End-to-End Measurements of Email Spoofing Attacks

Hang Hu, Gang Wang
hanghu@vt.edu
Computer Science, Virginia Tech
Spear Phishing is a Big Threat

• Spear phishing: targeted phishing attack, often involves impersonation
• 91% of targeted attacks involve spear phishing\(^1\)
• 95% of state-affiliated espionage attacks are traced to phishing\(^2\)

---

2. 2013 Data Beach Investigation Report, Verizon, 2013
Real-life Spear Phishing Examples

Yahoo Data Breach in 2014
- Affected 500 Million Yahoo! User Account
- John Podesta’s Gmail Account
  - From Google accounts.googlemail.com

Why can phishers still impersonate others so easily?
I Performed a Spear Phishing Test

- I impersonated USENIX Security co-chairs to send spoofing emails to my account (hanghu@vt.edu)
Background: SMTP & Spoofing

• Simple Mail Transfer Protocol (SMTP) defined in 1982
• SMTP has no built-in authentication mechanism
• Spoof anyone by modifying **MAIL FROM** field of SMTP

![Diagram of email communication and spoofing]

- **William** sends email to **ncsu.edu Mail Server** using **HTTP**.
- **Attacker Mail Server** with **SMTP** sends email to **vt.edu Mail Server** with a **MAIL FROM** address of **whenck@ncsu.edu**.
- **vt.edu Mail Server** responds with **HTTP POP IMAP**.

**ncsu.edu Mail Server** and **vt.edu Mail Server** are connected by **SMTP**.
Existing Anti-spoofing Protocols

SMTP, 1982

Sender Policy Framework (SPF), 2002
• IP based authentication

DomainKeys Identified Mail (DKIM), 2004
• Public key based authentication

Domain-based Message Authentication, Reporting and Conformance (DMARC), 2015
• Based on SPF and DKIM
• Publish policy

SPF Process

MAIL FROM: whenck@ncsu.edu
IP: 1.2.3.4
Is the IP authorized?
Yes

ncsu.edu
DNS
SPF Record
Publish
vt.edu

MAIL FROM: whenck@ncsu.edu
IP: 5.6.7.8
Is the IP authorized?
No

Attacker
How Widely are Anti-spoofing Protocols Used?

- Scanned SPF and DMARC records of Alexa top 1 million domains
- When an email fails SPF/DMARC:
  - Relaxed: No recommending policy
  - Strict: Rejecting failed emails

After years, the adoption rates are still low
And they also increase slowly
This Study

• Research questions
  - How do email providers detect and handle spoofing emails?
  - Under what conditions can spoofing emails penetrate the defense
  - Once spoofing emails get in, how do email providers warn users?

• Measurement + user study
  - 35 popular email providers’ reaction to spoofing emails
  - A user study (N=488) to examine users’ reaction to warnings
Outline

• Introduction

• End-to-end Spoofing Experiments

• User Study
End-to-end Spoofing Experiments

• **Goal:** Understand how email providers handle spoofing emails
• **Method:**
  - Black-box testing
  - Control input and observe output
• **Register our own accounts as email receivers**
• **Change input email**
Target Email Providers

- 35 Email providers

Our Mail Server → Target Email Server

Full Authentication Check (16)

Partial Authentication (15)

No Authentication (4)
Spoofed Sender x 30
- SPF/DKIM, strict policy (x10)
- SPF/DKIM, relaxed policy (x10)
- No SPF/DKIM/DMARC (x10)

Content x 5
- Phishing, Benign
- Blank, Blank w/ URL, Blank w/ attachment

IP x 2
- Static, Dynamic

Experiment Setup
- Repeat 5 times
- Randomized sending order
- 30 x 5 x 2 x 5 = 1500 emails per service
- 1500 x 35 = 52500 emails in total
- Carefully controlled sending rate

IRB Approved
Email providers still let spoofing emails in even if they conduct authentication check.
### Impacting Factors

<table>
<thead>
<tr>
<th>Sender Authentication</th>
<th>Strict</th>
<th>Relaxed</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Authentication</td>
<td>0.13</td>
<td>0.45</td>
<td>0.6</td>
</tr>
<tr>
<td>Partial Authentication</td>
<td>0.28</td>
<td>0.37</td>
<td>0.5</td>
</tr>
<tr>
<td>No Authentication</td>
<td>0.94</td>
<td>0.95</td>
<td>0.94</td>
</tr>
</tbody>
</table>

**Spoofed Sender Address Profile**

- **Strict**: When sender didn't publish authentication records, the penetration rate is highest.
- **Relaxed**: When receiver doesn't do authentication, the penetration rates are more than 94%.

**Penetration Rate**

- 0 - 0.25
- 0.25 - 0.5
- 0.5 - 0.75

1. It takes both senders and receivers to configure correctly.
2. Even so, there are 13% penetration rates.
How Do Email Providers Give Warning

29/35 web clients and 24/28 mobile clients didn’t give any warnings

<table>
<thead>
<tr>
<th>Provider</th>
<th>Web</th>
<th>Mobile</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gmail</td>
<td>✔️</td>
<td>✔️</td>
<td>🔄 Forged <a href="mailto:forged@easychair.org">forged@easychair.org</a> 🔄 to me</td>
</tr>
<tr>
<td>Naver</td>
<td>✔️</td>
<td>✔️</td>
<td>🔄 This message is not from [live.com]. Please note that the sender’s address may differ from the actual sender’s address. Learn more</td>
</tr>
<tr>
<td>Protonmail</td>
<td>✔️</td>
<td>✔️</td>
<td>🔄 This email has failed its domain’s authentication requirements. It may be spoofed or improperly forwarded!</td>
</tr>
<tr>
<td>163.com</td>
<td>✔️</td>
<td>✗</td>
<td>🔄 请注意：此邮件有可能存在仿冒，请不要轻易透露个人信息，提高警惕，谨防网络诈骗！查看详情</td>
</tr>
<tr>
<td>126.com</td>
<td>✔️</td>
<td>✗</td>
<td>🔄</td>
</tr>
<tr>
<td>Mail.ru</td>
<td>✔️</td>
<td>✗</td>
<td>We cannot verify the authenticity of the sender.</td>
</tr>
</tbody>
</table>
Outline

• Introduction

• End-to-end Spoofing Experiments

• User Study
How Effective are These Security Indicators

• Research Questions
  - How do users react to spoofing emails?
  - How effective are warnings?

• Challenge
  - How to capture the realistic user reactions?
  - Lab experiment has limited ability to reflect reality [3]

• Method
  - Try to make users not aware they are in an experiment to capture realistic reaction
  - Inform users after experiment
  - Users can withdraw data anytime with payment

Phase 1/2: Set Up Deception

• Frame the study as a survey to understand email using habits
  - Ask for users’ email address
  - Send the participant an email with 1x1 tracking pixel
  - Ask questions about the email using habits and other distraction questions
  - Pay users and make users believe the survey is over

• Purpose:
  - Collect and validate users’ email addresses
  - Test if the tracking pixel works
Phase 2/2: Sending Actual Spoofing Emails

- Wait for 10 days and send users spoofing emails
- Wait for another 20 days and send debriefing emails
Deception User Study: Recruiting Participants

- Amazon Mechanical Turk
- Recruited 488 users
  - 243 in no warning group
  - 245 in warning group

Gender
- Female 51%
- Male 49%

Age
- 30-39 39%
- 40-49 15%
- >=50 14%
- <= 29 32%

Education
- Bachelor 35%
- Some college 34%
- Graduate 21%
- Highschool 10%
Deception User Study: Results

<table>
<thead>
<tr>
<th>Phase</th>
<th>Users</th>
<th>Without Warning</th>
<th>With Warning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td>All Participants</td>
<td>243</td>
<td>245</td>
</tr>
</tbody>
</table>

1. Warning only slightly lowers the click rate
2. The absolute click rate is still high
Discussion

• A big gap between server detection and user protection
  - Most email providers let spoofing emails reach inbox
  - Most email providers lack necessary warnings
  - Warnings can’t fully eliminate the risk

• Countermeasures
  - Promote SPF, DKIM and DMARC
  - Place warning consistently across web and mobile clients

• Future work
  • Design more effective warnings
  • Defeat warning fatigue
  • User training and education
Thank You
Deception User Study: Results

Click Rate of Different Demographic Groups

- Male
- Female
- L-Edu
- H-Edu
- Young
- Old

No Security Indicator
W/ Security Indicator
Things are Worse with Less Popular Domains
Misleading UI Elements

When spoofing existing contacts or conducting same-domain spoofing

Profile Picture

Name Card

Email History
Misleading UI Elements

Seznam.cz
Spoofing is a Critical Step in Spear Phishing

• Email spoofing is widely used in spear phishing attacks
  - “Business email compromise” (BEC) scams became a major problem in 2015
  - Use similar domain names or spoofed domain names

2. Figure from Phishing Activity Trends Report 4th quarter 2017, APWG.
3. Phishing Activity Trends Report, 1st-3rd quarters 2015, APWG.
We noticed a login attempt to your VT account from an unrecognized device on Thur, March 02, 2017.

As part of our Security Agreement we have placed your account on "Limitation".

Please follow the link below to keep your VT account safe: Link

Thanks for taking these additional steps to keep your account safe.

©2017 VT students and staffs Affairs.
Misleading UI Elements

- Auto-loaded Profile Picture
- False Security Cue

- Auto-loaded name card and email history
## Deception User Study: Results

<table>
<thead>
<tr>
<th>Users</th>
<th>Without Indicator</th>
<th>With Indicator</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Desktop</td>
<td>Mobile</td>
</tr>
<tr>
<td>Opened Email</td>
<td>45</td>
<td>49</td>
</tr>
<tr>
<td>Clicked URL</td>
<td>21</td>
<td>25</td>
</tr>
<tr>
<td>Click Rate</td>
<td>46.7%</td>
<td>51.0%</td>
</tr>
</tbody>
</table>
End-to-end Spoofing Experiments: Results

Email providers still let forged emails in even if they conduct authentication check

163.com
126.com
gmail.com
gmail inbox
naver.com
yeah.net	
tutanota.com
yahoo.com
inbox.lv
protonmail.com
seznam.cz
aol.com
icloud.com
hotmail.com

Hotmail.com blocked all forged email
End-to-end Spoofing Experiments: Results

Email providers still let forged emails in even if they conduct authentication check.
End-to-end Spoofing Experiments: Results

No authentication group let almost all forged emails in
End-to-end Spoofing Experiments: Results

<table>
<thead>
<tr>
<th>Authentication</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Authentication</td>
<td></td>
</tr>
<tr>
<td>Check SPF DKIM But not DMARC</td>
<td>0.57 0.27</td>
</tr>
<tr>
<td>No authentication</td>
<td>0.95 0.94</td>
</tr>
</tbody>
</table>

1. It’s easier for static IP to conduct spoofing