Secure Email Communication

Agenda

- Email protection
- Failing to defend from email spoofing?
- What are DMARC, SPF and DKIM?
- How do we configure this?
- Best Practices
- How it can be bypassed?

Email protection

- Email protection is a broad concept that comprises many techniques
- One branch of email protection is the set of methods used to stop unauthorized access or compromise of email security systems. This includes:
  - Login Security
  - Spam Filtering
  - User Security
  - Email Encryption
  - Employee Education

Email protection

- Email remains top security concern
- Ten common email security threats as for 2020
  - Spoofing and Phishing
  - Email Security Gaps
  - Domain Squatting
  - Client-Side Attacks
  - Malicious Files
  - Ransomware
  - Misconfigurations
  - Browser Exploit Kit
  - Spear-Phishing and Business Email Compromise (BEC) Attacks
  - File Format Exploits

Failing to defend from email spoofing

- Business email compromise (BEC) is the most expensive form of online fraud
- DMARC significantly reduces attackers' abilities to spoof targeted domains

Failing to defend from email spoofing

- While the use of DMARC is growing — less than 20% of companies use it in most industries.
- Majority of phishing emails leverage impersonation

Why do we need DMARC?

- DMARC prevents spammers or phishers from using valid organizations names for email fraud
- DMARC ensures that legitimate email is properly authenticating against established DKIM and SPF standards

SPF DKIM DMARC

SPF

- Sender Policy Framework

DKIM

- DomainKeys Identified Mail

DMARC

- Domain Message Authentication Reporting & Conformance

SPF

- A DNS record that lists your senders of email outbound to the internet
- Does not contain a policy on what you want the receiver to do if the email fails SPF
- Works by validating the IP of the “return-path” address. This is the SMTP envelope “from” address and not the “From:” address you see in the email (as emails have two from addresses!)
- SPF does not protect against “From:” header address spoofing

Example SPF DNS Records

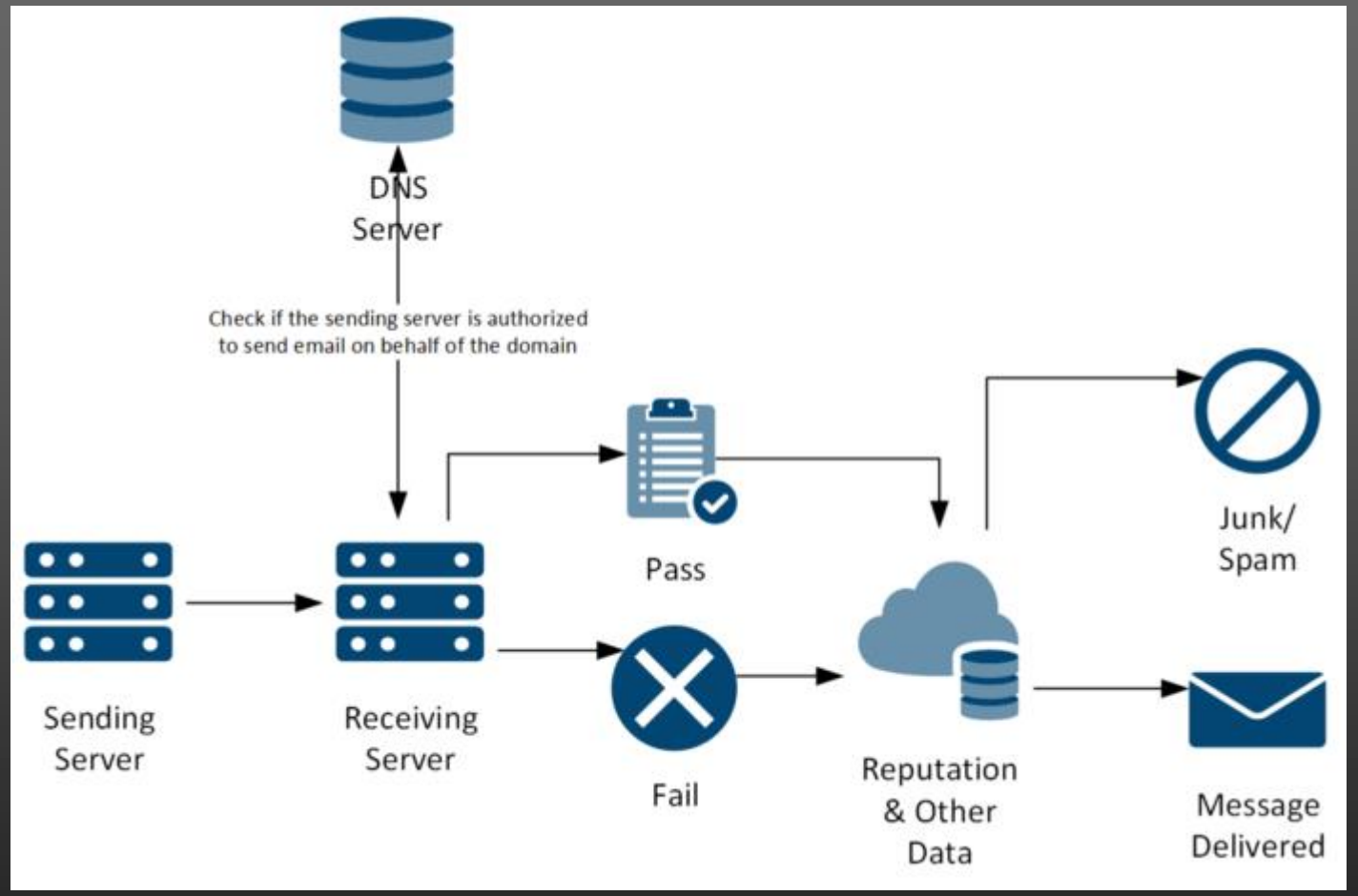
- v=spf1 mx ip4:17.15.21.14/32 ip4:17.15.21.18/32 ip4:17.15.20.23/32 include:spf.protection.outlook.com include:spf.mailer.net ~all

- v=spf1 ip4:1.2.5.5 ip4:8.2.7.4 ip4:7.3.2.2 ip4:5.5.1.8 include:_spf.salesforce.com include:spf.protection.outlook.com -all

- v=spf1 –all
- **+** (Pass)
  – (Fail)
  ~ (SoftFail)
  ? (Neutral)

- nslookup -type=txt google.com

SPF Flow


DNS
Server
Check if the sending server is authorized
to send email on behalf of the domain
Pass
Junk/
Spam
Sending
Server
Receiving
Server
Fail
Reputation
& Other
Data
Message
Delivered

DKIM

- Need a server or service that can add the encrypted header outbound and to optionally manage the keys and DNS records for you
- Email is sent in plain with encrypted hash of the original email body and some headers added as additional header to email
  - Note: Sending server can choose what data to include in encrypted header
- A DNS record that contains a public key is needed to allow receiving server to decrypt the DKIM-Signature email header on receipt and prove email legitimacy
  - The "selector" value allows you to have multiple public/private keys in use

Example DKIM DNS Records

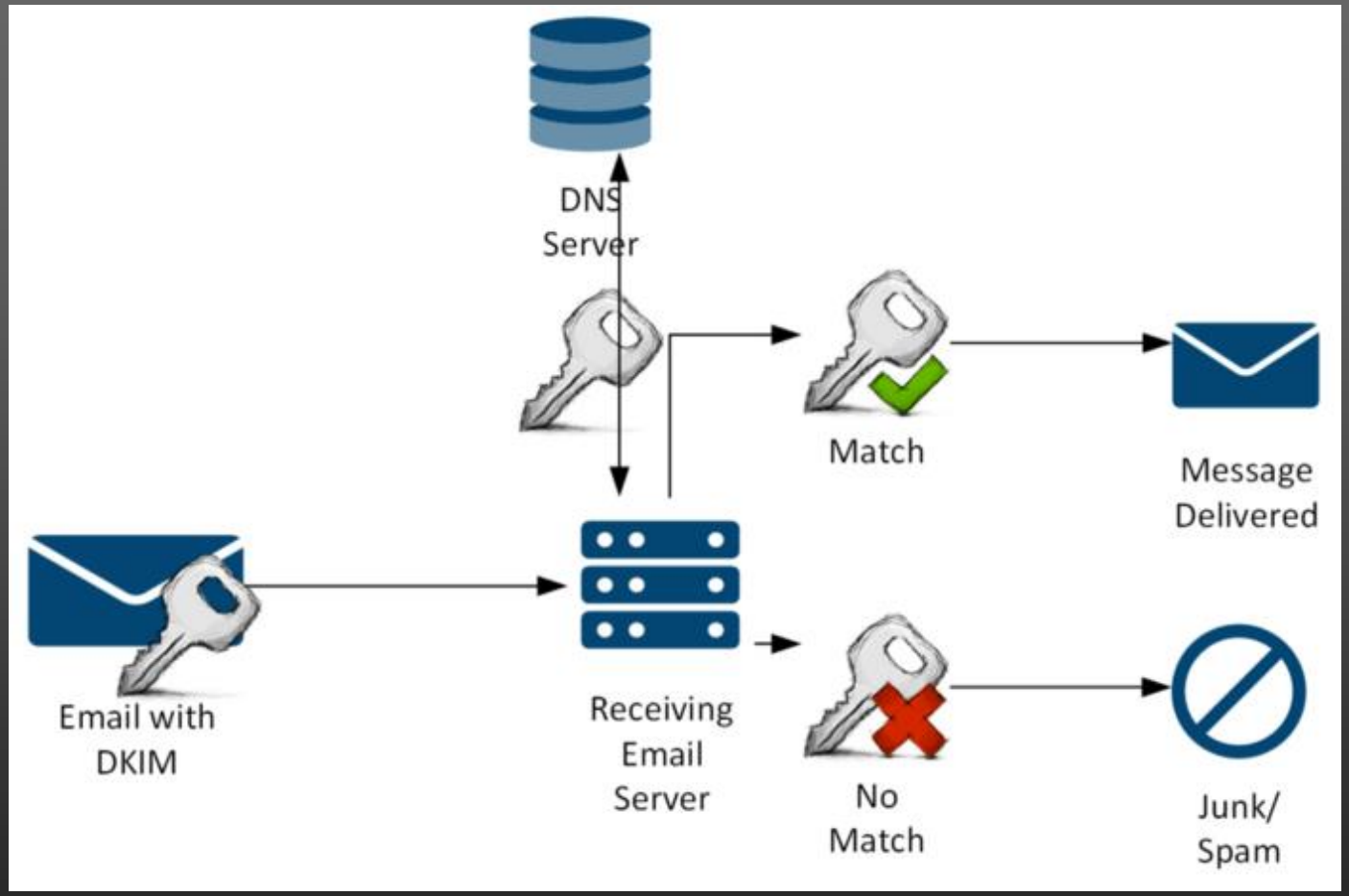
- Self managed DNS records, or pointers to other domain so someone else can manage the DNS and keys for you.
- TXT: Twitter: dkim._domainkey.twitter.com
- CNAME: selector1._domainkey.microsoft.com
  > selector1-*microsoft-com*._domainkey.*microsoft*.onmicrosoft.com
  > selector2-*microsoft-com*._domainkey.*microsoft*.onmicrosoft.com
- "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQ … QIDAQAB; n=1024,1435867505,1"

DKIM Headers In Email

- DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
- **d=**microsoft.com;
- **s=**selector1;
- **h=**From:Date:Subject:Message-ID:Content-Type:MIME-Version;
- **bh=**RReWBO26GDxuLUCUnsguWs8KWvyIL+vsEKOpAKkgoU4=;
- **b=**nUrVswRdttMonJci+GCY8KqSNr1g5MVxrY/MMbTrlmzD56TXYR2KfGWZgX43D+aF7cCTywJ6Y+DGy9OBYRqkryQBDO v2EjmiUD5B3JLkSANGUogWd+LP3shUi8h4eZmvfECJI+pzJiTWa1UQlG3Lr3f3wUo+SMINnDo/FLgNxac=

- X-DkimResult-Test: Passed

DKIM Flow


DNS
Server
Match
Message
Delivered
Email with
DKIM
Receiving
Email
Server
No
Match
Junk/
Spam

DMARC

- Allows you to get reports back on the effectiveness of your SPF and DKIM investments
- Validates that the “From” header is the same as the domains validated by SPF and DKIM
- Provides clear instructions to the receiving server on what to do with emails that fail SPF or DKIM
- Allows you to start simply and just report what your receivers are doing
- Allows you to control what receivers should do with your email that fails SPF or DKIM

Example DMARC

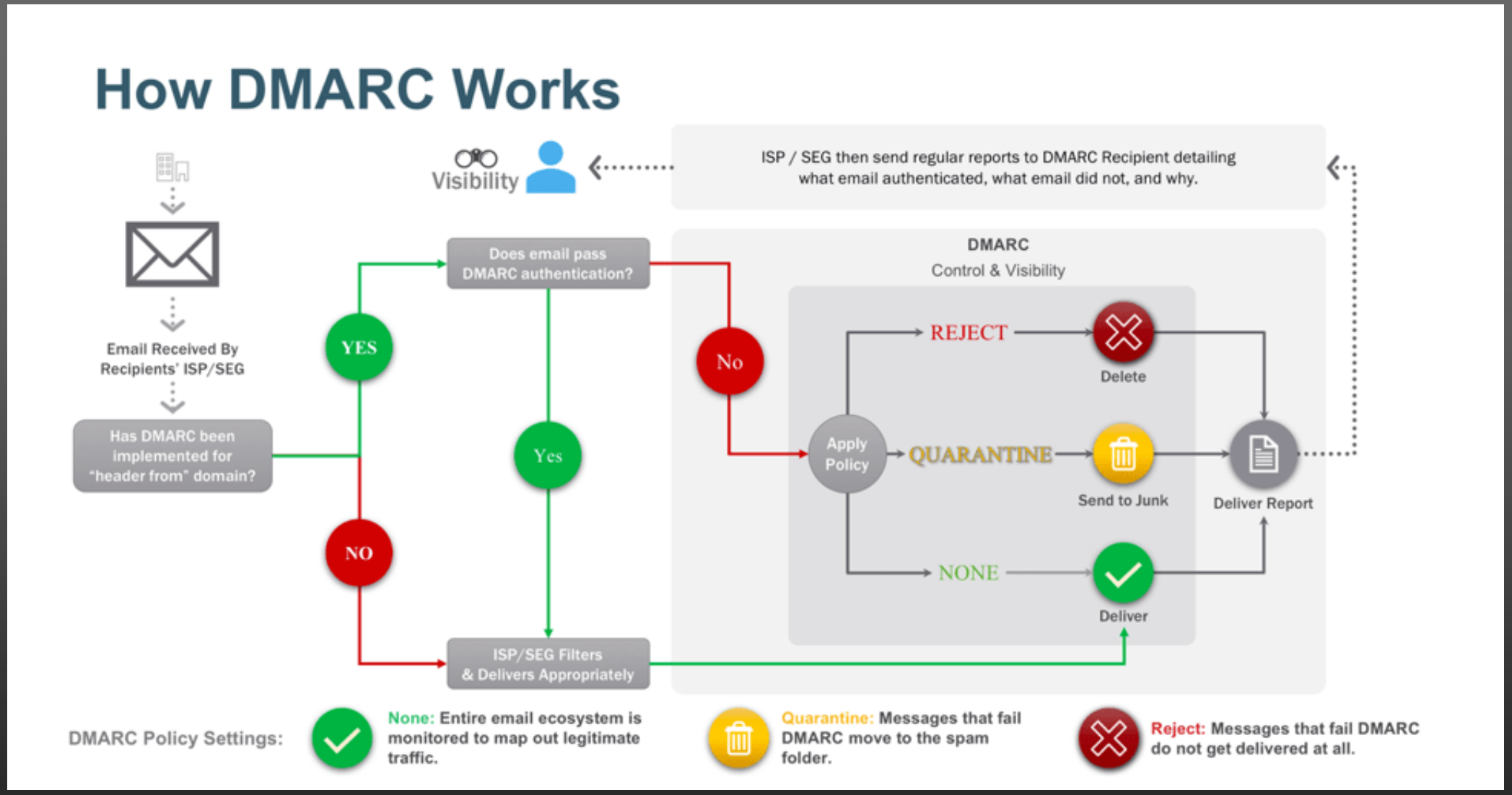
- Reporting Only
  - v=DMARC1; **p=none**;
- I'd like receiver to quarantine email authentication failures
  - v=DMARC1; **p=quarantine**;
- The receiver should reject SPF or DKIM failures
  - v=DMARC1; **p=reject**;

DMARC Reporting Attributes

- DMARC Version, which is case sensitive (v)
  - **v=DMARC1**; p=none; rua=mailto:dmarc@dmarc-aggregator.com; ruf=mailto:dmarc-ruf@dmarc-aggregator.com
- Daily analytics of passes and fails (rua)
  - v=DMARC1; p=none; **rua=mailto:dmarc@dmarc-aggregator.com**; ruf=mailto:dmarc-ruf@dmarc-aggregator.com
- Copies of failed emails (ruf)
  - v=DMARC1; p=none; rua=mailto:dmarc@dmarc-aggregator.com; **ruf=mailto:dmarc-ruf@dmarc-aggregator.com**

More DMARC DNS Attributes

- Treat Subdomains Differently
  - v=DMARC1; p=none; **sp=reject**; rua=mailto:dmarc@dmarc-aggregator.com; ruf=mailto:dmarc-ruf@dmarc-aggregator.com
- Receive reports on SPF and/or DKIM failure and not only on both
  - v=DMARC1; p=quarantine; rua=mailto:dmarc@dmarc-aggregator.com; ruf=mailto:dmarc-ruf@dmarc-aggregator.com; **fo=1**
- Defines a percentage of email that DMARC applies to
  - v=DMARC1; p=reject; rua=mailto:dmarc@dmarc-aggregator.com; ruf=mailto:dmarc-ruf@dmarc-aggregator.com; **pct=5**



DMARC Flow
Source: Proofpoint.com

Approach for DMARC implementation

Domain identification

- Identify all cust. domains
- Identify the key domains from cust. risk perspective
- Seek confirmation from all business units on outsourced email arrangements

DMARC implementation

- Move to DMARC monitoring mode
- Ensure DMARC record is implemented for all mail servers sending emails for the domain
- Move to DMARC quarantine/block mode

Integration with monitoring controls

- Integrate DMARC data feeds with anti-phishing process
- Integrate DMARC data feeds with Fraud Management System/SIEM

DMARC Check Tools

- https://www.spfwizard.net/
- https://mxtoolbox.com/spf.aspx
- https://dmarcian.com/dmarc-inspector/
- https://mxtoolbox.com/dmarc.aspx
- https://www.dmarcanalyzer.com/dmarc/dmarc-record-check/
- https://dmarcly.com/tools/dmarc-checker
- DMARC Reports Parser https://github.com/techsneeze/dmarcts-report-parser

DMARC Aggregators

- Companies that take the analytics and forensic data and allow you to review and determine trends and issues
- Examples include Agari, Dmarcian, DMARCAnalyzer, Return Path and others

Best Practices

- Start with DMARC to policy None then move to Quarantine
- Set DMARC p=reject as maturity grows
- Use only one DKIM key pair if possible
- Monitor reports periodically to make sure you aren't blocking legitimate emails (How many blocked? How many passed?)

Common Misconfigurations

- Bad IP Addresses
- Missing Records
- Old not updated key pairs
- Missed domains
- Misconfigured/None policies

DMARC Bypass

- DMARC can be bypassed with usage of public email cloud hosting as Office 365, Google Workspace or valid compromised domain
- Phishing campaigns successfully register domains alongside DMARC
- Why use it then? To cut the noise and acquire more information

Q&A