Slackspace

slackspace@elsevier.com.

Welcome to Slack Space, our regular column by industry insider Slack Alice, whose bounded duty is to inform, amuse and entertain, but not necessarily in that order.

'Slack Space: *A form of residual data, slack space is the amount of on-disk file space from the end of the logical record information to the end of the physical disk record. Slack space can contain information soft-deleted from the record, information from prior records stored at the same physical location as current records, metadata fragments and other information useful for forensic analysis of computer systems.' From the* Kroll Ontrack Glossary.

Now hear this

Now that the Skype (www.skype.com) VoIP service supports video, the Skype hype machine is playing up the alleged fact that the service's calls are secure.

Sure, encryption in Skype's virtual network is 256-bit AES, but what about calls that traverse the connection to landline or cellular networks?

For example, BT now allows the police and government agencies remote access to its network using a system known loosely as 'off-premises extensions'. With a myriad of UK agencies allegedly authorizing several hundred thousand telephone taps every year, BT engineers simply can't cope with the manual workload, so the system has to be automated.

And that's before we include the cable and cellular companies, who have more modern exchange equipment.

It's also relatively simple, (but illegal) to tap someone's phone line using kit you can pick up from any number of suppliers. These devices either clip over the wire from the user's phone to the local switch, or even transmit from inside the mouthpiece of the handset itself.

So, Skype VoIP to VoIP calls may be secure, but Skype to PSTN? I don't think so.

Charity begins at home

Reports suggest that APACS (www.apacs.org.uk) will shortly announce plans for most UK banks and financial institutions to give customers cheap two-factor authentication tokens such as RSA's SecurID to use when e-banking.

Sources say trials conducted by the likes of Lloyds-TSB, which had 30,000 customers in its program, have gone down a storm with customers and staff alike.

Banks will carry the cost of issuing tokens, expected to come in at under a fiver per customer. As these are the same banks that charge us around £30 to bounce a cheque, customers will appreciate their sacrifice.

No doubt the banks' magnanimity is prompted by the rule that requires them to compensate customers who are the victims of increasingly complex email and/or phishing attacks.

But there's likely to be a sting in the tail: expect that banks to pass liability for fraud to the customer if the devices are not used.

Sound familiar? It's the same buck-passing routine that the banks are using with Chip & PIN, which is, after all a form of two-factor authentication.

Since 14 February, retailers who allow customers to use a signature when they could have used a PIN are liable for any losses in connection with the transaction.

The banks will likely argue that it's all about risk management. Which makes stacking the deck in their favour OK, right? No wonder their profits are significantly ahead of the IT security industry, even when pro-rata-ed for income and turnovers.

MARA in the mire

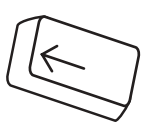
The 'gentlemen's rules' usually observed when IT security researchers discover a security threat may no longer be appropriate, judging from a squabble over the first PC-to-mobile virus.

By convention, IT researchers share information on new viruses and malware altruistically, no matter where in the commercial pecking order they rank. But MARA (www.mobileav.org), a non-commercial bunch of mobile malware researchers, has announced it will share details of the alleged Trojan with its members only.

So what? But there are some intriguing angles. Two of MARA's 12 members are said to have co-authored papers with Ratter, the pseudonym of one of the infamous 29A hacker group. According to the BBC, the two have also posted messages on the Vx Heavens (http://vx.netlux.org) underground virus information exchange.

Responding to criticism for its stand, MARA says it has no sympathy for commercial vendors, calling them a 'closed priesthood' that wants everything on their terms.

Still, there are signs that MARA is willing to negotiate with the brothers, if only on an ad-hoc basis. Common sense could even break out.



Anyone who wants to share their grumbles, groans, tip-offs and hot gossip with the author of Slack Space *should contact slackspace@elsevier.com.*