Analysis DictionaryAttack danModifikasi Password Cracking SertaStrategi Antisipasi

SayedAchmady
ProgramStudiS1-TeknikInformatika FakultasTeknikUniversitasJabalGhafur Sigli
sayedachmady@gmail.com

Abstrak

Dalam kontekskriptanalisisdankeamanan komputer,dictionary attackadalah sebuahteknikuntuk melawancipherataumelawan mekanismeotentikasidengan caramenentukankuncidekripsi denganmencari kemungkinan kombinasi kata yang terdapat di dalam sebuahkamus [1].
Padadasarnyadictionary attackadalahpengembangandari brute force attack,yaitumencobamemecahkankodedengan mencoba satuper satukemungkinansecaraberulang (exhaustive search).Akantetapidictionary attackbukan mencobakombinasisatu persatukarakteryangtersedia sepertibrute force,melainkanmencobakombinasikatayang palingmungkinberhasildengan inputsebuah "listofkata" yang dapat didefinisikan (disebut juga kamus),yang biasanya berasal dari daftar kombinasi kata-kata umum yang terdapat dalam kamus, misalnya kamus bahasa Inggris.
Dictionaryattackmerupakan seranganyang sangat efektif untuk memecahkan kode dan sering digunakan hacker untukmembobolsistemkeamanan yangberupapassword, seperti akun email,akunjejaringsosial,halaman administratorsitusweb,danlain-lain.Dictionary attack dianggapefektif karena memanfaatkanpsikologi manusia, yaitukebiasaanbahwa penggunaakunakanmenggunakan kata-kata yang lumrahdanmudah diingatsebagaipassword suatu akuntertentu [2]. Selain itu, dictionaryattack juga dikembangkanvariasinyadansemakin tinggiefektivitasnya, sehinggahinggasaatiniteknik inimasihseringdigunakan untukmembobolpasswordpenggunasebuahakun.
jurnalinimembahasmengenaistudidictionary attack mengenaipenjelasan singkat,prinsip kerja,danbagaimana pengembangandaridictionary attackdalam konteks penerapannyauntukmembobolpassword sebuah akun tertentu.Variasidaridictionaryattack yangakandibahas dalammakalahiniyaitudictionary attack,hybriddictionary attack,danpre-computed dictionary attack.Selainitu,pada makalah iniakandianalisiskelebihan dankelemahan dictionary attackdanmasing-masingmodifikasinya,serta solusi yang dapat dilakukan dalam melawan dictionary attack.

***Katakunci**:DictionaryAttack,password,bruteforce,kamus,listof hash.*

I. PENDAHULUAN

Dieraglobalisasiini,manusia diseluruh duniasemakin memanfaatkan teknologiinformasidalamkehidupannya sehari-hari.Saatiniinternetsudahbukanbarangbaru bagi masyarakat. Sudahbanyakkegiatan bisnis,transaksi keuangan,komunikasi, bahkan*blogging* danjejaring sosialyangmenggunakan internet.Informasipribadi seseorangsudah semakinmudahdicari melalui *search engine*danjejaringsosial.

Sebuah akun,baikakun email,administrator situsweb, akuntransaksijualbeli,danlain-lainmerupakan halyang bersifat pribadi karena bisa mengandung informasi sensitif.Olehkarenaitu,saatinikriptografi dansistem keamanan komputerterhadapakunsangatdibutuhkan. Akan tetapi,ironisnyaketikailmukriptografi untuk mengenkripsi sebuahinformasisemakinberkembang, semakinberkembang pulacarauntukmelawannya. *Dictionary attack*merupakan salahsatubentukserangan terhadapkriptografi yanghinggasaatinimasihdianggap efektifuntukmemecahkankode*password*sebuahakun.

*Dictionaryattack*memanfaatkan psikologimanusia. yaitukebiasaanbahwakebanyakan orangakan menggunakankombinasikatayangberhubungan dengan kehidupannya sehari-haridalammembuat*password*, misalnyatanggallahir,makanankesukaan,namaorang tua,danlain-lain.Kata-katainimerupakan katayang terdapatdalamkamus(karenamerupakan katayang digunakan sehari-hari)danmudahdiingat.Psikologi manusia dalammembuat *password*jugatelahdikajidan dibuktikandenganpenelitian.

Selain itu, ada sebuah penelitian yang menyatakan bahwasekitar30%penggunamemilih passwordyang panjangnya sama dengan atau di bawah 6 karakter, hampir60%pengunamemilih passworddarikarakter alpha-numeric, danhampir50%penggunamenggunakan nama, kata slang, kata-kata dalamkamusatau "trivial password" (digit berurutan, urutan huruf di keyboard, samadengannamaakun,danlain-lain). Password paling umumyangdimiliki pemilikakunadalah"123456". Dengan demikian,jika*hacker*telahberhasilmenebak *password*salah satu akunseseorang,makaiadapat membobol beberapa akun yang dimiliki oleh orang tersebut. Halini dapat menimbulkan kejahatan yang serius,misalnyamelakukan transaksisecaradiam-diam, mengubahkontenprofil,danmenyebarkanisuyangtidak

baikdenganmenggunakanakunkorban.

Olehkarenaitu,penulismerasa*dictionary attack* merupakan kriptanalisisyangpatutuntukdikaji,dengan harapan kajian dari*dictionary attack*inidapatmembuka wawasan pembaca akan pentingnya memproteksi *password*dariserangan*dictionary attack*,mengetahui kelemahannya, sertamenerapkantawaransolusiyang diajukanpadamakalahini untukmelawannya.

Makalah iniakanmembahasmengenaipenjelasan singkatmengenai *dictionaryattack*,prinsipkerjanya, dan bagaimana pengembangan (modifikasinya) dari *dictionary attack*dalamkontekspenerapannyauntuk membobol *password*sebuahakuntertentu.Selainitu, makalahinijugaakanmemaparkan kelebihandan kelemahan*dictionaryattack*danmodifikasinya, serta memberikansolusiuntuk melawan*dictionaryattack*.

Penulis berharapmakalahinidapatmemberikan kontribusi bagi pembaca, dalamhal ini pengguna dan penyedia aplikasiataulayanan suatuakuntertentu supaya dapatmeningkatkan keamanan*password*sehinggadapat memproteksidiridariserangan*dictionaryattack*.

II. KRIPTANALISIS

A. DefinisiKriptanalisis

Kriptanalisis berasaldaribahasaYunani*kryptos*yang berarti tersembunyi dan *analyein* yang berarti melepaskan.Kriptanalisis berartisebuahstudimengenai metodeuntukmendapatkan artidariinformasiyang terenkripsi, tanpamemilikikunciakseskeinformasi rahasiatersebut.

Studiinimelibatkan pengetahuanmengenaibagaimana sistembekerjadanmenemukan sebuahkuncirahasia. Metodekriptanalisisterusberkembang dansemakin kompleks,daripenggunaan penadankertasdimasalalu, sekarangmenggunakanskemaberbasiskomputer.

B. SumberDayaKomputasionalyangDibutuhkan

Penyerangan dapatdicirikandengansumberdayayang dibutuhkan.Sumberdayatersebutmeliputi:

- Waktu
  Jumlahlangkahkomputasiyangharusdilakukan.
- Memori
  Jumlahsumberdayayangdiperlukandalammelakukan serangan.
- Data
  Jumlahdari plainteksdan cipherteksyang diperlukan. Kadang-kadangsulit untuk memprediksi kuantitas inisecara tepat, tetapi kebanyakankripatanalissetidaknya menyediakanperkiraankekuatandariseranganmereka.

III. METODE*DICTIONARYATTACK*

A. *Overview Dictionary Attack*

Dalam lingkupkriptanalisis dankeamanankomputer, *dictionaryattack*adalahteknikuntukmengalahkancipher atau mekanisme autentikasi dengan cara menentukan kunci dekripsi atau frase khusus dengan mencari kombinasikata-katayangpalingmemungkinkan yang terdapatpadasebuahkamus[1].

*Dictionaryattack*menyerangtargetdengan mencoba semuakata-katayangdidefinisikan dalamsebuah *exhaustive list*secaraberulang,yangdisebutjugadengan istilahkamusataudictionary.Berbeda dengan*bruteforce attack* yang menggunakan semua kemungkinan kombinasi karakteryanglingkupdomainnyasangatluas, *dictionary attack*hanyamencobakemungkinan-kemungkinan yangmemilikipeluangkeberhasilantinggi (*mostlikelytosucceed*),yangsecaratipikalditurunkan darikata-katayangterdapatdalam kamus.Kamus disini didefinisikan sebagaisebuah“listofkata”yangtiap-tiap elemennya adalahkombinasi darikata-katayangterdapat dari sebuah kamus (misalnya kamus bahasa Inggris, kamusbahasaIndonesia,dansebagainya). D*ictionary attack*seringkaliberhasilkarenakebanyakan orang menggunakan kata-katayanglazimterdapatdalam percakapan sehari-haridalammenentukan*password* sebuah akunnya(*password*e-mail, situsweb,dan sebagainya)[3].

Pengembangan dari*dictionaryattack*juga memungkinkan penyeranguntukmenghemattenagadan waktudenganmelakukan komputasi“listofkata”,atau disebutjuga*listofhashes*,dalam kata-kata dalamkamus danmenyimpan kata-katatersebutdalambasisdata(atau file teks) denganmenggunakan*hash* sebagaikuncinya. Mengkomputasikan program*dictionaryattack* membutuhkanwaktuyang cukup lama, terutamauntuk mendefinisikankata-kata yang akan menjadi “amunisi” dalam menebak *password*. Namun ketika program tersebutsudahsiapuntukmenyerang, serangan dapat dieksekusi dengancepatdanefektif,tergantung dari komputasiataumodifikasiyangdisusunolehpenyerang.

B. CaraKerja*Dictionary Attack*

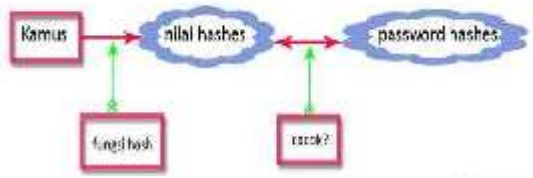
SistemoperasisepertiWindowsmenyimpan *password* ke dalam bentuk terenkripsi yang disebut *hashes*. *Password*tidakdapatdiambil (*retrieved*) secaralangsung dari*hashes*.Untukmelakukan *recoverpassword* diperlukan komputasiterhadap*hashes*dengan*possible password*(kata-katayangdidugasebagai*password*) dan memasukkannyakedalam*list ofhashes*.

Dalamkontekskeamanansebuah*password*,mis

alnya*password*akune-mail,akunadministratorsitusweb,dansebagainya,manusiaseringkalimemilih katayangmudah diingatsupaya tidaklupa dengan*password*akun yang telahdibuatnya, Sebagai contoh,banyak penggunaemail yang menggunakan kata „*admin*„„*administrator*„„*supervisor*„ „*password*„ dan sebagainya sebagai *password* default, atau menggunakan *password* yang berasal daritanggal lahir,namaorang tua,lokasi rumah,danlain-lainagarmudahdiingat[2].

Hacker mengumpulkan kata-kata yang sering digunakan sebagai *password* ini ke dalam sebuah file yangdinamakan sebagai*dictionary*(kamus)danfileini bisadidapatkan denganmudahdiInternetsepertidisitus http://lastbit.com/dict.asp,ataukitajugabisamembuatnya sendiriataumenambahkannya darifile*dictionary*yang sudahada[5].

Gambar di bawah ini merupakan alur proses dari*dictionaryattack*:



Gambar1- AlurProsesDictionaryAttack

Program*cracking*akanmengubahsatupersatukata-kata yangadadidalamkamusberdasarkan fungsi*hash*yang digunakankedalambentuktabel*hash*.Hasilperubahan inikemudiandicocokkandengan*hash*padafile*password* yangdidapatkan.

Apabila hasil*hash*inicocok,artinya*password* sudah berhasil diketahui. Dengan teknikini,*hacker*tidakperlu mencoba semua kombinasi karakter yang ada (seperti *brute force attack*) sehingga bisa menghematbanyak waktudantenaga.

IV. TEKNIK-TEKNIK*PASSWORDRECOVERY*DANPERBANDINGANNYA

Sebuah *password* dapat ditemukandengan berbagai cara, teknik yang umum digunakan antara lain:*brute forceattack*,*dictionary attack*,*hybriddictionary attacks*, dan*pre-computeddictionaryattack*[3].

A. *BruteForceAttack*

Dalam*bruteforceattack*,penyerangmenentukan *range ofcharacterset*danmengkomputasikanhashuntuksetiap kemungkinan kombinasikarakteryangada,dalamhalini pada umumnya *brute force attack* menggunakan kombinasi karakteryangterdiridarihurufsaja,hurufatau angka, hurufangkaatau *specialcharacter*,atau setiap karakterpadatabelASCIIsebagaidomainnya.

Denganmenggunakan *bruteforceattack*,semua *password*dalam bentukapapun sudahpastidijaminakan tertebak, namun yang menjadi masalah adalah waktu yangdiperlukan untukmenebak *password*tersebut, terutamajika *password* yanginginditebakterdiridari banyakkarakter.

Kelebihan dari*bruteforceattack*adalahjaminanbahwa *password* apapun dapat dipecahkan. Namun kelemahannya,waktuyangdibutuhkan*bruteforceattack*, yaitu tingkat kompleksitas*password* akan berpengaruh secaraeksponensial padabanyaknyapercobaanyang dilakukan.Untuklebihjelasnyalihattabeldibawahini:

Symmetric key length vs brute force combinations

Key size in bits[2]	Permutations
8	2^8
40	2^{40}
56	2^{56}
64	2^{64}
128	2^{128}
256	2^{256}

Gambar2-HubunganPanjang*Password*denganBanyaknyaKombinasiKarakter Pada *BruteForce*

B. *DictionaryAttack*

Dalam*dictionaryattack*,*hashes*dikomputasi secara berangsur-angsur dengansetiapkatatunggalatau modifikasikata dari sebuah kamus dan dicocokkan dengan*passwordhashes*darisetiappenggunatertentu.

Kentungan darimetode*dictionaryattack*adalahwaktu yang dibutuhkanrelatif singkat. Sedangkankelemahan darimetode iniadalahhanya dapatmenebak*password* yangterdiridarikombinasi kata-katayangterdapat pada kamus(contoh:jika *password*penggunamenggunakan kombinasihurufangkayangtidakterdapatdalam kamus, maka*password*tidakakantertebak).

Kamus dalam metode *dictionary attack* berbentuk sebuah“listofkata”,yangtiap-tiapelemen katanya merupakankata-kata dan kombinasinya yang terdapat padakamus.Kamusinisendiri dapat beragam,seperti kamusbesarbahasaIndonesia, kamusbahasaInggris, kamusmultilingual, ataubahkankata-katayangterdapat pada buku (bible, Al-Qur”an, novel, diary), dan sebagainya.

C. *Hybrid DictionaryAttack*

Secaraumum*hybriddictionary attack*serupadengan *dictionaryattack*biasa,yaitumenggunakankamus"listo f kata"sebagaisenjatauntukmenebak*password*. Namun *hybriddictionaryattack*jugadapatmenebak*password*y angmerupakan kombinasiantarkatadalamkamusdan jugaangka(*alpha-numeric*). *Hybriddictionaryattack* menambahkan karakter di sebelah kanan/kiri dari tiap kataataumodifikasi katayangterdapatdarikamus. Sebagaicontoh:kata"merdeka" dalamkamusdapat dikomputasi *hybriddictionaryattack*untukmenebakkata "merdeka1945".Hal serupa jugabisa terjadi misalnya untukkatakunci"if17123","122emergency", dan sebagainyasebagaielemendarikamusnya.

Keuntungan dari*hybriddictionaryattack*adalahteknik inidapatmenebak *password*yangterdiridarikombinasi katayanglumrah dengankarakterlain,karena*password* sejenisinijugaseringdigunakan olehpengguna.Namun kelemahannya jelasmembutuhkanwaktuyangjauhlebih lama daripada *dictionary attack* biasa karena menggunakankombinasi-kombinasidari*listofhashes*.

D. *Pre-Computed DictionaryAttack*

Untukdapatmelakukan*pre-computeddictionaryattack*, tiap *hash* akan direkomputasidan pasangan*password-hash*disimpan padasemuakombinasiyangmungkin dari setkarakteryang dipilih. Pasword*hashes*yang*available* dicaridari*pre-computed hashes*.Secarasingkat, *precomputedhashesattack*mendefinisikan kamusnya secara manual. Akan tetapi *pre-computed dictionary* attackakanmenjadisangatefektif dan efisienjika menggunakan teknologi*informationretrieval*dalam mendefinisikan listofkata.Misalnya"listofkata"yang akandijadikan senjatadalammembobol*password*terdiri darikata-katayangterdapat dariprofilFacebook seseorang,blog seseorang,dokumenpribadiseseorang, dansebagainya.Dengandemikian,"listof kata" yang akandijadikansenjatauntukmembobol *password*dapat diisiolehkata-katayangsesuaidenganinformasi pribadi yangdimilikipengguna(lebihpersonal).

Pre-computed dictionary attack menjadi semakin efektifketika*hacker*sedang beradadikondisiadabanyak *password*yangharus dibobol. Secara umum komputasi *dictionary attack*hanyacukupdi*generate* sekalisaja, setelahituprogramhasilkomputasi dapatdijalankan denganlebihcepatdibandingkan *dictionaryattack*biasa. *Passwordhashes*dapatmencocokkan tiapkatapadalist dengan *password* yang terkorespondensidengan waktu yanginstan.*Pre-computed dictionaryattacks*jugadapat dikenali sebagaipenggunaandari"salt",yaitu teknikyang memaksa*hashdictionary*untukdikomputasi ulangpada tiap*password*yangdicari.

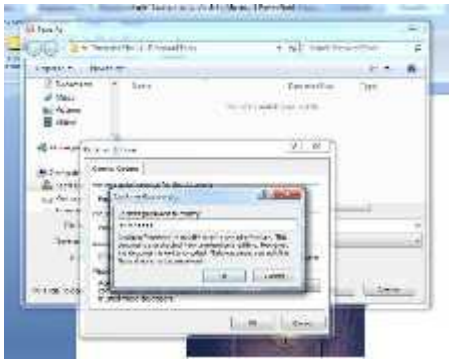
*Pre-computed hashesattack*jugadapatdikombinasikan dengan spam,yaituinjeksi kodekesuatuhalamanweb sehinggaiadapatmenerima informasi rahasiayang terdapat pada website tersebut, seperti *list of email address*padakontakseseorang, dansebagainya. Halini menambah efektifitasmetodeinidalammembobol *password*.

Keuntungandari metodeini adalahkecepatan(waktu yangdibutuhkan untukmembobol*password*)yang jauh lebihcepatdibandingkanmetode-metode sebelumnya karena"list of kata" hanya menyimpankata/informasi yang personal, yang didefinisikan sendiri berdasarkan hasilpencarianinformasi tentangpengguna.Namun kelemahan yangumum darimetodeiniadalahdibutuhkan waktuyanglamadalammengkomputasi*hashes*nya.

V. PERCOBAAN*DICTIONARYATTACK*UNTUK MEMBOBOL*PASSWORD*

Dibagianini,akandijelaskanmengenai caramembobol *password*denganmetode*dictionary attack*.Karenasulit ditemukantoolyangdapatmembobolpasswordakun(ad a aplikasi berbayar),makapadakasusdibawah ini percobaan*dictionaryattack* dilakukanpada filepowerpoint.ToolsyangdigunakanadalahPassword Tool versi Powerpointyangdapatdiunduh program demonya pada situshttp://lastbit.com/programs/msodemo.zip

Pertama-tama dibuatfilepowerpointdengannama contoh.ppt yang diatur *password security*nya dengan kunci "bathroom".

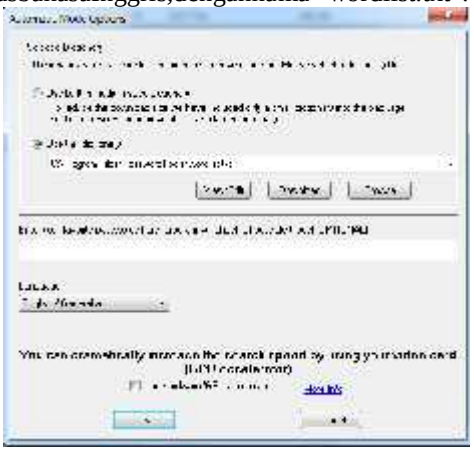


Gambar3- MembuatPowerpoint dengan*password*

Kemudian bukaaplikasiPowerTools versiPowerPoint. Berikutadalahtampilanantarmukanya.

Gambar4- AntarmukaPasswordToolsPowerpoint

Penggunadapatmenginput fileteksyang akan dijadikan kamusuntukdictionaryattack.Padaprogram demo, disediakanjugafilekskamusyangberisikata-katayang adadalam kamusbahasaInggris,dengannama “wordlist.txt”.

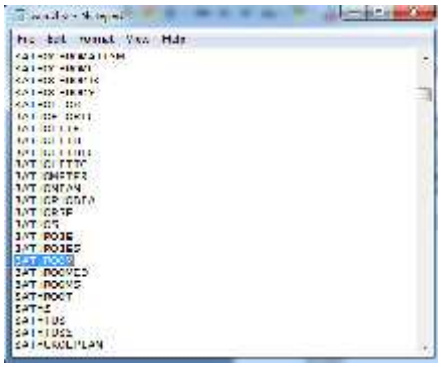


Gambar5- Inputfileteksyangdijadikankamus untuk*dictionaryattack*

Gambar6- Proses*dictionaryattack*berlangsung

Password“bathroom”berhasilditemukan dalamwaktu1menit22detik.Kemudianpercobaanberikutnyaadalah mengganti *security password* contoh.ppt dengan kata kunci“kamarmandi”.Ternyatahasilnya*dictionaryatta ck* yangdialkukanPasswordToolgagalmenemukansolusi password.

Daripercobaandiatas,dapatdisimpulkan bahwa *dictionary attack*dapat digunakan untukmemecahkan *password*jikadiketahuibahasayangdigunakan dan tersediafilekamusyangbersesuaian, sertadalam percobaan ini,hanyaefektif jika*password*hanyaterdiri darisatukatadalam bahasainggris,contohnya “bathroom”.Berikut ini adalah potongan gambar mengenai isidarikamusyangdigunakan, yaitu “wordlist.txt”.



Gambar7–Isifile*dictionary*wordlist.txt

Denganteknikmodifikasi*hybrid-dictionary attack*, denganfilekamusyangsama, dapatdikomputasi kombinasi antarkatadanangkasehinggamemungkinkan terjaditebakanyangmerupakan gabungandarisatuatau lebihkata(jumlahnyapunbisadikonfigurasi), seperti “establishedin1971”. Proses*attack*nyaakanjauhlebih lambat,namundapatlebihdipercayatercapainya solusi karenadapatmenebak passwordyangmerupakan kombinasi.

Sementara itu,denganteknikmodifikasi*pre-computed dictionary attack*, kita dapat menggunakan file kamus yangkitabuatsendiri.Kata-katatersebutbisa merujuk padainformasi pribadipemilikfile*password*, seperti tanggallahir,namaorangtua,danlain-lain. Proses*attack* akanjauhlebihefisien.

Kamusuntuk*hybrid-dictionary attack*dapatdiperoleh darisitushttp://lastbit.com/dict.aspsementaraituprogram untukmemperolehkamus*pre-computed-dictionaryattack* dapatdiperoleh darisitushttp://lastbit.com/dictmaker/default.asp

VI. SOLUSIUNTUKMELAWAN*DICTIONARY ATTACK*

Untukdapatmengalahkan *dictionaryattack*dalam memproteksi *password*yangkitamiliki,kitaharus mengetahui carakerjadanmengapa*dictionaryattack*dan modifikasinya dapatberfungsisecaraefektifdalam membobolsebuah*password*.

Caramelawan*dictionaryattack*dapatdigunakan

baik oleh pengguna akun maupun oleh *developer* yang membuatsistemkeamanannya. Berikutiniadalahcara-carauntukmelawan*dictionaryattack*:

A. Memperkuat*PasswordStrength*

*Password strength*adalahsebuahukurandariefektivitas ketahanansebuah*password*terhadap*bruteforceattack* dan sejenisnya.Ukuran ini didasarkan pada seberapa besarpeluangpercobaan yangdapatdilakukan *hacker* untuk dapat menebak *password* tersebut. *Passwordstrength*inidiukurdaripanjang *password*(*password length*),kompleksitas, dankesukaranprediksi(acakdan tidakberhubungan denganinformasipribadi).*Password strength*hanyamenentukankekuatan proteksi*password* dari tingkat kesukarannya,bukan dari *security control design* yang terdapat pada aplikasi saat autentifikasi sebuahakun[6].

B. Mengganti *Default Username* dan PesanKesalahan Login

Tidakhanya*password*yangharusdiproteksi, *username* sebuahakunjuga harusdijadikanbahanpertimbangan. Ketika usernamedapat ditebak *hacker*dengan mudah,maka*hacker*hanyaperluuntukmenebak *password* penggunasaja,tidakperlumenebakkombinasi *username* dan*password*.Halini menjadimasalahkarenabanyak webaplikasi atau*framework*webyangmenyediakan *defaultusername* padapengguna, contohnya padaakun Wordpress*defaultusername*nyaadalah“admin”[7].

Selainitu,pesanyangditimbulkan darikesalahaninput jugaberpengaruh. Misalnya,*hacker*gagalloginlalu kemudianditampilkan pesan“youfailedtologinbecause the password is incorrect”, pesan ini memberikanarti bahwa*hacker*telahberhasilmenebak *username*dengan benar,sehinggaiatinggalmenebak *password*yang berkoresponden dengan*username*tersebutdengan *dictionary attack*.Berbedajikapesanyangditampilkan adalah“youfailedtologinbecauseyourusername and *password*doesn‟tmatch”.Dengandemikian*hacker*tida k tahuapakah salahsatudariusername dan*password*yang ditebak*hacker*sudahbenarataubelum[7].

C. Membuat*Strong PasswordPolicy*

Salahsatupertahananutamadalammelawan*dicti onary attack*adalah adanya*strongpasswordpolicy*dalam membuatakundisuatu website.

Kitatelahmembahasmengenaikombinasikatap ada *dictionary attack*danpentingnya *passwordstrength*. Dengan adanya*strongpassword policy*,setiapkali pengguna inginmembuatsebuahakun,adabatasan-batasan tertentu (*guidelines*) dalam menentukan *password*,seperti:

- *Passwordlength*minimal7karakter
- *Password*terdiridarikarakter*upper*dan*lowercase*
- *Password*harusmengandungangka
- *Password*harusmengandungtandabaca

*Guidelines*diatasmemangagakmenyulitkanpen gguna, namunkebijakan sepertiiniakansangatmelindungi pengguna daripemboboland*dictionaryattack*,karenaakan ada hampir 70 triliun kombinasi karakter yang dapat dibuatdari7digit*password*yangmengandung*upper*dan *lowercase*,angka,dantandabaca.

Bahkan *dictionary attacktool*yangmampumelakukan penyocokan 100*password*perdetikpunmembutuhkan waktulebihdari11.000tahununtuk memecahkannya.

D. Strategi*Automatic Disable Account*

Strategilainyangdapatmemproteksi *password*dari *dictionary attack*adalahadanyafitur*disableaccount* secaraotomatis setelah penggunabeberapakaligagal melakukanlogin.

Contohnya,ketikaservermendeteksi pengguna“Bob” telahmelakukan gagalloginsetelah3kali,maka *password*nyaakandigantisecaraotomatis,ataupenggun a tersebuttidakbisamelakukan loginselamaselangwaktu tertentu,misalnyaselama30 menit. Hal ini mencegah iterasipencocokan kata*dictionaryattack*yangdilakukan berulang-ulang.

Adapendapatbahwasolusiinimerupakan solusiyang burukkarenamerugikan penggunayangasliketikaada *hacker* menyerang akunnya karena pengguna menjadi tidakbisaloginsepertibiasajika passwordnyadiubah atausedang. inginloginsaatakunsedang*temporary disabled*. Bahkan hal tersebut memungkinkan *hacker* untukmerusak sistemdenganmencegahpenggunauntuk loginkapan pun.Namun, solusiinibisadipakaiuntuk proteksi *password*dokumen yangbersifat sangatrahasia dantidakbisasembarangandiaksespublik[8].

E. Strategi*IncrementalResponseDelay*

Strategilainuntukmelawan*dictionaryattack*yait u dengancara menghasilkan*delaypageresponse*setelah percobaan login gagal secara inkremental. Sebagai contoh,pada percobaanpertamapenggunagagallogin, maka halaman akan melakukan *delay* selama 1 detik, padapercobaan keduagagallogin,halamanakan melakukan *delay*selama3detik,jikademikian pada percobaan ke-n,maka*hacker*akanmenunggu n+(n-1)+ (n-2)+…+1detik hinggahalaman webmerespon

kembali.

Solusi*incremental delay*dapatdikatakansebagaisolusi yangefektifkarena penggunaasliyang2atau3kali melakukangagal login seperti tidak mendapatkanefek apa-apakarenahanyamerasakan delayyangbesarannya hanya 2 atau 3 detik, namun efek ini menjadisangat bermasalah bagi *dictionary attack tool* yang mencoba loginribuankali,sehinggamembutuhkan waktuyang sangatlamauntukdapatmembobol*password*nya.

Untuk mencegahkesalahaninkremenyang terjadi di luarkontrol,sistem*incremental delay*juga mempertimbangkan IP Address pengguna yang melakukan aksi login dan mereset *incremental number*nyaketikapenggunaberhasillogin,ataudireset tiapperiodewaktu tertentu,yangmengacu pada*web session*[8].

F. Menggunakan*ReverseTuring Test*

Alternatif laindalammelawan*dictionaryattack*yaitu denganmenggunakan *ReverseTuringTest*,yaitudengan menggunakan validasi yang mengharuskan pengguna untukmenginputkatakunci yangditampilkankelayar untukmemastikan bahwainputtersebutbenar-benar dimasukkan olehmanusia,bukanmesinotomatisseperti *dictionaryattack tool*.Salahsatu *ReverseTuringTest* yang palingpopuler dan terpercayaadalah CAPTCHA (*Completely AutomatedPublicTuringTesttoTell ComputersandHumansApart*).

Adayangberpendapat bahwaadaperangkatlunak intelegensia buatandengangrafikvisualyang memungkinkan programuntukmenginterpretasikata tantanganCAPTCHAyangdipecahkan olehGregMori danJitendraMalikdariUCBerkeley ComputerVision Groupdenganprogrammereka,namun programtersebut tidaktersebarluasdimasyarakat[9].

Namun adajugarisetterakhirdaripaperJ.Xuetaldan workshopXeroxPARCyangmengembangkan *Reverse TuringTest*hihnggatakdapatdiparsing olehOptical CharacterRecognition (OCR)saatini.Hasil pengembangan itusekarangdigunakanuntukkebutuhan komersialsepertiPayPal,Yahoo!,danAltavista[8].

G. MenggunakanProtokol Autentifikasi

Ketika*offlinedictionaryattack*hanyamungkin terjadi ketika penyerangdapat mengambildata pada protokol denganmenyadapchannelkomunikasi dandapatdilawan denganmenggunakan *publickey*padakriptografi,*online dictionary attack*dapatdilakukan olehsiapasaja.Halini menyebabkanmunculnya alternatif melawan*dictionary attack*denganmenggunakanprotokolyangterautenfikasi.

Protokolterautentifikasimudahdiimplementasi kantanpa mengubahinfrastrukturdenganmenggunakan*one way hash functions* dan mengeliminasi *online dictionary attack*denganimplementasi*challangeresponsesystem* yangdidesainsedemikianrupa sehinggamenimbulkan kendala berat, menghabiskankan banyak waktu, dan menyiksa secara komputasional dengan meluncurkan ratusanribu*authenticationrequests*pada*onlinedictionary attack*. Protocol tersebut bersifat stateless dan tahan terhadap *denial of service* (DoS) *attacks*. Protokol terautentifikasi menjawab permasalahan *usability* dan *scalability*dibandingkansolusi-solusisebelumnya[9]. Sepanjangstudiliteratur yang dilakukanpenulis,protokol terautentifikasi adalah solusi paling aman dan efektif hinggasaatini.

V. KESIMPULAN

Dictionary attack merupakan serangan kriptanalisis yangsederhana danmudahdilakukan, akantetapiselama sistemkeamanan terhadap*password*tidakdiproteksi denganstandarpencegahan yangbaik, *dictionary attack* dapat menjadiancamanyangberbahaya.

Pre-computeddictionaryattack adalahseranganyang palingberbahayakarenapenyerangmemanfaatkan data- datapersonaltargetyangakunnyaingindibobol, sehingga serangan dapatlebih efisien,apalagijikamenggunakan teknologi*informationretrieval*otomatis.

Solusiuntukmengalahkan *dictionaryattack* membutuhkan partisipasi baik dari *user* maupun *developer*. Solusibagi*user*adalahdenganmenggunakan *strong password* yang terdiri dari minimal7 karakter, kombinasi huruf, angka,bahkantandabaca,serta mengganti *usernamedefault*.Solusidari*developer*yaitu denganmembuat *strongpassword policy,automatic disabled account,incremental responsedelay*, *Reverse TuringTest*,sertamenggunakan protokolterautentifikasi. Masing-masing solusi memiliki kelebihan dan kekuranganmasing-masing sehinggasebaiknya disesuaikan dengankebutuhan.Selainitu,beberapasolusi dapatsalingmelengkapisatusamalaindalammembentuk sistemkeamananyangsolid.

Denganmengikuti pedoman ini,diharapkan Andadapat memproteksi akundari*dictionaryattack*,baikdarisudut pandang*user*maupun*developer*.

REFERENCES

[1] http://en.wikipedia.org/wiki/Dictionary_attack

[2] The Imperva Application Defense Center (ADC).

(2010). http://www.imperva.com/docs/WP_ConsumerPassword WorstPractices.pdf
[3] http://lastbit.com/*password*-recovery-methods.asp
[4] http://lastbit.com/dict.asp
[5] http://lastbit.com/programs/msodemo.zip
[6] http://en.wikipedia.org/ wiki/*Password*_strength
[7] Sullivan,Bryan.*PreventingaBruteForceorDictionaryAttack: How to Keep the Brutes Away from Your Loot*, http://www.infosecwriters.com/text_resources/pdf/Brute_Force_BSullivan.pdf
[8] Pinkas,Benny. (2002). *SecuringPassword From DictionaryAttack*, http://www.pinkas.net/PAPERS/pwdweb.pdf
[9] Goyal, Vipul. (2005).*A New Protocol to Counter Online DictionaryAttacks*.Crypto Group,Institute of Technology, BanarasHindu University,India. http://www.cc.gatech.edu/~virendra/papers/GKS05-journal.pdf