KOEN VERVLOESEM

YUBIKEY

Betaalbare sterke authenticatie

Klassieke wachtwoorden zijn eigenlijk helemaal niet zo veilig. Worden ze gestolen of onderschept, dan kan een aanvaller er onmiddellijk misbruik van maken. In dit artikel bespreken we een veiliger alternatief voor dit systeem, namelijk door twee-factorauthenticatie te implementeren met de Yubikey.

De laatste tijd lezen we in de media steeds meer verhalen over gehackte servers en wachtwoordenlijsten die op internet worden gepubliceerd, met de Sony-hack voorop.
We gebruiken steeds meer cloud-diensten, waarbij onze informatie in handen is van een externe partij. En die kan gehackt worden. Maar ook kan een wachtwoord dat je invoert vanaf een onbetrouwbare computer, bijvoorbeeld in een internetcafé, afgeluisterd worden. Misschien is er een keylogger geïnstalleerd die je ssh-wachtwoord onderschept? Met een one-time password maakt het niet uit dat het wachtwoord onderschept wordt, omdat het maar eenmalig geldig is.

YUBIKEY

De Yubikey is sinds 2008 op de markt. Deze usb-sleutel steek je in je computer en is bedoeld om wachtwoorden te genereren. Inmiddels is een tweede versie van de Yubikey verschenen die verschillende modi ondersteunt. De Yubikey wordt als een usb-toetsenbord herkend en werkt dus op alle computers en platformen zonder dat er client-software nodig is. Met een druk op de knop genereert de Yubikey naar keuze een one-time password of statisch wachtwoord en geeft dit als toetsindrukken door aan de computer.
De Yubikey is heel dun (3 mm) en licht (2,5 gram), kan tegen een stootje en is waterdicht. Er zijn geen bewegende delen en er is dus weinig kans op slijtage. Er is zelfs geen batterij nodig, aangezien het apparaatje zich voedt via de usb-poort van de computer. Een standaard Yubikey kost 20 euro. Er is een gratis validatieservice en er bestaan heel wat open source-programma's die met de Yubikey integreren voor sterke authenticatie.
Een Yubikey kan twee identiteiten bevatten, die elk geconfigureerd kunnen worden in één van de volgende vier modi:

1. **Standaard Yubico OTP:** de sleutel geeft een ID van 12 tekens terug en een one-time password van 32 tekens voor gebruik in samenwerking met de Yubico-servers.
2. **OATH OTP:** geeft een one-time password van 6 of 8 cijfers terug voor gebruik met OATH-servers van derden.
3. **Statisch wachtwoord:** hierin kun je zelf een wachtwoord van 1 tot 64 tekens instellen voor een standaard login.
4. **Challenge-response:** in deze modus is er specifieke client-software nodig voor challenge-response.

Op de challenge-response modus gaan we niet in omdat die heel client-specifiek is. De mogelijkheid om een statisch wachtwoord in de Yubikey in te geven is ook wat speciaal, want dat schiet wat voorbij het doel van de Yubikey, maar is soms wel handig.
In een eerder artikel over de Yubikey in Linux Magazine 6, jaargang 10, hebben we van die laatste mogelijkheid gebruikgemaakt om de Yubikey offline te gebruiken voor het inloggen op onze Linux-computer. We programmeerden toen een AES-sleutel in de Yubikey met Yubico's programma ykpersonalize en installeerden dan de PAM-module YubiPAM, zodat je kon inloggen met een druk op de knop van je Yubikey. Lees voor meer informatie hierover dat artikel nog maar eens na.

OATH

Open Authentication (OATH) is een open standaard geïntroduceerd door Verisign voor sterke authenticatie. Normaal zijn OATH-hardwaretokens apparaatjes met een lcd-scherm en batterij die vereisen dat je zelf de getoonde code overtypt. De Yubikey 2 in de OATH-modus heeft deze nadelen niet. Voor de rest kan de Yubikey naadloos samenwerken met software die authenticatie via OATH vereist. Yubico levert zelf geen back-end software of dienst voor OATH, maar er bestaan heel wat andere back-ends. Voor wie zelf aan de slag wil met een open source implementatie van OATH, is de mod-authn-otp module voor de Apache-webserver een goede start.

1 Met de Yubikey Personalization Tool herprogrammeer je je Yubikey

YUBIPAM

In het eerdere artikel over one-time passwords gebruikten we YubiPAM om op een Linux-computer in te loggen met een Yubikey in plaats van met een gewoon wachtwoord. Zoals gezegd deden we dat toen door een eigen AES-sleutel als statisch wachtwoord in de Yubikey te programmeren. De reden? We wilden een offline-oplossing die ook werkt op computers die tijdelijk geen internetaansluiting hebben, en we wilden geen communicatie met Yubico's servers.
Ondertussen is echter de Yubikey 2 verschenen die twee configuraties ondersteunt én ook het OATH-protocol. Hierdoor kun je ook een twee-factorauthenticatie aanbieden waarbij de Yubikey voor een one-time-password zorgt en je zelf nog een statisch wachtwoord intypt. Dat kan met het project OATH Toolkit.

YUBICO OTP

In de meeste gevallen zul je gebruikmaken van de standaard Yubico OTP-modus, waarin je Yubikey zich bevindt als hij van de fabriek komt. Hierbij communiceert het formulier waar je authentiseert met een validatieserver van Yubico om te controleren of het one-time password van je Yubikey correct is. Deze dienst is gratis en wordt door heel wat websites ondersteund. Zo kun je ook op het forum en de wiki van Yubico inloggen met je Yubikey en Yubico heeft een demosite waarop je de Yubikey de eerste keer kunt testen. Je moet de knop een seconde ingedrukt houden om de OTP-code te genereren.
De e-mailprovider FastMail ondersteunt sinds vorig jaar ook authenticatie via een Yubikey. Ook interessant is de online wachtwoordbeheerder LastPass, die ondersteuning van de Yubikey heeft geïntegreerd met zijn volledige productlijn. Yubico verkoopt zelfs een LastPass/Yubikey-bundel die een Yubikey met een LastPass-licentie omvat. Na het registreren van een LastPass Premium-account kun je je Yubikey toevoegen als authenticatiemiddel in het Yubikeys-tabblad van de Account Management-portal. Je kunt overigens een willekeurige Yubikey gebruiken, dat hoeft er geen te zijn van een LastPass-bundel.

TOEGANGSCONTROLE EN VPN

Wie zijn draadloos netwerk of VPN op enterprise-niveau wil beveiligen, neemt vaak zijn toevlucht tot het Radius-protocol. Een Radius-server in combinatie met een VPN zorgt voor een flexibele en veilige manier om iemand toegang te geven tot een bedrijfsnetwerk. Daarbij kan ook op elk moment de toegang van die persoon eenvoudig ingetrokken worden. De authenticatie van gebruikers kan op verschillende manieren gebeuren, zoals een klassiek wachtwoord, een certificaat, of voor de grootste veiligheid twee-factorauthenticatie waarbij een klassiek wachtwoord en een eenmalig wachtwoord gecombineerd wordt.
Uiteraard kan voor die laatste mogelijkheid een Yubikey gebruikt worden. Yubico heeft speciaal hiervoor de YubiRADIUS Virtual Appliance uitgebracht, een virtual appliance die je gratis kunt downloaden in OVF- of VMware-formaat. Daarmee zet je een virtuele machine op die Yubikey-gebaseerde twee-factorauthenticatie voor je bedrijf aanbiedt. Deze appliance draait FreeRADIUS en gebruikt een bestaande LDAP- of Active Directory-server om de gebruikers te authenticeren. Naast hun normale netwerkwachtwoord moeten de gebruikers ook een Yubikey insteken voor een eenmalig wachtwoord. De appliance kan geconfigureerd worden om een Yubikey te valideren tegen Yubico's online validatieserver of tegen een interne validatieserver die met de appliance meegeleverd wordt. De bestaande LDAP/AD-configuratie hoeft niet aangepast worden. De appliance bevat ook een Webmin-server voor een webgebaseerde configuratie. Op de website van Yubico is een uitgebreide Configuration Guide te vinden voor de appliances, evenals de appliances zelf uiteraard.

OPEN SOURCE SOFTWARE

Yubico heeft implementaties van de Yubico webservice-api open source gemaakt voor verschillende programmeertalen. Een aantal daarvan zijn rechtstreeks ondersteund door Yubico, waaronder:

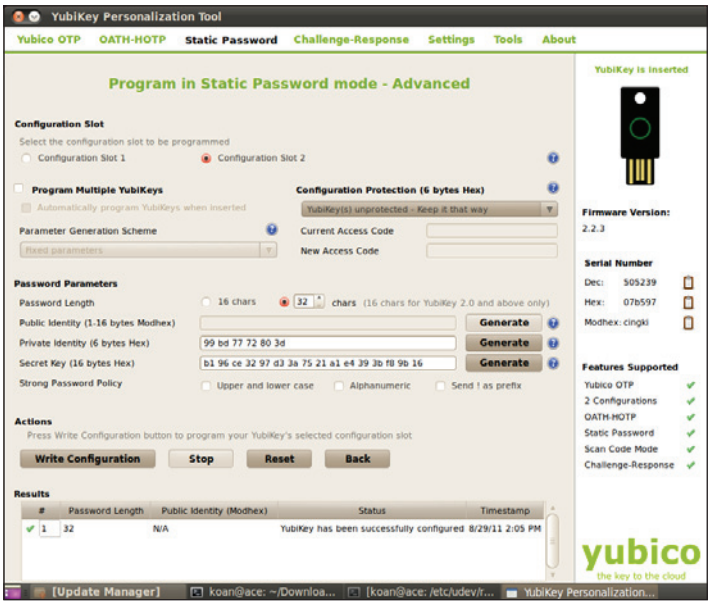
- **Php-yubico,** om Yubikeys in een php-website te valideren.
- **Yubico-c-client,** voor validatie in C-code.
- **Pam-yubico,** om via een PAM-module in te loggen op Linux of Solaris met een Yubikey.
- **Yubikey-drupal,** om Drupal uit te breiden met twee-factorauthenticatie.
- **Yubikey-mediawiki,** voor twee-factorauthenticatie op een MediaWiki-wiki.

Verder zijn er nog heel wat externe open source projecten die integreren met de Yubikey. Er zijn bibliotheken voor Java, .

VEILIG INLOGGEN MET OPENID EN YUBIKEY

De Yubikey kan ook gebruikt worden voor authenticatie op een OpenID-service. OpenID vervangt logins op allerlei plaatsen door één login, wat natuurlijk handig is, maar waardoor je wel al je eieren in één mandje legt. Iemand die je OpenID-account kan kraken, kan ineens op allerlei websites inloggen. Een Yubikey om je OpenID-account te beveiligen is daarom geen slecht idee. De Zwitserse provider Clavid biedt gratis een OpenID-service met ondersteuning voor Yubikey aan. Registreer je hiervoor door een gebruikersnaam te kiezen en je Yubikey een eenmalig wachtwoord te laten genereren. Nadat je je e-mailadres en andere gegevens ingesteld hebt, krijg je toegang tot uitgebreidere mogelijkheden, waaronder twee-factorauthenticatie met wachtwoord en Yubikey. Via de OpenID-account van Clavid kun je ook beveiligd inloggen op Google Apps. Overigens heeft Yubico zelfs de broncode van een Yubikey-compatibele OpenID-server openbaar gemaakt, zodat je zelf je eigen OpenID-server kunt draaien.

NET/C#, Ruby, Perl en Python, en er is de Apache-module mod_authn_yubikey die twee-factorauthenticatie aanbiedt via het Basic Auth-mechanisme.
Al deze software kun je gebruiken als je de Yubikey in je eigen project wilt integreren. Kijk in het kader 'Yubikey-implementaties in Nederland' voor enkele voorbeelden.
Deze projecten bevinden zich allemaal aan de client-kant, maar om een Yubikey OTP-code te valideren is er ook een server nodig. Standaard gebeurt dat met de online server van Yubico, maar als je dit niet vertrouwt, of als je clients slechts toegang hebben tot een intranet, kun je ook je eigen validatieserver draaien, tenminste als de client-library die je gebruikt dat ondersteunt.
Yubico heeft servercode in php uitgebracht en er is ook onofficiële Java-code en een third-party Python-server die zowel Yubikey OTP als OATH ondersteunt. Yubico heeft ook enkele low-level bibliotheken uitgebracht die de Yubikey OTP-codes parsen en ontcijferen. Met deze C- en Java-bibliotheken kun je in principe zelf serversoftware schrijven. Er zijn ook enkele third-party low-level bibliotheken in php, Perl en Python.



2 We hebben juist een statisch wachtwoord in het tweede configuratieslot van de Yubikey geschreven

TWEE IDENTITEITEN

De Yubikey kan twee identiteiten bevatten, maar bevat er standaard maar één, een Yubico-OTP. Je kunt de Yubikey aanpassen met de Yubikey Personalization Tool, die zowel voor Windows en Mac als voor Linux bestaat (zie *afbeelding* **1**). Dit is een grafische Qt-applicatie waarmee je beide configuraties kunt instellen, met voor elke configuratie de keuze uit de vier modi. Let wel op dat als je de standaard Yubico OTP-configuratie herinitialiseert, je niet meer de validatieserver van Yubico kunt gebruiken. Wil je dit toch nog, dan moet je de aes-sleutel opnieuw uploaden. Volg hiervoor de instructies op de pagina AES Key Upload van Yubico. Je kunt natuurlijk ook je eigen validatieserver hosten, maar niet alle software ondersteunt dit.
Download de cross-platform Personalization Tool van de website van Yubico. Dit is een tgz-bestand van 50 MB. Unpack het, waarna je het programma YKPersonalization en drie bibliotheken ziet, evenals een shellscript om het programma op te starten met gebruik van de bijgevoegde bibliotheken. Let op: de Personalization Tool heeft schrijftoegang nodig tot het usb-apparaat van de Yubikey, wat je standaard niet hebt. Je kunt het programma wel als root uitvoeren, maar dat is niet veilig. We maken daarom de volgende udev-regel aan in /etc/udev/rules.d/90-yubikey-permissions.rules die je normale gebruiker schrijftoegang geeft tot je Yubikey.

```
ATTR{manufacturer}=="Yubico",
ATTR{product}=="Yubico Yubikey
II", MODE="0660", OWNER="koan",
GROUP="koan"
```

Fredrik Thulin is sinds begin dit jaar open source manager bij Yubico. We vroegen hem wat open source voor Yubico betekent en wat zijn taak precies inhoudt.

LM: Jullie geven open source software uit, onder andere voor de validatieserver en low-level library's die met de Yubikey communiceren. Wat zijn jullie redenen hiervoor?
FT: We open sourcen bijna alles waarvan we denken dat anderen er voordeel van hebben, behalve de firmware van onze apparaten, de Yubikey en de YubiHSM. Yubico verdient vooral geld aan het verkopen van de apparaten, en we open sourcen de software die we geschreven hebben om de volgende redenen:
1. We willen niet vastlopen in softwareontwikkeling. Als we onze software niet open source hadden gemaakt, zouden we voor veel wensen van onze klanten voor betaalde ontwikkeling moeten kiezen. Zo zou onze software als bijvoorbeeld de validatieserver snel te maken gehad hebben met feature creep en de hele bureaucratie rond de softwareontwikkeling zou er nog bij komen.
2. We hopen dat onze producten door het open sourcen van de software geloofwaardigheid krijgen in het domein van de computerbeveiliging. We weten van een aantal personen in dit gevoelige IT-domein dat ze alles willen zien dat in hun beveiligingssystemen omgaat.
3. Open source kan echt tot software van betere kwaliteit leiden, wat uiteraard extreem belangrijk is als het over beveiligingstoepassingen gaat. Als we dit goed doen, kan het open sourcen van onze software ons ook economisch voordelig uitvallen door de hulp van externe open source-ontwikkelaars.

LM: Wat doe je precies als open source manager bij Yubico?
FT: Ik ben aangenomen 'om onze diverse open source applicaties succesvol te maken', of iets in die aard ;-). Dat betekent in de praktijk dat ik bug reports indien, patches toepas en organisaties en personen ook van het nut van twee-factor-authenticatie probeer te overtuigen. Ik heb een multi-factor login-handler toegevoegd aan het open source single sign-on programma Shibboleth, en ik heb het mogelijk gemaakt om een Yubikey 2.x HMAC-SHA-1 challenge-response als decryptiesleutel te gebruiken voor bestandssystemen die met eCryptfs versleuteld zijn.

Fredrik Thulin, open source manager bij Yubico

YUBIKEY-IMPLEMENTATIES IN NEDERLAND

Ook een aantal Nederlandse organisaties maken al gebruik van de Yubikey voor veilige authenticatie. Accelcloud.com heeft bijvoorbeeld een Ubuntu terminal server voor Free Press Unlimited opgezet, waarbij de authenticatie van de gebruikers gebeurt met de Yubikey.
"Free Press Unlimited wil kwaliteitsnieuws en -informatie beschikbaar maken voor iedereen en heeft ook een aantal medewerkers in repressieve landen," zegt Robert de Geus van Accelcloud.
"Daarom willen we hen een veilige manier aanbieden om in te loggen, bijvoorbeeld in internetcafés. Dat kan met de Yubikey, omdat keyloggers de veiligheid van de verbinding dan niet in gevaar brengen."
Voor gebruikersbeheer maakt Accelcloud gebruik van GOsa, wat ook door de stad München gebruikt wordt voor hun Linux-desktops.
"We hebben een plug-in voor GOsa geschreven om van in de beheerinterface Yubikeys in te voeren en te deactiveren. Deze plug-in zullen we onder een open source-licentie ter beschikking stellen."
Ook uitgeverij/drukkerij De Koninklijke BDU gebruikt de Yubikey. De BDU heeft een aantal tijdschriften die oorspronkelijk alleen maar op papier verschenen, maar sinds kort krijgen abonnees naast hun papieren versie ook een digitale versie in pdf.
Volgens Henk van de Brug van de uitgeverij was dit echter te eenvoudig: "In plaats van met onze service abonnees te winnen, bleek dat de pdf-bestanden na verloop van tijd een eigen leven gingen leiden en wij enkel maar abonnees kwijtraakten. Zelf lees ik regelmatig Linux Magazine en las ik in januari 2010 in een artikel over de Yubikey. Door het pdf-probleem dacht ik daaraan terug. Toen bleek er een Yubikey-plugin voor WordPress te bestaan en daarom hebben we een WordPress-site gemaakt waarbij abonnees zich authenticeren met de Yubikey, waarna ze hun digitale blad kunnen lezen. De pdf-bestanden hebben we omgezet naar swf-bestanden, zodat het bewaren en doorsturen niet meer mogelijk is."

Pas hierin OWNER en GROUP aan naar je eigen gebruikersnaam. Voer daarna de Personalization Tool uit.

```
$ sh ./Yubikey\ Personalization\
Tool.sh
```

Als je Yubikey in de computer steekt, toont het programma rechts enkele gegevens, zoals de firmwareversie en het serienummer van je Yubikey, evenals de ondersteunde features. Dat laatste is handig om het verschil met de eerste versies Yubikey te zien, die slechts één configuratie ondersteunden en enkel de Yubico OTP-modus en een beperkte modus voor een statisch wachtwoord.
Naar die twee configuraties is het overigens op het eerste gezicht wat zoeken in de Personalization Tool, maar je moet gewoon kiezen welk type wachtwoord je wilt configureren, waarna je het configuratie-slot kiest. Daarna kun je de Yubikey in de eerste configuratie gebruiken door een korte druk op de knop (0,3 tot 1,5 seconden) en de tweede configuratie door lang (2,5 tot 5 seconden) te drukken en dan los te laten.
Na het herprogrammeren moet je het programma overigens afsluiten en de Yubikey verwijderen en terug insteken voor je hem weer kunt gebruiken (zie *afbeelding* **2**).

YUBICO PAM

Tot slot tonen we hier hoe je de officiële PAM-module van Yubico kunt gebruiken om je authenticatie te beveiligen. Na de installatie controleer je of het bestand pam_yubico.so in /lib/security staat. Daarna moet je de PAM-configuratie nog aanpassen. Als je bijvoorbeeld voor het inloggen via ssh en voor lokale logins een Yubikey wilt gebruiken, zet dan vooraan het bestand /etc/pam.d/common-auth het volgende.

```
auth requisite pam_yubico.so au-
thfile=/etc/yubikeyid id=1683
```

Hierbij is het vermelde id je Client ID van de apikey die je bij Yubico moet aanvragen om van de validatieserver gebruik te kunnen maken.

De volgende regel in /etc/pam.d/common-auth is onder Ubuntu normaal het volgende.

```
auth [success=1 default=ignore]
pam_unix.so nullok_secure
```

Dit zorgt voor het vragen van het normale wachtwoord. We laten dat ook door de Yubico PAM-module afhandelen, en daarom moeten we achteraan deze regel nog 'try_first_pass' toevoegen.
In het bestand /etc/yubikeyid staat de mapping tussen gebruikersnamen en de eerste 12 tekens van de uitvoer van de Yubikey, bijvoorbeeld: 'koan:vveflvcdnduf'.
Voor elke gebruiker voeg je hier een regel toe met zijn gebruikersnaam en het bijbehorende Yubikey ID van 12 tekens.
Als je nu via ssh inlogt, moet je eerst je normale wachtwoord ingeven en vlak daarna, zonder op enter te drukken, op de knop van de Yubikey drukken. Je komt enkel binnen als beide correct zijn. Bij een sudo, console login, de schermbeveiliging of het aanmeldvenster van GDM wordt je expliciet eerst om je Yubikey-uitvoer gevraagd en dan om je normale wachtwoord. Achter de schermen wordt met de validatieserver van Yubico gecommuniceerd om je one-time passwords te verifiëren. Bekijk de website van Yubico PAM voor alle mogelijkheden.

VEILIGER OP INTERNET

Het mag duidelijk zin dat de Yubikey een mooie en betaalbare open source-oplossing is voor veilige twee-factorauthenticatie. Beveiliging van je persoonlijke gegevens is een groot goed, maar ook binnen bedrijven zou een dergelijke extra beveiligingslaag eigenlijk verplicht moeten zijn.

LINKS

Yubikey
www.yubico.com/yubikey

Yubikey webshop
www.yubikeyshop.nl

OATH
www.openauthentication.org

Mod-authn-otp
http://code.google.com/p/mod-authn-otp

Yubikey demo
http://demo.yubikey.com

Gebruik Yubikey met LastPass
http://helpdesk.lastpass.com/security-options/yubikey-authentication

YubiRADIUS
www.yubico.com/radius

Yubikey Personalization Tool
www.yubico.com/personalization-tool

Ykpersonalize
https://code.google.com/p/yubikey-personalization

OATH Toolkit
http://www.nongnu.org/oath-toolkit

Aes-key upload
https://www.yubico.com/aes-key-upload

Yubico API-sleutel
https://upgrade.yubico.com/getapikey

Yubico PAM
https://code.google.com/p/yubico-pam