

Wenn's mal wieder etwas länger dauert

Session Timeouts als Barriere für ältere Menschen

Meinem Sohn bin ich manchmal nicht schnell genug. Wenn ich dann nachfrage, bekomme ich schon mal zu hören: Ach, vergiss es! Mein Sohn ist 12. Ich bin 50 Jahre älter. Also eigentlich nicht richtig alt. Aber ich merke allmählich, dass einige meiner Fähigkeiten sachte entschwinden. Und als Mathematiker habe ich vor langer Zeit gelernt, was Extrapolieren bedeutet. Das kann ich noch ... Warum ich das hier erzähle? Nun, meine Studierenden fragen mich gelegentlich während der Vorlesung, warum ich dies oder jenes jetzt sage, zeige, mache. Zum Beispiel: genüsslich Jimi Hendrix nochmals gestatte, das Star-Spangled Banner zu zerfetzen. Woodstock 1969, einige erinnern sich vielleicht. Dann tue ich geheimnisvoll: „Sie werden schon sehen. Es hat alles mit dem heutigen Thema zu tun.“ Aber ich schweife ab. Bin eben ein Geschichtenerzähler ... Also, zurück zum Thema! Bitte Platz zu nehmen für:

Drei aufschlussreiche Experimente ...

... die ich früher unfreiwillig, sozusagen als Versuchskaninchen, wiederholt durchlaufen musste, bis ich endlich aus den Geschichten gelernt hatte. Und die ich hier jetzt kontrolliert, quasi in vitro, allen vorführen kann, die bereit sind zu lernen, bevor ihnen das Gleiche geschieht.

1. Meine Bank

Meiner Bank bin ich manchmal nicht schnell genug. Wenn ich mir nicht mehr sicher bin, ob ich eine bestimmte Rechnung schon bezahlt habe – bisweilen vergesse ich eben, eine gerade bezahlte Rechnung gleich korrekt abzulegen – sehe ich alle Buchungen der letzten Monate daraufhin durch. Das mache ich teilweise gleich online. Zum Beispiel, wenn ich noch nicht alle Kontoauszüge abgerufen habe. Oder wenn ich gerade keinen Zugriff auf meine Festplatte habe. Vielleicht ist das ungeschickt, aber ich bin mir recht sicher, dass andere das auch so machen. Die Umerziehung wirkt eben schon ein wenig – wir sollen ja gar keine Festplatte mehr haben, es ist ja jetzt alles in der Cloud.

Das Durchsehen der Kontenbewegungen dauert dann schon mal ein paar Minuten und erfordert außer dem Scrollen keine weiteren Aktionen. Der Server scheint nicht zu bemerken, dass ich am Problem arbeite, dass ich noch da bin. Also passiert das:

Sitzung abgelaufen

Sehr geehrte Kundin, sehr geehrter Kunde,

wir haben Ihre Banking-Sitzung aus Sicherheitsgründen beendet, da Sie das db Onlinebanking seit mehr als zehn Minuten nicht mehr benutzt haben.

Grundsätzlich sollten Sie das db Onlinebanking immer über den "Kunden-Logout" verlassen. Falls Sie das nicht tun, könnten sich Unbefugte, die Zugang zu Ihrem PC haben, Ihre Kontoinformationen über die History-Funktion Ihres Browsers anschauen. Transaktionen - zum Beispiel Überweisungen - sind aber nicht möglich, da dafür eine zusätzliche Legitimation per TAN erforderlich ist.

Dennoch sollten Sie Ihre Sitzung zu Ihrer eigenen Sicherheit ordnungsgemäß über den "Kunden-Logout" beenden.

Was möchten Sie als nächstes tun?

Ich will ...

Ah, „aus Sicherheitsgründen“, lese ich. Das gefällt mir. Die Bank ist besorgt um mein Wohl. Nein, nein, das ist jetzt nicht abfällig gemeint. Es ist zwar eine vielgehasste Bank, aber die einzige, die immer bereit war, mir bei der Erfüllung meiner Träume zu helfen. Nicht so wie die Banken, über die Mark Twain spottete. Meine Bank will also sichergehen, dass niemand an mein Konto kommt, falls ich vergesse, mich auszuloggen. Und dagegen ist prinzipiell ja auch nichts einzuwenden. Aber die Bank hätte ja mal fragen können, ob ich noch da bin, statt mir einfach die Tür vor der Nase zuzuschlagen. – Liebe Software-Industrie, guten Morgen! Könnte sich mal eben jemand um diesen Vorschlag kümmern?

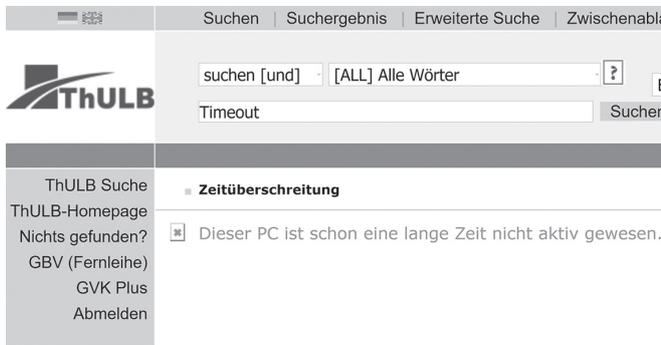
Um die nun leider doch als erforderlich erkannte Überweisung durchzuführen, muss ich wieder in mein Konto. Ich benutze also die Situation gleich für eine kleine Sicherheitsüberprüfung. Was wird passieren, wenn ich mich nicht brav wieder anmelde, sondern den *Back Button* betätige? Bin ich dann wieder drin? So leicht macht es mir das System aber nicht, zumindest in diesem Aspekt scheint es wirklich sicher zu sein. Wiedereinloggen ist also angesagt, etwas lästig, aber nicht wirklich schlimm.

Schon etwas vertrackter ist eine andere Situation, die ich nicht so ohne Weiteres demonstrieren kann, deren Opfer ich aber wiederholt geworden bin: Zur Freigabe einer Überweisung (oder einiger anderer Aktionen im Konto) muss eine Autorisierung mit Authentifizierung durch Eingabe einer TAN erfolgen. Wird die Sitzung nun kurz nach Einleitung der Autorisierung durch einen Timeout geschlossen, ist nicht unmittelbar erkennbar, ob die Autorisierung noch korrekt abgeschlossen wurde. Nach dem Wiedereinloggen ist weder ein Fehler- oder Statusbericht abrufbar noch lässt sich vor dem nächsten Buchungstag feststellen, ob die Buchung übermittelt wurde. Ich finde das beunruhigend. Und wenn mir das schon so geht, wie werden sich dann erst andere fühlen, die weniger technikaffin und leichter zu verunsichern sind?

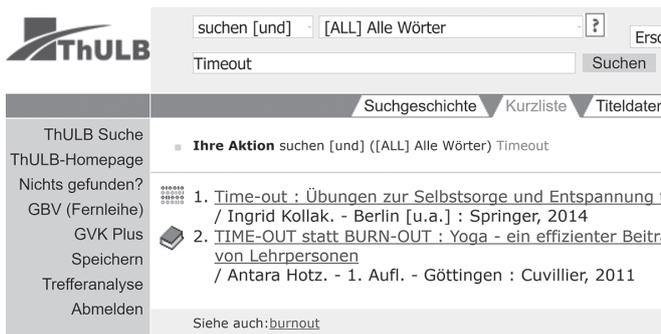
Lektion gelernt: Timeouts können der Sicherheit dienlich sein, auch wenn sie manchmal nerven. Wäre das System aber wirklich „intelligent“, würde es erkennen, ob ich es noch benutze. Bekommen wir das in den nächsten 10, 20 Jahren hin? Oder ist Ihre Majestät K. I. dieses Problem vielleicht zu banal?

2. Meine Bibliothek

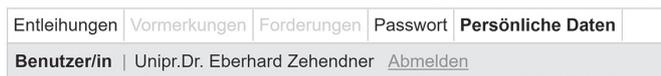
Mehr Freude als mein Konto zu durchwühlen macht mir das Stöbern in der Universitätsbibliothek. Elektronisch natürlich, das geht selbst von zuhause aus. Aber auch meiner Bibliothek bin ich wohl häufig nicht schnell genug. Zu häufig, wie ich finde. Und dann – das kennen wir ja schon – passiert es natürlich wieder, heißt es trocken: Ach, vergiss es!



Wie dramatisch das klingt: „eine lange Zeit nicht aktiv“. Das schreit nach Sicherheitsabschaltung. Oder lag es daran, dass ich nach dem Begriff „Timeout“ gesucht hatte? Schnell den Back Button gedrückt – et voilà! – alles ist wieder da. Keine Sicherheit!



Ich spiele ein wenig mit dem System herum. Kann ich Seiten aus der Such-Historie ansehen? Ich kann. Kann ich Bestellungen tätigen? Ja, falls ich das in der Session schon einmal getan habe. Komme ich an die Benutzerdaten heran? Ja, siehe unten.



Sicherheitstechnisch eine Katastrophe! Der Rollback klappt nicht immer, hat aber schon wiederholt funktioniert. Anscheinend gibt es noch einen zweiten Timeout, der zur Fehlermeldung „Die bisherigen Ergebnisse sind nicht mehr verfügbar“ führt. Dann geht auch der Login nicht mehr.

Warum also der ganze Zauber, wenn es doch keine Sicherheit bringt? Systemressourcen freigeben, scheint hier das Mantra

zu lauten. Aha. So mager sind also die professionellen Systeme ausgelegt, dass sie uns den Spaß verderben müssen, um nicht selbst unter der Last von zwischengespeicherten Suchanfragen und -ergebnissen zusammenzubrechen. Wie wäre es damit: Jeder Client speichert die von ihm veranlassten Zwischenergebnisse selbst. Möchte jemand diese Idee haben?

3. Mein Hotel

Es folgt der Tragödie dritter Teil. Asche auf mein Haupt, ich habe eingangs ein wenig übertrieben. Keine Screenshots! Die hätte ich machen sollen, als ich vor Ort war, jetzt ist es zu spät.

In einem großen Frankfurter Hotel (4 Sterne, ich war eingeladen) hatte ich kürzlich folgendes bizarre Erlebnis: Das Hotel bietet seinen Gästen unter anderem kostenlosen WLAN-Zugang ins Internet. Ich bräuchte keine Zugangsdaten, wurde mir an der Rezeption mitgeteilt, lediglich meine Zustimmung wäre nötig. Was dann auch so war: Zustimmung zu den AGB und – natürlich – Kenntnisnahme der Datenschutzbestimmungen. Da ich etwas Zeit hatte, las ich mir die Datenschutzbestimmungen genau durch. Sie waren ordentlich formuliert, einleuchtend und nicht länger als zu erwarten war. Zum Lesen benötigte ich vielleicht fünf Minuten. Im Studieren von Datenschutzerklärungen gut Geübte mögen das vielleicht in noch kürzerer Zeit bewältigen. Auf etliche Gäste dieses Hotels dürfte das aber schwerlich zutreffen. Ich nehme an, ich liege da eher im Mittelfeld. Auch, was die allgemeine Geschwindigkeit der Informationsverarbeitung angeht.

Zurück auf der Login-Seite setze ich nun (vollständig beruhigt) mein Häkchen, wollte mich zum Internet durchklicken – und musste erfahren: meine Sitzung sei mittlerweile abgelaufen. Was denn, ein Login-Prozess mit Timeout, der so knapp gehalten ist, dass ich in dieser Zeitspanne nicht einmal durchlesen kann, wozu ich meine Zustimmung geben soll? Ein Sicherheitsfeature? Wohl kaum. Ressourcenmangel? Ja, wahrscheinlich: ein Mangel an mitdenkenden Programmiererinnen und Programmierern im Herstellerunternehmen.

Es drängen sich Fragen auf

Nehmen wir einmal an, dass die Software-Unternehmen solchen Unsinn nicht absichtlich in die weite Welt schicken. Dass sie es vielleicht einfach nicht besser wissen. Dann sollten sie kompetent beraten werden.

Mich interessiert nun zunächst, nach welchen Kriterien Software-Unternehmen Timeouts in ihre Produkte einbauen und wie die jeweiligen Zeitschranken dimensioniert werden. Bestehen diesbezüglich Vorgaben von Auftraggeberseite? Gibt es Vorschriften, Leitfäden, Best Practice? Ist Barrierefreiheit überhaupt ein Thema?

Und mit Barrierefreiheit meine ich nicht nur Vorschriften, die sich auf Menschen mit einer amtlich festgestellten Behinderung beziehen. Hier kommt die Gruppe der Älteren ins Spiel, die in vollem Umfang teilhaben wollen, und auch sollen, an den Errungenschaften der Informatik. Graduelle Einschränkungen im

physischen wie auch im kognitiven Bereich verstärken sich dort negativ hinsichtlich der Einhaltung von Zeitschranken, die für alle gleich ausgelegt sind. Zu untersuchen wären also implizite wie explizite Mechanismen der Dynamisierung von Timeouts, um diese den aktuellen Fähigkeiten der von ihnen betroffenen Menschen anpassen zu können.

Von Seiten der Literatur habe ich dies bereits sondieren lassen, da scheint es nicht viel und wenig Konkretes zu geben. Derzeit bereitet einer meiner Bachelorstudierenden im Rahmen seiner Abschlussarbeit eine Befragung in Software-Unternehmen vor, überwiegend aus der Stadt Jena, in der es zahlreiche einschlägige Firmen gibt, die sich häufig auch für Sicherheitsaspekte interessieren. Wir werden sehen, ob es dort hinsichtlich praktischer Aspekte so etwas wie eine gemeinsame Linie gibt, auf die sich aufbauen ließe.

Völlig ungeklärt scheint mir auch, wie viel Sicherheit die verwendeten Timeout-Mechanismen denn nun wirklich bringen. Lässt sich das messen oder zumindest modellhaft quantitativ beschreiben? Und falls eine Veränderung der Timeout-Mechanismen mit dem Ziel einer besseren Benutzbarkeit durch ältere Menschen nur unter Verzicht auf einen gewissen Grad an Sicherheit mög-

lich wäre: gäbe es dann andere Mechanismen, die den Sicherheitsgrad wieder auf das gewünschte Niveau anheben würden?

Viele offene Fragen – aber mein Titel hatte ja auch keine Antworten versprochen. Ich denke, wir stehen noch ganz am Anfang, und die Zeit drängt, da brauche ich nur an § 12a (Barrierefreie Informationstechnik) im Behindertengleichstellungsgesetz zu denken.

Noch Klärungsbedarf? Ach so, Jimi Hendrix und das Star-Spangled Banner. Nun, der Bezug in der betreffenden Vorlesung war die unmittelbar vorausgehende Verkündung der neuen TOP-500-Liste für Supercomputer. Diese wurde angeführt von „Summit“ am Oak Ridge National Laboratory. Also wieder einmal: America First! Und wer die Geschichte der Kernwaffen kennt, weiß sicher, was es mit dem ORNL auf sich hat. Da ist Wachsamkeit geboten.

Eberhard Zehendner lehrt und forscht seit 1994 an der Friedrich-Schiller-Universität Jena u. a. im Bereich Informatik & Gesellschaft. Biografie auf Seite 26.



*Ob alt, ob jung!
Technik wird akzeptiert,
wenn sie erkennbare Vorteile
bietet und einfach zu
erlernen und zu bedienen ist.*

