Introduction

What is Alarm over IP?

Alarm over IP is the ability for security and fire alarm systems to transmit alarm signals over IP networks such as the Internet, private local, and wide area networks.

Before the advent of Internet-based alarm communications, telephone-based alarm systems were the most cost-effective option for the majority of installations. In most instances, no other affordable alternative for remotely supervising alarm systems existed.

However, the growth of the Internet has presented a new cost-effective option. In fact, not only is Internet-based alarm communications a functionally equivalent alternative, it also offers numerous advantages over telephone-based systems.

But what exactly is Internet-based alarm communication? More succinctly referred to as "Alarm over IP," this paper provides a very brief introduction for security professionals.

A simple way to understand Alarm over IP is to understand what it is not: Alarm over IP is not a telephone-based system for alarm communication. In very simple terms, Alarm over IP uses the Internet instead of telephone lines to transmit and receive communications.

Although the Internet was invented in the 1960s, it wasn't until recent years that its reliability and robustness improved to the point where it could replace landline telephones. Early systems were vulnerable to poor connection quality and frequently lost data. However, today's modern systems can provide the same stability offered by mobile or landline calls.

To understand how Alarm over IP works, it is useful to compare how alarms are transmitted using traditional PSTN (Public Switched Telephone Network) systems. Alarms on PSTN systems use traditional circuit-switched telephony. In such systems, a dedicated line is established between two points during the alarm call. The PTSN is based on copper wires carrying analog data over the dedicated lines.

In contrast, Alarm over IP uses packet-switched telephony. Using such systems, data travels to its destination in individual network packets. Instead of using a dedicated line between the two points as in PSTN systems, the network packets are guided to their destination with the help of routers, switches and other network infrastructure that are beyond the scope of this paper. Individual packets can follow different paths to the same destination.

Traditionally, the PSTN was selected for use in alarm systems for its familiarity and ease in regards to use, configuration, setup and maintenance. However, drawbacks include the cost of maintaining a dedicated line and the lack of scalability. Also, in recent years, many of those analog signals on the PSTN are converted to digital signals using various signal compression and de-compression algorithms, which can cause telephone alarm signals to be distorted and unreadable at the central station.

Scalability in Alarm over IP systems is a major advantage, as are the cost savings and reduction in modem hardware. Although quality and reliability issues were commonly cited as a major disadvantage of Alarm over IP, today's networks have enjoyed significant improvements to the point where performance is no longer an issue.

Benefits of Alarm over IP

Alarm over IP systems were designed to overcome many of the operational shortcomings of telephone-based alarm systems. Today's Alarm over IP systems offer several important benefits to both end-users and installers.

Higher speed

Telephone-based alarm communication typically experiences a delay of up to several minutes before an alarm signal can be relayed. This is because the system must make a telephone call, including dialing a number, waiting for an answer from the central station receiver and then relaying its message. In contrast, IP alarm communication is virtually instantaneous. Although a few minutes may not appear to be significant, it is noteworthy that sophisticated criminals can disable many alarm functions in only a few seconds. From this perspective, every second of operational efficiency counts. The higher speed of IP is also very appealing for remote maintenance and programming of the alarm panel.

More convenience

An IP communicator does not interrupt the phone line. This is especially important in an emergency situation where the end user is trying to use the phone to contact authorities. It is also important for small businesses that share their business phone with their alarm system. Interrupting a phone call can mean upset customers and potentially lost business.

Lower Cost

For those end users who previously used a separate phone line for their alarm system, Conettix IP can be used to convert dialer based panels to IP as the primary communication path – eliminating the monthly phone line costs.

Customer retention

A customer who eliminates or switches their standard telephone to VOIP (Voice over Internet Protocol), then suddenly loses the operation of their alarm system will be upset. IP communication allows the installer to retain this customer and solve their problem quickly.

Higher security

In telephone communicators, connections are tested to ensure proper system operation. However, the frequency of testing can be less than adequate, with several days between tests. Criminals can easily exploit this deficiency, plotting their crimes in between tests when they can sabotage the system. IP alarm communicators are supervised more frequently than standard telephone communicators. If the connection is lost, the central station knows almost immediately. The data transmitted is also authenticated and can be encrypted to prevent intercept attacks. Because PSTN based communications are not authenticated or encrypted, they are susceptible to being disabled by recording and replaying signals, or substituting the alarm panel with a fake.

Bosch Conettix IP Secure Communications:

Conettix IP has several aspects that provide higher security for Alarm over IP Communication:

- **An account database in the receiver for all network accounts**
  This is a unique and very special feature of the Conettix IP receiver that enables the following:

  - **Individual Supervision and ACK time** – Conettix IP allows each individual account that is transmitted to the receiver over IP to have its Supervision and Acknowledgement time adjusted in seconds (not just whole minutes). With this flexibility, accounts that have latency issues such as satellite transmissions can be adjusted to compensate for this latency. Other manufacturers receive the next supervision time from the panel with each transmission (typically in minutes) and have a system-wide fixed time to wait for the acknowledgement from the receiver. In a situation as described above, the receiver cannot be configured to compensate for these types of issues. The Conettix IP receiver is highly optimized for these situations.
  - **Ability to verify account status** – Conettix IP allows the user to look at the status of all IP accounts at anytime with the click of a button. You can see the state of the IP account and whether it is online or offline and when that last change of state took place. This is very important in the situation of switching from one operating receiver to another for an emergency, disaster recovery situations, or simply a UL test of the backup equipment. A typical problem in backup situations is that a panel fails to check in during the switch over of equipment. Conettix IP will allow you to verify that the network accounts are all online on the backup receiver with the click of a button. Other manufacturers rely on the panel checking in to establish that supervision. If a panel were to fail to check-in during this switch, they would not be aware that a panel is offline and not being supervised. This is because the receiver is not aware of what accounts are supposed to be supervised. If their receiver is not aware that a panel has stopped checking in and the main receiver that was supervising it is down, the operator in the central will not be aware of this either. The Conettix IP solution provides this fail-safe check in.
  - **Ability to disable individual accounts** – Conettix IP allows individual accounts to be disabled so that the receiver will not respond to messages coming from this account. This can be very helpful in a runaway situation where the panel is simply sending hundreds of signals. There have been reports of other manufacturer's panels in a runaway condition and the only way to stop the signals until a technician was on site was to submit an IT request to block the address. The Conettix IP solution allows this feature, similar to blocking an incoming phone number in a receiver or phone switch, but without the need for an IT request.
  - **Only processing data that the receiver is expecting** – If an account is not in the ConettixIP receiver, or if data isn't in the proper format, the receiver will not spend time processing and responding to the message. This is especially important in the prevention of Denial of Service Attacks. A common denial of service attack occurs when a hacker opens multiple TCP sessions with a device, rendering it unable to receive additional messages. If someone were to attempt to send packets of data to a Conettix IP receiver, it will not respond back to this data unless it is in a valid format and is a valid account that is enabled in the receiver. In this situation, you would not want to respond to packets that could be from a hacker or other attack coming from the network. This would only alert them that there is something there and it is responding. In the case of TCP, the connection would be created before the receiver would even be aware that it was not valid data. This is where a Denial of Service attack can occur. The Conettix IP receiver does not respond to any of these requests, which allows it to remain unseen so it is not vulnerable to Denial of Service attacks.

- **Authentication is performed on all messages**
  Conettix IP performs authentication on all messages. This authentication is done to prevent Replay or Substitution of panels. It is done by the using a key to verify each message that is received. The

key is changed with each message including Heartbeats (Supervision or poll messages), Openings/Closings, or actual alarm events.
Replay of messages would occur when a network sniffer is used to record messages and attempt to play them back. Substitution would occur when a panel is replaced by another panel. Both of these tactics are used to attempt to "fool" the receiver into believing that a panel is still online and working when in fact there is a problem. Conettix IP handles these situations very effectively.

- **Supervising every network account**
  The Conettix IP solution supervises all network accounts. It does not allow for un-supervised accounts to be entered into the system. With unsupervised accounts, you have no knowledge of a problem until it is unable to send a message. Other manufactures offer a mix of supervised and unsupervised accounts on a receiver. This allows them to "support" more accounts than would be expected. This is purely because the account is not going to check-in and consume bandwidth or processing overhead. For highest security, all IP accounts should be supervised.

- **AES Encryption support**
  Conettix IP supports the encryption of the data being transmitted over the network using up to 256-bit AES Encryption. Data that is sent over a network can be vulnerable to being intercepted and analyzed by packet sniffers on the network. Although in the exchange of events there is not information that would expose crucial data points such as a customer's passcode, address, etc., it is generally felt that this data should be encrypted. Bosch panels are also able to be remotely programmed over the network. When programming is done over a network, crucial information is sent to the panel and there should be some level of encryption to protect the data from being directly viewed. Conettix IP provides its own level of encryption of the data so that any packets that are captured from a network would not directly reveal sensitive data. Bosch supplies this basic encryption to ensure that even if the installation was not setup with encryption, there is a level of protection of the data that is being sent over the network. Because Bosch feels that data security is an extremely important aspect of Alarm over IP, all Bosch IP communicators also include AES encryption as a standard feature. Some manufactures only offer encryption on certain products and charge an additional fee for those products.
  AES encryption provides a very high level of encryption for all data that is sent over the network. Further, Bosch uses a very secure method of AES encryption known as Cipher Block Chaining (CBC). CBC encryption is generally regarded as a more secure method than some that are used by other alarm manufacturers such as Electronic Code Book (ECB). ECB is easier to crack than CBC because it contains a limited set of encryption keys that are repeated with every message. CBC changes the encryption key with each message, greatly reducing the possibility of decoding. Anyone who is concerned about data security should research the type of encryption that is used by their alarm manufacturer.

- **Hacking Prevention**
  It is not possible for a hacker to gain access to the Conettix IP network on premises from any of the alarm system's other communications methods such as PSTN or Cellular. There are no logical connections between the different technologies, so even if the hacker were to connect to the system using PSTN or Cellular, they would not be able to see or manipulate data on the premises IP network. Conettix IP uses specific ports for network communication. By protecting these ports and allowing only the security system to access them, IT managers can prevent outside access, thus eliminating the chance for hackers to connect.
  Through the use of CBC encryption, multiple passwords, anti-relay and ant-substitution, Conettix IP is able to greatly reduce any chance that a hacker could interrupt an alarm signal. The chance that any interruption would go undetected is completely eliminated.

Conettix IP has several modern-day IT features that simplify installation and service:

IPv6 Support:
IPv6 is the latest IP addressing method for Internet devices. IPv4 addresses (such as 192.168.100.200) have been exhausted and will eventually be replaced by IPv6. IPv6 supports (340 Undecillion addresses that's shown as: 340,000,000,000,000,000,000,000,000,000,000,000,000,000

IPv6 also simplifies connections for remote programming and for remote access from smart phones. Installing a system that supports IPv6 meets the latest standards and ensures that the system will be able to transition seamlessly as changes in the future call for a conversion to IPv6.

Universal Plug and Play (UPnP):
UPnP allows the Ethernet module to automatically configure port forwarding in the network router for remote connections such as RPS or mobile applications. Port forwarding enables secure outside connectivity by routing only permitted traffic from outside the network to the Ethernet Module.

Without UPnP, an IT manager may change a setting that hinders future RPS communication, not knowing that these settings are required for RPS.

UPnP reduces router configuration by security personnel and, avoids possibility of network issues related to manual port forwarding. This simplifies installation, especially for installers that are not IT savvy.

DNS Central Station Reporting:
DNS to the central station allows Bosch panels to use Domain Name Service to look up their reporting central station IP address if the IP address changes. This is particularly useful for disaster recovery and for simple migration of IP accounts among central stations. It means that the installer does not need to remotely program each panel if the IP address of the central station changes.

This provides simple, highly secure, instant central station disaster recovery, eliminates emergency service calls and allows easy migration to a new central station if desired.
This is particularly useful for banks and other high-security applications that desire disaster recovery or avoidance for the central station.

Dealers who would like to have the flexibility to migrate their IP accounts to other central stations can also take advantage of DNS.

Auto-IP:
Auto-IP allows installers to connect their laptop directly to the B Series or B426 without special hardware or PC configuration changes.

With Auto-IP, the IP module automatically acquires an IP address that can be used with the laptop to establish an RPS connection. The panel automatically assigns itself an IP address if it does not receive one from the network. This is the same as other modern IP appliances such as the laptop. This reduces installation and service costs and eliminates the need for special equipment such as a hub and cross over cable. It also eliminates the need to change IP address configuration in the PC.

Application Example – Davidson College

Davidson College is a highly selective independent liberal arts college for 1,700 students. Since its establishment in 1837 by Presbyterians, it has graduated 23 Rhodes Scholars and is consistently regarded as one of the top liberal arts colleges in the country. It is located north of Charlotte, North Carolina in the town of Davidson. This historic 450-acre campus is an excellent choice for the student who seeks a vigorous undergraduate education in a residential environment.

To protect the safety of its students, faculty and staff living and working on campus, the IT department at Davidson College has an extensive system of life safety and security equipment installed throughout the various buildings. This system previously required 140 dedicated phone lines to communicate with a central monitoring station. The IT staff needed to reduce recurring operating costs for the system.

With Bosch IP communications modules, the college can continue to use their existing fire and intrusion control panels, while taking advantage of the cost savings and other benefits achieved with communications to the central station via an Internet connection. More than 70 fire alarm systems from a variety of manufacturers protect the residence hall, classroom and administrative buildings throughout campus.

All of these systems now communicate to the central station using Conettix C900V2 Dialer Capture Ethernet Modules. The modules work equally well with the college's Bosch D6412 Control Panels as they do with the installed panels from other manufacturers. Administrative buildings are also protected by Bosch D7412GV2 and D9412GV2 security control panels and Conettix DX4020 Network Interface Modules, which communicate intrusion alarms via Ethernet connections. The Conettix DX4020 modules transmit more detailed alarm information to the central monitoring station. The DX4020 modules have helped improve alarm reporting capabilities for the college.

The central station can now tell the local authorities the exact location in a building where motion was detected or windows or doors were forced open by an unauthorized individual. With the new modules installed, the IT department has been able to eliminate the phone lines used for alarm communications.

Davidson College's IT department has calculated that the new equipment will result in an impressive return on investment. "By eliminating the expense of the phone lines, we are experiencing a 50 percent cost savings now and expect that number to increase to 75 percent in the near future," said Brent Babb, project manager, Davidson College. On top of the cost savings, the alarm communications from the college to the central station are now received faster than those previously transmitted via a phone line, which in turn improves the central station's response time.