Two-Factor Authentication at the Lorentz Institute

Introduction

After the recent increase in cracker activity and floods of phishing emails (cyber criminalilty), it is clear that the Lorentz Institute IT infrastructure is under constant attack. One of the major deficiencies in our current setup is that knowing a username and password is enough to get access to a wide variety of resources and data on our servers. When phishing e-mails are handled improperly, but also when users improperly disclose their credentials (for instance on public WiFi), cyber criminals can easily obtain account credential information. Once a user's credentials have been comprised, preventing the misuse of accounts and computer resources becomes impossible.

To avoid or at least drastically mitigate the problems described above, we have introduced Two-Factor Authentication (2FA) to add an extra level of security to your Lorentz Institute account. With 2FA enabled, knowledge of your username and password is no longer sufficient to gain access to the system, because you will have to provide an **additional**, **unique** security code (AKA one-time password or OTP) to successfully authenticate.

Lorentz Institute's OTPs are generated using the current time (hence the name TOTP) as a source of uniqueness and have a limited duration. If the TOTP has expired, authentication will automatically fail. Users can (re-)generate valid TOTPs by storing a copy of a **secret key** provided by the IL authentication system on a personal device. This copy of the secret key will be used as a seed in calculating the new TOTP (see instructions below). Because TOTPs are calculated by means of the **secret key**, it is of extreme importance that you do not share the key with anybody to prevent that your account is compromised.

More information can be found in the published TOTP open standard https://tools.ietf.org/html/rfc6238.

As an alternative to TOTPs, the Lorentz Institute offers the possibility of registering your own FIDO2 security key and use that as second factor authentication. Note however that self-registration of a security key is **only** possible after you have completed a first-time 2FA setup via one of the methods below and you have notified support@lorentz.leidenuniv.nl. If you do not possess a FIDO2-compatible key and would like to obtain one provided by the IL, please do not hesitate to email

support@lorentz.leidenuniv.nl. Login via a security key currently offers the strongest security possible to protect your IL account from cyber criminals.

Note on acronyms

First-time 2FA Setup

2FA setup is different depending on whether you own a smart phone, a personal computer or none of the two. Users without smart phone will have to use their personal computer or a FIDO2-compatible security key. 2FA requires you to provide the Lorentz Institute with your private email address [1]. Once that is on record, please follow the link below that is appropriate to your situation

- Setup via a smart phone
- Setup via a personal computer
- Setup via a FIDO2 Security Key

2FA-enabled Logins

Two-factor authentication is mandatory to

- access the following Single-sign on (SSO) Web Services

Account Services
Webmail
Remote Workspace
GitLab
xmaris OpenOnDemand

- gain Shell access to the Lorentz Institute SSH server
- login to the IL GNU/Linux workstations

1)

Used only for important security communications related to your IL account