

good behaviour

*a personal approach to
Internet authentication*

why is it

*after a generation of the
Internet, we still begin every
financial transaction with some
crude form of username and
password token?*

forty years ago

the first ATMs needed a PIN.

nothing has changed.

Contents3
Are we there yet?4
 Made to fit.....4
 What’s in a number?.....4
 We are where we’ve been, not what we know.....4
Common and uncommon knowledge5
 Memories and relationships.....5
 Applying CRM to commercial web authentication.....5
Catching the villains6
 Other advantages of uncommon knowledge.....6
 The Honey Trap.....6
So why isn’t behavioural CRM being used?7
 Money being spent, but in the wrong places.....7
 Web II: this time its personal.....7
About LANZen8
 Thanks for reading this white paper.....8

Made to fit

Internet Banking is an integral part of our lives and controls more of our money. *Wouldn't it be nice if the banks treated us like humans?*

Our cars wrap around us, our shoes fit our feet. Everywhere, our surroundings are adapted to suit us. But in banking, they need a password. In what other human situation are we asked for a password? *They only do that in really bad spy films...*

Just who decided it would be a good idea to give us some cumbersome bits of plastic hardware to access on the Internet the same information that's available in a bank branch. *Aren't computers supposed to be smarter than people?*

The only bank I know of that has applied some thought to customer security is the Alliance and Leicester. They use a CRM-based authentication system using adaptive technology and personally selected images to verify user identity.

The rest of our main high street banks seem happy to let our security be defined by marketing departments, not usability experts. "Let's give our customers tokens/card readers, we know they don't work, but it looks like we're doing something!"

What's in a number?

Let's take a step back. Let's look at what we're trying to achieve with a username and password. We're simply trying to ascertain if the person is the person they say they are. Some idiot thinks that by associating a random set of numbers and letters with us that we can be safe on line. *What a total load of rubbish.*

It doesn't prove I am who I am, it proves only I have acquired the numbers associated with that account. *How can that be good enough?*

We need a system that uniquely identifies us by tapping into information that's personal to us, not given to us on a piece of paper or via a set of numbers on a token.

We are where we've been, not what we know

OK, that sounds a bit cryptic, I know. But just think about it. The fact that we know a password, pin number or something means absolutely nothing. Its just a token associated with our account, just something that's been learnt, in other words, *what we know.*

Our lives contain a rich tapestry of personal experiences and memorable events. We don't just remember them as something told to us, those memories are the very fabric of our lives. They're what makes us, well, us. In other words, they're *where we've been.*

Memories and relationships

Common knowledge is what is known about us, our birth-date, mother's maiden name, our school, pet's name, etc. It's personal to us, but its knowledge easily acquired by others.

Uncommon knowledge is that pool of experiences we've all had. Our first bike ride, most memorable celebration, where we were when we proposed to our partners, favourite photo or place. An endless list and unique to us.

If we volunteer some of this uncommon knowledge and store it for authentication, it provides a far better guarantee of personal verification than anything else. Memories are almost impossible to forge, so for that reason, more secure.

Put in commercial terms, it's a form of Customer Relationship Management, CRM. But not the mind numbing, banal versions we use to manage suppliers, but intelligent, focussed *behavioural CRM*. *Could this be the answer?*

Applying CRM to commercial web authentication

Implementing CRM into web pages may sound an expensive and complex proposition. But any enterprise that's selling a product maintains some sort of CRM system, to keep track of client records, order history, whatever. Extending this to take in personal memory details would need research, but is a promising concept.

Linking a CRM backend to the authentication process would be relatively easy. The client enrolling in the service and be asked to describe a number of personal events or supply some images. The customer would choose what they wanted to provide.

The CRM system would then use this pool of information, selecting from it randomly during the transaction, requiring more information the more sensitive the transaction became.

Other advantages of uncommon knowledge

The *uncommon knowledge* approach to authentication has one big advantage. It can be used to trap an attacker by using incorrect responses to draw them into an area where they can be traced and caught. But first, let's look at why setting a trap is important.

Currently, identity theft costs are passed on to the customers themselves as inflated fees. A couple of points on a credit card's interest rate, or higher charges. In effect, the customer bears the cost of the system's failings. *Wouldn't that money be better spent catching the attacker than penalising customers?*

Economically, targeting the attacker makes sense. One attacker may steal from tens, hundreds or thousands of users. Each compromise incurs costs to rectify and lowers customer confidence in addition to the monetary loss. The best way to catch an attacker is with another real-life technique, *the Honey Trap*.

The Honey Trap

This involves allowing an attack to complete as if nothing's wrong. The system detects an incorrect response. The thief "sticks" with the attack, because they think the system is behaving normally. But the system is actually probing the attacker, using hacking tools to trace the attack source.

As soon as an attack is suspected, the real back end is disconnected and substituted with a back end containing dummy information. The attacker is slowly being drawn into the trap, into a pool of similar but fake customer account information.

The system reacts normally, even down to appearing to make a funds transfer to ascertain the receiving account while all the time building a portfolio of evidence to hand over to the designated investigating authority.

Catching one thief this way saves the costs of maybe thousands of lost transactions. *Basic, sound economics.*

Money being spent, but in the wrong places

It certainly isn't a lack of investment. Huge sums are paid to big-name consultancies who rack out the same old solutions, like two factor authentication and card readers. The problem is, good ideas don't come out of committees. They are borne by individuals.

Complacency plays a part, as does laziness. Most banks feel because they've spent the money, they've met their compliance obligations. Innovation doesn't come into it. Why worry about what's actually delivered. After all, losses are passed on to the customer, right?

Behavioural CRM would require thought and organisation. I could be controversial here and suggest neither are associated with retail banking, but let's just say it's not an easy sell to the banks.

Conventional consultancies push standard offerings and rarely offer something they can't show a good margin on. For them, research is a variable in a world driven by fixed deliverables so doesn't get considered.

In truth, the only way the banks will move forward is if they recognise that as Internet use grows, so does the determination of criminals. The banks should commit to investing time with specialists to research, develop and deliver new methods like behavioural CRM.

Web II: this time its personal

Web 2 poses many challenges, not the least of which is convincing CIO's that they need to apply 21st century solutions to 21st century problems. *Could CRM be the answer?*

Whether it's CRM, adaptive authentication, pictographs, or something else, one thing is clear. Tokens are not the way forward. Research has to be done to come up with a better way for us to interact with electronic banking and other sensitive environments.

Come on banks. think about your customers. You owe your existence to them!

Thanks for reading this white paper

I'm Neil Robinson and LANZen is my information technology strategy and design consultancy. I'm in Cheshire, in the North West UK. I've helped many clients, like City banks, Jamie Oliver, smaller and start up companies, even one-man operations discover new business IT strategies that work for them.

If you're looking to move your business forward, there is probably something I can help you with. Please take a moment to visit the LANZen website, or the LANZen strategy and design blog.

You'll be in good company, the blog is visited by most of the world's top banks and companies every day.

Neil Robinson

email neil.robinson@lanzen.co.uk

website <http://www.lanzen.co.uk>

blog <http://www.blog.lanzen.co.uk>