Promptus INFOCrypt™
Secure access to a digital world.

Secure Videoconferencing

What you should know about the ease of intercepting VC

What you can do to protect VC via strong encryption

Frequently, participants of videoconferences discuss valuable information that can be of critical importance to an organisation's current plans and future prospects. Organisations using videoconferencing are often victims of industrial espionage by hackers, sometimes third party individuals hired by rival organisations to steal mission critical data.

For any proposed or existing videoconferencing deployment, an analysis of the type of meetings planned, should indicate the value of the meeting content to the organisation and……to external parties.

What damage would be caused if meetings were compromised: what loss of competitive advantage or confidentiality; what unintended divulging of plans; what irreparable loss of intellectual property?

The value and usefulness of organisational information has a direct relationship with how much time and capital an attacker is prepared to invest to intercept circuits.

Until recently, an attack on ISDN videoconferencing was considered to be much more difficult to achieve than a voice call intercept.

While an ISDN voice call can be intercepted for a couple of dollars, an attack on videoconferences requires a little more hardware, but not much more. Off-the-shelf components costing less than US$100 can be combined to build a device capable of intercepting audio from ISDN videoconferences. Even high-speed BONDING calls with G.722 encoding are as susceptible to attack as voice calls.

For an investment of less than US$50,000, an eavesdropper can procure all the necessary tools to crack a videoconference wide open - full audio and video interception - an investment that obviously makes sense for certain parties.

The Solution

Strong encryption has proven to be the right solution for protecting communications of all types.

Threat

Circuit testing devices for monitoring videoconferences are required to diagnose technical connection problems. These hand-held devices are freely available and are easily abused for illegal videoconferencing interception. To decrypt encrypted videoconferencing sessions, an attacker must not only decode the signal but must first decode the encryption algorithm. The key length of the algorithm is of great importance.

Here are some conservative estimates for the $-investment and time required for successful 'brute-force' decryption attacks under different key-length regimes:

Decryption Investment	***Estimated Time Needed for Decryption***		
	40-Bit-Key	*56-Bit-Key*	*112-Bit-Key*
US$1,500	*1 Second*	*17.5 Hours*	*5 x10^{13} Years*
US$15,000	*0.1 Seconds*	*105 Minutes*	*5 x10^{12} Years*
US$1,500,000	*1 Millisecond*	*1 Minute*	*5 x10^{10} Years*

(Source: Schneier, Bruce: Applied Cryptography, 1993 - adapted according Moore, Gordon for 2002)

DES Has Been Publicly Cracked

Even the best encryption algorithm can be cracked by trying all possible keys; the so-called 'brute-force-attack'.

The longer the encryption key, the more encryption possibilities exist and therefore, the harder the transmission is to crack. This means a hacker needs more time or faster (and therefore more expensive) computers to try all of keys.

The Data Encryption Standard (DES), now more than 25 years old, has only 56-Bit keys, encrypts data just once and is now widely recognised as being insecure. Several public trials have shown that, with modern PCs, the full set of key combinations can be checked all too quickly.

Triple-DES on the other hand, also referred to as 'strong encryption', is regarded as safe for the immediate future. It encrypts data three times over before transmission and has a key length of 112-Bit (frequently specified as 128-Bit). In combination, these features make Triple-DES dramatically, and exponentially, more difficult to crack than DES.

Videoconferences frequently handle enterprise-critical information. They are therefore a profitable target for competitive espionage and should be protected by strong encryption of no less than Triple-DES (also known as 3DES).

An attack on unsecured videoconferences is not much more complicated than that on a plain telephone line. The additional effort required to crack weak encryption (e.g. DES with 56-Bit keys) is not great; successful outcomes are entirely feasible and achievable.

Encrypt Well.....or Not at All

Once an encrypted network is deployed, everyone, including attackers know that the transmissions must be very important or sensitive.

If weak encryption is deployed, attackers are *attracted* to an *easily-decrypted* network.

The apparent security advantage of DES encryption can be turned into a major disadvantage; the network owner can be living with a false feeling of security and, potentially more exposed than having no encryption at all.

'AES' - The DES Successor

The risk of using short Bit encryption keys is well known and cryptographic experts are constantly searching for improvements. The official replacement for DES will be the Advanced Encryption Standard (AES) which is based on the Rijndael algorithm.

The National Institute of Standards and Technology (NIST) has elected AES as the official US Encryption Standard.

AES works with 128, 192 or 256-Bit key lengths, is exponentially more secure and nearly three times faster in operation, than Triple-DES. AES will be available with Babylon in December 2002.

Security Considerations

When planning to deploy videoconferencing networks for confidential meetings, here are some important aspects to address:

- Analyse your communication and protection needs - of what value is the information to your organisation?
- What value is that information to outsiders?
- Use strong encryption (112 Bit Triple-DES or better) - weak encryption presents only a small barrier to attackers.
- Encrypt all meetings to avoid 'highlighting' important sessions.
- Close backdoors (e.g. participants connected via phone add-on).
- Deploy stand-alone systems, which work independently from the videoconferencing devices.

The Solution

Babylon is the market-leading platform for encryption of ISDN and Serial-Line-Based communication lines.

Triple-DES (168-Bit real key length, 192-Bit incl. Protocol) and AES (128, 192 or 256-Bit) provides voice calls, videoconferencing, fax and data transmissions with high levels of security, safety and confidentiality.

Babylon is the only modular encryption device. Employing interchangeable interface cards, Babylon ensures flexibility of deployment, in-field expandability and application adaptability.

Since 1996, Babylon has been in use throughout the World in thousands of installations within banks, organisations, government and companies of all sizes.

Performance & Innovation

To work in real-time, strong encryption needs a hardware platform. Importantly, Babylon is a dedicated, external hardware-based encryption solution. Only specialised encryption chips, as used in Babylon, can guarantee the encryption/decryption speed critical for the uniquely computational-intensive, real-time and bi-directional application of videoconferencing.

Distinctly and physically separated from the videoconferencing system, Babylon and its configuration settings are not influenced or disturbed when the accompanying videoconferencing system is intentionally, or accidentally reconfigured. Babylon's design inherently combines these positive features with flexible interoperability between different videoconferencing system manufacturers.

Multipoint & Point-To-Point Calls

Babylon is capable of encrypting both multipoint or point-to-point videoconference calls. Ideal for Multipoint Control Unit (MCU) hubs, Babylon PRI provides safe and secure conferencing functionality at full PRI (Primary Rate Interface) speeds for up to 30 ISDN B-channels.

Suitable for videoconferencing terminals, Babylon 4xBRI can encrypt up to eight ISDN B-channels or, by using Babylon Basic, two ISDN B-channels can be secured. All Babylon products support bridge encryption hardware and multipoint software and is compatible with, and interoperable within, all network architectures.

Industry Acceptance

Ninety-five per cent of all videoconferencing systems utilise ISDN lines and Babylon is the market-leading ISDN encryption solution.

The leading videoconferencing equipment manufacturers, including PictureTel, Polycom, Sony, Tandberg, VCON, VTEL and Motion-Media have successfully tested Biodata Babylon devices with their videoconferencing systems and MCUs.

Key Exchange - Babylon Addresses a Potential Flaw

Why try all key combinations when you can get the original encryption key? Remote administration of videoconferencing systems is important, and if not implemented correctly, poses a real threat for both unintended disabling of encryption devices or interception of the key exchange.

Babylon makes use of recognised exchange algorithms for safe key exchange. Babylon also protects remote management sessions with strong encryption.

Central Management Software

With a central management tool, Biodata Babylon systems ensure customer friendly configuration.

This software application allows authorised administrators to centrally manage encryption keys, install new firmware and configure devices. Babylon devices feature SNMP and Syslog. Extensive monitoring capabilities about every connection provide network managers with real time system status.

Promptus INFOCrypt™
Secure access to a digital world.

Promptus InfoCrypt, Inc.
207 Highpoint Avenue
Portsmouth, RI 02871
USA

119 Willoughby Road
Crows Nest NSW 2065
Australia

www.infocrypt.com

info@infocrypt.com