Review: Keamanan Kata Sandi

Tohari Ahmad
Teknik Informatika – ITS
Kampus ITS, Sukolilo Surabaya
E-Mail: tohari@if.its.ac.id

Abstrak

Penggunaan kata sandi (*password*) sebagai alat untuk melakukan otentikasi telah banyak digunakan dalam berbagai macam aplikasi, mulai dari yang sederhana sampai dengan yang kompleks. Dalam *single modal authentication*, keamanan suatu aplikasi sangat tergantung pada keamanan kata sandi itu sendiri. Akan tetapi, kata sandi ini sering menjadi titik terlemah dari suatu aplikasi dikarenakan penerapan kata sandi yang tidak tepat. Pada makalah ini, kami akan mendeskripsikan permasalahan-permasalahan otentikasi, kelemahan dan ancaman terhadap kata sandi dan kemungkinan solusi yang bisa digunakan untuk mengatasi kelemahan dan ancaman tersebut. Dalam hal ini, permasalahan-permasalahan yang dihadapi adalah berhubungan dengan tingkat ketidakpastian (*entropy*) dan seberapa sering kata sandi tersebut digunakan (*frequency of uses*). Serangan terhadap kerahasiaan kata sandi bisa berupa *cracking* (memecahkan kata sandi dengan menggunakan *tools* yang ada), atau pun *stealing* (mengambil kata sandi yang tersimpan dalam *storage* atau *transmission channel*). Makalah ini juga menambahkan satu faktor penting dalam manajemen kata sandi yang bisa digunakan untuk mengatasi permasalahan-permasalahan tersebut, yaitu faktor lingkungan. Ini adalah sebagai pelengkap dari beberapa faktor yang telah dikenal sebelumnya, yaitu: pengguna (manusia), proses dan teknologi.

Kata kunci: kata sandi, keamanan, otentikasi

Abstract

The use of passwords in an authentication process has been applied in various applications, from a simple to complex one. In a single modal authentication, security of applications much relies on the security of the password itself. However, a password is often to be the weakest point in the systems because of its inappropriate use. In this paper, we will describe the authentication problems, vulnerabilities and threats against passwords along with their possible solutions .In this case, the authentication problems relate to the password's entropy level and its frequency of uses. Threats to the security of passwords can be cracking and stealing The former is about guessing the password by using any means while the later is obtaining the password from the storage or transmission channel. This paper also introduces an important factor in managing passwords,which can be used to solve those problems, namely: the environmental factor. This can be viewed as a complement to the existing factors: people (users), process and technology.

Key words: password, security, authentication

PENDAHULUAN

Survei yang telah dilakukan oleh CSI [1] menunjukkan bahwa hanya terdapat sekitar 8.7% responden yang mengalami permasalahan finansial yang diakibatkan oleh serangan elektronik dalam beberapa tahun terakhir. Meskipun angka ini menunjukkan penurunan dari periode sebelumnya, kerugian secara finansial yang diakibatkan masih cukup tinggi, yaitu bisa mencapai 25 juta dollar. Sehingga, perlindungan terhadap komputer dan informasi yang ada di dalamnya masih menjadi hal yang penting.

Sebagai salah satu prinsip penting dalam keamanan komputer, otentikasi (*authentication*) dapat menjadi target utama dari suatu serangan elektronik. Begitu otentikasi bisa dilemahkan, prinsip-prinsip keamanan yang lain, misalnya kerahasiaan (*confidentiality*), integritas (*integrity*) data akan sangat mungkin menjadi target berikutnya. Dalam hal ini, otentikasi telah menjadi faktor yang sangat penting dalam *defense in depth approach* [2], selain integritas dan kerahasiaan. Lebih khsus lagi, kata sandi (*password*) adalah rawan untuk diserang, baik karena faktor internal (kelemahan kata sandi itu sendiri) dan eksternal (serangan yang dilakukan oleh pihak lain). Sehingga, dari segi keamanan informasi, proses otentikasi harus mendapatkan prioritas.

Proses otentikasi di dalam suatu jaringan komputer adalah lebih rawan diserang daripada yang ada di komputer yang berdiri sendiri (*stand alone)* karena terdapat lebih banyak titik (mesin/komputer) yang tersedia untuk melakukan serangan. Terlebih lagi, kata sandi itu sendiri mungkin dikirimkan dari satu komputer ke komputer lain, yang bisa diduplikasi dalam prosesnya.

Beberapa mekanisme telah diperkenalkan untuk meminimalisir penggunaan kata sandi, artinya, jumlah titik lemah yang bisa menjadi target serangan juga berkurang. Misalnya, *federated identity management* yang telah diaplikasikan dalam single sign on (SSO) [3, 4] seperti yang telah dibangun oleh Liberty Alliance Project [5]. Penggunaan kata sandi dalam jumlah yang lebih sedikit telah memudahkan pengguna (*user)* untuk mengaturnya. Namun demikian, bagaimana suatu kata sandi dibuat dan digunakan adalah tetap menjadi permasalahan yang harus diselesaikan dengan baik untuk melindungi keseluruahan proses otentikasi.

Dalam praktiknya, biaya yang diperlukan untuk membuat proteksi (dalam hal ini adalah otentikasi) terhadap suatu obyek tidak boleh melebihi nilai dari obyek yang akan dilindungi tersebut. Akan sangat tidak efisien untuk membuat suatu proses otentikasi yang kompleks untuk memprotek data yang bersifat umum dan bernilai rendah.

Meskipun kata sandi mempunyai beberapa permasalahan keamanan, implementasinya mungkin tidak dapat digantikan dalam jangka waktu dekat ini. Makalah ini mengidentifikasi faktor-faktor yang menentukan keamanan kata sandi dan kemungkinan langkah-langkah yang dapat dilakukan untuk menjaganya. Alernatif media otentikasi yang lain (misalnya biometrik) akan dibahas secara garis besar, disertai kelebihan dan kurangannya.

PERMASALAHAN OTENTIKASI

Kekuatan kata sandi dapat didefinisikan sebagai seberapa sulit kata sandi tersebut dapat dipecahkan, yang bisanya diukur dengan menggunakan tingkat *entropy*, meskipun dalam praktiknya, kesulitan untuk memecahkan suatu kata sandi juga ditentukan oleh banyak faktor, seperti seberapa sering kata sandi tersebut diubah, yang berarti pula seberapa sering suatu kata sandi digunakan.

Secara umum, faktor yang menentukan keamanan kata sandi dapat dikelompokkan menjadi: tingkat *entropy* (termasuk panjang kata sandi) dan seberapa sering digunakan (termasuk seberapa sering diubah). Terlepas dari kekuatannya, manajemen kata sandi, terutama dalam menghindari berbagi (*sharing*) kata sandi adalah penting dalam keamanan sistem otentikasi [17].

Ketidakpastian – Tingkat *Entropy*

Berdasakan teori Shanon [6] (dalam persamaan 1), semakin tinggi tingkat *entropy*, semakin tidak pasti (random) kata sandi tersebut.

$$H = -\sum_{i=1}^{n} p_i \log(p_i) \qquad (1)$$

Dimana H, n, dan p_i adalah entropy, nilai dengan probabilitas $p_1, p_2, ..., p_n$. Ini juga menunjukkan bahwa semakin tinggi jumlah kata sandi yang dapat dibentuk bisa

meningkatkan entropy. Hal ini dapat dicapai dengan:

- Menambah panjang kata sandi. Seperti yang ditunjukkan dalam [7] bahwa suatu kata sandi yang dibuat oleh 3, 6, dan 9 karakter dapat dipecahkan dalam waktu kurang dari 1 detik, 3 jam dan 70 tahun.
- Meningkatkan ukuran *domain space.* Suatu kata sandi yang disusun oleh 7 bit ASCII adalah lebih baik daripada kata sandi yang disusun oleh huruf dan angka saja atau huruf besar/kecil saja. Kata sandi-kata sandi yang tersusun atas kode karakter tersebut dapat dipecahkan dalam waktu 350 tahun, 1 tahun dan 9 jam [7].

Namun demikian, terdapat suatu timbal-balik dari dua faktor tersebut. Pertama, lebih panjang kata sandi akan memerlukan tempat yang lebih banyak untuk menyimpan. Meskipun memperpanjang kata sandi bisa mengurangi jumlah kata sandi yang terpecahkan[7, 8], tetap terdapat pertanyaan apakah kata sandi yang relatif panjang benar-benar diperlukan jika frekuensi menggunakan kata sandi yang salah sudah dibatasi [9]. Kedua, menambah ukuran ukuran *domain space*, bisa menghasilkan kata sandi yang lebih random, tetapi sulit diingat oleh pengguna[10]. Di sisi yang lain, pengguna lebih suka menggunakan kata sandi yang mudah diingat, misalnya kata ”password” dan kata-kata popular yang terdapat dalam kamus (*dictionary)* [11, 12].

Frekuensi penggunaan

Berdasarkan frekuensi penggunaannya, kata sandi dapat dikelompokkan menjadi dua bagian: *one time passwords (OTP)* dan *reusable passwords*, yang masing-masing bisa digunakan satu dan beberapa kali. Dalam hal ini, OTP adalah lebih aman karena informasi yang diperoleh darinya tidak bisa digunakan (sangat sulit) untuk memecahkan kata sandi yang lain.

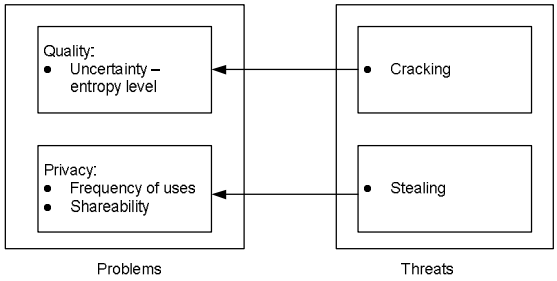
Berbagi (*Shareability*)

Permasalahan umum yang dihadapi oleh otentikasi dengan menggunakan sesuatu yang kita ketahui (misalnya kata sandi) atau sesuatu yang kita punyai (misalnya token/kartu identitas) adalah *shareability*, yaitu bagaimana mediumnya bisa digunakan oleh pengguna lain; sehingga, proses otentikasi mungkin tidak bisa membedakan mana pengguna yang asli dan mana yang tidak. Hal ini berarti bahwa proses yang ada tidak sesuai dengan prinsip *non-repudiation.* Sebuah survei[13] membuktikan bahwa sekitar 42% pengguna adalah tidak keberatan untuk membagi informasi kata sandinya kepada orang lain yang dipercaya. Hal ini menunjukkan bahwa berbagi informasi kata sandi adalah merupakan hal yang sudah relatif umum dipraktikkan.

Biometrik (sesuatu yang ada pada diri manusia) dapat menjadi salah satu solusi untuk permasalahan ini. Akan tetapi, biometrik juga menyebabkan permasalahan yang lain, misalnya, tingkat akurasinya masih dibawah kata sandi.

KELEMAHAN DAN ANCAMAN

Secara umum, ancaman terhadap kata sandi dapat dikelompokkan menjadi 2 grup, yaitu: *cracking* dan *stealing* [17]. Yang pertama adalah berhubungan dengan kualitas kata sandi (tingkat *entropy*), sedangkan yang kedua berhubungan dengan bagaimana pengguna menjaganya. Hal ini dapat dideskripsikan dalam gambar 1.



Gambar 1 Permasalahan kata sandi dan ancamannya

Cracking

Di satu sisi, informasi yang berhubungan dengan pengguna (misal: alamat, no telepon) mudah didapatkan. Di sisi yang lain, informasi ini sering digunakan sebagai kata sandi[14], yang sesungguhanya tingkat randomnya adalah sangat rendah. Tanpa menggunakn *tools* pun, kata sandi seperti ini mungkin bisa ditebak dengan mudah. Dengan kata lain, berdasarkan informasi yang berhubungan

dengan pengguna, kata sandi bisa dengan mudah ditebak.

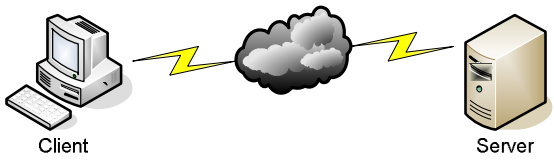
Metode yang lebih canggih bisa dilakukan dengan menggunakan *tools* baik perangkat keras maupun perangkat lunak. Hal ini bisa dilakukan dengan menggunakan *dictionary attack* atau *brute force attack*. Salah satu cara untuk menghindari serangan ini adalah dengan meningkatkan entropy dari kata sandi semaksimal mungkin.

Stealing

Terlepas dari kekuatannya, suatu kata sandi dapat dicuri, baik dilakukan secara teknis maupun secara non-teknis (misal dengan *social engineering)*.

Pendekatan teknis

Beberapa metode telah diperkenalkan untuk mendapatkan kata sandi, misalnya *password sniffing* dan *SQL injection*. Secara umum, kata sandi dapat diserang melalui beberapa titik seperti ditunjukkan dalam gambar 2: client, sever dan link antara keduanya.



Gambar 2 Komunikasi pada suatu jaringan komputer

Pada komputer *client*, suatu perangkat keras atau perangkat lunak bisa ditambahkan oleh penyerang untuk menangkap dan menganalisis kata sandi yang dituliskan oleh pengguna. Misalnya, *keystroke logger software* yang bisa merekam segala sesuatu yang pengguna tuliskan melalu *keyboard*. Meskipun beberapa metode sudah digunakan untuk mengantisipasinya (misalnya di [15]), tidak semuanya bisa benar-benar bisa melindungi kata sandi secara penuh. Dalam hal ini, *virtual-based password* lebih efektif untuk digunakan.

Dalam hal perlu mengirimkan kata sandi melalui jaringan, bisa dilakukan perlindungan dengan menerapkan algoritma enkripsi dan dekripsi. Namun demikian, penggunaan enkripsi juga mempunyai permasalahan yang lain, misalnya ukuran *key* yang digunakan dan juga distribusinya.

Pendekatan non-teknis

Seperti yang telah diketahui secara umum, pengguna bisa menjadi titik lemah dalam mekanisma keamanan data. Dalam hal ini, pengguna mungkin memberikan informasi kata sandinya secara tidak sengaja. Misalnya, mereka menuliskan kata sandinya pada suatu kertas dan meletakkannya di dekat komputer yang dipakainya sehingga mudah untuk dibaca. Hal lain yang mungkin terjadi adalah dengan melakukan *shoulder surfing* atau *masquarade attack.*

Shoulder surfing attack bisa dilakukan dengan memperhatikan apa yang pengguna tuliskan pada keyboard. Beberapa teknologi bisa digunakan untuk meminimalisir serangan ini, misalnya dengan tidak menampilkan sama sekali karakter kata sandi pada monitor ketika dituliskan pada keyboard, seperti yang sudah diterapakan pada UNIX; teknologi *eye-gaze* untuk kata sandi berbasis grafis[16] dan sebagainya.

Kata sandi bisa juga didapatkan dengan bertindak seolah-olah sebagai pengguna yang sebenarnya. Hal ini lebih mudah dilakukan jika informasi tentang pengguna telah didapatkan.

MANAJEMEN KATA SANDI

Dari pembahasan sebelumnya, permasalahan terhadap manajemen kata sandi dan keamanannya dapat dikelompokkan menjadi empat kategori, dimana tiga diantaranya telah didefinisikan di [17]. Empat kategori tersebut adalah:

- pengguna (*people*)
- teknologi (*technology*)
- proses (*process*)
- lingkungan (environment)

Hal ini bisa dijelaskan sebagai berikut. Manajemen kata sandi melibatkan pengguna yang menerapkan teknologi dengan mengikuti proses yang telah ditetapkan dalam suatu kebijakan keamanan (*security policy)*; keseluruhan proses ini dapat berjalan baik jika

semua hal yang terlibat di dalamnya dapat menyediakan dukungan satu sama lain dalam lingkungan yang baik. Dalam praktiknya, "proses" menjadi faktor utama dalam manejemen kata sandi. Keamanan kata sandi dapat dijaga selama semua hal yang berhubungan dengan manajemen kata sandi ini telah dideskripsikan secara detail dan diikuti oleh semua pihak dengan konsisten.

Faktor pengguna (*people*), seperti yang sudah didiskusikan pada bagian sebelumnya adalah berhubungan erat dengan faktor lingkungan dimana pengguna menghabiskan sebagaian besar waktunya. Lingkungan yang sesuai sangat dimungkinkan untuk memberikan efek yang positif terhadap manajemen kata sandi ini. Hal ini karena sumber daya yang diperlukan untuk mengimplementasikan *security policy* telah tersedia.

Terlebih lagi, pengguna yang telah mempunyai pengetahuan (*knowledge)* dan kesadaran (*awareness)* terhadap ancaman keamanan komputer dan pengaruhnya, dapat membangun lingkungan yang lebih baik. Mereka bisa mengingatkan satu sama lain jika terdapat hal-hal yang bisa mengancam keamanan data.

KESIMPULAN

Dari permasalahan-permasalahan yang telah dideskripsikan sebelumnya, terdapat beberapa hal yang perlu diperhatikan untuk menjaga keamanan kata sandi. Hal-hal tersebut menjadi topik penelitian selanjutnya, yang dapat dijelaskan sebagai berikut.

Sesuai dengan karakteristiknya, pengguna dapat menjadi titik terlemah di dalam proses otentikasi. Survei telah menunjukkan bahwa kelemahan ini tidak dikarenakan pengguna tersebut tidak mengetahui apa dan bagaimana kata sandi yang baik, akan tetapi dikarenakan pengguna lebih menyukai kenyamanan *(convenience*) daripada kemanan (*security*) itu sendiri. Seperti yang telah diketahui, bahwa convenience berbanding terbalik dengan security. Satu hal penting yang perlu dilakukan adalah membuat pengguna mempunyai kesadaran tentang ancaman keamanan komputer dan pengaruhnya terhadap mereka, baik secara langsung atau tidak langsung.

Di antara faktor-faktor yang telah teridentifikasi, pengguna (*people*) sebenarnya hanyalah salah satu di antara empat faktor yang ada, yaitu: pengguna, proses, teknologi dan lingkungan. Untuk meminimalisir kekurangannya, faktor-faktor yang lain, terutama faktor "proses", harus dioptimalkan penerapannya.

Penggunaan biometrik sebagai media otentikasi diharapkan dapat menyediakan keamanan dan kenyamanan secara bersamaan terhadap pengguna. Hal ini dapat memudahkan pengguna untuk melakukan proteksi data dan melakukan otentikasi. Lebih khusus lagi, ini dapat digunakan untuk memenuhi prinsip kerahasiaan (*confidentiality),* tidak adanya penyangkalan (*non-repudiation*), dan kesederhanaan (*simplicity*). Namun demikian, tingkat akurasi dari biometrik tidak setinggi kata sandi, dikarenakan adanya perbedaan data yang bisa diambil dalam waktu yang berbeda.

DAFTAR PUSTAKA

[1] Richardson R. 2010 / 2011 CSI Computer Crime and Security Survey. CSI Computer Security Institute, 2011.

[2] Talbot D.; Bishop M. Demythifying Cybersecurity. IEEE Security & Privacy, 8:56-59. 2010.

[3] Landau S., Gong H. L. V., dan Wilton R. Achieving Privacy in a Federated Identity Management System. LNCS, 5628:51-70. 2009.

[4] Alsaleh M. dan Adams C. Enhancing Consumer Privacy in the Liberty Alliance Identity Federation and Web Services Frameworks. LNCS. 4258:59-77. 2006.

[5] Liberty Alliance Project. 2012 (URL:http://www.projectliberty.org/).

[6] Verdu S. Fifty Years of Shannon Theory. IEEE Transactions on Information Theory. 44: 2057-2078. 1998.

[7] AusCERT. Choosing Good Passwords. 2012: AusCERT (Australian Computer Emergency Response Team). http://www.auscert.org.au/render.html?it=2260. 2009.

[8] Weir M., Aggarwal S., Collins M., dan Stern H. Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. 17th ACM conference on Computer and communications security. 2010.
[9] Schaffer K. Are Password Requirements too Difficult? IEEE Computer. 44:90-92. 2011.
[10] Vua K.-P. L., Proctorb R. W., Bhargav-Spantzelb A., Taib B.-L. B., Cookb J., dan Schultzc E. E. Improving Password Security and Memorability to Protect Personal and Organizational Information. International Journal of Human-Computer Studies. 65: 744–757. 2007.
[11] Prabhakar S., Pankanti S., dan A. Jain. Biometric Recognition: Security and Privacy Concerns. IEEE Security & Privacy. 1:33-42. 2003.
[12] Jain A. K., Ross A., dan Pankanti S. Biometrics: A Tool for Information Security. IEEE Transactions on Information Forensics and Security. :125–143. 2006.
[13] Tam L., Glassman M., dan Vandenwauver M. The Psychology of Password Management: A Tradeoff between Security and Convenience. Behaviour & Information Technology.29:233-244. 2010.
[14] Bishop M. Introduction to Computer Security. Boston, MA: Pearson Education. 2005.
[15] Nasaka K., Takami T., Yamamoto T. dan Nishigaki M. A Keystroke Logger Detection Using Keyboard-Input-Related API Monitoring. 14th International Conference on Network-Based Information Systems. 2011.
[16] Forget A., Chiasson S., dan Biddle R. Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords. 28th International Conference on Human Factors in Computing Systems. 2010.
[17] Ahmad T. Password Security: An approach to Mitigate Cyber Crimes. 3rd Information and Communication Technology Seminar. 2007.