Research on Utilizing Smart Phone Security Application to Improve Mine Operational Safety

Yongqiang Wei
School of Resource and Safety Engineering,
University of Mining and Technology,
Beijing, China

***Abstract*—This paper studies the relationship between the workers stress level and accidental rate for the oil and mine industry. The results show that either too much negative stress or too less positive stress will cause more accidents. To adjust the stress level on the venue, we have proposed a smart phone secure application based remedy, to either increase or reduce the seasonal stress, by providing the instant on-the-job safety-inspection-training of reminding nature, or rest-time call between heavy-duty tasks with ergonomic exercising and relaxing music. Both remedies are designed in a proprietary encrypted multimedia format. The Java source code of the encryption is released to the community for further research.**

Keywords-encrypted smart phone; mine safety; remote training; infotainment

I. BACKGROUND

To improve and enhance the safety mining, several measures must be taken. Since 1996, multi-channel wireless communications systems are provided by Mine Radio Systems Inc (MRS) of Canada, throughout Africa, Australia, and the rest of the world. In addition, distributed antenna system can be used for the transmission of integrated service. Focusing on ICT based solutions [1], the web enablement of applications and other capabilities delivered over broadband communications systems can be used. Tele-robotics, wireless technologies, radio-frequency identification (RFID), and global positioning system (GPS) indoor extension technologies, which track the movement of workers and equipments are few other features that may be added in mines. Chinese coalpit mobile communication has experienced significant growth for years. From early 1990s, over 80% of large and medium-sized coal mines were equipped with domestic leakage and inductive wireless communications system; recently many WiFi or CDMA systems are also getting into the place.

The mine accident is caused by either high negative stress or no positive stress. To solve the problem, we suggest using Smart Phone network and system to either reduce negative pressure or maintain the positive stress, such that the accident will be kept minimum. Some of the early research on stress and muscular fatigue was conducted by Schell [2] and Rohmert [3]. The later found an exponential relationship between fatigue and recovery. In other words, a doubling of the fatigue level required a quadrupling of recovery time. Based on these results, Rohmert's recommendations for rest breaks were "little and often." This research and that of many others has culminated in the general recommendation that breaks should be taken "before the onset of fatigue not in order to recover." Based on these findings, we conclude that we need a smart phone to provide a short rest reminder, similar to Workpace software designed for PC worker, as a start point. The remainder will be expended to cover many more other functions to form a complete solution explained in following section.

II. SECURED INFOTAINMENT NETWORK

There are a few major Smart Phones in the market right now: Android, iPhone, Phone7 and BlackBerry etc. Android is a rising star for sure, for its rich open source background, from bottom Linux driver to the top free Apps. Android is a software stack for mobile devices that includes an operating system, middleware, and key applications, promoted by Google.

The open source approach has brought the cost down, at the same time; it may bring the hacker in. The mine and oil industry belongs to energy industry, which is an economy pillar for a country. This industry has a concern of security for their network. It is too early to conclude if Android could be a fit, lots of work on security ahead. Having examined both Android and iPhone; let's look at the rest. BlackBerry is made by a Canadian company called Research In Motion, which is in between Android and iPhone, it is not that open, and also not that close. The security level is high. Under its ISV program, vendors are offered necessary tools to do modification and customization for mine applications. However, the most important, BlackBerry uses the unique Push architecture, it allows the server to send the immediate multimedia messages to the client in an instant manner that is critical for the oil and mine industry (Figure 1).

Now we have a good understanding of the mine problem, and good understanding of BlackBerry capability, let's put together a solution for the industry. This solution consists of three high level strategies and eight daily tips.

The first strategy is to constantly strengthen the effectiveness of safety education and emphasize the building for long-term mechanism of it. Also, it is indispensable to realize the normalization,

institutionalization, and standardization with regard to safety knowledge. The second strategy is that safe and security education constitutes a most long-term key task throughout the process of safe production. It is impossible for employees to do regular operation all along by getting the knowledge just once or twice. On the contrary, we must stick to it, and keep it up year around. The demand for BlackBerry safety-book is expected to increase continuously. The focal point is to set up the thought of long-term effort. The layout of further planning will witness the importance of safety education as an on-going target. The last is to treat workers as the subject of safety issue, based on the policy of people-oriented. In the course of safe production, it is required to focus on the study of staff's varied stress law of physically and mentally. According to different skill and age levels of worker groups, it is also necessary to pay attention to research about their different psychological need. Depended on the stress level, two methods are used to make adjustment, either increasing the stress or reducing it. Besides, with the principle of prevention, the content and means of safe education should be known.

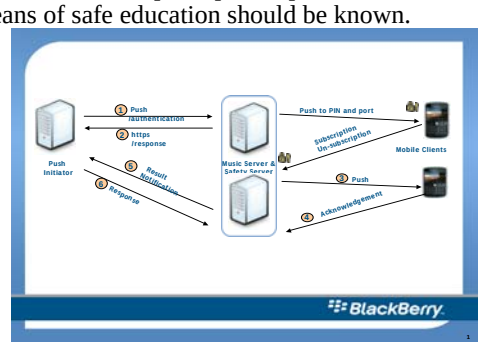

Figure 1. BlackBerry secured push architecture

Due to that the large amount of personal private data and sensitive corporate business data, an encryption is needed to protect the information going back and force between the wireless networks. We dedicate the next section to explain a proprietary multimedia encryption method.

III. JOINT ENCRYPTION SYSTEM (JES)

Data Encryption Standard (DES) was designed with an effective key length of 56 bits, which is vulnerable to exhaustive search. It also has some weaknesses against differential and linear cryptanalysis, due to its additive or confusion based mechanisms: these allow hacker to recover the key by comparing known plaintext such as a “never-changed” IP header against an encrypted block (an 8-byte block, for DES). In practical attack conditions, such as under VPN condition, large amounts of known text cannot be easily obtained, hence differential and linear cryptanalysis do not really impact too much of the actual security of DES; the weakest point is the short key.

A variant on DES is called 3DES: that’s, more or less, three DES instances in a row. This solves the key size issue: a 3DES key consists in 168 bits and exhaustive search on a 168-bit key is hard. However the price paid for it is three times computation, which is not very practical for battery powered handheld devices. Thus, Advanced Encryption Standard (AES) was defined with the following requirements:

- 128-bit blocks
- Accepts keys of size 128, 192, and 256 bits
- No worse than exhaustive key search
- Should be as fast as 3DES

The resistance of AES toward differential and linear cryptanalysis comes from a better “avalanche effect”—a bit flip at some point quickly propagates to the complete internal state; and specially designed bigger “S-boxes”—a small lookup table used within the algorithm, and is an easy way to add non-linearity; in DES, S-boxes have 6-bit inputs and 4-bit outputs; in AES, S-boxes have 8-bit inputs and 8-bit outputs. In mathematical term, AES has more diffusion operations than confusion ones.

However, both the key or data adding and shifting are still unnecessarily too complicated, note that both are linear operation, S-box operations are non-linear, but need extra memory. Especially, when we try to encrypt or decrypt the huge amount of image data on a small handheld device [4]. As such, we have proposed a non-linear diffusion dominated data centric encryption method to replace AES and DES algorithms, specifically for JPEG and MPEG encryption. In Ref. [5], we introduced the non-linear operation directly on to the data, instead of onto the key and then add on the data as AES or DES does; for this reason, we call our algorithm as one-step Joint Encryption System. The complexity analysis of JES was given there.

Following sample Java code is offered to share the principle of the JES algorithm for JPEG, with our academic research communities:

```
/* GenieviewLive.java
 * Copyright 2001-2011. GenieView Inc.
 * Any commercial use of the code requires written permission from the company.
// JES Multimedia Encryption Source Code
// Level I, Consumer Strength: Length=128.
    fec_blocks = leng/512;
//Number of bytes that are left over when dividing into 'fec_blocks' number of blocks.
leftOver = leng - (fec_blocks * 512);
//PART 1: ***JES DIFFUSSION ***
//Perform Encryption on every full block of data (236bytes or 59words).
for(encryption_count=0;encryption_count<fec_blocks; encryption_count++)
{
//For each block check each word against the EncryptionData key
//to determine whether or not the data should be swapped.
for (i=0; i<128; i++)
  {
  //If the key calls for swapping, swap the given word [0,1,2,3] -> [3,2,1,0].
```

```
If(key[i]==0x01)
{enc_swap_buffer[0]=bytes[(encryption_count*512)+(4*i
)];
enc_swap_buffer[1]=bytes[(encryption_count*512)+(4*i)
+1];
enc_swap_buffer[2]=bytes[(encryption_count*512)+(4*i)
+2];
enc_swap_buffer[3]=bytes[(encryption_count*512)+(4*i)
+3];
bytes[(encryption_count*512)+(4*i)]=enc_swap_buffer[3
];
bytes[(encryption_count*512)+(4*i)+1]=enc_swap_buffe
r[2];
bytes[(encryption_count*512)+(4*i)+2]=enc_swap_buffe
r[1];
      }
    }
  }
```

/*Perform Encryption on all complete remaining words. Any remaining bytes that do not form a complete word will be encrypted by Part 2 JES CONFUTION algorithm.

// Level II, Military Strength: Length=256.

// Omitted.

IV. APPLICATION DESIGN GUIDANCE

This section offers a design guidance for making the Java based applications, we take the safety book as an example, to explain how we can make use of the BlackBerry SDK to develop such applications. You can use the applications on a BlackBerry device or the BlackBerry Smartphone Simulator. The Simulator behaviors the exact the same as real BlackBerry, it is a great tool for debugging the applications.

Use BlackBerry UI components where possible so that your application can inherit the default behavior of the component. You can even build up your own browser dedicated to safety or music easily fitting the layout more extensible on BlackBerry devices with different screen sizes. Follow the standard interaction behaviors as closely as possible so that a particular user action produces a consistent result across applications. For example, allow users to see the next or previous image by swiping across the screen. Design a UI that allows users to explore the application without fear. Allow users to change their minds and undo commands. Be forgiving. Users sometimes click the wrong menu item or button accidentally. Create a seamless experience for users by anticipating tasks that users might need to do next. For example, play the safety or exercise clip automatically, if user doesn't manually stop.

Take advantage of known variables such as the location of the BlackBerry device. Early in the design process, consider designing your application so that it would be easy to localize it in different languages. BlackBerry devices applications are translated into over 30 languages, including languages that are not based on a Latin alphabet. The finished GUI design on the latest BlackBerry model will look like following pictures (Figures 2 and 3):

Figure 2. BlackBerry mine media entertainer

Figure 3. Rugged mine inspection reminder.

V. CONCLUDING REMARKS

In summary, the mine safety is a very interesting and very serious research topic, every idea, concept, design, test, line of code, is to save a life, if we could. In this paper, we have first analyzed the Mine accident statistics, from which we draw conclusion that some user-friendly instant reminding mechanisms needed to be put in place, conducting inspections with handheld devices produces inspection reports that include pictures, timestamps, and other critical data. A complete 3-8 suite of solution based on BlackBerry is proposed, and a strong but simple encryption source code is offered. The BlackBerry design customization of the interactive safety application is briefly illustrated. In the past, our university has already delivered Windows software and Linux software for the mine industry, but using BlackBerry Java program is new in progress, we plan to test it in mine usage early 2015.

VI. ACKNOWLEDGMENT

Great thanks go to Mr. Ruixin Zhang of *China University of Mining and Technology* for his help.

REFERENCES

[1] D. Srivastva, *An ICT Based Solutions to Make Mine Safer*. Open Access arXiv.org: 1007.1559, Cornell University Library, 2010.

[2] K.L. Schell, A.F. Grasha, State anxiety, performance accuracy, and work pace in a simulated pharmacy dispensing task. *Perceptual and Motor Skills*, **90**, pp. 547–561, 2000.

[3] W. Rohmert, Problems of determination of rest allowances. Part 1: Use of modern methods to evaluate stress and strain in static muscular work. *Applied Ergonomics*, **4**(2), pp. 91–95, 1973.

[4] I. Barbieri, P. Lambruschini, M. Raggio, et al., Real-time transmission and storage of video, audio, and health data in emergency and home care situations. *EURASIP Journal on Advances in Signal Processing*, University of Genova, 2007.

[5] J. Huang, H.X. Qian, Video encryption for security surveillance. *IEEE International Carnahan Conference on Security Technology*, pp. 207–211, 2007.