Breaking Bad Actors – transcript of presentation video

Good afternoon and it's not an acting audition that I'm here for.

I'm Rob, this is Raj and Peter and we're the breaking bad actors team.

We're 5 participant companies from I think 7 countries, so a very internationally diverse team.

You all saw the video earlier and I say some of you may have had a tear in your eye, the impact that financial crime has on people.

We've picked a use case, authorised push payment fraud or social engineering fraud as some people know it. That has real impacts on people and organisations working on it today, but we think there's a lot lot more that people can do.

Here in the UK it's a massive problem, it's £360m of impact on the people that live here and generally they're very vulnerable people. Unemployed, elderly, lower paid, whatever and there's untold downstream damage as well.

2 real problems that stop us interdicting this is the inability to share intelligence between organisations and the speed with which to get that information to where we need it.

And this is what we've been looking at, how to fix speed and information and do it in a way that is privacy preserving so we're not compromise any legal process along the way.

So the simple use case that we identified was the arbitrage that happens when an authorised push payment happens when you see an old person who makes a payment and think they're sending it to somebody but the account number has been changed, they don't recognise the number, they recognise the name, whereas the bank recognises the number and sends it on to some other place.

This could be easily solved if you could match the name to the number in the destination institution and the destination institution sends a reply back to say, those 2 things don't match there's a problem here.

So this is what we set out to address. Using privacy enhancing technologies to query the destination bank about the name and the number on a particular account.

We use a thing called secure multi-party computation and Nigel gave you a very very detailed explanation of what secure multi-party computation does. It essentially enables multiple parties to compute a result without disclosing the inputs to that result that are needed to create it.

It's a bit of cryptographic magic that takes a long time to explain, it took me weeks to really get my head around it.

We do that by creating a variety of taxonomies really, that allow us to derive behavioural intelligence or life patterns, stuff that looks weird, not normal and use that to create the computation that tells us something is not right.

So let's illustrate this with an example. Here we have Jean, recently widowed and she's been essentially duped into paying for an insurance product that she probably didn't need, but managed to unfortunately come into contact with a dubious salesman. She got an invoice in the post and paid it, because she recognised the name on the invoice. Royal insurance limited looked like a genuine institution and she recognised it. But the bank account on that invoice was not Royal Insurance limited. So we were trying to match this up.

She never got her policy and when she realised she hadn't go it, she went to the bank to investigate and low and behold, the money was gone and it was never coming back.

So what happens today? She fills in her remittance makes the payment. Everything looks perfectly in order, the bank may look at her life pattern and say this big payment to an insurance company might be a little bit odd, maybe give it a little question mark there, maybe she's a vulnerable person because she's old or whatever we'll give it another question mark there, but generally it will just flow through, because, the majority looks fine.

And this is where we come in. So we've created "PREXA", PRe EXecution Alerting. So before you send any money, you query the destination bank about all the information that you have. Does the name on the destination account, match the number of the destination account and we do that using secure multi-party computation. The result that comes back is "No, it does not match".

We will immediately stop the payment, notify the customer and tell them there's something wrong.

The beneficiary gets notified there's something wrong and they can now kick off an investigation and start to look at the life pattern associated with this account and does it have, weird, unusual patterns that need to be investigated. Yes, red risk, account frozen, SAR filed.

Here we have a demo, this is what we've built. So the first screen is a list of all of the participant organisations that we screened, so these are all the banks, the one at the top is law enforcement or a regulator.

The one that's on the screen is the transaction that we identified from Jean to the Bank and you can see, based on the attributes that we tested, the behaviours, everything was unusual except the login, because that was okay.

So we stopped it and you can see the source bank coming to the destination bank with the 2 dots and the red indicating this is a problem transaction.

If we look at the sender bank now, sorry the receiving bank, beg your pardon. The receiving bank, you can see that transaction number 5 which was the last one in the account has been stopped, but prior to that there were 4 other transactions.

The yellow ones were all marked dubious because that information came from the other bank through privacy enhancing communication channel and that one went out, meaning the crook had taken the money out of the funds through something that looked perfectly normal.

This looks weird in terms of the overall pattern so given the insight that you've been able to get from the communication process among all the banks, you would probably freeze this account.

So, in summary, if we just switch back.

So the benefits for the customer, we would stop fraudulent payments before they leave. The customer gets notified there's an issue, they can fix it, but the happiest thing they'll ever get is we haven't given your money away to a crook.

Financial industry, no personal data gets shared by financial institutions, this is really important. The only thing that gets shared is the insight youv'e derived from the knowledge that they already have.

Will help you reduce your false positives will help you increase your real positives. Which is really what you want to spend your time on, don't waste your time.

And it works across the whole banking system, retail, correspondent banking and it will work internationally to. There will be collaboration requirements here, governance structures that would have to be put in place among the banks to create taxonomies and so on, but that is all doable.

And then lastly, Law Enforcement, you get information, really, really quickly. You get a total picture across all of the banks where dodgy transactions have been identified.

Financial industry in terms of deployment. We can deploy this, roughly, the first iteration of it in maybe 90 days working closely with the team. So it's not hard to deploy and its low cost so relatively easy to do. It's about getting your data into the right shape.

So lastly, just remember Jean. We saved her money, the bank made her really happy and law enforcement put a bad guy in jail. That's what collaboration can do.