CSE508 Network Security

4/13/2016 Spam and Phishing

Michalis Polychronakis

Stony Brook University
I don’t like SPAM!
Spam Sources

Commercial entities
   Legitimate or “gray” businesses, advertisers, …

Spammers’ own hosts or open relays ➔ easily blocked

Botnets
   Abuse of ISPs and webmail providers
   Abuse of legitimate user email accounts
   Address harvesting from users’ address books

Not an email-only issue
   Facebook, Twitter, Yelp, Amazon, online comments, forum messages, …
   Beyond simple messages: “likes,” “clicks,” fake reviews, …
Spam lifecycle

Gathering addresses
  Valid, active addresses are precious
  Stolen address books, web crawling, black market, …

Message content
  Advertising, 419 scams, fraud, phishing, malware, …
  Anti-spam filter evasion: content obfuscation

Spam email delivery
  Valid accounts: newly created (sweatshops), hijacked ones, …
  Open relays/proxies (not common anymore)
  Malware: most spam comes from infected machines/botnets
Email Address Protection

Keep it safe from address harvesting

Munging: username [at] example.com

Image instead of text

CAPTCHAs
Fighting Spam

Content-based filtering
- False positives vs. false negatives
- Local vs. cloud-based

Blacklisting
- IPs/domains of known spammers, open relays, zombie machines, hosts that shouldn’t be sending emails (e.g., ISP DHCP pools), ...

Honeypots
- Relays, proxies, spamtraps (fake email addresses)

Outbound filtering (block port 25)
- SMTP authentication is now mandatory by most ISPs

Email authentication
Content-based Filtering

Machine learning
  Training with labeled “spam” and “ham” messages
  Feedback from user activities (e.g., “not spam” button)

Rule-based systems
  Signatures, regular expressions, patterns, …
  Certain keywords, phrases, unusual text, …
  Example: SpamAssassin

Spam authors try to evade filters
  V1agra, Via'gra, Vi@gra, vi*gra, Viagra
  Intentional spelling mistakes, symbols, weird punctuation, …
  Continuous arms race - example: attackers started using images, defenders started using OCR, …
False positives are a challenging problem

Please do not reply to this email as this email address is not monitored. To ensure delivery to your inbox (not bulk or junk folder), please add noreply@timewarnercable.com to your address book.

For additional information please review our most Frequently Asked Questions at any time.

©2013-2014 Time Warner Cable, Inc. All rights reserved. Time Warner Cable and the Time Warner Cable logo are trademarks of Time Warner, Inc. used under license.

This information is confidential and intended only for the use of the account owner it is addressed to. If you are not the account owner, then you have received this message in error and any review, dissemination, copying, or unauthorized use of this message is strictly prohibited and you should delete this message. Please do not reply to this e-mail.

Please add ConEdCustomerService.com to your address list to ensure future delivery of notifications.

Privacy Policy: This e-mail was sent by Con Edison of New York. To view our privacy policy, please click here.

© 2014 Con Edison
Con Edison - 4 Irving Place - New York, NY 10003 - 1-800-75-CONED

Important program update from MileagePlus.

To ensure delivery to your inbox, please add MileagePlus@news.united.com to your address book.
DNSBL Filtering

DNS Block List: IP addresses, domain names, and other information compiled as a DNS zone

DNS-based: easy to query, light on bandwidth/resources
False positives, IP addresses change hands, ...
SPF: Origin Authentication

SMTP allows anyone to send an email with an arbitrary “From” address

Sender Policy Framework

DNS TXT record with hosts that are allowed to send email from the domain
Receiving SMTP servers compare the IP address that attempts to send an email with the allowed addresses of the domain(s) provided in the HELO and MAIL FROM commands
Helps to block spam at it source

mikepo@styx:~> dig google.com TXT
;; ANSWER SECTION:
google.com. 3600 IN TXT "v=spf1 include:_spf.google.com ip4:216.73.93.70/31 ip4:216.73.93.72/31 ~all"
DKIM: Email Validation

DomainKeys Identified Mail: *digitally sign* some email headers and message body

Allowsthe recipient to verify that
  The message is sent from the domain it claims to be sent from
  The message has not been tampered with

Domain’s public key is stored in a DNS TXT record

```
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=1e100.net; s=20130820; h=x-gm-message-state:mime-version:date:message-
   id:subject:from:to :content-type;
bh=0BSnrwLTQ7KblIwINxoPJN40a/K5PZCIV8atl6a1Dvg=;
b=Nch9yEorgibAjkh90ukDL6SU0FYn70qP6AMsWFfpLO+W3iroMoVdKIjKk8Cv6Gc1TW ...
```

```
mikepo@styx:~> dig 20130820._domainkey.1e100.net TXT
  ;; ANSWER SECTION:
  20130820._domainkey.1e100.net. 86400 IN TXT "k=rsa\;
p=MIIBIjANBgkqhkiG9w0BAQEFAOAQ8AMIIBCgKCAQEAnOv6+Txyz+SEc7mT719QQt0j6g
  2MjpErYUGVrRGGc7f5rmE1cRP1lhwx8PV0HoiuRzyok7IqjvAub9kk9fBoE9u ...
```
**SPF + DKIM = DMARC**

Domain-based Message Authentication, Reporting & Conformance (DMARC)

Standardizes how email receivers perform email authentication using SPF and DKIM

Tells receivers what to do if neither of those authentication methods passes – such as junk or reject the message

DMARC policies are published as DNS TXT records

mikepo@styx:~> dig _dmarc.google.com TXT
;; ANSWER SECTION:
_dmarc.google.com. 600 IN TXT "v=DMARC1; p=quarantine; rua=mailto:mailauth-reports@google.com"
DMARC Email Authentication Process

1. Author Composes & Sends Email
2. Sending Mail Server Inserts DKIM Header
3. Email Sent to Receiver

Sender

Validate and Apply Sender DMARC Policy

Retrieve Verified DKIM Domains
Retrieve “Envelope From” via SPF
Apply Appropriate DMARC Policy

Receiver

Standard Validation Tests

IP Blocklists, Reputation, Rate Limits, etc.

Standard Processing

Anti-Spam Filters, etc.

Passed

Quarantine

Failure Report sent to Sender

Update the periodic Aggregate Report to be sent to Sender

http://dmarc.org/overview/
TorrentLocker spam has DMARC enabled

Use of email authentication technique unlikely to bring any advantage.

Last week, Trend Micro researcher Jon Oliver (who presented a paper on Twitter abuse at VB2014) wrote an interesting blog post about a spam campaign that was spreading the 'TorrentLocker' ransomware and which, unusually, was using DMARC.

TorrentLocker is one of the most prominent families of encryption ransomware — a worryingly successful kind of malware that first appeared two years ago. The malware initially implemented its cryptography rather poorly, but has since become one of the most successful of its kind.

DMARC is an email technology that builds on both SPF and DKIM. Both these technologies allow a domain owner to take some responsibility for the emails sent from their domain: SPF by listing those IP addresses used to send email; DKIM by digitally signing the emails.

DMARC adds to SPF and DKIM a mechanism that allows a domain owner to advise senders what to do about the emails, and to send copies of the email to another domain for analysis.
**SPF, DKIM, DMARC**

SPF validates MAIL FROM vs. its source server
   “Envelope” information

DKIM validates the “From:” message header
   Plus other message headers and the message body

Not effective against spammers who
   Use their own domains
   Use legitimate email services, such as webmail
   Pretend to be another user on the same domain

Good for whitelisting and verifying email from trusted sources (.gov, banks, …)

*Besides spam, we also care about phishing…*
Phishing

Spoofed emails pointing to spoofed webpages

Financial institutions, could services, and other targets

Asking for credentials, credit card numbers, and other sensitive information

“Your Fedex package information”
“Your account has been suspended”
“Your credit card statement”

Spear phishing

*Enticing* messages that appear to come from well-known individuals or businesses
**Address Obfuscation**

**Misspelled/similar domain names**

*From: info@paypa1.com*  
http://www.citybank.com

**Misleading <A> tags**


**Seemingly legitimate/complex/long URLs**

http://www.bankofamerica.com.attacker.net/
http://www.visa.com:UserSession=2f6q988316484495&usersoption=SecurityUpdate&From@61.252.126.191/verified_by_visa.html

**Homographs, internationalized domain names (IDN), punycode**


Most browsers display IDNs only for the system’s configured language
Punycode if a non-default language or mixed languages are used

**Dot-less addresses and other URL encoding tricks**

www.cs.stonybrook.edu ➔ http://130.245.27.2 ➔ http://2197101314

**URL shorteners and redirection chains**

Hide the actual destination URL
Recent phishing message targeting SBU users

From: SBU Team <ebrahle2@kent.edu>
Date: Tue, Feb 2, 2016 at 8:42 PM
Subject: cyber security
To: XXXXXXXXXXXX

We've detected spam-like activity in your webmail account, which is against our Acceptable Use Policy (AUP).

Kindly click on the link below to verify that you're the owner of the account and not a spammer.

http://is.gd/stonybrooksecure

We apologize for any inconvenience this may have cause you.

Thanks,
SBU Team
Legitimate message from an IT department

From: XXXXXXXXXX
Date: XXXXXXXXXX
Subject: Important! You must change your XXXXXXXX password
To: XXXXXXXXXX

[This is not a spam mail, this email is from me, XXXXXXXXXX]

Member of XXXXXXXXXX Department,

PLEASE CHANGE YOUR XXXXXXXX PASSWORD!

We just upgraded the security of XXXXXXXX. Your current password is no longer working. You must change your password if you want to log into XXXXXXXX. [...] 

To change your XXXXXXX password: http://xxxxxxxxxxxx.xxx -> forgot your password -> follow the instructions
More training of users to click on things...
Phishing Countermeasures

Stop confusing users
  Institutions shouldn’t include links in emails

User education
  Don’t trust links in emails – type the address in your browser
  (analogous to: don’t trust phone calls that ask for your info – always call the number at the back of your card)

Augmenting password logins
  Two-step login: show user-specific information before prompting for the password
  Probably too inconvenient

Anti-phishing filters, tools, …
Spear Phishing

Well-prepared, personalized, convincing messages targeted to particular individuals

Seemingly coming from trusted colleagues
Personalized for their target: real names, personal and business information, recent activity (e.g., real purchases), …

Highly effective, used extensively in targeted attacks
Document attachments exploiting 0day vulnerabilities

Many recent incidents
Maybe rethink email altogether?

Recent secure messaging apps offer many benefits

True end-to-end encryption: the provider shouldn’t be able to read message contents

User-friendly verification of contacts’ identities

Forward security: ensure past communications will be secure even if private keys are stolen

Open-source design and implementation, code audits

No spam! Only approved contacts can send messages

Many encouraging efforts

OTR, Signal, Pond, …

Proprietary, but better than nothing: WhatsApp, iMessage

Metadata is still there!
Is there an option to disable NSA/PRISM tracking?

CDHalo
Jul 27, 2013 7:21 PM

Hello, I was wondering is there an option to disable the NSA PRISM tracking which is apparently built into all Apple products/software?

Mac Pro, iOS 6.1.4

Barney-15E
Jul 27, 2013 7:53 PM

in response to CDHalo

Call the NSA and ask to be exempted.

This helped me (0)