ЗАШТИТА ПОДАТАКА

ЗАШТИТА СИСТЕМА

Управљање шифрама

Преглед

- Биће објашњено:
  - Заштита шифрама
  - Слаба тачка шифри
  - Контрола приступа
  - Стратегије за избор шифара

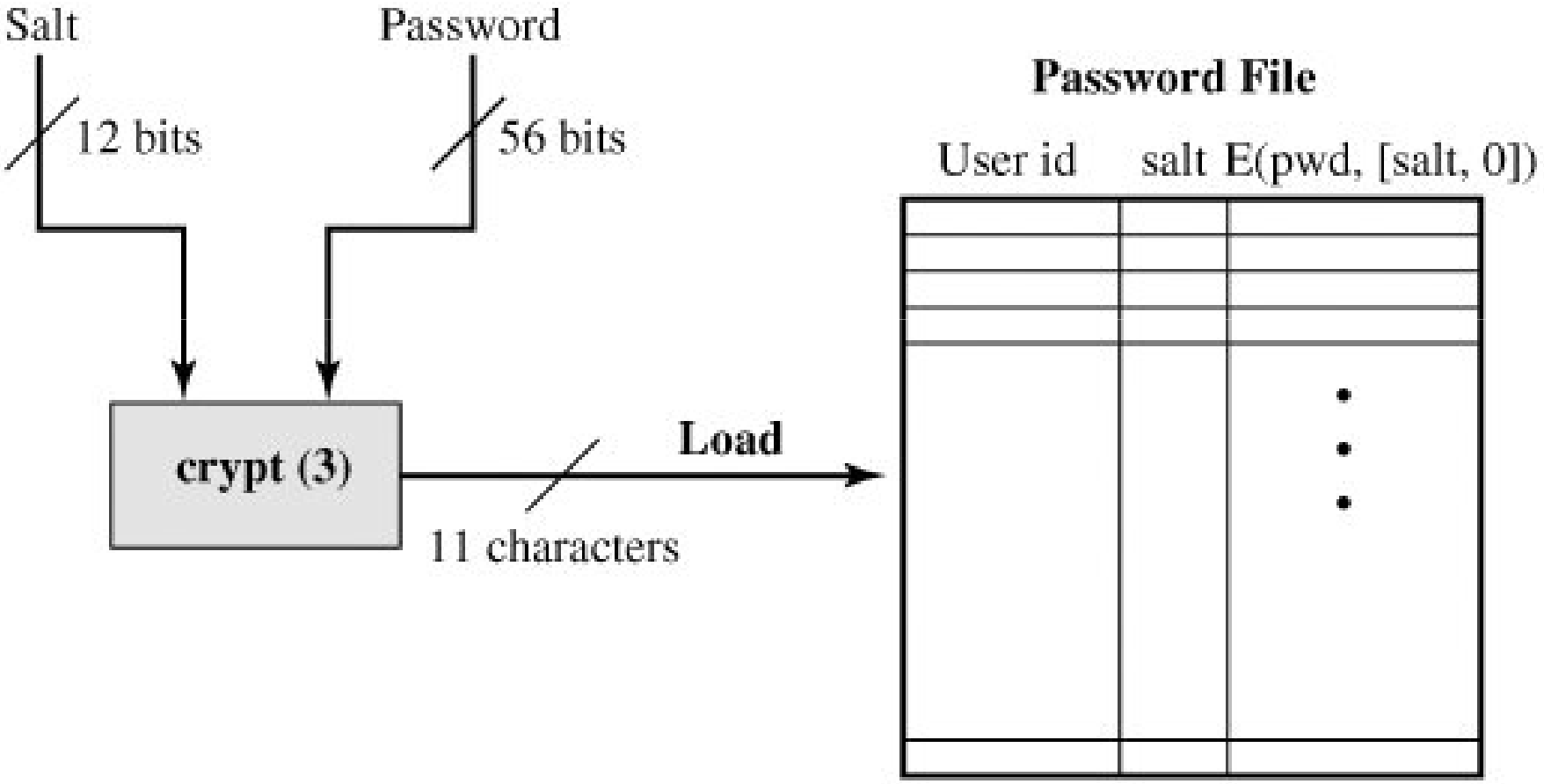
Заштита шифрама

- Прва линија заштите од уљеза су системи шифара.
- Користи се идентификатор корисника и шифра корисника.
- Шифра корисника служи за аутентикацију корисника.
- Идентификатор корисника помаже безбедност на следеће начине:
  - одређује да ли корисник уопште има право приступа систему (пример, рачунски центар, приступ имају само корисници који постоје у систему).
  - одређује привилегије које корисник има на систему (пример, ваше корисничко име у павиљону и администраторско корисничко име у павиљону). Неки системи дозвољавају корисницима који немају налог на систему да буду на систему (guest), као на пример на форуму ЕТФ-а.
  - користи се за дискреционо право приступа (нпр. један корисник може да дозволи групи осталих корисника да читају фајлове, чији је он власник, тако што наведе њихове идентификаторе).

Слаба тачка шифри

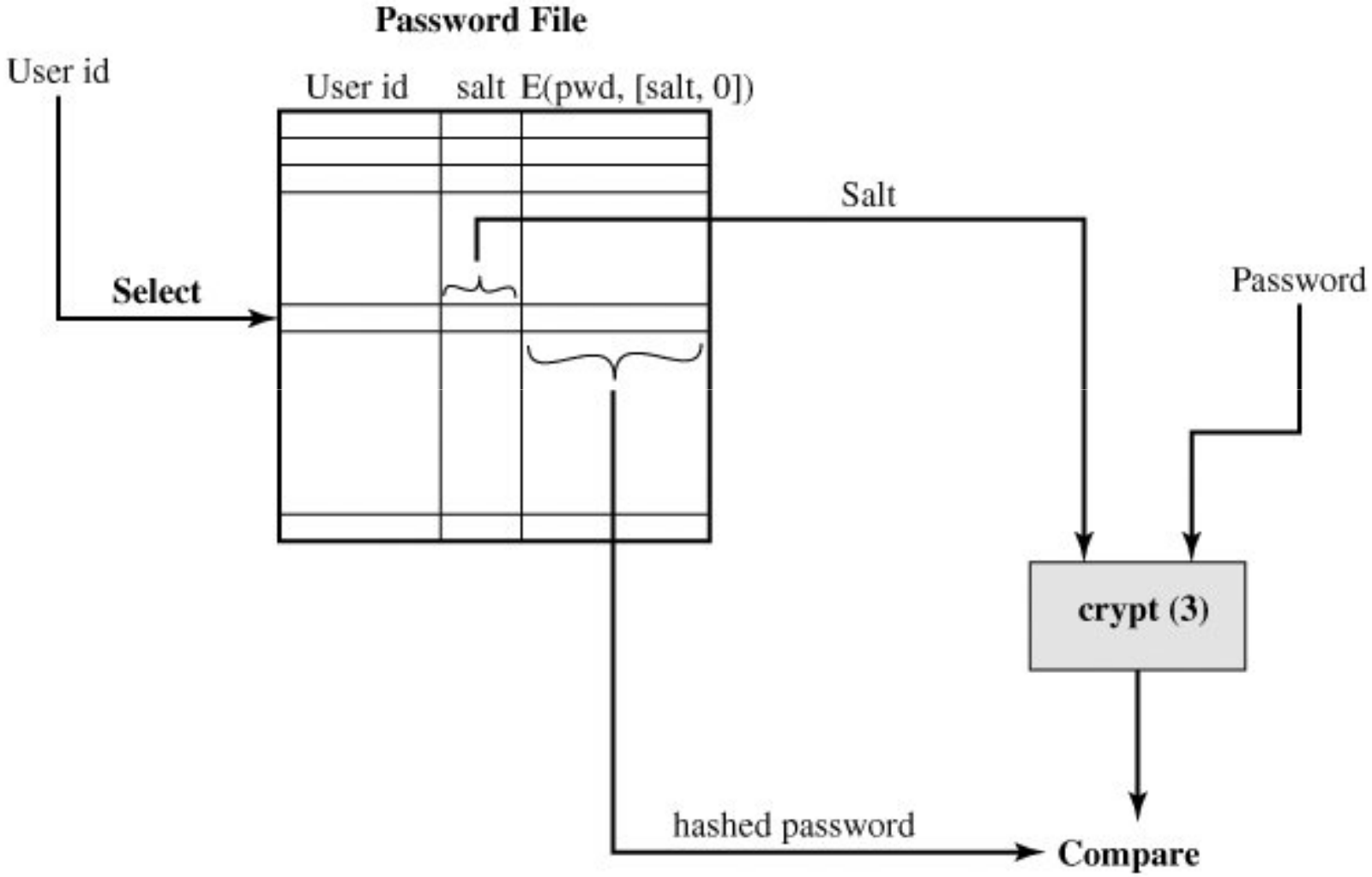
- Размотримо шему која се користи код UNIX оперативног система, код кога се шифре никада не чувају у оригиналу.
- Поштује се следећа процедура:
  - Сваки корисник бира шифру која је дужине до 8 принтабилних карактера,
  - Шифра се конвертује у 56-битну вредност (коришћењем 7-bit ASCII), која служи као кључ за енкрипцију,
  - Користи се енкрипција crypt(3), која је базирана на DES,
  - DES алгоритам је модификован коришћењем 12-битне "слане" вредности (salt = слано, метафора, зачињено, другачијег укуса), која је заснована на времену додељивања шифре кориснику,
  - DES алгоритам се примењује са улазом за податке који има 64-битне блокове нула,
  - Излаз служи као улаз за другу енкрипцију, и овај поступак се понавља 25 пута,
  - резултујућих 64-бита се на крају преводе у секвенцу од 11 карактера.
  - И на крају се овакав резултат снима, као и 12-битна слана вредност у оригиналу.

Слаба тачка шифри (2)



(a) Loading a new password

Слаба тачка шифри (3)



(b) Verifying a password

Слаба тачка шифри (4)

- Слана вредност се користи да:
  - Спречава да постоје дуплициране шифре.
  - Повећава дужину шифри.
  - Спречава коришћење хардверске имплементације DES алгоритма, чиме отежава brute-force нападе погађањем шифара.

Слаба тачка шифри (5)

- Предложена шема за шифровање дизајнирана је да обесхрабри нападе погажањем:
  - софтверска имплементација DES алгоритма је спорија,
  - плус користи се 25 шифровања.
- Међутим, од креирања ове шеме две ствари су се промениле:
  - појавиле су се нове имплементације алгоритма које су брже
  - и хардвер је напредовао, па су сада и софтверске имплементације брже.

Слаба тачка шифри (5)

- Постоје две претње за UNIX шему за шифре.
- Прва је да корисник који добије приступ машини као гост или на неки други начин може да изврши програм који погађа шифре на тој машини. А ако успе да добије копију фајла са шифрама, онда може да покреће програме за погађање шифри и на другим машинама.
- Друга је та, што су студије показале, да корисници када им се дозволи да слободно бирају шифре, бирају шифре са јако малим бројем карактера. Али поред тога бирају шифре које могу да се погоде.

Слаба тачка шифри (5)

- Пример из једне студије о дужини шифара.

Length	Number	Fraction of Total
1	55	.004
2	87	.006
3	212	.02
4	449	.03
5	1260	.09
6	3035	.22
7	2917	.21
8	5772	.42
Total	13787	1.0

Слаба тачка шифри (5)

- Пример стратегије за погађање шифара:
  - Покушати са именом, иницијалима и осталим личним информацијама корисника.
  - Покушати са речима из речника.
  - Покушати са пермутацијама речи из претходне тачке.
  - Покушати са комбинацијама малих и великих слова у речима из тачке 2.

Слаба тачка шифри (5)

- Резултати из претходног примера:

Type of Password	Search Size	Number of Matches	Percentage of Passwords Matched	Cost/Benefit Ratio[a]
User/account name	130	368	2.7%	2.830
Character sequences	866	22	0.2%	0.025
Numbers	427	9	0.1%	0.021
Chinese	392	56	0.4%	0.143
Place names	628	82	0.6%	0.131
Common names	2239	548	4.0%	0.245
Female names	4280	161	1.2%	0.038
Male names	2866	140	1.0%	0.049
Uncommon names	4955	130	0.9%	0.026
Myths & legends	1246	66	0.5%	0.053
Shakespearean	473	11	0.1%	0.023
Sports terms	238	32	0.2%	0.134
Science fiction	691	59	0.4%	0.085
Movies and actors	99	12	0.1%	0.121
Cartoons	92	9	0.1%	0.098
Famous people	290	55	0.4%	0.190
Phrases and patterns	933	253	1.8%	0.271
Surnames	33	9	0.1%	0.273
Biology	58	1	0.0%	0.017
System dictionary	19683	1027	7.4%	0.052
Machine names	9018	132	1.0%	0.015
Mnemonics	14	2	0.0%	0.143
King James bible	7525	83	0.6%	0.011
Miscellaneous words	3212	54	0.4%	0.017
Yiddish words	56	0	0.0%	0.000
Asteroids	2407	19	0.1%	0.007
TOTAL	62727	3340	24.2%	0.053

Контрола приступа

- Један начин да се спрече напади на шифре, јесте да се противнику забрани приступ до фајла са шифрама.
- Ако је приступ шифрованом делу фајлу омогућен само привилегованим корисницима, онда противник не може да га прочита, ако не зна шифру привилегованог корисника.
- Мане ове стратегије су:
  - Када неки нападач дође до било каквог налога на систему, онда може да покушава да дође до налога са већим привилегијама.
  - Незгода у заштити може да угрози читљивост фајла са шифрама и на тај начин онемогући приступ свим корисницима.
  - Неки корисници имају налоге на више машина са различитим начинима заштите. Такви корисници обично користе исте шифре, тако да неко може да дође до шифре корисника на некој слабије брањеној машини и да онда има приступ и на јаче брањеним машинама.
- Ефикаснија стратегија би била, натерати кориснике да бирају шифре које су теже за погађање.

Стратегије за избор шифара

- Корисници сами бирају шифре - шифре мале и лаке за погађање.
- Систем одређује шифре - шифре велике, тешке за погађање, тешке за памћење.
- Циљ је допустити корисницима да сами бирају шифре, али елиминисати шифре које су лаке за погађање.
- Четири основне технике којима се постиже претходно су:
  - Едукација корисника,
  - Рачунарски генерисане шифре
  - Реактивна провера шифре
  - Проактивна провера шифре

Стратегије за избор шифара (2)

- Едукација корисника - подразумева објашњавање корисницима важности коришћења шифара које су тешке за погађање и давање упутстава корисницима како да изаберу шифре које су тешке за погађање. Ова техника ретко даје резултате, јер ће већина корисника игнорисати инструкције, а много њих и неће разумети шта су јаке шифре (неки мисле да је то реч написана обрнуто, или мешање малих и великих слова).
- Рачунарски генерисане шифре - такође имају проблема. Ако су шифре скроз случајне, корисници ће их тешко памтити. Због тога ће корисници бити у искушењу да их записују.
- Реактивна провера шифара - подразумева систем који повремено сам покреће програме за погађање шифара, да би нашао шифре које су лаке за погађање. Систем поништава све шифре које су погођене и обавештава кориснике о томе. И овај метод има мана. Прво, заузима доста ресурса. А наравно да ће прави нападач имати више ресуурса на располагању за исту ствар. Друго, све шифре које су лаке за погађање остају незаштићене, све док их систем не пронађе.

Стратегије за избор шифара (3)

- Проактивна провера шифара - кориснику је дозвољено да изабере своју шифру, али, у време избора шифре, систем проверава да ли је шифра допустива и ако није, одбија такву шифру. Овај метод заснива се на филозофији да корисници, уз одговарајућа упутства, могу изабрати шифре које су лако памтљиве, а истовремено тешке за погађање.
- Трик код овог метода је да се нађе баланс између лакоће памћења шифре и јачине шифре.
  - Ако систем одбије превише шифара корисници ће се бунити
  - Ако систем користи једноставан алгоритам да дефинише шта је прихватљиво, онда омогућава нападачима да још више усаврше своје технике погађања.
- Неколико варијанти:
  - систем заснован на правилима (дуже од 8 карактера, мора бити једно велико слово, једно мало, ...) - праве добре шифре, откривају нападачима које шифре сигурно нису у игри
  - систем заснован на речнику недозвољених шифара (одбија све из речника) - добар систем, мане велик речник, време претраживања
  - систем заснован на вероватноћама (Марковљев модел) - моделом се опишу дозвољене и недозвољене шифре, помоћу вероватноћа