Digital ESSAY

「2つで十分ですよ」

坂口 裕靖

今文字種がk通りあるとして、n文字からなるパスワードを作る組み合わせの数を考えると、単純にk^n通りということになります。なので、ランダムなn文字がパスワードにヒットする確率は1/（k^n）ぐらいでしょう。m回の試行が可能なら、m/（k^n）ですね。具体的に数字4桁、1回試行だとk=10、n=4、m=1なので1/10,000となります。3回試行できるなら1/3,333ぐらいですね。パスワードを突破されないためには、試行回数に制限を掛ける必要性が高いことがわかります。まあそれでもネットワークを前提とした場合、同時にk^n個の端末から1回試行されたら終わりなわけですから、回数制限の実装は割と非現実的、もしくは非実用的だったりします。なので、kとかnとかを十分大きくして、mが無制限だとしてもヒットするまでに十分長い試行を必要とするように構成することが一般的です。大文字小文字だの記号だの言われているのはこの関係ですね。これに対して銀行のATMの場合は物理カードが1枚しかないため、一回の攻撃可能な端末は1台しかないため、この多重分散攻撃を気にする必要がなく、回数制限が成り立っているわけです。まあ、物理カードをコピーされてしまうならこの限りではないわけですが、なのでICチップタイプへの切り替えが進んでいると言えます。

さて、ここでパスワードの文字列を倍（すなわち2n文字）にすることと、2つの異なるパスワードを2回に分けて入力することを比較してみましょう。前者はnを2nにすればよいので、m/（k^2n）となります。数字8桁、3回試行だと3/100,000,000=1/33,333,333ぐらいでしょうか。後者については最初のパスワードがk^n通り、2番めのパスワードがk^n-1通りあるので、まあだいたいm/（k^n・（k^n-1））＝m/（k^2n-k^n）ぐらいとなります。数字4桁2つ、3回試行なら1/33,330,000ぐらいでしょうか。要するにオーダーとしてはパスワードの桁数を増やしたのと同程度の効果があることになります。物理計算とかだと二乗より高次の項を無視したりするのと同じで、RAIDとかと同様リスクを桁の単位で低下させることができるわけです。

こうした考え方が多段階認証の根っこにあるわけですが、二段目以降については別にパスワードである必要はありません。よくあるのが機材を持っていることを確認するような手順で、例えばケータイやスマホにSMSで数桁の番号を送信し、その値を入力させるというものです。送信したランダムな数字がきちんと入力されることで、当該通信機器にアクセスしてSMSを確認できる状態にあると想定し、本人であることを確認するわけです。この二段目の認証に対して同時k^nアクセスで突破しようとする場合、実際にはまず第一段のid/passチェックを通過しなければならないため、少なくとも前段で設定された正しいトークンと共に番号を返す必要があります。仮にシステムが同時に複数箇所からログインできるようになっていたとしても、このトー

One Point BUZZ WORD

1371人

某ニュースにて、「半数の1371人は、全体の中央値を下回っていて」という表現が流れたようです。脊髄反射的には当たり前…ですが、まあ真面目に考えてみましょう。

そもそも中央値とは、値の低い順にn個並べていったとき、n/2番目の値のことを言います。nが奇数、例えば2k+1だった場合、下からk+1番目の値が中央値です。下にk個、上にk個あるわけですね。一方nが偶数、たとえば2kだった場合、k番目とk+1番目の平均を取るようです。ちょうど真ん中のサンプルがないからですね。

さて、全体の半数が「中央値を下回る」状況を考えてみましょう。この報道ではnが2,744人で偶数、中央値を下回ったのが1,371人だったようです。2,744/2=1372ですから、中央値は1372番目と1373番目の平均値だったことになります。可能性としてあり得るのは（1）中央値が1372番目と一緒（2）中央値が1372番目より大きい、のいずれかでしょう。仮に（2）だとすると、「中央値を下回る」のは1372人でなければいけません。一方、実数は1371人だったため、（2）ではないことがわかります。すなわち、1372番目と1373番目は同じ値であり、かつ1371番目より大きいことがわかります。つまり、この報道は「中央値付近の3サンプルでは1371番目より1372番目が大きく、1373番目は1372番目と同じ値」である、という厳然たる事実をやわらかく伝えてくれているわけです。下回っていたのが1372人であれば、1373番目のサンプルは中央値より0.5以上大きいはずです。また、仮に1372番目と同じ値が何個も続いていたとしたら、「中央値以下」だったサンプル数は1372を上回っていたはずです。それではなぜこのような表現をしたのでしょうか。おそらくはこの値、「1371」の読み方に掛かってるんじゃないですかね。イミ…おや、誰か来たようだ

クン発行枚数は原理的に管理可能であり、k^n 攻撃をしようとしているかどうかは機械的に検出可能でしょう。３箇所から同時ぐらいならまあ、おそらく同一人が複数端末からアクセスしようとしているのでしょうけど、これが 1,000 とか 10,000 とかになると急速にアヤシくなってくるので、認証を拒否することができるかもしれません。

とはいえ、二段階認証は結構面倒なため、多くのサービスでは「端末認証」的な緩和策が取られている場合が多いようです。具体的には二段階認証に成功した場合、その端末は確認ずみであると解釈し、適当な有効期限を持ったクッキーを保存しておくというものです。次回認証時に期限が有効なクッキーがあれば、二段階目を省略できるようになってます。仮にこのブラウザを第三者が使ったとしても、そもそも一段回目の認証を突破できない（はず）なので、一段目を突破できた以上、そのブラウザを信頼してもよかろうというわけです。頻繁にアクセスするならこの恩恵があるわけですが、四半期に一度ぐらいしかアクセスしない場合、毎回２段階認証が必要になったりするわけではあります。

さて先日、社用携帯の切り替えがありました。業者さんの方でキッティングして出荷して頂いてるパターンなので、番号の引き継ぎもなく切り替えることになりました。まあ今まで使ってたスマホはあまり電話としては使っていなかったため、番号が変わってもさほど困ることはありません。というわけで、古いスマホから必要なデータだけ移行して、さっさと完全にリセットし、梱包して箱に入れ、あとは発送するだけだったのでした。

で、その状況で飛び込んできたのが、解約し忘れなサーバに設定していたコーポレートカードが無効で、未払いの請求が来てる、という情報です。今はなき部署で契約したものですが、当時の部署で保持していたコーポレートカードは特区の昔に解約されていたようで、たまたま年払い（にすると安くなるところ）だったので、発見が遅れた形だったのでした。

しかたないなー、と管理画面からアクセスしようとしたのですが、よく考えたら二段階認証にしてたのでした。そして、二段階認証に使う端末として設定してたのが、つい先程リセットして綺麗サッパリすべての情報を消去して梱包したスマホだったのです。

いやー焦った焦った。気がついたときさーっと血の気が引きました。

用意されていた二段階認証の手段は、認証アプリ、SMS、電話で連絡の３通りでした。このうち認証アプリについては、二段階認証で使うように設定していなかったため、今更どうにもなりません。SMS については、ついさっきフルリセットしたデータを入れ直さないと使えるようになりません。電話について確認しましたが、登録されている電話番号は会社の番号と、ついさっきフルリセットしたスマホの２つだけでした。深夜のリモートワーク中なので、受けてくれる人もおらず、会社の電話は使えません。スマホはガムテでがんじがらめになった箱の中です。別の電話番号に連絡させようと思うと、管理画面から変更する必要があります。で、管理画面に入るためには、二段階認証を突破できなければなりません。詰んだ、と思いました。

でも落ち着いて考えてみたところ、SMS を受信するには再設定が必要だとしても、電話を受けるだけなら初期状態でもなんとかなりそうです。しかたないので、せっかく作った梱包を開けてスマホを取り出し、しかも電池がほとんどなかったので起動する程度まで充電し、電源をいれて可能な限り「あとで設定する」を選択し、最短時間で電話を受けられる状態まで持っていきます。試しに手元の別のスマホから当該番号に電話すると、きちんと呼び出し音がなりました。リセットするまえに回線を解約しなくて本当に良かった！

これで電話では受けられるようになったので、あらためて二段階認証の方法を電話認証に変更し、無事二段階認証を突破できたのでした。二段階認証を秒でキャンセルしたのは言うまでもありません。アブねぇアブねぇ。

こういうことがあるため、二段階認証を設定する場合、連絡手段は可能な限り広くしておかないと危なくていけませんな。今回も複数個登録してはいたのですが、残念ながらコロナと端末変更という二乗の項が無視できない状態だったのをギリで回避できたところです。というわけで頑張って４つは登録しときましょうね、本当に ...

Hiroyasu Sakaguchi
株式会社 IMAGICA Lab.