Security & Encryption

Introduction: the importance of encryption

Encryption for security is thousands of years old. With the invention of telephone networks, it was inevitable that forms of encryption would be developed to keep communications secret. Radio networks made encryption critical, since the transmissions were easily intercepted.

Governments, militaries, and banks have employed encryption for decades. While encryption equipment was clumsy and expensive, those transferring critical data and voice had no other option.

Historically, the act of intercepting voice calls ("wire tapping") required a physical connection, often near the source, which made the interception of voice calls difficult. So there was a balance between risk and cost.

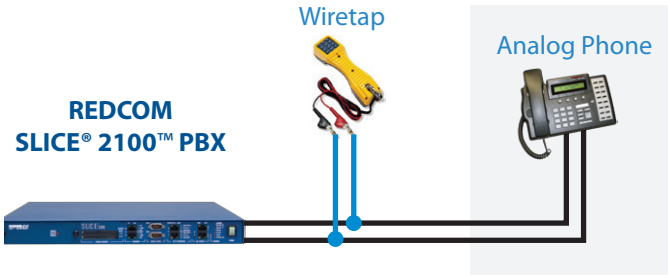

Figure 1. Traditional wiretaps generally required a physical connection, but with VoIP the wiretap may be on the other side of the world.

Voice over IP (VoIP) however, has ushered in a new level of concern for loss of secrecy. The protocol itself is publicly available, making it easy to hack. With worldwide interconnected networks, spies can tap into the "connection" from anywhere. Even the tools to find and intercept calls are free! No longer can any business or government agency take the risk of not employing encryption; luckily, the cost of encryption in modern IP networks is very low.

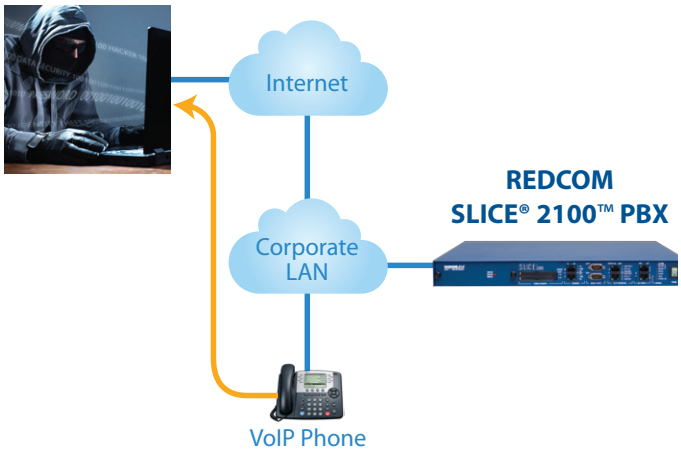

Figure 2. Any network attached to a public IP network can be hacked.

Part 1: The Basics of Encryption

This treatise will guide those who are not IT or VoIP experts through the confusing world of securing their networks with encryption.

It is often easy for a hacker located anywhere in the world to target a desk or mobile phone user connected to a VoIP network and intercept and record the conversation. While this type of crime is commonly reported to be committed by governments, what is not often reported (though also happens every day) is corporate espionage of VoIP networks. Many of these intrusions go undetected.

How easy is it? So easy a schoolboy can do it. With VoIP software programs, spies (and children) can find networks and locate VoIP connections. Free, downloadable programs such as Wireshark® make it easy to see the digitized voice, to export it to a recorder, and even listen to a conversation in real time.

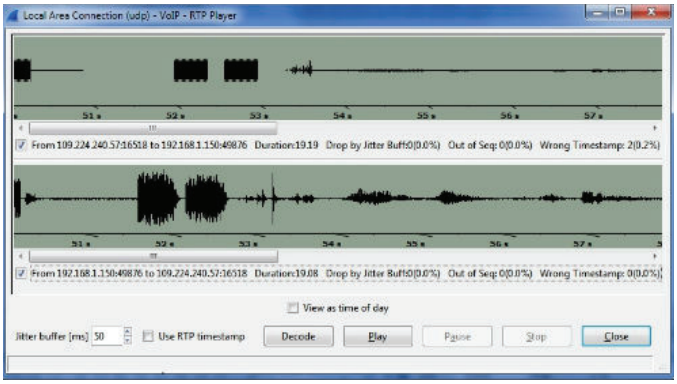

Figure 3. Free computer software enables hackers to analyze networks, locate targets, and record both voice and data.

The Basis of Encryption: Algorithms and Keys

Encryption is the process of changing a message so that it cannot be easily read or deciphered. With digital (including VoIP) encryption, the series of 1s and 0s that make up the message are scrambled so that they do not resemble the original data packet and are not easily deciphered. This process uses mathematical algorithms to produce the encrypted data.

The problem with algorithm encryption alone is that it can be decrypted and intercepted with computers. To make the decryption far more difficult, a different base key is used for each call when it is subject to the encryption algorithm. This results in different output for each call, even though the same key is used. Key lengths vary greatly depending on the encryption algorithm used. They can range from 128-bit to 2048-bit or more. For best results, use a combination of a proven secure algorithm and a key length that minimizes the likelihood of compromise via brute-force computing. Even then, there are concerns that governments with billion-dollar budgets for computing resources can compromise this encryption.

Popular encryption algorithms include:

- SCIP: Secure Communications Interoperability Protocol
- AES: Advanced Encryption Standard
- Suite B: US government group of encryption algorithms which includes AES

Encryption Architectures

There are two main architectures for implementing security encryption: End-to-End and the Secure (or non-secure) Enclave.

End-to-End encryption means that the user devices (phones, tablets, etc.) each have their own encryption capabilities, either built-in or just outside of the device. Both ends of a call (that is, both devices) must have matching encryption; if they do not the call will still work, but it will not be encrypted.

Figure 4. Typical encrypted secure end-to-end VoIP call.

Figure 5. Even though one device is secure, the other is not, so the call will not be encrypted.

The problem with end-to-end encryption has historically been that any device or service *must* have a matching encryption. This was often expensive just for end-to-end scenarios, but becomes technically difficult and very expensive to encrypt trunk-level calls, such as those to Conference bridges and Automated Attendant services. Typically most core equipment does not offer an internal

encryption interface; the solution is to front-end the device with encryption and keep the entire package in a room or enclosure that is considered trustworthy, and any humans with access are also considered trustworthy. This is called a **Secure Enclave**.

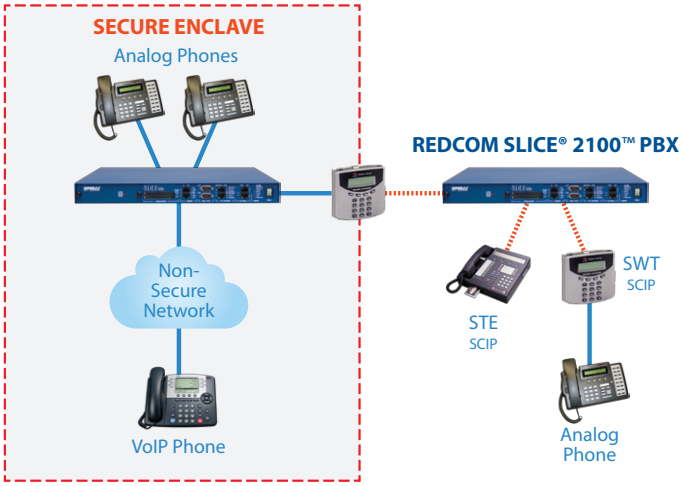

Figure 6. Secure Enclave is a building or room which itself, and everything in it, is considered secure even though the equipment inside may be non-secure equipment.

Part 2: Encryption Protocols and Devices

By far the greatest users of legacy (i.e. before VoIP) encryption were military. Today though, open and free encryption standards for VoIP have made highly secure communications available to many VoIP users.

REDCOM's solutions support both legacy and VoIP encryption protocols and devices, an important ability since most networks are not all legacy or all IP, but hybrid. In this case, it is imperative that the core intelligent network nodes (switches) are capable of translating between the various encryption methods.

Legacy Encryption

Legacy encryption refers to non-VoIP encryption methods, and includes encryption for analog telephones, and military encrypted devices such as the analog STU and analog or ISDN-based STE.

Encryption limited to US military-licensed use is categorized as "Type 1" encryption. Typical legacy devices include:

- SWT: Secure Wireline Terminal from General Dynamics
- STU: Secure Telephone Unit
- STE: Secure Terminal Equipment from L3
- vIPer: Secure VoIP phone from General Dynamics
- OMNI: L3 device compatible with SWT

Some encryption devices are similar to the US military Type 1 encryption, but the encryption algorithms are "de-tuned" to a lower standard and are categorized generically as "non-Type 1" encryption. A common non-Type 1 commercial line-side encryption device is General Dynamic's Sectéra BDI.

All of the above devices listed are intended for end-to-end (i.e. phone-to-phone) encryption. REDCOM supports interfaces for these devices such that encryption and decryption can be utilized to deliver secure access to REDCOM Unified Communications features such as Conferencing.

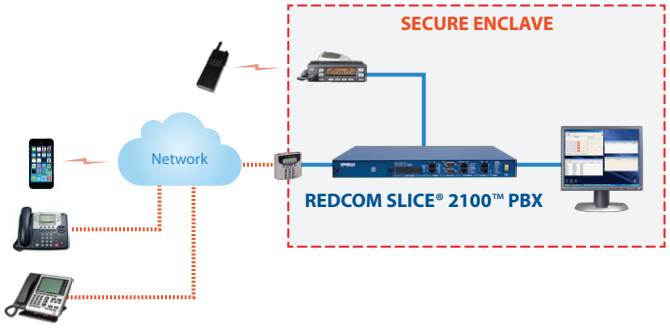

Figure 7. REDCOM Secure Conference server for encrypted VoIP, secure, and radio users.

VoIP Encryption

As previously noted, VoIP communications are easily intercepted. However, the high computing power available on small chips and the publication of open standards has made VoIP encryption both imperative and relatively inexpensive.

VoIP communications differ from legacy communications in that VoIP actually has two "paths" for communications: one for call set-up, and one for the actual voice or data. Neither are secure by default, meaning hackers can obtain phone

numbers, URLs, IP addresses, and listen to — and even manipulate — the voice conversation.

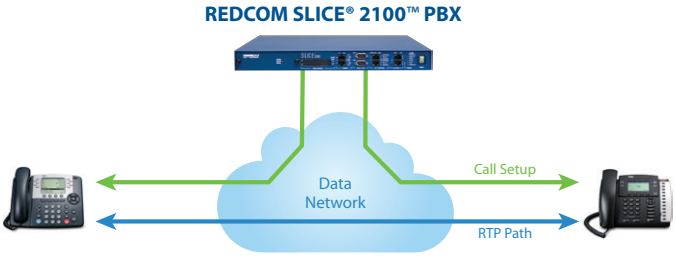

Figure 8. Non-secure (not encrypted) VoIP call showing separate call setup and voice routing.

VoIP call setup information is, by default, not secure when using typical industry-standard protocols such as SIP. Transport Layer Security (TLS) can add a layer of security to this signaling. The voice payload (as well as video and data) of VoIP is conveyed using Real Time Transport Protocol (RTP), which has an encrypted version, Secure RTP (SRTP). Thus, the combination of TLS and SRTP encrypt both the voice and the call set-up for VoIP calls.

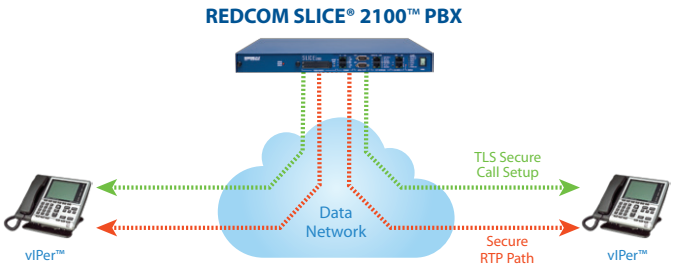

Figure 9. Secure VoIP call with both call setup information and voice encryption.

IPSec

VoIP communications contain many "layers" with upper layers being encapsulated into the lower layers. TLS and SRTP are upper layers of encryption and secures an individual data stream between two endpoints. IPSec is a lower layer encryption, and secures all data streams between its endpoints. Think of TLS and SRTP as trains with the doors locked, and IPSec as a long tunnel for the trains, completely secured.

IPSec is typically provided by networking devices, such as the Brocade® vRouter. It is ideal for IP-based virtual private networks. Some, but not all, devices (phones) support IPSec, so the link between the phone and IPSec-enabled router is not secure. In this case it is wise to use TLS and IPSec in the network.

It is important to note that SRTP, TLS, and IPSec encrypt not only voice, but data, video, and instant messaging as well.

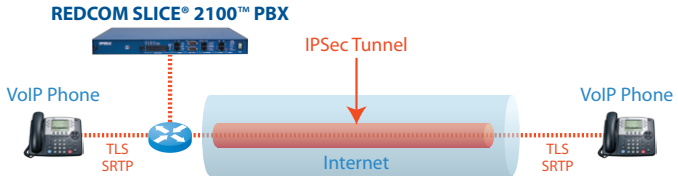

Figure 10. IPSec Tunneling adds an additional level of security for calls transiting non-secure networks

Mobile, Radio, and Wi-Fi Encryption

Intercepted radio transmissions have won (and lost) wars. Any radio-transmitted signal is easy to intercept, and as a result mission-critical radios have enjoyed encryption for years. It must be realized that the term radios includes not only military radios, but also handheld radios, mobile and smart phones, microwave, Wi-Fi, and even satellite phones.

Today, many radios include encryption, such as WEP and WPA2 on commodity Wi-Fi routers. This encryption though only encrypts between the radio devices (for example, between the Wi-Fi router and the laptop), not through the remainder of the network.

Given that radio (especially Wi-Fi) is the easiest transmission to capture, it is imperative that any VoIP traffic going over radio is encrypted end-to-end.

V.150.1 for Proprietary Encryption Devices

Though powerful commercial encryption equipment is commercially available, recent world events have cast doubt on the true security offered by this equipment.

The solution for those untrusting of commercial encryption products is to design their own. While this is not terribly difficult to do, the problem lies in that networks may not be able to successfully pass modem-based proprietary encryption. However, this problem is mitigated by the V.150.1 protocol supported in REDCOM's HDX and SLICE 2100 platforms, allowing reliable transport between encryption devices across an IP network.

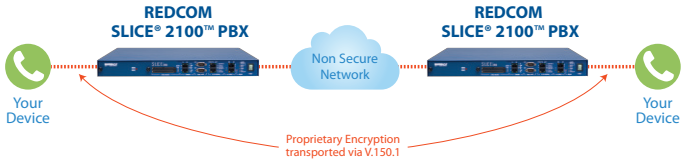

Figure 11. Create your own encryption with the V.150.1 protocol

Network Security by Design

Beyond encryption, the poor design of some VoIP networks may increase their susceptibility to attack. Security deficient designs can include centralization architecture and/or substandard equipment.

Distributed vs. Centralized architecture

The trend to "save money" by using one large VoIP softswitch (centralized) rather than many smaller ones (distributed) simply makes it easier to locate a targeted victim. In simple math, it's harder to find a particular target in one of twenty switching cores than it is to find the target in one large one.

Figure 12. Centralized network, susceptible to single-point of attack.

Distributed networks, by their very design, are also more resilient. Networks that rely on one softswitch core have one single point of failure; if it is attacked and fails, the whole network fails. On the other hand, with a distributed network consisting of many smaller softswitch cores, attackers must disable every single core in order to effect the same total failure.

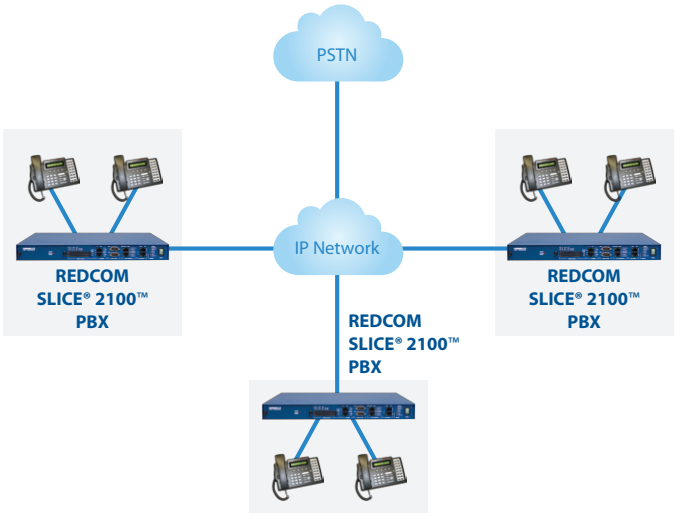

Figure 13. Distributed network provides redundancy and resilience.

Distributed architectures are used in PC networks, so why would anyone do the exact opposite in VoIP networks?

REDCOM's products are scalable from a small number of users to thousands. REDCOM systems make a variety of options available to network designers, but those truly focused on security will deploy many small systems rather than one large one.

Firewalls and SBCs

Most people know that a firewall can block certain types of intrusions. However, traditional firewalls are deficient for VoIP networks because they are unable to recognize VoIP traffic and apply proper security measures. As a workaround, administrators often create static firewall policies to allow all traffic for selected sources and destinations, ultimately making the network more vulnerable and limiting flexibility.

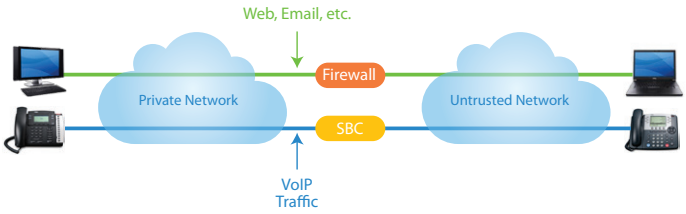

Figure 13. Private IP networks carrying voice should be defended by both a Firewall and SBC.

For complete protection, networks require both a firewall and a Session Border Controller (SBC). Each serves different functions to analyze IP traffic data and protect the network. SBCs tend to be more intelligent concerning the voice and video applications of the network, and thus can better analyze data and stop attacks and fraud.

Conclusion

At no time in the history of mankind have communications been so susceptible to malicious attacks, fraud, and eavesdropping. VoIP networks are particularly vulnerable. The internet knowledge base — along with free tools for analyzing and listening — have proven time and time again that almost anyone can breach an unsecured network. Thus encryption is no longer an option; it is absolutely mandatory.

Developments of IP security mechanisms and devices have made encryption inexpensive and relatively easy to deploy. Given that many networks are in a state of migration (not wholesale replacement), gateways and core switches must be capable of supporting both legacy and IP encryption.

REDCOM's product solutions bridge the divide between secure and unsecure networks, and secure legacy and secure IP. With REDCOM's products, networks can enjoy Unified Communications by capping the existing network without replacing it, and moving secure communications to REDCOM's IP-based platforms. Equipped with a vast variety of landline, VoIP, radio, and secure interfaces, REDCOM products build the bridge that enable network transformation while offering a secure setting for business continuity.

Security Features by Platform

Security	SLICE	SLICE 2100	SLICE IP	HDX	Sigma Core
VoIP Encryption		✓	✓	✓	✓
AES		✓	✓	✓	✓
V.150.1		✓		✓	
TLS		✓	✓	✓	✓
SRTP		✓	✓	✓	✓
Radio Gateway	✓	✓		✓	
Firewall					✓
Distributed Network	✓	✓	✓	✓	✓