

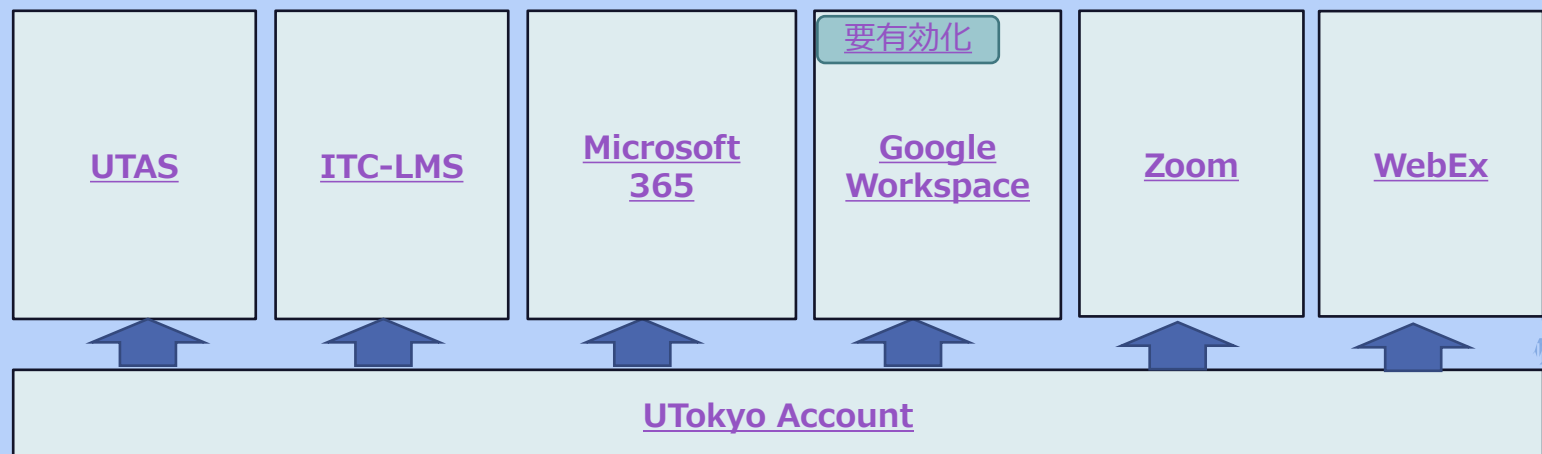
A Better Security and Multi-Factor Authentication

Kenjiro Taura


Information Technology Center

Data we can never leak ...

- ◆ Every single day, some 50,000 members of our university have
 - ◆ UTokyo Account (10-digits@utac.u-tokyo.ac.jp)
 - ◆ Google Account (@g.ecc.u-tokyo.ac.jp)
- accessible from the Internet ...



Basics for a better protection

- ◆ **Never** use easy-to-guess passwords
 - ◆ If you do, change it today!
 - ◆ Change it to a long and complex password (you can generate one by [this](#))
- ◆ **Multi-Factor Authentication (today's )**

What is Multi-Factor Authentication (MFA)?

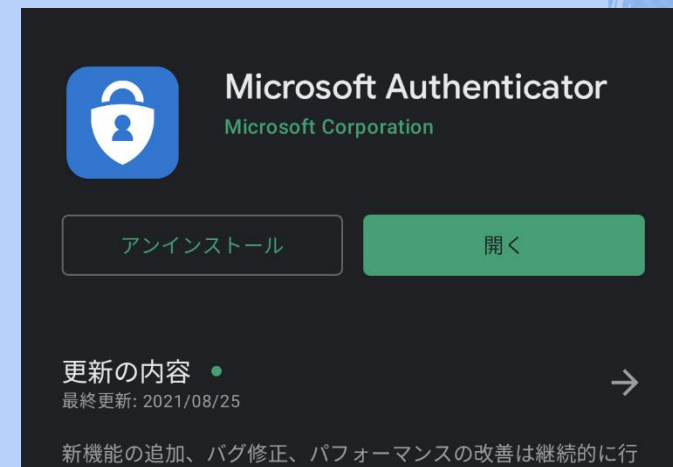
- ◆ In general, it is a sign-in process that confirms two or more pieces of information the only claimed user can know or possess
 - ◆ password, phone, smartphone, biometrics, a special device, etc.
- ◆ In practice, a sign-in process using “a password + one more thing”

Why MFA?

- ◆ Without it, your password is guessed, and you are all over
- ◆ MFA makes you *much, much* safer
 - ◆ A crude analogy: the probability your account is compromised, which might be like 0.001 without MFA, becomes $0.001 \times 0.001 = 0.00001$
- ◆ Consolidate various service accounts into one and protect it strongly, thereby achieving both security and convenience

Isn't MFA cumbersome?

- ◆ Depends on the method, but the one using smartphone authenticator app is convenient
- ◆ As easy as just opening your phone (particularly easy you are addicted anyways)
 - ◆ Demo: [Microsoft Authenticator](#) to [login ITC-LMS](#)
 - ◆ There is an [iOS app](#), too



Methods other than Microsoft Authenticator

- ◆ SMS (6 digits sent to your cell phone)
- ◆ Voice phone (pick your phone and press #)
 - ◆ Cell phone
 - ◆ Home phone
- ◆ Google authenticator, anyway
 - ◆ Like Microsoft Authenticator, but UTokyo Account works better with the Microsoft one
- ◆ Please register at least one method besides Microsoft Authenticator, so you can change your smartphone safely

Will MFA be mandatory?

- ◆ When the service starts on Sep 27, “*strongly recommended*”
- ◆ Future: we wish to mandate it when everybody becomes ready for it
- ◆ You will have enough time to prepare
- ◆ We mandate it for new security-critical services associated with UTokyo Account
 - ◆ VPN (Chapter 3 by Tamatsukuri)

How to use them

- ◆ We will make a summary page on utelecon soon

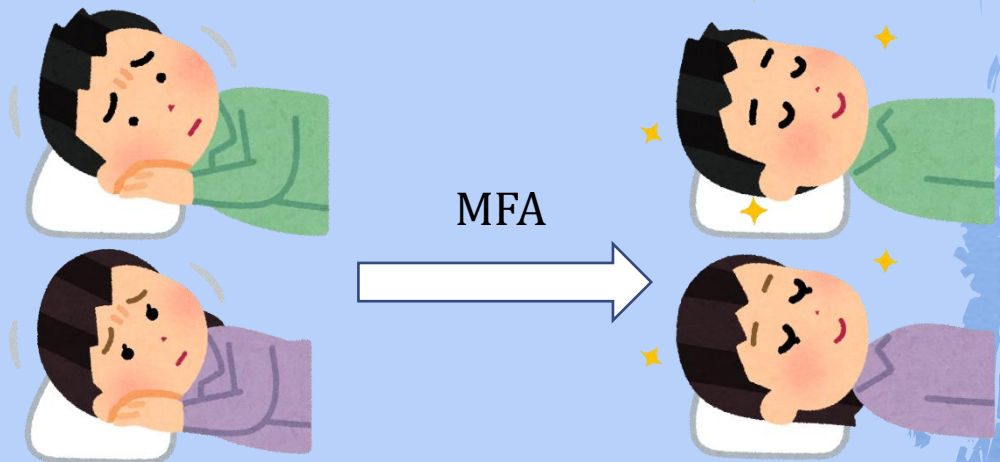
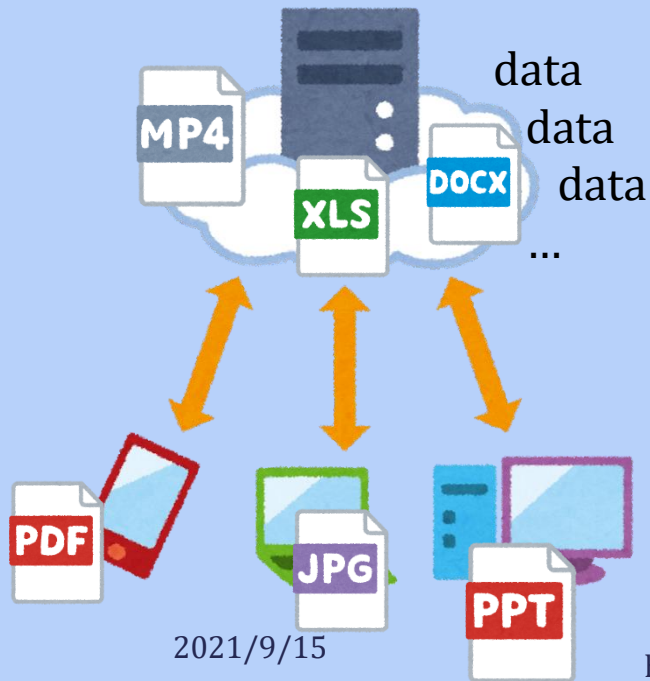
Account	Multi-Factor Authentication	Change password
UTokyo	Turn it on (after Sep 27) https://utacm.adm.u-tokyo.ac.jp/webmtn/LoginServlet → and configure https://mysignins.microsoft.com/security-info?domain_hint=utac.u-tokyo.ac.jp	https://utacm.adm.u-tokyo.ac.jp/webmtn/LoginServlet
Google	https://myaccount.google.com/security	https://idm.ecc.u-tokyo.ac.jp/webmtn/

How to cancel it?

- ◆ Don't.
- ◆ But if you have to ...
- ◆ The system cannot automatically allow it as doing so would defeat its purpose; we need to verify your identity offline
- ◆ We accept cancellation requests via you → your respective office → utelecon
 - ◆ We appreciate a cooperation (forwarding requests) by department offices
 - ◆ Like routing password reset requests for UTokyo Account

To sleep in piece ...

Data are in ...	The major threat	Precautions
cloud (UTokyo/Google Account)	password leak / break-in	strong passwords; MFA (smartphone, cell phone)
smartphone	physical loss	screen lock (biometric, PIN number)
PC	physical loss	disable auto-login, screen lock, encrypted drive



Misc.

- ◆ Review your shared docs on Google Drive, OneDrive (these are what you ought to protect)
 - ◆ Remove or cancel sharing when no longer necessary
 - ◆ Share with only specific people if practical
- ◆ See also [在宅勤務のPC利用ガイド](#)