Analisa Sistem Keamanan *Online Password Manager* LastPass

Ramda Yanurzha
13506011
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
13506011@students.if.itb.ac.id / ramda.yz@gmail.com

LastPass adalah sebuah online password manager yang bertujuan untuk menyimpan berbagai password ke dalam sebuah user *account* yang diamankan dengan sebu*ah master password*.

Dengan adanya LastPass, user hanya perlu mengingat master password untuk dapat login ke berbagai layanan dan website tanpa perlu menghafal detail *account* masing-masing. Kemampuan ini diterapkan secara online, sehingga user dapat mengakses password yang disimpan dari manapun dan tak terbatas hanya dari komputer pribadi saja. Hal ini menyebabkan perlunya sistem keamanan yang kompleks untuk menjaga konfidensi data user dari pihak yang tidak bertanggung jawab.

Dalam makalah ini penulis akan membahas tentang sistem keamanan LastPass dan keputusan yang diambil dalam pembuatannya serta menganalisa kelemahan yang mungkin ada pada software tersebut.

***Index Terms*— AES, browser add-on, CBC, enkripsi, hash salt, LastPass, password manager, multi-factor authentication, rainbow table**

I. PENDAHULUAN

1.1 Latar Belakang

Pada era serba online sekarang ini, pengguna internet mengalami pertumbuhan secara konstan. Pertambahan ini disebabkan oleh semakin berkembangnya teknologi informasi dan telekomunikasi yang menyebabkan tingginya aksesibilitas masyarakat terhadap layanan dan konten berbasis online. Perkembangan alat telekomunikasi seperti smartphone dan komputer portabel terjadi dalam bentuk pengaksesan internet yang lebih mudah dan cepat. Faktor-faktor di atas menyebabkan banyaknya website atau layanan online yang memerlukan pembuatan *account* untuk personalisasi user sehingga dapat memberi layanan yang lebih baik. Kebanyakan dari mereka membutuhkan data user yang kemudian dilindungi oleh sebuah username dan password.

Walaupun begitu, hal sederhana ini berubah menjadi kompleks karena banyaknya layanan yang tersedia dan masing-masing memiliki persyaratan yang berbeda-beda. Sebagai contoh, sebuah *account* mungkin diasosiasikan dengan sebuah alamat e-mail pribadi, sedangkan *account* lainnya menggunakan alamat e-mail bisnis. Untuk alasan keamanan, setiap *account* mungkin memiliki ketentuan password yang berbeda-beda. Sebagai contoh, pendaftaran sebuah layanan membutuhkan password sepanjang 6 karakter, sedangkan sebuah layanan perbankan online membutuhkan 10 karakter yang terdiri dari huruf kapital dan angka. Untuk alasan yang sama pula, sangat tidak dianjurkan untuk menggunakan password yang sama dalam dua *account* yang berbeda. Hal ini untuk mencegah terkomprominya data pribadi pada berbagai *account* sekaligus jika salah satunya disalahgunakan oleh pihak yang tidak berwenang. Akan sangat berbahaya jika *account* yang penting seperti e-mail bisnis diakses oleh pihak tersebut.

Oleh karena itu, muncul solusi berupa password manager, yaitu software yang dapat menyimpan kumpulan data login berbagai *account* ke dalam sebuah basis data yang dilindungi oleh sebuah master password. Dengan ini, kumpulan data tersebut menjadi lebih aman dan password dapat dibuat menjadi sekompleks mungkin tanpa harus dihapal secara manual. Metode ini dipilih oleh banyak pengguna internet yang menggunakan banyak layanan sekaligus dan ingin kepraktisan dengan tidak harus membuat password yang sulit dihapal untuk setiap *account*.

1.2 Tentang LastPass

LastPass adalah sebuah software *password manager* berbasis online. Software ini tersedia sejak tahun 2009 dan saat ini tersedia dalam 2 versi, freeware untuk penggunaan personal dan berbayar (LastPass Premium) untuk keperluan enterprise dengan fitur-fitur kemanan tambahan. LastPass tersedia juga dalam berbagai bahasa. LastPass terpasang dalam bentuk plugin atau add-on untuk 5 browser modern, yaitu Microsoft Internet Explorer, Mozilla Firefox, Opera, Apple Safari, dan Google Chrome. User juga dapat menambahkan password secara manual dengan mengakses portal web mereka (http://www.lastpass.com). Versi premium LastPass juga menyediakan fungsinya dalam bentuk

mobile application untuk digunakan di tablet device maupun smartphone dengan platform Apple iOS, Android, Symbian S60, HP WebOS, RIM Blackberry, Windows Mobile, Windows Phone, dan browser mobile seperti Dolphin atau Firefox Mobile. Berikut adalah fitur-fitur yang juga disediakan oleh versi freeware LastPass:

1. *Automatic Form Filling*
   LastPass dapat mengisi formulir pendaftaran layanan online dengan data yang sudah disediakan sehingga menghemat waktu

2. *One-click Login*
   Untuk melakukan login, user yang sudah terautentifikasi hanya perlu mengklik sebuah tombol pada browser dan tidak perlu mengetikkan password dan username secara manual

3. *Multi Identities*
   LastPass dapat menyimpan kumpulan data login menjadi beberapa set identitas jika diperlukan

4. *Universal Access*
   Data *account* dapat diakses dari mana saja melalui browser

5. *Password Sharing*
   User dapat memberi password kepada user lain melalui media yang aman

6. *Password Generation*
   LastPass dapat membantu membuat password kompleks dengan aturan yang sudah ditentukan

7. *Keylogger Protection*
   LastPass memiliki berbagai proteksi untuk melindungi user dari *keylogger* yang dapat merekam karakter yang diketikkan di keyboard oleh user.

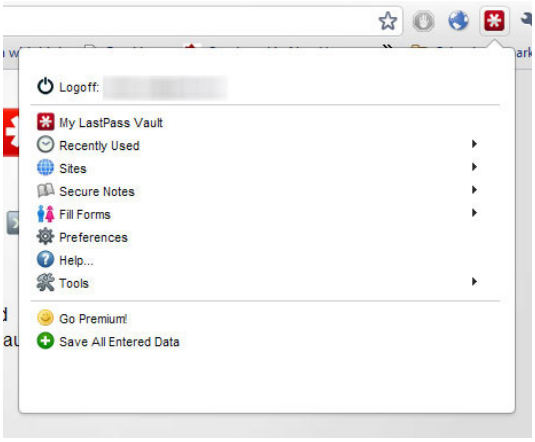
LastPass versi premium menambahkan akses mobile application dan opsi untuk *menambahkan multi-factor authentication*, yaitu penggunaan media lain sebagai pengaman tambahan.

II. PEMBAHASAN UMUM

2.1. Cara Penggunaan

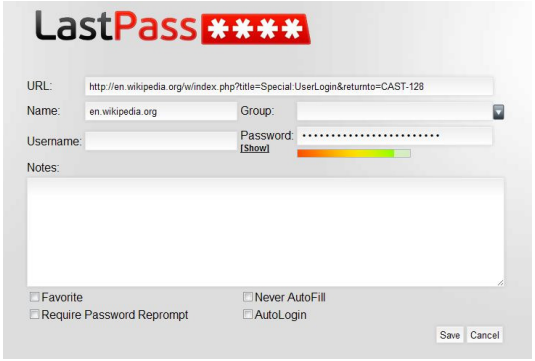
Berikut ini adalah cara penggunaan software LastPass versi *add-on* browser:

1. Menginstal *add-on* browser dari website LastPass (http://www.lastpass.com)
2. Mendaftar *account* LastPass dan membuat master password
3. Ketika user mengakses website yang memerlukan login, LastPass akan menawarkan opsi untuk menyimpan data login tersebut



Gambar 1 : Dialog LastPass pada add-on Chrome

4. Jika user menyetujuinya, maka LastPass akan memunculkan dialog yang berisi informasi login dan data lain seperti tingkat keamanan password, pemberian label, dan opsi pengisian otomatis



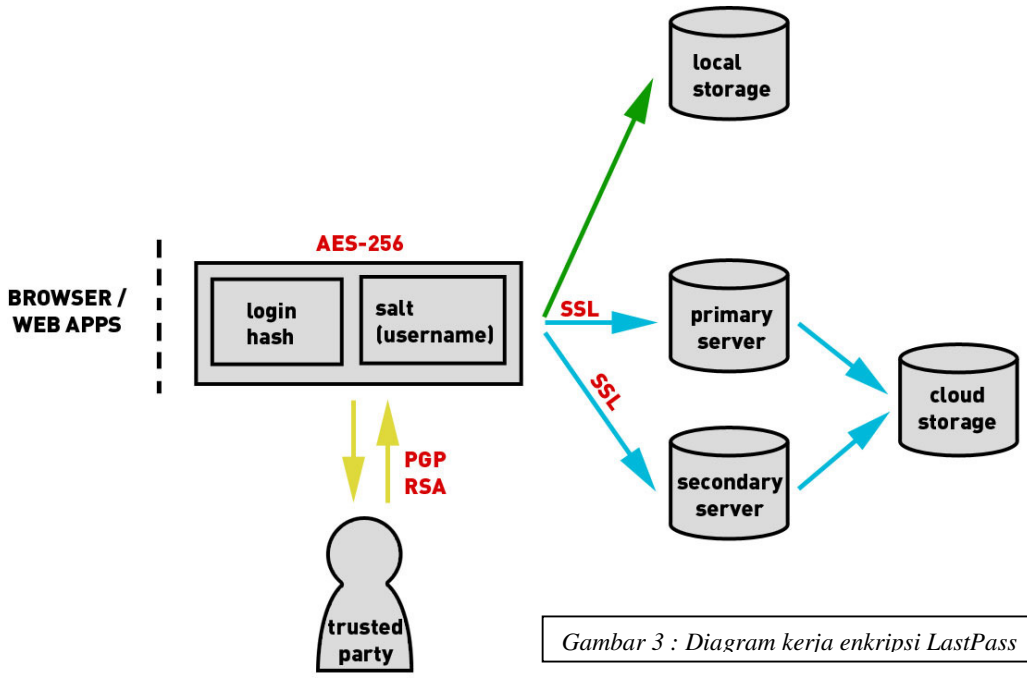
Gambar 2: Dialog penambahan data login

5. LastPass menyimpan data tersebut ke dalam dua tempat: lokal dan *off-site* berupa server LastPass
6. Selanjutnya, jika user mengunjungi website tersebut, user hanya perlu mengklik tombol add-on LastPass untuk melakukan login. User juga dapat mengaksesnya dengan melakukan login pada website LastPass
7. User juga dapat melakukan langkah di atas secara manual

2.2. Cara Kerja

Begitu user memilih untuk menyimpan data di LastPass, berikut adalah hal yang dikerjakan oleh software:

1. Setiap field login yang disimpan akan dijadikan *one-way salted hash* dengan metode enkripsi AES



Gambar 3 : Diagram kerja enkripsi LastPass

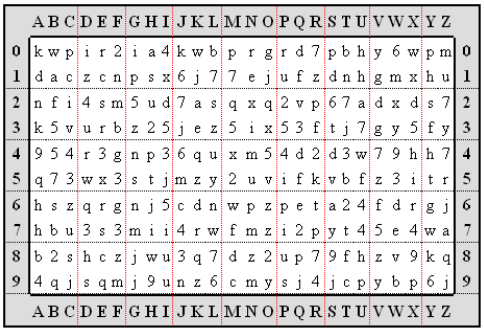
256-bit oleh library enkripsi berbasis C++ (untuk add-on) dan Javascript (untuk browser). Salt yang digunakan adalah username pada login tersebut

2. Hash tersebut disimpan ke dalam dua jenis media penyimpanan : sebuah basis data lokal terenkripsi dan dua buah server LastPass melalui koneksi SSL (Secure Socket Layer) untuk keperluan redundansi dan keamanan koneksi
3. Hash yang dikirimkan akan disimpan ke dalam server LastPass dan dibungkus lagi dalam sebuah hash dan salt dengan metode enkripsi AES 256-bit
4. Data tersebut kemudian dibackup ke dalam layanan *cloud service* Amazon S3 secara berkala
5. Untuk keperluan sharing password, digunakan metode kunci-simetri yaitu GPG (GNU PGP) yang diaplikasikan melalui library Crypto++ dengan enkripsi RSA 128-bit

2.3 Fitur Keamanan Tambahan

Selain proteksi terhadap Trojan dan *keylogger*, LastPass versi premium juga menyediakan metode two-factor authentication (TFA). Metode ini dipakai jika user merasa tidak aman, misalnya jika menggunakan computer public yang mungkin sudah disisipi program yang bertujuan untuk merekam input user. Metode TFA menggunakan dua bagian bukti identitas untuk melakukan verifikasi entitas user. Dua bagian ini pada umumnya adalah sesuatu yang user ketahui (PIN, password) dan sesuatu yang user miliki (ID card, token). LastPass menyediakan 3 metode berbasis TFA:

1. Grid
   Juga tersedia dalam versi freeware, Grid adalah metode yang memungkinkan user untuk mencetak sebuah set yang terdiri dari 260 koordinat dan respon. LastPass akan meminta 4 respon dari koordinat yang diberikan untuk melakukan verifikasi



Gambar 4 : Grid

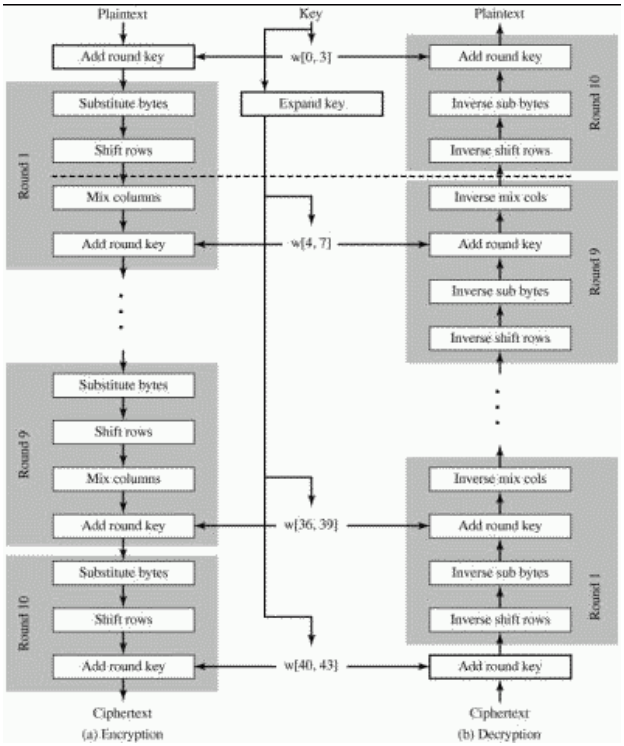
2. Sesame
   Sesame adalah nama fitur LastPass untuk menjadikan sebuah USB flash drive sebagai token TFA

3. Yubikey
   Yubikey adalah sebuah *device* USB yang memberikan *one-time passcode* untuk autentifikasi. Passcode tersebut dienkripsi dengan metode enkripsi AES 128-bit.

III. PEMBAHASAN ENKRIPSI

3.1 AES

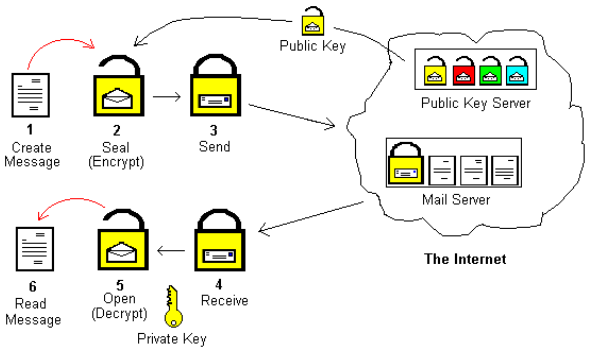
AES (Advanced Encryption Standard) adalah standar enkripsi kunci-simetri block-cipher yang diadopsi oleh pemerintah Amerika Serikat. Digunakan secara resmi sejak tahun 2002, AES dibuat berdasarkan prinsip desain Substitution permutation network. Tergantung tipenya, AES mempunyai ukuran kunci 128, 192, atau 256 bit dan ukuran block tetap sebesar 128 bit. Cipher AES didefinisikan sebagai sebuah jumlah repetisi transformasi yang mengubah input plaintext menjadi output ciphertext. Setiap tahap transformasi terdiri dari beberapa proses, termasuk salah satu yang bergantung pada kunci enkripsi. Walaupun AES memiliki requirement hardware dan software untuk proses enkripsi dan dekripsinya, besarnya block dan key (sampai 256 bit) menyebabkan sangat sulitnya serangan untuk memecahkan enkripsi AES. Dengan kombinasi 2^{256}, diperlukan waktu yang sangat lama walaupun menggunakan komputer tercepat saat ini sekalipun. LastPass menggunakan varian AES-256.



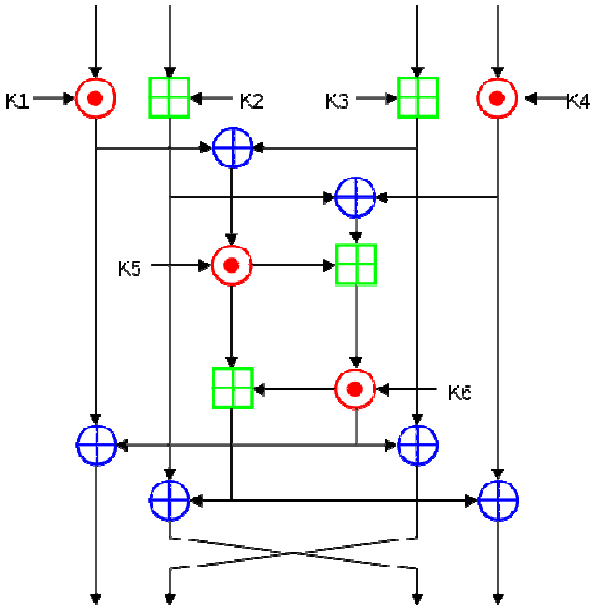
Gambar 5 : Diagram enkripsi AES

3.2 PGP

PGP (Pretty Good Privacy) adalah software yang digunakan untuk mengenkripsi dan mendekripsi data, umumnya digunakan dalam kasus digital signature e-mail. PGP menggunakan sebuah varian sistem *public key*, dimana setiap user mempunyai *public key* dan *private key*. PGP tersedia dalam dua variasi, RSA (Rivest-Shamir-Adleman) yang menggunakan algroitma IDEA berbasis hash MD5 dan Diffie-Hellman yang menggunakan algoritma CAST berbasis SHA-1. Setiap versi PGP mempunyai spesifikasi yang berbeda-beda, namun pada prakteknya setiap algoritma yang digunakan tidak memiliki kelemahan kriptoanalisis. Dalam pengaplikasiannya, LastPass menggunakan varian RSA dari library Crypto++ (C++) dan jsbn (Javascript).



Gambar 6 : Prinsip kerja PGP

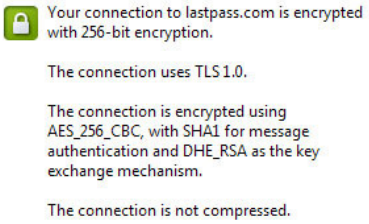


Gambar 7 : Diagram enkripsi IDEA

3.3 SSL

SSL (Secure Socket Layer) adalah protocol kriptografis yang menyediakan kemanan komunikasi melalui internet. SSL melakukan enkripsi segmen komunikasi dengan menggunakan kriptografi simetris. SSL biasanya diimplementasikan diatas protocol transport layer, misalnya HTTPS. Sejak dikembangkan tahun 1995, SSL (dan penerusnya TLS) sudah mencapai versi 3.3 (TLS 1.2) dengan metode enkripsi SHA-256.

Website LastPass sendiri menggunakan TLS 1.0 dengan enkripsi AES-256 yang mencakup enkripsi SHA1 untuk *message authentication* dan RSA untuk *key exchange*.



Gambar 8 : Informasi penggunaan protokol SSL

IV. ANALISA

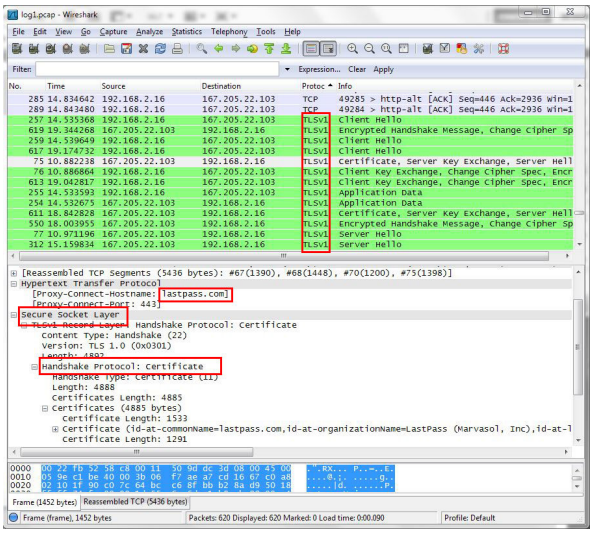
4.1 Analisa Umum

Dengan menggunakan enkripsi berlapis dengan tingkat kekompleksan yang tinggi seperti AES-256, sistem keamanan LastPass memiliki derajat keamanan yang sangat tinggi. Pengiriman data melalui protokol HTTPS juga menjamin bahwa data yang sudah terenkripsi dikirim melalui saluran yang terenkripsi pula.

Selain melalui *code review* internal, pihak LastPass juga menggunakan beberapa software off-the-shelf seperti Paros (www.parosproxy.org) untuk menganalisa kelemahan web application terhadap serangan seperti XSS (cross site scripting) atau SQL injection. Performa software juga dianalisa menggunakan tool Funkload dan dimonitor menggunakan software Nagios (www.parosproxy.org).

4.2 Analisa Koneksi

Salah satu komponen penting dari LastPass adalah penggunaan koneksi SSL untuk pengiriman hash data login ke server. Dengan menggunakan software WireShark untuk menganalisa paket data yang dikirimkan melalui interface network, penulis mengkonfirmasi bahwa LastPass, baik melalui website maupun add-on browser, menggunakan protokol TLS untuk transportasi data. Dengan kompleksitas enkripsi 256-bit, akan sangat sulit mendekripsi paket data yang sebenernya sudah terenkripsi saat terkirim.



Gambar 9 : Penggunaan WireShark

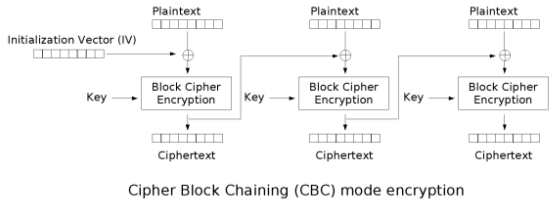
4.3 Analisa Antarmuka

Antarmuka memegang peranan yang penting, karena sebuah sistem yang aman sekalipun terkadang memiliki titik lemah di bagian yang berfungsi sebagai interface kepada user. Dalam hal ini, LastPass memiliki satu kelemahan yaitu kebanyakan user masih melakukan input data melalui keyboard yang rentan terhadap serangan *keylogger*. Walaupun begitu, hal ini tidak berkaitan dengan enkripsi yang digunakan LastPass yang tidak memiliki kelemahan kriptoanalisis.

4.4 Analisa Penggunaan Enkripsi

Penulis menemukan suatu kelemahan yang secara teori mempermudah penyerangan kriptografis pada database lokal LastPass, yaitu penggunaan salt berupa username. Berdasarkan keterangan dari produsen LastPass, software tersebut menggunakan salt dalam membuat hash terenkripsi data login. Hal ini tidak dianjurkan, karena pemakaian salt yang sama akan memberi hasil yang sama pada dua buah hash yang sama. Salt (pemberian nilai acak) dilakukan agar penyerang kesulitan ketika menggunakan metode serangan Rainbow Table, yaitu set nilai hash yang sudah terkomputasi dalam jumlah yang sangat besar untuk melakukan dekripsi sebagai trade-off dari tenaga komputasi. Salt memberikan perlindungan tambahan karena jika diberi maka Rainbow Table akan berukuran terlalu besar untuk digunakan secara praktis. Secara psikologis kebanyakan user memiliki username yang sama di beberapa *account* berbeda sehingga mengurangi keefektifan salt. Seharusnya setiap *account* memiliki salt rahasia yang berbeda pula sekalipun memiliki username dan password yang sama. Menurut database CWE (Common Weakness Enumeration), hal ini termasuk kategori CWE-329 yaitu tidak digunakannya random initialization vector (IV) dalam cipher block

chaining (CBC).



Gambar 10 : Prinsip Cipher Block Chaining

Walaupun begitu, fakta ini tidak bisa dikonfirmasi oleh penulis karena tidak ada keterangan apakah hash tersebut hanya diberi salt berupa username saja dan tidak dengan salt yang digenerasi secara acak. Pemberian hash dan salt dan bertumpuk akan membuat usaha penyerangan kriptografis semakin sulit. Untuk mengkonfirmasi hal ini, diperlukan source code yang tentunya tidak tersedia. Penggunaan random password generator yang tersedia di semua versi LastPass dinilai cukup untuk menutupi kekurangan ini. Untuk saat ini, ukuran Rainbow Table yang diperlukan untuk memecahkan enkripsi AES-256 tanpa salt adalah $3.06499108 \times 10^{54}$ byte. Menggunakan *Lenstra & Verheul Updated Equations*, enkripsi kunci-simetri 256-bit dianggap aman sampai tahun 2282. Saat ini terdapat beberapa teori serangan terhadap AES, namun belum ada yang mencapai level praktikal.

V. KESIMPULAN

Software LastPass memiliki sistem keamanan yang sangat baik dan aman sampai jangka waktu yang cukup lama dengan kemajuan teknik kriptografi saat ini melalui penggunaan enkripsi 256-bit yang berlapis, koneksi SSL, dan tersedianya opsi two-factor authentication.

REFERENSI

[1] Munir, Rinaldi. Bahan Mata Kuliah Kriptografi IF3058. 2011.

[2] Arief, Raditya. Analisis Perbaikan Keamanan Algoritma Enkripsi AES sebagai standar enkripsi baru dibandingkan DES. 2010.

[3] Birkuyov, Alex. et.al. Distinguisher and Related-Key Attack on the Full AES-256. August 2009.

[4] Birkuyov, Alex. et.al. Related-key Cryptanalysis of the Full AES-192 and AES-256.

[5] LastPass : Technology, *http://lastpass.com/whylastpass_technology.php.*

[6] LastPass: Is it the password manager for you? : Interview with Joe Siegrist, *http://www.techrepublic.com/blog/security/lastpass-is-it-the-password-manager-for-you/3291*

[7] Pretty Good Privacy, *http://en.wikipedia.org/wiki/Pretty_Good_Privacy*.

[8] CWE-329: Not Using a Random IV with CBC Mode, *http://cwe.mitre.org/data/definitions/329.html.*

[9] Transport Layer Security, *http://en.wikipedia.org/wiki/Transport_Layer_Security.*

[10] Advanced Encryption Standard, *http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.*

[11] LastPass vulnerability - complete account compromise, *http://forums.lastpass.com/viewtopic.php?f=7&t=37499.*

[12] Two-Factor Authentication, *http://en.wikipedia.org/wiki/Two-factor_authentication.*

[13] AES-256 and Reputational Risk, *http://lukenotricks.blogspot.com/2009/05/aes-256-and-reputational-risk.html.*

[14] BlueKrypt Cryptographic Key Length Recommendation : Lenstra and Verheul Equations, *http://www.keylength.com.*

[15] StackOverflow : Is it possible to attack a user password with known salt?, *http://stackoverflow.com/questions/5064105/is-it-possible-to-attack-a-user-password-with-known-salt*

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23 Maret 2011

Ramda Yanurzha - 13506011