Scammers can abuse security flaws in email forwarding to impersonate high-profile domains

September 5 2023

Researchers were able to spoof a wide range of email addresses. Credit: University of California San Diego

Sending an email with a forged address is easier than previously thought, due to flaws in the process that allows email forwarding, according to a research team led by computer scientists at the University of California

San Diego.

The issues researchers uncovered have a broad impact, affecting the integrity of email sent from tens of thousands of domains, including those representing organizations in the U.S. government—such as the majority of U.S. cabinet email domains, including state.gov, as well as security agencies. Key financial service companies, such as Mastercard, and major news organizations, such as The Washington Post and the Associated Press, are also vulnerable.

It's called forwarding-based spoofing and researchers found that they can send email messages impersonating these organizations, bypassing the safeguards deployed by email providers such as Gmail and Outlook. Once recipients get the spoofed email, they are more likely to open attachments that deploy malware, or to click on links that install spyware on their machine.

Such spoofing is made possible by a number of vulnerabilities centered on forwarding emails, the research team found. The original protocol used to check the authenticity of an email implicitly assumes that each organization operates its own mailing infrastructure, with specific IP addresses not used by other domains.

But today, many organizations outsource their email infrastructure to Gmail and Outlook. As a result, thousands of domains have delegated the right to send email on their behalf to the same third party. While these third-party providers validate that their users only send email on behalf of domains that they operate, this protection can be bypassed by email forwarding.

For example, state.gov, the email domain for the Department of State, allows Outlook to send emails on their behalf. This means emails claiming to be from state.gov would be considered legitimate if they

came from Outlook's email servers.

As a result, an attacker can create a spoofed email–an email with a fake identity—pretending, for example, to come from the Department of State—and then forward it through their personal Outlook account. Once they do this, the spoofed email will now be treated as legitimate by the recipient, as it is coming from an Outlook email server.

Versions of this flaw also exist for five other email providers, including iCloud. The researchers also discovered other smaller issues that impact users of Gmail and Zohomail—a popular email provider in India.

Researchers reported the issue to Microsoft, Apple and Google but to their knowledge, it has not been fully fixed.

"That is not surprising since doing so would require a major effort, including dismantling and repairing four decades worth of legacy systems," said Alex Liu, the paper's first author and a Ph.D. student in the Jacobs School Department of Computer Science and Engineering at UC San Diego. "While there are certain short-term mitigations that will significantly reduce the exposure to the attacks we have described here, ultimately email needs to stand on a more solid security footing if it is to effectively resist spoofing attacks going forward."

The team presented their findings at the 8th IEEE European Symposium on Privacy and Security, July 3 to 7, 2023, in Delft, where the work won best paper.

Different attacks

Researchers developed four different types of attacks using forwarding.

For the first three, they assumed that an adversary controls both the

accounts that send and forward emails. The attacker also needs to have a server capable of sending spoofed email messages and an account with a third party provider that allows open forwarding.

The attacker starts by creating a personal account for forwarding and then adds the spoofed address to the accounts' white list—a list of domains that won't be blocked even if they don't meet security standards. The attacker configures their account to forward all email to the desired target. The attacker then forges an email to look like it originated from state.gov and sends the email to their personal Outlook account. Then all the attacker has to do is forward the spoofed email to their target.

More than 12% of the Alexa 100K most popular email domains—the most popular domains on the Internet—are vulnerable to this attack. These include a large number of news organizations, such as the Washington Post, the Los Angeles Times and the Associated Press, as well as domain registrars like GoDaddy, financial services, such as Mastercard and Docusign and large law firms.

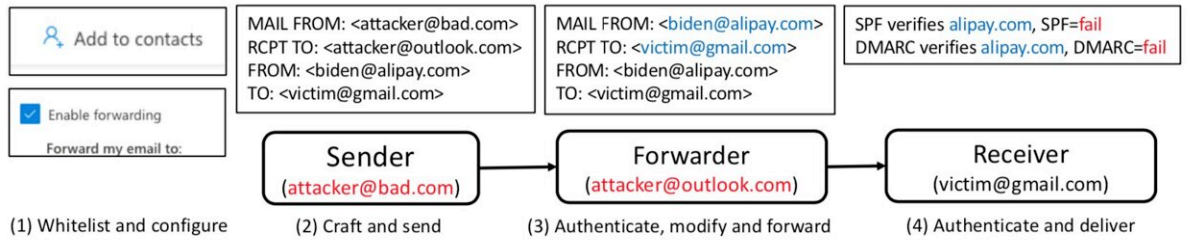

Figure 7: Example of a spoofed email attack exploiting open forwarding and relaxed validation for forwarded email from well-known providers (§ 5.2). Note that the spoofed domain, `alipay.com`, has a DMARC policy of Quarantine and thus should not be delivered.

Example of a spoofed email attack exploiting open forwarding and relaxed validation policies for forwarded email from well-known providers. Credit: University of California San Diego

In addition, 32% of .gov domains are vulnerable, including the majority of US cabinet agencies, a range of security agencies, and agencies working in the public health domain, such as CDC. At the state and local level, virtually all primary state government domains are vulnerable and more than 40% of all .gov domains are used by cities.

In a second version of this attack, an attacker creates a personal Outlook account to forward spoofed email messages to Gmail. In this scenario, the attacker takes on the identity of a domain that is also served by Outlook, then sends the spoofed message from their own malicious server to their personal Outlook account, which in turn forwards it to a series of Gmail accounts.

Roughly 1.9 billion users worldwide are vulnerable to this attack.

Researchers also found variations of this attack that work for four popular mailing list services: Google groups, mailman, listserv and Gaggle.

Potential solutions

Researchers disclosed all vulnerabilities and attacks to providers. Zoho patched their issue and awarded the team a bug bounty. Microsoft also awarded a bug bounty and confirmed the vulnerabilities. Mailing list service Gaggle said it would change protocols to resolve the issue. Gmail also fixed the issues the team reported and iCloud is investigating.

But to truly get to the root of the issue, researchers recommend disabling open forwarding, a process that allows users to configure their account to forward messages to any designated email address without any verification by the destination address. This process is in place for Gmail and Outlook. In addition, providers such as Gmail and Outlook implicity trust high-profile email services, delivering messages forwarded by these

emails regardless.

Providers should also do away with the assumption that emails coming from another major provider are legitimate, a process called relaxed validation policies.

In addition, researchers recommend that mailing lists request confirmation from the true sender address before delivering email.

"A more fundamental approach would be to standardize various aspects of forwarding," the researchers write. "However, making such changes would require system-wide cooperation and will likely encounter many operational issues."

Methods

For each service, researchers created multiple test accounts and used them to forward email to recipient accounts they controlled. They then analyzed the resulting email headers to better understand which forwarding protocol the service used. They tested their attacks on 14 email providers, which are used by 46% of the most popular internet domains and government domains.

They also created mailing lists under existing services provided by UC San Diego, and by mailing list service Gaggle.

Researchers only sent spoofed email messages to accounts they created themselves. They first tested each attack by spoofing domains they created and controlled. Once they verified that the attacks worked, they ran a small set of experiments that spoofed emails from real domains. Still, the spoofed emails were only sent to test accounts the researchers created.

"One fundamental issue is that email security protocols are distributed, optional and independently configured components," the researchers write. "This creates a large and complex attack surface with many possible interactions that cannot be easily anticipated or administrated by any single party."

The research is published on the *arXiv* preprint server.

More information: Enze Liu et al, Forward Pass: On the Security Implications of Email Forwarding Mechanism and Policy, *arXiv* (2023). DOI: 10.48550/arxiv.2302.07287

Provided by University of California - San Diego