Secret Computers - transcript of presentation video

Hi I'm Kevin McCarthy and I work on secret computing at Inpher and I'm part of team Secret Computers.

Hi I'm Simon Bucket I work for Standard Chartered in Financial Crime investigations.

So, it's an age old parable around 3 blind men who stumble upon an elephant each trying to deduce its identity.

One feels it's leg and infers a tree.

The next its trunk and thinks a snake.

And the 3rd its tail, thinking a broom.

If they had shared information, it's likely they may have deduced an elephant.

In the financial services industry, we face similar challenges, trying to identify the elephant in the room.

Yet, despite these challenges, we individually use our respective information within each of our banks to challenge common problems that we face in the fraud anti money laundering or even the credit determination space.

And if we were able to share this information we might be able to derive greater insights.

But rightly so, we're regulated in the way that we store manage and share customer information and that's had detrimental effects, up until today in which new technologies like privacy enhancing technologies, multi-party computation and secret computing have come of age.

So one of the examples that we're going to run through and use as our base is the Russian laundromat scheme that got unveiled to us and frankly embarrassed the banking community in 2017. There will be a lot of blank faces from banks around here who wouldn't want to be really reminded of this.

It was a huge network of 20 billion dollars that got laundered around the world through hundreds and hundreds of institutions across thousands of entities and nobody spotted it in the banking community.

Why not? Well the reality is that we all work in silos, we don't work together effectively. So actually, as a bank, all I see is my transactions, I don't see a network, I don't see everything that's going on.

So, maybe I don't think that that's a problem.

It's not 2017 anymore it's not 2012 when this happened, it's 2019.

What exciting new technologies have we got, that can help stop this from happening again.

So, let me provide a set up on something around multi-party computation and follow on from Nigel's talk and secret computing. The premise is that there are 2 respective banks this extensible to n number of players through the system. Each of which have their own private repositories of information protected of some form of requirement to keep them separate and distinct. Whether that be rationalised by GDPR, data residency, intellectual property, conflicts of interest, the list goes on.

And to kind of expand it a bit what we can do is change our database image into something that is a bit more representative in which we can locally encrypt this dataset and secretly share the encrypted version of that dataset with our respective counter-parties in a joint analysis.

No personal data is exposed only encrypted secret shares are exchanged amongst the participants in a computation.

Classically this is often used to use simply more data, more data can create better insights. We've gone a bit beyond that here in kind of reaching into the graph and network analysis practice to bring in some of the networks that criminals used against us as financial institutions, to networks that we can use to refute those criminals.

The way that we have essentially applied that, is injecting MPC protocols into existing work flows where classically accounts and transactions are run through scoring engines and flagging systems that might segregate them into a suspicious database for future investigation.

Interestingly, what we do is we take those transactions and develop a network graph, which is then flattened into a matrice representing either quantities or summation information without the transactions happening amongst individuals. We take those tables and secret share them amongst the participating institutions 2, 3, 4, n number of banks.

That can then investigate an aggregate graph leveraging private secret shares, to infer things like between us, centrality, shrink and other metrics around the network, that would allow us to detect not just 1 suspicious account, but clusters of suspicious accounts.

These identified accounts in the respect of transactions can always be scored, but really in trying to drive actionable insights we can take these clusters and develop aggregate statistics on top of them, that might support individuals like Simon and his team and further diligence in suspicious activity.

So we've talked a lot about MPC, secret sharing of information, but what does that actually look like. So we've taken the test data that we were given her at the TechSprint and we've run our solution over the top. We've run a global transaction monitoring rule to find networks.

We built it, Inpher built it, put it together, and slight panic moment to see if there were any networks within the data and if not this would have been an embarrassing presentation and thankfully, we found this. This was actually in the data that was given to us. So we ran a very simple rule that says "Money into an account, if it goes out of that account within a week, within a 10% variance, flag it, start building a network, start building it up" and this is what we found. But, this is just like Russian money laundering, nobody can see this. This is 6 different 5 different banks information, nobody can see all of that in 1 go.

What we can say, is that one of the banks has this exposure. That is their clients, that is their transactions that has gone through their bank. We can take this data and give it to each bank that's involved in the network. The issue is here that if I give that information and say "Hey bank, you've got these clients involved in this transaction and it's a risk". I've actually increased risk there because I've given you problem, with absolutely no insight into the solution.

What we can do with our solution, is give an analysis report as well. So I'm sat there at my desk as a financial crime investigator. I get my transactions, my clients. It tells me in this network I've got 16 accounts of a 112 of these clients and it will send me the transactions it will tell me it's a money laundering network. But then I get everything else of the network. I can't be told the data I can't be told the full picture because that would breach privacy. But I can been told a few statistics, myself and the other 4 banks will get all of this. Hey there's £70m has already gone through this network there's 13,000 transactions. We've got high risk countries of Iran and Pakistan in here and these are the other banks that are involved, so we can tell them the banks involved, but we can't tell them exactly what. But I can start building up my picture, because I've got a typology as well as some information.

So the cool thing about this again is that we can develop these typologies and insights on the clusters, clicks or typologies themselves while preserving the underlying privacy of their respective transactions and account data and bring aggregate, insightful and actionable insights to individuals charged with investigating these activities.

And we're talking about actionable, what can I do next? So traditionally under section 331 I'll file a SAR, great! But what can we do that's much much better. Under the new regulations under section 399zb we've read it, extensively. I can actually say to the NCA I'm going to pause filing my SAR and I'm going to work with the other banks I'm going to work with a network, to beat a network. And we're going to work as a network of banks to beat a network of criminals by stopping transactions, by stopping accounts, stopping that entire network, not just giving them a go around. And then we can as together as banks, file a SAR together or as individuals, which has got better information for law enforcement to prevent the criminals from doing this again put them into jail or do whatever is needs to be necessary.

So again, we're team Secret computers comprised of a number of different financial institutions and privacy enhancing technology companies. We built this solution on top of a commercially available platform. We think it's ready for production but needs configuration. It takes only 2 to build a network and we would love to talk to any interested parties.