SecureComm | 2020

EAI

Email Address Mutation for Proactive Deterrence Against Lateral Spear-phishing Attacks

Md Mazharul Islam*, Ehab Al-Shaer+ and Basit Rahim*

*University of North Carolina at Charlotte

+Carnegie Mellon University

October 21-23, 2020

Motivation

- Email spear-phishing attack is one of the most devastating cyber threats against individual and business victims.
- Spear-phisher can impersonate identities to incite victims to perform desired actions.
- Recent reports show that:
  - Spear-phishing attacks constitute **90%** of data breaches in 2017-2018.
  - Spear-phishing attacks constitute **74%** of public sector, and **64%** of organizations.
  - Spear-phishing attacks constitute **71.4%** of phishing attacks/data breaches in the US.
- Over $26B (FBI report) has been lost to spear-phishing and account takeover only in 2019.

Threat Model: Lateral Spear-phishing Attack

- Spear-phishing is more targeted than phishing attack.
- Spear-phishing from compromised benign accounts is known as ***lateral spear-phishing attack***.
- To make the attack trustworthy, adversaries choose compromised accounts:
  - Employees from the same organization.
- Lateral spear-phishing are very hard to detect because of the cleverly crafted content.
- Adversaries inherently beats defenders by
  - Evading sender authentication security.
  - behavioral anomaly detectors.

Example of lateral spear-phishing

```
From: Alice <alice@org.com>
To: Bob <bob@org.com>
Subject: February, 2020 Meeting Budget (Event venue booking)
Hi Bob,
Process wire transfer of $100,543 to Trudy (account no. 5648132796, routing no. 026001234) to
finalize upcoming  event venue bookings. Send me an invoice of that transaction ASAP, thanks.
Alice
CEO, org.com
```

Listing: A carefully crafted lateral spear-phishing email sends to Bob from a compromised account Alice, without any malicious attachments or URLs.

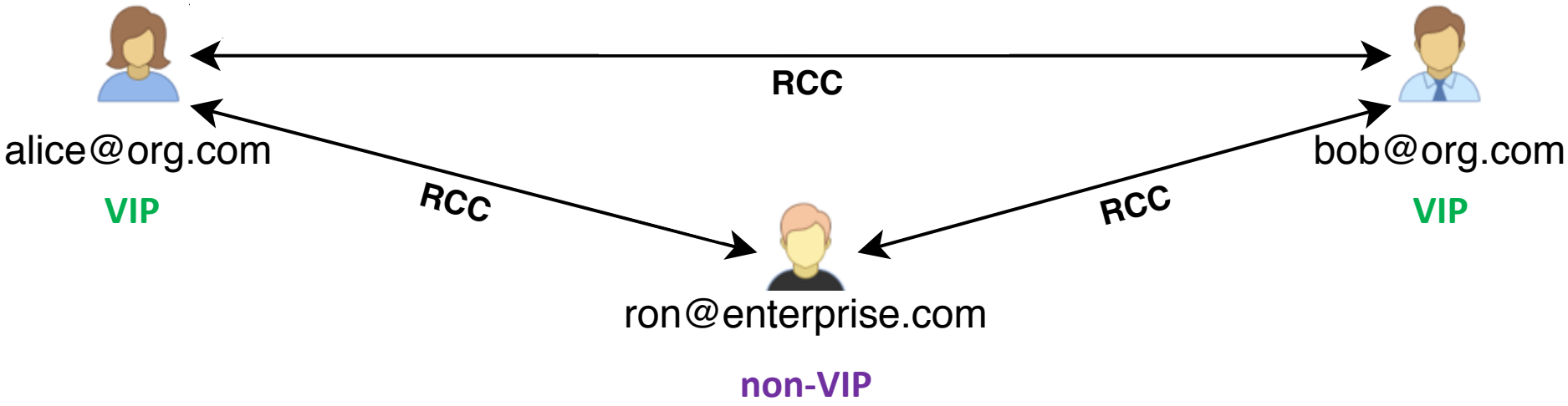
Related Work

- Behavioral Analysis
  - + Uses distinct attack signature (URL/attachments) and features for header or content analysis.
  - - Requires large historical dataset for training and subject to high FP and FN rates.
  - - It fails to detect lateral spear-phishing attack because:
    - LSP attacks mimic benign user behavior.
    - Can avoid bad signature, and
    - They composed from legitimate email account.
- Standard email protocols (SPF, DKIM, and DMARC) can not detect it.
- Cryptographic Approaches (PGP, S/MIME)
  - + Can ensure sender authenticity by digitally signed/encrypt the email.
  - - *Low usability: requires* end-users to use public-keys cryptography.
  - - *Low transparency:* PGP encrypted cyphertext prevents using other technologies such as IDS.
  - - PGP signatures can be spoofed as well.

Our Email Mutation Approach

- We developed a novel proactive defense technique using sender Email address Mutation (EM) to protect a group of users (VIP) form LSP.
- We change the sender email address randomly while forwarding an email that can only be verified by the trusted peers.
- A secure gateway in the cloud do the ***mutation*** and ***verification***.
- EM does not impose any restriction on email communication with external users.
- Email mutation technique is transparent.
- Allows users to use their email as usual.

Email Mutation Protocol

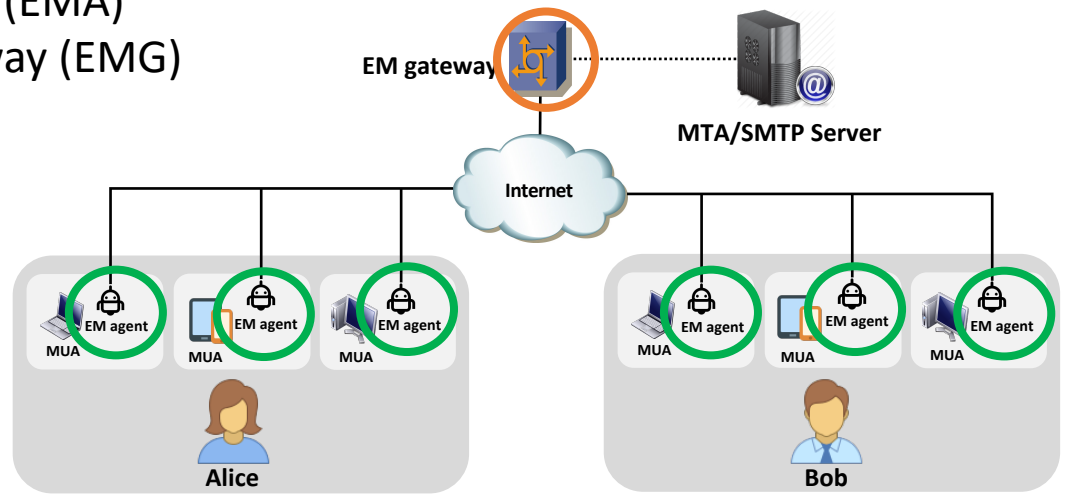


Shadow Email Address

- Pre-created email accounts.
- Kept hidden from VIP users.
- Only used in email transmission as a sender address.
- VIP user gets different number of shadow email accounts based on their impact.
- A possible shadow email address may look like: real.email.address.x@domain.
- Example: *alice.sid8aiy5vgia0ta4uec@org.com is a shadow of* alice@org.com

Email Mutation Architecture

1. Email Mutation Agent (EMA)
2. Email Mutation Gateway (EMG)



Email Mutation Workflow

Sender: alice@org.com
Receiver: bob@org.com
Body: Hello World!

Sender: alice.sid8aiy5vgia0ta4uec@org.com
Receiver: bob@org.com
Body: Hello World!

Sender: alice@org.com
Receiver: bob@org.com
Body: Hello World!

Alice
alice@org.com

Agent

Client Environment

Agent

Bob
bob@org.com

Client Environment

Email Mutation Algorithm

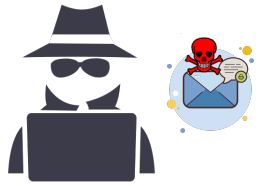
- When a VIP user *i* sends an email to another VIP user *j:*
  - The last *l* emails between them will be used as ground truth $G_{i,j}$
  - $G_{i,j}$ is hashed (SHA-512) to generate a mutation ID, *mID*
  - By indexing the *mID*, a shadow email address gets selected from a secret arrangement of shadow email addresses S_i assigned for the sender *i*

Algorithm 1 Shadow Selection

1: **procedure** SELECTSHADOW($G_{i,j}$, S_i)
2: $h \leftarrow$ SHA-512($G_{i,j}$)
3: $mID \leftarrow h \ mod \ len(S_i)$
4: $shadow \leftarrow S_i[mID]$
5: **return** *shadow*

Shadow email list (S_i)
alice.sid8aiy5vgia0ta4uec@org.com
alice.sid0iqeapz9a9yqylvd@org.com
…
alice.sid6o5int4xi00k23s3@org.com

Identifying Lateral Spear-phishing Attack



Trudy

Case 1
Sender: alice@org.com
Receiver: bob@org.com
Body: Send money!

Case 2 (EM Engineering Attack)
Sender: alice.sidgiwdj12531okg@org.com
Receiver: bob@org.com
Body: Send money!

Threat

EMG | Mail Server | EMG

Alice
alice@org.com

Agent

Client Environment

Alice's Shadow email list
alice.sid8aiy5vgia0ta4uec@org.com
alice.sid0iqeapz9a9yqylvd@org.com
...
alice.sid6o5int4xi00k23s3@org.com

Agent

Bob
bob@org.com

Client Environment

Communication with External Users

- **No Mutation:** A VIP user sends an email to a non-VIP user.

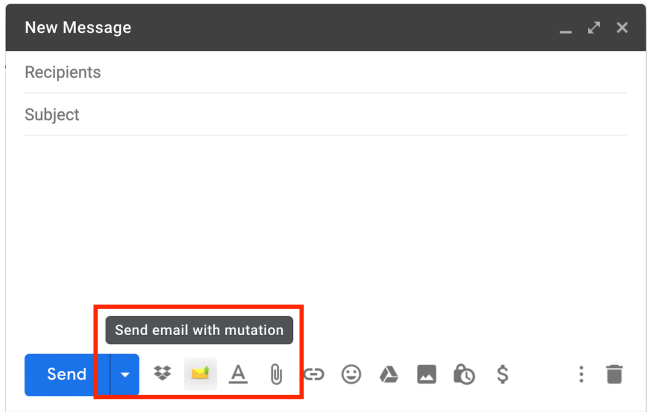
  {sender : x, recipient : y; where, $x \in R$ and $y \notin R$}

  where, *R* is the list of real email addresses of all VIP users.
- **No Verification:** A VIP user receives an email from a non-VIP user.

  {sender : x, recipient : y; where, $x \notin R$ and $y \in R$}

Challenges and Solutions

- Does Multiple Shadow Email Accounts Requires extra **Storage**?
  - Shadow email accounts only used for sending emails.
  - The receiver email address will always be the real email address.
  - EMG uses IMAP APPEND command to populate the real email sent-box.
- Does Email Mutation Decrease **Usability**?
  - Using EM is completely transparent to users.
  - Easy-to-use: It requires NO user training.
  - Easy-to-Integrate: It requires NO changes in client side.
- Is EM Vulnerable to **Insider Attackers**?
  - John uses his EMA to send a phishing email to Bob impersonating Alice.
  - EMA is synchronized with its corresponding EMG through a unique **authentication token**.



Challenges and Solutions

- Does EM cause any **Privacy Violations**?
  - EMG does not keep any copy of the email.
  - EMA connects with EMGs through secure channels (SSL/TLS).
  - The secret shadow email lists can not be retrievable from any EMGs.
  - Many organizations are adopting secure email gateways (Cisco, Microsoft, Barracuda, Mimecast, etc.)
- Can EM Gateways Assure **Consistency**?
  - A user deletes any email from his inbox/sent-box.
  - EMG keeps the hashed (SHA-512) digest of the last *l* number of emails between two VIP users.

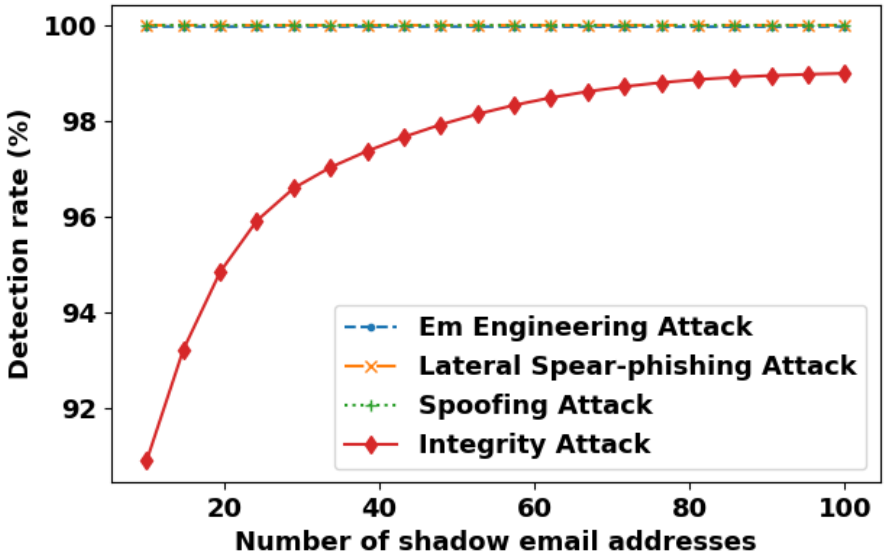
Email Mutation System Verification

- EM is a new technique; therefore, it is necessary to ensure the design correctness.
- We use UPPAAL model checker to formally specify, model, and verify EM system to find any unknown behavior if it exists.
- We modeled EM using timed automata and verified against three temporal properties:
  1. ***Reachability*** describes that every good state is reachable, and every bad state is unreachable.
  2. ***Liveness*** describes the system is progressing to achieve a specific goal.
  3. ***Deadlock-freeness*** ensures that the system is not stopped, and it is always progressing.

Evaluation

- Metrics
  - *Accuracy:* Lateral spear-phishing and spoofing identification.
  - *Overhead:* Overhead added to the system.
  - *Breaking:* Brute-force approach to break EM.
  - Other attack detection: integrity violation.
- Experimentation Methodology and Setup:
  - Protected 5,000 VIP members over five different organizations.
  - The JPL red team sends more than half a million attack emails.
  - The VIP members use different mail services and email clients:
    - Gmail, Microsoft Exchange, Apple iCloud, etc.
    - mail.google.com, Outlook, Thunderbird, and more.

Attack Identification



- The Lateral spear-phishing and spoofing detection rate is 100% for all values of shadow email addresses.
- The integrity attack can be detected with 99% accuracy by using 100 shadow email addresses.

Attack Identification

Metric	Data
Total attack emails	516,000
Lateral spear-phishing attack	153,207
Spoofing attack	145,291
EM engineering attack	201,437
Integrity attack	16,065
EM engineering attack missed	3
Integrity attack missed	167
L. spear-phishing detection	100%
Spoofing detection	100%
EM engineering detection	99.99%
EM engineering false negative	0.0015%
Integrity attack false negative	1.04%

Table: Lateral spear-phishing and other attack detection results by EM

Shadow Email Computation Overhead

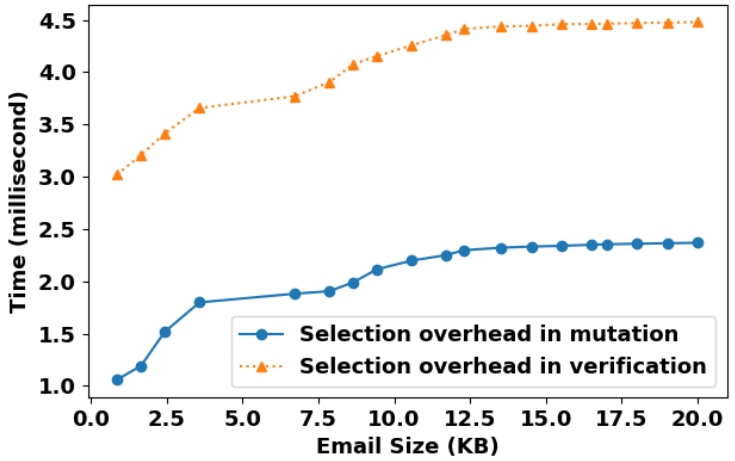


Fig: Without attachment

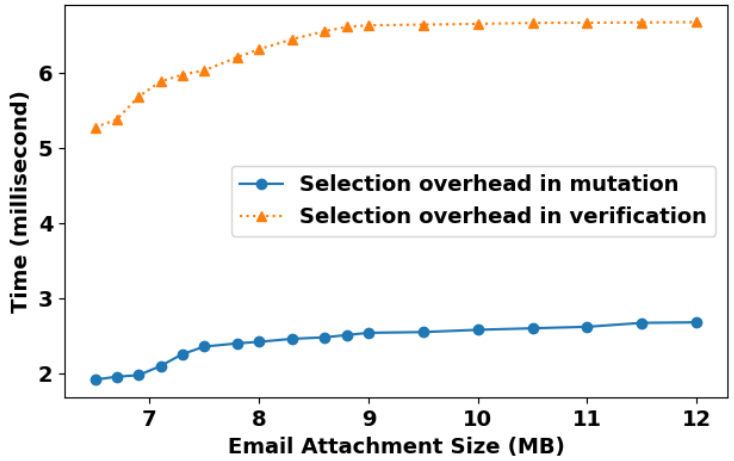


Fig: With attachment

- We evaluated the shadow email address selection time against different email sizes.
- The delay is between 3 to 7 milliseconds for email sizes 7-12MB.

Mutation Overhead

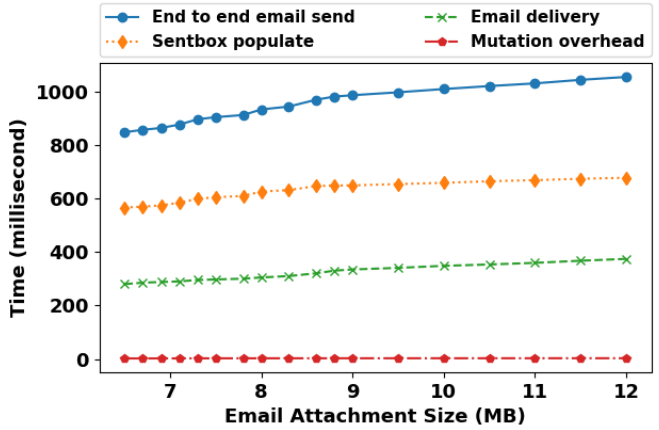


Fig: Without attachment

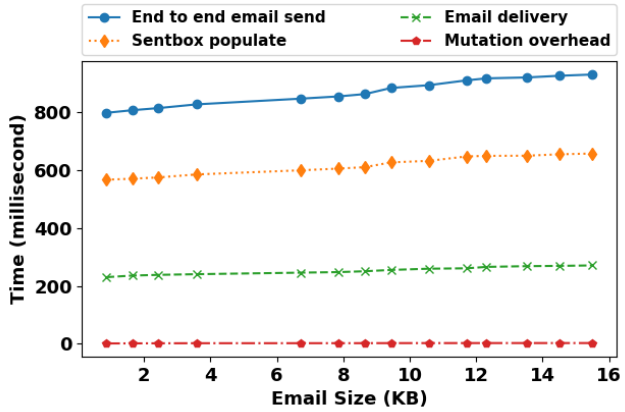


Fig: With attachment

- We evaluated the mutation overhead compared to the end to end email forwarding delay.
- For email sizes 7-12MB, mutation delay is 4.5 milliseconds, and overall sending time is 1.5 seconds.
- The mutation overhead is 0.5% compared to the end-to-end email forwarding delay.

Verification Overhead

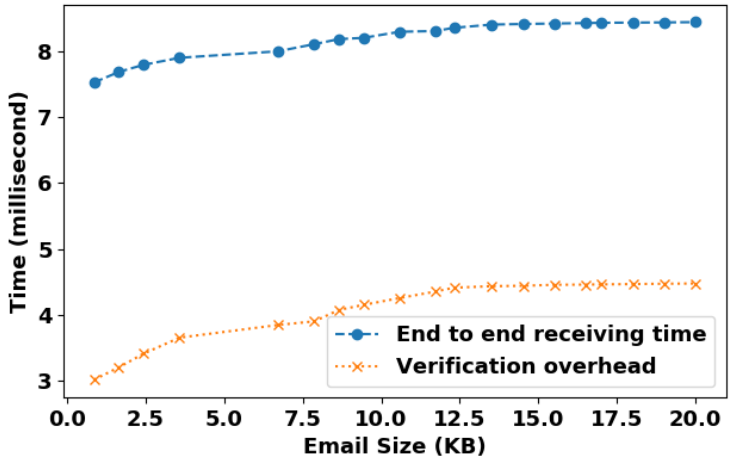


Fig: Without attachment

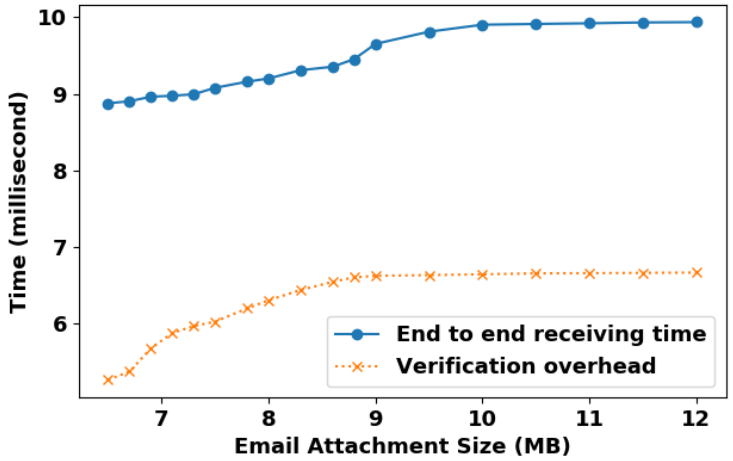


Fig: With attachment

- Emails having 7-12MB sizes have overall 10 milliseconds receiving delay where the verification delay is 7 milliseconds.

Email Processing Rate

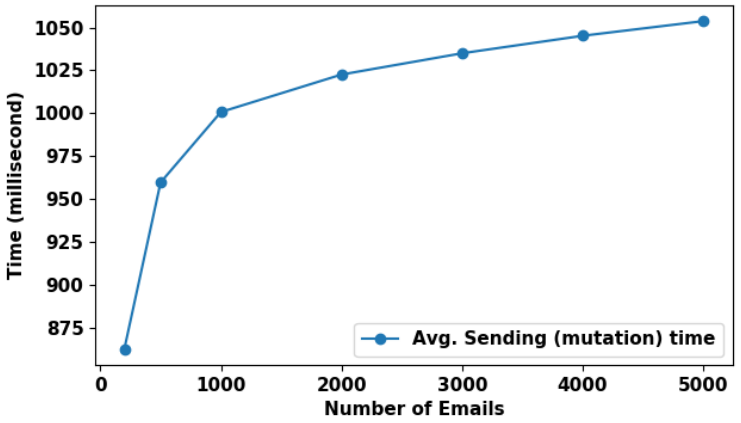


Fig: Mutation overhead

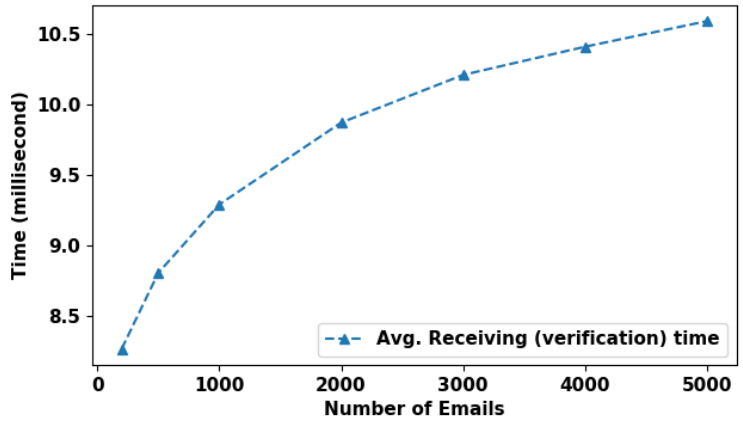
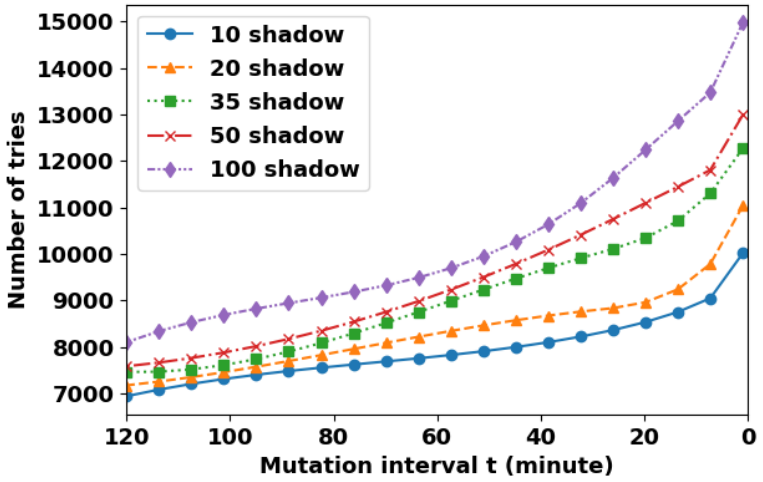


Fig: Verification overhead

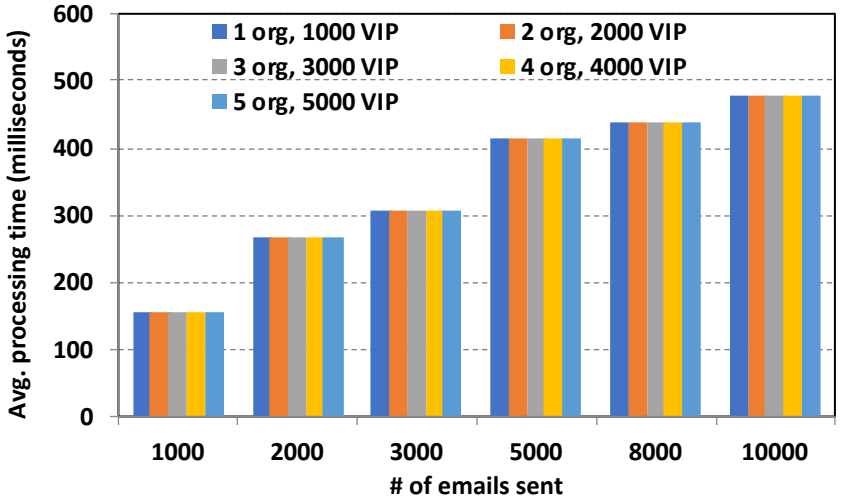
- While dealing with 5000 emails per second the average processing delay:
  - For mutation is 1.1 seconds.
  - For verification is 10.9 milliseconds.

Attack Identification



- We evaluated brute force attack to break EM.
- It takes more than 14,500 tries for an adversary to phish a VIP user having 100 shadow email address.

Cross-Enterprise Architecture Overhead



- We showed that increasing organizations or VIP members do not impose any overhead into the system.
- The delays only increase when the total number of emails dealt at a time increases.

Conclusion & Future Work

- Existing spear-phishing detectors are limited on using the email contents(e.g. malicious ULRs).
- We presented a novel approach using sender email address mutation to proactively defend against the most devastating and stealthy spear-phishing called lateral spear-phishing attacks.
  - Our system guarantees the phishing emails sent from trusted users will be detected immediately.
  - EM integrates well with existing email infrastructures, and it requires no special handling by users.
  - EM requires an agent to be deployed on the client-side and a central gateway in the cloud.
  - We implemented and evaluated EM in a large scale real-world enterprise network with well-known email service providers (Gmail, for example).
- Our evaluation showed that EM causes 0.5% overhead on overall email transmission while detecting lateral spear-phishing and spoofing attacks.
  - Moreover, we showed that it is very hard to break EM (probability 0.000069).
- Limitations and Future Work
  - EM can not protect users if their physical machine gets stolen.
  - VIP users need an EMA instance for every single device they use.
  - In the future, we want to enhance EM to protect users if their device gets compromised.
  - We want to leverage EM on the server-side to remove the use of EMA.

Thank you