Computer Security List 3

Bartosz Michalak

14 April 2024

1 Task 1

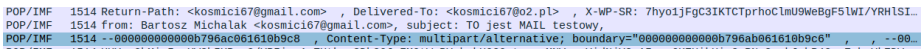


Figure 1: First mail

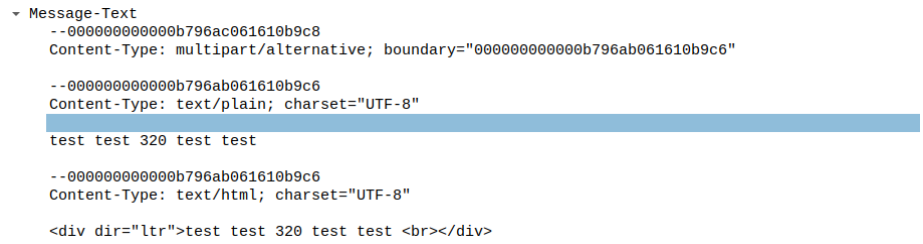


Figure 2: First mail contents

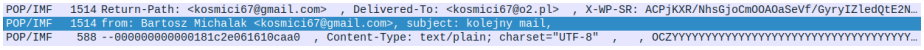


Figure 3: Second mail

1.6: We see information about who send it, what was the title and what were the contents.
1.7: Yes, but not in "pure form". You either need to use SMTPS (older, less safe) or STARTTLS option in SMTP to send messages safely.
1.8: No, SSL and TLS secure data during transfer time but at sender's and receiver's ends data can be obtained by 3-rd party users (for e.g. E-Mail service provider).
1.9: For vulnerabilities described in 1.8 we may use end-to-end encryption(E2EE) such as PGP (Pretty Good Privacy) or S/MIME (Secure/Multipurpose Internet Mail Extensions).
1.10: It uses E2EE and "zero-access encryption" which means that Emails

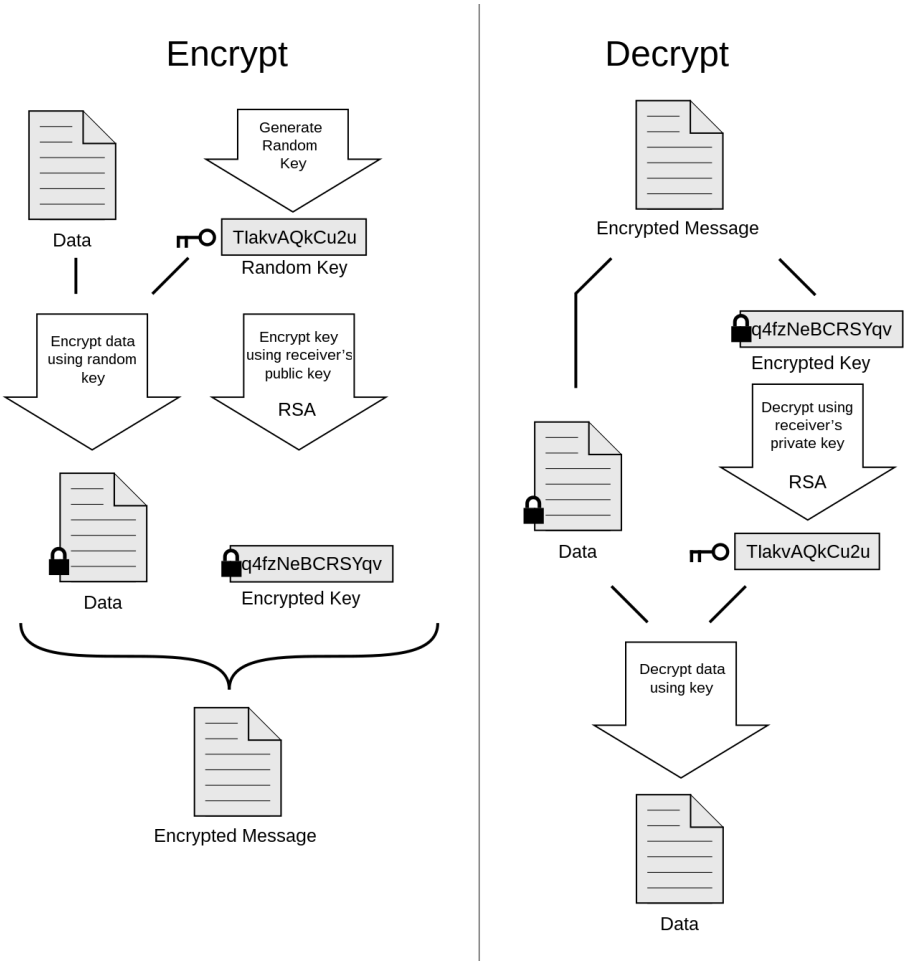


Figure 4: Remainder how PGP works

from other providers are automatically encrypted using your public key. Proton also offers 2FA and "Enhanced tracking protection" which basically states that don't allow other companies to track your data/activities by hiding your IP address and blocking tracking pixels.

2 Task 2

1. SPF (Sender Policy Framework): SPF is an email authentication method used to detect forged sender addresses during the email delivery process. It allows the domain owner to specify which servers are authorized to send

emails on behalf of their domain. Email receivers can check SPF records to verify the authenticity of incoming emails.

2. DKIM (DomainKeys Identified Mail): DKIM is another email authentication method that allows an organization to take responsibility for a message in a way that can be verified by the recipient. It involves signing outgoing emails with a cryptographic signature, which is stored in DNS. The recipient's email server can then use the public key from DNS to verify the signature and ensure the message has not been tampered with.

3. DMARC (Domain-based Message Authentication, Reporting, and Conformance): DMARC builds on SPF and DKIM to provide email domain owners with control over how their emails are handled if they fail SPF or DKIM checks. It allows domain owners to specify policies for how email servers should handle emails that fail authentication checks, such as quarantine or reject. DMARC also provides reporting capabilities to help domain owners monitor email authentication activity.

Figure 5: Spf in wireshark

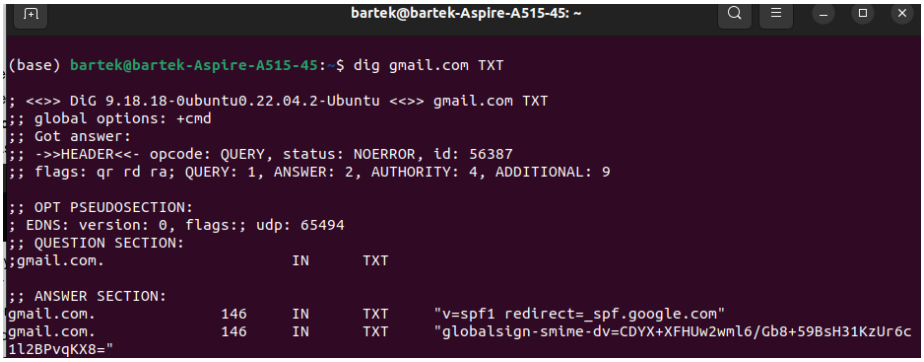


Figure 6: Spf in dig

DKIM usually signs header but it may also sign body of email.

```
        for <kosmici67@o2.pl>; Mon, 15 Apr 2024 01:08:36 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20230601; t=1713168516; x=1713773316; darn=o2.pl;
        h=content-transfer-encoding:subject:from:to:content-language
         :user-agent:mime-version:date:message-id:from:to:cc:subject:date
         :message-id:reply-to;
        bh=eS/OMKDj0inzPO4drRczZhSaGOP+/Hbw5ptwcFUPB3Q=;
        b=iq+jrLPCCCdvc8hfwD30VleggsM5v2ExP0KCBonudHUr3fiepb04ppV6nRBsSsdQ3h
         5mVMEBPvFhcs5bxA+iQLi9EriChF7lI/4Zz4PvkWVmvRSQ0WtcAu4cxZBJFj6psJ8W35
         a/i2eC1GHS1H9XEWf/GVDGpvfCii64ZHLBxxmywfRC5Erz4KSrN+ZxR/KEODZC4iearv
         /r//2Aq3eMrPjefQdyv8HLAFW86hjZbqgT2TQMVWp92n/sA9zopFD3s7mZJMhCryWTvj
         yVFCvX76EBlQmZfTH74GdNgV4CBl0iqaT/QnZsCanmSgS8Yxq4D++jclaXnf/vrtMF79
         vEAw==
X-Google-DKIM-Signature: v=1;
```

Figure 7: DKIM in wireshark

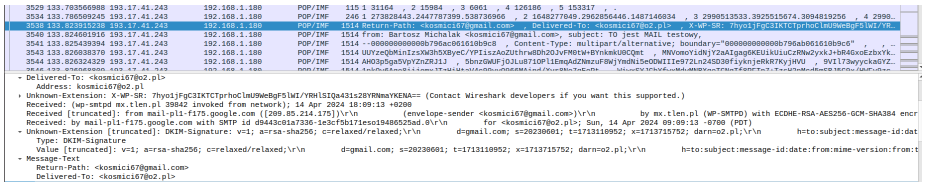


Figure 8: DKIM signature in wireshark

Dmarc policies:

1. none - no action taken after failing spf or dkim,

2. quaratine - sent to spam folder or marked as suspicious after failing spf or dkim,

3. reject - message is not even delivered to mailbox after failing spf or dkim.

It is possible that mail passes spf,dkim and dmarc while containing ill-natured link and being put in spam folder.

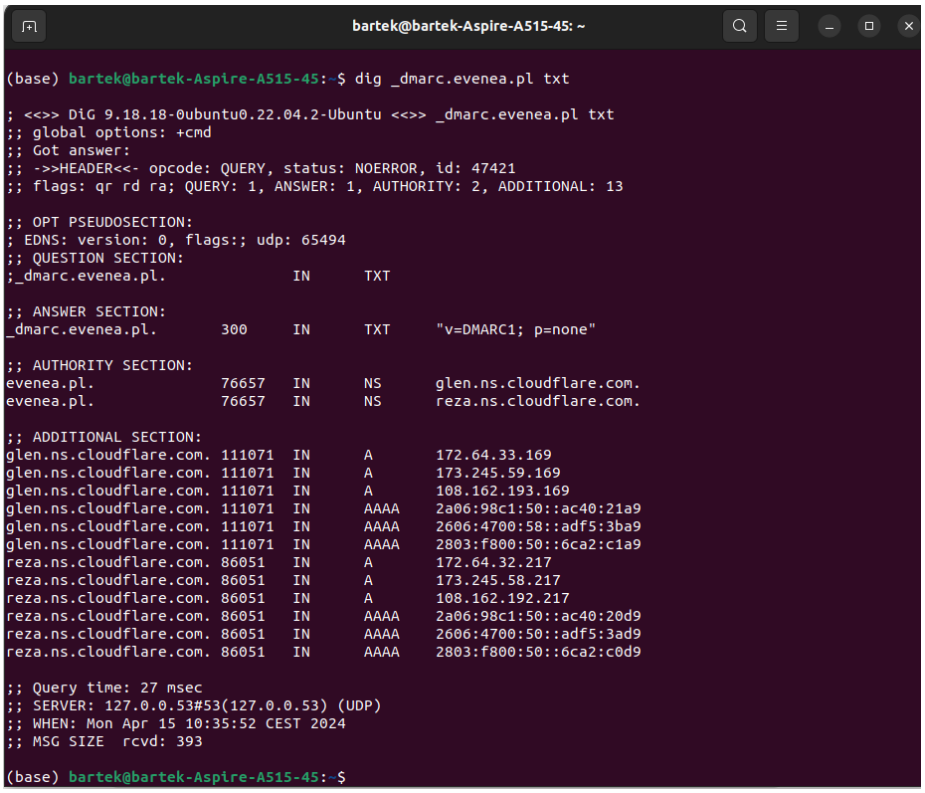


Figure 9: DmarcPolicy

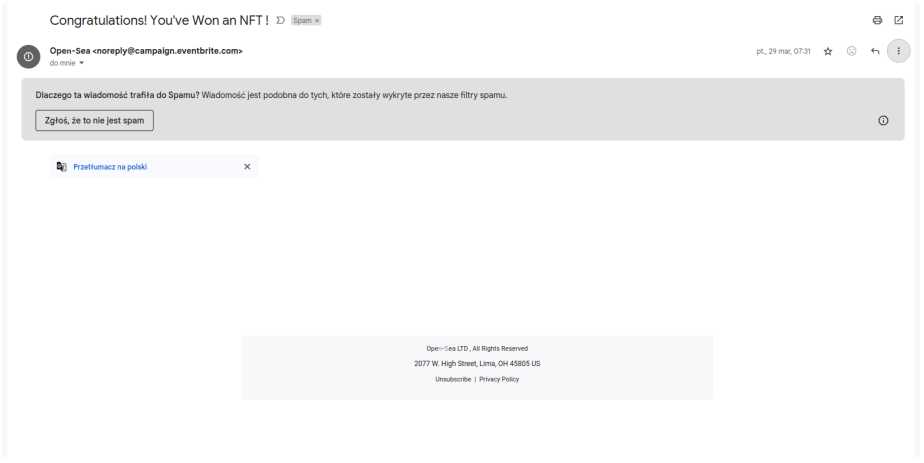
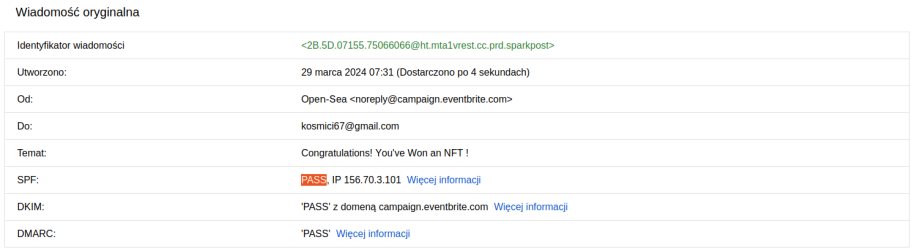


Figure 10: Fake Email



Wiadomość oryginalna

Identyfikator wiadomości	<2B.5D.07155.75066066@ht.mta1vrest.cc.prd.sparkpost>
Utworzono:	29 marca 2024 07:31 (Dostarczono po 4 sekundach)
Od:	Open-Sea <noreply@campaign.eventbrite.com>
Do:	kosmici67@gmail.com
Temat:	Congratulations! You've Won an NFT !
SPF:	PASS, IP 156.70.3.101 Więcej informacji
DKIM:	'PASS' z domeną campaign.eventbrite.com Więcej informacji
DMARC:	'PASS' Więcej informacji

Figure 11: Fake Email dmarc spf and dkim