Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Webification and Authentication Insanity

I don't even have an easy way to count the number of Web sites I use with different user IDs, passwords, and starting next month, hardware tokens for access. As a starting point I looked in my collection of text files containing notes on sites, accounts, and passwords, and found 137 files containing, in some cases more than 10 different accounts, all related to the same general thing (a client, banking, airlines, etc.). So as an estimate, I have say 1,000 of these lingering accounts, not including those that are automatically kept by my browsers in different systems. And each has its special little requirements – like length, makeup, must be changed rate, questions and answers in case you can't remember it or they timed you out. I now have a calendar day reserved every month just to go through my list of required access sites changing passwords and accessing them so my account stays active. It has gone nuts!

For my protection?

As I look at site after site, I find that all of them claim to want to protect me. That's why they all have to have unique requirements for user IDs, passwords, tokens, fall-back mechanisms, password resets, etc. After all, my browsing at Google has to tie me to my activities in order to assure that I am safe...

What??? How exactly does it keep me safe for them to remember my browsing habits? How does having a user ID and password on their system protect me? Actually, it almost never does. It protects them – from liability for changes made – from liability for charges to my stolen credit cards from their sites – from loss of revenue due to inability to get me to buy from them on their up-sell – from lost advertising revenues. I have seen few cases where any of this protects me. It's usually a pretty distant claim from reality.

Come the hardware tokens

Of course now I am starting to see something even worse. I am now required – by select clients – to have a special hardware token that I use to access their site. For a company employee having such a token is likely no big deal. You have one, you use it for lots of different things, it's part of your badge, an interface to it is embedded in your company computer hardware, no big deal. Or maybe you have a token in addition to your badge. OK, we can live with it.

But for someone like me, I am starting to see requirements for tokens and badges for more and more clients. This means that I have a need for more and more of these things. Imagine what happens when I need a different token and badge for each of the many different locations I visit in any given year. Imagine what happens when I have to start updating accounts using these tokens on a monthly basis. If you think all the ID and credit cards you need to carry around is getting bad, just wait till they are in different form factors, interfaces, use methods, etc. Along with the 4 different safes I have for the different requirements they have to meet, the increasing set of keys on my keychain, and files of lists of passwords, we now add the hardware tokens. Soon I will need an assistant just to carry it all around.

Everybody does it their way

The great thing about a free society is that everyone can do things their own way. And the place this is so clearly true is in the Web. There are something like 150 million Web sites in use today, many using different approaches to do nearly the same thing. The variety is incredible, but the convenience, not so much.

For example, I want a mailing list for a class I teach, but the Web site we are forced to use doesn't support this. It has only Web-based forums, and 10 of them for the class, one per portion of the class. So each student and professor has to login to a Web site, navigate through it (direct URLs don't work), look at all of the different portions of the course (it is asynchronous because it is Web-based so it can be), and do so again and again. Of course you can configure it to send you an email every time there is a posting, so now you get emails with the notice that you have to go to the Web site and navigate to look for a posting, thus wasting even more of your time instead of sending you the actual message and allowing a response. This process, by the way, involves at least 2 different user IDs and passwords per user, all for a simple function that could be handled by a single email. Multiply this by all the different classes at different universities I am involved in, and you see the start of the problem.

Each government contract I work on has its own Web site now, with a different user interface for each, different site certificates, login and password requirements, password change rates, usage restrictions, and menu interfaces with several levels of depth for what can fit on one page. The same is starting to be true for each corporate contract as well. Each one thinks it's more convenient for them to use this interface, and each time I try to explain up front that it's going to be a problem because the technology will get in the way of the work rather than facilitate it, and each time the story runs about the same... (1) You must use our Web site, it will be so much better over time. (2) The problems are explained to them but they refuse to listen. (3) We adopt their approach because they are the client and we follow it for the things they request. (4) They start to use the site less as it becomes inconvenient for them, but we continue to. (5) We do our work and put it on the Web site. (6) Their Web site fails in one way or another, causing them to be unable to communicate and delaying the project. (7) We tell them the results were put on the Web site, but that we can no longer access it. (8) They start a password resetting and re-authorization effort but that just delays things further. (9) They start to coordinate things with emails and revert to other older and more reliable technologies. (10) We are forced to redo the things we already did in the new form they are now using.

This exchange, which I have repeated scores of times by now, is a waste of time and effort by well-meaning folks who think Webification is good and ignore simplicity as a key to success.

The solution

The solution to these problems is surprisingly easy, and likely completely infeasible. It calls for people creating these systems that seemingly favor them to think about what they are doing to others before proceeding, and consider the big picture. Listening to others would also help, but that's even more unlikely. We will likely continue to make these mistakes again and again, until someone in government somewhere forces a solution on us – the national / global ID card perhaps – complete with Web tokens, pictures, digitized biometric data like fingerprints and eye scans, perhaps medical and dental records, licenses, permits, passports, credit details, etc. In terms of the Webification, I predict mailing lists will make a big comeback...

One possible future

Suppose we went to a single global identity mechanism. As an objective, it will include a vast array of different biometric information, including medical records (dental records, operations, diseases, etc.), pictures, hand geometry, retinal scans, pictures of identifying marks, and on and on. It will also include a wide array of cryptographic mechanisms, say 40 different systems and any number of instances of each, so that sets of multiple systems that may be required for different approaches are handled, when a cryptographic system is broken, others will be available for continuity, and so it can hold all credit card, licensing, badging, and other data. It will have multiple interfaces for the various modes of use (wireless, direct connect, locality sensors, etc.). And of course, this will be agreed upon as an objective by all countries globally, so that any country can produce its own authoritative mechanisms and all others will adopt it in the single credit-card- or key- sized token carried with every person on Earth from the womb to the tomb.

And suppose we had similar tokens for every digital system/device, each owned by an individual and granted authority to act as that individual only in limited ways. Every piece of code, writing, action, activity, and every other thing leaving a digital footprint would also have the proof of who did it embedded with it, so that all actions could be attributed to all involved sources and the paths by which it came to be. And let's go further. All of the surveillance cameras and sensors in the emerging digitized world could be coordinated with the GPS locations of all devices and people so that all observable activities of every person and thing would be readily retrievable and you could literally watch the movie of each person's life. And imagine all the sensors were always on and recording at maximum capacity. All of this has been in the science fiction literature for along time, and movies have shown variations on the resulting worlds.

Now let's go a step further. Suppose all of the underlying data and the ability to access and analyze it is stored in a global cloud system in which each country and anyone else who wants a copy gets the authenticated copies and makes them available on the Internet for free. And let's suppose that anyone and everyone can access any of it at any time for any purpose they wish. So in essence, there are no more secrets except the ones you hold in your head and the ones contained in non-digital systems and forms. Each time someone comes up with a new idea, as soon as they codify it in digital form, it becomes part of the permanent record. They can claim credit for it, and all of the supporting data will show that they did it. If someone tries to lie about it, the inconsistencies with their story and the vast array of records will make their lie transparently obvious to anyone who looks. Take a bribe? We will all see the whole thing. Step out on your spouse, they will be able to see it if they care to. The money system no longer requires all of the handshakes and providers, it is all part of the system – you know who it is, the money transfers transparently, you know how much they have in all of their their bank accounts, and that it came to you. Worried about someone extorting you? They will be in jail before they get the money. The full range of human behavior will be exposed, and those who cast a stone will be subject to everyone interested watching all of the things they have done or not done in their lives. Oppressive government? Not if everyone can watch how all the sausage is made.

This utopia/dystopia is at one extreme of “information needs to be free” in the era of the digital world. Full responsibility, no anonymity, everything known by anyone who cares to know it.

Another extreme future

At a different extreme of the spectrum, we have full anonymity of all actions all the time. Anyone can claim anything they wish, lie about where they are, who they are, what they are, when they were where, and who did what, why, how, where, and when. We live in caveat emptor – let the buyer/seller beware. Forged credentials? No problem. Take money from others with technical means? Easy enough. Don't have the skill to protect yourself? That's not my problem. Kind of like the investment system of today – the investment class does what they want and tells us that we are responsible for our own investment decisions – so why shouldn't the technology class act the same way. Want your money? Get the technical skills to take it back from me and it's yours.

Of course the privacy thing ends up more or less the same. While some will have privacy because they are able to attain it through their skills and ability to trick others, the rest of the folks will have their information revealed, perhaps even forged at will, with advantage taken by those with the skills and power to do their will. Worried about legal precedent for your current case? Don't worry, we will alter the digital records of precedent so that when the judge and lawyers go to look it up, it will come out differently. Worried about the opinion released? Don't. It can be rewritten and automatically signed. If the judge claims they ruled differently, point to the official court documents, suitably altered in digital form. It's the record that counts, not the claims of an unstable justice who writes one thing and says another. Expect digital warfare at all levels of intensity – from extreme violence to low level intelligence gathering and subtle military subversions of enemy systems.

All of this will go fine, as long as there is enough semblance of a free and fair society left. Of course the line moves as you move it, so the digital records of loans and home ownership will come out wrong some of the time, when it advantages one party or another, but as long as you don't get too greedy and try to take too many homes all at once, the frauds will go largely covered up. Want political cover? No problem – fund their campaigns and threaten to expose their lies if they fail to comply.

Of course since we can't trust anyone but ourselves, if them, we will have to build up individual methods for everything, requiring hundreds or thousands of different identifiers and authenticators for our connected world. Cooperatives will form, leading to efficiency for those who can afford it, and this will lead to a desire to do business with the business partners who make things easy and convenient. Trust will build up for periods of time between partners, with proper contractual limitations and legal systems that all can buy into at a similar level.

Privacy? Of course you can have it. Trust us. But if we get broken into, it's not our fault. After all, who could have anticipated … you name it. Want to sue us? We will limit liability by contract, which you cannot possibly read or understand, and which flashes by in digital form without a written and signed copy to use later on to prove that what you read and agreed to is what you actually have as the “agreement”. And it's subject to change at their whim and without further notice.

This dystopia is brought to you by … the present. This is, in some sense, a good summary of the current situation. Imperfect, slightly exaggerated ... perhaps, but pretty much the way it is.

Somewhere in between?

Both of these futures and a wide swath of the region between them is within the capability of our global society over time. The question we need to answer as a society is where we want to be in this spectrum. If and when we make this decision, we can achieve it. Of course it's not likely to happen this way. The world rarely works by architecting a future, designing it, developing it, and living in it. We live by evolution based on circumstance. Precedent takes precedence and what is tends to remain until it hurts enough to change it. And then it is only changed toward another end that produces some local optima based on the ability to persuade or force some portion of the population to buy into it.

My dystopian vision is pretty simple for the short run. I am willing to give up some privacy in exchange for transparency in my public / work life, but not in my private life. I want the right to be left alone in the digital world. I don't want anything to be shared with anyone who doesn't absolutely need to see it for the functions I have requested, and I only want it used for the purposes necessary to carry out my requests. If you make up a phoney reason, you should go to jail for fraud, along with everyone you gave the information to. I want this enforced by constant surveillance on anyone who gains access to any such information – when they are at work. Of course I want them to be unable to remove the information to other places, so when they are not at work, we can leave them alone and they can have their privacy. And I want equity – so that anyone who has access to my information has to grant me the same access to the same information about them. If they can see my medical records, I should be able to see theirs. It's a simple matter of equity. If someone wants to sell my information, I should be able to set the price I want, and they can sell it for more to make a profit. My current rate is US$1M/bit/instance. So backups are quite expensive. I want these things enforced with permanent warrants and surveillance on anyone who chooses to be in that business and transparency for their actions with rapid and strict enforcement for cheaters. As to breakins, the liability should sit with the person holding the content – personal liability to the executives, with a statute of limitations equal to the duration of the data in all its forms.

As to my Web accounts, I think a single unified digital ID with proper protections is reasonable enough. Combine it with the other features, like storing all my credit cards, biometrics, enforced submit commit mechanisms, and use it for global transparent and automatic access and I will be good to go. Report a card lost/stolen and get another one at any local store within minutes. No problem. The old one is no longer valid, and we don't have to worry about getting a fake one because it has mutual authentication of the card to me and me to it. Nobody can use the stolen one without my biometrics anyway, and when I go to pick it up, the person handing it to me sees my picture and verifies my identity with their biometrics systems. Yes there will be forgery attempts, and when caught, they will have to go to jail. It will be pretty quick since the proof of where I actually was is relatively easy to produce and their biometrics will be stored everywhere they tried to use the phoney card. And in my private life? It's nobody's business. As long as they can't share my records, it's OK that the store where I buy my birth control can get actual payment, with the records destroyed as soon as they are paid.

Conclusions?

This is only an outline of my views. What are yours? How would you manage the tradeoffs? Engage in the discussion and start to think through it and discuss it. Our future depends on it.

