“Der Ur-Kerberos”

von MIT
Aus dem RFC „übersetzt“ von Mathias Feiler

Ein spannendes Stück über Beziehungen, Vertrauen und gut gehütete Geheimnisse aus der Welt der elektronischen Datenverarbeitung.

~ Der Ur-Kerberos ~

Es spielen :

A: Der auktoriale Erzähler 'Admin' des Königreiches 'Realm' (R)
U: Frau Usula die Kundin , wohnhaftig im Königreich 'R'
K: Der Kerberos , König des Reiches 'R'
S: Der Pfefferminz-Server aus dem Königreich 'R'
N: Der neugierige Nachrichtenkurier 'Netzer' , Kumpane der Räuber im Wald.

Spielregeln:

1. Ein Schlüssel ist das, was man umhängen kann.
2. Der Besitz eines Schlüssels (Farbe) wird durch das Umhängen desselben zur Schau gestellt.
3. Hat ein Spieler eine Farbe umgehängt, so kann er Nachrichten, die in dieser Farbe verschlüsselt sind, entschlüsseln. Auch kann er in dieser Farbe verschlüsseln.
4. Für die 2. Spielgruppe gilt : Gelb=Weiß , Orange=Rot , Grün=Blau

Akt 1 Szene 1 :

Der Erzähler (A) macht Frau Usula (U) und den König Kerberos (K) miteinander bekannt.
Sie schütteln sich die Hände.
Zum Zeichen Ihrer innigen Bekanntschaft nehmen beide von A ein gemeinsames ROTES Geheimnis entgegen. (Es kann aus dem Passwort der U hergestellt werden.)
Sie gehen wieder auseinander.

Akt 1 Szene 2:

Der Erzähler (A) macht den Pfefferminz-Server (S) und und den König Kerberos (K) miteinander bekannt.
Sie schütteln sich die Hände.
Zum Zeichen Ihrer innigen Bekanntschaft nehmen beide von A ein gemeinsames BLAUES Geheimnis entgegen. Sie gehen wieder auseinander.

Akt 2 Szene 1 :

Der Erzähler berichtet :

Usula sehnt sich nach Pfefferminz-Zuwendung. Sie hat gehört, dass der S dieses an gute Bekannte im Reich R vertreibe. Leider kennen sich S und Usula nicht persönlich. Darum wendet sich die Usula mit dem Brief "MSG 01" an den König Kerberos (K).

- MSGS01 Vorlesen -

Sie übergibt den Brief (durchsichtig verpackt) an den suspekten neugierigen Netzer (N) zur Zustellung an König Kerberos (K) .

Akt 2 Szene 2:

Netzer (N): Kommt zum K und übergibt den Brief – nicht ohne ein schmunzelndes Lächeln , welches verrät, dass er Kenntnis vom Inhalt des Briefes hat.

Der König K des Reiches R liest den Brief.
Er denkt sich nun erst einmal etwas aus.
Dabei kommt er auf den Schlüssel-Code "WEISS" .

Zwei dieser WEISSEN Schlüssel werden hergestellt.

Er verfasst die Nachricht "MSGS 02" .

- MSGS02 Vorlesen

Er steckt die Nachricht zusammen mit einem der WEISSEN Schlüssel in eine Tasche und versiegelt diese mit dem BLAUEN Geheimnis, welches er und Server (S) gemeinsam haben.

Der K verfasst außerdem eine weitere Nachricht "MSGS 03",

- MSGS 03 Vorlesen

steckt sie zusammen mit dem anderen WEISSEN Schlüssel in eine Tasche und versiegelt diese mit dem ROTEN Geheimnis, welches er und die Usula (U) gemeinsam haben.

Dazu schreibt K eben noch ein Begleitschreiben "MSGS 04"

- MSGS 04 Vorlesen

Alle 3 Dinge zusammen (in der durchsichtigen Netzwerktasche) übergibt er dem suspekten neugierigen Netzer (N) zur Zustellung an Usula (U).

Akt 3 Szene 1

Die Usula erhält die Sendung des K. Sie liest das Begleitschreiben "MSG 04" und legt es beiseite.

- MSGS 04 Vorlesen

Nun öffnet Usula mit dem gemeinsamen ROTEN Geheimnis die Tasche die

entsprechend ROT versiegelt ist. Ein WEISSER SCHLÜSSEL und die Nachricht "MSG 03" kommen zum Vorschein.

- MSGS 03 Vorlesen

Sie ist äußerst entzückt über den zuschlägigen Bescheid und den Erhalt des passenden Sessionkeys (WEISS), den sie sich sogleich umhängt.
Da Sie vor falschen, im Wald herumlungernden bösen Servern gehört hatte, die vergiftetes Pfefferminz versenden, um dann die wehrlosen Kunden aus zu rauben, will sie sicherstellen, dass sie auch wirklich nur vom echten Pfefferminz-Server (S) des Reiches (R) bedient wird.

In Ihrem Brief "MSGS 05" fordert sie darum den Pfefferminz-Server auf, zu beweisen, das auch er Er ist. Dazu schreibt sie ihre kommagenaue Urzeit auf und merkt sich dies auch selbst.

- MSGS 05 vorlesen

Den Brief versiegelt die U mit dem soeben erhaltenen WEISSEN Schlüssel.

Diesen sendet Sie zusammen mit dem BLAU verschlüsselten Ticket (oder Token) und dem Begleitschreiben "MSGS 06" (in einer durchsichtigen Netzwerk-Tasche) an den Pfefferminz-Server S.

- MSGS 06 vorlesen

Für die Zustellung bemüht sie den N. Dieser zeigt sich missmutig, weil er, abgesehen vom Begleitschreiben, nicht lesen kann was er zu transportieren hat. Mit solchen Paketen kann er und seine delinquente Freunde aus dem Wald nichts anfangen.

Akt 3 Szene 2

Server S erhält die Nachricht von Netzer.
Das Begleitschreiben MSGS 06 nimmt er ohne weitere Regung zur Kenntnis.

- MSGS 06 vorlesen

Er ist aber noch nicht bereit tätig zu werden, denn soweit hätte jeder diese Nachricht senden können. Zunächst kann er auch den WEISS versiegelten Brief nicht öffnen, darum nimmt S seinen BLAUEN Schlüssel und öffnet damit das Ticket (oder Token).
Sehr aufmerksam liest S das enthaltene Schreiben "MSGS 02"

- MSGS 02 vorlesen

Sofort blickt er auf seine Uhr und rechnet genau nach, ob er wirklich tätig werden soll. Daraufhin hängt er sich den beiliegenden WEISSEN Sessionkey um.
Mit dem so erhaltenen WEISSEN Key öffnet S nun die WEISS verschlüsselte Nachricht von Usula und liest diese ebenfalls aufmerksam.

- MSGS 05 vorlesen

Er erstellt die Nachricht "MSG 07", in der er , wie aufgefordert, auch die ihm übermittelte Komma-genaue Urzeit erwähnt.

- MSGS 07 vorlesen

Er legt sie in eine Versandtasche und versiegelt diese mit dem Schlüssel „WEISS".

Des weiteren nimmt S eines der frisch hergestellten Pfefferminz, packt dies in eine weitere Versandtasche und versiegelt auch diese mit dem Session-Key „WEISS“. Dann wird noch eben ein Begleitschreiben „MSGS08“ verfasst, welches recht kurz ausfällt.

- MSGS 08 vorlesen

Zur Zustellung an die U wird alles zusammen als Paket (in der üblichen durchsichtigen Netz-Tasche vereint) dem neugierigen NETZER (N) übergeben. Dieser erscheint recht deprimiert , weil weder er, noch seine Kumpanen im Wald eine Chance sehen die U zu täuschen , zu betäuben und dann aus zu rauben.

Nachdem der N weg ist verwirft der Pfefferminz-Server (S) den WEISSEN Sessionkey, da dieser keine weitere Bedeutung für ihn hat. Sollte die U weitere Anfragen starten wollen , so wird Sie wieder eine Kopie des Tickets (bzw.Tokens) mitsenden. In diesem steckt dann auch wieder der passende Sessionkey – Welche Farbe auch immer dieser dann haben wird.

Akt 3 Szene 3

Der suspekte N übergibt der U die Nachricht von Pfefferminz-Server 'S'.
Misstrauisch entnimmt die U das Begleitschreiben und liest.

- MSGS 08 vorlesen

Es ist ein gutes Zeichen, dass das Pfefferminz nicht lose der Nachricht bei lag, sondern vermutlich von S verschlüsselt wurde. Andernfalls hätte unterwegs jeder das Pfefferminz austauschen können. Die Usula will aber wirklich sicher sein.
Sie öffnet den ersten Umschlag mit dem WEISSEN Schlüssel und begutachtet zunächst die Nachricht MSGS07.

- MSGS 07 vorlesen

Die gestellte Aufgabe ist gelöst. Der S hat genau die von U für diese Anfrage verschickte kommagenaue Urzeit in seiner Antwort erwähnt. Daran erkennt Usula, dass der Pfefferminz-Server ebenfalls im Besitz eines WEISSEN Schlüssels gewesen sein muss. Diesen konnte er nur aus dem von ihr selbst weitergereichten Ticket (bzw. Token) entnommen haben, welches die Usula mit der 'Anfrage um Pfefferminz' mit sandte. Das Ticket (oder Token) kam nachweislich von dem K, der mit der Usula das gemeinsame Geheimnis “ROT” hat.
Da der Pfefferminz-Server dieses Ticket entschlüsseln konnte muss er ebenfalls ein gemeinsames Geheimnis mit K haben (BLAU). Damit liegt der Verdacht nahe, dass der Pfefferminz-Server wirklich der ist, dessen Pfefferminze die Usula begehrt.
Die U öffnet mir ihrem Sessionkey „WEISS“ die zweite „WEISS“ verschlüsselte Versandtasche und entnimmt das Pfefferminz.

Sie verwirft den nicht mehr benötigten WEISSEN Sessionkey und konsumiert im Kreise ihrer Freunde das Produkt des S .

MSGS 01

AN : Kerberos K
VON : Usula der Kundin

Hallo König Kerberos,
bitte stelle mir ein Ticket für den Pfefferminz-Server S aus. Der glaubt mir sonst nicht, dass ich auch zu unserem Reich gehöre und berechtigt bin das Pfefferminz zu bekommen.

Deine Usula die Kundin.

P.S.:
Da Du kein „Preauthentication“ verlangst, habe ich auch nicht das verschlüsselte Datum beigefügt.

MSGS 02 /BLAU

AN : Pfefferminz-Server S
VON : Kerberos K

Hallo Pfefferminz-Server S,
Da Du diese Nachricht mit unserem Geheimnis entschlüsseln konntest, weißt Du, dass sie vom mir kommt.
Es ist gerade _____ Uhr.
Falls die Kundin U (Usula) in den nächsten 20 Minuten etwas will, so darfst Du ihr gerne helfen.
Benutze den beiliegenden Key in dieser Zeit als gemeinsames Geheimnis mit U.

MFG Kerberos

MSGS 03 /ROT
AN : Kundin Usula (U)
VON : Kerberos K

Hallo Kundin Usula ,
Da Du diese Nachricht mit unserem Geheimnis entschlüsseln konntest, weißt Du, dass sie vom mir kommt.
Es ist gerade _____ Uhr.
Gegen Vorlage des beigefügten Tickets darfst Du in den nächsten 20 Minuten vom Pfefferminz-Server S bedient werden. Benutze beiliegenden Key in dieser Zeit als gemeinsames Geheimnis mit S. Ich warne Dich vor falschen Servern.

MFG Dein Kerberos

MSGS 04
AN : Kundin Usula (U)
VON : Kerberos K

Hallo Kundin Usula ,
anbei erhältst du

- Ein Ticket (oder Token) für S
- Einen dazu passenden Sessionkey (verschlüsselt in unserem gemeinsamen Geheimnis)

Beides ist ausschließlich zur Kommunikation mit dem S.
Das ganze ist 20 Minuten gültig.

Gruß Kerberos.

MSGS 05 /WEISS
AN : Pfefferminz-Server S
VON : Kundin Usula (U)

Herr Pfefferminz-Server S,
bei mir ist es jetzt gerade
1 331 974 827,045 UTC.
Da Sie diese Nachricht mit dem Sessionkey von unserem gemeinsamen bekannten K entschlüsseln konnten, wissen Sie nun, dass ich pfefferminzberechtigt bin. Beweisen auch sie mir Ihre Identität und senden Sie mir bitte verschlüsseltes Pfefferminz.

Danke, MfG. Kundin Usula (U)

MSGS 06
AN : Pfefferminz-Server S
VON : Kundin Usula (U)

Guten Tag Pfefferminz-Server S ,
anbei
> Ein Ticket (bzw. Token)
> Eine verschlüsselte Nachricht
(auch Authenticator genannt)

Freundlichst fordere Sie auf, mir
Ihre Identität zu beweisen.
Außerdem bitte Ich Sie, mir
umgehend Pfefferminz zu senden

Gruß Usula.

MSGS 07 /WEISS
AN : Kundin Usula (U)
VON : Pfefferminz-Server S

Liebe Kundin Usula,
dies ist die Antwort auf Ihr
verschlüsseltes Schreiben
von 1 331 974 827,045 UTC.
Ja, offenbar ist Kerberos, der
Wächter über unser Reich R, ein
gemeinsamer Freund.
Anbei ihr Pfefferminz separat
verschlüsselt.
Guten Appetit.

MfG Pfefferminz-Server

MSGS 08
AN : Kundin Usula (U)
VON : Pfefferminz-Server S

Liebe Kundin Usula,
anbei
> Eine verschlüsselte Nachricht
> Das verschlüsselte begehrte Gut.

MfG Pfefferminz-Server