Linnaeus University
Computer Science
Ola Flygt

2021-12-28

# 2DV703 Mobile and Wireless Data Security
# Assignment #6

## A. Theoretical about Authentication

Read the following articles about Authentication:
- "SecuriCast: Zero-Touch Two-Factor Authentication using WebBluetooth", Dressel T., List E., Echtler F.
- "NFC Unlock: Secure Two-Factor Computer Authentication Using NFC ", Hufstetler W. A., Ramos M. J. H., Wang S. P.
- "Using smart cards to enhance security of Android smartphones in tactical scenarios", Mancini F.
- "A novel Two-Factor HoneyToken Authentication Mechanism", Papaspirou V. et al.

You will find the articles in MyMoodle. Write an individual short summary of each the four articles (in total 3-4 pages). Add your own views on both the quality of the articles and the results presented in them.
Submit the report at latest 2 January. We will discuss them on the seminar 3 January.

## B. SmartCard

In this task you will work with the Smart Cards, other NFC devices and the Gemalto IDBridge CT30 reader/writer (you will have to share one reader between the groups). You need to investigate what the cards can be used for except authentication. What type of information can you write/read from the cards and other tags? What encryption algorithm/s are supported? Are there any other cards (access cards, credit cards, etc.) you have that you can read using either that reader or the other readers in the lab (there are both contact and contactless card readers)?

There are four primary standards for smartcards, all specified by International Organization for Standards. Mention the main differences between the standards.

In this task you will also implement a system that will use the reader and the provided smartcards to authenticate on a computer. You need to implement login for either a stand-alone computer or a client connected to your Windows server. Useful information can be found at: http://www.mysmartlogon.com/eidauthenticate/

Linnaeus University
Computer Science
Ola Flygt

2021-12-28

## C. YubiKey

Each group get one YubiKey 5 NFC. You should test using it to authenticate in different situations. Test each scenario and note how much effort it requires to setup and use. In what situations do they work? Also think about how secure it is. Can you come up with some ways to attack it?

The Scenarios you should test are:

- Login in to some Microsoft service (like Outlook.com, Skype or Onedrive) on a laptop
- Login to a Google service (like Gmail or Google drive) on a laptop
- Test the app Yubikey Authenticator on a mobile device supporting NFC to authenticate on some service
- Use the YubiKey to login to Windows on a laptop

## D. Two-Factor authentication

Every group will be doing two-factor authentication. You should implement a system using two-factor authentication. The authentication should allow you access to one of the computers in the lab and preferably also access to the inside network, either using VPN and/or accessing the trusted wireless network.

One of the factors you should use is something you carry with you (hardware token) e.g. a mobile phone (e.g. using Bluetooth technology) or a USB memory stick containing special software and/or authentication hardware. Other hardware tokens might be possible, discuss ideas with the TA. The second factor can be something you know or a biometric method. You can select methods in the groups, but two groups cannot choose the same combination of factors! Check in MyMoodle for availability of methods and add your group when you have decided!

Extra credits the more general your solution works (wireless access, VPN, wired etc).

Each group should make a proper documentation of their research on both part B, C and D and share this with all teachers. Submit at latest 7 January.