at the National School of Government; head of the Information Assurance and Certification Schemes at CESG; head of the UK Common Criteria Certification Body; and head of Information Security and Accreditation at GCHQ.

Amanda Finch has specialised in information security management since 1991. In addition to her role as general manager of the IISP she works with the Information Security Forum (ISF) and the British Computer Society (BCS) to gain recognition for the discipline as a recognised profession. She has a Master’s degree in Information Security, is a Full and Founder Member of the IISP and a Fellow of the BCS. In 2007 she was awarded European Chief Information Security Officer of the year by Secure Computing magazine.

References
4. ‘Cyber-security Unemployment Rate Drops To Zero Percent’.


Fighting fraud on mobile networks

Andy Gent, Revector

In a recent comprehensive global survey of 150 telecommunications network operators, two issues were identified as the most significant threats to operators’ revenues. One of these has already cost operators an average of 20% of their termination revenues this year. The other has been a risk for many years but continues to threaten revenues on 80% of the networks surveyed. So what are these threats and what can we do about them?

Mobile targets

Mobile network operators have long been targets for fraud and revenue risk. The
nature of these companies’ businesses – providing huge volumes of communications services to vast numbers of people – mean these companies generate significant revenues. Wherever revenues are large, risk of fraud will be too.

Mobile service providers generate revenues in two ways. The first is by having their own subscribers that pay the company to access the networks they run and associated services such as voice calls, text messages and data usage. The second – known as termination revenue – involves transporting calls from other networks.

**Termination revenues**

Revenues from termination are relevant when a subscriber from network A wishes to call a subscriber on network B. Both networks are involved in delivering a successful call. Network A will have a direct relationship with the customer which generates revenue. Network A will then pay network B to connect the call to its customer.

This becomes infinitely more complicated when multiple networks are involved in the call – for example if the call is from the UK to Australia. This will pass through several service providers that will each take a small percentage of the call revenues. Termination revenues come from both calls in-country and roaming fees. One of the reasons why roaming costs have historically been high has been due to the number of companies involved in delivering the call – meaning more companies need a slice of the cake.

Telecommunications companies establish relationships with others around predictable calling patterns. For example BT may know that it needs one million minutes of calls to South Africa per month. It may therefore establish a relationship with a South African company to provide this. The issue comes when the unexpected happens, such as an earthquake in Cape Town. Now UK residents with relatives in Cape Town suddenly demand a lot more telephone time with the country. BT needs more minutes than it has. It is unlikely that its partner in South Africa can provide these – they are facing the same issue due to the increased volume of calls in and out of the country – so it will look to the open market for the minutes it needs.

**“Grey routes are so named because they are not provided by the telecommunications companies but by third parties or through fraudulent means. Typically, the grey routes come at a lower cost”**

Termination minutes are traded in the same way as other commodities. Exchanges combine minutes from multiple sources, bundle these together and sell them on. The issue is where these minutes come from. The bundles may well include ‘white’ routes – premium minutes provided by legitimate telecommunications companies. However, many will include so-called ‘grey’ routes. These are so named because they are not provided by the telecommunications companies but by third parties or through fraudulent means. Typically, the grey routes come at a lower cost than the white routes, but some telecommunications service providers may not know this or care.

The natural pressure on costs will mean that some telecommunications companies will end up using grey route minutes. The two primary threats to network providers’ termination revenues both come from grey routes.

**SIM box fraud**

SIM box fraud has been identified for many years as a threat to mobile network providers. It occurs where there is a differential price between the cost of routing a call in a country and the cost of terminating a call.

Imagine a network is offering free calls to others on the same network – not an unusual occurrence. At the same time, the value of terminating a call to that network’s customers is $0.05 per call.

As long as someone can procure SIM cards with the free call promotion, these can be loaded into a SIM box – a device that can house hundreds of SIM cards in racks and be connected to the Internet – to terminate calls. SIM boxes are readily available for purchase. The owner of the SIM box can then offer to terminate calls for $0.03 per call. The cost to the SIM box owner is close to zero (minimal costs for equipment, management and Internet) – the local minutes they are using to terminate calls are bundled with the SIM deal. The $0.03 per call is pure profit after the SIM cards and SIM boxes have been purchased.

While this sounds like a complicated scam, it can be exceptionally lucrative. A single SIM card being used in this way can generate $3,000 per month and hundreds if not thousands of SIM cards are in each SIM box.

Service providers can quickly find a large proportion of revenues are lost to SIM boxes. In some cases (where there is a particularly large delta between the cost of a local call in country and the value of terminating a call) operators can see up to 90% of termination revenues being lost. The nature of SIM box fraud is fairly transitory: fraudsters will pick the countries with the strongest opportunities to generate revenues quickly, sweep in and terminate calls for a month or two before the operator notices the revenue drop and takes action.

**Network losers**

The losers are primarily the networks – but there is also an impact on two other groups. Users of telecommunications services may find that call quality is noticeably lowered and additional functionality and services such as caller line identity can often be missing. In addition, many telecommunications regulators or governments take the issue of SIM box fraud seriously. The absence of revenues to telecommunications providers impacts the taxation that governments can raise from the industry.
دریافت فوری
متن کامل مقاله

امکان دانلود نسخه تمام متن مقالات انگلیسی
امکان دانلود نسخه ترجمه شده مقالات
پذیرش سفارش ترجمه تخصصی
امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
امکان دانلود رایگان ۲ صفحه اول هر مقاله
امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
دانلود فوری مقاله پس از پرداخت آنلاین
پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات