ХАБАРШЫ ВЕСТНИК

Д.А. КУНАЕВ АТЫНДАҒЫ УНИВЕРСИТЕТ

№3 2017

УНИВЕРСИТЕТ ИМЕНИ Д.А. КУНАЕВА

ISSN 1606-4208

3	8	1. b_1, b_2, b_3 - кездейсоқ цифрлар. 2. b_4, b_5 - жиыннан кездейсоқ символдар {!,",#,$,%,&,',(,),*}. 3. b_7 - ағылшын алфавитінің кездейсоқ үлкен әріпі. 4. b_8 - P –ні реті бойынша кіші ағылшын алфавиті , мұнда $P = N^2 \bmod 10 + N^3 \bmod 10 + 1$.
4	9	1. $b_1,\ldots,b_{1+Q}$ - жиыннан кездейсоқ символдар {!,",#,$,%,&,',(,),*}, мұнда $Q = N \bmod 5$. 2. Бұдан басқа паролдің қалған символдары b_4 , - ағылшын алфавитінің кездейсоқ кіші әріпі. 3. b_9 - кездейсоқ сан.
5	10	1. $b_{10-Q},\ldots,b_{10}$ - кездейсоқ цифрлар, мұнда $Q = N \bmod 6$. 2. b_1, b_2 - ағылшын алфавитінің кездейсоқ үлкен әріпі. 3. $b_3,\ldots,b_{10-Q-1}$ - ағылшын алфавитінің кездейсоқ кіші әріпі.
6	11	1. b_1, b_2 - кездейсоқ цифрлар. 2. $b_3,\ldots,b_{3+Q}$ - ағылшын алфавитінің кездейсоқ үлкен әріпі, мұнда $Q = N \bmod 8$. 3. $b_{4+Q},\ldots,b_{11}$ - жиыннан кездейсоқ символдар {!,",#,$,%,&,',(,),*}.
7	11	1. b_1, b_2 - кездейсоқ цифрлар. 2. $b_3,\ldots,b_{3+Q}$ - орыс алфавитінің кездейсоқ кіші әріпі, мұнда $Q = N \bmod 8$. 3. $b_{4+Q},\ldots,b_{11}$ - жиыннан кездейсоқ символдар {!,",#,$,%,&,',(,),*}.
8	12	1. $b_1,\ldots,b_{1+Q}$ - ағылшын алфавитінің кездейсоқ кіші әріпі, мұнда $Q = N^3 \bmod 5$. 2. $b_{1+Q+1},\ldots,b_{1+Q+1+P}$ - ағылшын алфавитінің кездейсоқ үлкен әріпі, мұнда $P = N^2 \bmod 6$. 3. Парөлдің қалған символдары – кездейсоқ цифрлар.
9	12	1. $b_1,\ldots,b_{1+Q}$ - орыс алфавитінің кездейсоқ кіші әріпі, мұнда $Q = N^3 \bmod 5$. 2. $b_{1+Q+1},\ldots,b_{1+Q+1+P}$ - орыс алфавитінің кездейсоқ үлкен әріпі, мұнда $P = N^2 \bmod 6$. 3. Паролдің қалған символдары – кездейсоқ цифрлар.
10	6	1. b_1, b_2 - орыс алфавитінің кездейсоқ үлкен әріпі. 2. $b_3 = N^2 \bmod 10$ (мұнда mod 10 санды бөлуден қалған қалдық10).

ЭКОНОМИКА, ФИЗИКА И МАТЕМАТИКА

ПСИХОЛОГИЯ И ПЕДАГОГИКА ОБРАЗОВАНИЯ

ТРИБУНА МОЛОДОГО УЧЕНОГО

ЛИТЕРАТУРНОЕ ТВОРЧЕСТВО

Дүйсебекова А.К.
Л.А. Қошаев атындағы университеттің
ф-м.ғ.к. профессоры, «Экономика және бизнес»
кафедрасының меңгерушісі
Молдықожакова Б.Ж.
Л.А. Қошаев атындағы университеттің
оқытушысы

«Берілген талаптар бойынша парөлдер генераторын жүзеге асыру»

Ақпаратты қорғау жүйесін құру барысында тұтынушыны идентификациялау және аутентификациялауды іске асырудың мәні зор. Қағида бойынша, қорғаныстың алғашқы қадамында тұтынушының аутентификация парольдік жүйесіне байланыстылар қолданылады. Бұл берілген жүйелерде тұтынушыны тек өзінен басқа ешкімге белгілісіз пароль бойынша аутентификациялайды.

Идентификациялау және аутентификациялау жүйелерінің тәзімділігі көбінесе тұтынушы парөлінің дұрыс құрылғанымен анықталады. Парөлді таңдауға қойылатын талаптардың біразын сақтамау *берілген тәзімділікті бірінама дәреже*ле азайтады және идентификациялау және аутентификациялау жүйелері дұрыс құрылған шабуылдарға осал болады.

Тұтынушы парөлін таңдауда карастырылуы тиіс негізгі талаптар төменде көрсетілген:

1. Парольдің ұзындығы ең аз дегенде 6 символдан тұруы тиіс. Қысқартылған пароль ұзындығы, көбіне олардың ашып кету толық сәтті шабуылдарының ықтималдылығын арттырады.

2. Пароль әртүрлі символдар тобынан тұрады (үлкен және кіші латын әріптері, цифрлар, арнайы символдар '(', ')', '#' и ж.б.). Символдардың нақты бір тобын парөлді құру кезінде қолдану «маска» бойынша сәтті шабуылға шығу ықтималдылығын бірінама дәрежеде арттырады.

3. Пароль ретінде нақты сөз, аты-жөнімізді және т.с.с. қолдануға болмайды. Нақты сөзді, атымызды пароль ретінде қолдану сөздік бойынша сәтті шабуылға шығу ықтималдылығын бірінама дәрежеде арттырады.

Жоғары дәрежелегі қорғалған болуы үшін тұтынушыларға арналған парөлдерді таңдау есебін адам көмегімен емес бағдарламамен – парөлдер генераторы арқылы шешілгені, себебі тұтынушы санының көптігі администратор-адамға жоғарыда көрсетілген талаптарды қанағаттандыратын парөлдерді құру кезінде қиындықтық туғызады.

Кейде , пароллдер генераторы берілген элементті генерациялау барысында тұтынушы идентификаторына енетіндер (жекеленген символдары, символдар саны және т.б.) қолдануы мүмкін. Жеке варианттарда, пароль белгілі алгоритм негізінде бүтіндей идентификатордан да құрылуы да мүмкін. Соңғы жағдайда, идентификатор негізінде құрылған дара парольге сәйкес берілген тұтынушы идентификаторына қойылады. Бұл вариантта тұтынушы тіркелуін міндеттейтін көптеген коммерциялық бағдарламаларда парольдерді құру қолданылады (например, WinZip).

Мысалы.

Тұтынушы идентификаторы Kanagatov

Пароль 1Op(0Q)p+

Бұл жерде, 1Op(0Q)p+ парольді құру кезінде Kanagatov идентификаторына кіретін жекеленген символдар қолданылуы мүмкін.

1. Пароль генераторын канағаттандыратын талаптарды 1 кестеден табыңыз.

2. Кестедегі талаптарға сәйкес бағдарлама жазуға болады – пароллдер генераторы. Бағдарлама төмендегі әрекеттерді орындауы тиіс:

a. Тұтынушы идентификаторын пернетақтадан енгізу. Бұл идентификатор $a_1a_2...a_N$ символдар тізбегінен тұрады, бұл жерде N идентификатор символдарының саны (кез келген болуы мүмкін), a_i - тұтынушы идентификаторының i -ші символы.

b. Берілген идентификаторға тұтынушы парольін құру $b_1b_2...b_M$, бұл жерде M сіздің вариантыңызға сәйкес пароль символының саны және оны экранға шығару, b_i символдар парольін алу алгоритмі сіздің вариантыңызға сай 1 кестедегі талаптар тізімінде көрсетілген.

Кесте 1

Вариант	Пароль символдары нақ саны	Талаптар тізімі
1	6	1. b_1 - ағылшын алфавитінің кездейсоқ үлкен әрпі. 2. $b_2 = N^2 \bmod 10$ (мұнда mod 10 - санды 10 бөлуден қалған қалдық). 3. b_3 - кездейсоқ сан. 4. b_4 - жиынның кездейсоқ символы $\{!,@,\#,\$,\%,\&,^*,(,),-,+\}$. 5. b_5 - ағылшын алфавитінің кездейсоқ кіші әрпі.
2	7	1. $b_1b_2b_3$ - ағылшын алфавитінің кездейсоқ кіші әрпі. 2. b_4b_5 - ағылшын алфавитінің кездейсоқ үлкен әрпі. 3. b_6b_7 - екімәнді сан. $N^2 \bmod 100$ ден бөлегіш. (Егер қалдық - бірмәнді сан болса, то $b_6 = 0$).

		3. b_4 - кездейсоқ сан. 4. b_5 - жиынның кездейсоқ символы {!,",#,$,%,&,',(,),*}. 5. b_6 - орыс алфавитінің кездейсоқ кіші әріпі.

ЕСКЕРТУ

1. Ағылшын символдарының коды - «A»=65,…,«Z»=90, «a»=97,…, «z» =122.
2. Цифр коды – «0» = 48, «9» = 57.
3. Арнайы символдар коды ! – 33, " – 34, # - 35, $ - 36, % - 37, & - 38, ' – 39, (- 40,) – 41, * - 42.
4. Орыс әріптері символдарының коды – «А» - 128, … «Я» - 159, «а» - 160,…, «п» - 175, «р» - 224,…, «я» - 239.

Генерацияланған бағдарлама пароллдерінің мысалдары:

1) ИДЕНТИФИКАТОР1 ….. ПАРОЛЬ1 ……
2) ИДЕНТИФИКАТОР2 ….. ПАРОЛЬ2 ……
3) ИДЕНТИФИКАТОР3 ….. ПАРОЛЬ3 ……
4) ИДЕНТИФИКАТОР4 ….. ПАРӨЛЬ4……
5) ИДЕНТИФИКАТОР5 ….. ПАРӨЛЬ5……

Әдебиеттер:

1. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации, М.: Горячая линия - Телеком, 2004
2. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность, М.: Компания АйТи; ДМК Пресс, 2004..
3. Зегжда Д.П., Ивашко А.М.. Основы безопасности информационных систем. — М.: Горячая линия – Телеком, 2000.
4. Галатенко В.А. Основы информационной безопасности. Курс лекций. М.: ИНТУИТ.РУ «Интернет-университет Информационных технологий», 2004.
5. http://www.infosecurity.ru/
6. http://www.void.ru/

Резюме

В работе рассмотрены актуальные вопросы защиты информации, в частности, формирование пароля для входа в систему, приведены основные требования к длине, к содержанию пароля и дано определение понятию безопасное время работы системы.

Summary

Actual questions of information security, parole formation to the system are considered in the work. Main requirements to the length and the definition safety time of system.