International Council For Industrial Security & Safety Management

Newsletter: July 2012

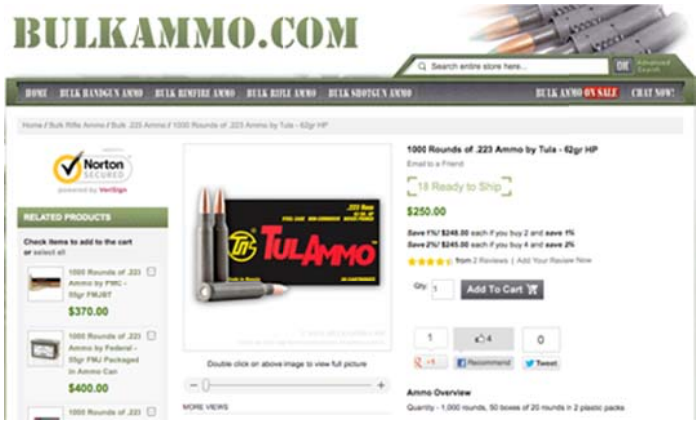
Let's professionalize the professionals…

http://www.wix.com/sbtyagi/iciss

Aurora theatre suspect James Holmes stockpiled 6,000 rounds of ammunition online.

Spend just a few minutes browsing the internet and it becomes clear how James Holmes was able to stockpile 6,000 rounds of ammunition without any alarms sounding. "The Guardian" did little research on internet and found that huge amounts of ammunition can be purchased online in a matter of minutes and can be shipped straight to customers' doors, no questions asked. Yet those familiar with gun ownership in the US are unlikely to have been surprised.

BulkAmmo.com is one of many websites which allow for the purchase of lots of rounds at knockdown prices. On the website one can buy 1,000 .223, 62grain TulAmmo rounds, which can be fired by an AR15 assault rifle, for just $250, or 25 cents a round.



Luckgunner.com stocks Fiocchi .223 remington rounds in boxes of 1,000, described as "perfect for your AR-15!". When "The Guardian" perused the website on Monday there were 41 boxes in stock. Again, "The Guardian" we were able to follow the purchasing procedure through – potentially getting 41,000 rounds delivered within three days, for $17,428.39.

Access Control System

Courtesy: Col D R Semwal (callsamydr@yahoo.com)

Today it's significantly different! Yesterday we operated with fences, gates, guards and cameras. We were worried about people taking minor items out of the workplace. But the fences, guards and gates are not as important these days for many businesses.

An IT services company that prides itself on its relaxed and open philosophy is unlikely to appreciate a security leader whose focus is on locking the employee population out of newer communication technologies, for example. Staff and management may look at that individual as a roadblock to be surmounted rather than a partner.

Planning for access control system needs innovative approach and deep knowledge of the business and work-culture of the organization. It calls for not only keeping the bad guys out bust also encouraging the good guys to come in without hassle!

Physical access by a person may be allowed depending on payment, authorization, etc. Also there may be one-way traffic of people. These can be enforced by personnel such as a border guard, a doorman, a ticket checker, etc., or with a device such as a turnstile. There may be fences to avoid circumventing this access control. An alternative of access control in the strict sense (physically controlling access itself) is a system of checking authorized presence, see e.g. Ticket controller (transportation). A variant is exit control, e.g. of a shop (checkout) or a country.

In physical security, the term access control refers to the practice of restricting entrance to a property, a building, or a room to authorized persons. Physical access control can be achieved by a human (a guard, bouncer, or receptionist), through mechanical means such as locks and keys, or through technological means such as access control systems like the mantrap. Within these environments, physical key management may also be employed as a means of further managing and monitoring access to mechanically keyed areas or access to certain small assets.

Physical access control is a matter of who, where, and when. An access control system determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. Historically this was partially accomplished through keys and locks. When a door is locked only someone with a key can enter through the door depending on how the lock is configured. Mechanical locks and keys do not allow restriction of the key holder to specific times or dates. Mechanical locks and keys do not provide records of the key used on any specific door and the keys can be easily copied or transferred to an unauthorized person. When a mechanical key is lost or the key holder is no longer authorized to use the protected area, the locks must be re-keyed.

He is highly experienced (29 years' service in Indian Army) with proven skills in managing Safety and security issues of establishments, managing large human resource deployments, logistics & mobility.

Col. Semwal has experience & passion for protection of ecology & environment. He changed the face of Delhi in Bhati Mines Area while he was commanding Eco-Battalion of Territorial Army in Delhi and turned it into lush green area!

He was successful in restoration of mining land by afforestation activities in coordination with Deptt of Environment, Government of Delhi.

He has vast experience and knowledge in Industrial Security and Safety in combination with expertise related to Environment and Ecology. He is deeply committed in the field of SHSE (Security; Health Safety & Environment).

He is ICISS Councilor for NCR Region.

Electronic access control uses computers to solve the limitations of mechanical locks and keys. A wide range of credentials can be used to replace mechanical keys. The electronic access control system grants access based on the credential presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is refused, the door remains locked and the attempted access is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked.

Access Control System Operation

When a credential is presented to a reader, the reader sends the credential's information, usually a number, to a control panel, a highly reliable processor. The control panel compares the credential's number to an access control list, grants or denies the presented request, and sends a transaction log to a database.

When access is denied based on the access control list, the door remains locked. If there is a match between the credential and the access control list, the control panel operates a relay that in turn unlocks the door. The control panel also ignores a door open signal to prevent an alarm. Often the reader provides feedback, such as a flashing red LED for an access denied and a flashing green LED for an access granted.

The above description illustrates a single factor transaction. Credentials can be passed around, thus subverting the access control list. For example, Alice has access rights to the server room but Bob does not. Alice either gives Bob her credential or Bob takes it; he now has access to the server room. To prevent this, two-factor authentication can be used. In a two factor transaction, the presented credential and a second factor are needed for access to be granted; another factor can be a PIN, a second credential, operator intervention, or a biometric input.

There are three types (factors) of authenticating information:

- something the user knows, e.g. a password, pass-phrase or PIN
- something the user has, such as smart card
- something the user is, such as fingerprint, verified by biometric measurement

Passwords are a common means of verifying a user's identity before access is given to information systems. In addition, a fourth factor of authentication is now recognized: someone you know, where another person who knows you can provide a human element of authentication in situations where systems have been set up to allow for such scenarios. For example, a user may have their password, but have forgotten their smart card. In such a scenario, if the user is known to designated cohorts, the cohorts may provide their smart card and password in combination with the extant factor of the user in question and thus provide two factors for the user with missing credential, and three factors overall to allow access.

Credential

A credential is a physical/tangible object, a piece of knowledge, or a facet of a person's physical being, that enables an individual access to a given physical facility or computer-based information system. Typically, credentials can be something you know (such as number or PIN), something you have (such as an access badge), something you are (such as a biometric feature) or some combination of these items. The typical credential is an access card, key fob, or other key. There are many card technologies including magnetic stripe, bar code, Wiegand, 125 kHz proximity, 26 bit card-swipe, contact smart cards, and contactless smart cards. Also available are key-fobs which are more compact than ID cards and attach to a key ring. Typical biometric technologies include fingerprint, facial recognition, iris recognition, retinal scan, voice, and hand geometry

Access Control System Components

An access control point, which can be a door, turnstile, parking gate, elevator, or other physical barrier where granting access can be electronically controlled. Typically the access point is a door. An electronic access control door can contain several elements. At its most basic there is a stand-alone electric lock. The lock is unlocked by an operator with a switch. To automate this, operator intervention is replaced by a reader. The reader could be a keypad where a code is entered, it could be a card reader, or it could be a biometric reader. Readers do not usually make an access decision but send a card number to an access control panel that verifies the number against an access list. To monitor the door position a magnetic door switch is used. In concept the door switch is not unlike those on refrigerators or car doors. Generally only entry is controlled and exit is uncontrolled. In cases where exit is also controlled a second reader is used on the opposite side of the door. In cases where exit is not controlled, free exit, a device called a request-to-exit (RTE) is used. Request-to-exit devices can be a push-button or a motion detector. When the button is pushed or the motion detector detects motion at the door, the door alarm is temporarily ignored while the door is opened. Exiting a door without having to electrically unlock the door is called mechanical free egress. This is an important safety feature. In cases where the lock must be electrically unlocked on exit, the request-to-exit device also unlocks the door.

Access Control Topology

Access control decisions are made by comparing the credential to an access control list. This lookup can be done by a host or server, by an access control panel, or by a reader. The development of access control systems has seen a steady push of the lookup out from a central host to the edge of the system, or the reader. The predominant topology circa 2009 is hub and spoke with a control panel as the hub and the readers as the spokes. The lookup and control functions are by the control panel. The spokes communicate through a serial connection; usually RS485. Some manufactures are pushing the decision making to the edge by placing a controller at the door. The controllers are IP enabled and connect to a host and database using standard networks

Types of Readers

Access control readers may be classified by functions they are able to perform –

- **Basic (non-intelligent) readers:** simply read card number or PIN and forward it to a control panel. In case of biometric identification, such readers output ID number of a user. Typically Wiegand protocol is used for transmitting data to the control panel, but other options such as RS-232, RS-485 and Clock/Data are not uncommon. This is the most popular type of access control readers. Examples of such readers are RF Tiny by RFLOGICS, ProxPoint by HID, and P300 by Farpointe Data.
- **Semi-intelligent readers:** have all inputs and outputs necessary to control door hardware (lock, door contact, exit button), but do not make any access decisions. When a user presents a card or enters PIN, the reader sends information to the main controller and waits for its response. If the connection to the main controller is interrupted, such readers stop working or function in a degraded mode. Usually semi-intelligent readers are connected to a control panel via an RS-485 bus. Examples of such readers are InfoProx Lite IPL200 by CEM Systems and AP-510 by Apollo.
- **Intelligent readers:** have all inputs and outputs necessary to control door hardware, they also have memory and processing power necessary to make access decisions independently. Same as semi-intelligent readers they are connected to a control panel via an RS-485 bus. The control panel sends configuration updates and retrieves events from the readers. Examples of such readers could be InfoProx IPO200 by CEM Systems and AP-500 by Apollo.

Security Risks

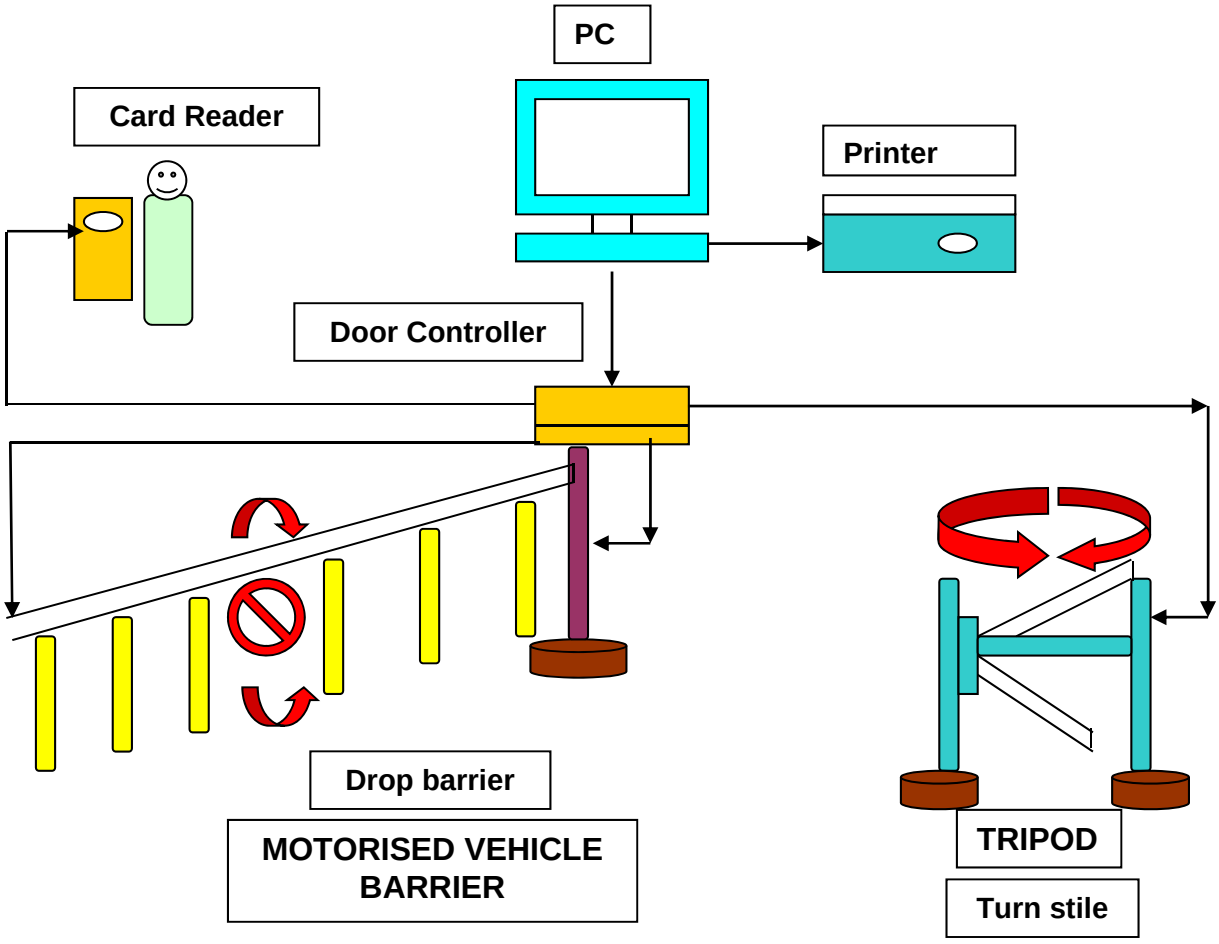
The most common security risk of intrusion of an access control system is simply following a legitimate user through a door. Often the legitimate user will hold the door for the intruder. This risk

can be minimized through security awareness training of the user population or more active means such as turnstiles. In very high security applications this risk is minimized by using a sally port, sometimes called a security vestibule or mantrap where operator intervention is required presumably to assure valid identification.[citation needed]
The second most common risk is from levering the door open. This is surprisingly simple and effective on most doors. The lever could be as small as a screw driver or big as a crow bar. Fully implemented access control systems include forced door monitoring alarms. These vary in effectiveness usually failing from high false positive alarms, poor database configuration, or lack of active intrusion monitoring.

Similar to levering is crashing through cheap partition walls. In shared tenant spaces the divisional wall is vulnerability. Along the same lines is breaking sidelights. Spoofing locking hardware is fairly simple and more elegant than levering. A strong magnet can operate the solenoid controlling bolts in electric locking hardware. Motor locks, more prevalent in Europe than in the US, are also susceptible to this attack using a donut shaped magnet. It is also possible to manipulate the power to the lock either by removing or adding current.

Access cards themselves have proven vulnerable to sophisticated attacks. Enterprising hackers have built portable readers that capture the card number from a user's proximity card. The hacker simply walks by the user, reads the card, and then presents the number to a reader securing the door. This is possible because card numbers are sent in the clear, no encryption being used. Finally, most electric locking hardware still have mechanical keys as a fail-over. Mechanical key locks are vulnerable to bumping

Components of Access Control System



Another Credit / Debit Card Scam

Forwarded by - Col NN Bhatia, Veteran (narindra_bhatia@hotmail.com)

This appears to be another credit / debit card scam starting to make the rounds. Beware! - just received from a friend in Sydney. Well worth a read....

There is a new and clever credit card scam - be wary of those who come bearing gifts. Please circulate this to everyone you know, especially your family and friends. It just happened to friends a week or so ago in Singapore , and it can pretty well now be happening anywhere else in the world.

It works like this: Wednesday a week ago, I had a phone call from someone who said that he was from some outfit called "Express Couriers" asking if I was going to be home because there was a package for me, and the caller said that the delivery would arrive at my home in roughly an hour. And sure enough, about an hour later, a deliveryman turned up with a beautiful Basket of flowers and wine. I was very surprised since it did not involve any special occasion or holiday, and I certainly didn't expect anything like it.

Intrigued about who would send me such a gift, I inquired as to who the sender is. The deliveryman's reply was, he was only delivering the gift package, but allegedly a card was being sent separately; (the card has never arrived!). There was also a consignment note with the gift.

He then went on to explain that because the gift contained alcohol, there was a $3.50 "delivery charge" as proof that he had actually delivered the package to an adult, and not just left it on the doorstep to just be stolen or taken by anyone. This sounded logical and I offered to pay him cash. He then said that the company required the payment to be by credit or debit card only so that everything is properly accounted for.

My husband, who, by this time, was standing beside me, pulled out of his wallet his credit/debit card, and 'John', the "delivery man", asked my husband to swipe the card on the small mobile card machine which had a small screen and keypad where Frank was also asked to enter the card's PIN and security number. A receipt was printed out and given to us.

To our surprise, between Thursday and the following Monday, $4,000 had been charged/withdrawn from our credit/debit account at various ATM machines, particularly in the north shore area! It appears that somehow the "mobile credit card machine" which the deliveryman carried was able to duplicate and create a "dummy" card(?) with all our card details, after my husband swiped our card and entered the requested PIN and security number.

Upon finding out the illegal transactions on our card, of course, we immediately notified the bank which issued us the card, and our credit/debit account had been closed. We also personally went to the Police, where it was confirmed that it is definitely a scam because several households have been similarly hit.

Warning: Be wary of accepting any "surprise gift or package", which you neither expected nor personally ordered, especially if it involves any kind of payment as a condition of receiving the gift or package. Also, never accept anything if you do not personally know and/or there is no proper identification of who the sender is.

Above all, the only time you should give out any personal credit/debitcard information is when you yourself initiated the purchase or transaction!

How they swindle?

Following is the reproduction of the e-mail received by one acquaintance which appears to be benevolent in nature! However, on further investigation it was found that it was an attempt to gather important personal / financial information. The given link with lots of difficulty got connected after repeated attempts over three months' time, but for a short while without getting any useful information, indicating that these were non-functional URLs. The Yellow Button asking to **click here to activate your account** was sending the information to third party!

Readers are advised not to respond to such mails unless they verify the background of the sender of the mails.

PayPal

Information Regarding Your account:

Dear PayPal Member!

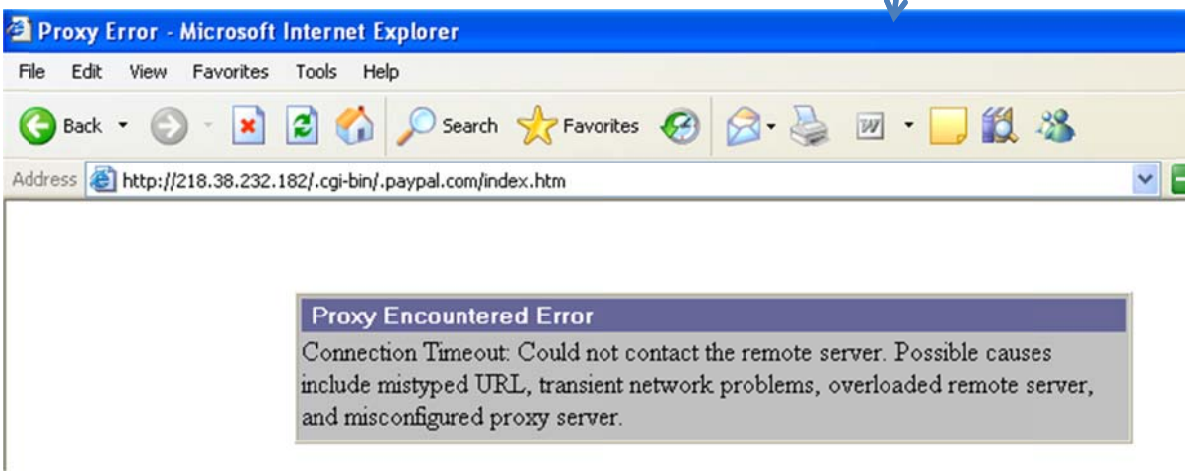
Attention! Your PayPal account has been violated! Someone with IP address 86.34.211.83 tried to access your personal account! Please **click the link below** and enter your account information to confirm that you are not currently away. You have 3 days to confirm account information or your account will be locked.

Click here to activate your account

You can also confirm your email address by logging into your PayPal account at http://www.paypal.com/ Click on the "**Confirm email**" link in the Activate Account box and then enter this confirmation number: 1099-81971-4441-9833-3990

Thank you for using PayPal!

- **The PayPal Team**



Hello frequent traveler!

Please take a minute from your busy schedule and read this letter. I assure you will not regret it. Imagine yourself in a car zooming at high speed and suddenly you see the driver has gone to sleep before you can take control of the situation a loud bang! All is finished! Your car had all the gadgets but did not have NO NAP an in- expensive safety device

More than 2 million people die and an equal number are injured in accidents caused by dozing / drowsy / sleepy drivers. All of us are at a risk of drowsy driving; we live in a twenty four hour society where a lot of people are tired all the time.

At 60 mph if you close your eyes for a second you have traveled 88 feet. Much worse drowsy drivers' judgment is impaired, sleepiness induces tunnel vision it's a recipe for an accident. Accidents by dozing drivers are generally fatal because

- Dozing drivers do not brake before an accident
- The impact is at high speed and this can be fatal.
- Drowsiness / sleepiness is red alert
- Do not build sleep debt
- Adequate rest before a long journey is recommended
- Use doze off alert gadgets

We manufacture and purchase the most expensive cars with latest comfort gadgets but have never thought of manufacturing a safety device which could warn the driver and co-passengers when the driver is in danger of dozing off and preventing a possible accident.
At last we have developed an intelligent safety device.

Functional Description

When the gadget is active and driver's head falls forward due to drowsiness, the intelligent NO NAP will buzz loudly and instantly bring the driver to full concentration. The gadget gives the alarm at preset angle.

The angle can be varied according to requirement. The gravity switch inside the gadget keeps the track of the position of the driver's head. If not in use, the switch should be kept at OFF position.

Salient Features

- Very light weight
- Compact and Ergonomically designed
- Low maintenance cost
- Easy to use and very cost effective
- Low cost and high reliability

For more information – Visit: http://www.thenonap.com/nni-fd.htm

Gastech SPECIALIST events

Revealing best practice strategies and technologies to respond to the latest and most urgent security threats affecting both offshore and onshore oil and gas.

Bringing together senior-level security, business resilience and safety personnel, this must attend event will address key topics in the form of case studies and cover aspects of the value chain, particularly in upstream and midstream oil and gas operations, including:

- Security and Patrol Forces
- Satellite and Surveillance
- Telecommunications Data Feeds, Analysis and Instant Interpretation
- Technologies used for Cyber and Maritime Security
- Security Risk Analysis
- Fencing and Other Physical Security Measures, Sensors
- CCTV, Infrared, SCADA
- Information Security
- Insurance and Liability
- Acts of Militancy and Terrorism
- Activism, Corporate Social Responsibility

Computer Crazy!

Don't Talk While He Drives!

Suggestions & feedback may be sent to us on e-mail: captsbtyagi@yahoo.co.in

P.S. - If you don't like to receive our newsletter, we apologize for bothering you. Please let us know your mail address, we will move it out of our contact list, thank you!