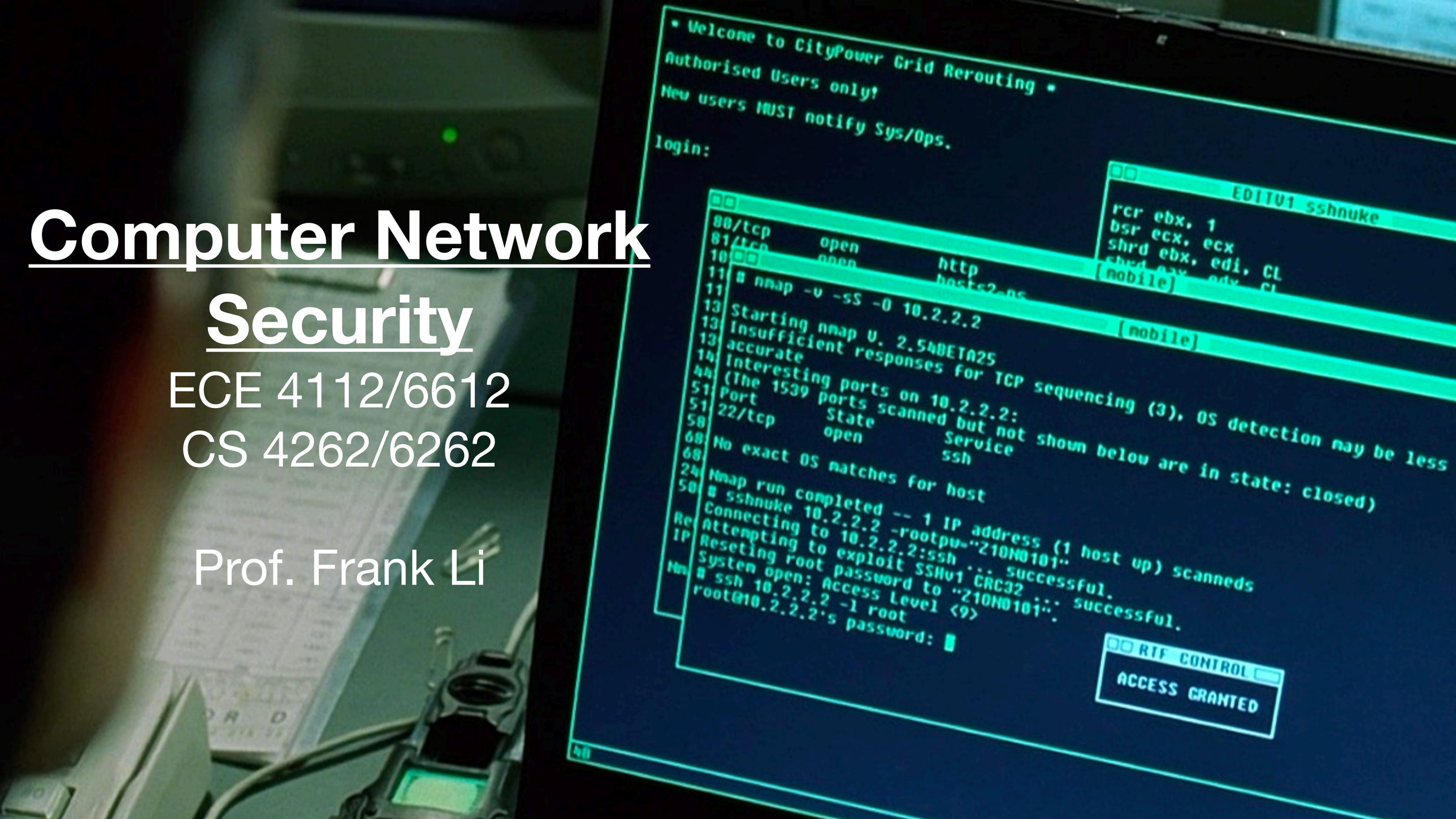
Computer Network Security

ECE 4112/6612
CS 4262/6262

Prof. Frank Li



Logistics

Happy Halloween! 

HW3 on web + email security to be released today, due Monday Nov 13.

Quiz 2 grades to be released soon (with regrade requests open)

Work on your projects!

Tue, Oct 10	**No Class (Fall Break)**
Thu, Oct 12	Web security Part 1: Web attacks and defenses
Tue, Oct 17	Web security Part 2: Web attacks and defenses
Thu, Oct 19	Web security Part 3: Web attacks and defenses
Tue, Oct 24*	**Quiz 2**
Thu, Oct 26*	Authentication
Tue, Oct 31	Email Security (Spam, Phishing)
Thu, Nov 2	Network Access Control
Tue, Nov 7	DoS attacks and defenses
Thu, Nov 9	Malware, Botnet
Tue, Nov 14	Last lecture: Censorship and Anonymous Communication
Thu, Nov 16	**Quiz 3**
Tue, Nov 21	**No Class (Early Thanksgiving Break)**
Thu, Nov 23	**No Class (Thanksgiving Break)**
Tue, Nov 28*	Project: Final Project Presentations
Thu, Nov 30*	Project: Final Project Presentations
Tue, Dec 5	Final Class: Final Project Presentations
Thu, Dec 7	**Final Exam: 2:40 - 5:30 PM (Undergraduate Sections Only)**

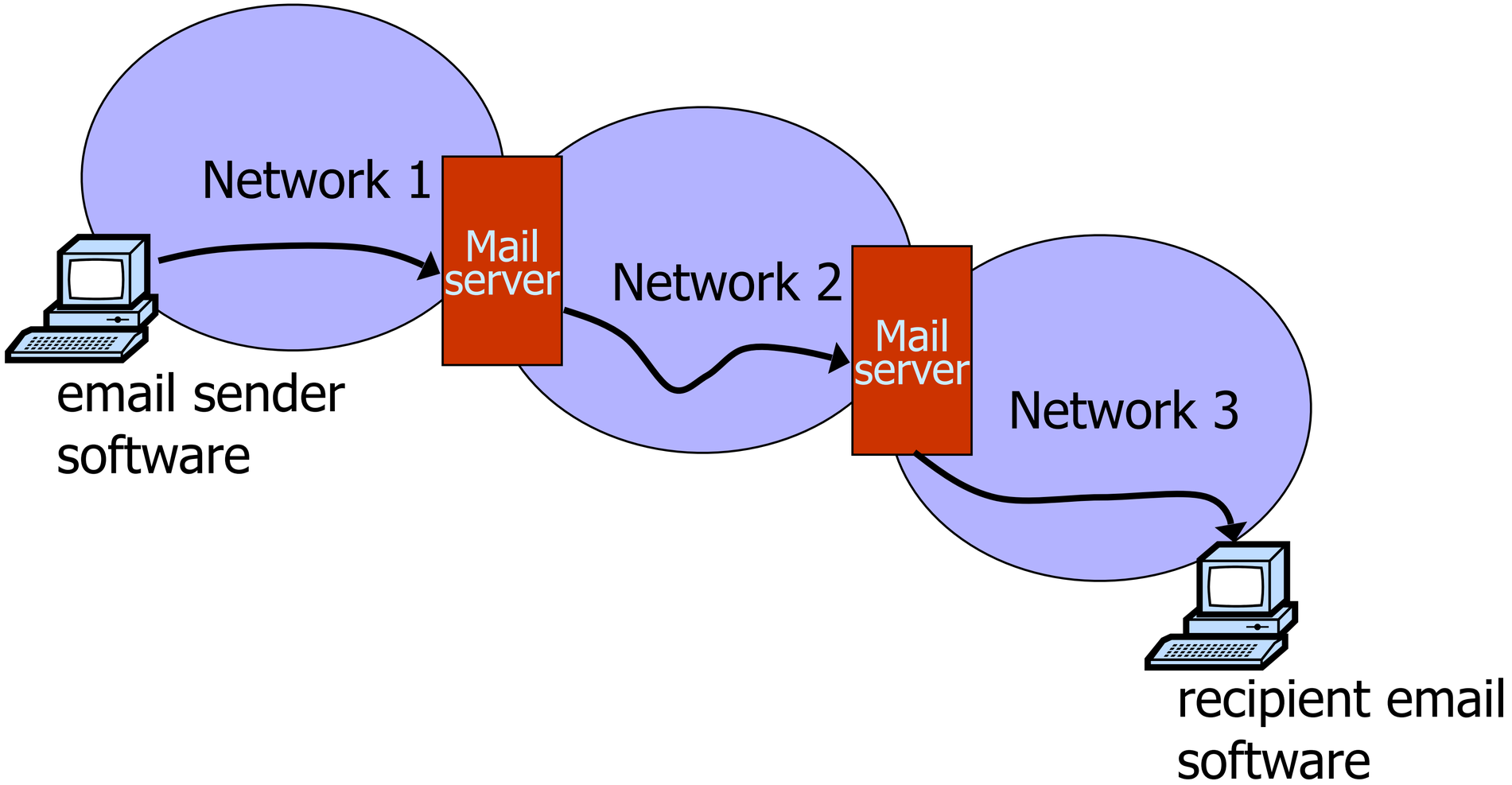
Today: Email Security

Why study email?

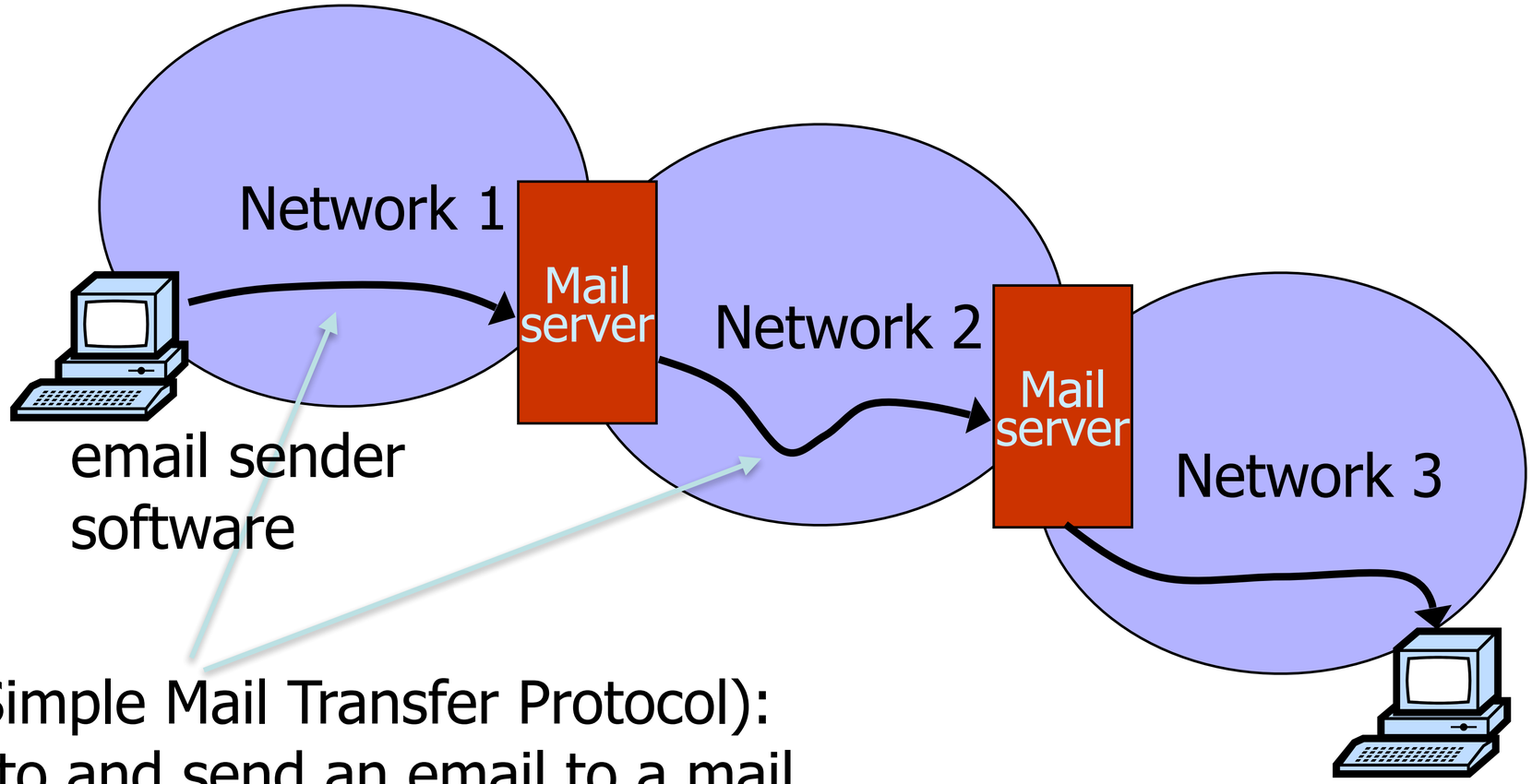
- While an "old" digital messaging method, many more recent messaging protocols share similarities in design and security considerations

- Still ***hugely*** important!
  - 54% of world population is estimated to use email
  - Estimated 350 billion emails sent a day
    - Caveat: significant portion are spam emails though (~40% by some estimates)

Email Protocols



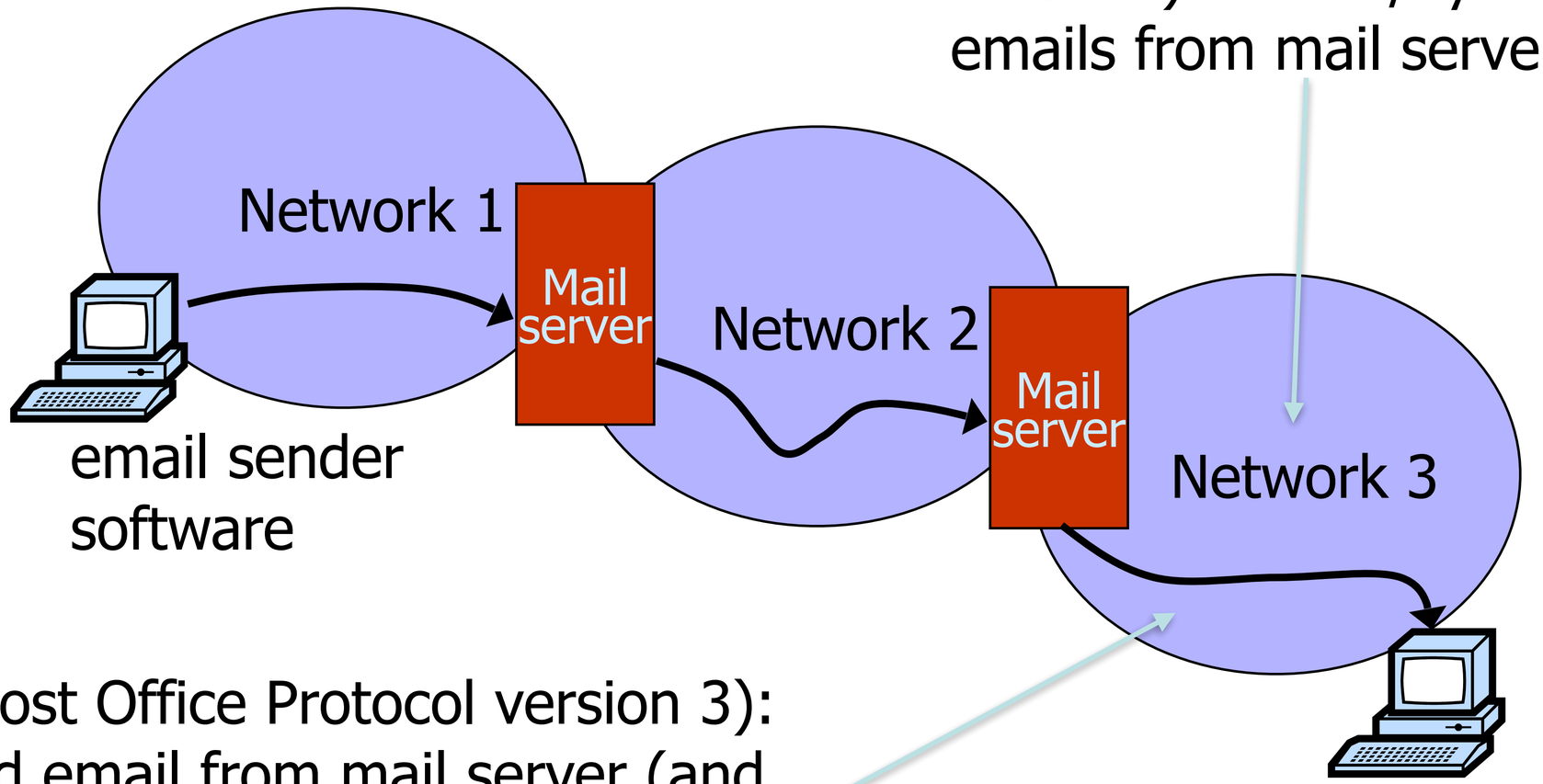
Email Protocols: Transmission



SMTP (Simple Mail Transfer Protocol): Connect to and send an email to a mail server. Used between sender client and mail server, and between mail servers.

Email Protocols: Retrieval

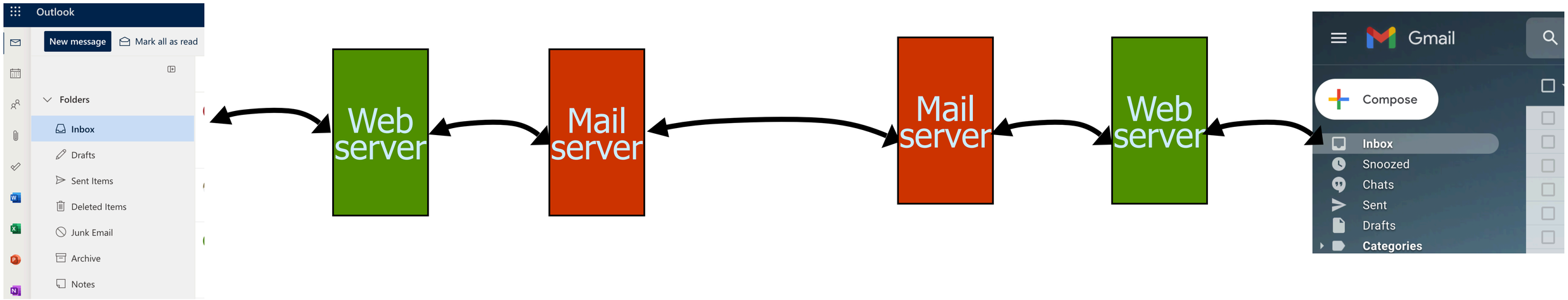
IMAP (Internet Message Access Protocol): Online/dynamic access to emails from mail server.



POP3 (Post Office Protocol version 3): Download email from mail server (and potentially delete from server). Supports offline email access at recipient.

Web Interfaces for Email

Web interfaces (GMail, Outlook.office.com) are *web applications* (so using HTTP). Those web apps will coordinate with mail servers though for sending/receiving email (via SMTP).



Email Protocols

- Default email protocol ports:
  - SMTP: plaintext - TCP/25
  - POP3: plaintext - TCP/110
  - IMAP: plaintext - TCP/143

Email Protocols and TLS

- All 3 email protocols offer an option to "upgrade" an existing plaintext connection a TLS one.
  - For example, if an SMTP client connects to an SMTP server over plaintext (i.e., port 25), the server can issue a *STARTTLS* command to the client.
    - If the client supports TLS, they do the TLS handshake /connection setup, and continue further SMTP communication over TLS (but still on the same port, 25).
    - If not, the client ignores the *STARTTLS* command and continues in plaintext.

Email Protocols and TLS

- Example SMTP exchange w/ STARTTLS:

```
S: <waits for connection on TCP port 25>
C: <opens connection>
S: 220 mail.example.org ESMTP service ready
C: EHLO client.example.org
S: 250-mail.example.org offers a warm hug of welcome
S: 250 STARTTLS
C: STARTTLS
S: 220 Go ahead
C: <starts TLS negotiation>
C & S: <negotiate a TLS session>
C & S: <check result of negotiation>
C: EHLO client.example.org
```

S= SMTP server ; C = SMTP client

Email Protocols and TLS

- All 3 email protocols offer an option to "upgrade" an existing plaintext connection a TLS one.
  - This is **opportunistic TLS encryption** b/c it defends against passive, but not active monitoring (MITM could drop the STARTTLS command).

Email Protocols and TLS

Neither Snow Nor Rain Nor MITM . . .
An Empirical Analysis of Email Delivery Security

Zakir Durumeric[†] David Adrian[†] Ariana Mirian[†] James Kasten[†] Elie Bursztein[‡]
Nicolas Lidzborski[‡] Kurt Thomas[‡] Vijay Eranti[‡] Michael Bailey[§] J. Alex Halderman[†]

[†] University of Michigan [‡] Google, Inc. [§] University of Illinois, Urbana Champaign

{zakir, davadria, amirian, jdkasten, jhalderm}@umich.edu
{elieb, nlidz, kurtthomas, vijaye}@google.com
mdbailey@illinois.edu

ACM Internet Measurement Conference, 2015

Email Protocols and TLS

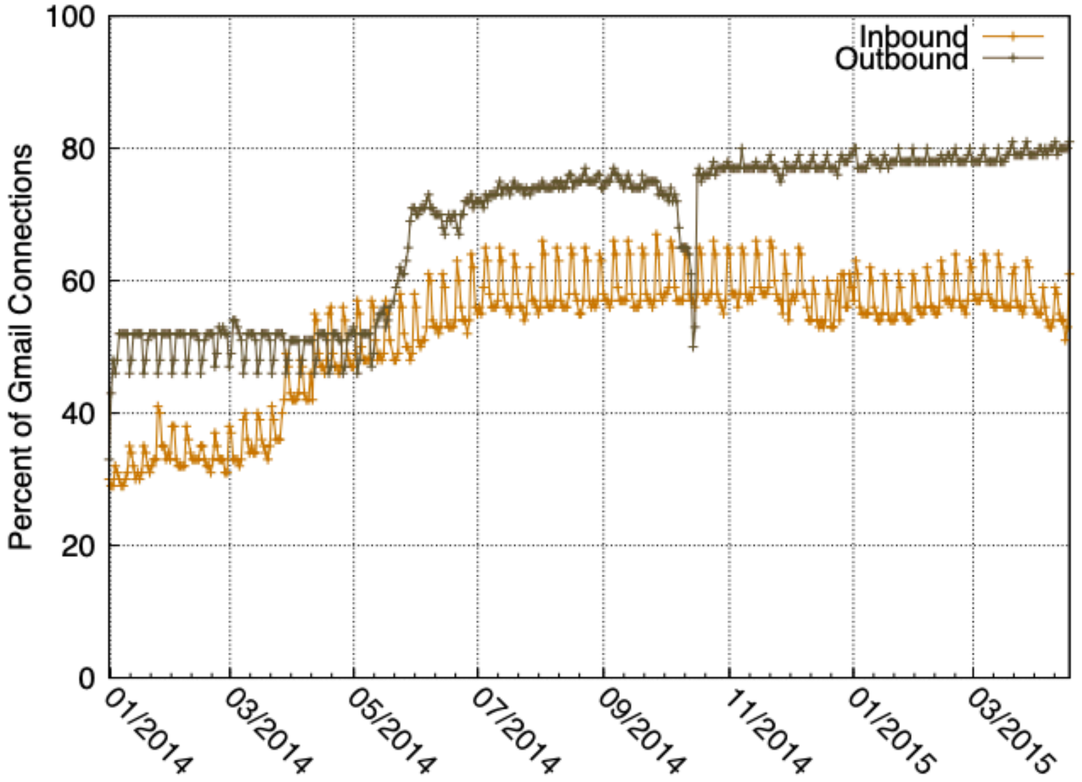
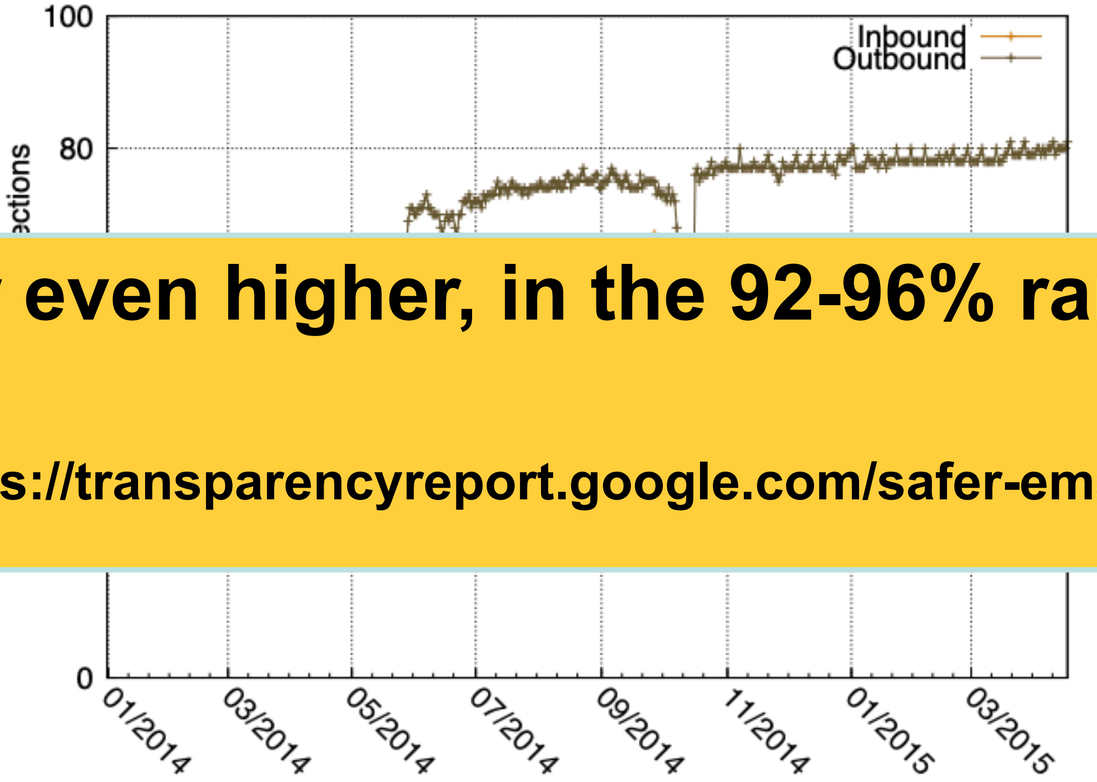


Figure 3: **Historical Gmail STARTTLS Support**—Inbound connections that utilize STARTTLS increased from 33% to 60% for weekdays between January 2014 and April 2015. Weekends consistently have close to 10% more connections that support STARTTLS than weekdays. Support for outgoing STARTTLS increased from 52% to 80% during this period.

Email Protocols and TLS



Now even higher, in the 92-96% range

https://transparencyreport.google.com/safer-email/

Figure 3: **Historical Gmail STARTTLS Support**—Inbound connections that utilize STARTTLS increased from 33% to 60% for weekdays between January 2014 and April 2015. Weekends consistently have close to 10% more connections that support STARTTLS than weekdays. Support for outgoing STARTTLS increased from 52% to 80% during this period.

Email Protocols and TLS

Status	Top Million Domains	
SMTP Server—No STARTTLS support	144,464	(18.2%)
SMTP Server—STARTTLS support	648,030	(81.8%)

Table 3: **STARTTLS Deployment by Top Million Domains**—Our scan results show that 79% of Alex Top Million domains have incoming SMTP servers, of which 81.8% support STARTTLS.

Mail Provider	Domains	STARTTLS	Trusted Certificate	Certificate Matches
Gmail	126,419 (15.9%)	Yes	Yes	server
GoDaddy	36,229 (4.6%)	Yes	Yes	server
Yandex	12,326 (1.6%)	Yes	Yes	server
QQ	11,295 (1.4%)	Yes	Yes	server
OVH	8,508 (1.1%)	Yes	Yes	mismatch
Other	597,717 (75.4%)	–	–	–

Table 4: **Top Mail Providers for Alexa Top Million Domains**—Five providers are used for mail transport by 25% of the Top Million domains. All five support STARTTLS for incoming mail.

Email Protocols and TLS

- Some SMTP servers will "echo" back unknown commands to the client. Using this, the paper tried detecting if some ASes were explicitly stripping/ downgrading the STARTTLS command

Category	IPv4 Hosts	
Command not echoed	3,606,468	(85.26%)
`STARTTLS` echoed correctly	617,093	(14.59%)
`STARTTLS` replaced	5,756	(0.14%)
Command truncated to four characters	786	(0.02%)

Table 11: **Detecting STARTTLS Manipulation**—We could extract an echoed command from 14.75% of servers that sent errors in response to our `STARTTLS` command. 0.14% of these responses indicate that the command was tampered with before reaching the server.

Type	ASes	
Corporation	182	(43.0%)
ISP	74	(17.5%)
Financial	57	(13.5%)
Academic	35	(8.3%)
Government	30	(7.1%)
Healthcare	14	(3.3%)
Unknown	12	(2.8%)
Airport	9	(2.1%)
Hosting	7	(1.7%)
NGO	3	(0.7%)

Table 12: **ASes Stripping STARTTLS**—We categorize the 423 ASes for which 100% of SMTP servers showed behavior consistent with STARTTLS stripping.

Implicit TLS

- You can also directly use TLS with the email protocols, to secure email transfer/retrieval. Default ports:
  - SMTP: plaintext - TCP/25 ; TLS - TCP/587
  - POP3: plaintext - TCP/110 ; TLS - TCP/995
  - IMAP: plaintext - TCP/143 ; TLS - TCP/993

- Here, a client connects to the TLS default port using TLS first, then sends the email protocol traffic encapsulated within TLS. This is called *implicit TLS for an email protocol.*

- Not as popular yet (~20% of email servers)

End-to-End Email Security?

- All email + TLS protocols provide *channel security* for email traffic, but not data security.
  - Mail servers on path can still read/tamper with email (e.g., Google can see all your Gmail messages)
  - **End-to-end email security?**

End-to-End Email Security

- **Approach:** Encrypt and/or sign emails before sending, such that recipient can decrypt/authenticate.
  - Two similar strategies that both require distributing public keys, but have different key trust models: PGP and S/MIME

- Encryption steps (Alice sending to Bob):
  1. Alice generates a random symmetric key K_S
  2. Alice encrypts email M with K_S
  3. Alice also encrypts K_S using Bob's public key K_B
  4. Alice's encrypted email includes Enc(K_S, M) and Enc(K_B, K_S).

End-to-End Email Security

- **Approach:** Encrypt and/or sign emails before sending, such that recipient can decrypt/authenticate.
  - Two similar strategies that both require distributing public keys, but have different key trust models: PGP and S/MIME

- Decryption steps (Alice sending to Bob):
  1. Bob uses his private key to decrypt Enc(K_B, K_S) and get the plaintext symmetric key K_S
  2. Bob uses K_S to decrypt the encrypted email Enc(K_S, M).

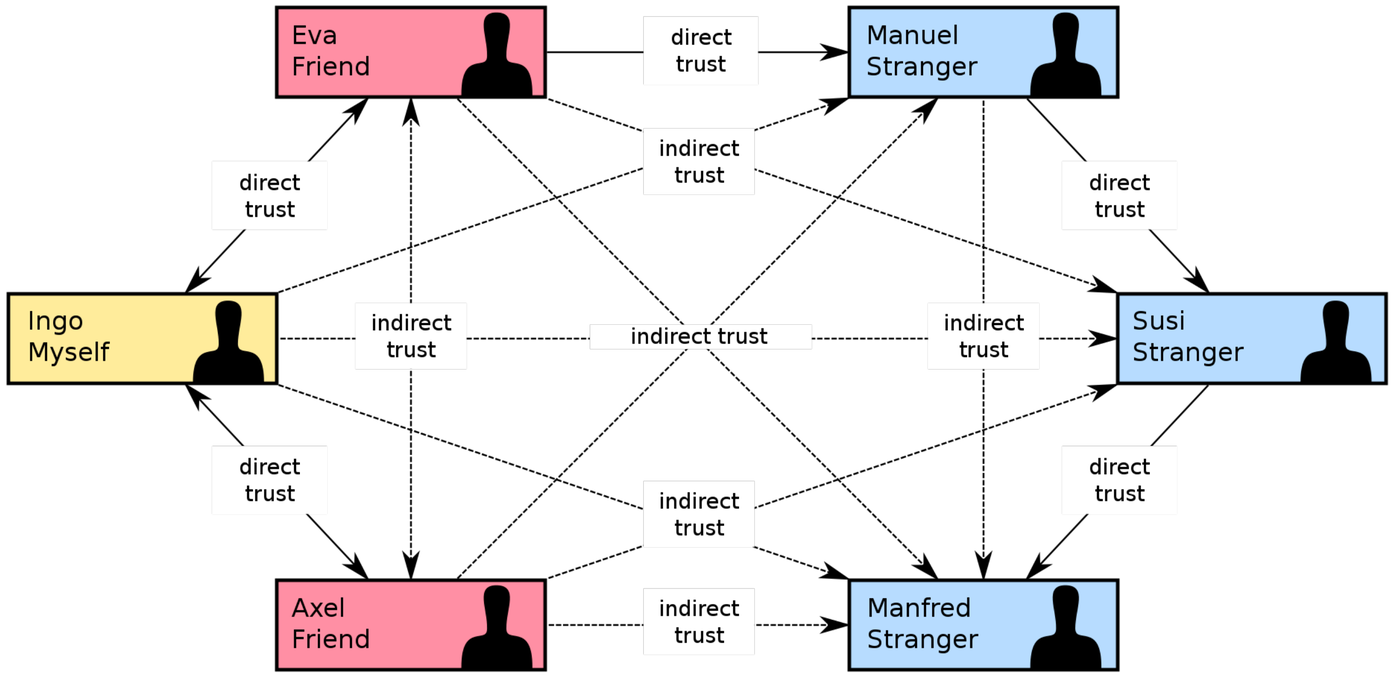
End-to-End Email Security

- **Approach:** Encrypt and/or sign emails before sending, such that recipient can decrypt/authenticate.
  - Two similar strategies that both require distributing public keys, but have different key trust models: PGP and S/MIME

- Authentication steps (Alice sending to Bob):
  1. Alice hashes her message and signs it using Alice's private key, including the signature in the email
  2. Bob hashes the received message and checks it against the included signature using Alice's public key.

PGP vs S/MIME

- Different key trust models
  - PGP uses *Web of Trust* (WOT) where people who trust each other sign each other's keys (each person is an "endorser", sort of like a certificate authority).



PGP vs S/MIME

- Different key trust models
  - PGP uses *Web of Trust* (WOT) where people who trust each other sign each other's keys (each person is an "endorser", sort of like a certificate authority).
    - » Makes sharing public keys easy, but requires some indirect chain of trust from recipient to sender
    - » Can have different levels of trust for endorsers/keys and complex policies of trust
      - » Ex: trust levels for an endorser can be none, partial, or full, and maybe 3 partially trusted endorsers are needed to trust a key, whereas 1 fully trusted endorser is enough

PGP vs S/MIME

- Different key trust models
  - S/MIME uses a traditional PKI design with certificate hierarchy/authorities.
    - » Makes sharing public keys harder (need to get a certificate from a CA first), but trust is more easily established
    - » Often used in an enterprise setting where the enterprise can provide a CA as a root of trust

Challenges w/ End-to-End Email Security

- Key distribution is still hard
  - Either need infrastructure or community for establishing trust ("key signing parties")
  - Still have to deal w/ key revocation (harder in WOT)
- Email is encrypted end-to-end, so limits email inspection/spam filtering
- Encryption tools are hard to understand and use
  - Average email user doesn't know about keys and signatures

Challenges w/ End-to-End Email Security

- Encryption tools are hard to understand and use

Why Johnny Can't Encrypt:
A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

J. D. Tygar[1]
EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu

USENIX Security, 1999

Why Johnny Still, Still Can't Encrypt:
Evaluating the Usability of a Modern PGP Client

Scott Ruoti, Jeff Andersen, Daniel Zappala, Kent Seamons
Brigham Young University
{ruoti, andersen} @ isrl.byu.edu, {zappala, seamons} @ cs.byu.edu

CHI, 2016

Is that you, Alice? A Usability Study of the Authentication Ceremony of Secure Messaging Applications

Elham Vaziripour, Justin Wu, Mark O'Neill, Ray Clinton, Jordan Whitehead,
Scott Heidbrink, Kent Seamons, Daniel Zappala
Brigham Young University
{*elhamvaziripour,justinwu,mto,rclinton,jaw,sheidbri*}*@byu.edu*, {*seamons,zappala*}*@cs.byu.edu*

SOUPS, 2017

Email Messages

- Emails consist of headers and then the message body (just like HTTP requests/responses)
- A few notable headers:
  - **From**: message sender
  - **To**: message recipient
  - **Received**: Each hop in the email delivery path (this header is added at each hop, so may show up multiple times)
  - **Subject**: Email subject line

Email Messages

Received: by 10.78.68.6 with SMTP id q6cs394373hua;
Mon, 12 Feb 2007 06:43:30 -0800 (PST)
Received: by 10.90.113.18 with SMTP id l18mr17307116agc.1171291410432;
Mon, 12 Feb 2007 06:43:30 -0800 (PST)
Return-Path: <wvnlwee@aviva.ro>
Received: from onelinkpr.net ([203.169.49.172])
by mx.google.com with ESMTP id 30si11317474agc.2007.02.12.06.43.18;
Mon, 12 Feb 2007 06:43:30 -0800 (PST)
Received-SPF: neutral (google.com: 203.169.49.172 is neither permitted nor
denied by best guess record for domain of wvnlwee@aviva.ro)
Message-ID: <20050057765.stank.203.169.49.172@ASAFTU>
From: "Barclay Morales" <wvnlwee@aviva.ro>
To: <raykwatts@gmail.com>
Subject: This is totally not spam

Email Messages

- Emails consist of headers and then the message body (just like HTTP requests/responses)
- A few notable headers:
  - **From**: message sender, **set by the sender client**
  - **To**: message recipient
  - **Received**: each hop in the email delivery path (this header is added at each hop, so may show up multiple times). **Receiving mail server only knows the sending mail server (and must trust that the prior Received headers are correct)**
  - **Subject**: email subject line

Email Spoofing

- An email client could send a message with a fake/ wrong *From* field.
  - Unless the first-hop mail server validates this sender, but many mail servers do not (people can also run their own mail server, as can the attacker)
  - After the first hop, hard for later mail relay/servers to determine if the original sender is legitimate

Email Spoofing

Received: by 10.78.68.6 w hua;
Mon, 12 Feb 2 T)
Received: by 10.90.113.18 with SMTP id l18mr17307116agc.1171291410432;
Mon, 0 -0800 (PST)
Return-Path: <wv
Received: from oneiinkpr.net ([203.169.49.172])
by mx.google.com with ESMTP id 30si113174 4agc.2007.02.12.06.43.18;

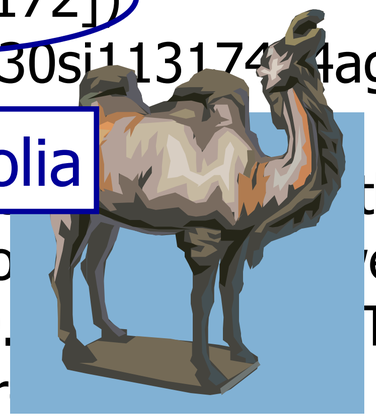
Receive ther permitted nor
best guess record for do ee@aviva.ro)
Messag 50057765.stank.203.169. TU>
From: "Barclay Morales" <wvnlwee@aviva.r
To: <raykwatts@gmail.com>
Subject: This is totally not spam

Inserted by relays

Bogus!

Puerto Rico

Mongolia



Email Spoofing

- An email client could send a message with a fake/ wrong *From* field.
  - Unless the first-hop mail server validates this sender, but many mail servers do not (people can also run their own mail server, as can the attacker)
  - After the first hop, hard for later mail relay/servers to determine if the original sender is legitimate

- **Why bother doing this?**


SPAM
Spread
SPAM
SPAM
Lite
SPAM
HAWAII
SPAM
25% LESS SODIUM
SPAM
Garlic
SPAM
with Cheese
SPAM
Oven Roasted
TURKEY
SPAM
SPAM
Bacon
SPAM
BBQ
SPAM
HOT & SPICY
SPAM
Hickory Smoke

Email Spoofing

- **Why bother doing this?**
  - Attackers want their emails to look like they're coming from a legitimate sender (e.g., bankofamerica.com), particularly for phishing attacks.

  - Many email providers blacklist domains/IP addresses that generate lots of spam or phishing emails. Spoofing helps attackers avoid these blacklists. (Botnets also help with this, and are a big source of spam.)

Email Spoofing

From: fraud@bankofamericans.com

To: targets@contoso.ltd

Date: Thu, 13 Jun 2019 09:35:31 -0700

Subject: **Your Account Has Been Locked**

Bank of Americans

Dear Online Banking Customer:

We are writing to inform you that there have been a number of invalid login attempts to access your account. As a result, we have temporarily locked your account and added an extra verification process intended to ensure your identity and protect the security of your account in the future.

Please click here to begin the account verification process. If you fail to update your account information in the next 24 hours, you will be required to go into our branch to reestablish your account.

Sincerely,
Bank of Americans Fraud Detection

Spoofing Defenses

- **Sender Policy Framework (SPF):** Allows a domain to indicate authorized senders (claiming to be sending from that domain)
- **DomainKeys Identified Mail (DKIM):** Allows a domain to publish a public key used to sign emails sent by authorized senders
- **Domain-based Message Authentication, Reporting and Conformance (DMARC):** Allows a domain to indicate what mail servers should do if SPF and/or DKIM checks fail (and who to report to)

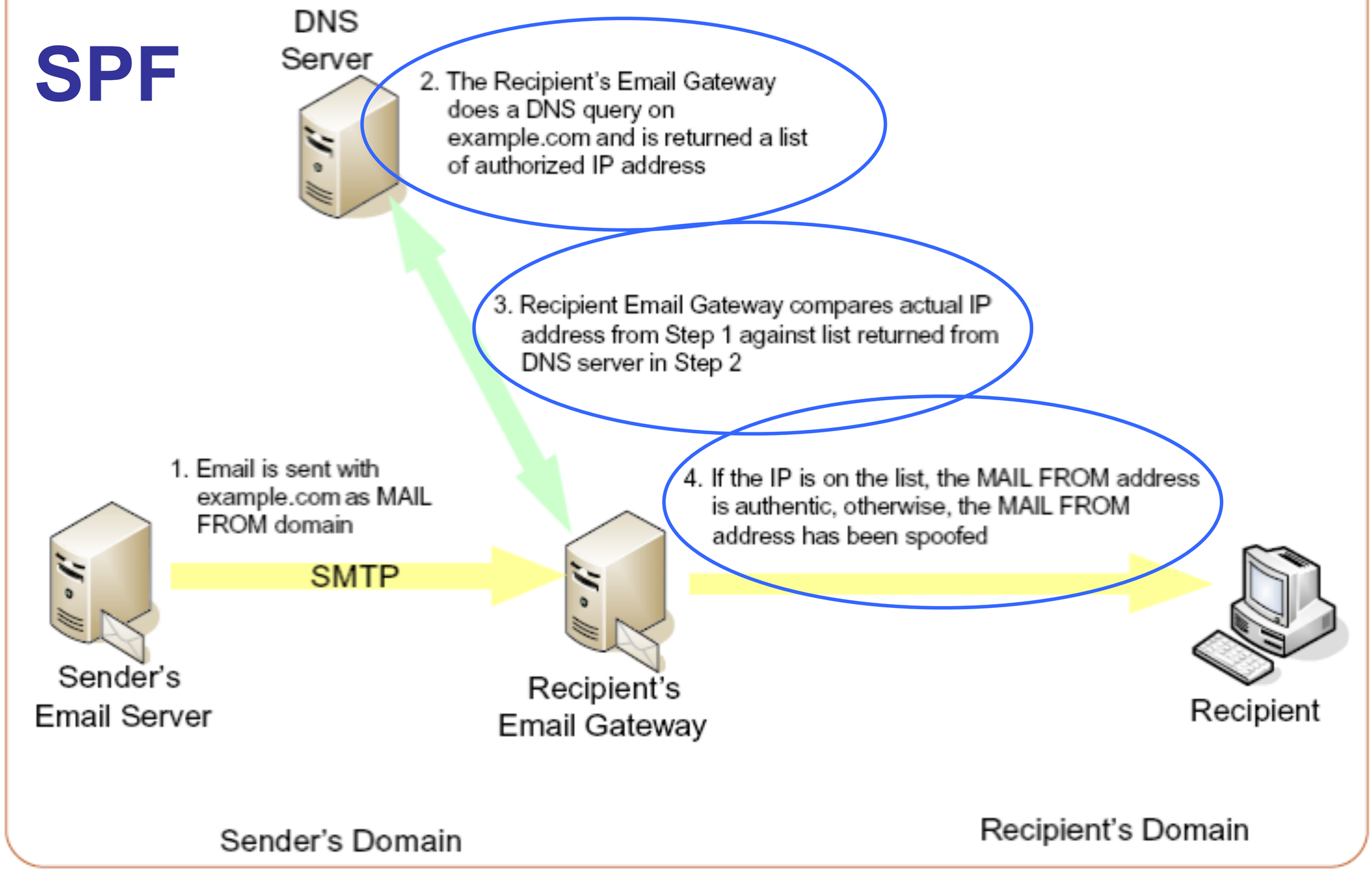
SPF

- A domain can publish a DNS TXT record indicating the mail servers authorized to send emails from that domain
  - Can list the authorized mail servers' IP addresses or domain names
  - Example: frank.com can list which IP addresses are allowed to send @frank.com emails.

- When receiving an email, a mail server can lookup the SPF DNS record for the sender's domain, and see if the email was received from an authorized sender. If not, could be spoofing.

- SPF records can also indicate a policy of what to do for unauthorized senders (e.g., allow, drop)

SPF


DNS Server
2. The Recipient's Email Gateway does a DNS query on example.com and is returned a list of authorized IP address
3. Recipient Email Gateway compares actual IP address from Step 1 against list returned from DNS server in Step 2
1. Email is sent with example.com as MAIL FROM domain
SMTP
4. If the IP is on the list, the MAIL FROM address is authentic, otherwise, the MAIL FROM address has been spoofed
Sender's Email Server
Recipient's Email Gateway
Recipient
Sender's Domain
Recipient's Domain

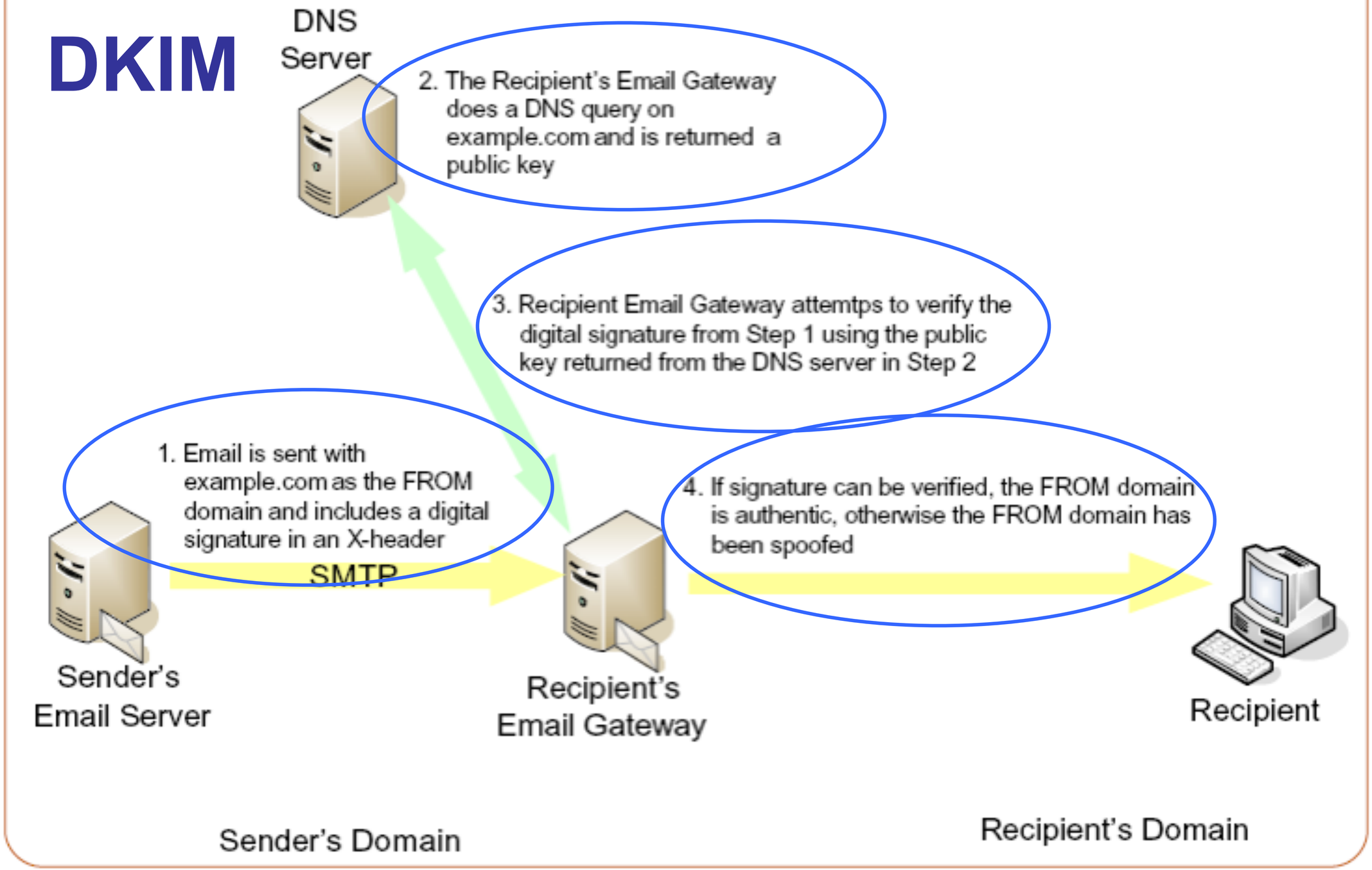
DKIM

- A domain can publish a DNS TXT record with a public key used to sign legitimate email from that domain.

- All legitimate email from that domain must include a signature created using the published key, put in the DKIM-Signature email header.
  - Authorized mail servers can generate this signature for every sent email.

- When receiving an email, a mail server can lookup the DKIM DNS record for the sender's domain, and see if the public key there can validate the email's DKIM signature. If not, email could be spoofed.

DKIM


DNS Server
2. The Recipient's Email Gateway does a DNS query on example.com and is returned a public key
3. Recipient Email Gateway attemtps to verify the digital signature from Step 1 using the public key returned from the DNS server in Step 2
1. Email is sent with example.com as the FROM domain and includes a digital signature in an X-header
SMTP
4. If signature can be verified, the FROM domain is authentic, otherwise the FROM domain has been spoofed
Sender's Email Server
Recipient's Email Gateway
Recipient
Sender's Domain
Recipient's Domain

DKIM-Signature Header (HW3)

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=coe.gatech.edu; s=gt1; h=from:to:date:message-id:content-id:
content-transfer-encoding:mime-version:subject:reply-to:
sender:list-id:list-archive:list-help:list-owner: list-
post:list-subscribe:list-unsubscribe; bh=GuDd4TCd/
gkGXXG5B7j3aTtSIbh41BhM7KFbHa8Oi/A=; b=NFL8jSdKfYSkzdZBbEVZG+K/
qQH32v7pVb4tzRv7MbjKEAHbNNktAsof hzH/
MJOKvzISunXwxs855ChR+UCFLKQ2xb4B/aZXJvTr7FKGsmX78hwC5
JtmdnBHyKXOSzk7CYWHLpV4QpLdGh4L2piERO/xNyyEzIBr9VXFjHiP39
NLgrcPFSW+towhsJNpX8EcGX8LwO+pzUL+qQ2Ez/xGYn0DRTQOQFxMxzQ
5KTyQAz1dzGIL7r8QU3xZt5hmfFurO0ZetaHaNKpT5+5eBtUwKke8agmV
vhBqZXpHLH3zkUkvkMlXoWyIJnkjQAugAcajNOU8L6+0+W8fim9YZvO37 g==;
```

SPF vs DKIM

- Need to check both in practice, b/c some domains only deploy one and not the other (SPF is older, DKIM is newer).

- Some tradeoffs:
  - SPF requires being able to enumerate authorized senders.
  - DKIM requires modifying mail servers to generate DKIM signatures.
  - If email routing legitimately requires many hops, this can screw up SPF (b/c later hops don't directly communicate with/see the address of authorized senders). DKIM isn't affected.
  - SPF provides defense-in-depth though (more information on authorized senders). For example, DKIM doesn't prevent message replay attacks (although the threat seems(?) rather limited).

SPF and DKIM in practice

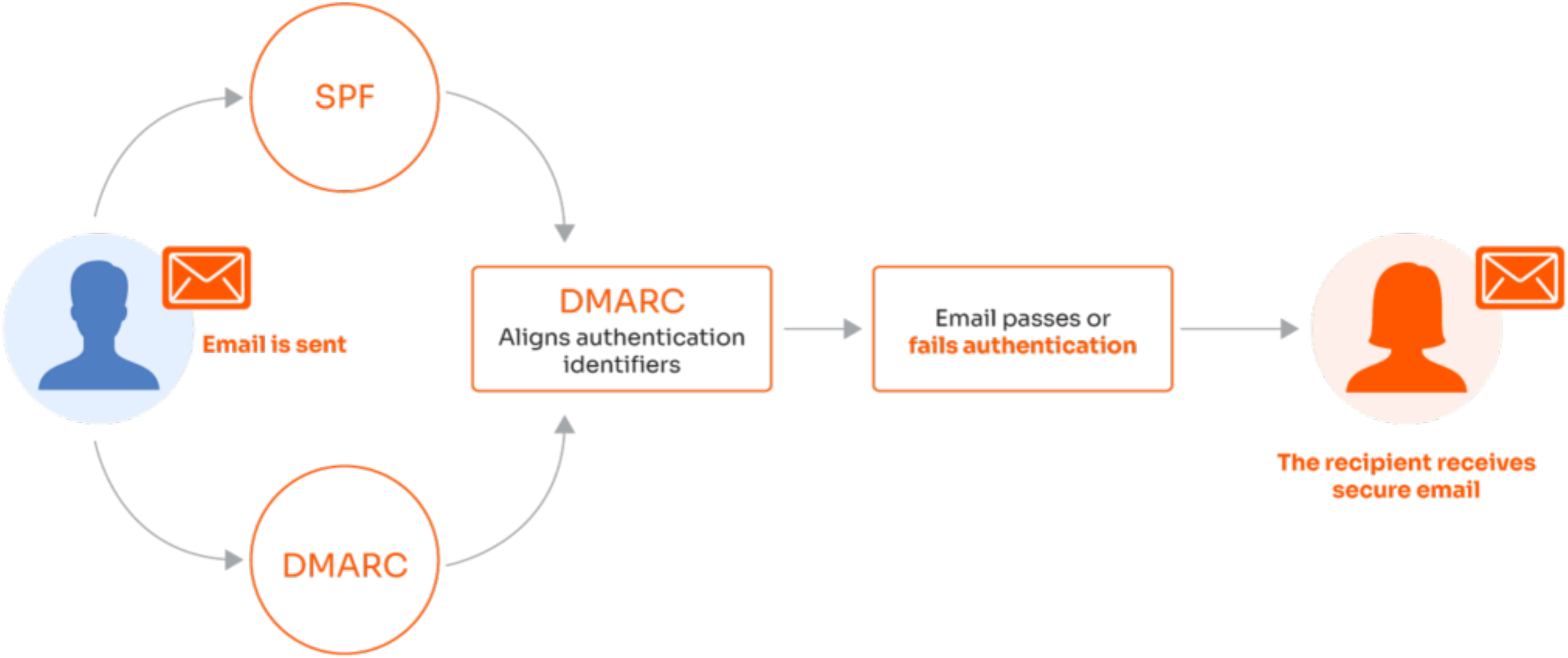
Authentication Method	Nov. 2013	Apr. 2015	Change
DKIM & SPF	74.66%	81.01%	+6.31%
DKIM only	2.25%	1.98%	−0.27%
SPF only	14.44%	11.41%	−2.99%
No authentication	8.65%	5.60%	−3.00%

Table 18: **Gmail Incoming Mail Authentication**—During April 2015, 94.40% of incoming Gmail messages were authenticated with DKIM, SPF, or both.

DMARC

- What should a mail server do if either SPF and/or DKIM fail for an email?
  - DMARC can specify a policy combining both.
  - A domain can publish a DNS TXT record indicating a policy for what to do with SPF/DKIM errors for emails from that domain.
    - Action: Reject, quarantine, accept the email
    - Reporting: Whether the error should be reported. If so, who to contact and what information to provide (automated process).
  - A receiving mail server that observes SPF/DKIM errors can consult the DMARC policy to determine how to respond, and who to report observed errors to.
    - Reporting helps the sending domain identify SPF/DKIM misconfigurations (or potential attacks spoofing that domain).

DMARC


SPF
Email is sent
DMARC
Aligns authentication identifiers
Email passes or
fails authentication
The recipient receives secure email
DMARC

DMARC

Published Policy	Gmail Messages	Top Million Domains
Quarantine	1.34%	709 (0.09%)
Empty	11.66%	6,461 (0.82%)
Reject	13.08%	1,720 (0.22%)
Not published	73.92%	783,851 (98.9%)

Table 22: **DMARC Policies**—We categorize DMARC policies for incoming Gmail messages from April 2015 and for Top Million domains with MX records on April 26, 2015.

- DMARC hasn't been as widely deployed yet, perhaps as DMARC came after SPF/DKIM and sites are hesitant to publish a meaningful policy that drops emails.
- Affects DKIM more than SPF (as SPF has a policy component)
- SPF/DKIM can still be used as signals/features even w/o DMARC

Other Email Security: Spam Filtering

- Many email providers deploy spam filters
  - Filter emails from blacklisted sources
  - Rate limit emails from a source
  - Use machine learning to detect likely spam emails
  - Cluster users/emails sending high volume of identical/similar emails

- Attackers can still often circumvent
  - Use botnets to avoid blacklists/rate limits
  - Change spam strategy to avoid ML detection/clustering

Other Email Security: Legal

- CAN-SPAM Act passed in 2003
  - Bans email harvesting, misleading header information, deceptive subject lines, use of proxies/spoofing
  - Requires opt-out and identification of ads
  - Imposes penalties

- FTC has brought a number of cases against violators.
  - Doesn't affect non-US spam though
  - Botnets and open relays/proxies make attribution hard

Other Email Security: Legal

FTC Announces First Can-Spam Act Cases

Two Operations Generated Nearly One Million Complaints to Agency

April 29, 2004

The FTC has cracked down on two spam operations that have clogged the Internet with millions of deceptive messages and violated federal laws. A complaint targeting Detroit-based Phoenix Avatar was developed in a joint investigation with the U.S. Attorney's Office in Detroit and the U.S. Postal Inspection Service. At the request of the FTC, a U.S. District Court judge has barred the illegal spamming and frozen the defendants' assets. Federal

FTC lawsuit reminds businesses: CAN-SPAM means CAN'T spam

By: Seena Gressin, Attorney, Division of Consumer and Business Education, FTC | August 14, 2023

Recent News

GMAIL

New Gmail protections for a safer, less spammy inbox

Oct 03, 2023
2 min read

Starting in 2024, we'll require bulk senders to authenticate their emails, allow for easy unsub under a reported spam threshold.

Neil Kumaran
Group Product Manager, Gmail Security & Trust

New requirements for bulk senders

By February 2024, Gmail will start to require that bulk senders:

1. **Authenticate their email:** You shouldn't need to worry about the intricacies of email security standards, but you should be able to confidently rely on an email's source. So we're requiring those who send significant volumes to strongly authenticate their emails following well-established best practices. Ultimately, this will close loopholes exploited by attackers that threaten everyone who uses email.

2. **Enable easy unsubscription:** You shouldn't have to jump through hoops to stop receiving unwanted messages from a particular email sender. It should take one click. So we're requiring that large senders give Gmail recipients the ability to unsubscribe from commercial email in one click, and that they process unsubscription requests within two days. We've built these requirements on open standards so that once senders implement them, everyone who uses email benefits.

3. **Ensure they're sending wanted email:** Nobody likes spam, and Gmail already includes many tools that keep unwanted messages out of your inbox. To add yet another protection, moving forward, we'll enforce a clear spam rate threshold that senders must stay under to ensure Gmail recipients aren't bombarded with unwanted messages. This is an industry first, and as a result, you should see even less spam in your inbox.

Email Security Summary

- Key email protocols: SMTP, IMAP, POP3
  - Hop-to-hop secure communication using TLS
  - End-to-end secure communication using PGP or S/MIME

- Email spoofing is a major problem
  - Leads to spam/phishing
  - Can use SPF, DKIM, and DMARC to defend