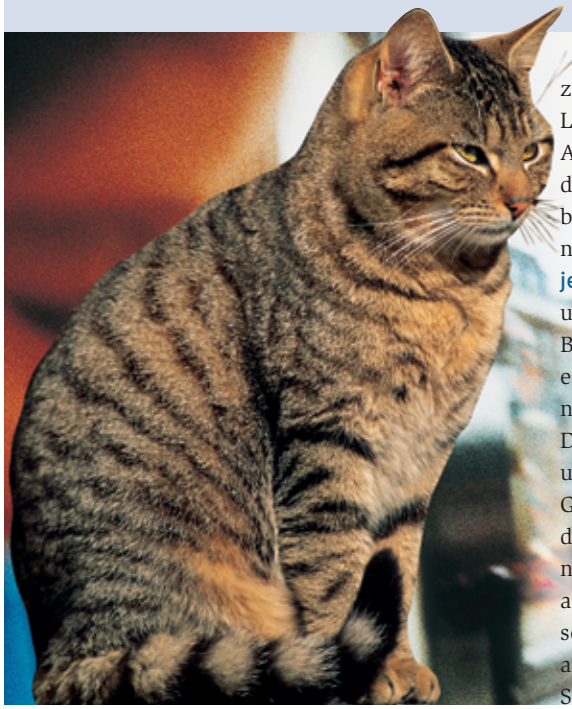
No Cat Auth authentifiziert WLAN-Benutzer am NAT-Router

Schnurlos schnurren

Ohne Kabel online – technisch kein Problem, nur die Sicherheitsprobleme der Funknetze stören die Gemütlichkeit. Jedem Besucher im Café gegenüber beliebig Bandbreite schenken ist nicht jedermanns Sache, also muss eine Authentifizierung her. Die sollte plattformunabhängig funktionieren. Jochen Stärk



Dass die WLAN-eigene Verschlüsselung und Authentifizierung löchrig ist [1] und sich in Sekundenschnelle knacken lässt [2], hat sich mittlerweile herumgesprochen. Tools wie Airsnort, D-Wepcrack und Kismet [3] führen das recht anschaulich vor. Ein WLAN muss daher als externes, unsicheres Netz gelten: Hier könnten unangenehme Zeitgenossen ihr Unwesen treiben. Wer seinen Laptop dennoch ins interne Netz einbinden will, greift am besten auf die etablierten VPN-Techniken [4] zurück, beispielsweise IPsec oder OpenVPN.

Soll ein WLAN aber als Hotspot vielen Benutzern Zugang zum Internet verschaffen, sind VPNs nicht unbedingt nötig, die User müssen und können sich selbst für eine geeignete Sicherheitstechnik entscheiden. Eine Authentifizierung ist dennoch wichtig, schließlich soll nicht jeder beliebige Nachbar den Netzzugang schnorren und kostenlos surfen. Lösen lässt sich das Problem mit No Cat Auth [5]. Auf dem Client hält sich dazu der nötige Aufwand in sehr überschaubarem Rahmen – ein Webbrowser genügt. No Cat (siehe Kasten „Der Projektname“) wacht auf dem Gateway und lässt nur die Daten der erwünschten Benutzer passieren. Bei Bedarf schränkt es sogar die Bandbreite ein, die ein Benutzer beanspruchen darf.

Die Software besteht aus einem Gateway und einem Authentifizierungsserver. Das Gateway arbeitet als adaptive Firewall, die den Übergang vom WLAN ins Internet kontrolliert. Bevor sich ein Benutzer authentifiziert hat, fängt das Gateway seine Pakete ab und leitet Webanfragen an das No-Cat-Formular um. Der Auth-Server prüft die Userdaten gegen eine MySQL-Datenbank, gegen Shadow-Passwörter, LDAP, IMAP, PAM, Samba oder NIS (Tabelle 1).

Registrierung inbegriffen

Setzt der Authentifizierungsserver eine MySQL- oder PostgreSQL-Tabelle als Nutzerdatenbank ein, müssen Zugriffsaspiranten zunächst ein Registrierungsformular ausfüllen. Der Admin kann den dabei erzeugten Accounts später zusätzliche Rechte zuweisen. Ist schon ein Nutzerverzeichnis – etwa NIS – vorhanden, bedient sich der Auth-Server auf Wunsch auch dort. Neben externen Tools wie PHP MyAdmin bietet sich auch »admintool« an. Das Kommandozeilenprogramm wartet die No-Cat-Accounts (Tabelle 1, rechte Spalte).

Greift ein Benutzer in einem No-Cat-Netz mit seinem Browser auf eine beliebige Webseite zu, leitet das IPTables-basierte Gateway die Anfrage auf den Authentifizierungsserver um. Dort gibt der User seine Kennung und das Passwort ein. Stimmt beides, darf er (genauer sein Rechner, siehe Kasten „Sicherheit“) über das Gateway ins Internet. Der Gateway-Daemon aktiviert NAT (Network Address Translation) und erlaubt reguläre Protokolle wie SSH, POP3, IMAP, HTTP, HTTPS, passives FTP und viele mehr. Nur SMTP ist aus Spamschutzgründen in der Default-Konfiguration ausgeschlossen.

Bequem per Webmin konfigurieren

Wer das No-Cat-Gebilde nicht manuell konfigurieren will, findet Hilfe in einem Webmin-Modul [9]. Trotz der vergleichsweise niedrigen Versionsnummer (0.51) ist es recht stabil und sofort einsatzbereit, nur die Pfade zu den Konfigurationsdateien sind noch anzupassen. Das folgende Beispiel setzt einen DHCP-Server mit Adressbereich 192.168.0.10 bis 192.168.0.254 voraus. Die Benutzerdatenbank liegt auf einem eigenen Server mit der internen IP-Adresse 192.168.0.1. Darauf laufen MySQL, PHP MyAdmin und ein Apache mit Mod_SSL-Modul.

Für den ersten Test sollten die Anforderungen noch niedrig sein, ein offenes Gateway ist zunächst ausreichend. Es ist schnell installiert – aber Achtung: Per Default installiert No Cat sowohl Gateway als auch Authserver in das Verzeichnis »/usr/local/nocat«. Ein Präfix trennt beide Pakete:

```
tar xvfz NoCatAuth-0.82.tar.gz
cd NoCatAuth-0.82
make PREFIX=/usr/local/nocat/gw gateway
```

Tabelle 1: Authentifizierung

Feature	Beschreibung	No Cat Auth	Admintools
Radius	Authentifizierung über einen Radius-Server	experimentell	–
LDAP	Authentifizierung über LDAP	–	nein
DBI::MySQL	Benutzerdatenbank in MySQL mit Authentifizierung und Registrierung	ja	–
DBI::PostgreSQL	Benutzerdatenbank in PostgreSQL mit Authentifizierung und Registrierung	ja	–
Passwd	Authentifizierung über lokale Dateien	ja	ja
PAM	Authentifizierung über PAM	–	–
Samba	Authentifizierung über Samba oder Windows (Primary Domain Controller)	–	nein
IMAP	Authentifizierung über IMAP-Accounts	–	nein
NIS	Authentifizierung über NIS	–	nein

Der offene Gateway-Modus lässt sich durch den Eintrag »GatewayMode Open« in der Konfigurationsdatei »/usr/local/nocat/gw/nocat.conf« aktivieren. No Cat kennt drei Modi:

- »Open«: Das Gateway zeigt hier nur eine Begrüßungsseite und verlangt vom User, dass er die Benutzungsbedingungen akzeptiert.
- »Passive«: Hier kann sich der Benutzer authentifizieren. Dies ist die empfohlene Einstellung.
- »Captive«: Ähnlich wie Passive, unterstützt aber kein NAT.

Ein beherztes »/usr/local/nocat/gw/bin/gateway« startet das Gateway.

Nutzerdatenbank

Da das Gateway in den meisten Fällen nicht jeden Wunsch eines beliebigen Notebooks erfüllen soll, braucht es eine Nutzerdatenbank. Mit der Einstellung »GatewayMode Passive« greift das Gateway auf den Authentifizierungsserver zurück und fragt dort, ob ein Benutzer auch berechtigt ist. Wo dieser Server zu finden ist, lässt sich mit »AuthServiceAddr 192.168.0.1« festlegen.

Der Projektname

No Cat ist der Name einer Community, die in Sonoma County (Kalifornien) Hotspots betreibt. Ihre Mitglieder gewähren sich gegenseitig unentgeltlichen drahtlosen Zugang zum Internet.

Ein Text auf der Homepage des Projekts [http://nocat.net/] erklärt den lustigen Namen. Er geht auf ein berühmtes Zitat zurück. Auf die Frage, wie Funk funktioniert, antwortete Albert Einstein: „Ein Kabel-Telegraph ist so etwas wie eine sehr, sehr lange Katze. Sie ziehen in New York an ihrem Schwanz und hören den Kopf in Los Angeles miauen. Funk funktioniert genauso: Sie schicken Signale hier ab und empfangen sie dort. Der Unterschied: Es gibt keine Katze."

Zentraler Server

In einer größeren Community sollte nicht jeder Hotspot-Betreiber seinen eigenen Auth-Server betreiben – es genügt ein zentraler Dienst. So kommen die Mitglieder mit einem einzigen Account aus und müssen sich nicht überall einzeln anmelden. Wer den Authentifizierungsserver selbst betreiben will, muss ihn zunächst kompilieren:

```
make PREFIX=/usr/local/nocat/as authserv
make PREFIX=/usr/local/nocat/as pgpkey
chown -R wwwrun /usr/local/nocat/as/pgp
cp /usr/local/nocat/as/trustedkeys.gpg ➥
   /usr/local/nocat/gw/pgp
```

Um ausschließlich authentifizierte User zuzulassen und keinen öffentlichen Access Point zu betreiben, ist in der Gateway-Konfiguration »/usr/local/nocat/gw/nocat.conf« zusätzlich der Eintrag »MembersOnly 1« nötig. Auch auf dem Auth-Server sind noch ein paar Änderungen erforderlich: Der Apache muss die CGI-Skripte ausführen und die richtigen HTML-Files anzeigen. Was dazu zu ändern ist, steht in der Vorlage »/usr/local/nocat/as/httpd.conf«.

Die User-Datenbank will auch gepflegt sein; hier hilft PHP MyAdmin. Mit diesem MySQL-Frontend legt der Admin zunächst einen Datenbanknutzer und eine Datenbank für No Cat an, erzeugt die nötigten Tabellen (siehe MySQL-Dump »etc/nocat.schema« im Quellpaket) und passt die Konfiguration des Auth-Servers an (»/usr/local/nocat/as/nocat.conf«):

```
DataSource   DBI
Database     dbi:mysql:database=nocat
DB_User      nocat
DB_Passwd    rubbeldiekatz
```

Apache kann nun als Authentifizierungsserver laufen (»apachectl startssl«). Das Gateway leitet jeden Besucher erst einmal zu diesem Apache um (siehe Abbildung 1), wo er sich anmeldet (Abbildung 2) oder zumindest die Benutzungsbedingungen akzeptiert.

Weitere Informationen finden sich auf der No-Cat-Homepage [5], den entsprechenden Mailinglisten und im Howto von Toni Diaz [6]. Schade, dass das Thema No Cat Auth dem No-Cat-Initiator in seinem eigenen Buch [10] nur drei Seiten wert war.

Kabelgebundene Netze

No Cat ist für Access Points ausgelegt, die als Bridges konfiguriert sind. Daher eignet sich diese Software auch als Gateway für andere Netztechniken. Egal ob Firma oder Studentenwohnheim – den

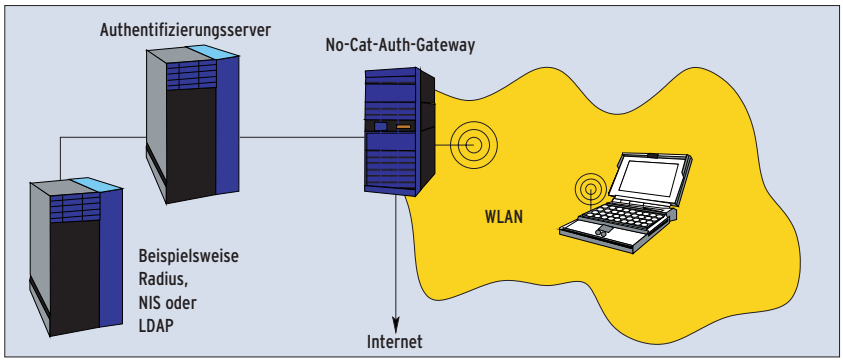


Abbildung 1: Drahtlose Clients greifen über einen Access Point auf das Internet dazu. Dazu müssen sie aber erst das No-Cat-Auth-Gateway passieren. Ob sie das dürfen, entscheidet der Authentifizierungsserver.

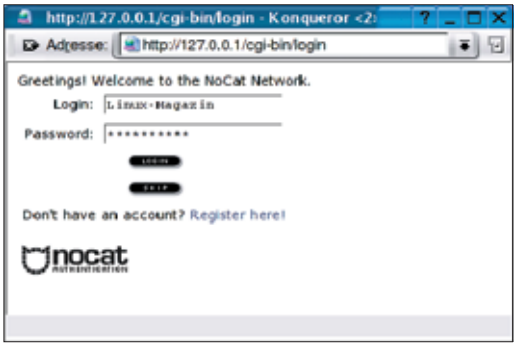


Abbildung 2: Dieser Screen begrüßt jeden Besucher. Der User loggt sich ein und darf dann über das No-Cat-Gateway online gehen. Der Admin kann die HTML-Quelltexte seinen Wünschen anpassen.

Admin freut's, wenn er bei jedem neuen Rechner im Netz erfährt, wer dafür zuständig ist. Durch interne No-Cat-Gateways kann er den Wirkungsbereich eines unbekannten Rechners recht gut eingrenzen.

Die Authentifizierung arbeitet aufgrund des No-Cat-Designs auch zentral für Benutzergruppen an verschiedenen Standorten. Sie unterscheidet eingeloggte von nicht eingeloggten Benutzern und kann ihnen beispielsweise unterschiedliche Bandbreite bereitstellen. Traffic Control (TC) schränkt die Datenrate je nach Gruppe (Total, Owner und Public) ein, dieses Feature ist derzeit aber noch experimentell.

Accounting

Accounting, also das Protokollieren der übertragenen Datenmenge, lässt sich über ein Patch [7] nachrüsten. Das Accounting ist unabhängig von der eingesetzten Authentifizierungsmethode und schreibt in Radius oder beliebige Dateien (»File«). Der Test, ob das Accounting in Dateien auch klappt, fiel leider recht dürftig aus: Accounting ins No-Cat-Log (»Log«) und in Datenbanken (»DBI«) scheint zwar vorgesehen, aber noch nicht implementiert zu sein.

Loggt sich ein User ein oder aus, schreibt das No-Cat-Gateway dieses Ereignis in die Datei »nocat.log«. Deren Name und Ort lässt sich per »GatewayLog«-Option konfigurieren, ihre Ausführlichkeit per »Verbosity«. Die »LogFacility« bringt No Cat auch dazu, ins Syslog zu protokollieren.

Eine zentrale Übersicht, wann sich welcher Nutzer ein- beziehungsweise ausgeloggt hat, ist so allerdings nur schwer zu erreichen. Der Autor dieses Artikels hat daher ein Patch [8] entwickelt, das in einer eigenen Datei pro User festhält, wann sich dieser authentifiziert hat, welche MAC- und IP-Adresse er dabei benutzte und wann er seine Anmeldung aufgefrischt hat. Ein zweites File pro User gibt seinen aktuellen Status (angemeldet oder nicht) wieder.

Eine Auswertungsseite (ein Beispiel ist ebenfalls auf [8] zu finden) zeig dann dem Administrator, welche User gerade online sind, ob ein Nutzer gegebenenfalls seine Anmeldung weitergegeben hat (erkennbar an verschiedenen MAC-Adressen) und wie lange jeder Anwender am Hotspot angemeldet war.

No Cat Auth eignet sich für Netze, die eine Zugangsbeschränkung an zentraler Stelle auflegen können und wollen. Als Client-Software genügt ein Browser. Dieser Vorteil ist gleichzeitig ein Nachteil: Derzeit ist noch kein Client verfügbar, der sich in No-Cat-Netze automatisch einloggen oder einen Timeout verhindern könnte. Damit die Verbindung stehen bleibt, muss der User ein Browserfenster offen halten.

Perl oder C

Zurzeit steht eine Neuimplementierung auf dem Programm: Während No Cat Auth in Perl programmiert ist, setzt der Nachfolger No Cat Splash auf Ansi-C und Multithreading. Der Grund dafür sind Embedded-Anwendungen, bei denen ein Perl-Interpreter meist die Grenzen der verfügbaren Ressourcen sprengt. Die Autoren pflegen No Cat Auth aber weiterhin. *(fjl)*

Sicherheit

Die Sicherheit einer No-Cat-Authentifizierung ist nicht zu vergleichen mit einem guten Client-to-Site-VPN. Der Grund: Bei No Cat sind Authentifizierung und Datenübertragung nicht kryptographisch aneinander gebunden. Die Authentifizierung ist durch SSL zwar gut geschützt (vorausgesetzt das Zertifikat ist in Ordnung – siehe PKI-Artikel in diesem Heft), auf die Datenübertragung nimmt No Cat aber keinen Einfluss. Damit bietet No Cat auch keine Verschlüsselung. Die Übertragungen sind von allen Hotspot-Usern grundsätzlich abhörbar. Eine zusätzliche Verschlüsselung ist also sehr zu empfehlen.

Hat sich ein Benutzer erfolgreich authentifiziert, schaltet das No-Cat-Gateway seine IP- und MAC-Adresse frei. Ein Angreifer kann diese Daten aber abhören und selbst mit dieser IP und MAC senden.

Authentifizierung klauen

Bis die Authentifizierung des regulären Anwenders abläuft, hat der Angreifer Zugriff auf das Netz hinter dem Gateway. Für die meisten WLAN-Communities ist dieses Risiko tragbar. Wer einen besseren Schutz benötigt, sollte IPsec, OpenVPN oder andere sichere VPN-Techniken [4] einsetzen. *(Achim Leitner)*

Infos

[1] Scott Fluhrer, Itsik Mantin und Adi Shamir, „Weaknesses in the Key Scheduling Algorithm of RC4": [http://www.crypto.com/papers/others/rc4_ksaproc.ps]

[2] Adam Stubblefield, John Ioannidis und Aviel D. Rubin, „Using the Fluhrer, Mantin, and Shamir Attack to Break WEP": [http://www.cs.rice.edu/~astubble/wep/]

[3] Mark Vogelsberger, „Kismet & Co.: WLAN-Sicherheit unter der Lupe", Linux-Magazin 12/03, S. 36

[4] Titelthema „VPN-Techniken", Linux-Magazin 10/03

[5] No Cat Auth: [http://nocat.net/wiki/]

[6] Howto-Beschreibung zu No Cat Auth: [http://blyx.com/public/wireless/nocatbox/nocatbox-howto-en.pdf]

[7] Patches für IPFW2, Accounting, Radius udn SNMP-Monitoring: [http://www.pogozone.net/projects/nocat/]

[8] Patch zum Protokollieren der Nutzerzugriffe: [http://www.usegroup.de/software/nocat/]

[9] Webmin-Modul für No Cat: [http://sourceforge.net/projects/nocat-webmin/]

[10] Rob Flickenger, „Building Wireless Community Networks. Planning and Deploying Wireless Local Networks": O'Reilly 2003, Kap. 7, S. 113

Der Autor

Jochen Stärk studiert Wirtschaftsinformatik an der Berufsakademie Mannheim.