SCRAMBL

Bootstrapping Secure Channels of Communication Over Public Networks

Human Interaction Security Protocols (HISPs) offer an entirely new way of authenticating teams to create robust security where none exists. Originally developed to support battlefield communications, they now allow organisations to mitigate the risk posed by the growing volume of unsecured mobile business communications.

The need to secure radio frequency communications between teams in the field has long been recognised in scenarios where coalition working is required. But the growing volume of unsecured mobile business communications and the threat posed by hackers and malicious attacks means organisations today are increasingly vulnerable to data breaches, eavesdropping and other types of monitoring and surveillance by third parties.

Trends such as bring your own device (BYOD) continue to create new challenges for those tasked with securing corporate networks, devices, applications and data. Breaches can result in significant financial penalties, loss of Intellectual Property (IP) and reputational damage for those that fail to protect sensitive data.

The recent revelations around pervasive surveillance and privacy-invading mobile apps have raised the stakes further.

Growing threat posed by mobile phones

- 68% of organisations affected by mobile security breaches in the last 12 months
- Average cost of a mobile security breach is estimated at £28,000
- 42% of executives say a mobile security incident costs more than $250,000

The UK's Information Commissioner's Office (ICO) recommends that corporate mobile devices be protected using encryption software meeting current standards. It also warns that password protection alone is insufficient. In the US, a patchwork system of federal and state laws and regulations creates a significant challenge for organisations concerning data protection, with the Federal Trade Commission (FTC) being the chief enforcer should a breach occur.

Types of mobile threats and attacks

Mobile phones face a range of cyber security threats. They can be unintentional threats in the form of software upgrades or defective equipment that inadvertently disrupt systems, or targeted and untargeted threats such as such as botnets, hacking, and corporate espionage.

The biggest threat is posed by the nature of mobile devices themselves. Because of their small size and use outside the office, they can be easy to misplace and present valuable targets for thieves. If mobile devices are lost or stolen, it can be relatively easy for those with the right knowhow to gain access to the information they store.

Another major area of concern is data interception. This can occur when an attacker is eavesdropping on communications originating from or being sent to a mobile device. Electronic eavesdropping is possible through various techniques, such as man-in-the-middle attacks, which occur when a mobile device connects to an unsecured WiFi network and an attacker intercepts and alters the communication; and WiFi sniffing. The latter can take place when data is sent to or from a device over an unsecured (i.e. not encrypted) network, allowing an eavesdropper to 'listen to' and record the information being exchanged.

Mobile malware on the rise

- 16 million mobile devices worldwide have been infected by malicious software
- 25% increase in malware infections in mobile devices during 2014
- 65% of subscribers expect their service provider to protect both their mobile and home devices

Malware presents another common threat. Malware is the term used to describe malicious applications that are able to perform a variety of functions, including accessing location data and other sensitive information, gaining read/write access to a user's browsing history, as well as initiating telephone calls, activating the mobile phone's microphone or camera to surreptitiously record information, and downloading other malicious applications.

Even channels previously thought of as being secure are being exploited in new ways, with security experts warning recently that a mobile phone can be hacked within two minutes via text message. Analysts at Positive Research found that around 20% of 100 SIM cards of different origin had vulnerabilities, with SS7, the protocol that powers legacy mobile carrier networks said to be riddled with serious vulnerabilities undermining the privacy of mobile phone users.

Mobile security gap

Despite the rising threat of a mobile security breach or malicious attack, many businesses are failing to make adequate provisions to protect their valuable data. A report published by BT

Security in October 2014 found that more than 90% of large organisations (1,000+ employees) had corporately owned, BYOD or connected mobile devices in the field, yet only a quarter of them believed they had sufficient resources in place to prevent mobile security breaches.

The mobile phone security gap

- 15% of organisations have no mobile security (Information Security, 2014).
- 86% of workers said their employers couldn't remotely wipe their device's data. That includes if the device is lost or stolen (Cisco, 2013).
- Between 75% and 97% of apps – on both Android and iOS devices – have been hacked (Arxan, 2014)

Almost 70% of the 600+ organisations participating in the report said they had been affected by a mobile security breach within the previous 12 months, and around half of those had suffered more than four such breaches during that same period. On average, the cost of a mobile security breach was estimated at £28,000, with about one quarter of organisations reporting that their most significant mobile security breach cost them over £30,000.

The increasing level of risk has prompted wider interest in solutions that can ensure the confidentiality of communications via mobile voice and text. According to analysts at Gartner, several technologies for mobile voice and text protection have emerged as a result.

The market watcher defines such technologies as those that 'provide confidentiality and/or integrity of voice and text communications that originate and/or terminate on mobile devices, and are sent over mobile and wireless networks'.

Gartner also notes that while there has been a proliferation of solutions addressing consumer privacy concerns, there are few that offer comprehensive enterprise-level security that goes beyond simple payload encryption. What's more, it warns that encryption itself is not enough to ensure proper enterprise-level security. Not only do forms of cryptography vary from solution to solution; deployment can also prove difficult where additional hardware is required, while the user experience can be impacted by a solution's performance.

Fundamental challenge

Currently, much of the domain of computer security is based on networks of shared secrets, or relies on certification structures and public key cryptography. Standard cryptographic techniques are encryption, digital signature, message authentication codes, and distribution of secret keys and public-key certificates. However, these types of security architectures are rigid and unable to support situations where requirements are hard to identify upfront, or where flexibility is essential.

Indeed, the more informal the security setting, the less appropriate these types of conventional computer security infrastructures are. For example, one solution is to rely on trusted third parties such as Public Key Infrastructure (PKI), whereby a trusted authority issues certificates to validate the identity of a machine. Such infrastructures are expensive to maintain and there are examples of where they have been compromised – paralysing end user organisations and even governments as a result.

Moreover, developing group key management in highly dynamic environments such as wireless and mobile is difficult due to their inherent characteristics. On the one hand, mobile phones are constrained in terms of available computational resource; on the other, the mobility of group members increases the complexity of designing a group key management scheme. It is notoriously difficult to make such structures dynamic, because decisions about how parties are accredited and connections are made are fixed by the designers of systems rather than by those using them.

Given these multiple challenges, the ability to create ad-hoc security in mobile and team environments where none exists previously has proved a fundamental challenge. A natural alternative is to use the context in which parties sit to identify them. Also known as 'contextual authentication', the aim of this approach is to enable spontaneous security by allowing users to decide ad-hoc on what systems can communicate with each other without pre-existing structures or infrastructures of encryption keys.

Bootstrapping security

Over the past decade, there has been considerable effort to enable spontaneous security. One key aspect of this research has been the development of Human Interactive Security Protocols (HISPs). These are protocols for authenticating systems and exchanging encryption keys based on the comparison of authentication codes over an empirical channel – i.e. a separate channel of communication where an individual trusts the identity of the party they are speaking with, and where an intruder cannot forge the messages being exchanged.

The empirical channel can be trusted either because the participants are in close physical proximity (where they can see and talk to one another directly), or because it involves a real-time interaction that cannot be faked, such as speaking to an individual they know on the phone. HISPs use the empirical channel to overlay security onto an insecure channel – a process known as 'bootstrapping' – and by using knowledge that a user can only have gained via direct interaction with the system.

By combining a digital channel with an empirical channel, HISPs allow two or more parties who trust one another to bootstrap a secure network using no more than a small quantity of information – e.g. a short authentication code – passed over the empirical channel.

But there is an important difference between HISPs and other types of security protocols that bootstrap security using a password or authentication code: with HISPs, the authentication code does not have to be secret. Rather, their security is derived from the idea of commitment before knowledge, whereby protocol participants must be jointly committed to a small part of the authentication code before knowing exactly what the full authentication code will be. They reveal their respective shares in a second stage of the protocol run.

Commitment before knowledge

The concept of commitment before knowledge was borne out of a project funded by the UK Ministry of Defence, who approached Oxford University's Dr Bill Roscoe to help with addressing the significant security flaws in Bluetooth – the protocol used for short-range wireless communications.

Bluetooth employs a secret shared password that was subject to severe off-line password guessing attacks, whereby it was possible for an attacker to search for the password being used, deduce the main key that it created from the protocol, and then use that key to decrypt all the traffic that had passed between the devices in question.

To address this challenge, Dr Roscoe realised that if all legitimate parties were committed to a final value of a key they were going to be using for secure communication before actually knowing what that value would be, this would eliminate the possibility of an unauthorised party guessing it before a secure connection had already been established. Dr Roscoe and his team at Oxford University's Department of Computer Science subsequently invented the 'Hash Commitment Before Knowledge (HCBK)' protocol. HCBK makes use of a 'digest' function that allows users of portable devices that want to agree on the same data – such as their public keys, addresses and identities – to easily create a strong private key that is used to encrypt or decrypt subsequent communication.

In the absence of password and PKI, users of HCBK first exchange the public data over an insecure but high-bandwidth channel (e.g. WiFi or the internet) and then display a short and non-secret digest of the protocol's run that is generated by software on the user's device, which they will manually compare over an empirical channel to ensure that they have agreed on the same data – i.e. it uses human trust and interaction among users to prevent fraud and identity theft.

The device then checks that the value entered matches with its own version. When this is completed, all members raise their hands to indicate that the digest comparison is successful; or speak loudly if the digest comparison has failed. Should the digest values not match during the comparison between device users, this indicates the presence of an unauthorised party, because the communication channel used to exchange the digest value is an empirical channel where no one can alter or fake the origin of the digest value. In this scenario, the connection remains insecure and the protocol must be run again.

Proven on the battlefield, applied in mobile business

Due to its use of a second empirical channel as part of the authentication process, HCBK is demonstrably immune to man-in-the-middle attacks and is particularly suited to cases where either a high level of security must be created where none exists, or where additional security, such as enhanced authentication, must be provided between several parties in an existing network.

Having successfully completed peer review and been employed by the UK and US military on manoeuvres, further development and review of the HCBK protocol is on going with national security agencies. Over time, it is anticipated that HISPs such as HCBK will allow security to become more organic, based on human trust rather than on a rigid infrastructure that most users neither understand nor use properly.

However, HISPs are not intended as a replacement for PKIs and conventional forms of authentication, rather they will become common in areas where one or more humans have to form a pair or group of devices, because HISPs allow conventional security to be boot-strapped more efficiently and with less leakage of private information.

Crucially, the premise of HISPs is that users can control the security themselves and restrict the availability of sensitive information to a select few – making them a perfect fit for bringing military-grade security to unsecured mobile business communications. They eliminate the cost and risk associated with third-party infrastructure, and prevent hackers from exploiting vulnerabilities inherent in conventional encryption and off-the-shelf technologies.

SCRAMBL

Introducing Scrambl

A decade in development and validated on the battlefield, the HCBK protocol has been patented by OxCEPT Limited, a privately owned technology company with offices in London (UK) and California (US), who has invented an entirely new way of sending messages and files securely between authenticated team members and between authenticated teams.

Securing mobile device communications over public networks.

This first commercial application of OxCEPT's patented technologies is a smartphone app called 'Scrambl'. It is available on iOS and Android and is designed for any individual or organisation wanting to share private information with trusted third parties over their smartphones. It allows users to create a secure Virtual Private Channel (VPC) over any available public network in an instant, and serves users in sectors including:

- **Financial Services** – e.g. broker needing to share important information on a trade quickly and securely
- **Law Enforcement and Security Services** – e.g. IT manager looking to de-risk mobile communications in the field
- **Legal/Accounting** – e.g. CISO that needs to fill gaps in current security infrastructure
- **Oil and Gas** – e.g. project manager wanting to meet workers' desire to communicate securely

To create a VPC, a team leader runs the Scrambl app, which uses a precise piece of cryptography to generate a short one-time authentication code. The team leader reads this authentication code out to each member of the team, who must enter it into the app on their smartphone to confirm their identity. Team members know the identity of the team leader because they can see their face or recognise their voice.

Each team member is then able to send messages and share files securely over the VPC, which remains safely in place for a user-configured period of time without the need for re-authentication. All communication traffic is safeguarded using the strongest encryption standards available. This includes AES 256-bit and Diffie–Hellman key exchange (D–H). Received messages and files are stored securely within the Scrambl app and can be shredded after a configured period of time.

With its unique combination of authentication and encryption, Scrambl is totally secure and immune to ‘man-in-the-middle’ and guessing attacks. Crucially, the application doesn’t rely on any 3rd party physical infrastructure, while the data packets it transmits cannot be seen or intercepted by anyone. This makes Scrambl the world’s most secure way to send messages and share files on smartphones and provides organisations with a simple yet ingenious means of closing the mobile security gap.