How do you Solve a Problem like Authentication?

Karen Renaud & Joe Maguire

Abstract

The security aspect that the computer user encounters most often is the password prompt - a demand that they verify their identity by providing a shared secret. Authentication, for the deployer, regulates access and enforces accountability. Authentication, for the user, obstructs, intrudes and delays gratification. Whereas users could probably put up with this if it happens relatively infrequently, this tends not to be the case. An authentication prompt is presented a number of times during the day. Sometimes it has serious consequences, such as when it is required to authorise the purchase of a digital item, and the permits consequent credit card charge. Other times it merely identifies the user to allow the system to customise the interface. The range of consequences and the multiplicity of systems mandating shared secrets collide with human limitations and the current password bloat and general end-user exasperation.

Is it at all possible to improve authentication? As researchers, we have primarily addressed this problem in one of three ways: (1) by trying to find a password replacement, (2) by formulating rules and regulations to coerce users into choosing stronger passwords, or (3) fostering a security culture within the organisation, hoping that the social pressure will induce people to behave more securely. These endeavours have met with limited success. Alternatives have not been embraced by the developer community, rules and regulations are often ignored, subverted or deliberately flouted. Fostering a security culture has had more success, in relative terms, but still has not really addressed the "authentication problem". The one thing these approaches have in common is their focus on the human agent: the end user.

Consider a related problem in the physical world: locks on doors. These have not changed in centuries and the doors themselves are probably weaker than they were a hundred years ago. Yet do locks really prevent intrusion? A determined intruder finds the average lock an minor deterrent, and the door itself is sometimes even made of glass, allowing the thief to subvert the lock entirely. Yet one never hears about a desperate search for a door or lock replacement. One doesn't hear the refrain, '*How do you solve a problem like the door lock?* This even though they, too, are lost, copied and shared. Why, when it comes to virtual locks, is there such a drive to come up with the *perfect* locking mechanism? The password and the average door lock function similarly: neither is perfect but both provide an acceptable measure of security. Here we will argue that it might be time to suspend our unrealistic expectations that we can find a perfect lock in the virtual world when we live quite happily with imperfect security in the physical world.

Introduction

Most security research efforts focus on the human, with the commonly accepted maxim that the human is the weakest link in any security solution. Humans most often encounter security when they are required to authenticate, and this usually by confirming that they know a shared secret. This worked well when users were primarily trained computer experts. When computers became ubiquitous, and users more diverse in terms of abilities and knowledge, it quickly became clear that users did not take security nearly as seriously as those who designed the systems thought they ought to. When such users were employees, employers tried to ameliorate the situation with mandated policies. When users are customers it becomes far more difficult. IT desks were, and still are, plagued by requests for password replacements and the need to institute procedures to help people to recover from intrusions into their accounts. Some organisations, realising that policies have limited effectiveness, have attempted to grow a security culture within the organisation, and this has had some measure of success.

Researchers, identifying this problem as worthy of attention, have often focused on replacing the mechanism. They reason that users behave insecurely because the password itself is so flawed and a replacement, which is obviously superior, will help to ameliorate the problem. The research community were puzzled for some time that their offerings of superior mechanisms were not embraced by industry. Whereas researchers focused on a password replacement, organisations focused on the users, on trying to make them behave more securely.

These strategies are not proving as effective as hoped. Moreover the three prongs are a legacy approach, and do not accommodate an emerging world with new trends. For example, some trends that are particularly relevant are the "*bring your own device*" movement, the way people now work on the move, in a variety of environments, and the fact that the Internet now allows people from a variety of cultures and persuasions to mount attacks. The user-centred approach was designed to deal with threats *within* the organisation. Employees, for example, are instructed not to write their passwords down. This is clearly to prevent colleagues from getting hold of the password. An attacker from the other side of the world, via an Internet connection, has no way of getting hold of the written record, the admonition does not protect against their increasingly sophisticated attacks.

The common 30-day forced password change requirement also has its roots way back when the password-cracking process was very time-consuming. The forced change is a defence against leaked or hacked password being used for unlimited periods. Intuitively this is a good solution, but in practice it is counter-productive. Computer users, when forced to change passwords, will tend to gravitate towards easier passwords, to offset the unpleasantness and consequences of a forgotten password. Whereas this requirement is meant to make systems more secure it ends up making them easier to breach.

Twitter Hacked

In February 2013 Twitter was hacked and a number of accounts breached (BBC News,2012). Twitter responded by locking down compromised accounts and sending out emails to affected users. The hackers then also sent out (phishing) emails to harvest the new passwords. People were expecting these emails and believed them to be from Twitter so were taken in by the Phish.

What was interesting about this exploit was that the BBC report allowed people to respond to the article. The comments provide an interesting insight into some viewpoints on the reasons for this kind of breach.

We analysed the user comments on the BBC website. The first very strong theme that emerged was that this was a non-story, what one responder called "*a calm in a teacup*". Some commenters derided the BBC for making a story out of this when there were much bigger issues to be concerned about.

> "Who cares? Meanwhile while we talk about trivia, David Cameron and George Osborne steal tax payers money making millions live below the poverty line. Oh, but let's talk about 250,000 people who will have to reset their passwords."
> **Comment**

Here is another comment on the same theme:

> "Another NON story on the BBC HYS forums.

> Must be a slow news day”
> **Comment 172**

Another strong theme was that people ought not to use sites like Facebook and Twitter, and if they did it was their own fault if their accounts were hacked.

> “I knew there was a good reason I don't use so called social networks!...I find it strange that most of the people shouting about this deliberately put mountains of personal stuff out for the world to see anyway & most never or rarely change their passwords! It's a fact that if only a little info is known about most individuals then their passwords are fairly easy to suss by a pro hacker anyway!”
> **Comment 64**

Indeed, another comment suggests that users simply deserve such attacks as both websites are essentially time-wasting tools:

> “Twitter (& facebook) is used by twits so it does not suprise me that it is insecure. It is not just kids but kidults in there 20s, 30s and older trying to appear on-message and part of the crowd. Most of the info is just opinion and the childish activities of last night like where I got as pissed as I did. Why in a recession so much time, money and resource wasted on these purile activities?”
> **Comment 56**

Many felt that such sites were worthless, allowing people to draw attention to their boring lives and encouraging inane outpourings that other people were not interested in.

> “OMG this is soooo serious. I've tweeted about the relative merits of different coffee beans and someone and has changed my ratings - I'm distraught!!”
> **Comment 74**

Some sounded a warning, advising people to use fake information when using this kind of website. There was an unwritten sense of blame - people got what they deserved if they had accounts on this kind of website.

> Just serves as a reminder to everyone never to use or give real information, let alone the same password across accounts on line. Never use the likes of Twitter or Facebook
> **Comment 38**

A small number pointed out that, unlike many other sites, Twitter was unregulated and therefore performed an important function in allowing people to post news that some governments would prefer to suppress. They argued the value of Twitter as a tool which enabled democracy.

> “If people are 'down' on Twitter they don't want the truth and the real news to come out as you won't get it in the media generally FREE SPEECH should be protected and celebrated.”
> **Comment 140**

There were those who pointed the finger of blame away from the users. A small group wondered why Twitter had not secured the details properly so that they could not be stolen. They argued that the web tends not to be secure, and that those who hack sites often have more time, resources and skills than those who are paid to secure sites. Hence anything put online these days is bound to be revealed sooner or later. The other, larger, group wondered who was behind the hack. Many blamed China but others took exception to this unfounded conclusion and demanded evidence which, of course, no one has.

> "It's time that countries like China, India, Nigeria were told to get their houses in order or be disconnected from the civilized world's communication systems. I am sick of moronic Indian crooks phoning me trying to get me to cripple my computer and half-witted Nigerians telling me I'm due to inherit millions. Cut them all off, they have NOTHING I want to hear, watch or read!"
> **Comment 44**

Indeed, many more suggest a trade or communication block was favourable, as other cultures simply do not know how to play fairly in a shrinking world:

> "They know which countries these hackers continually operate from...why not just block internet access to these countries until the authorities in those countries get off their a***s and do something about it."
> **Comment 9**

Yet another comment suggested that punishment in form of trade blocks should be used to deal with problem of Twitter being compromised.

> "China blatantly ignores any Western laws, rules or etiquette. They just do whatever the hell they want. They think they're too big, and that they have too much of what we want for us to make a fuss.
> We should pull out our trade links until they learn to play by the rules."
> **Comment 68**

The abiding theme across many of the comments was to point the finger of blame. Perhaps the "nanny state" really has impacted on our psyche to such an extent that we childishly want things to be perfect and if they aren't we want the guilty party to be identified so that punishment can be meted out. That this is impossible in the global world of the Internet has not yet penetrated the populace's mindset.

What was very interesting was that many of the core ideas in password policies have been assimilated by the general population. This is, of course, good advice but impossible to follow. There were also a number who argued that people should use stronger passwords. There were a number of admonitions for people not to reuse passwords on multiple websites:

> "People who use the same password for everything are screwed. That's why you should have at least 4 levels of password, and change them every so often -
>
> 1. financial accounts
> 2. email accounts
> 3. merchant accounts
> 4. everything else (like Twitter)"
>
> **Comment 5**

> "Just another reason to use different passwords for all services and do backup on regular bases :)"
> **Comment 190**

The reality is that users are not necessarily ignorant of policy, culture or mechanism. Users are savvy, as the user below suggests.

> “To those who say what are people going to do with emails and passwords? Well think it about it clever clogs.
>
> A lot people use the same passwords for everything! so with those stolen twitter emails and passwords they could login to facebook and even paypal etc!”
>
> **Comment 45**

Unfortunately, there still seems to be a silver bullet mentality to the authentication problem: *if only passwords were stronger*. *If only* we did not reuse them. *If only* we could remember them. Unfortunately, there is no silver bullet that will solve the virtual locking problem. However, organisations, researchers and journalists still peddle the idea the password can be made perfect with very little effort. The BBC’s technology correspondent, for example, in writing about the hack, concludes his piece with the following statement: “*That means passwords like “password” and “123456” just won’t do any more*”.

This attempt to drive people to choose stronger passwords, as a defence, is misguided and doomed. The Twitter hack obtained a database containing email addresses and encrypted passwords. It is trivial to break these passwords using brute force techniques, and computing power is so cheap and plentiful that they can be brute forced by hundreds of machines in parallel. A password such as “T3i%%er” will not take much longer to break than “123456”. Yet the stronger password will take the user much longer to type in, and cost them extra effort every time they use the website. For all this extra effort they are unlikely to get a great deal more protection.

One commenter makes a related comment: “*There is a fortune waiting for the person who comes up with an alternative to passwords*”. We have news for this commenter. The research community has been trying for years to do this, with very little success. This is probably because we have focused far too myopically on the mechanism itself, and on the end-user, and not taken the bigger view. The main question we need to answer is “what the essence of the authentication problem?”. In essence, it is not merely related to the memorability and guessability of the password itself.

The Password and the Door Lock

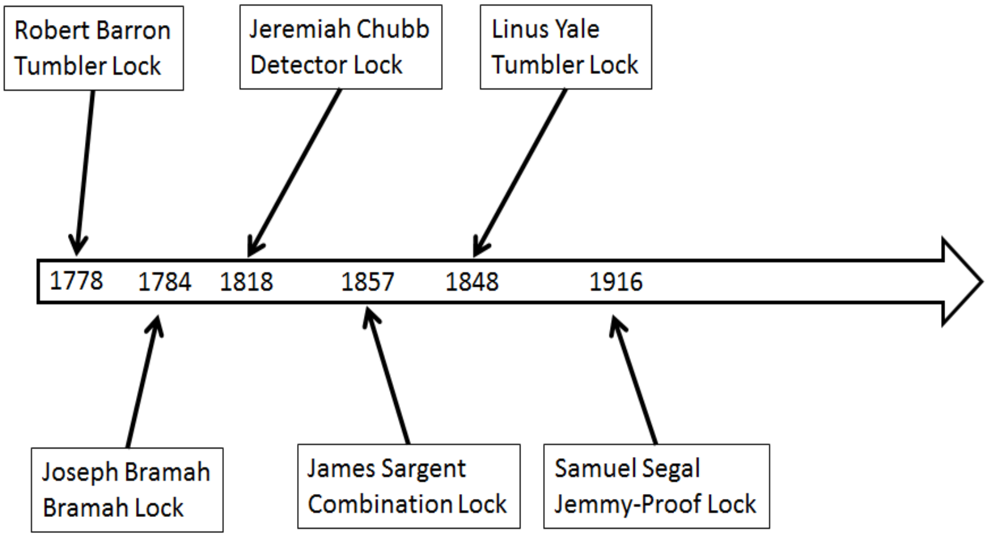


Figure 1: Lock Invention Timeline

Figure 1 depicts the progress of the most commonly used door locks. Most locks in use today are based on the inventions of Bramah, Yale and Sargent. It is interesting to note that no significant changes have been made to domestic locks since the early 20th century.

When it became necessary to implement a “lock” in a virtual world, the obvious choice was to use a secret. The password, being a well known metaphor, now seems the obvious choice. Indeed, there are many similarities between the physical door key and the password.

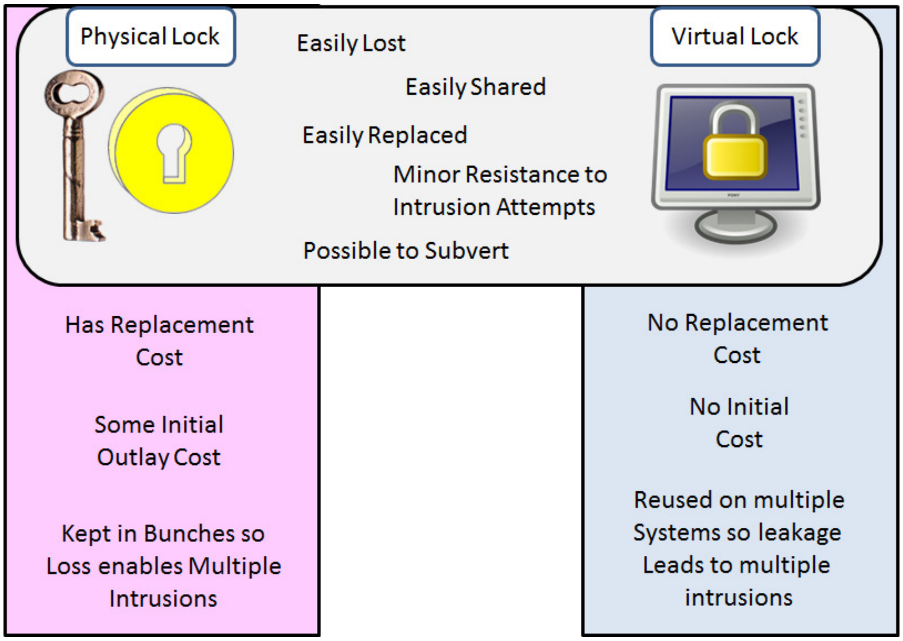
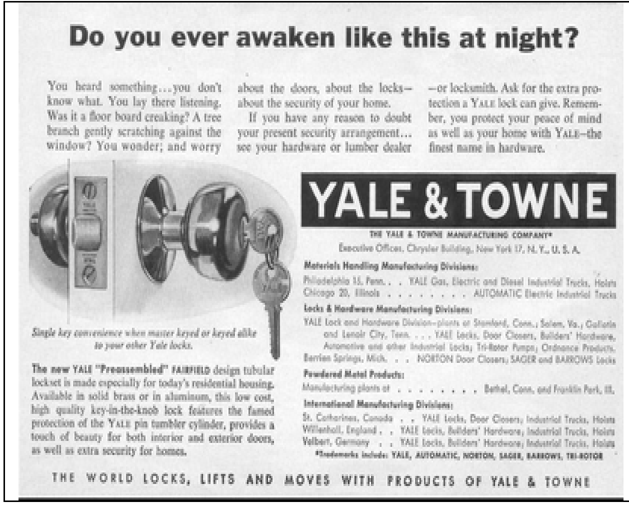


Figure 2: Locks, Physical and Electronic

We accept the fact that the locks on our houses are not perfect. The fact that they probably constitute enough of a deterrent to the casual thief appears to be sufficient. A determined intruder will not be deterred by the lock and we implicitly accept this. There is no widespread call for a perfect door lock replacement. When someone experiences a burglary they will probably replace their locks, but there is no suggestion that they will try to make the new lock unbreakable. They usually replace like with like but they might add another safeguard such as a house alarm. Yet when a digital lock is breached there are demands for a better mechanism. We want something more secure, something impermeable. Are we being unrealistic? Is there really a need for a password replacement?



Do you ever awaken like this at night?

You heard something…you don't know what. You lay there listening. Was it a floor board creaking? A tree branch gently scratching against the window? You wonder; and worry about the doors, about the locks—about the security of your home.

If you have any reason to doubt your present security arrangement… see your hardware or lumber dealer—or locksmith. Ask for the extra protection a YALE lock can give. Remember, you protect your peace of mind as well as your home with YALE—the finest name in hardware.

Single key convenience when master keyed or keyed alike to your other Yale locks.

The new YALE "Preassembled" FAIRFIELD design tubular lockset is made especially for today's residential housing. Available in solid brass or in aluminum, this low cost, high quality key-in-the-knob lock features the famed protection of the YALE pin tumbler cylinder, provides a touch of beauty for both interior and exterior doors, as well as extra security for homes.

YALE & TOWNE

THE YALE & TOWNE MANUFACTURING COMPANY*
Executive Offices, Chrysler Building, New York 17, N. Y., U. S. A.

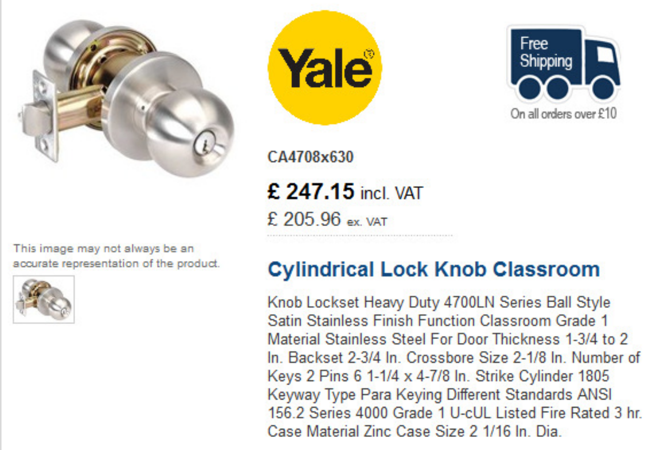
Materials Handling Manufacturing Divisions:
Philadelphia 15, Penn. . . YALE Gas, Electric and Diesel Industrial Trucks, Hoists
Chicago 20, Illinois . . . . AUTOMATIC Electric Industrial Trucks

Locks & Hardware Manufacturing Divisions:
YALE Lock and Hardware Division—plants at Stamford, Conn.; Salem, Va.; Gallatin and Lenoir City, Tenn. . . . YALE Locks, Door Closers, Builders' Hardware, Automotive and other Industrial Locks; Tri-Rotor Pumps; Ordnance Products.
Berrien Springs, Mich. . . . NORTON Door Closers; SAGER and BARROWS Locks

Powdered Metal Products:
Manufacturing plants at . . . . Bethel, Conn. and Franklin Park, Ill.

International Manufacturing Divisions:
St. Catharines, Canada . . YALE Locks, Door Closers; Industrial Trucks, Hoists
Willenhall, England . . YALE Locks, Builders' Hardware; Industrial Trucks, Hoists
Velbert, Germany . . YALE Locks, Builders' Hardware; Industrial Trucks, Hoists
*Trademarks include: YALE, AUTOMATIC, NORTON, SAGER, BARROWS, TRI-ROTOR

THE WORLD LOCKS, LIFTS AND MOVES WITH PRODUCTS OF YALE & TOWNE



This image may not always be an accurate representation of the product.

CA4708x630

£ 247.15 incl. VAT
£ 205.96 ex. VAT

Cylindrical Lock Knob Classroom

Knob Lockset Heavy Duty 4700LN Series Ball Style Satin Stainless Finish Function Classroom Grade 1 Material Stainless Steel For Door Thickness 1-3/4 to 2 In. Backset 2-3/4 In. Crossbore Size 2-1/8 In. Number of Keys 2 Pins 6 1-1/4 x 4-7/8 In. Strike Cylinder 1805 Keyway Type Para Keying Different Standards ANSI 156.2 Series 4000 Grade 1 U-cUL Listed Fire Rated 3 hr. Case Material Zinc Case Size 2 1/16 In. Dia.

http://gogd.tjs-labs.com/show-picture?id=1064246191&size=FULL (advert from 1953)	http://www.tizaro.com/ (2013)

It is perhaps time for us to refrain from focusing on the end-user. We keep urging them to use strong passwords, and the associated cost is significant and cumulative. Yet this practice does not protect them nearly as much as we promise. The sophistication of recent hacking attacks, combined with the availability of resources with which to carry out these attacks, means that such effort is essentially almost futile.

No one blames a householder when they experience a burglary. We might shake our heads and tut about the wickedness of the world, but our overriding emotion is one of gratitude that we have escaped this time. One also does not hear calls for stronger doors, and better locks. We accept this risk ruefully. Perhaps due to the relative newness of the virtual world we have not yet realised that it mirrors our physical world in many ways. We have time-honoured ways of dealing with risk in the physical world, so we should deploy the same techniques in the virtual world. The ease with which new solutions can be deployed in the virtual world should not fool us into thinking that new social rules can be made. The human in the loop has not changed.

One commenter displays this insight too:

> "You would have thought that the internet would have brought people freedom, all it has given in reality is government control and terrorist attacks.
> Just like the real world then."
> **Comment 200**

Conclusion

The password, like its physical equivalent, does not offer full and total protection. It acts as a deterrent to repel the casual intruder. The determined intruder will find a way in, in both the physical and virtual worlds. In the physical world we deal with this by purchasing insurance to mitigate the risk or by adding additional safeguards. The price is determined by the insurance company risk assessors. Perhaps, instead of looking for a password replacement, we should be mirroring the risk mitigation strategies of the physical world, and start managing the risk in the age old way: accept it, prevent it (by not using online banking, for example), or by mitigate it (by insuring or adding extra layers of security). Funnily enough, these techniques are suggested by those who commented on the Twitter hack. Prevention (don't use social networking sites), acceptance (everything that is online is unsafe, live with it) and mitigation (use fake details).

We believe that the strident calls for a password replacement should not be taken seriously. They are the cries of idealists, those who wish the world could be safer place. We have accepted the realities of the dangers inherent in the physical world - it is perhaps time for us to accept them in the virtual world as well.

So, how do you solve a problem like authentication? You crowd source - you identify places where people comment about authentication problems on publicly accessible fora, and you mine comments for fresh insights. Ranade and Varshney (2012) argue that one should harness the skills of a diverse set of people to solve intractable problems. People contributing to web fora are far more diverse than academics trying to solve these problems. We can learn a great deal from the combined wisdom of others.

References

Ranade, G., & Varshney, L. R. (2012, July). To Crowdsource or not to Crowdsource?. In *Workshops at the Twenty-Sixth AAAI Conference on Artificial Intelligence*.

BBC News, Twitter: Hackers target 250,000 users. February 2013.
http://www.bbc.co.uk/news/technology-21304049