PREVEIL

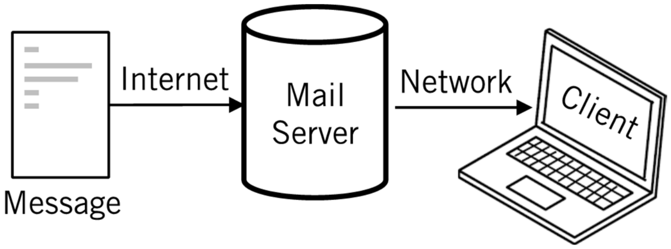
A Framework for Assessing Email Security Risk

Overview

This paper is intended to be used as a tool for information security professionals to assess risks associated with email infrastructure. Email vulnerabilities can harm organizations in two key ways:

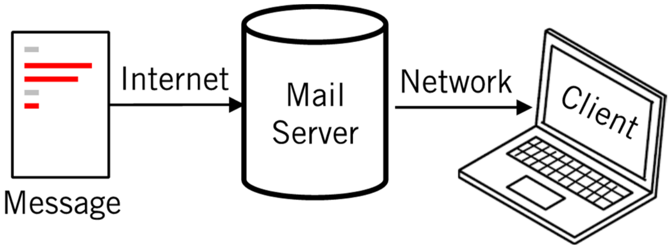
1. **Sensitive content in emails leaked to unintended recipients** can disclose trade secrets, undermine business relationships, and destroy competitive advantage.
2. Email is the primary way **attackers penetrate an organization**, whether by causing unwitting recipients to download malware onto PCs or give up passwords (phishing). Email can also enable an attacker to to appear to be a trusted colleague (spoofing).

Framework



To evaluate vulnerabilities, consider the core elements of electronic mail: A message, often originating outside an organization and transmitted via the Internet is ultimately sent to a recipient's mail server, which delivers the message (via a public or private network) to a mail client running on a device. Using the diagram to the left, one can systematically review the attack methodologies and their risk to organizations.

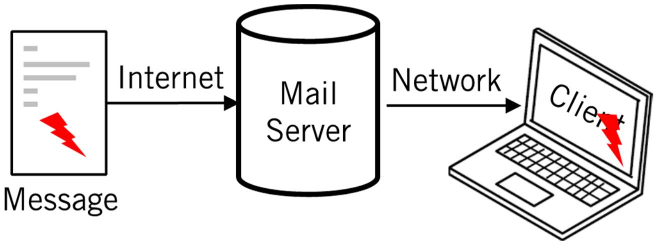
Spoofing



Spoofing involves an attacker masquerading as a legitimate user in order to convince an unsuspecting recipient to give up sensitive information or take some action (e.g. wiring money). Spoofing requires very little technical sophistication as almost any email program will allow a user to generate credentials that appear to be those of someone known to the recipient.

Spoofing attacks are very difficult to prevent, as it's the very nature of email to be open to the outside world, where both trusted people and charlatans reside. The most basic form of protection is to ensure that users are vigilant — reminding users to take extra steps to verify requests received via email. But even the best educated users will sometimes fall victim to spoofing. The best way to protect against spoofing, in combination with user vigilance, is to deploy a special mailbox which is only accessible to a "**trusted community**." By definition, messages received in this special mailbox are most likely authentic.

Phishing

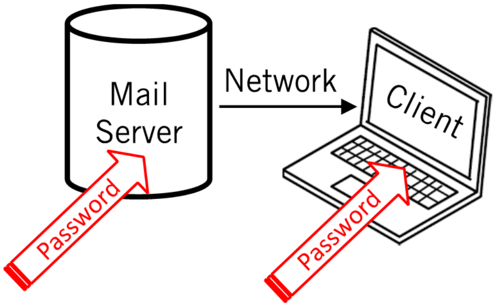


Phishing attacks generally involve convincing a user to click on something in a message, either causing malware to be installed on the client device or visiting a web site that cajoles the recipient to disclose their password or other personal information. One recent study concluded that 95% of enterprise cyber-attacks originated via phishing emails.

Defending against phishing attacks amounts to reducing the "attack surface," in other words minimizing the probability that a user will click on the wrong element of a message. It starts with user education, but additional tools and services are available that attempt to prevent phishing mechanisms from being activated. Email filtering and anti-virus services can reject messages that are already known to be compromised, but these products play a constant cat-and-mouse game to keep up with the attackers. Some organizations block users from clicking on any attachments or links in messages, but these methods place impractical constraints on the usefulness of email. The notion of a "walled garden" associated with t**rusted communities** (as noted above) can significantly reduce the attack surface. Users can be confident in downloading attachments from their trusted mailbox.

Password Authentication

Passwords are the primary means for authenticating users to IT systems. Password proliferation is becoming a growing problem, however. Users hate having to remember and change the passwords for the many systems and services with which they interact. This frustration creates security problems because users replicate similar passwords across different services. Attackers use sophisticated password guessing algorithms and that attempt thousands of passwords logins every second. Because users often reuse the same or similar passwords across services, a successful attack on one service can yield passwords for many other personal and work services. Users often store lists of all passwords in a single place which, if compromised, will leak many access codes. For example, when Russian attackers penetrated Yahoo several years ago, they noted that many users were storing lists of passwords on the site. Many enterprises were compromised, even though their own password policies were solid, because individual users decided to trust the Yahoo service with their work information.



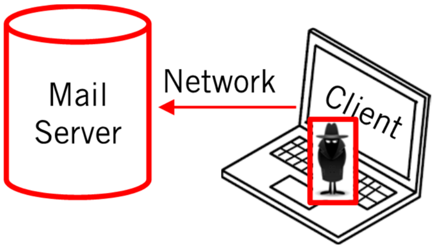
There are several strategies to avoid password attacks. User education is usually the starting point, reminding users to choose complex passwords that are rotated often. As noted above, this sophistication can backfire as users will find their ways to centralize their storage of these passwords, which creates a central point of vulnerability. Password managers are getting more popular, where complex passwords are automatically generated, stored, and pre-entered in known web sites and apps. But these programs are themselves central points of vulnerability (i.e. users' entire digital lives will be compromised if attacked) and often incompatible with apps and services in a user's portfolio.

Security professionals are fond of the adage that one should combine "something you now with something you own" to create "two-factor authentication." So-called "2FA" requires a password to be used in combination with a secret code sent to a mobile phone. However, 2FA systems can be compromised via a "man-in-the-middle" attacks, for example whereby attackers' computers provide the codes sent to the users' cell phones.

An even better approach is to use a secret encryption key instead of a password to authenticate a user. The key is a very large, complex number that's impossible to guess. It's stored in a secure place in the user's phone or computer. Stored keys won't allow a remote attacker to authenticate into a service by stealing a password. And the keys can be generated and stored automatically; users don't need to remember them or write them down. Finally, stored keys can be combined with 2FA to reduce the attack surface even further, thus requiring the possession of **two** devices for authentication.

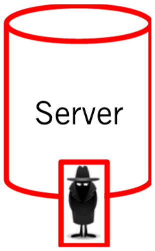
Administrators

IT administrators are often overlooked as central points of vulnerability. Almost all IT systems have administrators, and most admins have very broad privileges. These "super-user" privileges are necessary for the proper functioning of an enterprise. Administrators are the ones who add and delete users, who reset passwords, and who collect enterprise wide information for archival, diagnostic, or even investigative purposes. This means that an attacker who compromises an administrator's role will be able to access all the information on that system. The notorious Edward Snowden had admin privileges.



Protecting against administrator compromise starts with effective policies and procedures for vetting who has admin privileges, who has the authority to approve the execution of these privileges, and how authentication passwords and devices are secured. Better still is to *cryptographically distribute trust* amongst administrators and approvers, just as the proverbial nuclear launch keys require at least two individuals to unlock the firing of a missile. Requiring cryptographic authorization from multiple approvers significantly reduces the attack surface as it's much more difficult to compromise several people than it is to co-opt or attack a single administrator.

Networks and Servers



The mother lode for an attacker is the enterprise server infrastructure because it contains the vast repository comprising an organization's most valuable asset: its data. All of the large breaches harmed businesses are ultimately aimed at servers. Very often, these mega-breaches start with an adversary exploiting the phishing, password, or administrator vulnerabilities noted above to access the server. But attackers also frequently exploit network or software vulnerabilities that they use to reach the mother lode.

Much of the cybersecurity technology available today in essence tries to build electronic moats around servers. There are advanced firewalls, artificially intelligent intrusion detection mechanisms, integrated information and event management platforms, etc.

The holy grail of protection is **encryption**. Specifically, **end-to-end encryption** is the gold standard whereby all server data is encrypted all the time, not just "at rest" or "in transit." With end-to-end encryption the server can never access decryption keys, and information is only decrypted downstream at a client's device. This means that only intended recipients can access data. Even if an attacker can successfully exfiltrate all the data on the server, it appears a gibberish. The best way to secure the email server is by a combination of end-to-end encryption, secret keys for authentication, and administrative access cryptographically authorized by multiple approvers. Together, these techniques represent best practices because the emails on the server are not visible in plaintext and cannot be accessed with stolen user passwords or a by single compromised administrator.

Finally, it's important to note that email messages exchanged across enterprises are often stored on servers owned by different businesses. These messages are only as secure as the weakest link in the communications chain. One way to address this issue is to utilize a single "best practices" based system (such as a cloud service) to secure email across organizations.

Summary

The following table summarizes the various attack vectors described above, along with "good" and "best" practices to defend against them:

	Spoofing	Phishing	Passwords	Admin	Servers
User Education	🟨	🟨	🟨		
Trusted Communities	🟩	🟩			
Email Filtering		🟨			
Advanced malware detection		🟩			
Password complexity & rotation			🟨		
2 Factor Authentication			🟨		
Private Key Authentication			🟩	🟨	
Administrative policies				🟨	🟨
Firewalls					🟨
End-to-end encryption					🟩

Legend
🟨 Good
🟩 Best