SPECIOUS SYLLOGISMS RIFE WITHIN THE ACCESS CONTROL MARKET

Having recently seen a headline similar to this, albeit associated to a different market, I was perplexed as to what it meant, so I referred to my trusty online dictionary and found the following explanation:

Specious *adj* [**Spee**-shuss] apparently true, but actually false.
Syllogism *n* form of logical reasoning consisting of two premises and a conclusion.

Therefore a specious syllogism is a form of logical reasoning consisting of two premises that lead to a false conclusion. So how does this apply to the access control market?

Applying a popular syllogism to the cards and credential portion of the Access Control Market it is a popular belief that; cheap readers and credentials are available; the use of readers and credentials with Access Control systems are necessary therefore cheap readers and credentials are necessary. As we will discuss below, this premise is false hence, the specious statement. English lesson 101 over I will attempt to address the reasoning behind this statement.

Over the last 10 years, readers and cards have become a commodity purchase with sections of the marketplace merely looking for the cheapest product available without any consideration of reliability let alone credential security. Maximum profit, minimum hassle sounds like good business sense! However, this has lead to a widespread use of mass produced generic technologies, with random numbered cards or limited commonly used

card formats that create and use duplicate card numbers on mass. For instance with some of the most commonly used Proximity makes, it is estimated that there are literally 5 - 10K duplicates of every 26 bit Wiegand format card. 26 bit Wiegand format cards are the most commonly used format within the access control market. This format allows for only 256 facility codes and only 65000 individual cards per facility code. See addendum.

Although there is the perception that biometrics is the universal panacea within the end-user community, there are several operational and usability issues associated with this technology that I will not address here. There is still a massive market for readers and credentials due to their ease of use, cost effectiveness, monetary storage capabilities and long read range capabilities. Many companies now empower their employees to act as an additional security layer. They do this by insisting that all employees wear a Photo Identification badge, so that employees are encouraged to inform security personnel if they see any person within a facility or campus who is not wearing a badge, as this person could be a threat. The use of Proximity and Smart Card credential facilitates this by allowing photographs and text to be printed onto them. Thus it is imperative to select a card and reader supplier that can offer the advantages of the technology without compromising security let alone reliability.

In the context of an access control system, readers and credentials are the key and lock replacements of the security system. When a customer is issued with a Proximity or Smart Card, they are given a new front door key and there is an expectation that this “front door key” is unique and secure, and that only authorized credentials will access their facility.

Farpointe Data Inc is a Californian company consisting of the original founders of Indala and the team from Motorola Indala. The Indala team invented the RFID technology and applied it to readers and credentials within the security industry and have been making quality readers and credentials since the early 1980‘s Their new range of Proximity and SmartCard readers and credentials is based upon brand new technology, built from the ground up, and not inherited generic products. Farpointe were therefore able to refer back to there 30 years of experience to develop a totally new range that addressed and overcame the deficiencies in earlier products and have an approach to readers and cards that ensures the security for their customers.

If the readers and cards are electronic keys and locks, Farpointe Data takes on the role of an Electronic locksmith. They have numerous technology advancements that enable them to customize the readers and cards to ensure that whether it is Proximity or a contact-less SmartCard solution, the customers credentials are unique, secure and ensure that only bone fide credentials, and not duplicates, are able to access the building.

In order to address and support the Europe, Middle East and African market place, Farpointe looked for a distributor with not only sales and marketing skills but more importantly the technical support, logistics infrastructure, stock holding capabilities and experience to sustain growth within the region, by providing superior levels of customer satisfaction. Most distributors within the security arena tend to operate on a “jack of all trades rather than masters one trade” basis. This is all very well if, as a customer, you know everything about a product that you wish to purchase, as you will most likely be speaking to an order entry telephone sales person when calling. If you are looking for in-depth technical information then this is where a dedicated distributor excels. .

Simultaneously STG were seeking a manufacturer, as an alternative to the existing suppliers of RFID readers and credentials, to address the issues discussed above for

some time. Their criterion was not merely price but security, quality, reliability, flexability and value for money. Exhaustive searches by both companies led them to each other.

Fig.1 P640 Keypad Reader

An example of Farpointe's commitment to reliability is their popular P-640 illuminated Keypad reader (See Fig.1). This reader is the logical conclusion of almost 30 years of developing combination Keypad and Proximity readers. The design issues for this product revolve around the Keypad technology itself. Traditional pin & Proximity readers use membrane based Keypads as metal Keypads interfere with the Proximity read range and are very expensive. The main problem with the membrane technology, apart from usual wear and tear, is that in environments with climatic extremes, the rubber or plastic used in the membranes can deteriorate dramatically with the variations in temperature. This leads to failed pin reads and broken readers in fairly short periods of time. To overcome this deficiency, Farpointe introduced the P-640 with a capacitive Keypad technology which experiences no wear and tear whatsoever irrespective of number of presses or whether it is in direct sunlight. The technology is so robust that the Keypad overlay could be slashed with a knife and it would still work! As there is no metal present in the Keypad, the proximity read range is maximized and Farpointe uses highly effective blue LED lighting to illuminate the Keypad for darker locations and night time usage. This LED lighting shuts down after 20 seconds to illuminate only the number 5 in the center of the reader, with either credential presentation or depressing a Keypad key required to reactivate full illumination. This feature was requested by some of Farpointe's more experienced Keypad customers who found a brightly illuminated reader can attract the wrong sort of attention when on the outside of a building.

Fig.2 Bullet Proof Reader

Farpointe's flexibility manifested itself in their ability to develop and adapt their technology to meet custom demands. This was possible as we were able to deal with a small dedicated team of professionals rather than a cog within a large corporation. A case in point is as follows, within the security industry, sometimes applications are requested that would never have been expected. Farpointe encountered one client that had a rather disturbing and extraordinary product requirement at an inner city urban project. Their external readers were being targeted by street gangs using the illuminated Proximity readers LED's as target practice. Hooligans were shooting readers off the exteriors of their buildings. Needless to say, that by the time the client had paid for their installer to come out and replace the reader, each incident was costing them $1000's. The client put out a tender for someone to produce a bullet proof reader and Farpointe responded with what was to become its P-

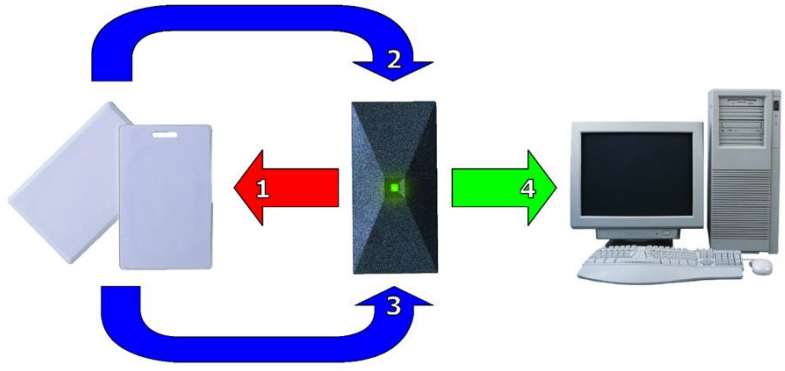
400 Gibraltar proximity reader (See Fig.2). The P-400 is made of stainless steel with a Fiber-Tex® insert (UL752 listed for bulletproof integrity) making it probably one of the most vandal resistant and robust proximity readers in the world. Indeed it is capable of taking a direct gunshot from most typically available hand guns. The P-400's robust construction has made it a favourite with military, construction, and inner city high risk installations throughout the world.

There are many suppliers of low cost readers in the market place but we have seen that reliability as well as security can be an issue. Although these low cost products do offer a warranty it still entails costs. When a reader fails, a new reader has to be shipped to an engineer, who has to attend site, remove the defective unit, replace it with the new unit and then ship the defective unit back to the manufacturer under a laborious RMA procedure. Therefore, although the reader will be replaced free of charge by the manufacturer, the cost of a single call-out for a warranty replacement will cost more than supplying a slightly more expensive and reliable unit in the first place and so can destroy margins and customer relationships.

Farpointe has 3 main product offerings, Pyramid, which utilizes 125Khz Proximity technology, Delta, which utilises 13.56Mhz contactless SmartCard solution (Mifare based) & Ranger, which is a 433Mhz active long range solution. All have been designed to provide multiple technological advantages to help secure facilities. Pyramid and Delta Series offer multi-technology solutions with HID and AWID compatibility available

The product range is American designed and built to deliver the highest quality product offering available in the marketplace. The robustness of the designs can be demonstrated in that most of the Farpointe readers are IP-67 rated, not only can they operate effectively in all wind, rain, snow and dust conditions, but are also warranted to keep on working if a building was temporarily flooded and after the water recedes! Furthermore, Farpointe readers have the greatest temperature range available in the industry, being rated between -40 Deg C and +65 Deg C. It goes without saying that with this level of build, the Farpointe range has a Lifetime Warranty; however Farpointe's approach is not just to give a lifetime warranty, but to build the products to exceed the lifetime of the access control systems.

Fig. 3 MAXSecure Theory of operation



1. Reader powers proximity card or tag.
2. Card transmits MAXSecure code to reader.
3. Card transmits access data (facility code, ID number, etc.) to reader.
4. If reader authenticates card's MAXSecure code, then reader transmits access data to access controller via an industry standard protocol. If reader does not authenticate card's MAXSecure code, then the reader transmits nothing to the access controller.

In the Pyramid Series Proximity products, Farpointe recognized that much of the access control market place is still looking for the convenience and reliability that 125Khz Proximity provides. Most of all, the new industry SmartCard solutions struggle to match the read ranges that Proximity provides. So Farpointe decided to enhance the security of Proximity by including a SmartCard inspired Security key between the card and the reader. This technology is called

MAXSecure™ and effectively ensures that the readers only read cards with the correct security key, before any data is sent to the access control system (see Fig 3.). Each time a MAXSecure™ key is issued to a customer, they have a unique range of Wiegand formats that could be reissued whilst guaranteeing no duplicates being in the field.

Consider MAXSecure™ as an "electronic doorman" that is built into the Pyramid Series readers. MAXSecure™ effectively creates the "list" of authorized credentials, it then checks every credential to make sure that they are "on the list" before allowing them to access your facility! Smart Card security with Proximity read range! Even Wiegand 26 bit once again becomes secure!

An additional powerful advantage of the Pyramid series readers is the ability to activate a Farpointe developed technology called fleaPower™. This is Farpointe's own eco friendly "green technology" designed to help conserve the environment and reduce energy costs. The way they like to think about this is; would you leave a light bulb on overnight? Proximity Readers stay on 24 hours a day, 7 days a week. By activating fleaPower™ mode on the Pyramid Series readers they can draw as little as 5mA, in their quiescent state, which can equate to an 90% reduction in current draw as compared to traditional readers in their quiescent standard mode. This energy reduction will result in long term energy savings. Also, in emergency situations, i.e. during a power outage, fleaPower™ enabled readers can be powered much longer by back-up batteries.

The access control industry, like the CCTV industry before it, is rapidly moving towards TCP/IP connectivity, meaning that the systems are being run on the corporate network. As part of this swing, controllers that support Power Over Ethernet (PoE) are now available. Consequently controllers and their peripherals, such as locks and readers, are powered from a network switch. This device will supply the power for the controller and its peripherals as well as the data over a single network cable (CAT5 or 6). At the moment the power from these devices is limited to 14.5 watts therefore utilizing a reader in fleaPower™ mode expands peripheral selection as devices with higher power consumption can now be considered.

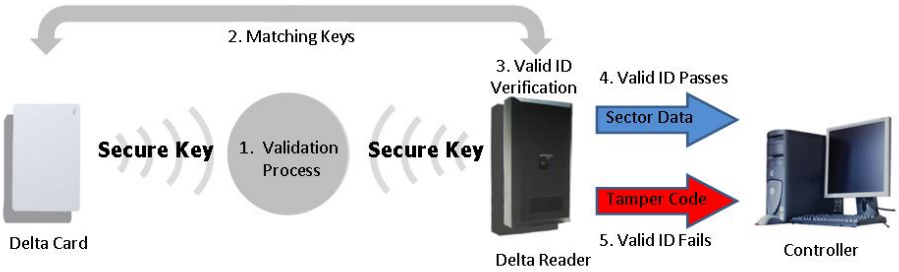
Previously Energy Conservation was not high on the priority list; however recently, with the worldwide economic situation, the ability to show the customers that they can secure their premises, and save money on their bills is a combination that is winning approval worldwide!

Delta is Farpointe's line of 13.56-mHz contactless Smart Card readers and cards based upon the industry standard MIFARE technology. A true multi-technology platform, Delta readers feature card adaptive technology, allowing them to read a wide range of credentials, including 13.56-mHz US Government FIPS201 cards, ISO 14443 Type A & B cards, MIFARE secure sector and card serial number (CSN), plus 125Khz Pyramid Series Proximity® cards and tags. Additionally an optional feature allows the Delta readers to be configured to be read by HID and AWID 125Khz Proximity credentials.

Recently the Smart Card industry was rocked when MIFARE security was cracked in Europe. This widely available technology had become an industry standard and was probably one of the most economically viable of the Smart Card solutions. Knowledge of this vulnerability put many existing Smart Card projects in jeopardy, and affected the industries confidence in MIFARE as a solution. The manufacturers of the MIFARE cards

are working on MIFARE Plus which will address the security issues by using 128 bit keys, however the speed at which MIFARE Plus is being introduced and deployed is not fast enough to save many of the projects that are currently in “limbo”, additionally there is a cost uplift for MIFARE Plus which is negatively affecting projects.

Fig. 4 Valid ID Theory of operation



Valid ID Process

Mifare validation process (first layer of protection)

1. Delta Reader and Card exchange and compare standard-security MIFARE keys.
2. Keys match, reader collects Delta card's access control data.

Valid ID (second layer of protection)

3. Delta Reader performs Valid ID cryptographic algorithm to confirm the integrity of the Farpointe-programmed access control data.
4. Valid ID validates Farpointe-programmed access control data; Delta Reader outputs the access control data.
5. Valid ID repudiates access control data, indicating the presence of tampering; Delta Reader outputs tamper code blocking counterfeit access control data.

In reaction to this problem, Farpointe developed their Valid ID™ technology to identify and reject counterfeit or unofficially modified Smart Cards. Cards that have been modified or duplicated will be sent a tamper code to the security system controller and thus access to the facility will be denied and the customer will be alerted to the fact that a rogue credential has been utilized at the reader. If the security data in one of their secure sectors is duplicated or modified in any way, Valid ID™ identifies and rejects the modified card (see Fig 4). This exciting development is outside of MIFARE’s own sector security and its application ensures that the Delta solution exceeds the security requirements of any projects undertaken. Now you can enjoy MIFARE classic pricing without having worrying about the security and tampering issues.

Ranger is Farpointe’s 433Mhz active long range technology. The solution consists of a 2 channel receiver and an active transmitter (key fob).The transmitters can send Wiegand data over 50m securely. The read range is tunable at the receiver and can be reduced to as little as 2m if required. The information between Transmitter and receiver includes 128bit TEA (Tiny Encryption Algorithm as used by financial institutions for monetary transactions) encryption, which incorporates a rolling code, so the Wiegand data cannot be “sniffed” and reproduced. Each Transmitter comes with a secondary 125Khz coil built in for the transmitter enabling the active Key fob to be used as a passive Key fob. This dual function allows the 1 credential to be utilized with both the standard Pyramid Proximity readers installed within a building as well as providing long range access to the car park for example.

One of the final pieces to the puzzle to meet all of the marketplace requirements has been met by Farpointe’s Master Distributor, Security Technologies Group (STG), who now offers a unique range of customized covers, available in finishes to match any installation that you wish to undertake, including various wood effects, marble and stone. All too often in the past the customer was lumbered with the industrial look of readers in their standard black, grey or tan finishes. This was acceptable where aesthetics was not a problem, but for those discerning customers who had spent considerable time, effort and money

designing areas of their building to reflect corporate image, the addition of these readers would be an eyesore.

Fig. 5 Custom Finishes

STG saw a rising tide of requests from customers who had designed their lobbies utilizing glass, marble, stainless steel or who had designed a VIP area with walnut finishes that were demanding a solution that blended into their chosen décor. To address this STG developed an innovative, patented, bespoke and customized printing service using a unique environmentally friendly process. Customers can choose from a range of 22 base colours and 86 styles that include Animal, Carbon, Graphics, Metal, Nature, Stone and Wood. Each coating is available in a matt, satin or gloss finish (see Fig. 5)

Additionally STG have seen, all too often in the past, customers struggling to reorder additional cards and tags (credentials) for their systems, with the original suppliers being of little assistance. Within their advanced Card Management software, STG are able to search via multiple criteria, in order to identify the correct technology, card format, facility code, and numbering sequence thus eliminating this headache for customers. Our philosophy is to make the whole process as painless as possible.

About the author

This article was written by Mr. Denis Kane, Director at Security Technologies Group with acknowledgements to Mr. Scott Pearson, Director at Farpoint Data Inc.

Denis has been in the security industry since leaving school and joining Chubb to serve his apprenticeship. Having spent over 30 years in the security industry working and living in the UK, Ghana, UAE, Saudi Arabia and Sri Lanka he has built up a wealth of experience and knowledge of both installation practices and technology through his exposure to the key brands in the integrated security system market. This together with his vast knowledge of local customs led him to set up Security Technologies Group, with a group of other industry veterans, to impart their various skill sets to their customers. Denis can be contacted via e-mail on denis@SecurityTechnologiesGroup.co.uk or telephone on +44 (0) 1234 865004.

Security Technologies Group
9 Nags Head Lane,
Hargrave
Northamptonshire.
NN9 6BJ
United Kingdom
www.SecurityTechnologiesGroup.co.uk

Addendum A - Additional information on 26bit Wiegand Technology for those who are interested.

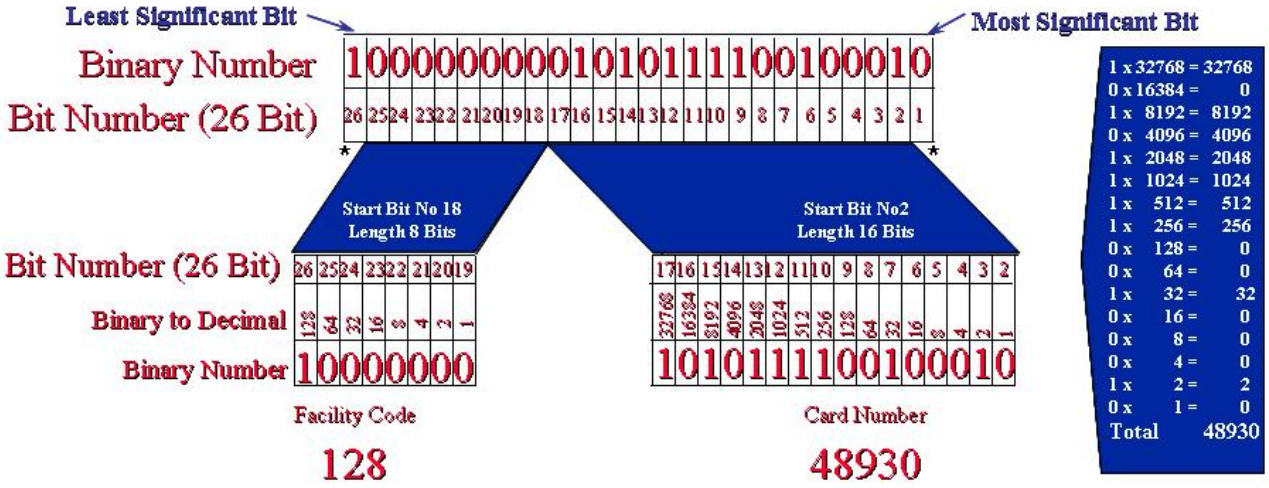
In the early days of card based access control systems the memory within controllers was limited and so cards that stored information as 26 1's and 0's (binary) needed less storage space than formats requiring 32 bit for example. With the 26 bit format the first 8 bits of information was reserved for a facility code. A different facility code could then be allocated to each customer therefore differentiating card number 230 belonging to company a from card number 230 belonging to company b. Eight 1's in binary provides for the maximum of 256 individual facility codes. 16 bits are used for the individual card number which provides for a maximum of 65535 unique card numbers per card format. Just to clarify the 1st bit and the last bit are used for other functions.

If a facility code was added then the controller would only need to store the facility code once. The controller then only needed to store each individual 16 bit card number rather that the full 26 bits, which greatly reduced storage requirements even further.

It is obvious that if each customer is allocated a dedicated facility code that only 256 customers can have unique credentials. It is also obvious that the 257th customer would have to have a duplicate facility code and possible card population, however as so few people were using access control systems, it was highly unlikely that a person from a company with facility code 12 and card number 230 would present their card to reader belonging to another company using that same format and numbering sequence.

Given the length of time that systems have been in use and the exponential increase in adoption of access control systems and the use of the 26bit format as in industry standard, that fear is more than real now, given that between 5000 and 10000 duplicates of each card are out there in the market.

Wiegand 26 bit Principles



* Bits 1 and 26 used for error checking