Cellcrypt Voice Data Compliance Brief

January 2010

An Introduction to Policies, Best Practices and Legislation around Mobile Voice Security

Cellcrypt

Simplifying security in a complex world

Confidentiality, integrity and availability are integral to an effective and secure IT system. That's why successful organizations make it their priority to stay in the know.

Ensuring the security, confidentiality and privacy of communication is essential for organizations that deal with sensitive information. Once focused on conventional data, today's IT security manager must take into account the transfer of information in many different forms including email, on storage devices and increasingly in the form of voice traffic.

Organizations are motivated to stay up-to-date with their information security for a number of reasons. For some, it's led by the requirement to be seen to be implementing Best Practice or to meet relevant legislative requirements. For others, the driver is the specific risk of loss of information, whether the concerns relate to consumer safety or the need to protect against competitive espionage and the potential impact on both customers and reputation if such loss were to appear in the public domain. Whatever the motivation, staying on top of security threats requires remaining up to date with the preventative measures that are available now and into the future.

Today, IT infrastructure is routinely regarded as including data networks, data storage and both fixed line and mobile voice communication systems. Indeed, these areas increasingly overlap – for instance it may be possible to send email or access corporate information from a mobile phone or make a voice call from a laptop. As a result, vast improvements have been made to the internal security of most organizations' IT data. However, the safety of external voice calls, particularly over mobile, is often overlooked because it is regarded as being outside the organizations' direct control.

Mobile voice is increasingly regarded as vulnerable. In a recent survey by the analyst ABI, interviewing 250 US corporations in 2009, companies reported regarding mobile voice as being at least as vulnerable or even more vulnerable than email. However, while 98% of organizations had in place effective policies for managing their email, only 18% had effective measures to secure their mobile voice traffic.

To give this issue the attention it deserves, this article focuses on three simple facts related to mobile voice security. We also provide examples of the legislation, policy and best practices that regulate it.

Fact #1: Voice data is vulnerable to external attacks.

There is a growing demand to guarantee voice security of all competitive, executive and potentially sensitive communication – and it is not just legislation that's driving it. Whether or not legislation requires an organization to deal with this threat, most understand that it is in their best interests to assess this potential vulnerability.

Over the last 15 years, the vast majority of agencies and companies have adopted IP (Internet Protocol) technology for fixed communications and integrated appropriate security measures for internal communications. The resulting benefits have been significant. Through unifying different systems on to a single platform, CIOs (Chief Information Officers) now have much greater control over a network's internal features. The problem is that threats to external security have not been improved. Once data is passed outside of the system's secure perimeter, a CIO's influence is completely removed.

The problem is broader in mobile communications where the organization has no control over the security end to end. Particularly in the case of calls that transition from one carrier to another (e.g. international calling), no single body will give guarantees as to the security of the calls. Recent evidence, such as that reported in Jan 2010 in the Financial Times, suggests that the mobile infrastructure provided by carriers is coming under increasing threat and the security of calls is increasingly brought into question.

Fact #2: Existing solutions cannot single-handedly provide the necessary security.

While circuit-switched networks and fixed mobile integration can provide some internal security for organizations, they cannot single-handedly provide an end-to-end solution. Here's why:

Circuit-switched networks

External voice security relies upon an aging infrastructure managed by an array of different telecommunication companies. These circuit-switched voice networks, also known as POTS (Plain Old Telephone Service), were never designed to prioritize security. What's more, mobile networks are little better. The privacy features of both landline and mobile networks are only acceptable up to the standard of the average household user.

Fixed Mobile Integration

Significant strides have been made to completely overhaul the systems that organizations use to communicate with. FMI (Fixed Mobile Integration) technology presents an innovative model that delivers all forms of communication via a single platform design. Unfortunately, this technology is still in its infancy with almost all of the alternatives relying on existing, circuit-switched telecommunications networks.

Fact #3: End-to-end voice encryption guarantees the privacy of voice conversations.

To ensure the safety of voice data, more organizations are now opting for end-to-end encryption to augment their existing measures. How does this work? The technology is innovative, but the solution is simple.

The core to end-to-end voice encryption addresses the problem that the network is so complex, it is not possible to trust it. In end-to-end, the voice is encrypted at the phone itself

and travels over the open network to be decrypted at the far end. Because the encryption stretches from the microphone to the loudspeaker, there is no intermediate point where an intruder has access to the open communications channel. Intruders may be able to record the encrypted stream but that gives them no access to the important content. A further advantage of this method, is entirely untrusted networks (such as open WiFi connections) can now be used freely as there is no longer a requirement for the network to be secure.

The use of end-to-end encryption applies equally to landline and mobile conversations and conversations between the two. Such encrypted communications generally use IP technologies which allow tight integration between all voice communication systems and the ability to mix bearers to include landlines, mobile, satellite and other wireless technologies.

As the leading provider of secure mobile voice calls, Cellcrypt enables users to make encrypted voice calls via IP (Internet Protocol). Using popular smartphones, such as BlackBerry and Nokia Symbian, users receive government-grade encryption of voice calls. It is as easy to use as making a normal phone call and provides unparalleled voice quality and performance over mobile (cellular), Wi-Fi and satellite networks.

By providing end-to-end encryption, Cellcrypt protects against the risk of call interception along each stage of a call's journey. This includes the wireless network between mobile phone and base stations, fixed lines within and between carrier networks and Internet backhaul.

The voice of industry: legislation, policy and best practices

Numerous laws, policies and practices impact the IT security requirements of different organizations. Depending on the nature of your business, the penalty for non-compliance can be financially crippling.

Staying on top of the constant changes within the industry can feel daunting at times. To help navigate through the maze of different regulatory bodies and assorted acronyms, we've compiled a list of some of the more commonplace examples.

Keep in mind that while best practices are global recommendations, some of this legislation affects companies located in other jurisdictions (such as in the case of foreign companies listed on NASDAQ and NYSE).

Please follow the links to access a detailed breakdown of each legislation, policy and best practice that can impact your organization:

Legislation

FISMA	IT security legislation for US Federal agencies
GLBA	Privacy in financial services
HIPAA	Privacy in healthcare services
SOX	Accuracy in financial reporting for public companies

Policy

DoD 8500.1	US Department of Defense Information Assurance
CO SPF	UK Cabinet Office HMG Security Policy Framework
NERC CIP	Critical Infrastructure Protection from the North American Electric Reliability Corp.

Best practices

ISO/IEC 27002	Standard for implementation and maintenance of Information Security Management Systems
CAG	Consensus Audit Guidelines

FISMA *(Federal Information Security Management Act)*

Enacted in 2002, this is a United States federal law. The act recognized the importance of information security to the economic and national security interests of the United States.

The act requires federal agencies to develop, document, and implement programs to provide information security. This includes co-ordination between civilian, national security and law-enforcement communities. Moreover, it defines a framework for managing information security and requires federal agencies to develop a cyber-security strategy.

FISMA assigns responsibility to NIST (National Institute of Standards and Technology) to develop the appropriate standards to achieve its objectives. NIST's Special Publication, 800-53, section 2.4, defines the security protections that federal agencies must put in place to secure their external data.

FISMA Requirement	Cellcrypt capabilities
Cryptographic modules must be FIPS 140 approved.	Cellcrypt Encryption Engine is currently undergoing CMVP (Cryptographic Module Validation Program) at NIST for FIPS 140-2 validation.
NIST Special Publication, 800-53, section 2.4, Security Controls in External Environments.	Lowers the risk profile associated with voice communications when using an external telecommunications provider.

GLBA (*Gramm-Leach-Bliley Act*)

This law was introduced in the United States in 1999. It mandates the need for financial service institutions to protect information against threats to security and data integrity.

The act deals with three main areas, Financial Privacy, Safeguards and Pretexting Protection. According to the 'Safeguard' section of the act, there is a duty to protect against the possibility of eavesdropping over telecommunication networks. Financial institutions are responsible for securing all information which could result in substantial harm or inconvenience to their customers.

GLBA Requirement	Cellcrypt capabilities
Safeguards Rule: Disclosure of Non-public Personal Information (15 U.S.C. § 6801)	Provides security, confidentiality and protects against unauthorized access to customer information over voice calls.

HIPAA (*Health Insurance Portability and Accountability Act*)

This act came into effect in 1996 in the United States. An act in two parts, it includes maintaining the privacy of personal information.

Included in Title II of HIPAA is a set of rules known as Administrative Simplification. This requires the Department of Health and Human Services to draft rules that create appropriate standards for the use and dissemination of health care information.

Within the Technical Safeguards of the Security Rule, focus is placed on protecting communications that contain PHI (Protected Healthcare Information). According to HIPAA, information systems housing PHI must be protected from intrusion. When information flows over open networks, encryption must be in place.

HIPAA Requirement	Cellcrypt capabilities
Security Rule: Technical Safeguards mandates encryption if PHI is transmitted over open networks.	Provides end-to-end encryption to PHI and protects against unauthorized access to covered entities.

SOX (*Sarbanes-Oxley Act*)

This act, dating from 2002, is also known as the Public Company Accounting Reform and Investor Protection Act. It is designed to improve standards for US public company boards, management and public accounting firms.

SOX requires the Securities and Exchange Commission to implement rules in order to comply with the mandate. The main focus of the law is to ensure accuracy in the reporting of financial information.

There are eleven separate titles included in SOX that describe specific conditions for financial reporting. Section 404 requires management and the external auditor to report on the adequacy of the company's internal control over financial reporting.

SOX Requirement	Cellcrypt capabilities
Section 404: Assessment of internal controls. Period-end financial reporting control.	Provides additional controls over period-end financial reporting process by protecting voice communications of the management team and its auditors.
Section 404: Assessment of internal controls. Fraud risk assessment control.	Provides a secure voice infrastructure for the auditors to perform a fraud audit including analysis of management override of controls and the company IT system.

DoD 8500.1 (*Department of Defense directive 8500.1*)

Introduced in the United States in 2002, this directive establishes a policy for information assurance.

Section 4.26 describes the level of protection that must be given to all military voice transmissions. A level of security appropriate to the classification or sensitivity of the information in question should be maintained at all times.

DoD 8500.1 Requirement	Cellcrypt capabilities
Section 4.26. All military voice radio systems, to include cellular and commercial services, shall be protected consistent with the classification or sensitivity of the information transmitted on the system.	Protects up to Controlled Unclassified Information (CUI) communications over cellular, satellite and Wi-Fi from unauthorized access. Encrypts voice communications end-to-end with AES 256bit.

CO SPF (*Cabinet Office Security Policy Framework*)

This policy represents a new approach from the UK Government's Cabinet Office to protective security and risk management. It takes and adapts much of the Manual of Protective Security (MPS) and the Counter-Terrorist Protective Security Manual (CTPSM). It demonstrates the UK government's need to focus on the protection of citizen records. The last of its four tiers contains detailed technical standards, supplementary policy and guidance. It also provides the tools to support the core policy and principles.

Information security compliance is now audited as part of the annual Government internal audit and control process, under advice from the UK's National Technical Authority on Information Assurance. The Security Policy Framework is aligned to The International Standard for Information Security Management Systems (ISO/IEC 27001).

SPF Requirement	Cellcrypt capabilities
SPF Policy 4 Requirement 41 Departments and Agencies must manage the risk posed by eavesdropping.	Protects up to Unclassified But Sensitive (UBS) communications over cellular, satellite and Wi-Fi from unauthorized access. Encrypts voice communications end-to-end with AES 256bit.

NERC CIP (*North American Electric Reliability Corporation Critical Infrastructure Protection*)

A set of reliability standards designed to protect IT systems that control North America's bulk electric systems.

This Critical Infrastructure Protection (CIP) from the North American Electric Reliability Corporation was developed in 2006. At that time, the Federal Energy Regulatory Commission (FERC) made the CIP standard mandatory for operators of bulk-power systems. Specifically, CIP 005 mandates requirements from control and protections of electronic security perimeters and its access points.

CIP Requirement	Cellcrypt capabilities
CIP 005-2 Section R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.	Prevents unauthorized access to the voice communications systems from non-authenticated users. Protects the contents of voice calls by means of end-to-end encryption.

ISO/IEC 27002

Originating from the British Standard 7799, this provides best practice recommendations on information security management.

ISO/IEC 27002 was ratified in 2007 for use by those responsible for Information Security Management Systems (ISMS). It addresses the confidentiality, integrity and availability with a comprehensive set of management controls.

ISO/IEC 27002 Requirement	Cellcrypt capabilities
Section 10.3.2 Encryption shall be applied to protect the confidentiality of sensitive or critical information.	Provides end-to-end encryption to voice communications to the management team and board of directors to protect against interception of critical information.
Section 12.3.1 Policy on how to protect information on mobile devices and across communication lines.	Provides end-to-end encryption across cellular, satellite and Wi-Fi communications lines to protect against unauthorized access of voice calls.

CAG 2.1 (*Consensus Audit Guideline)*

Developed in 2009, this guideline is comprised of information security measures and controls.

CAG was developed by consensus between SANS, US Federal Agencies and the wider IT security community. The core principle of CAG is a prioritized baseline of defense assuming finite resources available for protection. CAG is mostly focused on practical protection of IT systems and deals with currently known high-priority attacks, as well as expected risks.

CAG 2.1 Requirement	Cellcrypt capabilities
Critical Control 14: Wireless Device Control. Section 14.8 Config/Hygiene: Organizations should ensure all wireless traffic leverages at least AES encryption used with at least WPA2 protection.	Provides end-to-end AES 256bit encryption to voice communications over cellular, satellite and Wi-Fi.
Critical Control 15: Data Loss Prevention. Section 15.5 Config/Hygiene: Data should be moved between networks using secure, authenticated, encrypted mechanisms.	Provides end-to-end encryption across cellular, satellite and Wi-Fi communications lines only to authorized users to prevent unauthorized access of voice communications.

Europe & Asia Pacific
222 Regent Street
London, W1B 5TR
United Kingdom
tel: +44 (0) 2070 995 999

North America
One Freedom Square
11951 Freedom Drive, 13th Floor
Reston, VA 20190
United States
tel: +1 703 251 4887

530 Lytton Avenue
Palo Alto, CA 94301
United States
tel: +1 650 617 3219

Latin America
7791 NW 46 St, Suite 104
Miami, FL 33166
United States
tel: +1 786 999 8425

Middle East & Africa
JLT Lake Plaza
Unit 1504, P.O. Box 38255
Dubai, UAE
tel: +971 (0)4390 2908

info@cellcrypt.com
www.cellcrypt.com

Cellcrypt