ICISS

Newsletter: January 2017

International Council of Industrial Security & Safety Management

When we technologically advance, it is not always true that our worries and requirement to work hard will be lessened. In fact technologies bring their set of woes along with wows! So many gizmos around us make our lives comfortable yet also make them vulnerable – in the sense of loss of privacy, loss of precious and privileged data and also threat to our own well beings. The security management is opening up to fast paced technological advancement and no more we talk only about integration of various security systems and gadgets; we in security & safety profession in fact started talking about Internet of Things (IoT) and wearable security solutions.
This edition of our newsletter covers this specific aspect.

Capt SB Tyagi,
For International Council for Industrial Security & Safety

DO NOT SEND YOUR LIFE IN A TEXT MESSAGE
ICISS
International Council of Security and Safety Management
http://onlineicissm.wix.com/iciss

Internet of Things (IoT)

The network of 'Wearables" is called the Internet of Things (IoT), which cuts a wide swath across the technology landscape. IoT has the potential to radically modify the quality of human life. The dream was articulated as early as 1961 when MIT professor Aaron Fleisher wrote "The Influence of Technology on Urban Forms." The idea that there exists in technology a potential capable of radically modifying the conditions of human existence has made prophecy a matter for general concern," Fleisher stated. Today, predictions continue to expound on the potential and pitfalls of the IoT.

Wearables are rapidly invading the workplace in much the same way that smartphones did. Fitness trackers, smartwatches, head-mounted displays and other new form factors are beginning to capture the public imagination. Sales of wearable electronic devices topped 232 million in 2015, and Gartner forecasts they'll rise 18.4% this year, when another 274.6 million devices are sold.

This new wave of interdependent smart devices is functional, reliable, and convenient, not to mention discreet. A good example would be fitness trackers. Designed to look like ordinary bracelets, these smart devices are equipped with biosensors that can measure your body's data and compute your real-time progress without disrupting your regular workout routine. With the addition of Bluetooth, updates are sent to your mobile device so you know exactly where you left off.

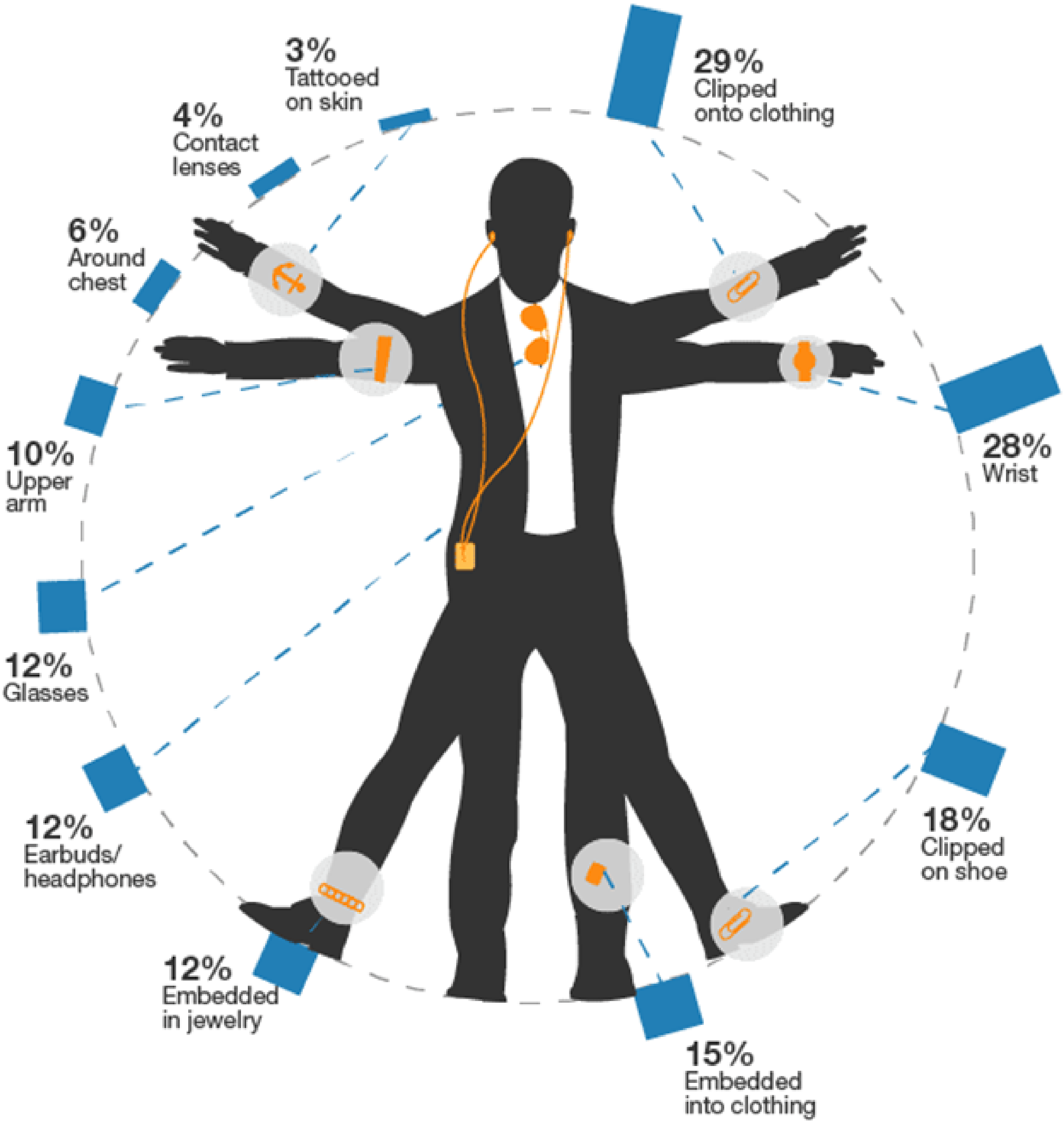
Smart watches, on the other hand, are engineered to serve as extensions of your smartphones. They function like normal digital watches, but they have the added ability of displaying incoming notifications from your smartphone. Many early adopters of smart watches claim that their gadget saves them the trouble of physically checking their phones while they're busy doing something else. Though the current function of these watches seem rudimentary, electronics companies have already promised the development of more useful and productive apps for smart watches in the near future.

These wearable devices represent some appealing opportunities for businesses to increase efficiency and gather data, but in the rush to win market share, security concerns are taking a backseat for many manufacturers and app developers. The potential ramifications of unchecked wearable device usage within the enterprise are alarming.

To do this, many leading industry players are spending an increasing amount of time in the world's innovation centres looking for technology partners to power the next generation of products and services, while at the same time staffing up their own innovation efforts to at least keep pace with the table stakes in the industry - think iPhone apps! For instance, one technology offering allows homeowners to arm and disarm their home security system, light control, and climate via their iPhone; it also sends notifications to smartphones if alarms are triggered.

From your email account to your smartphone, there are already an incredible amount of devices for hackers to target. With wearables and their increasingly personal nature, the argument goes that fitness trackers and smartwatches are the latest potential goldmine for cybercriminals to tap into.

"How would you be interested in wearing/using a sensor device, assuming it was from a brand you trust, offering a service that interests you?"



Base: 4,657 US online adults (18+)
(multiple responses accepted)

Source: North American Technographics® Consumer Technology Survey, 2013

Source: Forrester Research, Inc.

Wearables and security aren't natural bedfellows, and every few months a new headline emerges about big-name devices that don't make the grade in terms of data privacy. While a recent study revealed that Pebble and Microsoft boasted the most secure wearables, it's not always clear exactly what the real-world risks are for those of us wearing devices susceptible to hackers.

Security researchers have proved that it's possible to snoop on the devices we're wearing on our bodies with the right code and enough determination - so just how concerned should we be?

Research reveals threat of wearables leaking password details

Researchers from Binghamton University and the Stevens Institute of Technology have revealed that wearable devices have the ability to leak passwords. In the paper, titled “Friend or Foe?: Your Wearable Devices Reveal Your Personal PIN”, the researchers collated data from embedded sensors in wearable technologies, such as smartwatches and fitness trackers, along with a computer algorithm to ascertain PINs and passwords. The team managed to crack the pin on the first attempt...

Wearables to be primary source of security breaches

Companies connecting wearables to their network have seen a nearly 100% increase, rising from 13% to 24% since Spiceworks released its 2014 IoT report. Video equipment (50%), physical security (46%) and appliances (45%) are the other sources liable to attack. Only around 33% of organisations are busy preparing for the effect IoT (Internet of Things) can have on the business though 90% of IT professionals believes the adoption of connected “things” leads to security and privacy issues at the workplace.

Kaspersky and WISeKey collaborate on cybersecurity for wearables

Kaspersky and WISeKey argue that wearables are particularly vulnerable to cyberattacks, and that several connected devices do not come with enough protection. The solution that results from the partnership will be hinged upon WISeKey's ‘Cryptographic Root of Trust for IoT’ system, which has been installed on over 2.6 billion desktops, browsers, mobile devices, SSL certificates and connected devices, and on its NFCTrusted technology.

Wearables & Security

‘Security technology’ was widely considered to be one of the major upcoming industries in past decade and it was felt that its time will come! That time is now! The sector's growing significance and generous government aid in leading economies has made the industry one of the winners in the decades to come.

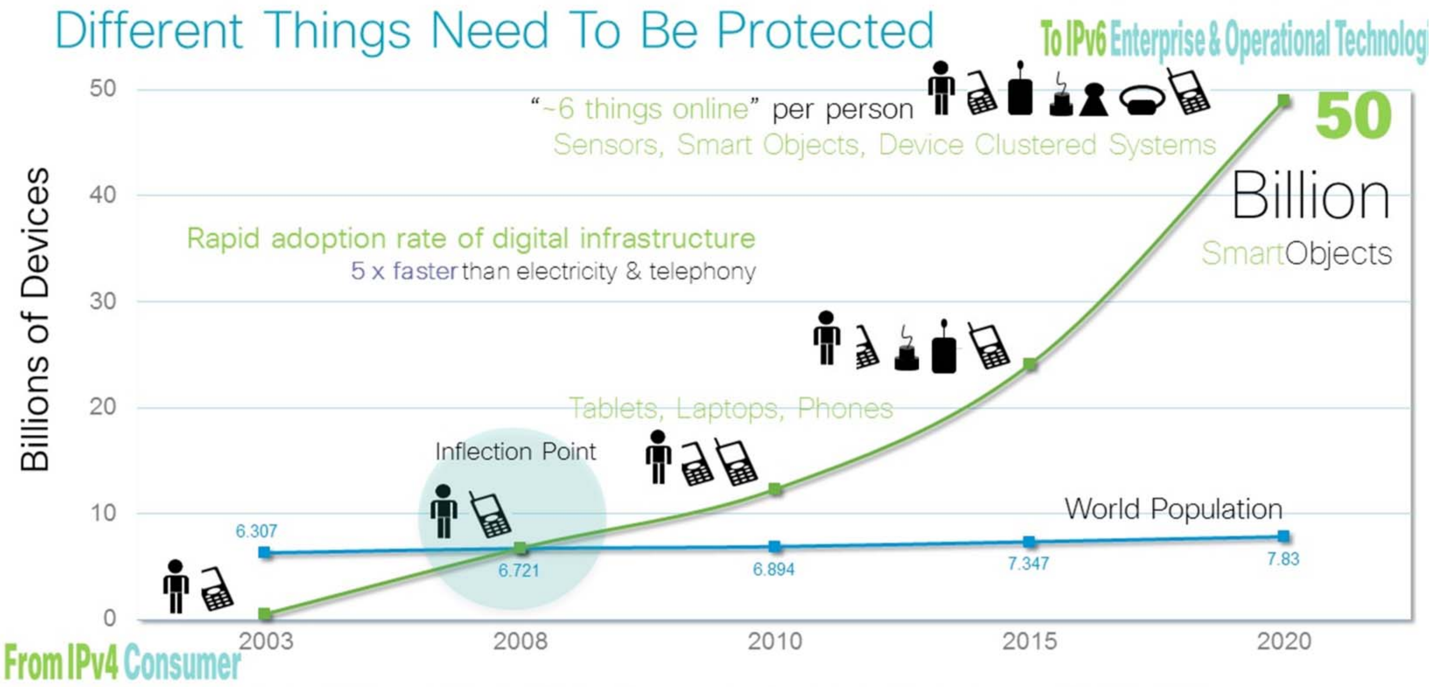
The dawn of this year promised to bring a bevy of new products and innovations to the physical security industry. End users continue to migrate away from legacy security systems towards technologies that enable them to be more proactive in mitigating their risks.

The investigation into the bombing at the Boston Marathon showed the potential waiting to be unlocked in using big data analytics to comb through troves of video evidence. The ability to remotely access and control security systems from mobile devices also continues to rise in prominence.

In the melee, 'wearable technology' is creating its niche. It will be used for hordes of security applications, major being –

- Personal Security - for individuals' own security
- Used by Security personnel
- Biometrics Identification for logging-in and other authorisations
- Data storage and data sharing / migration
- Access control System
- Remote Access to CCTV and data transfer through Smartphones
- Asset Monitoring and inventory Control
- Alarm Notifications & Verifications

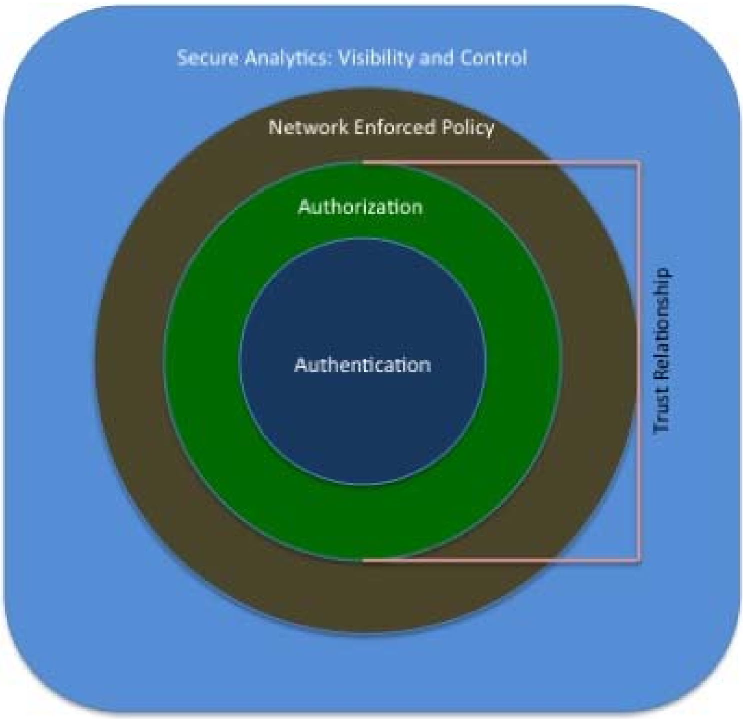
During 2014, we expected to see the first phases of mobile access deployments in which smartphones will function similar to that of a card transaction today, with limitations due to technology and business ecosystems. In subsequent phases, the phone's on-board computing power and multimedia capabilities will be leveraged to overcome limitations and provide a more functional and rich user experience.



Billions of connected devices promise to make our lives easier but can also carry serious security risks. The Internet of Things (IoT) presents unique security challenges that can only be addressed through intelligent management that ensures device control and security into the future.

In 2015, while looking forward, the connectivity of smartphones will now be used to perform most tasks that today are jointly executed by card readers and servers or panels in traditional access control systems. This includes verifying identity with rules such as whether the access request is within a permitted time and, using the phone's GPS capability, whether the person is actually in the vicinity of the door. The user can then be validated using a cloud application and granted access via a trusted message over secure communication to the door.

These wearable devices represent some appealing opportunities for businesses to increase efficiency and gather data, but in the rush to win market share, security concerns are taking a backseat for many manufacturers and app developers. The potential ramifications of unchecked wearable device usage within the enterprise are alarming.



Easy Physical Access to Data
The fact that many wearables store data on the local device without encryption is a real issue. There's often no PIN or password protection, no biometric security and no user authentication required to access data on a wearable. If it falls into the wrong hands, there's a risk that sensitive data could be accessed very easily.

Ability to Capture Photos, Videos and Audio
The kinds of discreet abilities that many modern wearable devices have in terms of video and audio surveillance surpass high-end spy gear from just a few years ago. It's easy for someone to surreptitiously take photographs or record video or audio files using something like a smartwatch or smart glasses. Covert capture of confidential information, and videos and images of sensitive areas, is a very real possibility.

Insecure Wireless Connectivity
The fact that wearable devices tend to connect to our smartphones or tablets wirelessly using protocols such as Bluetooth, NFC and Wi-Fi creates another potential point of entry. We may have Bluetooth on our smartphones turned on all the time now so they can sync with the wearable, but what else could be connecting? Many of these wireless communications are insufficiently secure to guard against a determined brute-force attack. The first step for securing networks is simply to get visibility on how many connected devices there are. One-third of the organizations surveyed by AT&T recently revealed they have more than 5,000 connected devices.

Lack of Encryption
We already mentioned the lack of encryption on many wearable devices, but there are also serious issues with data in transit when it's being synced and with data being stored on manufacturer's or service provider's cloud servers. Some third-party apps neglect basic security standards and send or store information that's not encrypted. The kind of data that's automatically being collected by wearables is very valuable to the right people.

No Regulation or Compliance
Because many of the security issues around wearables really have to be addressed by the manufacturers, the issue of whether they'll self-regulate or be bound by government regulations is an important one. In either case, companies suffering a data breach that breaks compliance or

regulatory requirements for their specific industry will not be able to shift the blame onto wearables. They'll still be held fully accountable. Ignorance of wearable device security and manufacturer or third-party app policy is no defence.

Control & Security

Billions of connected devices promise to make our lives easier but can also carry serious security risks. The Internet of Things (IoT) presents unique security challenges that can only be addressed through intelligent management that ensures device control and security into the future.

As technology becomes more entwined with the physical world, the consequences of security failure escalate. Already we have seen examples of car ignition systems failing, allowing engines to be started in the absence of the real authenticator. Since a computer now governs much of a car's engine, it requires little imagination to consider the potential disaster scenarios. Following would be key denominators for effective scalable security measures entwined with physical and logical security measures-

Security	Scalability	Monetization
• End to end security with hardened, multi-tenanted partitions • Devices and services are proactively monitored to automatically detect issues • Firmware updates to avoid device recalls and keep device configuration, downloaded applications and personal data secure	• Support for billions of endpoints on a single instance • Scalable, automated provisioning • Ability to manage cellular as well as the growing number of non-cellular device	• Create new revenue streams • Monetize small cell service faster • Reduce customer care costs

The wearable devices used by workforce in factories, sales Teams on ground and service providers in the areas will continuously stream the information to the Top Management providing them real time situational awareness and will provide them edge while taking strategic decisions and formulating their policies. For the Safety and security team, these wearable devices worn not only by their team members but by all the stakeholders will be a game changer! It will not only provide realistic information from Ground Zero but will also work as potent tool for decision making.

Stay secured! Happy New Year!!

ICISS at LinkedIn: http://www.linkedin.com/groups?gid=4413505&trk=hb_side_g
ICISS at Google Group: https://groups.google.com/forum/?fromgroups#!forum/icissm

Suggestions & feedback may be sent to us on e-mail: onlineicissm@gmail.com

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

Dates to Remember:

International Council of Industrial Security & Safety Management

Proudly presents

FSIE

FIRE & SECURITY INDIA EXPO

2017 FEB 23-25 www.fsie.in

IEML • Greater Noida • Delhi NCR

ICISS

onlineicissm.wixsite.com/iciss

a member of BUILD FAIR ALLIANCE Integrated Building Solutions

Secure not just the 'living'.
But 'life' itself.

The event that will change the way we look at
Fire & Security solutions in India

All ICISSM Members are requested to book their seats for the seminar under intimation to FSAI & ICISSM. For booking, please contact -

Jyoti Manaktala
FSAI Regional Head – North & East
Email: jyoti@fsai.in | Mobile: +91 9711198159

For information only please send mail to -

Yuvraj Bhushan
ICISSM Secretariat,
Email: onlineicissm@gmail.com