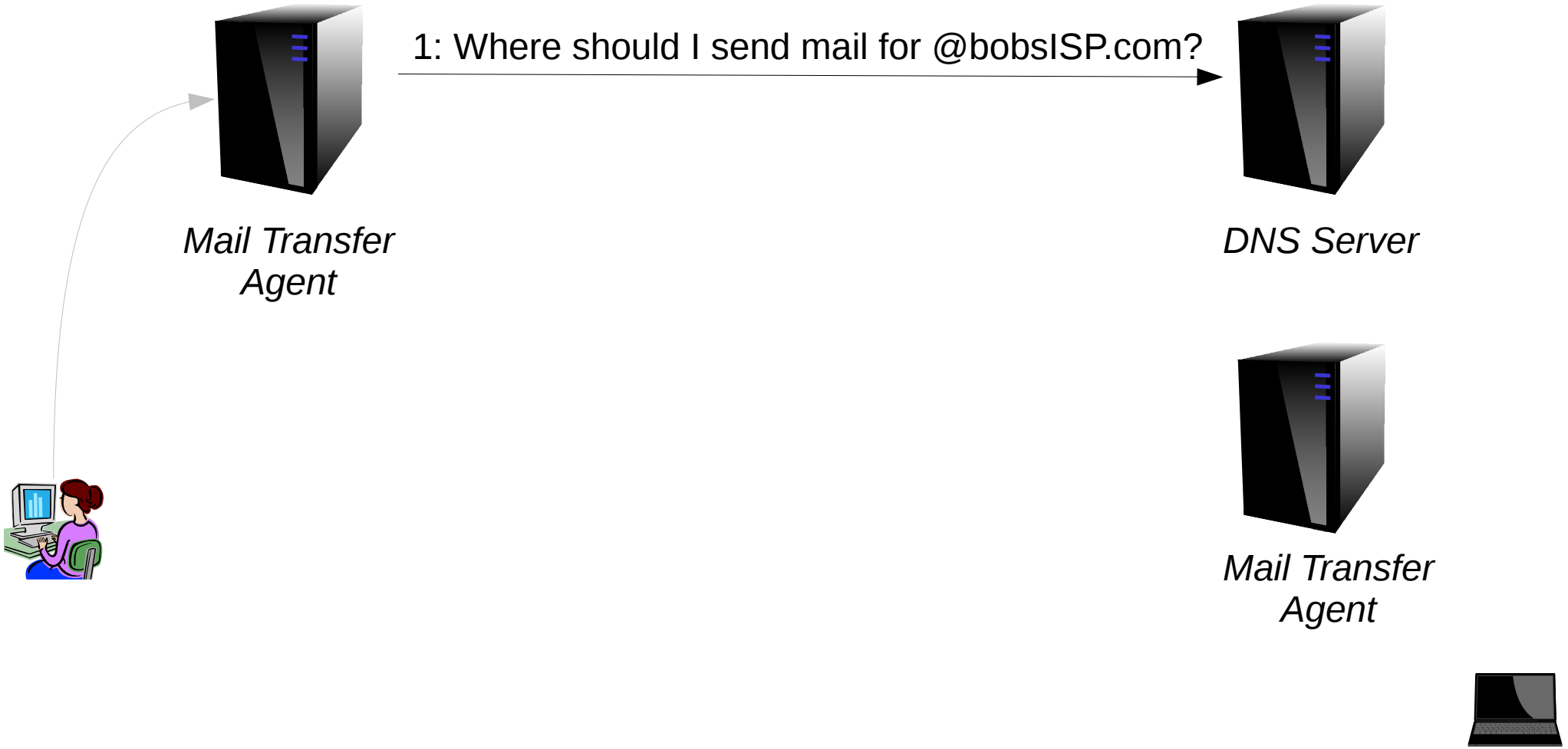


wes.hardaker@parsons.com

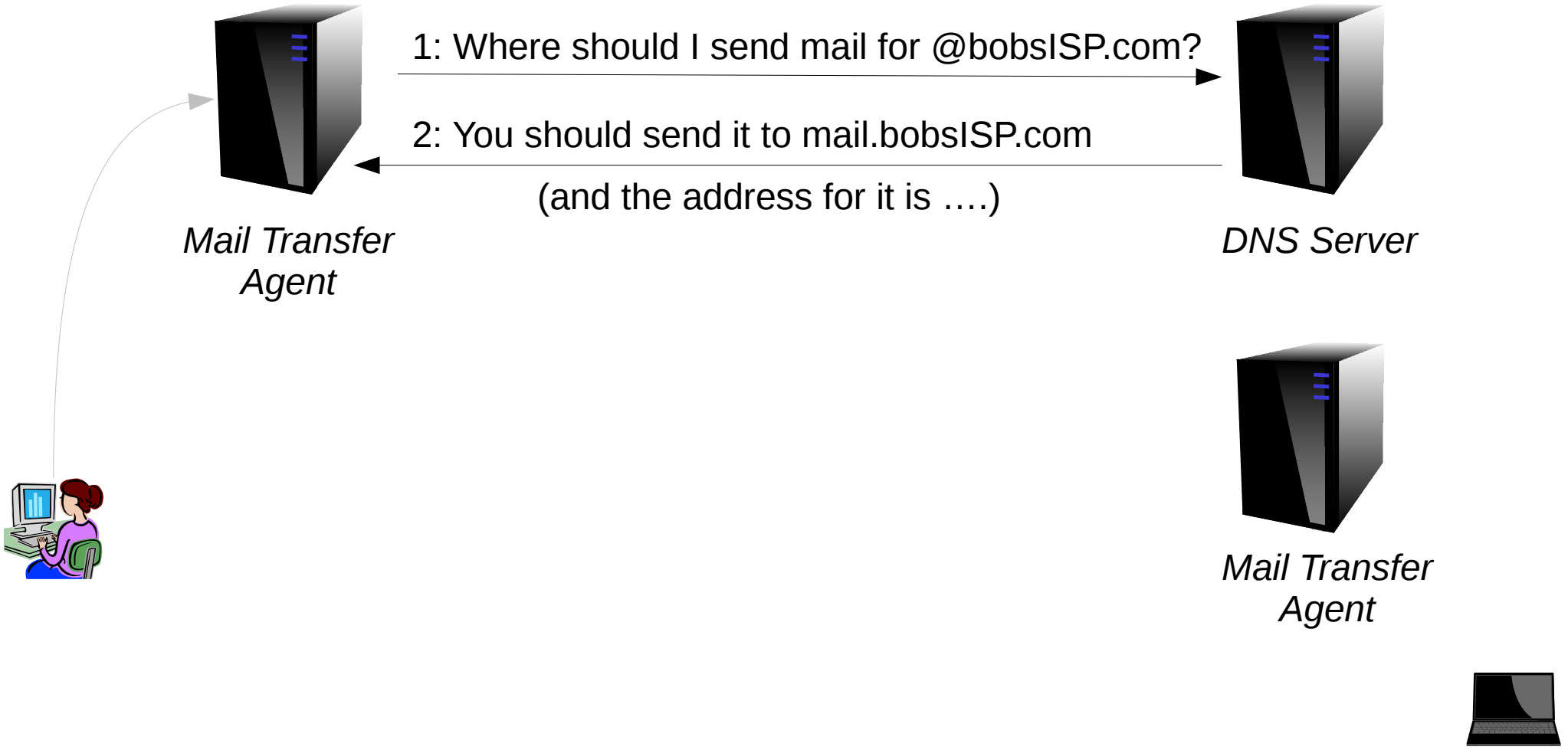
E-mail Server to E-Mail Server

How DNS Is Involved

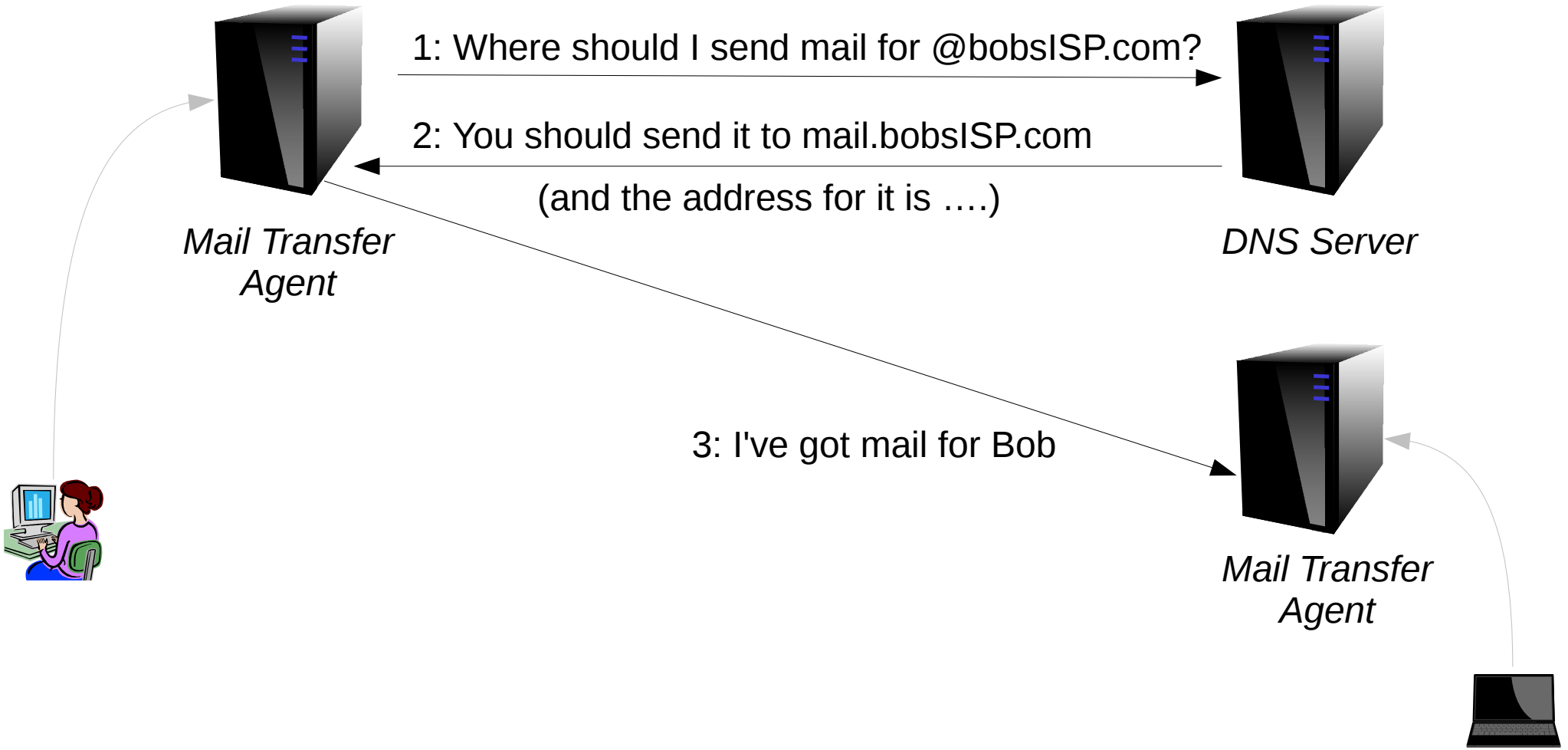
Server-to-Server Email with DNS



Server-to-Server Email with DNS



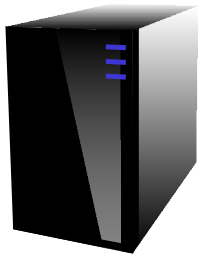
Server-to-Server Email with DNS



I Wish It Were So Simple

- There can be multiple DNS servers
  - Every domain should have at least two
- Alice's mail server asks her ISP's resolver
  - It doesn't talk directly to the distant DNS server
  - There may be multiple resolvers
- There can be multiple mail servers

Server-to-Server Email
Reality Sets In



DNS Server

1: Where should I send mail for @bobsISP.com?

2: You should send it to mail1, mail2 or mail3

3: Do you have an address for mail1?

4: Yep, it's 192.0.2.3

DNS Server

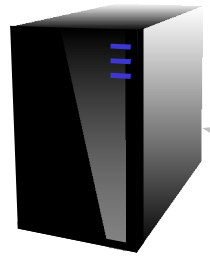
Mail Transfer Agent

5: Hi, I'm representing Alice, I have mail for Bob

6: Hi, I'll take mail for Bob; **PS: I don't do security**

7: Here's the mail for Bob from Alice

8: Thanks, I'll make sure he gets it



Mail Transfer Agent

*(Actually, reality is **even worse** but wouldn't fit on this slide)*

Back To: I Wish It Were So Simple

- There can be multiple DNS servers
  - Every domain should have at least two
- Alice's mail server asks her ISP's resolver
  - It doesn't talk directly to the distant DNS server
  - There may be multiple resolvers
- There can be multiple mail servers

What could possibly go wrong???

- There can be multiple DNS servers
  - Compromised?
- Alice's mail server asks her ISP's resolver
  - It doesn't talk directly to the distant DNS server
  - Compromised?
- There can be multiple mail servers
  - Compromised?
- Man In The Middle

Network Attack

DNS Attack Point!!!

DANE/DNSSEC To The Rescue

- There can be multiple DNS servers
  - Compromised?
- Alice's mail server asks her ISP's resolver
  - It doesn't talk directly to the distant DNS server
  - Compromised?
- There can be multiple mail servers
  - Compromised?
- Man In The Middle

Use DNSSEC

Use DANE

SMTP Vulnerabilities

- MX, A and other DNS records can be spoofed
  - DNS redirects SMTP clients to the.....
  - DNSSEC detects this, and clients won't proceed
- Eavesdropping is Easy
  - SMTP is **un**encrypted by default
  - Opportunistic encryption helps
    - See if they offer a certificate
    - Start encryption if they do
    - However, you may just be encrypting to the.....

SMTP Vulnerabilities

- If DNS is spoofed, you get a...
- ...Man In The Middle
  - SMTP is unauthenticated by default
  - SMTP is unencrypted by default
  - Clients ***can*** turn on opportunistic encryption
    - Server indicates “I do security”
    - But a man-in-the-middle can just say “I don't do security”
  - CA based solutions don't help because:
    - The man-in-the-middle says “I don't do security”
    - You've been redirected to a name the attacker controls

DNSSEC/DANE For The Win

- DNSSEC and DANE solves all these problems!
- With DNSSEC:
  - The MX record set is correct
  - The TLSA record has not been tampered with
- With DANE's TLSA record:
  - States: “This is my certificate” or “This is my CA”
  - You MUST expect security!!! *(i.e., must do TLS)*
- Result: You connected to the right place. Period.
  - And it's an encrypted connection

Deployment Options

- Postfix 2.11
  - Server side (receiving mail):
    - Publish a TLSA record: _25._tcp.smtp.example.com
    - smtpd_tls_cert_file = /path/to/mycert.crt
    - smtpd_tls_key_file = /path/to/mycert.key
  - Client side (sending mail):
    - smtp_tls_security_level = dane
    - smtp_dns_support_level = dnssec
    - **CAVEAT: MUST use a secure local resolver**
- Exim: 4.85

SMTP with DANE Deployment

- Standardization:
  - Almost an RFC
- Deployment:
  - Yes!!
  - 1400 domains using it
    - 20 are listed in google's transparency report
- Test it!
  - https://dane.sys4.de/

Known Large Early SMTP Adopters

- posteo.de
- mailbox.org
- bund.de
- denic.de
- umkbw.de
- freebsd.org
- unitybox.de
- debian.org
- ietf.org
- nlnet.nl
- nic.cz
- t-2.net

Questions?

wes.hardaker@parsons.com

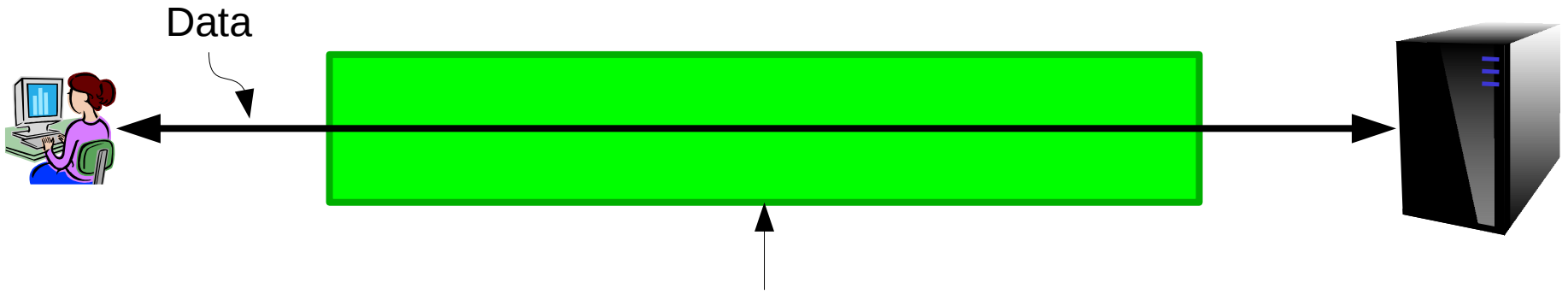
Extra Slides

Resources

- RFC6698 DANE
- RFC7218 Acronyms
- draft-ietf-dane-smtp-with-dane SMTP
- draft-ietf-dane-ops Guidance
- draft-ietf-xmpp-dna XMPP
- draft-ietf-dane-srv SRV
- http://www.dnssec-tools.org/
  - (bloodhound!)
- http://postfix.org/

TLS Overview

- TLS is:
  - An application-layer security tunnel
  - A TCP-based security protocol to secure TCP
    - DTLS secures datagram protocols (eg, UDP)
  - Can provide authentication and encryption
    - Typically based on X.509 Certificate bootstrapping

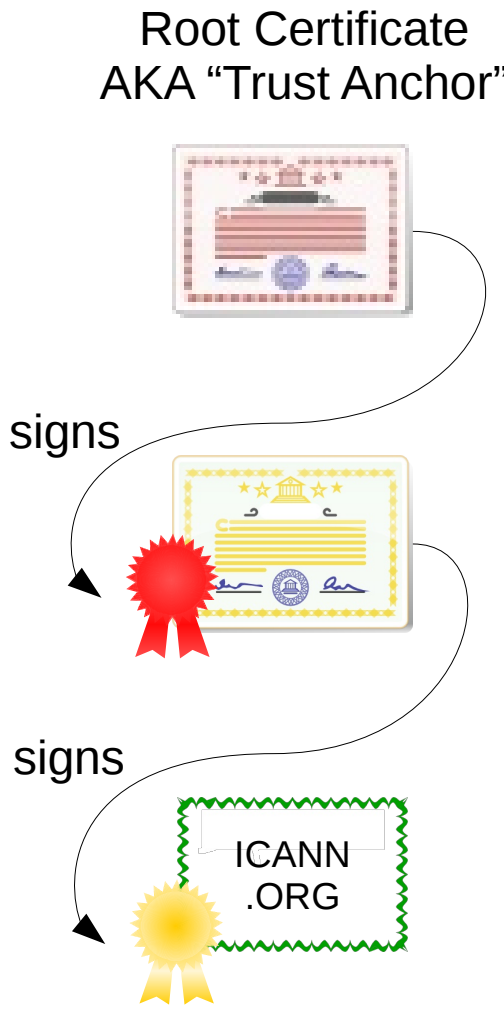


TLS Properties

- TLS ensures that:
  - Eves-dropping is impossible
  - The client connected to the correct server
  - But, this only works when properly anchored
- TLS certificates and trust anchors
  - A server must present a X.509 certificate
  - The client checks this certificate
    - Did it present one with the right name?
    - Did it present one with the right IP address?
    - Was it signed by a CA I trust?

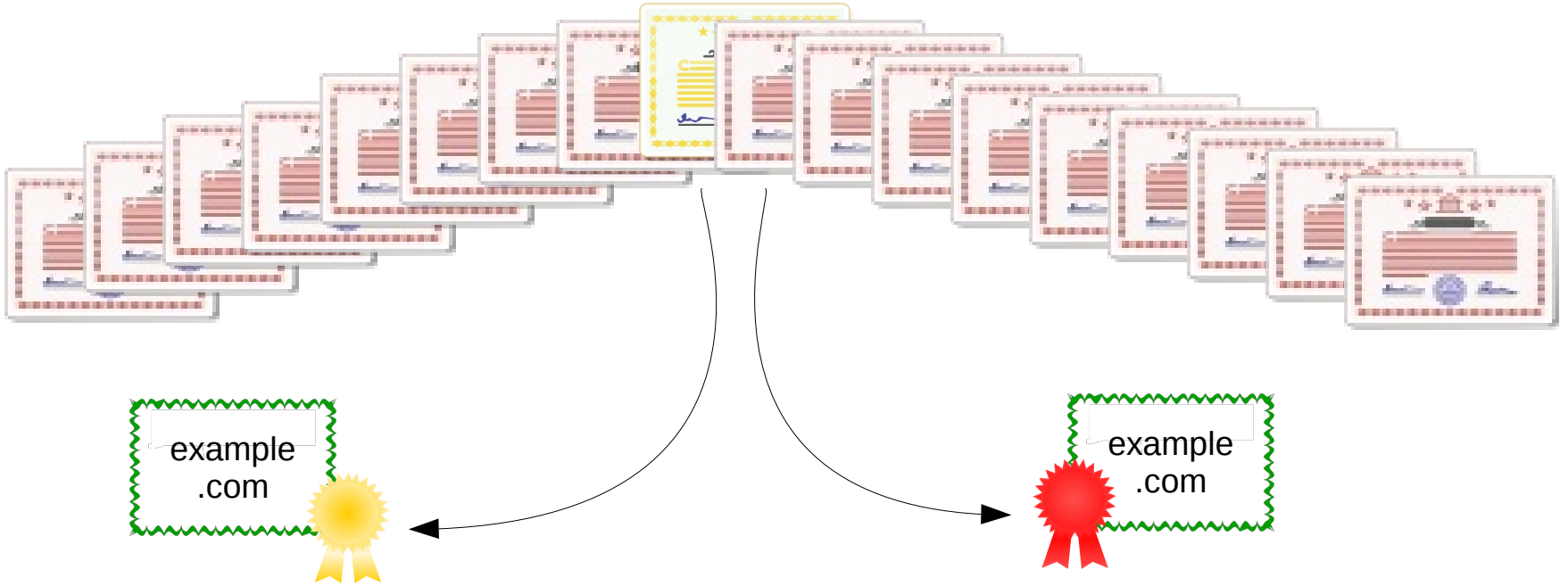
PKIX / X.509 Certificate Trees

- Certificate Authorities (CAs)
  - **Sign** child certificates
  - Should **verify** the child's **identity**
    - Domain ownership
    - Or their legal business name
  - Can be “Trust Anchors” (**TAs**)
- TLS clients
  - Trust their trust anchors
- All is good? CAs are trustworthy?



The “Too Many CAs” Problem

- TLS clients often have an abundance of TAs
  - Modern web browsers have **1300+ TAs**
  - Any of them can issue a certificate for example.com

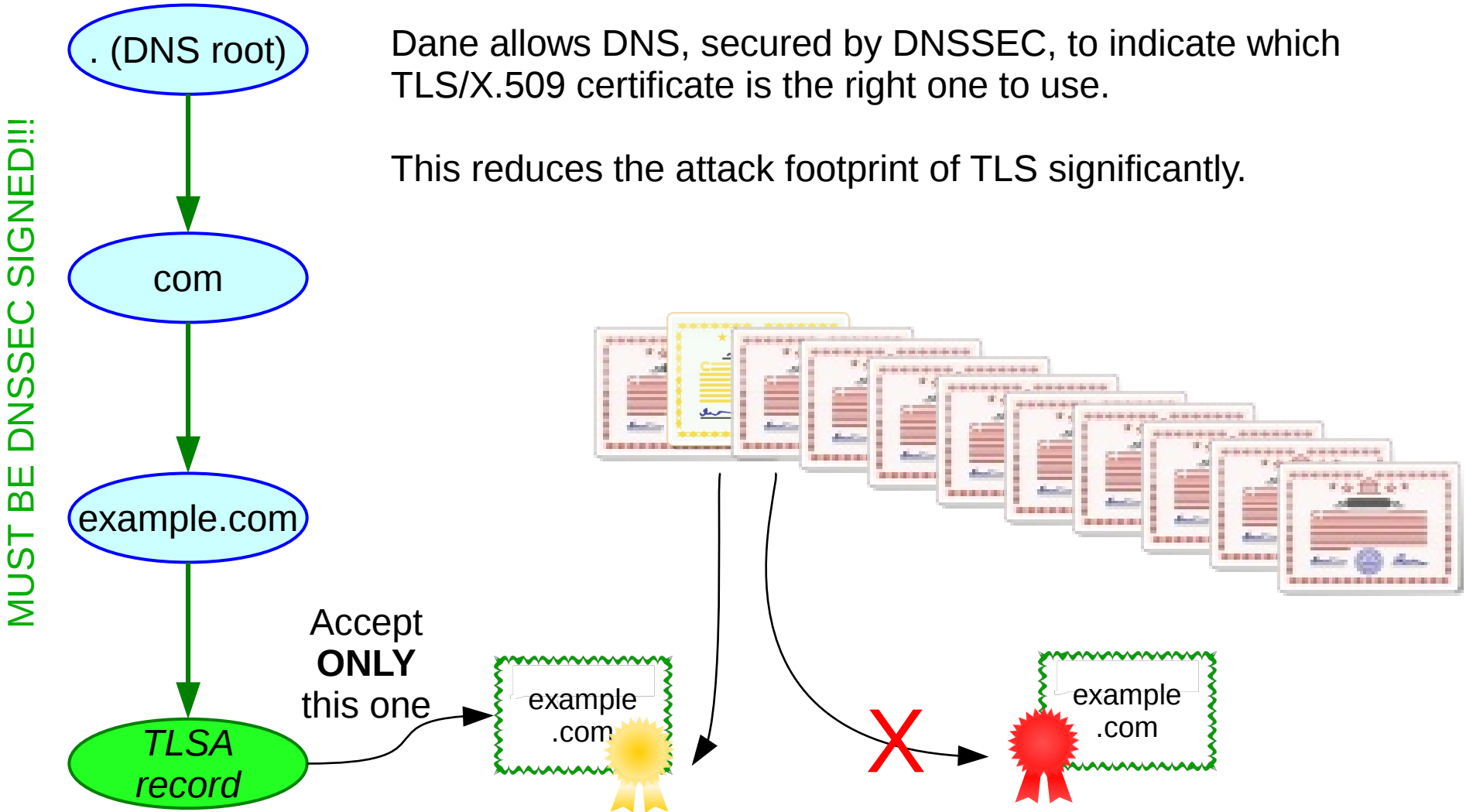


The TLS Client Accepts Them Both!!!
This has happened multiple times!

DANE To The Rescue!

- DNS-Based Authentication of Named Entities
  - A new DNS resource record: "**TLSA**"
  - Indicates the correct server certificate
  - MUST be DNSSEC **signed** to be valid
  - Marries the DNSSEC tree to the X.509 tree
  - Defined in RFC6698
    - Updated by RFC7218

DNSSEC, DANE and X.509



Dane allows DNS, secured by DNSSEC, to indicate which TLS/X.509 certificate is the right one to use.

This reduces the attack footprint of TLS significantly.