Faktaruta:
Namn: Joakim Brorsson
Gör: Arbetar med säkerhetsarkitektur på HYKER Security parallellt med forskarstudier inom datasäkerhet och kryptografi vid Lunds Universitet.
Bor: Malmö
Ålder: 30 år
Utbildning: Gick på LTH med HYKERs andra grundare Jonas Hallin, Jakob Folkesson och Emil Boman. Redan där började de starta verksamheter. Med lite skilda resultat, kan nog konstateras. Appen som mätte hur mycket alkohol man kunde få per krona på Systembolaget fungerade dock utmärkt…
Fritid: Gillar att spela gitarr och att åka skateboard.

Rubrik:
Med framtiden säkrad

Underrubrik:
HYKER sätter alltid din säkerhet främst. Även när du själv glömmer…

Ingress:
Smart cities och end-to-end kryptologi. Låter det märkligt och svårt att förstå?
Inte om man låter Joakim Brorsson, en av grundarna till HYKER Security förklara.

Under de senaste åren har digitaliseringen ändrat vårt sätt att arbeta och leva: Vi vill jobba hemifrån. Vi delar inte längre USB-stickor med varandra utan lägger all vår information i molntjänster. Vi vill att vårt kylskåp skall berätta för oss när ketchupen är slut och självkörande fordon är redan en reell verklighet.

I takt med att vi blir mer och mer digitala har många också börjat uppmärksamma vikten av datasäkerhet och att online security är ett begrepp vi inte bara behöver fundera över utan även praktisera. Ett av de företag som var snabbt ute inom datasäkerhet och som nu är väletablerade och har en bred teknisk plattform inom området, som är under ständig förbättring genom fortsatt forskning, är HYKER Security.

Jag träffade Joakim Brorsson, en av HYKERs grundare, för att få svar på komplexa frågor om en förhoppningsvis säker men framförallt spännande teknisk framtid.
Till vardags delar Joakim Brorsson sin tid mellan forskning på Lunds universitet inom

datasäkerhet och kryptografi med sin roll som ansvarig för HYKER Labs, företagsdelen som forskar och arbetar vidare på HYKERs tekniska plattform. Allt för att säkerställa att den håller vad den lovar, bland annat genom att undersöka attacker på den. Men Joakim Brorsson tittar även på användningsområden av denna end-to-end kryptologi i ett framtida samhälle, till exempel i en smart city.

Kryptologi! Hur hamnar man där?

– Jag vet inte varför eller var det kommer ifrån men jag har alltid haft intresse för datasäkerhet. Tyckt att det var kul att ha sönder saker och undersöka dem.

– Från början var det nog egentligen ”attacksidan” som intresserade mig mest men genom att vara det blir man också automatiskt intresserad av hur man kan förhindra intrång.

Ni (Jonas Hallin, Jakob Folkesson och Emil Boman, reds anm) startade HYKER redan under tiden på universitetet. Hur kommer det sig?

– Vi hade CSN och en massa tid. Det var en lyxig situation att sitta i och vi ville driva ut saker i verkligheten så redan första och andra året under utbildningen började vi lägga vår tid på annat än bara studier. Fast de allra flesta av alla våra många projekt blev aldrig avslutade. Kanske tre av dem, varav HYKER var ett.

Så vad är det egentligen HYKER har skapat?

– Jag upplever att det skedde ett systemskifte kring 2005. Innan dess behövde du bara lita till dig själv. Lita på att du inte blev av med den externa hårddisk där du lagt din information. Men idag när vi istället använder molntjänster till nästan all lagring så lägger vi allt det vi tidigare hade på vår egen lilla USB-sticka i händerna på en tjänsteleverantör.

– Vi delar infrastruktur med så många aktörer att vi inte ens kan hålla reda på det själv. Därför måste man hela tiden fundera på vem man litar på och tänka på att leverantören i regel äger koden som rullar i bakgrunden och har på så sätt tillgång till all min information. HYKERs breda tekniska plattform med end-to-end kryptering tar bort alla dessa problem. Vi ser till att det endast är den som skickar informationen och den som mottar den som kan läsa den. Inte ens vi på HYKER har tillgång till den. Och det är precis så det alltid borde fungera!

– Men alltså, det är viktigt att påpeka att vi på HYKER gillar att vi delar på gemensamma system. Så det handlar inte om att vi skall ta bort några av fördelarna med molntjänsterna utan i stället att vår teknik låter människor återta lite av sin kontroll.

Men kan du förklara för mig, en icke-techie, hur HYKERs krypteringsteknologi fungerar på ett lätt sätt?

– HYKERs produkt är enkelt uttryckt en automatiserad tjänst för nyckeldelning. Vi är lite som en låda med svängdörr där det inte behövs en omväg till tredje part.

– Eller om vi säger så här, tekniken med nerlåsningsnyckel och upplåsningsnyckel finns sedan länge, tänk dig en vanlig spargris med skåra upptill där man kan lägga mynt eller papperslappar med meddelanden i. Under spargrisen finns ett lock med ett lås. Jag lägger ett meddelande i spargrisen och skickar den via molnet till den som skall ha mitt meddelande. Skillnaden är att den spargris jag har skickat har ett lock med ett lås som leverantören inte har nyckeln till. Nyckeln har jag däremot sett till att min mottagare har så när han får spargrisen kan han öppna den.

– Lite som på 1700-talet, då skrev du ett brev och den ende som hade en chans att läsa vad du skrivit innan mottagaren var brevbäraren. Vi har reducerat bort brevbäraren också!

– Jag tror det är viktigt att påpeka att vår teknik egentligen inte är ny men vi har uppdaterat nyckelhanteringen. Vår innovation är att tekniken är smidig, enkel och lätt för alla användare att ta till sig.

Förutom att plattformen är användarvänlig så har ni avsiktligen byggt en bred och generell teknisk lösning. Hur kommer det sig?

– Se det som att vår produkt är en kanonbra bil. Andra företag har kanske samma bil men inte lika bra och vissa av våra kunder vill ha hela bilen och då köper de kanske vår kundportal Konfident. Men ett annat företag behöver bara en växellåda för att kunna göra sitt system top notch. Då tar vi den fantastiska växellåda vi redan har och optimerar den ytterligare för att den skall passa deras behov och lösa deras problem. Någon annan behöver hela motorn men ytterligare en tredje kund bara krock-kuddar eller ett tändstift.

– Detta innebär i sin tur att HYKER alltid ligger i framkant. Vi utvecklar inte för utvecklandets skull utan för kundnyttan. Och för att kunna jobba på så vis ringer vi runt till alla våra kunder en gång i kvartalet och ber om input på vad de behöver.

– Vår grundteknik är väldigt bred och den kan användas på så många olika sätt. Visst, vi breddar den inte så ofta. I stället går vi in i alla delar och vidareutvecklar dem till perfektion. Vi vill helt enkelt göra vår växellåda bättre och bättre och bygga in nya delar med fantastisk kvalitet i stället för att byta färg på hela bilen.

Varför är det så viktigt för er att inte fuska med användarvänligheten?

– Vi vet att shadow IT, när personalen på ett företag själva tar till olika lösningar eftersom det centrala datasystemet är för svårt att använda är vanligt. Så fort ett system blir för krångligt hittar människor genvägar.

– Detta leder till att många IT-chefer inte har en aning om hur många olika leverantörer som i praktiken har tillgång till företagets information. Genom att då erbjuda en användarvänlig lösning så kan vi hjälpa företag att slippa detta problem.

– Som Konfident! Den plattformen är egentligen byggd utifrån tanken att bara ”fungera”. Den är byggd för att appliceras och snurra på din egen dator utan någon inblandad tredje part. Varken mer eller mindre.

Det talas mycket om smart cities nuförtiden. Vad är det egentligen?

– Det undrar jag också ibland men tanken är väl att medborgarna skall kunna dra nytta av den teknik som finns. ”Staden” skall kunna samla in data till fördel för staden och medborgarna. Ser man att det är mycket trafik eller mycket utsläpp på en gata skall man till exempel kunna dirigera om trafiken.

– Detta är bra men man måste vara medveten om att det finns en fara i att man börjar samla in information om medborgarna. Syftet är gott, men vill vi verkligen att alla skall ha koll på vårt rörelsemönster hela tiden, till exempel.

Vad kan HYKER erbjuda en sådan stad?

– Jag skulle vilja se en mer allmän adoption av ett ändrat mindset. Att vi tänker ’trust’ i stället för ’infrastruktur’. Att vi istället för att nöja oss med att länken mellan A och B är säker, funderar på om vi tycker A och B ska ha tillgång till våra data. Det vill säga vi fokuserar mer på aktören i stället för tekniken.

– Detta kan vi göra bland annat genom mindre central kontroll. Idag har man oftast en stor server där allt samlas. ”A single point of failure.” Den blir ett väldigt attraktivt mål att attackera. I stället för en central databas med krypterad data som är hårt fortifierad så borde man ha mellankanaler. Datan skall krypteras så att endast den som skall använda den kan komma åt den. Här kan HYKER gå in och bidra.

– Detta kan tillämpas inom kollektivtrafiken till exempel. En buss skickar sin position upp till en databas och en passagerare som vill veta var bussen är och hur länge den dröjer klickar ner informationen. Här vet systemet inte vem den mottagare som informationen skall krypteras till är och då kan HYKERs nyckeldelning komma in i bilden.

Hur då?

– Vi kan gå tillbaka till spargrisen. I de allra flesta fall med kryptering så skapar man nyckeln med någon redan i åtanke men det fungerar inte om mottagaren är en produkt eller den väntande busspassageraren.

– Avsändaren är aktiv fast i efterhand kan man säga. A lägger dokumentet i spargrisen och skickar den, men skickar spargrisen med ett lock utan nyckelhål eftersom A inte vet vem som tar emot grisen. Så småningom när spargrisen når mottagare B ber denne A att skicka ritningen på nyckelhålet så att B kan skapa nyckelhålet själv.

IoT, Information of Things är också något som diskuteras mycket idag. Var befinner sig HYKER när det kommer till det?

– Oj, det finns massor av användningsområden. Fastighetsägare som med vår teknik kan kolla värmemätare. Boende som kan blippa sig in i fastigheten utan att låset krånglar. Som jag sade tidigare: Vi har en generell teknik som kan användas till en mängd user cases och vi har faktiskt redan bidragit med vår forskning och teknik till en autonom bil i Singapore.

Det tycks finnas ett ökat intresse för digital säkerhet i samhället. Varför är det så?

– 2013 var helt klart en vattendelare när Snowden läckte NSA-uppgifterna. Då började intresset för säkerhet online växa och med mängden sådana här fall på senare år har det ökat.

– Små som stora. Som när Target (amerikansk detaljhandelskedjan, reds anm) skickade ut rabattkuponger på babykläder vilka nådde entonårspappa innan dottern hunnit berätta att hon var gravid eller cyberattacken som stängde ner stora delar av Ukrainas elnät under Krimkrisen 2015. För att inte nämna hela Cambridge Analytica-skandalen.

– Här hemma har vi Transportstyrelsens IT-upphandling som ledde till att utländsk personal som inte var säkerhetsklassad fick arbeta med myndighetens information och 1177-skandalen där känsliga samtal låg helt öppet på en server på nätet i flera år. Men framförallt tror jag att GDPR-lagstiftningen påverkade när den kom och man blev skyldig att rapportera läckor.

– Genom, bland annat, medietrycket började det plötsligt gå upp för folk att internet och verkligheten är en och samma sak i och med digitaliseringen. Vår verklighet har flyttats upp på molnet.

– Data ger makt så vi måste alla helt enkelt börja tänka mer på potentiella hot och fundera på vilka är de rätta händerna att lägga min data i? Fenomenet som sådant med önskad ökad säkerhet är oundvikligt och där kan HYKER verkligen leverera.

Lever ni upp till vad ni lovar då?

– Ja, det tycker jag verkligen och vi bidrar också till en bra utveckling genom att vi är forskningsbaserade. Vi är öppna med våra resultat och vidareutvecklar hela tiden vår redan etablerade teknik. Verkligen forskar och undersöker på djupet.

– Kunskapen skall ut och vi lägger vårt största fokus på kunden och kundens faktiska problem.

– Dessutom har vi varit igång ett bra tag nu och man kan bara se på våra omdömen, se på vilka kunder och finansiärer vi har. Till exempel ABB på kundsidan och Saab Ventures som finansiär. Den senare har ju ett stort förtroende inom säkerhetsteknik i stort. Vi är verkligen certifierade av tredje part!

– Med HYKERs teknik är datan skyddad från producent till konsument och man kan känna sig säker på att man slipper lita på alla mellanhänder. Det finns ingen mellan dig och din mottagare som du behöver bekymra dig för!

Översättning:

Facts:
Name: Joakim Brorsson
Profession: Head of HYKER Labs where Joakim works with security architecture at HYKER Security in parallel with postgraduate studies in data security and cryptography at Lund University.
Live: Malmö
Age: 30
Education: Attended LTH with the other founders of HYKER, Jonas Hallin, Jakob Folkesson and Emil Boman.

Already at university, they started different businesses. With slightly different results, should be said. The application that measured how much alcohol you could get per Swedish krona at Systembolaget worked, however, excellently…
Outside work: Likes to play the guitar and skateboard.

Headline:
With the future secured

Subhead:

HYKER always puts your security first. Even when you yourself forget…

Lead paragraph:

Smart cities and end-to-end cryptology. Does that sound strange and hard to grasp?
Not if you let Joakim Brorsson, one of the founders of HYKER Security, explain.

Body text:

In recent years, the digitalization has changed the way we work and live: We want to work from home. We no longer share flash drives with each other, instead we store all our data in cloud services. We want our refrigerator to tell us when we are out of ketchup and self-driving vehicles are already a reality.

As we become more and more digital, many have begun to pay attention to the importance of data security and that online security is a concept we not only need to think about but also practice. One company that early on developed a wide-ranging technology platform within data security, which is constantly improved through further research, and today is well established in the field is HYKER Security.

I met Joakim Brorsson, one of the founders of HYKER, to get some answers to complex questions about a hopefully secure but above all exciting technical future.

On a daily basis, Joakim Brorsson divides his time between research at Lund University in data security and cryptography with his role as Head of HYKER Labs. A corporate part of HYKER that do research and continues to work on the company's technical platform. All to ensure that it keeps its promises, among other things by investigating attacks on it. But Joakim Brorsson is also looking at the uses of this end-to-end cryptology in a future society, for example in a smart city.

Cryptology! How does one end up there?

– I do not know why or where it comes from but I have always had an interest in data security. I have always loved to break things to get the chance to examine them.

– In the beginning, it was probably the "hacker side" that interested me the most, but through that kind of thinking, you also automatically become interested in how to prevent intrusion.

How come you (together with Jonas Hallin, Jakob Folkesson and Emil Boman, editor's note) started a company like HYKER already during your time at university?

– We had student loans to live on and lots of spare time. It was a luxurious situation and we wanted to create things but also see how and if they worked out in "the real world" so already during our first and second year at uni we wanted to do other things than just study. However, the vast majority of our many projects were never completed. Maybe three of them were, of which HYKER was one.

So exactly *what* has HYKER created?

– I feel like a change of system came into existence around 2005. Before that, you only had yourself to trust. Trust that you did not lose the external hard drive where you had stored your information. But today, when we instead use cloud services for almost all storage, we store everything we previously had on our own private, little USB flash drive in the hands of a service provider.

– We share infrastructure with so many stakeholders that we cannot even keep track of it ourselves. Because of that, you constantly have to think about who you trust and keep in mind that the service provider usually owns the background code and consequently and as a result has access to all your information. HYKER's technology platform with end-to-end encryption eliminates all these problems. We make sure that only the person who sends the information and the person who receives it can read it. Not even we at HYKER have access to it. And that's exactly how it always should work!

– But, listen! It is important to point out that HYKER likes that we share common systems. So it is not at all about removing any of the benefits of cloud services. It is about how our technology instead allows people to regain some of their control.

Can you explain to me, a non-techie, in an easy-to-understand-manner, how HYKER's encryption technology works?

– HYKER's product is simply put an automated key sharing service. We are a bit like a box with a revolving door where there is no need to take a detour via a third party.

– Or if we put it this way, the technology with encryption keys has been around for a long time, like an ordinary piggy bank with a notch at the top where you can put coins or slips of paper with messages in it. Under the piggy bank there is a lid with a lock. I put a message in the piggy bank and send it via the cloud to the person who are supposed to receive my message. The difference is that the piggy bank I have sent has a lid with a lock that the

service provider does not have the key to. On the other hand, I have made sure that my recipient has the key so that when he receives the piggy bank, he can open it.

– A bit like the 18th century when, if you wrote a letter the only one who had a chance to read it before the recipient was the postman. We have abolished the postman too!

– I think it is important to point out that our technology is not really new, but we have updated the key management part of it. Our innovation is that the technology is flexible, simple and easy for all users to adopt and use.

In addition to the platform being user-friendly, HYKER deliberately has built a wide and general technical solution. Why did the company make this choice?

– Look at it as if our product is a great car. Other companies may have the same car but not as great and some of our clients want the whole car and in that case they might buy our customer portal, Konfident. But another client only needs a gearbox to be able to make their system top notch. In that case, we use the fantastic gearbox we already have and optimize it so it will suit their needs and solve their problems. Someone else needs the whole engine but another third client only airbags or a spark plug.

– This means that HYKER is always at the forefront. We do not develop for the sake of development but for the benefit of the customer. And to be able to work this way, we call all our customers once a quarter and ask for their input on what they need.

– Our basic technology is very extensive and wide-ranging and it can be used in so many different ways. Sure, we do not expand or broaden it that often. Instead, we go into all parts and develop them to perfection. We simply want to make our gearbox better and better and integrate new parts with fantastic quality instead of changing the color of the whole car.

Why is it so important for HYKER not to cheat when it comes to usability and user-friendliness?

– We know that shadow IT, when the staff at a company themselves resort to different solutions because the central IT system is too difficult to use, is common. As soon as a system becomes too cumbersome and unmanageable, people find shortcuts.

– This means that many IT managers do not have a clue how many different service providers actually have access to the company's data. So by offering a user-friendly solution, we can help companies avoid this problem.

– Like Konfident! That platform is actually built on the idea of simply "functioning". It is built to be applied and work on your own computer without any third party involved. Neither more, nor less.

There is a lot of talk about smart cities these days. What actually is a "smart city"?

– I also wonder that sometimes, but I guess the idea is that citizens should be able to take advantage of existing technology. "The city" shall be allowed to collect data for the benefit of the city and its citizens. If you discover that there is a lot of traffic or a lot of emissions on a street, you should, for example, be able to redirect the traffic.

– The idea is good, but you must be aware that there is always a danger when you start to collect information about citizens. The purpose is good, but do we really want everyone to be aware of our movements at all times, for example.

What can HYKER offer such a city?

– I would like to see a more general adoption of a changed mindset. That we think 'trust' instead of 'infrastructure'. That, we instead of being content with the fact that the link between A and B is secure, instead consider whether we think A and B should have access to our data. That we focus more on the stakeholders than the technology.

–We can do this, among other things, through less central control. Today you usually have a large server where everything is gathered and stored. "A single point of failure." That server becomes a very attractive target to attack. Instead of a central database with encrypted data that is heavily fortified, you should have intermediate channels. The data must be encrypted so that only those who are to use it, can access it. This is where HYKER can contribute.

– This can be applied in public transport for example. A bus sends its position to a database and a passenger who wants to know where the bus is and how long it takes collects the information. In this case, the system does not know who the recipient is for whom the information is to be encrypted and this is where HYKER's key sharing technology may become relevant.

How?

– Let’s go back to the piggy bank. In most cases with encryption, you create the key with someone already in mind, but that does not work if the recipient is a product or the waiting bus passenger.

– You could say that sender is active in retrospect. A adds a document to the piggy bank and sends it. However, A sends the piggy bank with a lid without a keyhole because A does not know who the receiver of the piggy bank is. Eventually, when the piggy bank reaches recipient B, he asks A to send the drawing of the keyhole so that B can create the keyhole himself.

IoT, Information of Things is also something that is much discussed. Where is HYKER when it comes to that?

– Oh, there are lots of uses and applications. Property owners who with our technology can check their heat meters. Residents that easily can enter their apartment building without a lock malfunction. As I said earlier: We have a general technology that can be used for a variety of user cases and we have actually already contributed our research and technology to an autonomous car in Singapore.

There seems to be an increased interest in digital security in society. Where did this come from?

– Snowden leaking the NSA data was clearly a watershed in 2013. After that, the interest in online security began to grow and with the number of such cases in recent years, it has increased.

– Small and large cases. Like when Target (American retail chain, editor’s note) sent out discount coupons on baby clothes which reached a father of a teenager before the daughter herself had told him that she was pregnant or the cyberattack that shut down large parts of Ukraine's electricity network during the Crimean crisis 2015. Not to mention the whole Cambridge Analytica scandal.

– In Sweden we have The Swedish Transport Agency's IT procurement, which led to foreign personnel who were not security-classified being allowed to work with the authority's information and the 1177 scandal where sensitive calls could be found completely open on an online server for several years. But above all, I think that the GDPR legislation had an impact when it came and people were obliged to report leaks.

– Through, among other things, the media pressure, it suddenly began to dawn on people that the internet and the reality are one and the same thing thanks to the digitalization. Our reality has been moved up on the cloud.

– Data provides power so we all simply have to start thinking more about potential threats and think about which people are the right ones to hand my data to? The phenomenon as

such, with the desire for increased security is inevitable and when it comes to this HYKER really can deliver.

So can HYKER deliver what the company promise?

– Yes, I really believe so and we also contribute to a worthy development by being research-focused. We are open with our results and constantly develop our already established technology. We are really serious about our research and doing it in depth.

– We want the knowledge to be out there and we put our greatest focus on the customer and the customer's actual problems.

– In addition, we have been up and running for a long time now and people can simply look at our reviews or which customers and financiers we have. For example, ABB on the customer side and Saab Ventures as a financier. The latter, which, for example, enjoys a great confidence when it comes to security technology in general. We are really certified by third parties!

– With HYKER's technology, the data is protected from producer to consumer and you can feel confident that you do not have to trust any intermediaries. There is no one between you and your recipient that you need to worry about!