Computer Security List 3

Bartosz Michalak

14 April 2024

1 Task 1

POP/IMF 1514 Return-Path: <kosmici67@gmail.com> , Delivered-To: <kosmici67@o2.pl> , X-WP-SR: 7hyo1jFgC3IKTCTprhoclmU9weBgF5lWI/YRHISI.
POP/IMF 1514 from: Bartosz Michalak <kosmici67@mail.comp, subject: TO jest Mall testowy,
POP/IMF 1514 -080080090809786380615108082 , Content-Type: multipar/Alternative; boundary="08080809090909796ab0616108066" , , --08.

Figure 1: First mail

```
Message-Text
--0000000000b796ac061610b9c8
Content-Type: multipart/alternative; boundary="00000000000b796ab061610b9c6"
--00000000000b796ab061610b9c6
Content-Type: text/plain; charset="UTF-8"

test test 320 test test
--00000000000b796ab061610b9c6
Content-Type: text/html; charset="UTF-8"

<div dir="ltr">text/html; charset="UTF-8"
```

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

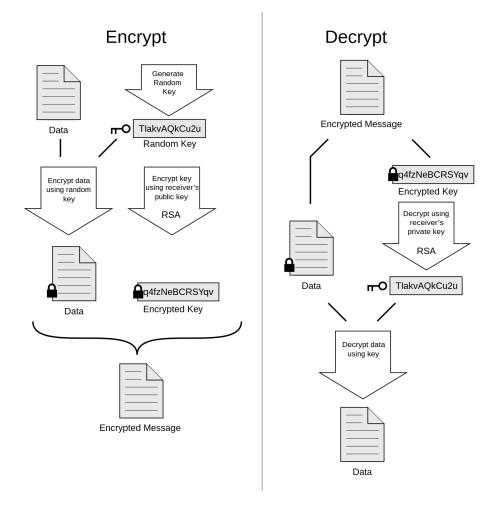


Figure 4: Remainder how PGP works

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.

```
179 0 19-19700000 109-17-41-23 10-192-17-70 POP/TWF 409 1-77320449 - 247777799 - 207720049 - 24777799 - 207720049 - 24777799 - 207720049 - 24777799 - 207720049 - 24777799 - 207720049 - 24777799 - 207720049 - 24777799 - 207720049 - 24777799 - 207720049 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 2477799 - 24
```

Figure 5: Spf in wireshark

Figure 6: Spf in dig

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

```
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/OMKDj@inzPO4drRczZhSaGOP+/Hbw5ptwcFUPB3Q=;
b=iq+jrLPCCCdvc8hfwD3@VleggsM5v2ExP@KCBonudHUr3fiepb@4ppV6nRBsSsdQ3h
5mVMEBPvFhcs5bxA+iQLi9EriChF7II/4Zz4PvkWVmvRSQ@WtcAu4cxZBJFj6psJ8W35
a/i2eC1GHS1H9XEWf/GVDGpvfCii64ZHLBxxmywfRc5Erz4KSrN+ZxR/KEODZC4iearv
/r//2Aq3eMrPjefQdyv8HLAFW86hjZbqgT2TQMVWp92n/sA9zopFD3s7mZJMhCryWTvj
yVFCvX76EBlQmZfTH74GdNgV4CBl@iqaT/QnZsCanmSgS8Yxq4D++jclaXnf/vrtMF79
vEAw==
X-Google-DKIM-Signature: v=1;
```

Figure 7: DKIM in wireshark

3529 133.	03566988 193.17.41.243	192.168.1.189	POP/IMF	115 1 31164 , 2 15984 , 3 6961 , 4 126186 , 5 153317 , .		
3534 133.	86509245 193.17.41.243	192.168.1.189	POP/IMF	246 1 273828443.2447787399.538736966 , 2 1648277649.2962856446.1487146034 , 3 2990513533.3925515674.3094819256 , 4 2990		
3538 133.	323915238 193.17.41.243	192.168.1.180	POP/IMF	1514 Return-Path: <kosmici67@gmail.com> , Delivered-To: <kosmici67@o2.pl> , X-WP-SR: 7hyo1jFgC3IKTCTprhoClmU9WeBgF5lWI/YR</kosmici67@o2.pl></kosmici67@gmail.com>		
3549 133.1	324691916 193.17.41.243	192.168.1.189	POP/IMF	1514 from: Bartosz Michalak <kosmici67@gmail.com>, subject: TO jest MAIL testowy,</kosmici67@gmail.com>		
3541 133.0	325439394 193.17.41.243	192.168.1.189	POP/IMF	15149808080808080796ac061610b9c8 , Content-Type: multipart/alternative; boundary="000808080808080796ab061610b9c6" , ,		
	326938379 193.17.41.243	192.168.1.180	POP/IMF	1514 UUYzeQbMinIzsXW3h5XByeC/YPIiszAoZUthrw8Dh2OJvFN0tW+BYnkmkU0CQmt , NNVomoYidNjY2aAIgag6KEUikUiuCzRNw2yxkJ+bR4GxoEzbxYk		
	326324329 193.17.41.243	192.168.1.189	POP/INF	1514 AHO3p5ga5VpYZnZRJ1J , 5bnzGWUFjOJLu871OPl1EmqAdZNmzuF8WjYmdNi5eODWIIIe972Ln24SD30fiyknjeRkR7KyjHVU , 9VIl73wyyckaGYZ		
	776060000 407 47 A4 7A7	107 160 1 100	DOD/TMF	ARAA Anbhurkannol i innu 17-00 UbayAnobanborkMaind /YuroNinThenbb blivney tekyfuvMdiMNDYnnTeMnTfoDetn7 : TanU3nMndkneo trecu /Ubburann 1		
- Delivered-To: <kosmici67@02.pl></kosmici67@02.pl>						
Address: kosmici67@o2.pl						
> Unknown-Extension: X-WP-SR: 7hyoijFgC3IKTCTprhoClmU9WeBgF5lWI/YRHlSIQa431s2BYRNmaYKENA== (Contact Wireshark developers if you want this supported.)						
Received: (wp-smtpd mx.tlen.pl 39842 invoked from network); 14 Apr 2024 18:09:13 +0200						
Received [truncated]: from mail-pl1-f175.google.com ([289.85.214.175])\r\n (envelope-sender <kosmici67@gmail.com>)\r\n by mx.tlen.pl (WP-SMTPD) with ECDHE-RSA-AES256-GCM-SHA384 encr</kosmici67@gmail.com>						
Received: by mail-pl1-f175.google.com with SMTP id d9443c81a7336-1e3cf5b171eso19486525ad.0\r\n for <kosmici67@02.pl>; Sun, 14 Apr 2024 09:09:13 -0700 (PDT)</kosmici67@02.pl>						
- Unknown-Extension [truncated]: DKIM-Signature: v=1: a=rsa-sha256: c=relaxed/relaxed:\r\n d=gmail.com: s=28238681: t=1713118952: x=1713715752: darn=02.0l:\r\n h=to:subject:message=id:dat						
Type: DKIM-Signature						
Value [truncated]: v=1; a=rsa-sha256; c=relaxed/relaxed;\r\n d=gmail.com; s=28238681; t=1713118952; x=1713715752; darn=02.pl;\r\n h=to:subject:message-id:date:from:mime-version:from:t						
- Message-Text						
Return-Path: <kosmici67@gmail.com></kosmici67@gmail.com>						
Deliver	Delivered-To: <kosmici67@o2.pl></kosmici67@o2.pl>					

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.

```
bartek@bartek-Aspire-A515-45: ~
                                                                                                                                                                                                              Q =
 (base) bartek@bartek-Aspire-A515-45:~$ dig _dmarc.evenea.pl txt
  ; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> _dmarc.evenea.pl txt
;; global options: +cmd
;; Got answer:
;; Got answer:
;; ->>HEADER<<-- opcode: QUERY, status: NOERROR, id: 47421
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 13
   ; OPT PSEUDOSECTION:
EDNS: version: 0, flags:; udp: 65494
; QUESTION SECTION:
     _dmarc.evenea.pl.
                                                                                TN
 ;; ANSWER SECTION: _dmarc.evenea.pl.
                                                            300
                                                                                                                          "v=DMARC1; p=none"
 ;; AUTHORITY SECTION:
                                                            76657
76657
                                                                                IN
IN
                                                                                                    NS
NS
                                                                                                                          glen.ns.cloudflare.com.
reza.ns.cloudflare.com.
 evenea.pl.
;; ADDITIONAL SECTION:
glen.ns.cloudflare.com. 111071
glen.ns.cloudflare.com. 111071
glen.ns.cloudflare.com. 111071
                                                                                                                           172.64.33.169
                                                                                                                         173.245.59.169
108.162.193.169
2a06:98c1:50::ac40:21a9
2606:4700:58::adf5:3ba9
                                                                                                     A
A
AAAA
AAAA
glen.ns.cloudflare.com. 111071
glen.ns.cloudflare.com. 111071
glen.ns.cloudflare.com. 111071
glen.ns.cloudflare.com. 86051
reza.ns.cloudflare.com. 86051
                                                                                 IN
IN
                                                                                                                         2606:4700:58::adf5:3ba9

2803:f800:50::6ca2:c1a9

172.64.32.217

173.245.58.217

108.162.192.217

2806:98c1:50::ac40:20d9

2606:4700:50::adf5:3ad9

2803:f800:50::6ca2:c0d9
                                                                                                      AAAA
 reza.ns.cloudflare.com. 80651
reza.ns.cloudflare.com. 86651
reza.ns.cloudflare.com. 86651
reza.ns.cloudflare.com. 86651
reza.ns.cloudflare.com. 86651
                                                                                 IN
IN
IN
IN
                                                                                                     A
AAAA
AAAA
   ; Query time: 27 msec
; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
; WHEN: Mon Apr 15 10:35:52 CEST 2024
; MSG SIZE rcvd: 393
 (base) bartek@bartek-Aspire-A515-45:~$
```

Figure 9: DmarcPolicy

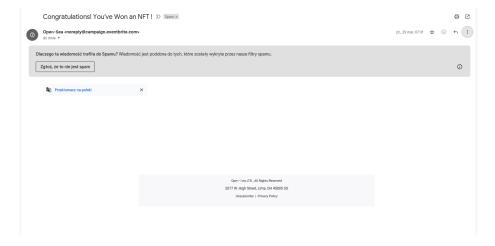


Figure 10: Fake Email

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></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