WPROWADZENIE

Autoryzacja to przydzielanie uprawnień dla określonych typów dostępu do zastrzeżonych informacji. W prawdziwym świecie upoważnienie jest przyznawane prawdziwym istotom ludzkim; z kolei technologia informacyjna zwykle przyznaje autoryzację identyfikatorom użytkownika (identyfikatorom). Systemy komputerowe muszą łączyć określone identyfikatory z określonymi upoważnionymi użytkownikami tych identyfikatorów. Nawet nieożywione komponenty, takie jak karty sieciowe, zapory sieciowe i drukarki, wymagają identyfikatorów. Identyfikacja to proces przypisywania identyfikatora człowiekowi lub innemu komputerowi lub elementowi sieci. Uwierzytelnianie to proces wiązania identyfikatora z określoną jednostką. Na przykład uwierzytelnianie tożsamości użytkownika ogólnie obejmuje zawężenie zakresu możliwych podmiotów twierdzących, że autoryzowały użycie określonego identyfikatora do jednej osoby. W tym rozdziale skupiamy się na uwierzytelnianiu typu „osoba do komputera". W praktyce potrzebujemy również uwierzytelniania między komputerami, aby zapobiec fałszowaniu usług w sieci. Ten rodzaj uwierzytelniania ma coraz większe znaczenie, zwłaszcza w sieciach otwartych, takich jak Internet, gdzie użytkownicy mogą być wprowadzani w błąd co do tożsamości odwiedzanych witryn internetowych. Na przykład niektórzy przestępcy wysyłają do ofiar niechciane wiadomości e-mail w języku Hypertext Markup Language (HTML); wiadomości zawierają linki, które są oznaczone etykietami sugerującymi nieszkodliwą lub szanowaną witrynę internetową, ale znajdujący się pod nim kod HTML w rzeczywistości prowadzi do oszukańczej witryny zaprojektowanej w celu nakłonienia ludzi do ujawnienia danych osobowych, takich jak numery kart kredytowych lub dane umożliwiające kradzież tożsamości. Mówiąc bardziej ogólnie, wzajemne uwierzytelnianie komputer-komputer, zwykle w obu kierunkach, jest niezbędne do zabezpieczenia transakcji o znaczeniu krytycznym, takich jak przelewy międzybankowe i handel elektroniczny między przedsiębiorstwami. We wczesnych dziesięcioleciach użytkowania komputerów większość komputerów uwierzytelniała użytkowników, którzy uzyskiwali dostęp do komputerów typu mainframe z jednego przedsiębiorstwa. Dlatego też identyfikatory użytkowników można przypisywać w sposób scentralizowany i kontrolowany. Mimo to identyfikatory nigdy nie były niepowtarzalne, ponieważ nie ma obowiązkowej relacji jeden do jednego między identyfikatorem użytkownika a rzeczywistą tożsamością człowieka. Na przykład kilka osób może udostępniać konto takie jak inwentarz bez ingerencji ze strony komputera; co najwyżej system operacyjny można skonfigurować tak, aby uniemożliwić jednoczesne udostępnianie identyfikatora poprzez ograniczenie liczby sesji inicjowanych z określonym identyfikatorem do jednego. I odwrotnie, pojedynczy użytkownik często ma wiele identyfikatorów użytkowników. Na przykład mogą istnieć unikalne identyfikatory dla każdej z kilkudziesięciu witryn internetowych klubów muzycznych, klubów książki, e-mil firmy e-mail i tak dalej. Nawet na tym samym komputerze dany użytkownik może mieć kilka kont zdefiniowanych do różnych celów; jane doe i jdoe mogą być identyfikatorami dla dwóch różnych pakietów aplikacji w systemie. Te wielokrotne identyfikatory powodują problemy dla administratorów, jeśli nie wiedzą, że ten sam użytkownik jest powiązany z różnymi identyfikatorami; powodują również praktyczne problemy dla użytkowników, którzy muszą używać różnych metod uwierzytelniania dla różnych identyfikatorów. Jednym z krytycznych celów dzisiejszych badań i rozwoju w zakresie identyfikacji i uwierzytelniania (I&A) jest opracowanie niezawodnych i ekonomicznych metod pojedynczego logowania, dzięki którym użytkownicy nie musieliby ponownie identyfikować i uwierzytelniać się podczas uzyskiwania dostępu do różnych systemów komputerowych połączonych z Internetem.

CZTERY ZASADY UWIERZYTELNIANIA.

Uwierzytelnienie deklarowanej tożsamości można ustalić na cztery sposoby:

1. Co wiesz tylko Ty (hasła i hasła)

2. To, co masz tylko Ty (tokeny: klucze fizyczne, karty inteligentne)

3. Kim tylko Ty jesteś (statyczne dane biometryczne: rozpoznawanie odcisków palców, twarzy, siatkówki i tęczówki)

4. Co tylko Ty robisz (dynamiczne dane biometryczne: rozpoznawanie głosu, pisma ręcznego i pisania)

W każdym podejściu zakłada się, że nikt inny oprócz autoryzowanego użytkownika identyfikatora nie ma dostępu do hasła lub tokena, a prawdopodobieństwo symulacji danych statycznych lub biometrycznych jest akceptowalnie niskie. Metody te można łączyć; na przykład hasła często są łączone z tokenami lub danymi biometrycznymi w celu zapewnienia silniejszego uwierzytelnienia niż jest to możliwe w przypadku jednego z nich. Znany przykład tego dwuskładnikowego uwierzytelniania występuje w przypadku kart do bankomatów. Posiadanie karty (tokena) oraz znajomość osobistego numeru identyfikacyjnego (PIN, odpowiadający hasłu) są niezbędne do uzyskania dostępu do konta bankowego użytkownika. W tym rozdziale przedstawiono każdą z tych czterech metod uwierzytelniania i podano dodatkowe szczegóły dotyczące każdej z nich. Omówienie metod omijania i osłabiania technik identyfikacji i uwierzytelniania znajduje się w rozdziale 15 niniejszego podręcznika.

Co tylko Ty wiesz.

Uwierzytelnianie oparte na haśle lub frazie jest tak szeroko stosowane, że każda osoba, która miała jakikolwiek kontakt z komputerami i sieciami, prawdopodobnie miała kilka haseł. Chociaż technologia haseł jest często źle administrowana i niezabezpieczona (i frustrująca) dla użytkowników i administratorów, hasła mogą być wdrażane znacznie bezpieczniej i wygodniej niż zwykle. Wielu specjalistów ds.bezpieczeństwa od lat miało poczucie i nadzieję, że hasła zostaną ostatecznie wycofane i zastąpione tokenami lub danymi biometrycznymi, ale obecnie panuje zgoda co do tego, że hasła prawdopodobnie nie znikną wkrótce i będą nadal dominującą techniką uwierzytelniania Nadchodzących latach. Wykazanie się znajomością hasła nie powoduje bezpośredniego uwierzytelnienia człowieka. Po prostu uwierzytelnia znajomość hasła. Nieautoryzowana znajomość lub zgadywanie hasła może prowadzić do podszywania się pod jednego użytkownika przez innego; nazywa się to podszywaniem się. Kradzież hasła może być trudna do wykrycia, ponieważ nie jest to aktywa materialne. Hasła są również bardzo łatwe do udostępnienia. Kierownictwo wyższego szczebla często podaje swoje hasła swoim asystentom, aby ułatwić im pracę, mimo że przypisywanie uprawnień pełnomocnika byłoby równie skuteczne i bezpieczniejsze. Studenci hakerów zajmujących się bezpieczeństwem, w tym hakerów kryminalnych, szybko dowiadują się, że słabe zarządzanie hasłami może być powszechne, jeśli organizacje nie zapewnią spójnej świadomości, edukacji i szkoleń; na przykład naiwni użytkownicy czasami umieszczają swoje hasła na karteczkach samoprzylepnych pod klawiaturą lub nawet na widoku z boku swoich monitorów.

Co masz tylko Ty.

Uwierzytelnianie oparte na posiadaniu tokena jest stosowane tam, gdzie pożądane jest większe zapewnienie tożsamości niż jest to możliwe przy użyciu samych haseł. Podobnie jak w przypadku haseł, posiadanie tokena nie oznacza bezpośredniego uwierzytelnienia istoty ludzkiej; raczej poświadcza posiadanie tokena i możliwość jego użycia. Czasami do korzystania z tokena wymagane jest hasło lub kod PIN, ustanawiając w ten sposób uwierzytelnianie dwuskładnikowe; zgodnie z teorią wymóg posiadania obu elementów zmniejsza prawdopodobieństwo skutecznego spoofingu. Tokeny mogą przybierać różne formy. Najstarszym tokenem jest fizyczny klucz do fizycznego zamka, ale nie są one często używane do zabezpieczania systemów komputerowych. Miękkie tokeny są przenoszone na nośnikach przenośnych lub nawet dostępne przez sieć z serwera. Miękkie tokeny zawierają tylko dane;

zazwyczaj wymagają hasła, aby uzyskać dostęp do zawartości. Nowoczesne tokeny są zwykle implementowane na niezależnym sprzęcie z możliwością przetwarzania. Przykłady zawierają:

* Urządzenia wielkości karty kredytowej z wyświetlaczem ciekłokrystalicznym (LCD), które wyświetlają pseudolosowe numery lub inne kody.

* Urządzenia LCD w kształcie breloczka wykorzystujące te same algorytmy, co urządzenia w kształcie karty kredytowej.

* Urządzenia sprzętowe zwane kluczami sprzętowymi, które podłącza się do portów wejścia-wyjścia w komputerach. Przykłady obejmują klucze sprzętowe do portów szeregowych, portów równoległych, portów uniwersalnej magistrali szeregowej (USB) i interfejsów kart PC. Wszystkie tokeny używane do uwierzytelniania komputerów wymagają oprogramowania do przetwarzania informacji znajdujących się na nich lub przez nie wytworzonych. Najważniejsze rozróżnienie dotyczy tego, czy tokeny wymagają elektronicznego kontaktu z systemem uwierzytelniania. Tokeny zbliżeniowe są łatwiejsze do wdrożenia, ponieważ nie wymagają wyspecjalizowanych czytelników. Na przykład generatory pseudolosowych numerów kart kredytowych i breloków po prostu wymagają od użytkownika wprowadzenia widocznego kodu w odpowiedzi na monit oprogramowania uwierzytelniającego. Tokeny zbliżeniowe mają bardziej ograniczone funkcje niż tokeny kontaktowe. Na przykład token kontaktowy może służyć do tworzenia podpisów cyfrowych, podczas gdy token zbliżeniowy nie może tego zrobić praktycznie. W cyberprzestrzeni token nie jest uwierzytelniany na podstawie cech fizycznych. Raczej token ma jakiś sekret, albo wyłączny dla siebie, albo prawdopodobnie współdzielony z serwerem w sieci. Uwierzytelnienie tokena jest tak naprawdę uwierzytelnieniem wiedzy o sekrecie przechowywanym na tokenie. W związku z tym uwierzytelnianie oparte na posiadaniu tokena jest równoznaczne z uwierzytelnianiem na podstawie tego, co wie token. Jednak ten sekret może być dłuższy i bardziej losowy niż sekret, który użytkownik musi zachować w ludzkiej pamięci, na przykład hasło. Niestety, budowanie opłacalnych i bezpiecznych tokenów, z których sekretu nie można wydobyć poprzez manipulowanie lub zgadywanie brutalnej siły, okazało się znacznie trudniejsze niż początkowo przewidywano. We wczesnych latach 90. wielu specjalistów ds. Bezpieczeństwa wierzyło, że tokeny zastąpią hasła; w rzeczywistości jednak, chociaż tokeny nadal stanowią atrakcyjną technologię uwierzytelniania, prawdopodobnie nie staną się one wkrótce powszechne ze względu na konsekwentne (ale wysoce dyskusyjne) przekonanie, że wdrażanie i zarządzanie hasłami jest tańsze niż inne metody uwierzytelniania (patrz sekcja 28.7).

Kim tylko Ty jesteś.

Biometria przenosi uwierzytelnianie bezpośrednio na człowieka. Jako ludzie rozpoznajemy się na podstawie wielu cech. Uwierzytelnianie biometryczne ma na celu osiągnięcie podobnego rezultatu w cyberprzestrzeni. Biometria statyczna jest cechą charakterystyczną osoby, taką jak odcisk palca, geometria dłoni lub wzór tęczówki; bardziej dramatycznie, może to być DNA osoby. Prawdopodobieństwo, że dwie osoby będą miały identyczne odciski palców, wzory tęczówki lub DNA jest znikome (z wyjątkami dla identycznego genetycznie rodzeństwa). Biometria wymaga wyspecjalizowanych i drogich czytników do przechwytywania danych biometrycznych, co utrudnia ich powszechne wdrożenie. Biometria również boryka się z problemami związanymi z odtwarzaniem i manipulowaniem. Dlatego też czytnik biometryczny sam musi być zaufany i odporny na manipulacje; Zmniejsza to prawdopodobieństwo przechwycenia przez napastnika wprowadzonych danych i odtworzenia ich w późniejszym czasie lub tworzenia fałszywych profili biometrycznych, aby oszukać system i zaakceptować oszusta. Ponadto same dane biometryczne muszą być przechwytywane w pobliżu użytkownika, aby zmniejszyć prawdopodobieństwo zastąpienia, na przykład w przypadku kradzieży krwi wykorzystywanej do oszukania systemu biometrycznego opartego na DNA. Jeśli dane są

przesyłane do odległego serwera w celu uwierzytelnienia, transmisja wymaga bezpiecznego protokołu, z rozbudowanymi możliwościami oznaczania czasu i szybkim wygaśnięcie danych.

Co tylko ty robisz.

Dynamiczna biometria rejestruje dynamiczny proces, a nie statyczną charakterystykę osoby. Dobrze znanym przykładem jest dynamika podpisu. Dynamika podpisu polega na rejestrowaniu prędkości i przyspieszenia dłoni osoby, ponieważ podpis jest zapisywany na specjalnym tablecie. Nie tylko kształt podpisu, ale dynamiczna charakterystyka ruchu podczas pisania podpisu uwierzytelnia ruchy osoby, które są niezwykle trudne do zasymulowania. Inną możliwością jest rozpoznanie cech głosu osoby, gdy jest ona proszona o przeczytanie na głos określonego tekstu. Kolejną alternatywą jest dynamika naciśnięć klawiszy podczas pisania na klawiaturze. Podobnie jak we wszystkich innych formach uwierzytelniania, dynamiczna biometria polega na wykluczeniu ataków przechwytywania i odtwarzania, w których na przykład nagranie czyjegoś głosu może zostać użyte do oszukania systemu rozpoznawania głosu. Podobnie, system dynamiki sygnatur może zostać oszukany przez odtwarzanie danych zarejestrowanych z autentycznej sygnatury.

Techniki szyfrowania pomagają utrudnić takie ataki. Eksperci ds. Bezpieczeństwa są zgodni co do tego, że dane biometryczne zapewniają silniejszą gwarancję uwierzytelnienia, ale ich wdrożenie na dużą skalę nie zostało jeszcze wykazane. To, czy ta technologia stanie się w końcu wszechobecna, może ostatecznie zależeć od jej społecznej i politycznej akceptacji, a także od ulepszonej technologii.

UWIERZYTELNIANIE NA PODSTAWIE HASŁA.

Hasła to obecnie wszechobecna technologia uwierzytelniania w cyberprzestrzeni. Według ostrożnych szacunków dziennie dochodzi do blisko miliarda uwierzytelnień opartych na hasłach. Przykłady obejmują ogromną liczbę użytkowników Internetu i liczba haseł, z których każdy z nich korzysta na co dzień. Jednak obecne wdrażanie technologii haseł wymaga wielu ulepszeń. Obecnie użytkownicy muszą pamiętać zbyt wiele tożsamości i odpowiednich haseł. Ponadto zastosowana technologia jest bardziej wrażliwa niż powinna; na przykład wielu użytkowników wybiera hasła, które można łatwo odgadnąć. Hasła nigdy nie będą tak bezpieczne, jak najsilniejsze systemy biometryczne, więc nie można ich używać jako jedynej podstawy, powiedzmy, do wystrzeliwania pocisków jądrowych. Jednak ich użycie może być wystarczająco silne dla wielu mniej krytycznych transakcji. W następnych sekcjach omówiono główne zagrożenia związane z używaniem haseł i ich łagodzenie za pomocą środków technicznych, społecznych i proceduralnych.

Dostęp do haseł użytkowników przez administratorów systemu.

Jedną z najbardziej niebezpiecznych praktyk stosowanych obecnie jest przechowywanie niezaszyfrowanych haseł użytkowników dostępnych dla administratorów systemu. W niektórych witrynach nowi użytkownicy otrzymują hasła, które są przypisywane i zapisywane przez administratorów systemu. Jeśli te hasła zostaną użyte tylko raz, podczas pierwszego logowania, użytkownik może zostać zmuszony do wybrania lub utworzenia prawdziwie tajnego hasła, którego nikt inny nie zna. Jednak w wielu takich witrynach administratorzy zachowują kontrolę nad dokumentami papierowymi lub elektronicznymi, zwykle w celu szybkiego dostępu, gdy użytkownicy zapomną własnych haseł. Taki dostęp całkowicie niszczy ważny element I&A: niezaprzeczalność. Jeśli ktoś inny ma dostęp do hasła, upoważnieni użytkownicy mogą rozsądnie odrzucić transakcje, twierdząc, że ich tożsamość została sfałszowana. Takiemu zaprzeczeniu trudno przeciwdziałać, zwłaszcza w sądzie rozpatrującym zarzut nadużycia ze strony uprawnionego użytkownika tego hasła. Zasadniczo haseł, które będą używane wielokrotnie, nie powinny być zapisywane i nie powinny być dostępne dla administratorów systemu. Krytyczne hasła można zapisać, przechowywać w pojemnikach

zabezpieczonych przed manipulacją i zamknąć, gdzie co najmniej dwa podpisy będą wymagane do odzyskania w nagłych wypadkach.

Ryzyko niewykrytej kradzieży.

Być może największym nieodłącznym ryzykiem związanym z hasłami jest to, że można je ukraść bez wiedzy użytkownika. Do wycieku wystarczy obserwacja, jak ktoś wpisuje hasło. Może się to zdarzyć potajemnie bez wyraźnej wiedzy ofiary. Powiązanym ryzykiem jest ujawnienie hasła atakującemu, który przekonuje uprawnionego użytkownika do jego ujawnienia, udając administratora systemu, który potrzebuje hasła, aby zrobić coś korzystnego dla użytkownika. W końcu można odkryć utratę fizycznego tokena, ponieważ go brakuje, chociaż nadal istnieje możliwość sklonowania tych urządzeń. Utratę hasła można jednak wykryć jedynie poprzez wykrycie jego niewłaściwego użycia lub znalezienie go w posiadaniu nieautoryzowanego użytkownika (np. Na liście haseł złamanych przy użyciu programu do łamania haseł opartego na słownikach, jak opisano w sekcji 28.3.6). Istnieje kilka sposobów ograniczania tego ryzyka. Po pierwsze, edukacja i świadomość użytkowników są niezwykle ważne. Ludzie powinni traktować ważne sekrety z troską, na jaką zasługują. W niebezpiecznym środowisku hasło powinno zostać wpisane dyskretnie. Należy zdecydowanie wzmocnić starania o dyskrecję, a zaniedbanie w ujawnianiu haseł podczas wchodzenia należy traktować jako przejaw złego zachowania społecznego. Edukacja i świadomość użytkowników, choć niezwykle ważne, nigdy nie mogą stanowić całościowego rozwiązania. Ludzie nieuchronnie wpadną w błąd i popełnią błędy. Niektórzy z nas są bardziej niedbali niż inni. Inni będą ukradkiem obserwowani. W niektórych przypadkach hasła zostaną ujawnione komputerom, na których znajdują się konie trojańskie, które je przechwytują. Technolodzy muszą poszukiwać rozwiązań technicznych i ludzkich, aby ograniczyć to ryzyko. Ponieważ utrata kontroli nad hasłami jest nieunikniona, logicznie wynika z tego, że uwierzytelnianie oparte na haśle powinno być stosowane tylko w sytuacjach, w których wykrywanie nadużyć jest nie tylko wykonalne, ale wręcz wygodne do wykonania w czasie rzeczywistym. Aby było to możliwe, architektura systemu powinna scentralizować informacje potrzebne do wykrywania nadużyć w jednym miejscu. Jeśli wymagane informacje są rozproszone na wielu serwerach, trudno będzie koordynować różne ścieżki audytu. Tradycyjnie użytkownicy systemów haseł nie brali pod uwagę potrzeby wykrywania nadużyć. Jednak współczesne zabezpieczenia są mocno oparte na połączeniu technik zapobiegania i wykrywania. Specjaliści ds. Bezpieczeństwa powinni podobnie myśleć w przypadku systemów uwierzytelniania. Łatwość wykrywania nadużyć powinna być ważnym kryterium przy projektowaniu każdego systemu uwierzytelniania. W przypadku systemów opartych na hasłach za zasadniczy wymóg należy uznać funkcję wykrywania nadużyć. Co jeszcze mogą zrobić projektanci systemów, aby zmniejszyć to ryzyko? Należy ułatwić użytkownikom samodzielną zmianę haseł. Zmiana hasła przez administratora systemu, które będzie używane więcej niż raz, jest nielogiczne. Jeśli użytkownik uważa, że mogło dojść do złamania hasła, jego zmiana powinna być prostą sprawą. W szczególności system nigdy nie powinien uniemożliwiać użytkownikowi zmiany hasła. Niektóre wdrożone systemy odmówią zmiany hasła, jeśli hasło zostało zmienione niedawno, powiedzmy w ciągu ostatnich 24 godzin. Chociaż istnieją powody tego rodzaju ograniczeń, może to stwarzać większe ryzyko niż to, którym rzekomo ma zapobiegać. Należy zachęcać użytkowników do dość częstej zmiany haseł; typowy dopuszczalny okres ważności hasła wynosi od 30 do 90 dni. Bez sporadycznych zmian złamane hasło może zostać zatrzymane do momentu, gdy złośliwy napastnik znajdzie okazję do jego użycia. Częste zmiany haseł zmniejszają możliwości dla takich napastników.

Ryzyko niewykrytego udostępniania.

Innym poważnym ryzykiem związanym z hasłami jest łatwość, z jaką można je udostępniać. Jest wiele przykładów dzielenia się między dyrektorami i ich sekretarkami, między lekarzami i personelem biurowym lub pielęgniarkami, między profesorami i ich sekretarkami lub studentami, a także między

współpracownikami w dowolnej działalności. Edukacja użytkowników i surowe zasady dotyczące udostępniania haseł i kont to oczywiste pierwsze kroki, aby powstrzymać tę możliwość. Rygorystyczne zasady mogą być skuteczne w organizacji, ale ich efekt odstraszający może nie przenosić się na duże populacje konsumentów. Wykrywanie nadużyć można również zastosować do egzekwowania ścisłej polityki. Podstawową przyczyną udostępniania haseł w organizacji jest brak skutecznych mechanizmów delegowania, dzięki którym wybrane uprawnienia jednego użytkownika mogą być delegowane na innego. Lepsze mechanizmy autoryzacji mogłyby wyeliminować większość postrzeganej potrzeby udostępniania haseł. Sekretarze powinni mieć możliwość odczytywania e-maili swoich szefów przy użyciu własnych tożsamości i haseł. W rzeczywistości szefowie powinni mieć możliwość oddzielenia wiadomości e-mail, które mogą przeczytać sekretarze, jednocześnie odmawiając dostępu do bardziej poufnych wiadomości e-mail. Co więcej, czytanie e-maili szefa powinno być możliwe bez zezwalania sekretarzowi na wysyłanie e-maili pod tożsamością szefa; uprawnienia pełnomocnika mogą pozwolić sekretarzom odpowiadać na e-maile szefa, podpisując odpowiedzi własnymi nazwiskami. W świecie nieelektronicznym sekretarki rutynowo odbierają pocztę w imieniu innych osób, nie podszywając się pod nich, i tak powinno być również w przypadku komputerów. Udostępnianie haseł konsumentom jest prawdopodobne, gdy koszt dla konsumentów jest minimalny. Chociaż konsumenci raczej nie będą udostępniać innym haseł do banku internetowego lub konta maklerskiego, mogą być skłonni udostępniać hasła do internetowego usługa subskrypcji, prawdopodobnie z wieloma znajomymi. Nieuczciwy konsument może nawet odsprzedać usługę. Jednym ze sposobów powstrzymania takiego piractwa byłoby powiązanie ujawnienia hasła z ujawnieniem wrażliwego sekretu konsumenta, takiego jak numer karty kredytowej. Niewiele osób, przestępców lub nie, przekazałoby hasło zawierające numer ich własnej karty kredytowej. Innym podejściem, które ogranicza współdzielenie kont, są jednorazowe hasła generowane przez niedrogie tokeny, które niedawno zostały rozesłane konsumentom przez sprzedawców internetowych i banki (np. Citibank od maja 2006 r.) Jako metoda uwierzytelniania tożsamości.1 Te tokeny generują losowe hasła, które zmieniają się mniej więcej co minutę i które można przypisać konkretnej jednostce, która je utworzyła - i tę jednostkę można dokładnie powiązać z pierwotnym odbiorcą. Taki system nie tylko sprawia, że udostępnianie hasła jest praktycznie niemożliwe, ale wspólne hasło można prześledzić bezpośrednio do osoby, która narusza warunki użytkowania, i skutkować postępowaniem prawnym i grzywną.

Ryzyko najsłabszego łącza.

Jedną z frustracji haseł jest to, że użytkownicy muszą pamiętać zbyt wiele. Dlatego użytkownicy mają tendencję do powtarzania wyboru tego samego hasła w wielu witrynach. To poważne zagrożenie. Ujawnienie hasła użytkownika w źle utrzymanej witrynie może prowadzić do penetracji konta użytkownika w wielu innych witrynach. Nie jest łatwo wdrożyć środki techniczne w celu bezpośredniej ochrony przed tym ryzykiem. Określona witryna może zmusić użytkownika do wybrania złożonego hasła lub nawet wybrać hasło dla użytkownika. Nie może jednak uniemożliwić użycia tego samego hasła w innym miejscu. Jest to obszar, w którym edukacja użytkowników, świadomość i własny interes są najważniejsze. Złośliwi atakujący mogą łatwo tworzyć fałszywe witryny internetowe, aby zachęcić użytkowników do zarejestrowania się w atrakcyjnych usługach, po czym może zostać ujawnione hasło użytkownika do innych witryn. Dostępne są sejfy na hasła, w których trudne do odgadnięcia hasła można przechowywać i uzyskiwać do nich dostęp po podaniu hasła głównego. Narzędzia te mogą być pomocne, ale zwiększają wagę tworzenia odpowiedniego hasła głównego i zabezpieczenia go przed wykryciem. Rozwiązaniem technicznym mającym na celu złagodzenie tego problemu jest uniknięcie wymogu rejestracji użytkownika w wielu witrynach przy użyciu identyfikatorów użytkowników i haseł. Zamiast tego użytkownik powinien zarejestrować się w kilku zaufanych witrynach, ale identyfikator użytkownika powinien być użyteczny w wielu witrynach dzięki bezpiecznemu udostępnianiu

zapewnień, że użytkownik został faktycznie zidentyfikowany i uwierzytelniony w stopniu wystarczającym do kontynuowania działalności. Zasadniczo do tego dąży infrastruktura klucza publicznego (PKI). Gdy użytkownik zidentyfikuje się u dostawcy takich elektronicznych danych uwierzytelniających (certyfikatów klienta), certyfikat staje się metodą uwierzytelniania, na przykład niektóre banki świadczą usługę, która umożliwia użytkownikowi utworzenie unikalnego numeru, który może zastąpić numer karty kredytowej w danej transakcji. Użytkownik uwierzytelnia się w witrynie banku, uzyskuje unikalny certyfikat zastępujący numer karty kredytowej i przekazuje go sprzedawcy. Sprzedawca może sprawdzić, czy generuje prawidłową autoryzację transakcji, ale nigdy nie zna oryginalnego numeru karty kredytowej. W przypadku uwierzytelniania opartego na certyfikatach klienta nie jest konieczne ujawnianie hasła użytkownika w wielu witrynach. Skuteczne połączenie haseł i PKI zmniejszyłoby narażenie na najsłabsze ogniwo. Podobne podejście przechowuje poufne informacje w jednym miejscu, a następnie kieruje do tego miejsca firmy w celu uzyskania informacji o płatnościach. Na przykład obecnie wiele systemów (np. PayPal) umożliwia użytkownikowi jednorazową rejestrację danych karty kredytowej w zaufanej usłudze, a następnie płacenie sprzedawcom internetowym (sprzedawcom internetowym) za pośrednictwem tej usługi.

Ryzyko zgadywania online.

Systemy uwierzytelniania są podatne na zgadywanie. Podczas zgadywania online osoba atakująca próbuje uwierzytelnić się przy użyciu prawidłowego identyfikatora użytkownika i odgadniętego hasła. Jeśli hasło zostało źle wybrane, napastnik może mieć szczęście. Atakujący może również być w stanie wykorzystać osobistą wiedzę ofiary, aby wybrać prawdopodobne hasła. Podejście to wykorzystuje udokumentowaną tendencję naiwnych użytkowników do wybierania haseł z list oczywistych słów, rodziny, przyjaciół, zwierząt domowych, sportu, marek handlowych i innych łatwo dostępnych informacji. Na przykład badania plików haseł konsekwentnie pokazują, że najczęściej wybieranym hasłem na świecie jest „hasło”; drugim najczęściej występującym jest sam identyfikator użytkownika lub identyfikator użytkownika wstecz. Konto z tym samym hasłem co identyfikator użytkownika jest często nazywane kontem Joe, na przykład w User ID: joe; Hasło: joe. Innym rodzajem hasła podatnego na odgadnięcie jest hasło przypisane domyślnie; na przykład wiele instalacji oprogramowania tworzy konta z tym samym hasłem we wszystkich systemach. Dokumentacja zwykle ostrzega użytkowników przed zmianą tych kanonicznych haseł, ale wiele osób ignoruje ostrzeżenie. Hasła kanoniczne są szczególnie niebezpieczne, gdy zapewniają dostęp do potężnych kont, takich jak konta root lub do obsługi funkcji. Pierwszą linią obrony przed atakami online jest egzekwowanie zasad złożoności haseł, a także edukacja i świadomość użytkowników. Wiele współczesnych systemów wymaga haseł składających się z co najmniej ośmiu znaków, składających się z dużych i małych liter, cyfr i ewentualnie znaków specjalnych. Niemniej jednak ataki polegające na zgadywaniu online są nadal możliwe, a rejestrowanie systemu lub rejestrowanie aplikacji może być pomocne w identyfikowaniu udanej personifikacji. Na przykład pliki dziennika mogą wskazywać, że określony użytkownik nigdy nie logował się na określone konto poza godzinami pracy, a mimo to ktoś zalogował się jako ten użytkownik w środku nocy. Niektóre systemy reagują na ataki online prostą regułą, która blokuje konto po określonej liczbie nieudanych prób. Ta zasada mogła być zapożyczona z podobnej zasady z kartami bankomatowymi. Zasada ma sens w kontekście bankomatów, gdzie uwierzytelnianie dwuskładnikowe polega na posiadaniu karty i znajomości kodu PIN. Jednak w przypadku schematu polegającego tylko na haśle reguła „trzech ostrzeżeń i wylogowania” może prowadzić do odmowy usługi uprawnionym użytkownikom. Atakujący może łatwo zablokować wiele kont, wprowadzając wielokrotnie trzy błędne hasła, co omówiono w rozdziale 18 dotyczącym odmowy usługi w niniejszym podręczniku. Bardziej wdzięczna reguła spowalnia tempo, z jakim można próbować odgadnąć hasło, tak że uprawniony użytkownik może odczuwalnie spowolnić uwierzytelnianie, ale nie może odmówić. Na przykład zablokowanie konta na kilka minut po trzech błędnych hasłach wystarczy, aby zgadywanie metodą

brutalnej siły stało się niepraktyczne. Ponadto systemy wykrywania włamań można skonfigurować tak, aby ostrzegały administratorów systemu natychmiast po ponownym wprowadzeniu złych haseł. Wtedy ludzie mogą interweniować, aby określić przyczynę błędnych haseł - błąd użytkownika lub nadużycie.

Ryzyko ataków słownikowych off-line.

Najważniejszym atakiem technicznym na systemy uwierzytelniania opartego na hasłach jest atak słownikowy. Takie ataki rozpoczynają się od skopiowania pliku haseł do systemu docelowego i umieszczenia go na komputerze znajdującym się pod kontrolą atakującego. Plik haseł zwykle wykorzystuje szyfrowanie jednokierunkowe, które pozwala systemowi zaszyfrować wprowadzone hasło i porównać je z zaszyfrowaną formą prawidłowego hasła. Jeśli dwa zaszyfrowane ciągi pasują do siebie, wprowadzone hasło jest prawdopodobnie poprawne, a więc system uwierzytelnia identyfikator użytkownika. Atak słownikowy jest opisywany jako off-line, ponieważ osoba atakująca uzyskuje informacje niezbędne do przeprowadzenia ataku, a następnie wykonuje obliczenia w trybie offline, aby odkryć hasło na podstawie tych informacji. Jest to atak polegający na odgadywaniu, ponieważ osoba atakująca próbuje różnych prawdopodobnych haseł z obszernej listy możliwych haseł (ze słownika). Lista prawdopodobnych haseł jest nazywana słownikiem, ponieważ zawiera słowa z co najmniej jednego języka naturalnego, takiego jak angielski i hiszpański; wyspecjalizowane wersje używane w programach do łamania haseł mogą sortować słowa według częstotliwości użycia, a nie alfabetycznie, aby przyspieszyć udane odgadnięcie. Początkową odpowiedzią na ataki słownikowe było powstrzymanie użytkowników przed wybieraniem haseł, które można złamać za pomocą ataku słownikowego. W istocie system próbowałby ataku słownikowego; jeśli się powiedzie, uniemożliwi użytkownikowi wybranie tego hasła. Nie jest to produktywne podejście, ponieważ słowniki atakujących często wyprzedzają słowniki systemu. Produktywne podejście polega na zapobieganiu gromadzeniu przez napastnika informacji niezbędnych do przeprowadzenia ataku słownikowego. Projektanci systemów uwierzytelniania opartych na hasłach wolno rozpoznawali ryzyko ataków słownikowych. Od dawna wiadomo, że hasła nie powinny być przechowywane na serwerze w postaci zwykłego tekstu, ponieważ staje się to pojedynczym punktem katastrofalnej awarii. Systemy z podziałem czasu z początku lat 70. przechowywały hasła w postaci „zaszyfrowanej". Znajomość zakodowanej formy hasła nie ujawniła rzeczywistego hasła. Uwierzytelnienie haseł zostało osiągnięte poprzez obliczenie skrótu z przedstawionego hasła i porównanie z przechowywanym hashem. W rzeczywistości system UNIX sprawił, że zaszyfrowana forma haseł użytkowników była łatwa do odczytania, ponieważ odwrócenie skrótu zostało poprawnie uznane za niewykonalne obliczeniowo. Jednak znajomość zakodowanej formy hasła jest wystarczająca do ataków słownikowych. Atakujący odgaduje hasło z listy lub słownika prawdopodobnych haseł, oblicza jego skrót i porównuje go z przechowywanym hashem. Jeśli są zgodne, domysł atakującego jest weryfikowany; w przeciwnym razie napastnik próbuje innego przypuszczenia. Od późnych lat 80-tych systemy UNIX przestały czynić plik zaszyfrowanych haseł łatwym do odczytania, więc ta luka została zmniejszona. UNIX wprowadził również koncepcję soli, aby utrudnić ataki słownikowe. Hasło użytkownika i losowa liczba zwana solą są mieszane i przechowywane na serwerze. Sama sól jest również przechowywana na serwerze. Aby uwierzytelnić użytkownika, przedstawione hasło i przechowywana sól są mieszane i porównywane z przechowywaną wartością skrótu. Użycie soli oznacza, że dla każdego użytkownika wymagany jest oddzielny atak słownikowy, ponieważ każde odgadnięte hasło musi być zaszyfrowane razem z solą. W przeciwnym razie sam atak może być przeprowadzony jednocześnie na wielu przedstawionych hasłach.

Ryzyko powtórzenia hasła.

Jeśli hasło jest przesyłane w postaci zwykłego tekstu z klienta na serwer, jest narażone na przechwycenie w sieci przez intruza. Nazywa się to wykrywaniem hasła. Wiele systemów wymaga

przesłania hasła do serwera w postaci zwykłego tekstu. Inne wymagają przesłania skrótu hasła (zwykle bez soli). Przesyłanie skrótu hasła jest ryzykowne z dwóch powodów:

1. Hasz jest wystarczający do ataku słownikowego, chyba że używa się soli i jest trzymana w tajemnicy.

2. Atakujący nie musi nawet odzyskiwać hasła. Zamiast tego atakujący może w razie potrzeby odtworzyć skrót hasła.

Wiele istniejących systemów jest podatnych na podsłuchiwanie haseł w sieci w postaci zwykłego tekstu lub zaszyfrowanej. Na szczęście istnieją techniczne rozwiązania tego problemu. Jednym z podejść do zagrożenia powtórką jest użycie klucza publicznego serwera do zaszyfrowania dowolnej transmisji informacji związanych z hasłem do serwera: w ten sposób tylko serwer może odszyfrować informacje przy użyciu klucza prywatnego. Zasadniczo to właśnie robią Secure Shell (SSH) i Secure Sockets Layer (SSL) po stronie serwera. Tryb SSL i SSH po stronie serwera wymaga, aby serwer miał certyfikat klucza publicznego. Tryb tych protokołów po stronie klienta wymaga, aby klient miał również certyfikat klucza publicznego. Takie podejście może być skuteczne, ale wiąże się z własnym ryzykiem. Alternatywnym podejściem jest uniknięcie przesyłania hasła, ale zamiast tego zastosowanie protokołu wymagającego znajomości hasła do pomyślnego działania. Jednym z najwcześniejszych i najbardziej znanych systemów stosujących to podejście jest Kerberos. W tym systemie hasło użytkownika jest konwertowane na tajny klucz na komputerze klienckim, a także przechowywane na serwerze Kerberos. Gdy użytkownik żąda uwierzytelnienia, serwer Kerberos wysyła do komputera użytkownika tajny klucz sesji zaszyfrowany za pomocą wspólnego tajnego klucza uzyskanego z hasła użytkownika. Możliwość prawidłowego odszyfrowania tej wiadomości świadczy o znajomości hasła bez faktycznego przesyłania go, w postaci zwykłego tekstu, zaszyfrowanej lub zaszyfrowanej. Niestety protokół Kerberos jest podatny na ataki słownikowe; każdy komputer kliencki może udawać dowolnego użytkownika i może uzyskać niezbędne informacje wymagane do ataku słownikowego. Kerberos również nie używa soli, więc ten sam atak słownikowy można zastosować do wielu użytkowników jednocześnie. Protokół Kerberos w wersji 5 zapewnia opcję wstępnego uwierzytelniania, co utrudnia nieco zebranie informacji potrzebnych do ataku słownikowego. Dane nie są już dostępne, po prostu prosząc o nie serwer Kerberos; zamiast tego muszą być podsłuchiwane w sieci. Niedawne eksperymenty pokazały, że ataki słownikowe na Kerberos są bardzo praktyczne, więc jest to poważna luka w szeroko rozpowszechnionym systemie uwierzytelniania opartym na hasłach. Od wczesnych lat 90. opublikowano wiele protokołów uwierzytelniania opartych na hasłach, które nie są narażone na ataki słownikowe, na które Kerberos jest tak podatny. W szczególności weryfikacja haseł o zerowej wiedzy opiera się na założeniu, że dwie strony (komputery i ludzie) mogą wykazać, że znają tajne hasło bez jego ujawniania. Metody te zależą od zdolności do ustalenia, że obie strony niezależnie wybrały tę samą liczbę - ale nie wiedząc, jaka jest konkretna liczba2. Jednym z popularnych modeli koncepcyjnych tego procesu jest weryfikacja hasła o zerowej wiedzy, która przebiega w następujący sposób:

1. Dwie osoby chcą sprawdzić, czy mają wspólną sekretną liczbę (w tym eksperymencie myślowym jedna cyfra od 1 do 10). W tym przykładzie udostępnionym numerem jest 3.

2. Dwie osoby mają talię 10 pustych kart.

3. Pierwsza osoba odlicza do trzeciej karty i robi znak na prawej krawędzi tej karty.

4. Talia kart jest ułożona w taki sposób, że druga osoba może zaznaczyć lewą krawędź kart, ale nie widzi prawej krawędzi.

5. Druga osoba również odlicza do trzeciej karty (w tym przykładzie) i zaznacza lewą krawędź.

6. Talia kart jest tasowana, aby kolejność sekwencji została utracona, a następnie wyświetlona obu stronom.

7. Jeśli pojedyncza karta ma znak zarówno na prawej, jak i lewej krawędzi, obie strony mają wspólny numer, ale żadna z nich nie musiała dokładnie ujawnić, która to była.

Ciekawie będzie sprawdzić, czy takie podejście do uwierzytelniania można wdrożyć na rzeczywistych komputerach i czy będzie wykorzystywane komercyjnie na znaczną skalę w nadchodzących latach.

Ryzyko fałszowania serwera.

Jak wspomniano wcześniej, jednym z powszechnie stosowanych sposobów zapobiegania ujawnianiu haseł podczas przesyłania w sieci jest wysyłanie haseł z klienta do serwera zaszyfrowanych przy użyciu klucza publicznego serwera. Serwer, który ma odpowiedni klucz prywatny, może odszyfrować hasło, aby je odzyskać. Znajomość klucza publicznego nie jest wystarczająca, aby spoofer mógł określić klucz prywatny. Naiwne protokoły ochrony klucza prywatnego mogą być podatne na ataki typu „replay". Jednak obecnie w powszechnym użyciu są dwa dobrze zaprojektowane protokoły. SSL po stronie serwera to protokół używany przez większość internautów. W tym protokole klucz publiczny serwera służy do zabezpieczenia transmisji hasła użytkownika z klienta na serwer. Podobnie jak w przypadku wszystkich schematów opartych na kluczu publicznym, pięta achillesowa tego protokołu leży w autentycznej znajomości klucza publicznego serwera. Technologia certyfikatów klucza publicznego ma na celu zapewnienie kluczy publicznych z dobrą gwarancją tożsamości serwera, do którego należą. Pełne omówienie zagadnień związanych z technologią infrastruktury klucza publicznego znajduje się w rozdziale 37, ale wystarczy zauważyć, że istnieją pułapki związane z wykorzystaniem certyfikatów do uwierzytelniania serwerów. Nieuczciwy serwer może zebrać hasło użytkownika, udając coś innego niż to, czym jest. Poleganie na wyglądzie i działaniu strony internetowej w celu uwierzytelnienia serwera jest niewystarczające, ponieważ łatwo jest skopiować całą stronę internetową do wykorzystania jako wabik i uzyskać zaufanie przed przechwyceniem poufnych informacji. Udoskonaleniem uwierzytelniania Witryny jest powiązanie określonego obrazu i identyfikujących ciągów znaków (np. Zdjęcie hipopotama z etykietą „Ulubione zwierzątko Archiego") z identyfikatorem użytkownika; witryna uwierzytelnia się dla określonego użytkownika (np. Archie), wyświetlając wybrany przez niego obraz.4 Autentyczność certyfikatu serwera może zostać sfałszowana na wiele sposobów, które są trudne do wykrycia przez użytkownika, oraz manipulowanie zaufanymi certyfikatami głównymi, które są konfigurowane w przeglądarce internetowej użytkownika. Co więcej, podczas gdy zaufanie ostatecznie łączy się z certyfikatem głównym, właściciel pojedynczego certyfikatu znajdującego się poniżej zaufanego katalogu głównego może dokonać znacznych szkód. SSH po stronie serwera to podobny protokół, zwykle używany do zapewniania bezpiecznego zdalnego dostępu do serwerów UNIX. SSL po stronie serwera i SSH po stronie serwera mają te same podstawowe luki w zabezpieczeniach: obie mogą zostać sfałszowane przez manipulację certyfikatem. Użycie SSL po stronie serwera do ochrony transmisji haseł z klienta do serwera jest powszechne obecnie w Internecie, ale klienci korzystający z produktów do uwierzytelniania powinni rozumieć ryzyko związane z tym podejściem. W trybie tych protokołów po stronie klienta nie ma potrzeby przesyłania hasła z klienta do serwera, ponieważ uwierzytelnianie klient-serwer opiera się na wykorzystaniu przez klienta własnego klucza prywatnego do generowania podpisu cyfrowego. Dlatego protokoły po stronie klienta nie są podatne na przechwytywanie haseł przez fałszowanie serwera.

Ryzyko ponownego użycia hasła.

Potrzeba zmiany haseł z rozsądną częstotliwością jest dobrze znana, ale jaka jest rozsądna częstotliwość? A jak drakońskie powinno być egzekwowanie? Wygląda na to, że administratorzy bezpieczeństwa posunęli się za daleko w tych kwestiach. Zmuszanie użytkowników do zmiany haseł co

miesiąc i bezwzględne egzekwowanie takich reguł może w rzeczywistości prowadzić do mniejszego niż większego bezpieczeństwa, ponieważ tak wielu sfrustrowanych użytkowników zapisuje i przechowuje swoje ciągle zmieniające się hasła w niezabezpieczonych miejscach. Istnieje tutaj realne ryzyko, stworzone przez administratorów bezpieczeństwa o dobrych intencjach, którzy pogorszyli problem, niż jest on z natury rzeczy. Systemy, które wybierają hasło dla użytkownika, mają swój własny zestaw problemów i są generalnie zbyt nieprzyjazne dla użytkownika, aby były opłacalne w dobie Internetu. Ta dyskusja koncentruje się na systemach, które umożliwiają użytkownikom wybieranie własnych haseł. W jaki sposób ujawnienie hasła wzrasta z czasem? Nawet najsilniejszy system oparty na hasłach, odporny na ataki słownikowe off-line i przechwytywanie haseł przez spoofing serwera, staje w obliczu zwiększonej ekspozycji w miarę upływu czasu. Przez długi czas powolny, ciągły atak polegający na zgadywaniu online może zakończyć się sukcesem. Z czasem wzrasta również prawdopodobieństwo nieumyślnego ujawnienia informacji poprzez potajemną obserwację lub narażenie na komputer zainfekowany koniem trojańskim. Niemniej jednak dobre hasło, starannie wybrane przez użytkownika, aby było bezpieczne przed atakami słownikowymi i dobrze zapamiętane przez użytkownika, nie powinno być zmieniane od niechcenia. Zmiana co sześć miesięcy może być odpowiednia w przypadku dobrze dobranych haseł odpornych na brutalną siłę. Wymuszanie zmian haseł to skomplikowana sprawa, w której społeczność zajmująca się bezpieczeństwem nie wykonała dobrej pracy. Nie jest trudno śledzić wiek hasła i wymusić jego zmianę po upływie odpowiedniego czasu. Trudność polega na wymuszeniu niezależności nowego hasła od starego. W rzeczywistości istnieje prawdopodobieństwo, że nowe hasło będzie nieznaczną odmianą starego. Na przykład dołączenie cyfry oznaczającej miesiąc do stałego ciągu umożliwia użytkownikom posiadanie prawie tego samego hasła, nawet jeśli są zmuszeni zmieniać je co miesiąc. Niektóre systemy przechowują historię ostatnio używanych haseł, aby zapobiec ich ponownemu wykorzystaniu. System, który przechowuje historię, powiedzmy, pięciu haseł, można oszukać, szybko zmieniając hasło sześć razy. Aby temu zapobiec, istnieją systemy, które nie pozwalają użytkownikowi zmieniać hasła częściej niż raz dziennie. Ma to niefortunny skutek w postaci faktycznego zwiększenia ryzyka ujawnienia hasła, ponieważ użytkownik, który zdaje sobie sprawę, że bieżące hasło mogło zostać nieumyślnie ujawnione, nie może go zmienić, dokładnie wtedy, gdy jest to największe.

Uwierzytelnianie z wykorzystaniem rozpoznawania symboli.

Ciekawym nowym podejściem do uwierzytelniania użytkowników jest rozpoznawanie konkretnych twarzy spośród dużego wyboru losowych zdjęć. Oprogramowanie Passfaces działa w ten sposób:

[A] użytkownik ustawia tablicę zdjęć i umieszcza kilka znajomych w puli, aby używać ich jako kluczy - twarzy osób, które rozpoznaje użytkownik; następnie oprogramowanie może utworzyć siatkę 3 × 3 losowych wyborów, w tym jeden z kluczowych obrazów. Użytkownik wybiera znajomy obraz, a następnie dwukrotnie powtarza ćwiczenie z nowymi zestawami ośmiu nieznajomych i jednego znajomego, aby uwierzytelnić użytkownika. Biała księga wyjaśnia, w jaki sposób ludzie są szczególnie dobrzy w rozpoznawaniu twarzy; rzeczywiście wydaje się, że mamy specjalne obwody, które ewoluowały w celu szybkiego i dokładnego postrzegania twarzy. Według artykułu, zaletą „korzystania z funkcji Passfaces zamiast haseł" jest to, że Passfaces:

* Nie można zapisać ani skopiować

* Nie można przekazać innej osobie

* Nie można zgadnąć

* Zaangażuj zdolności poznawcze, a nie pamięć

* Może być używany jako pojedyncza forma uwierzytelnienia lub jej część

Siła systemu jest zwiększona poprzez ustawienie parametrów, które uniemożliwiają niewłaściwe użycie twarzy. Na przykład: W niektórych aplikacjach o wysokim poziomie bezpieczeństwa siatki twarzy mogą być wyświetlane tylko przez bardzo krótki czas

czas. Pół sekundy to wystarczająco długo, aby doświadczeni użytkownicy rozpoznali swoje Przepusty. W połączeniu z maskowaniem (twarze w siatce są nadpisywane zwykłą twarzą maski) „surferom na ramieniu" niezwykle trudno jest nauczyć się przejść, gdy użytkownik je kliknie.

UWIERZYTELNIANIE W OPARCIU O TOKEN.

Uwierzytelnianie oparte na tokenach opiera się na czymś, co użytkownik posiada, a żaden inny użytkownik identyfikatora nie powinien posiadać ani nie mieć do niego dostępu. To uwierzytelnienie można osiągnąć na wiele sposobów, w tym:

* Karty dostępu

* Karty zbliżeniowe i dotykowe

* Karty inteligentne i klucze sprzętowe

* Jednorazowe generatory haseł

* Miękkie tokeny

Systemy wprowadzania kart.

Sposoby kodowania danych identyfikacyjnych na kartach obejmują optyczny kod kreskowy, pasek magnetyczny, karty inteligentne z wbudowanymi chipami przechowującymi dane biometryczne oraz karty z osadzonymi kawałkami metalu. Większość kodów kreskowych nie jest bezpieczna; karty można łatwo powielić. Chociaż nowsze, dwuwymiarowe kody kreskowe są prawie odporne na manipulacje, nie mogą przechowywać wielu informacji. Karty z paskiem magnetycznym mają również wiele wad: nie mogą przechowywać wielu danych i można je łatwo zmienić, skopiować lub usunąć (często przez przypadek). Z czasem dane magnetyczne zanikają i należy je przeprogramować. Czytniki kart magnetycznych nie są praktyczne na zewnątrz z powodu pogody i aktów wandalizmu. Intensywnie używane czytniki kart magnetycznych i same karty szybko się zużywają. Karty z osadzonymi metalowymi końcówkami są skuteczne. Kodowania nie można zobaczyć inaczej niż na zdjęciu rentgenowskim i jest trwały i trwały. Karty należy przyłożyć do czytnika lub włożyć do czytnika, który skanuje kartę pod kątem położenia każdego bitu. Przechowują bardzo ograniczone dane, kodowanie jest zainstalowane fabrycznie i nie można go zmienić, a zapasowe karty należy zinwentaryzować. Ponadto przy odpowiednim wyposażeniu karty te można skopiować. Metody korzystania z kart wstępu obejmują zbliżeniowe, dotykowe, wkładanie do gniazda, które zwraca kartę po uwierzytelnieniu, lub przeciąganie karty przez wąski kanał lub do i z gniazda. Przeciąganie jest szybkie, ale kartę należy trzymać w ręku. Włożenie karty ma takie same wady jak przeciągnięcie i jest wolniejsze. Zużycie, pogoda lub akty wandalizmu mogą spowodować uszkodzenie karty i czytnika kart.

Karty zbliżeniowe i dotykowe.

Najlepsze z nowych systemów kontroli dostępu do kart wykorzystują karty zbliżeniowe lub dotykowe. Karty te komunikują się z czytnikami za pomocą transmisji podczerwieni lub mikrofal. Czytnik zasila niektóre typy kart, podczas gdy inne zawierają miniaturowe baterie. Fizycznie karty i czytniki kart są odporne na warunki atmosferyczne, akty wandalizmu i nie zużywają się. Czytniki kart zbliżeniowych mogą być montowane na powierzchni, wpuszczane w ścianę lub całkowicie ukryte w ściance działowej,

aby nie zwracały uwagi na drzwi bezpieczeństwa. Karty dotykowe są funkcjonalnie podobne do kart zbliżeniowych, ale należy je krótko przyłożyć do czytnika, który jest zwykle widoczny. Karty dotykowe kosztują nieco mniej niż karty zbliżeniowe i nadają się tylko do wejść o małym natężeniu ruchu. System kart dotykowych jest wolniejszy, a karty są łatwiejsze do zgubienia, kradzieży lub zabrania siłą. Karty zbliżeniowe (które obejmują również karty RFID) mogą być używane, gdy są schowane w kieszeni, torebce lub portfelu. Niektóre są noszone ukryte lub zawieszone na smyczy na szyję. Karta zbliżeniowa, która jest jednocześnie identyfikatorem, którą wszyscy w miejscu pracy noszą przez cały czas, mogą uzyskać dostęp do drzwi i stacji roboczych bez dotykania. Tymczasowe identyfikatory są zwykle wydawane wszystkim odwiedzającym, nawet gdy są eskortowani i mogą być używane do kontroli dostępu i monitorowania wchodzących obszarów. Tymczasowe odznaki są szybko aktywowane z określonymi uprawnieniami i mogą być automatycznie i natychmiastowo unieważnione w razie potrzeby. Coraz częściej karty gości są tworzone szybko na miejscu ze zdjęciem gościa i być może z danymi biometrycznymi, a także drukowanymi na karcie. Długoterminowe tymczasowe odznaki mogą być wydawane dostawcom, wykonawcom i pracownikom zewnętrznym, chociaż najlepiej jest, aby personel ochrony przechowywał identyfikatory w bezpieczny sposób, gdy dana osoba znajduje się poza obiektem. Nowe systemy zapewniają wiele przydatnych funkcji. Zwykle są laminowane i uszczelniane, aby zapobiec zużyciu, uszkodzeniu lub zmianie. Poszczególne karty są szybko przygotowywane, aktywowane i anulowane - wszystko na miejscu. System może ograniczyć wejście do określonych miejsc, dni i godzin, a także można zaprogramować ograniczenia związane z wakacjami. Każda karta może zostać natychmiast zablokowana, jeśli zostanie zgubiona, skradziona lub gdy właściciel odejdzie. Nowsze karty zbliżeniowe 13,56 MHz działają w odległości do trzech stóp od czytnika kart; starsze karty miały zasięg około czterech cali. Nowsze karty są również szybsze, przechowują więcej danych i oferują większą funkcjonalność. Wiele czytników kart może również zapisywać dane na karcie. Istnieje jednak kompromis między użytecznym zakresem roboczym a ilością przechowywanych danych. Im większy zakres, tym mniej przechowywanych danych. Większość systemów zbliżeniowych można regulować, aby zoptymalizować odległość i prędkość. Na przykład w zewnętrznych drzwiach obwodowych, gdzie szybki i wygodny dostęp jest ważniejszy niż szczelne bezpieczeństwo, systemy są ustawione na maksymalny zasięg. Drzwi wewnętrzne, które wymagają większego bezpieczeństwa, są przystosowane do wykorzystywania większej ilości informacji i działania w mniejszej odległości, która jest nadal znacznie większa niż pozwalały na to starsze systemy. Nie jest to łatwe bez bardzo nowoczesnego sprzętu, ale karty zbliżeniowe i dotykowe mogą być zagrożone. Istnieją również automatycznie wygasające plakietki dla gości, które wyraźnie zmieniają kolor lub wyraźnie pokazują słowo „wygasła" po upływie określonego czasu. Identyfikatory, które tracą ważność, są wielokrotnego użytku i mają ustalony okres ważności, który zwykle wynosi od dwóch do 24 godzin po każdej aktywacji. Tych odznak nie można reaktywować, z wyjątkiem bardzo wyrafinowanego sprzętu. Karty nie są jedynymi urządzeniami zbliżeniowymi czy dotykowymi. Używane są również klucze lub łaty. Klucze mogą być małe, wytrzymałe i łatwe do przymocowania do breloczka lub małej ręcznej różdżki, której mógłby użyć ochroniarz. Poprawki działają zamiast kart dotykowych lub z oddzielnymi systemami kontroli dostępu, aby uaktualnić istniejące starsze systemy. Naszywki mają rozmiar i grubość około jednej czwartej i można je łatwo przymocować do wszystkiego, co normalnie nosi osoba, np. Dowód osobisty lub identyfikator, pager lub telefon komórkowy lub wnętrze portfela. Nowsze urządzenia RFID będą jeszcze mniejsze. Dostęp za pomocą karty jest często używany we wszystkich pomieszczeniach wyposażonych w serwery, komponenty sieciowe lub sprzęt telefoniczny; do dostępu poza godzinami pracy do systemów informatycznych dla użytkowników, techników i administratorów; i dla wszelkich obszarów, w których przechowywane są przedmioty o wysokiej wartości. Systemy kart są zwykle zintegrowane z bezpieczeństwem pomieszczeń w celu kontroli dostępu do budynku i wyjścia z niego, wind, miejsc obsługi, parkingów i toalet oraz innych części infrastruktury informatycznej, które również mogą korzystać z kontroli dostępu. Planuj z wyprzedzeniem i rozważ, gdzie mogą być potrzebne

dodatkowe punkty kontroli dostępu. Dodanie częściowych posiłków w późniejszym terminie może być kosztowne. Każde wejście na teren kontrolowany powinno być rejestrowane w sposób, który nie może zostać naruszony. Dzienniki powinny zapewniać dokładną ścieżkę audytu każdego, kto szukał dostępu, kiedy i czy odmówiono dostępu. Tam, gdzie potrzebne są silniejsze zabezpieczenia, każde wyjście powinno być rejestrowane w ten sam sposób. System rejestrowania najlepiej monitorować za pomocą oprogramowania, które może przeglądać wszystkie dane systemowe w czasie rzeczywistym, szybko sygnalizować problemy, wystawiać okresowe raporty podsumowujące oraz szybko wyszukiwać i podsumowywać nietypowe zdarzenia. Ręczne przeglądanie dzienników jest uciążliwym i czasochłonnym zadaniem. Jeśli możliwy jest tylko ręczny audyt, musi istnieć sztywna polityka przeprowadzania tego co kilka dni. Systemy wejściowe oparte na tokenach same w sobie nie zapewniają silnej ochrony. Dlatego wymagany jest pewien stopień uwierzytelnienia.

Karty inteligentne i klucze sprzętowe.

Inną formą tokena jest karta inteligentna. Karty te można umieścić w czytniku kart PC lub odczytać za pomocą specjalnego czytnika. Klucze sprzętowe to karty inteligentne, które pasują do portów wejścia-wyjścia, takich jak Universal Serial Bus (USB). Karta inteligentna ma własne możliwości przetwarzania i zazwyczaj przechowuje klucz prywatny skojarzony z użytkownikiem. Często do uzyskania dostępu do karty wymagane jest hasło lub kod PIN, co zapewnia możliwość uwierzytelniania dwuskładnikowego. Karta inteligentna umożliwia uwierzytelnianie użytkownika poprzez podpisanie przedstawionego jej wyzwania kluczem prywatnym użytkownika. Podpis jest weryfikowany za pomocą klucza publicznego użytkownika. Pełne omówienie takich kart inteligentnych obejmuje uwzględnienie kryptografii klucza publicznego, certyfikatów klucza publicznego lub tak zwanych certyfikatów cyfrowych oraz infrastruktury pomocniczej lub PKI (patrz Rozdział 37 w niniejszym Podręczniku). Dość powiedzieć, że karty inteligentne od dawna uważane są za niezbędne do powszechnego stosowania technologii klucza publicznego, ale jak dotąd nie zostały one szeroko rozpowszechnione. Tokeny sprzętowe oferują potencjał silniejszego uwierzytelniania niż hasła, ale ich zastosowanie jest ograniczone ze względu na ich postrzegane koszty i wymagania dotyczące infrastruktury. Nie wiadomo, czy uda się je wdrożyć w skali milionów użytkowników. Uwierzytelnianie za pomocą tokenów jest tak naprawdę uwierzytelnianiem za pomocą czegoś, co wie token. Ponieważ tokeny można zaprogramować tak, aby zapamiętywały i wykorzystywały sekrety znacznie skuteczniej niż ludzie, oferują one potencjał silnego uwierzytelniania kryptograficznego, ale tokeny odporne na manipulacje nie są łatwe do wytworzenia. W ostatnich latach ataki oparte na analizie mocy różnicowej okazały się skuteczne w określaniu tajnych kluczy i kodów PIN przechowywanych na kartach inteligentnych. Ataki te wymagają fizycznego dostępu do karty, której utrata prawdopodobnie byłaby znana, więc chociaż nie zawsze są one wykonalne, z pewnością podają w wątpliwość domniemaną odporność kart inteligentnych na manipulacje. Ponieważ karty inteligentne są coraz szerzej stosowane, prawdopodobnie zostaną przeprowadzone inne genialne ataki. Karty inteligentne są bardziej podatne na tajne wydobycie niż tokeny, ponieważ ich obliczenia powodują wyciek takich informacji w postaci promieniowania elektromagnetycznego. Porównując tokeny z hasłami, można argumentować, że niewykryta kradzież jest łatwiejsza dzięki hasłom. Token jest fizycznym przedmiotem, którego brak jest zauważalny. Jednak tokeny stwarzają własne problemy. Podobnie jak generatory haseł, są one podatne na uszkodzenia fizyczne i złamanie zabezpieczeń. Karty inteligentne są zwykle zbudowane z cienkiego plastiku z wbudowanym chipem, co sprawia, że całe urządzenie jest podatne na uszkodzenie w wyniku uszkodzenia. Ponadto użytkownicy zazwyczaj mogą przechowywać karty wraz z innymi kartami kredytowymi w portfelu lub kieszeni, z których każda stanowi dodatkowe zagrożenie dla środowiska. Jednak w niektórych branżach koszt zastąpienia utraconych lub uszkodzonych tokenów może być wart zmniejszenia niewykrytego udostępniania, ponieważ token może być używany tylko przez jedną osobę naraz.

Tokeny miękkie.

Idea miękkich tokenów lub tokenów programowych została zaproponowana jako tania alternatywa dla tokenów sprzętowych. Wczesne miękkie tokeny składały się z klucza prywatnego użytkownika zaszyfrowanego hasłem i przechowywanego na jakimś przenośnym nośniku, takim jak dyskietka. Taki schemat jest niezwykle podatny na ataki słownikowe, ponieważ odgadnięte hasło można łatwo zweryfikować (testując domniemany klucz prywatny, aby sprawdzić, czy odszyfrowuje on wiadomość zaszyfrowaną przy użyciu znanego klucza publicznego użytkownika). Co więcej, fizyczny transport dyskietek i możliwy brak stacji dyskietek skłoniły ludzi do przechowywania tych miękkich tokenów na serwerach sieciowych, aby były dostępne w razie potrzeby. Niestety ta lokalizacja sprawia, że są one również łatwo dostępne dla atakujących. Ochrona przez dostęp do tokenów programowych na serwerze sieciowym za pomocą hasła po prostu powraca do problemów związanych z uwierzytelnianiem za pomocą hasła. Sugerowano, że klucz publiczny użytkownika może być utrzymywany w tajemnicy i znany tylko zaufanym serwerom, aby uniknąć ataków słownikowych na zaszyfrowany klucz prywatny. Takie podejście wiąże się z poważnymi kosztami zamkniętej infrastruktury PKI, a nie otwartej infrastruktury PKI. Schematy odzyskiwania klucza prywatnego za pomocą bezpiecznego protokołu opartego na hasłach zostały opublikowane i są wdrażane przez niektórych dostawców. Te schematy ostatecznie powracają do uwierzytelniania opartego na hasłach jako podstawy. Opracowano schematy polegające na podzieleniu klucza prywatnego na dwie części. Jedna część klucza prywatnego jest obliczana na podstawie hasła; druga część jest przechowywana na serwerze online, który działa jako wirtualna karta inteligentna oparta na sieci. Obie części klucza prywatnego są potrzebne do uwierzytelnienia użytkownika, ale nigdy nie są zebrane w jednym miejscu. Alternatywnym sposobem byłoby przechowywanie całego klucza prywatnego użytkownika na serwerze online i uzależnienie jego używania od bezpiecznego protokołu opartego na hasłach. Takie podejście umożliwia serwerowi podszywanie się pod dowolnego użytkownika i może nie być odpowiednie we wszystkich środowiskach. Jednak we wszystkich przypadkach bezpieczeństwo tokena zależy od integralności używającego go komputera. Nowsze implementacje miękkich tokenów opierają się na kryptografii asymetrycznej, aby wyeliminować obawy dotyczące bezpieczeństwa związane z przechowywaniem kluczy prywatnych w pliku lub innej przenośnej lokalizacji. Token programowy może generować własną parę kluczy i wymieniać klucze publiczne z serwerem uwierzytelniającym. Chociaż zwiększa to bezpieczeństwo miękkich tokenów, koncepcja jest z natury słaba i podatna na ataki. Rząd federalny Stanów Zjednoczonych ustanowił standard dla posiadanych dowodów osobistych, obowiązkowy dla wszystkich pracowników federalnych i wykonawców. Oryginalna Prezydencka Dyrektywa Bezpieczeństwa Wewnętrznego 12 (HSPD 12) z dnia 27 sierpnia 2004 r. Nosiła tytuł „Zasady dotyczące wspólnego standardu identyfikacji pracowników federalnych i wykonawców". Zdefiniował te wymagania dotyczące bezpiecznej i niezawodnej identyfikacji, która - jest wydawana w oparciu o solidne kryteria weryfikacji tożsamości pracownika, jest silnie odporna na fałszowanie, fałszowanie, podrabianie i terrorystów

* Można szybko uwierzytelnić elektronicznie

* Jest wydawany tylko przez dostawców, których wiarygodność została potwierdzona w oficjalnym procesie akredytacji

Generatory haseł jednorazowych.

Popularna forma tokena, od dostawców takich jak RSA Data Security Inc. i CryptoCard, wyświetla jednorazowe hasło, zwykle sześcio- lub ośmiocyfrową cyfrę, która zmienia się za każdym naciśnięciem przycisku dostępu lub po upływie określonego czasu. upłynęło od ostatniego użycia hasła. Użytkownik uwierzytelnia się, wprowadzając identyfikator użytkownika i aktualną wartość wyświetlaną przez

token. Hasło jest nazywane jednorazowym, ponieważ wygasa po upływie dopuszczalnego okresu użytkowania. Token jest zazwyczaj bezdotykowy, ponieważ nie wymaga kontaktu elektrycznego z komputerem, na którym użytkownik przedstawia dane uwierzytelniające. Użytkownik przekazuje niezbędne informacje z tokena za pomocą klawiatury lub innego urządzenia wejściowego. Aby było to uwierzytelnianie dwuskładnikowe, oprócz zmiany hasła jednorazowego wyświetlanego przez token wymagane jest również stałe hasło użytkownika. Te tokeny są oparte na wspólnych tajnych kluczach, więc zarówno token, jak i serwer mają wspólny sekret. Serwer i token muszą zostać zainicjowane, a następnie zsynchronizowane, aby ten schemat działał. W przypadku SecurID firmy RSA, jeśli rozbieżność czasowa między konkretnym tokenem a systemem uwierzytelniającym przekracza określony limit, oprogramowanie uwierzytelniające dostosowuje wartość w wewnętrznej tabeli, aby skompensować poślizg czasu. Dostawcy tacy jak CryptoCard opracowali algorytmy uwierzytelniania oparte na zdarzeniach, aby rozwiązać problem „poślizgu". Te tokeny wykorzystują ziarno z algorytmem do generowania unikalnej wartości dla każdego naciśnięcia przycisku lub innej akcji aktywującej. Po następnym zalogowaniu ta wartość jest teraz „znana" systemowi uwierzytelniającemu i należy podać nową wartość. Wartość tokena wzrasta w oparciu o ziarno, bez konieczności synchronizacji z systemem uwierzytelniania. Generatory haseł muszą być chronione przed fizyczną manipulacją. Urządzenia te zazwyczaj obejmują kilka środków powodujących zniszczenie obwodów elektronicznych w przypadku otwarcia obudowy zewnętrznej; na przykład, oprócz kleju z żywicy epoksydowej, żetony mogą zawierać elementy wrażliwe na światło, które są natychmiast niszczone pod wpływem światła, co czyni urządzenie bezużytecznym. Niektórych generatorów haseł i kart inteligentnych nie można nawet otworzyć w celu wymiany baterii, więc cała karta musi zostać wymieniona zgodnie z przewidywalnym harmonogramem. Dostępne są żetony tego typu, które mają gwarancję trwałości przez rok, dwa lub trzy lata bez zużywania się baterii.

Uwierzytelnianie przy użyciu urządzeń mobilnych.

Inna forma uwierzytelniania opartego na tokenach, która jest coraz częściej dostępna w celu uzyskania dostępu do zastrzeżonych witryn internetowych, takich jak strony kont bankowych, rejestruje urządzenie mobilne, takie jak telefon komórkowy lub tablet, które mogą odbierać wiadomości tekstowe w ramach usługi Short Message Service (SMS). Podczas logowania autoryzowany użytkownik otrzymuje jednorazowy kod do wprowadzenia na stronie WWW. Takie podejście nadaje dodatkową wartość środkom bezpieczeństwa chroniącym urządzenie mobilne; na przykład krótkie limity czasu wymagające wprowadzenia kodu PIN, szyfrowanie danych w pamięci urządzenia oraz metody zdalnej dezaktywacji lub czyszczenia urządzenia w przypadku jego zgubienia lub kradzieży.

AUTORYZACJA BIOMETRYCZNA.

Uwierzytelnianie biometryczne wygląda na doskonałe rozwiązanie problemu uwierzytelniania w cyberprzestrzeni. Istnieje jednak kilka wyzwań związanych z wdrażaniem danych biometrycznych, w tym wady dokładności (wyniki fałszywie dodatnie i fałszywie ujemne), utrata identyfikatorów biometrycznych, bezpieczeństwo szablonów i obawy dotyczące prywatności

AUTORYZACJA MIĘDZYDOMENOWA.

Ponieważ coraz więcej systemów i procesów włącza się do Internetu, ludzie oczekują bezproblemowego połączenia organizacji i aplikacji w Internecie. Ponadto stale rosnące ryzyko kradzieży tożsamości sprawia, że osoby i organizacje są bardziej ostrożne w przesyłaniu zbyt dużej ilości informacji o tożsamości przez niezaufaną sieć. W ciągu ostatnich kilku lat wzmożono wysiłki, aby umożliwić łatwą, ale bezpieczną wymianę informacji dotyczących uwierzytelniania i autoryzacji między organizacjami. Korzystając z języka SAML (Security Assertion Markup Language), badacze opracowują metody umożliwiające jednej organizacji dzielenie się wystarczającą ilością informacji między

systemami, aby umożliwić transakcję bez naruszania prywatności. Shibboleth, projekt rozpoczęty w 2000 roku jako inicjatywa dotycząca oprogramowania pośredniczącego w Internecie, to projekt typu open source wykorzystujący SAML. Organizacje używające Shibboleth jako podstawy do projektowania nowych federacyjnych implementacji uwierzytelniania i autoryzacji obejmują InCommon i brytyjską Federację Zarządzania Dostępem dla Edukacji i Badań. Aby ułatwić tego rodzaju wymianę informacji, organizacje uczestniczące muszą udostępniać szczegółowe informacje na temat swoich zasad i procedur bezpieczeństwa, aby każda z nich mogła z góry zdecydować, czy będzie ufać potwierdzeniom uwierzytelniania drugiej strony. Ten rodzaj wymiany informacji osiąga się najskuteczniej dzięki politykom i praktykom stosowanym w PKI.

WZGLĘDNE KOSZTY TECHNOLOGII UWIERZYTELNIANIA.

Jedną z częstych odpowiedzi specjalistów ds. Bezpieczeństwa w dyskusjach na temat identyfikacji i uwierzytelniania przy użyciu czegokolwiek innego niż hasła jest to, że koszt zakupu nowego sprzętu jest wygórowany. Jednak hasła nie są darmowe. W analizie kosztów zarządzania hasłami, RSA Data Security, twórców tokena SecurID, szacowane koszty wdrożenia (inicjalizacja kont użytkowników) na około 12 USD na użytkownika w ciągu trzech lat oraz koszty zarządzania (zastąpienie zapomnianych haseł i resetowanie zablokowanych kont) około 660 USD na użytkownika w ciągu trzech lat. Co gorsza, utrwalony błąd większości użytkowników w wyborze silnych haseł (tj. Tych odpornych na zgadywanie, ataki słownikowe i ataki siłowe) sprawia, że hasła są w praktyce słabym trybem uwierzytelniania. Dla porównania uwierzytelnianie oparte na tokenach i uwierzytelnianie biometryczne jest tańsze i skuteczniejsze niż hasła.

WNIOSKI.

Identyfikacja i uwierzytelnianie są podstawą dla prawie wszystkich innych celów bezpieczeństwa w cyberprzestrzeni. W przeszłości problemy te często były postrzegane jako proste, których rozwiązanie zakładano, zanim pojawiły się rzeczywiste kwestie bezpieczeństwa. Ważne standardy bezpieczeństwa komputerowego zostały opublikowane i praktykowane bez zwracania większej uwagi na identyfikację i uwierzytelnianie. W cyberprzestrzeni problemy związane z I&A są poważne i ledwie zaczęto je skutecznie rozwiązywać. Solidna, skalowalna infrastruktura identyfikacji i uwierzytelniania jest niezbędna do osiągnięcia bezpieczeństwa. Technologie takie jak tokeny i biometria mają duże znaczenie obiecujące, ale ich wdrożenie wymaga kosztów infrastruktury zdominowanych przez koszt sprzętu dla czytelników i tym podobnych. W międzyczasie hasła są nadal wzmacniane, ponieważ lepiej rozumiemy rzeczywiste ryzyko związane z ich używaniem i opracowujemy środki techniczne mające na celu ograniczenie tego ryzyka. Fakt, że nowoczesne systemy operacyjne nadal zapewniają proste uwierzytelnianie oparte na hasłach, podatne na ataki słownikowe, słabo odzwierciedla tempo, w jakim technologia bezpieczeństwa jest wdrażana na rynku. Patrząc w przyszłość, można przewidzieć, że zobaczymy mieszankę haseł, danych biometrycznych i tokenów w użyciu, być może w konfiguracjach dwu- lub trójczynnikowych. Biometria i tokeny prawdopodobnie zdominują segment z wysokim poziomem pewności, podczas gdy hasła zdominują segment niższy. Jednym z błędnych przekonań, które specjaliści ds. Bezpieczeństwa powinni starać się rozwiać, jest to, że identyfikacja i uwierzytelnianie wystarczą do poprawy bezpieczeństwa publicznego. Jednak przypisanie komuś wiarygodnej i niezaprzeczalnej tożsamości nie jest w żaden sposób równoznaczne z potwierdzeniem wiarygodności tej osoby. W populacjach zamkniętych, takich jak pule pracowników, pracodawcy mogą sprawdzać pochodzenie potencjalnych pracowników i monitorować wydajność obecnych pracowników; w takich okolicznościach znajomość czyjejś tożsamości przy bramie wejściowej może rzeczywiście poprawić bezpieczeństwo. Jednak gdy mamy do czynienia z dużą liczbą osób, które nie zostały poddane kontroli bezpieczeństwa, np. Potencjalnymi pasażerami linii lotniczych, możliwość ich nazwiska nie mówi nam nic o ich wiarygodności. Fakt, że urzędnik w urzędzie rządowym zerka na

faktury za olej opałowy i akt urodzenia przed wydaniem komuś dokumentu tożsamości ze zdjęciem, nie jest podstawą do przypuszczenia, że posiadacz ważnego dokumentu tożsamości jest nieszkodliwym podróżnikiem. Jak zauważyło kilku autorów, jednoznaczna znajomość nazwiska zamachowca-samobójcy siedzącego obok ciebie w samolocie nie jest rozsądną podstawą do samozadowolenia. Timothy McVeigh, bombowiec z Oklahoma City, był doskonale rozpoznawalnym obywatelem Stanów Zjednoczonych, ale mimo to popełnił swoje okrucieństwo. Od 11 września 2001 r. Branża transportu lotniczego jest bardzo publicznym przykładem zarówno trudności związanych z silną identyfikacją i uwierzytelnianiem, jak i wykorzystaniem identyfikacji i uwierzytelniania jako substytutu public relations dla bezpieczeństwa materialnego obejmującego dokładną kontrolę pasażerów. Nieodłączne trudności związane z uwierzytelnianiem stają się oczywiste dla laika oraz dla przywódców politycznych i korporacyjnych. Zapewnienie niezawodnej identyfikacji i uwierzytelnienia w wolnych społeczeństwach jest bardzo trudne, a może nawet niemożliwe. Jako technologowie zdajemy sobie sprawę, że w cyberprzestrzeni nie da się osiągnąć absolutnych gwarancji. Zbyt wielu specjalistów ds. Bezpieczeństwa dąży do osiągnięcia absolutnych celów, a zbyt wiele technologii zabezpieczeń jest sprzedawanych jako silniejsze niż w rzeczywistości. Nasz zawód odniesie ogromne korzyści, jeśli zajmiemy się praktycznymi problemami za pomocą praktycznych, opłacalnych technik i rozwiniemy rozsądną dyscyplinę bezpieczeństwa, która zawiera, ogranicza i łagodzi nieuniknione ryzyko rezydualne, z którym musimy się zmierzyć w każdej sytuacji ludzkiej na dużą skalę.

PODSUMOWANIE

Hasła są szeroko stosowane w praktyce i nadal będą dominującą formą uwierzytelniania użytkowników. Wdrażanie haseł wiąże się z wieloma zagrożeniami, a wiele powszechnie używanych systemów haseł ma poważne luki w zabezpieczeniach. Niemniej jednak środki techniczne mogą złagodzić nieodłączne luki w zabezpieczeniach haseł. Chociaż wymaga to wielkich umiejętności i staranności, przy naszym obecnym zrozumieniu jest technicznie możliwe zbudowanie i wdrożenie silnych systemów uwierzytelniania opartych na hasłach przy użyciu produktów komercyjnych. Prawdziwie nieodłączne ryzyko niewykrytej kradzieży i niewykrytego udostępniania można w znacznym stopniu złagodzić dzięki nowym technologiom, takim jak systemy wykrywania włamań. Niewykryte udostępnianie może być dodatkowo zniechęcane przez system, który łączy tajne dane o wysokiej wartości, takie jak numery kont kart kredytowych, z hasłami. Dostępne są tokeny do generowania haseł jednorazowych lub do bezpośredniej komunikacji z systemami uwierzytelniania. Chociaż koszty spadają, tokeny nadal nie są tak szeroko rozpowszechnione, jak sugerowały wczesne prognozy. Uwierzytelnianie biometryczne jest wdrażane rzadko i na małą skalę, ale oferuje duży potencjał, szczególnie w aplikacjach o wysokim poziomie bezpieczeństwa. Ciekawe nowe badania i aplikacje rozszerzają stosowanie uwierzytelniania (i autoryzacji) na niezaufane sieci między organizacjami federacyjnymi.