Groupe de travail Réseau
Request for Comments : 1760
Catégorie : Information

N. Haller, Bellcore
février 1995
Traduction Claude Brière de L'Isle

Système S/KEY de mot de passe à utilisation unique

Statut de ce mémoire
Le présent mémoire apporte des informations pour la communauté de l'Internet. Le présent mémoire ne spécifie aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document décrit le système S/KEY* de mot de passe à utilisation unique tel que publié pour l'utilisation du public par Bellcore et tel que décrit dans la référence [3]. Une mise en œuvre de référence et une documentation sont disponibles par ftp anonyme à ftp.bellcore.com dans le répertoire pub/nmh/...

Vue générale
Une forme d'attaque sur les systèmes informatiques connectés à l'Internet est l'espionnage des connexions réseau pour obtenir les identifiants de connexion et les mots de passe des utilisateurs légitimes. Les identifiants de connexion et les mots de passe capturés sont, ultérieurement, utilisés pour obtenir l'accès au système. Le système S/KEY de mot de passe à utilisation unique est conçu pour contrer ce type d'attaque, appelée attaque par répétition.

Avec le système S/KEY, seul un mot de passe à utilisation unique traverse le réseau. La phrase de passe secrète de l'usager ne traverse jamais le réseau, à aucun moment, y compris lors de la connexion ou lors de l'exécution d'autres commandes qui exigent une authentification, telles que la commande UNIX passwd ou su. Donc, il n'est pas vulnérable à l'espionnage/attaques en répétition. Une sécurité améliorée est fournie par le fait qu'aucune information secrète n'a besoin d'être mémorisée sur un système, y compris sur l'hôte qu'on veut protéger.

Le système S/KEY protége des attaques passives externes contre le sous-système d'authentification. Il n'empêche pas que l'espionnage du réseau donne accès à des informations confidentielles, et ne fournit pas de protection contre les "chevaux de Troie" ou contre les attaques actives où l'intrus potentiel est capable d'intercepter et modifier le flux de paquets.

Introduction

Le fonctionnement du système S/KEY de mot de passe à utilisation unique présente deux faces. Du côté client, le mot de passe à utilisation unique approprié doit être généré. Du côté de l'hôte, le serveur doit vérifier le mot de passe à utilisation unique et permettre le changement en toute sécurité de la phrase de passe secrète de l'usager.

Un système client S/KEY passe la phrase secrète de l'usager à travers plusieurs applications d'une fonction de hachage sécurisé pour produire un mot de passe à utilisation unique. À chaque utilisation, le nombre d'applications est réduit de un. Donc une séquence unique de mots de passe est générée. Le système hôte S/KEY vérifie le mot de passe à utilisation unique en faisant un passage à travers la fonction de hachage sécurisé et pour comparer le résultat avec le mot de passe à utilisation unique précédent. Cette technique a été suggérée pour la première fois par Leslie Lamport [1].

Fonction de hachage sécurisée

Une fonction de hachage sécurisée est une fonction qu'il est facile de calculer dans la direction montante, mais qu'il est impossible de calculer dans le sens inverse. Le système S/KEY se fonde sur l'algorithme de résumé de message MD4 conçu par Ronald Rivest [2]. Depuis que le système d'authentification S/KEY est utilisé, le résumé de message MD5 a été publié. Nous avons choisi de continuer d'utiliser MD4 du fait qu'un grand nombre de programmes client ont été distribués. Certains sites ont généré des systèmes fonctionnellement similaires fondés sur MD5. Il est clair que clients et hôtes doivent utiliser la même fonction de hachage sécurisé pour interopérer.

Les mots de passe à utilisation unique du système S/KEY sont longs de 64 bits. On estime que c'est assez long pour être sûr et assez court pour être entré à la main (voir ci-dessous "Forme des mots de passe) lorsque nécessaire.

Le système S/KEY applique plusieurs fois la fonction de hachage sécurisé, ce qui produit un résultat final de 64 bits. MD4 accepte un nombre arbitraire de bits en entrée et produit un résultat de 128 bits. La fonction de hachage sécurisé S/KEY consiste à appliquer MD4 à une entrée de 64 bits et à replier le résultat de MD4 avec l'opération OU exclusif ou à produire un résultat de 64 bits.

Génération des mots de passe à utilisation unique

Cette section décrit le calcul des mots de passe S/KEY à utilisation unique. Il consiste en une étape préparatoire dans laquelle toutes les entrées sont combinées, en une étape de génération où la fonction de hachage sécurisé est appliquée plusieurs fois, et en une fonction de résultat où le mot de passe à utilisation unique de 64 bits est affiché sous une forme lisible.

La phrase de passe secrète du client peut être de n'importe quelle longueur et devrait être de plus de huit caractères. Comme la fonction de hachage sécurisé S/KEY décrite ci-dessus accepte une entrée de 64 bits, une étape préparatoire est nécessaire. Dans cette étape, la phrase de passe est enchaînée avec un germe qui est transmis en clair depuis le serveur. Ce germe qui n'est pas secret permet au client d'utiliser la même phrase de passe secrète sur plusieurs machines (en utilisant des germes différents) et de recycler en toute sécurité les mots de passe secrets en changeant le germe. (Pour faciliter l'analyse, le germe ne doit pas contenir de blancs, et devrait consister en caractères strictement alphanumériques.) Le résultat de l'enchaînement est passé par MD4, puis est réduit à 64 bits par l'opération de OU exclusif sur les deux moitiés de huit octets.

Le fragment de code qui suit utilise la mise en œuvre de MD4 définie dans la RFC1320 [2] et définit l'étape préparatoire :

```
strcpy(buf,seed);
strcat(buf,passwd);
MDbegin(&md)
MDupdate(&md,(unsigned char *)buf,8*buflen);          /* Replier le résultat sur 64 bits */
md.buffer[0] ^= md.buffer[2];
md.buffer[1] ^= md.buffer[3];
```

Une séquence de mots de passe à utilisation unique est produite en appliquant plusieurs fois la fonction de hachage sécurisé au résultat de l'étape préparatoire (qu'on appellera S). C'est-à-dire que le premier mot de passe à utilisation unique est produit en passant S à travers la fonction de hachage sécurisé en certain nombre de fois (N) spécifié par l'usager. Le mot de passe à utilisation unique suivant est généré en passant S N-1 fois à travers la fonction de hachage sécurisé. Un espion qui aura surveillé la transmission d'un mot de passe à utilisation unique ne sera pas capable de générer un mot de passe qui réussisse parce que le faire exigerait d'inverser la fonction de hachage.

Forme des mots de passe

Le mot de passe à utilisation unique généré par la procédure ci-dessus fait 64 bits. Entrer un nombre de 64 bits est un processus difficile et enclin à l'erreur. Certains programmes de calcul de mot de passe à utilisation unique de systèmes S/KEY insèrent ce mot de passe dans le flux d'entrée, d'autres le rendent disponible par un système de couper/coller. Certains arrangements exigent que le mot de passe à utilisation unique soit entré manuellement. Le système S/KEY est conçu de façon à faciliter cette entrée manuelle sans gêner les méthodes automatiques. Le mot de passe à utilisation unique est donc converti, et accepté comme une séquence de six courts (de 1 à 4 lettres) mots anglais. Chaque mot est choisi dans un dictionnaire de 2048 mots ; à 11 bits par mot, tous les mots de passe à utilisation unique peuvent être codés. L'interopérabilité exige que tous les hôtes et calculateurs de système S/KEY utilisent le même dictionnaire. Le dictionnaire standard est joint à la présente RFC.

Vérification des mots de passe à utilisation unique

Une fonction sur le système hôte qui exige l'authentification S/KEY est supposée produire un défi S/KEY. Ce défi donne au client les paramètres S/KEY actuels – le numéro de séquence et le germe. Il est important que le défi S/KEY soit de format standard afin que les clients automatisés (voir ci-dessous) puissent reconnaître le défi et extraire les paramètres. Le format du défi est :

```
s/clé séquence_entier germe
```

Les trois jetons sont séparés par un seul caractère espace. Le défi est terminé par un blanc ou une nouvelle ligne.

Les paramètres et la phrase de passe secrète étant donnés, le client peut calculer (ou rechercher) le mot de passe à utilisation unique. Il le passe alors au système hôte où il peut être vérifié.

Le système hôte a un fichier (sur la mise en œuvre UNIX de référence, c'est /etc/skeykeys) qui contient, pour chaque utilisateur, le mot de passe à utilisation unique provenant de la dernière connexion réussie, ou il peut être initialisé avec le premier mot de passe à utilisation unique de la séquence en utilisant la commande keyinit (ce nom de commande peut varier selon les mises en œuvre). Pour vérifier une tentative d'authentification, il passe le mot de passe à utilisation unique

transmis une fois à travers la fonction de hachage sécurisé. Si le résultat de cette opération correspond au mot de passe à utilisation unique précédent mémorisé, l'authentification est réussie et le mot de passe à utilisation unique accepté est mémorisé pour la prochaine utilisation.

Comme le nombre d'applications de fonctions de hachage exécuté par le client diminue de un à chaque fois, à un moment, l'usager doit réinitialiser le système pour pouvoir se connecter à nouveau. Cela se fait en utilisant la commande keyinit qui permet le changement de la phrase de passe secrète, le compte d'itérations, et le germe. Une technique fréquente est d'incrémenter un ou plusieurs chiffres en queue du germe et de réinitialiser le compte d'itérations (à quelque chose dans la gamme de 500 à 1000).

Clients

Plusieurs programmes sont disponibles pour calculer les mots de passe S/KEY à utilisation unique. La mise en œuvre de référence comporte les interfaces de ligne de commande pour les systèmes UNIX et PC (key), les interfaces TSR pour les PC (ctkey, termkey, et popkey), et les interfaces GUI pour Macintosh et Windows (keyapp et une interface Macintosh sans nom).

Le calculateur le plus basique est la commande key dont le format est :

key [compte -n] séquence germe

Le compte facultatif est utilisé pour afficher plus d'un seul mot de passe à utilisation unique. C'est utile pour créer une liste sur papier des mots de passe à utilisation unique.

Le calculateur le plus automatisé est le programme termkey qui fonctionne comme programme "Terminate and Stay Resident" (TSR) sur un PC. Il examine l'écran pour trouver les paramètres S/KEY, invite à la phrase de passe secrète, et range le mot de passe à utilisation unique dans la mémoire tampon du clavier.

Remerciements

L'idée de base de l'authentification S/KEY a d'abord été proposée par Leslie Lamport [1]. Le système spécifique décrit a été proposé par Phil Karn, qui a aussi écrit la plus grande partie de la mise en œuvre de référence.

Références

[1] Lamport, L., "Password Authentication with Insecure Communication", Communications à ACM 24.11, novembre 1981, pages 770-772.

[2] R. Rivest, "Algorithme de résumé de message MD4" RFC1320, avril 1992. *(Historique, Information)*

[3] Haller, N., "The S/KEY One-Time Password System", Minutes du Symposium ISOC sur les réseaux et la répartition de la sécurité des systèmes, février 1994, San Diego, CA

[4] N. Haller et R. Atkinson, "Authentification sur l'Internet", RFC1704, octobre 1994. *(Information)*

Considérations pour la sécurité

La totalité du présent document concerne la sécurité.

Adresse de l'auteur

Neil Haller
Bellcore
MRE 2Q-280
445 South Street
Morristown, NJ, 07960-6438,
USA

téléphone : +1 201 829-4478
fax : +1 201 829-2504
mél : nmh@bellcore.com

Dictionnaire pour la conversion de mot S/KEY en formats binaires

Le présent dictionnaire est tiré du module put.c. Le code pour ce module, et une mise en œuvre du système complet de mot de passe S/KEY à utilisation unique est disponible par FTP anonyme à ftp.bellcore.com dans le répertoire pub/nmh/skey.

{ "A", "ABE", "ACE", "ACT", "AD", "ADA", "ADD", "AGO", "AID", "AIM", "AIR", "ALL", "ALP",
"AM", "AMY", "AN", "ANA", "AND", "ANN", "ANT", "ANY", "APE", "APS", "APT", "ARC", "ARE",
"ARK", "ARM", "ART", "AS", "ASH", "ASK", "AT", "ATE", "AUG", "AUK", "AVE", "AWE", "AWK",
"AWL", "AWN", "AX", "AYE", "BAD", "BAG", "BAH", "BAM", "BAN", "BAR", "BAT", "BAY", "BE",
"BED", "BEE", "BEG", "BEN", "BET", "BEY", "BIB", "BID", "BIG", "BIN", "BIT", "BOB", "BOG",
"BON", "BOO", "BOP", "BOW", "BOY", "BUB", "BUD", "BUG", "BUM", "BUN", "BUS", "BUT",
"BUY", "BY", "BYE", "CAB", "CAL", "CAM", "CAN", "CAP", "CAR", "CAT", "CAW", "COD", "COG",
"COL", "CON", "COO", "COP", "COT", "COW", "COY", "CRY", "CUB", "CUE", "CUP", "CUR", "CUT",
"DAB", "DAD", "DAM", "DAN", "DAR", "DAY", "DEE", "DEL", "DEN", "DES", "DEW", "DID", "DIE",
"DIG", "DIN", "DIP", "DO", "DOE", "DOG", "DON", "DOT", "DOW", "DRY", "DUB", "DUD", "DUE",
"DUG", "DUN", "EAR", "EAT", "ED", "EEL", "EGG", "EGO", "ELI", "ELK", "ELM", "ELY", "EM",
"END", "EST", "ETC", "EVA", "EVE", "EWE", "EYE", "FAD", "FAN", "FAR", "FAT", "FAY", "FED",
"FEE", "FEW", "FIB", "FIG", "FIN", "FIR", "FIT", "FLO", "FLY", "FOE", "FOG", "FOR", "FRY", "FUM",
"FUN", "FUR", "GAB", "GAD", "GAG", "GAL", "GAM", "GAP", "GAS", "GAY", "GEE", "GEL", "GEM",
"GET", "GIG", "GIL", "GIN", "GO", "GOT", "GUM", "GUN", "GUS", "GUT", "GUY", "GYM", "GYP",
"HA", "HAD", "HAL", "HAM", "HAN", "HAP", "HAS", "HAT", "HAW", "HAY", "HE", "HEM", "HEN",
"HER", "HEW", "HEY", "HI", "HID", "HIM", "HIP", "HIS", "HIT", "HO", "HOB", "HOC", "HOE",
"HOG", "HOP", "HOT", "HOW", "HUB", "HUE", "HUG", "HUH", "HUM", "HUT", "I", "ICY", "IDA",
"IF", "IKE", "ILL", "INK", "INN", "IO", "ION", "IQ", "IRA", "IRE", "IRK", "IS", "IT", "ITS", "IVY",
"JAB", "JAG", "JAM", "JAN", "JAR", "JAW", "JAY", "JET", "JIG", "JIM", "JO", "JOB", "JOE", "JOG",
"JOT", "JOY", "JUG", "JUT", "KAY", "KEG", "KEN", "KEY", "KID", "KIM", "KIN", "KIT", "LA",
"LAB", "LAC", "LAD", "LAG", "LAM", "LAP", "LAW", "LAY", "LEA", "LED", "LEE", "LEG", "LEN",
"LEO", "LET", "LEW", "LID", "LIE", "LIN", "LIP", "LIT", "LO", "LOB", "LOG", "LOP", "LOS", "LOT",
"LOU", "LOW", "LOY", "LUG", "LYE", "MA", "MAC", "MAD", "MAE", "MAN", "MAO", "MAP",
"MAT", "MAW", "MAY", "ME", "MEG", "MEL", "MEN", "MET", "MEW", "MID", "MIN", "MIT", "MOB",
"MOD", "MOE", "MOO", "MOP", "MOS", "MOT", "MOW", "MUD", "MUG", "MUM", "MY", "NAB",
"NAG", "NAN", "NAP", "NAT", "NAY", "NE", "NED", "NEE", "NET", "NEW", "NIB", "NIL", "NIP",
"NIT", "NO", "NOB", "NOD", "NON", "NOR", "NOT", "NOV", "NOW", "NU", "NUN", "NUT", "O",
"OAF", "OAK", "OAR", "OAT", "ODD", "ODE", "OF", "OFF", "OFT", "OH", "OIL", "OK", "OLD",
"ON", "ONE", "OR", "ORB", "ORE", "ORR", "OS", "OTT", "OUR", "OUT", "OVA", "OW", "OWE",
"OWL", "OWN", "OX", "PA", "PAD", "PAL", "PAM", "PAN", "PAP", "PAR", "PAT", "PAW", "PAY",
"PEA", "PEG", "PEN", "PEP", "PER", "PET", "PEW", "PHI", "PI", "PIE", "PIN", "PIT", "PLY", "PO",
"POD", "POE", "POP", "POT", "POW", "PRO", "PRY", "PUB", "PUG", "PUN", "PUP", "PUT", "QUO",
"RAG", "RAM", "RAN", "RAP", "RAT", "RAW", "RAY", "REB", "RED", "REP", "RET", "RIB", "RID",
"RIG", "RIM", "RIO", "RIP", "ROB", "ROD", "ROE", "RON", "ROT", "ROW", "ROY", "RUB", "RUE",
"RUG", "RUM", "RUN", "RYE", "SAC", "SAD", "SAG", "SAL", "SAM", "SAN", "SAP", "SAT", "SAW",
"SAY", "SEA", "SEC", "SEE", "SEN", "SET", "SEW", "SHE", "SHY", "SIN", "SIP", "SIR", "SIS", "SIT",
"SKI", "SKY", "SLY", "SO", "SOB", "SOD", "SON", "SOP", "SOW", "SOY", "SPA", "SPY", "SUB",
"SUD", "SUE", "SUM", "SUN", "SUP", "TAB", "TAD", "TAG", "TAN", "TAP", "TAR", "TEA", "TED",
"TEE", "TEN", "THE", "THY", "TIC", "TIE", "TIM", "TIN", "TIP", "TO", "TOE", "TOG", "TOM",
"TON", "TOO", "TOP", "TOW", "TOY", "TRY", "TUB", "TUG", "TUM", "TUN", "TWO", "UN", "UP",
"US", "USE", "VAN", "VAT", "VET", "VIE", "WAD", "WAG", "WAR", "WAS", "WAY", "WE", "WEB",
"WED", "WEE", "WET", "WHO", "WHY", "WIN", "WIT", "WOK", "WON", "WOO", "WOW", "WRY",
"WU", "YAM", "YAP", "YAW", "YE", "YEA", "YES", "YET", "YOU", "ABED", "ABEL", "ABET",
"ABLE", "ABUT", "ACHE", "ACID", "ACME", "ACRE", "ACTA", "ACTS", "ADAM", "ADDS", "ADEN",
"AFAR", "AFRO", "AGEE", "AHEM", "AHOY", "AIDA", "AIDE", "AIDS", "AIRY", "AJAR", "AKIN", "ALAN",
"ALEC", "ALGA", "ALIA", "ALLY", "ALMA", "ALOE", "ALSO", "ALTO", "ALUM", "ALVA", "AMEN",
"AMES", "AMID", "AMMO", "AMOK", "AMOS", "AMRA", "ANDY", "ANEW", "ANNA", "ANNE", "ANTE",
"ANTI", "AQUA", "ARAB", "ARCH", "AREA", "ARGO", "ARID", "ARMY", "ARTS", "ARTY", "ASIA",
"ASKS", "ATOM", "AUNT", "AURA", "AUTO", "AVER", "AVID", "AVIS", "AVON", "AVOW", "AWAY",
"AWRY", "BABE", "BABY", "BACH", "BACK", "BADE", "BAIL", "BAIT", "BAKE", "BALD", "BALE",
"BALI", "BALK", "BALL", "BALM", "BAND", "BANE", "BANG", "BANK", "BARB", "BARD", "BARE",
"BARK", "BARN", "BARR", "BASE", "BASH", "BASK", "BASS", "BATE", "BATH", "BAWD", "BAWL",
"BEAD", "BEAK", "BEAM", "BEAN", "BEAR", "BEAT", "BEAU", "BECK", "BEEF", "BEEN", "BEER",
"BEET", "BELA", "BELL", "BELT", "BEND", "BENT", "BERG", "BERN", "BERT", "BESS", "BEST", "BETA",

"BETH", "BHOY", "BIAS", "BIDE", "BIEN", "BILE", "BILK", "BILL", "BIND", "BING", "BIRD", "BITE", "BITS", "BLAB", "BLAT", "BLED", "BLEW", "BLOB", "BLOC", "BLOT", "BLOW", "BLUE", "BLUM", "BLUR", "BOAR", "BOAT", "BOCA", "BOCK", "BODE", "BODY", "BOGY", "BOHR", "BOIL", "BOLD", "BOLO", "BOLT", "BOMB", "BONA", "BOND", "BONE", "BONG", "BONN", "BONY", "BOOK", "BOOM", "BOON", "BOOT", "BORE", "BORG", "BORN", "BOSE", "BOSS", "BOTH", "BOUT", "BOWL", "BOYD", "BRAD", "BRAE", "BRAG", "BRAN", "BRAY", "BRED", "BREW", "BRIG", "BRIM", "BROW", "BUCK", "BUDD", "BUFF", "BULB", "BULK", "BULL", "BUNK", "BUNT", "BUOY", "BURG", "BURL", "BURN", "BURR", "BURT", "BURY", "BUSH", "BUSS", "BUST", "BUSY", "BYTE", "CADY", "CAFE", "CAGE", "CAIN", "CAKE", "CALF", "CALL", "CALM", "CAME", "CANE", "CANT", "CARD", "CARE", "CARL", "CARR", "CART", "CASE", "CASH", "CASK", "CAST", "CAVE", "CEIL", "CELL", "CENT", "CERN", "CHAD", "CHAR", "CHAT", "CHAW", "CHEF", "CHEN", "CHEW", "CHIC", "CHIN", "CHOU", "CHOW", "CHUB", "CHUG", "CHUM", "CITE", "CITY", "CLAD", "CLAM", "CLAN", "CLAW", "CLAY", "CLOD", "CLOG", "CLOT", "CLUB", "CLUE", "COAL", "COAT", "COCA", "COCK", "COCO", "CODA", "CODE", "CODY", "COED", "COIL", "COIN", "COKE", "COLA", "COLD", "COLT", "COMA", "COMB", "COME", "COOK", "COOL", "COON", "COOT", "CORD", "CORE", "CORK", "CORN", "COST", "COVE", "COWL", "CRAB", "CRAG", "CRAM", "CRAY", "CREW", "CRIB", "CROW", "CRUD", "CUBA", "CUBE", "CUFF", "CULL", "CULT", "CUNY", "CURB", "CURD", "CURE", "CURL", "CURT", "CUTS", "DADE", "DALE", "DAME", "DANA", "DANE", "DANG", "DANK", "DARE", "DARK", "DARN", "DART", "DASH", "DATA", "DATE", "DAVE", "DAVY", "DAWN", "DAYS", "DEAD", "DEAF", "DEAL", "DEAN", "DEAR", "DEBT", "DECK", "DEED", "DEEM", "DEER", "DEFT", "DEFY", "DELL", "DENT", "DENY", "DESK", "DIAL", "DICE", "DIED", "DIET", "DIME", "DINE", "DING", "DINT", "DIRE", "DIRT", "DISC", "DISH", "DISK", "DIVE", "DOCK", "DOES", "DOLE", "DOLL", "DOLT", "DOME", "DONE", "DOOM", "DOOR", "DORA", "DOSE", "DOTE", "DOUG", "DOUR", "DOVE", "DOWN", "DRAB", "DRAG", "DRAM", "DRAW", "DREW", "DRUB", "DRUG", "DRUM", "DUAL", "DUCK", "DUCT", "DUEL", "DUET", "DUKE", "DULL", "DUMB", "DUNE", "DUNK", "DUSK", "DUST", "DUTY", "EACH", "EARL", "EARN", "EASE", "EAST", "EASY", "EBEN", "ECHO", "EDDY", "EDEN", "EDGE", "EDGY", "EDIT", "EDNA", "EGAN", "ELAN", "ELBA", "ELLA", "ELSE", "EMIL", "EMIT", "EMMA", "ENDS", "ERIC", "EROS", "EVEN", "EVER", "EVIL", "EYED", "FACE", "FACT", "FADE", "FAIL", "FAIN", "FAIR", "FAKE", "FALL", "FAME", "FANG", "FARM", "FAST", "FATE", "FAWN", "FEAR", "FEAT", "FEED", "FEEL", "FEET", "FELL", "FELT", "FEND", "FERN", "FEST", "FEUD", "FIEF", "FIGS", "FILE", "FILL", "FILM", "FIND", "FINE", "FINK", "FIRE", "FIRM", "FISH", "FISK", "FIST", "FITS", "FIVE", "FLAG", "FLAK", "FLAM", "FLAT", "FLAW", "FLEA", "FLED", "FLEW", "FLIT", "FLOC", "FLOG", "FLOW", "FLUB", "FLUE", "FOAL", "FOAM", "FOGY", "FOIL", "FOLD", "FOLK", "FOND", "FONT", "FOOD", "FOOL", "FOOT", "FORD", "FORE", "FORK", "FORM", "FORT", "FOSS", "FOUL", "FOUR", "FOWL", "FRAU", "FRAY", "FRED", "FREE", "FRET", "FREY", "FROG", "FROM", "FUEL", "FULL", "FUME", "FUND", "FUNK", "FURY", "FUSE", "FUSS", "GAFF", "GAGE", "GAIL", "GAIN", "GAIT", "GALA", "GALE", "GALL", "GALT", "GAME", "GANG", "GARB", "GARY", "GASH", "GATE", "GAUL", "GAUR", "GAVE", "GAWK", "GEAR", "GELD", "GENE", "GENT", "GERM", "GETS", "GIBE", "GIFT", "GILD", "GILL", "GILT", "GINA", "GIRD", "GIRL", "GIST", "GIVE", "GLAD", "GLEE", "GLEN", "GLIB", "GLOB", "GLOM", "GLOW", "GLUE", "GLUM", "GLUT", "GOAD", "GOAL", "GOAT", "GOER", "GOES", "GOLD", "GOLF", "GONE", "GONG", "GOOD", "GOOF", "GORE", "GORY", "GOSH", "GOUT", "GOWN", "GRAB", "GRAD", "GRAY", "GREG", "GREW", "GREY", "GRID", "GRIM", "GRIN", "GRIT", "GROW", "GRUB", "GULF", "GULL", "GUNK", "GURU", "GUSH", "GUST", "GWEN", "GWYN", "HAAG", "HAAS", "HACK", "HAIL", "HAIR", "HALE", "HALF", "HALL", "HALO", "HALT", "HAND", "HANG", "HANK", "HANS", "HARD", "HARK", "HARM", "HART", "HASH", "HAST", "HATE", "HATH", "HAUL", "HAVE", "HAWK", "HAYS", "HEAD", "HEAL", "HEAR", "HEAT", "HEBE", "HECK", "HEED", "HEEL", "HEFT", "HELD", "HELL", "HELM", "HERB", "HERD", "HERE", "HERO", "HERS", "HESS", "HEWN", "HICK", "HIDE", "HIGH", "HIKE", "HILL", "HILT", "HIND", "HINT", "HIRE", "HISS", "HIVE", "HOBO", "HOCK", "HOFF", "HOLD", "HOLE", "HOLM", "HOLT", "HOME", "HONE", "HONK", "HOOD", "HOOF", "HOOK", "HOOT", "HORN", "HOSE", "HOST", "HOUR", "HOVE", "HOWE", "HOWL", "HOYT", "HUCK", "HUED", "HUFF", "HUGE", "HUGH", "HUGO", "HULK", "HULL", "HUNK", "HUNT", "HURD", "HURL", "HURT", "HUSH", "HYDE", "HYMN", "IBIS", "ICON", "IDEA", "IDLE", "IFFY", "INCA", "INCH", "INTO", "IONS", "IOTA", "IOWA", "IRIS", "IRMA", "IRON", "ISLE", "ITCH", "ITEM", "IVAN", "JACK", "JADE", "JAIL", "JAKE", "JANE", "JAVA", "JEAN", "JEFF", "JERK", "JESS", "JEST", "JIBE", "JILL", "JILT", "JIVE", "JOAN", "JOBS", "JOCK", "JOEL", "JOEY", "JOHN", "JOIN", "JOKE", "JOLT", "JOVE", "JUDD", "JUDE", "JUDO", "JUDY", "JUJU", "JUKE", "JULY", "JUNE", "JUNK", "JUNO", "JURY", "JUST", "JUTE", "KAHN", "KALE", "KANE", "KANT", "KARL", "KATE", "KEEL", "KEEN", "KENO", "KENT", "KERN", "KERR", "KEYS", "KICK", "KILL", "KIND", "KING", "KIRK", "KISS", "KITE", "KLAN", "KNEE", "KNEW", "KNIT", "KNOB", "KNOT", "KNOW", "KOCH", "KONG", "KUDO", "KURD", "KURT", "KYLE", "LACE", "LACK", "LACY", "LADY", "LAID", "LAIN", "LAIR", "LAKE", "LAMB", "LAME", "LAND", "LANE", "LANG", "LARD", "LARK", "LASS", "LAST", "LATE", "LAUD", "LAVA", "LAWN", "LAWS", "LAYS", "LEAD", "LEAF", "LEAK", "LEAN", "LEAR", "LEEK", "LEER", "LEFT", "LEND", "LENS", "LENT", "LEON", "LESK", "LESS", "LEST", "LETS", "LIAR", "LICE", "LICK", "LIED", "LIEN", "LIES", "LIEU", "LIFE", "LIFT", "LIKE", "LILA", "LILT", "LILY", "LIMA", "LIMB", "LIME", "LIND", "LINE", "LINK", "LINT", "LION", "LISA", "LIST", "LIVE", "LOAD", "LOAF", "LOAM", "LOAN", "LOCK", "LOFT", "LOGE",

"LOIS", "LOLA", "LONE", "LONG", "LOOK", "LOON", "LOOT", "LORD", "LORE", "LOSE", "LOSS", "LOST", "LOUD", "LOVE", "LOWE", "LUCK", "LUCY", "LUGE", "LUKE", "LULU", "LUND", "LUNG", "LURA", "LURE", "LURK", "LUSH", "LUST", "LYLE", "LYNN", "LYON", "LYRA", "MACE", "MADE", "MAGI", "MAID", "MAIL", "MAIN", "MAKE", "MALE", "MALI", "MALL", "MALT", "MANA", "MANN", "MANY", "MARC", "MARE", "MARK", "MARS", "MART", "MARY", "MASH", "MASK", "MASS", "MAST", "MATE", "MATH", "MAUL", "MAYO", "MEAD", "MEAL", "MEAN", "MEAT", "MEEK", "MEET", "MELD", "MELT", "MEMO", "MEND", "MENU", "MERT", "MESH", "MESS", "MICE", "MIKE", "MILD", "MILE", "MILK", "MILL", "MILT", "MIMI", "MIND", "MINE", "MINI", "MINK", "MINT", "MIRE", "MISS", "MIST", "MITE", "MITT", "MOAN", "MOAT", "MOCK", "MODE", "MOLD", "MOLE", "MOLL", "MOLT", "MONA", "MONK", "MONT", "MOOD", "MOON", "MOOR", "MOOT", "MORE", "MORN", "MORT", "MOSS", "MOST", "MOTH", "MOVE", "MUCH", "MUCK", "MUDD", "MUFF", "MULE", "MULL", "MURK", "MUSH", "MUST", "MUTE", "MUTT", "MYRA", "MYTH", "NAGY", "NAIL", "NAIR", "NAME", "NARY", "NASH", "NAVE", "NAVY", "NEAL", "NEAR", "NEAT", "NECK", "NEED", "NEIL", "NELL", "NEON", "NERO", "NESS", "NEST", "NEWS", "NEWT", "NIBS", "NICE", "NICK", "NILE", "NINA", "NINE", "NOAH", "NODE", "NOEL", "NOLL", "NONE", "NOOK", "NOON", "NORM", "NOSE", "NOTE", "NOUN", "NOVA", "NUDE", "NULL", "NUMB", "OATH", "OBEY", "OBOE", "ODIN", "OHIO", "OILY", "OINT", "OKAY", "OLAF", "OLDY", "OLGA", "OLIN", "OMAN", "OMEN", "OMIT", "ONCE", "ONES", "ONLY", "ONTO", "ONUS", "ORAL", "ORGY", "OSLO", "OTIS", "OTTO", "OUCH", "OUST", "OUTS", "OVAL", "OVEN", "OVER", "OWLY", "OWNS", "QUAD", "QUIT", "QUOD", "RACE", "RACK", "RACY", "RAFT", "RAGE", "RAID", "RAIL", "RAIN", "RAKE", "RANK", "RANT", "RARE", "RASH", "RATE", "RAVE", "RAYS", "READ", "REAL", "REAM", "REAR", "RECK", "REED", "REEF", "REEK", "REEL", "REID", "REIN", "RENA", "REND", "RENT", "REST", "RICE", "RICH", "RICK", "RIDE", "RIFT", "RILL", "RIME", "RING", "RINK", "RISE", "RISK", "RITE", "ROAD", "ROAM", "ROAR", "ROBE", "ROCK", "RODE", "ROIL", "ROLL", "ROME", "ROOD", "ROOF", "ROOK", "ROOM", "ROOT", "ROSA", "ROSE", "ROSS", "ROSY", "ROTH", "ROUT", "ROVE", "ROWE", "ROWS", "RUBE", "RUBY", "RUDE", "RUDY", "RUIN", "RULE", "RUNG", "RUNS", "RUNT", "RUSE", "RUSH", "RUSK", "RUSS", "RUST", "RUTH", "SACK", "SAFE", "SAGE", "SAID", "SAIL", "SALE", "SALK", "SALT", "SAME", "SAND", "SANE", "SANG", "SANK", "SARA", "SAUL", "SAVE", "SAYS", "SCAN", "SCAR", "SCAT", "SCOT", "SEAL", "SEAM", "SEAR", "SEAT", "SEED", "SEEK", "SEEM", "SEEN", "SEES", "SELF", "SELL", "SEND", "SENT", "SETS", "SEWN", "SHAG", "SHAM", "SHAW", "SHAY", "SHED", "SHIM", "SHIN", "SHOD", "SHOE", "SHOT", "SHOW", "SHUN", "SHUT", "SICK", "SIDE", "SIFT", "SIGH", "SIGN", "SILK", "SILL", "SILO", "SILT", "SINE", "SING", "SINK", "SIRE", "SITE", "SITS", "SITU", "SKAT", "SKEW", "SKID", "SKIM", "SKIN", "SKIT", "SLAB", "SLAM", "SLAT", "SLAY", "SLED", "SLEW", "SLID", "SLIM", "SLIT", "SLOB", "SLOG", "SLOT", "SLOW", "SLUG", "SLUM", "SLUR", "SMOG", "SMUG", "SNAG", "SNOB", "SNOW", "SNUB", "SNUG", "SOAK", "SOAR", "SOCK", "SODA", "SOFA", "SOFT", "SOIL", "SOLD", "SOME", "SONG", "SOON", "SOOT", "SORE", "SORT", "SOUL", "SOUR", "SOWN", "STAB", "STAG", "STAN", "STAR", "STAY", "STEM", "STEW", "STIR", "STOW", "STUB", "STUN", "SUCH", "SUDS", "SUIT", "SULK", "SUMS", "SUNG", "SUNK", "SURE", "SURF", "SWAB", "SWAG", "SWAM", "SWAN", "SWAT", "SWAY", "SWIM", "SWUM", "TACK", "TACT", "TAIL", "TAKE", "TALE", "TALK", "TALL", "TANK", "TASK", "TATE", "TAUT", "TEAL", "TEAM", "TEAR", "TECH", "TEEM", "TEEN", "TEET", "TELL", "TEND", "TENT", "TERM", "TERN", "TESS", "TEST", "THAN", "THAT", "THEE", "THEM", "THEN", "THEY", "THIN", "THIS", "THUD", "THUG", "TICK", "TIDE", "TIDY", "TIED", "TIER", "TILE", "TILL", "TILT", "TIME", "TINA", "TINE", "TINT", "TINY", "TIRE", "TOAD", "TOGO", "TOIL", "TOLD", "TOLL", "TONE", "TONG", "TONY", "TOOK", "TOOL", "TOOT", "TORE", "TORN", "TOTE", "TOUR", "TOUT", "TOWN", "TRAG", "TRAM", "TRAY", "TREE", "TREK", "TRIG", "TRIM", "TRIO", "TROD", "TROT", "TROY", "TRUE", "TUBA", "TUBE", "TUCK", "TUFT", "TUNA", "TUNE", "TUNG", "TURF", "TURN", "TUSK", "TWIG", "TWIN", "TWIT", "ULAN", "UNIT", "URGE", "USED", "USER", "USES", "UTAH", "VAIL", "VAIN", "VALE", "VARY", "VASE", "VAST", "VEAL", "VEDA", "VEIL", "VEIN", "VEND", "VENT", "VERB", "VERY", "VETO", "VICE", "VIEW", "VINE", "VISE", "VOID", "VOLT", "VOTE", "WACK", "WADE", "WAGE", "WAIL", "WAIT", "WAKE", "WALE", "WALK", "WALL", "WALT", "WAND", "WANE", "WANG", "WANT", "WARD", "WARM", "WARN", "WART", "WASH", "WAST", "WATS", "WATT", "WAVE", "WAVY", "WAYS", "WEAK", "WEAL", "WEAN", "WEAR", "WEED", "WEEK", "WEIR", "WELD", "WELL", "WELT", "WENT", "WERE", "WERT", "WEST", "WHAM", "WHAT", "WHEE", "WHEN", "WHET", "WHOA", "WHOM", "WICK", "WIFE", "WILD", "WILL", "WIND", "WINE", "WING", "WINK", "WINO", "WIRE", "WISE", "WISH", "WITH", "WOLF", "WONT", "WOOD", "WOOL", "WORD", "WORE", "WORK", "WORM", "WORN", "WOVE", "WRIT", "WYNN", "YALE", "YANG", "YANK", "YARD", "YARN", "YAWL", "YAWN", "YEAH", "YEAR", "YELL", "YOGA", "YOKE" };