No Phishing With the Wrong Bait: Reducing the Phishing Risk by Address Separation

SecWeb 2020

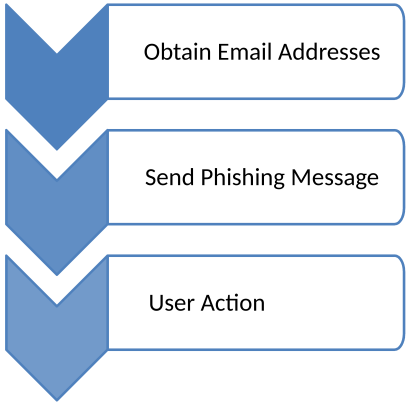
Vincent Drury, Ulrike Meyer
RWTH Aachen University
Research Group IT-Security

Graduiertenkolleg "Human Centered Systems Security"
NERD.NRW

IT SEC Research Group IT-Security
RWTH AACHEN UNIVERSITY

Idea

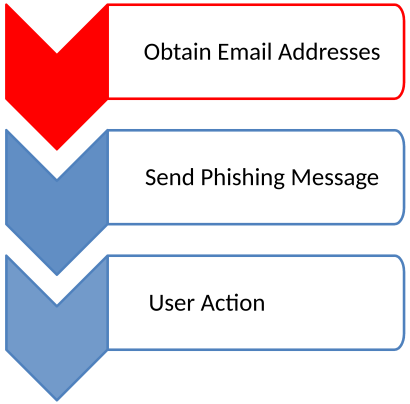
- Phishing still problem for Internet users
- Structured analysis: Killchain
- Early disruption?



Idea

- Phishing still problem for Internet users
- Structured analysis: Killchain
- Early disruption?

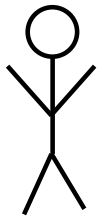
→ Prevent accurate information gathering



Approach

- Attacker's assumption: Email address associated with targeted service

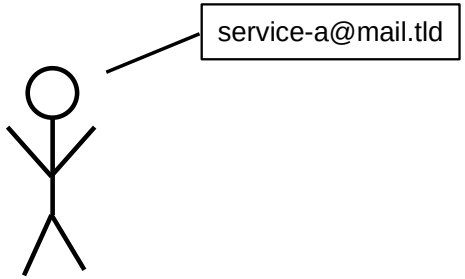
→ Aim to make this likelihood as small as possible



Approach

- Attacker's assumption: Email address associated with targeted service

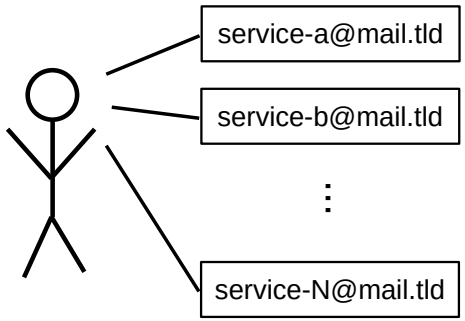
→ Aim to make this likelihood as small as possible



Approach

- Attacker's assumption: Email address associated with targeted service

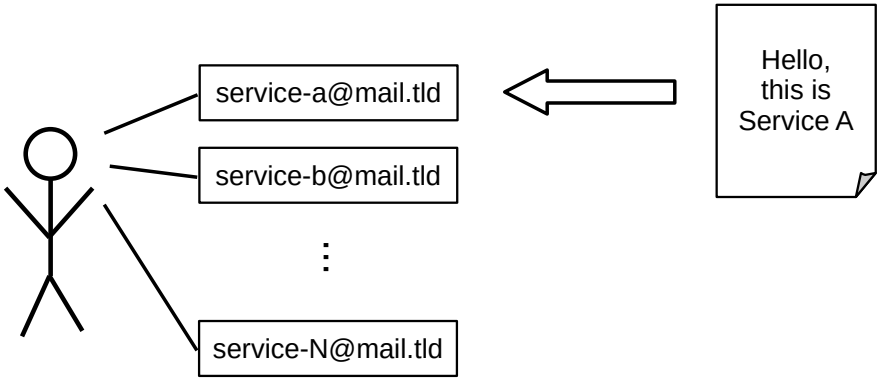
→ Aim to make this likelihood as small as possible



Approach

- Attacker's assumption: Email address associated with targeted service

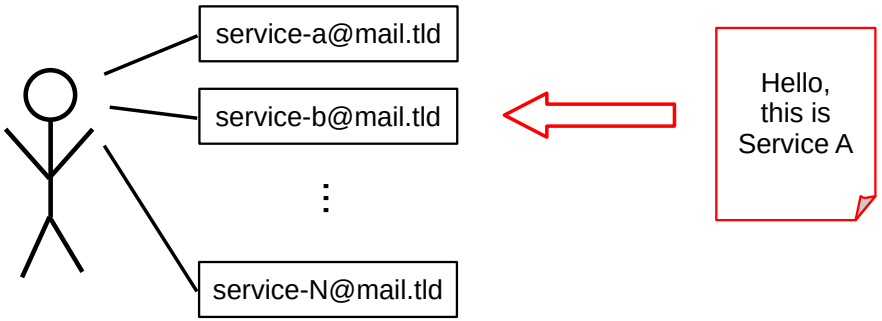
→ Aim to make this likelihood as small as possible



Approach

- Attacker's assumption: Email address associated with targeted service

→ Aim to make this likelihood as small as possible



Related Work

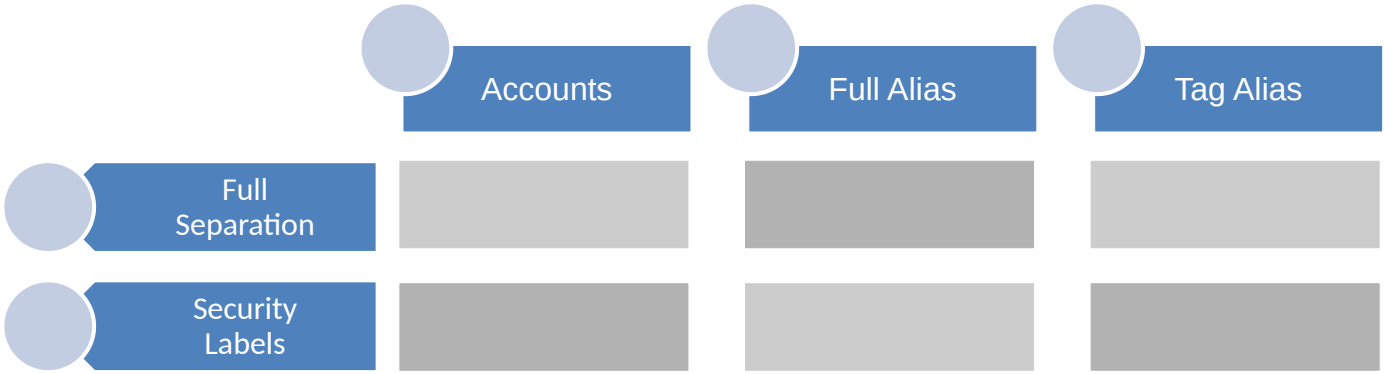
- Not studied in detail
- Phishing Models/Taxonomies: Usually skip this step
- Existing literature on alias systems
- Integrates with existing anti-phishing techniques

Email Address Separation: Techniques

- Several ways to achieve address separation
- Full Alias: Often restricted in number

Email Address Separation: Techniques

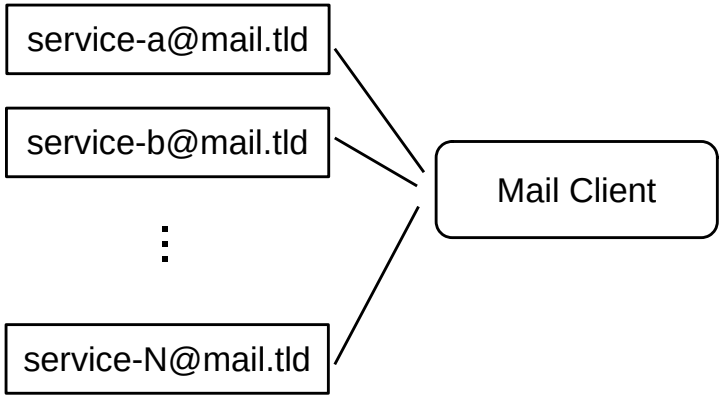
- Several ways to achieve address separation
- Full Alias: Often restricted in number



Email Address Separation: Goal

- Automated sorting based on recipient address

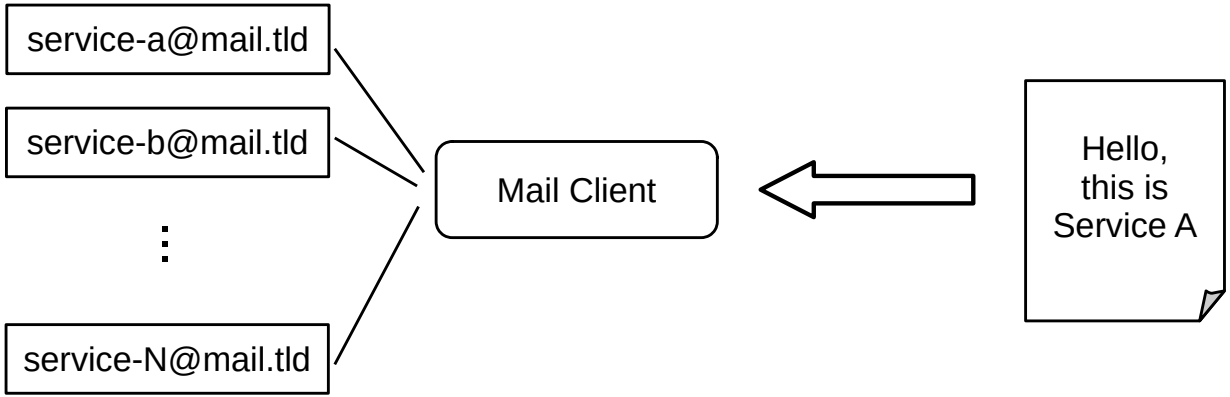
→ "Safe-sender list" enforced via addresses



Email Address Separation: Goal

- Automated sorting based on recipient address

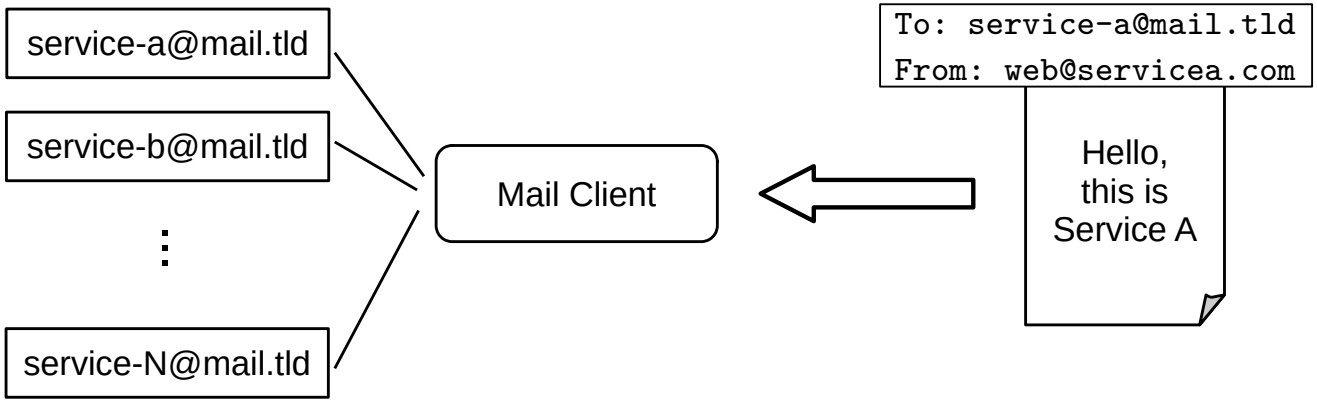
→ "Safe-sender list" enforced via addresses



Email Address Separation: Goal

- Automated sorting based on recipient address

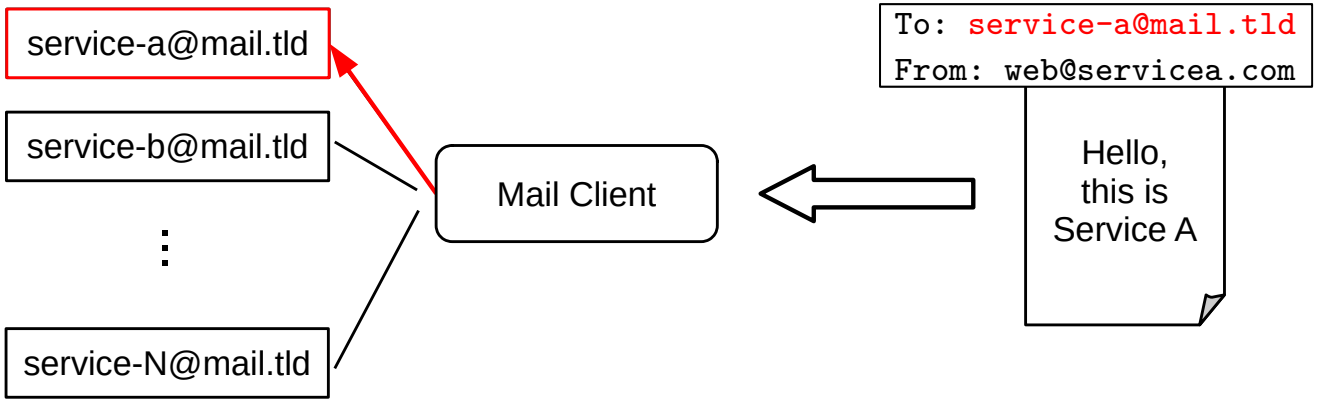
→ "Safe-sender list" enforced via addresses



Email Address Separation: Goal

- Automated sorting based on recipient address

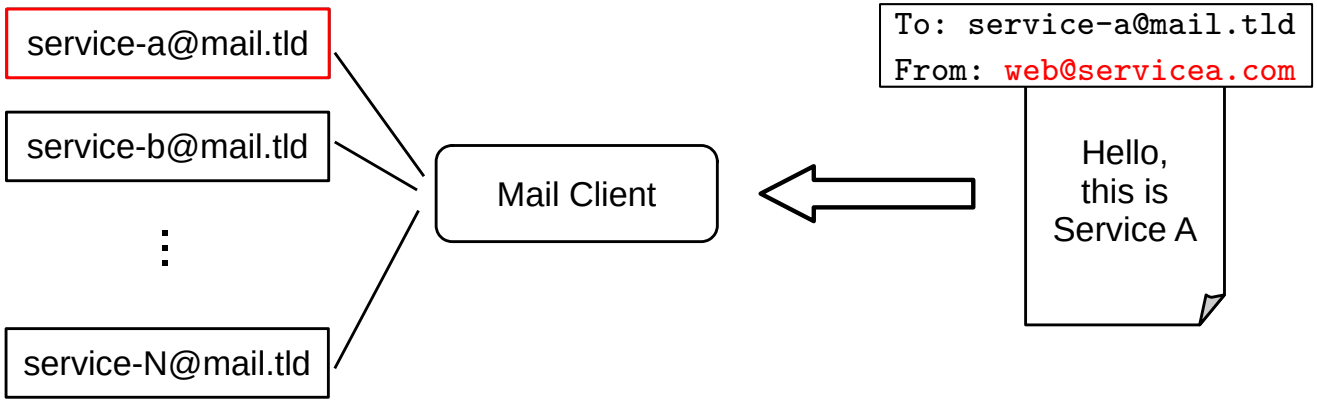
→ "Safe-sender list" enforced via addresses



Email Address Separation: Goal

- Automated sorting based on recipient address

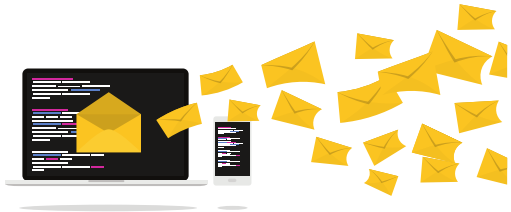
→ "Safe-sender list" enforced via addresses



Attacker Perspective: Address Collection

Email address collection:

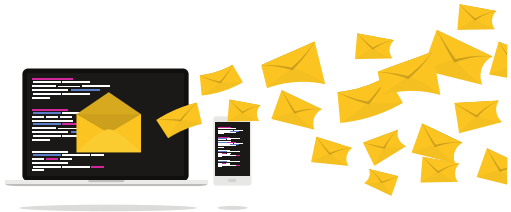
- Website Scraping
  - Separate addresses for public posts



Attacker Perspective: Address Collection

Email address collection:

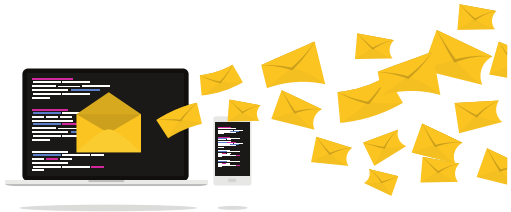
- Website Scraping
  - Separate addresses for public posts
- Data Leaks
  - Separate addresses per account



Attacker Perspective: Address Collection

Email address collection:

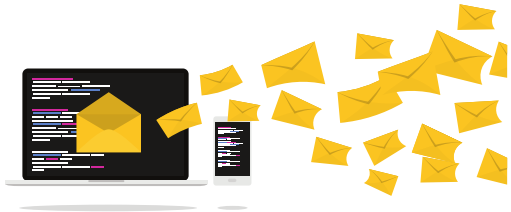
- Website Scraping
  - Separate addresses for public posts
- Data Leaks
  - Separate addresses per account
- Dictionary Attacks
  - Hard-to-guess addresses for used services



Attacker Perspective: Address Collection

Email address collection:

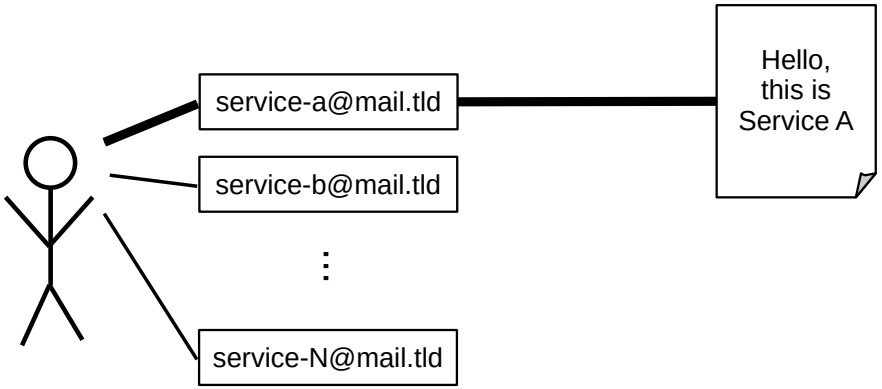
- Website Scraping
  - Separate addresses for public posts
- Data Leaks
  - Separate addresses per account
- Dictionary Attacks
  - Hard-to-guess addresses for used services
- Malware
  - Not prevented by address separation



Attacker Perspective: General Phishing

General phishing:

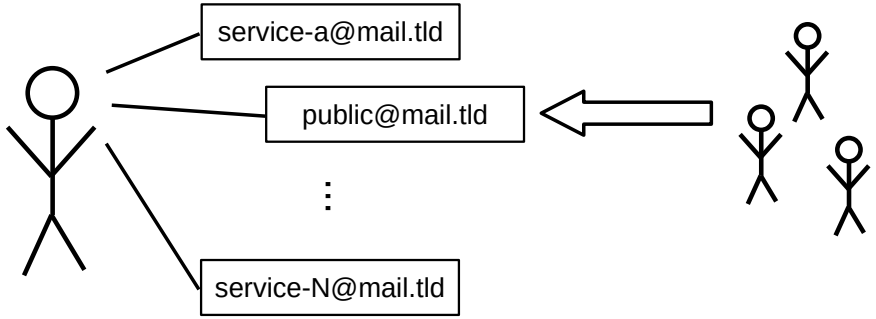
- “Channel” between address and service
- Attacker has to obtain correct address



Attacker Perspective: Public Addresses

Public Address:

- Unknown senders are expected
- Example attack: Malicious CV



Discussion

- Usability
  - Management complexity
- Positive Effect: Awareness?
- General problems
  - Applicability: Can users choose address?
  - Conflict: Services try to prevent use of aliases

Conclusion

- Approach to fight phishing early in the process
  - Hide email addresses from attackers
  - Potentially reduce attack surface for several types of attacks
- Problems:
  - Not effective against all attacks
  - Will typical users do it? (How?)
- Future: Create and evaluate prototype

Conclusion

- Approach to fight phishing early in the process
  - Hide email addresses from attackers
  - Potentially reduce attack surface for several types of attacks
- Problems:
  - Not effective against all attacks
  - Will typical users do it? (How?)
- Future: Create and evaluate prototype

Thank you for your attention!

Backup: Discussion

- Additional address collection methods
- Advanced attacks
- (Problematic) Usage scenarios
- Usability
- Automation

Backup: Alias Types Offered by Popular ESPs

Provider	Full Alias	Tag Alias	Filtering	Purpose
Gmail	-	yes	yes	Sorting
iCloud	3	-	yes	Conceal+Monitor
Outlook	9	-	yes	Conceal+Prevent
Yahoo	1[a]	-	yes	Conceal

Numbers indicate restrictions on the possible amount of aliases in addition to the original address.

[a]Plus 10 send-only and 500 throwaway addresses.