BAB I
PENDAHULUAN

1.1. Latar Belakang

Kata sandi adalah metode yang paling umum dan paling murah digunakan dalam otentikasi terutama web. Namun, otentikasi dengan kata sandi membuat banyak masalah terhadap proses otentikasi itu sendiri. Berdasarkan survei yang dilakukan oleh Hoonnaker, dkk. ke 836 karyawan dengan komposisi 3% *novice users*(baru menggunakan komputer), 69% *average users*(dapat menggunakan *word processors, spreadsheets,* email, browsing), 22% *advanced users*(dapat menginstall perangkat lunak, set up konfigurasi tertentu) dan 6% *expert users*(dapat menginstal OS, mengerti beberapa bahasa pemrograman), diketahui bahwa **94%** dari responden menyimpang dari satu atau lebih *best practices* penggunaan kata sandi [1].

Protokol otentikasi kata sandi sendiri sering kali tidak aman karena kata sandi dapat dicuri. Sering kali terjadi pembobolan basis data terutama pada server perusahaan yang keamanan datanya kurang kuat. Jika basis data terbobol, data pengguna beserta kata sandi didapatkan peretas. Banyak dari pengguna kata sandi menggunakan satu kata sandi yang sama berulang-ulang pada situs yang berbeda sehingga jika satu pengguna menggunakan kata sandi yang sama pada satu situs yang telah diretas, peretas dapat masuk ke seluruh akun korban tersebut dengan menggunakan kata sandi yang sama. Banyak pula serangan-serangan lain pada sistem otentikasi kata sandi yang tidak akan dibahas pada penelitian ini.

Permasalahan yang ada pada kata sandi ini sebenarnya sudah cukup terselesaikan dengan adanya konsep *Multi Factor Authentication* (MFA). Konsep MFA menggabungkan dua atau lebih faktor otentikasi yang terdiri dari tiga faktor yaitu *something you know* (SYK), *something you have* (SYH), dan *something you are* (SYA). Proses otentikasi dengan kata sandi saja termasuk ke dalam faktor SYK. Beberapa situs terkenal sudah banyak yang menerapkan otentikasi dengan dua faktor yaitu faktor SYK dan SYH dikarenakan teknologi SYA masih relatif jauh lebih mahal.

Adapun masalah yang timbul dari jenis MFA yang paling sering digunakan yang berupa SYK dan SYH, yaitu tetap menggunakan faktor SYK dalam proses

otentikasi. MFA hanya mengubah faktor SYK dari yang harus panjang dan kompleks menjadi lebih singkat tetapi tetap tidak mengubah kenyataan bahwa pengguna harus tetap mengingat kata sandi tersebut. Walau terlihat sebagai tugas yang lebih mudah tetapi pengguna harus tetap mencari kata sandi yang diinginkan dari berbagai kata sandi yang diketahui dan pernah digunakan.

Salah satu contoh penggunaan faktor kedua MFA yang sering digunakan sekarang adalah *One Time Password* (OTP). OTP sendiri prosesnya relatif panjang dan memerlukan banyak waktu untuk melakukan otentikasi. Selain melakukan input kata sandi utama, pengguna diharuskan untuk menunggu (contoh: SMS/email OTP), membuka aplikasi (contoh: Google Authenticator), atau menekan tombol (contoh: token bank) untuk mendapatkan OTP yang nantinya harus diingat sementara atau dicatat dan diketikkan lagi ke sistem. Proses ini relatif memerlukan waktu yang lama dan waktu pembelajaran yang relatif tidak singkat. Selain itu, walaupun OTP memperkuat sisi *security* tetapi tidak menutup fakta bahwa OTP tetaplah sebuah *password* sehingga masih dapat dilakukan serangan *phishing*.

Penggunaan kartu NFC sekarang sedang gencar didukung oleh semakin maraknya metode pembayaran cashless, produsen smartphone semakin gencar memproduksi smartphone dengan NFC. Diperkirakan 64% smartphone di dunia memiliki teknologi NFC pada tahun 2018 [2]. Dengan demikian, penulis yakin bahwa sebagian besar orang akan memiliki dan menggunakan teknologi NFC dengan semakin intensif di masa yang akan datang. Oleh karena itu, kartu NFC dirasa sangat cocok oleh penulis untuk dijadikan faktor SYH kedua.

Protokol *2fysh* (*two factor you should have)* dikembangkan pada skripsi ini menggunakan dua faktor SYH yang berupa ponsel dan kartu RFID/NFC dengan metode yang lebih aman dari pada kata sandi. Terdapat juga faktor SYK atau SYA yang berupa pengaman pada ponsel tetapi hal ini tentatif tergantung masing-masing pengguna dan dibutuhkan sosialisasi untuk pengamanan ekstra ini. Faktor SYH kedua yaitu kartu NFC didasarkan atas penggunaannya semakin luas terutama di Indonesia. Kartu NFC digunakan pada universitas untuk absen, pada uang elektronik untuk pembayaran, pada perusahaan untuk akses masuk gedung, dan sebagainya. Sehingga hal ini membuat *2fysh* dirancang terutama untuk pengguna yang sudah mengerti komputer sampai dengan tahap *average* dan relatif sering / mengerti penggunaan kartu NFC seperti mahasiswa dan karyawan.

1.2. Rumusan Masalah

Berdasarkan dari latar belakang dapat di rumuskan masalahnya menjadi poin-poin berikut :

1. Bagaimana merancang sebuah protokol otentikasi pengganti kata sandi yang ramah pengguna?
2. Bagaimana merancang sebuah protokol otentikasi pengganti kata sandi yang aman?
3. Bagaimana mengimplementasikan protokol tersebut ke dalam sebuah purwarupa?

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan dari penelitian ini adalah:

1. Merancang protokol otentikasi pengganti kata sandi yang ramah pengguna;
2. Merancang protokol otentikasi pengganti kata sandi yang aman; dan
3. Mengimplementasikan protokol tersebut ke dalam sebuah purwarupa

1.4. Batasan Masalah

Batasan masalah adalah sebagai berikut:

1. Penelitian hanya akan berfokus pada sistem otentikasi web.
2. Pengujian purwarupa protokol hanya mencakup aspek keamanan dan kebergunaan saja.
3. Pengujian aspek keamanan protokol dilakukan dengan cara studi literatur saja. Uji keamanan langsung (*penetration testing*) bukan merupakan fokus penelitian.
4. Perancangan purwarupa hanya berfokus pada otentikasi, sistem server untuk penulisan data ke dalam kartu tidak termasuk fokus penelitian.
5. Perancangan purwarupa tidak dirancang untuk benar-benar sempurna agar dapat tahan dari serangan jenis apa pun. Purwarupa dibuat hanya untuk keperluan penelitian saja.

1.5. Manfaat Penelitian

Hasil dari penelitian dapat menjadi acuan untuk mengimplementasikan alternatif protokol otentikasi web *2fysh* yang lebih aman dan lebih ramah pengguna dengan menggunakan ponsel Android dan kartu RFID/NFC.