USING BIO-METRICS IN A ACCELERATOR PERONNEL SAFETY SYSTEM[*]

N. W. Williams[†], J. Reich, BNL, Upton, NY 11949, USA

Abstract

Local key trees were installed at the counting houses to minimize the time it takes for the Relativistic Heavy Ion Collider (RHIC) users to access the experimental areas. To further streamline the process, iris scanners are being used to verify the C-AD Access training required to release the access keys. Iris scanner technology was chosen based on its high reliability rating. Its rate of false identification is a factor of a 1000 lower than hand reader technology. This ensures more accurate tracking of users accessing beam enclosures. The advantages and disadvantages for using iris scanners in an experimental access system will be presented.

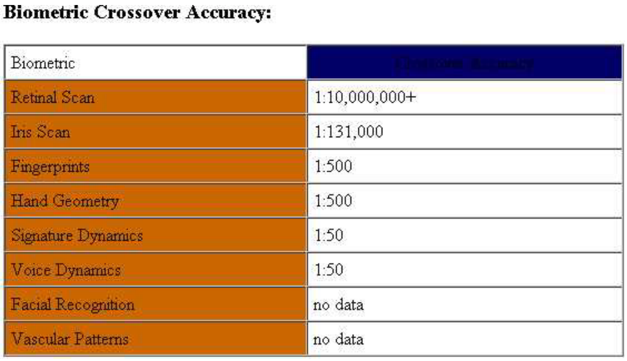
1. INTRODUCTION

From our experience of operating the RHIC over the past two years, we established that the time required for experimenters to access the beam enclosures took longer than expected or was acceptable. Under the original process for controlled access, an experimenter was required to travel 2-3 miles to the Main Control Room (MCR) to get access keys and have their training verified. This took an average of one hour for a short entry into an enclosure. To reduce the access time, local key trees were installed in the experimental counting houses. Iris scanners were installed to streamline the process of verifying C-AD User training required for access. It now takes experimenters 15-20 minutes to obtain access to their enclosures.

2. ACCESS CONTROLS SYSTEM

Most modern accelerator access control systems use PLCs for logic control. To streamline the access process Brookhaven National Laboratory (BNL) has incorporated biometrics into the RHIC and NASA Space Radiation Laboratory (NSRL) access systems. Iris-based identification and verification technology has now gained acceptance in a number of different areas. The technology in its early days was fairly cumbersome and expensive, however, recent technological breakthroughs have reduced both the size and price of iris recognition (also know informally as iris scan) devices. This, in turn, has allowed for much greater flexibility of implementation. Iris-based biometric technology has always been an exceptionally accurate one, and it may soon grow much more prominent.

The exceptionally high levels of accuracy provided by iris recognition technology, claimed to have a false acceptance rate of 1 in 10^{78}, broadened its applicability to high-risk, high-security installations.

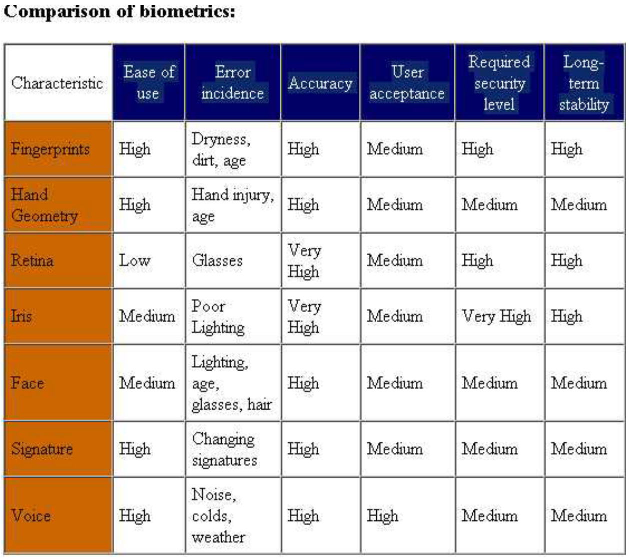


Biometric Crossover Accuracy:

Biometric	Crossover Accuracy
Retinal Scan	1:10,000,000+
Iris Scan	1:131,000
Fingerprints	1:500
Hand Geometry	1:500
Signature Dynamics	1:50
Voice Dynamics	1:50
Facial Recognition	no data
Vascular Patterns	no data

Fig. 1

In addition the user acceptance of iris scanner is very favorable in comparison to other biometric technologies (fig. 2)



Comparison of biometrics:

Characteristic	Ease of use	Error incidence	Accuracy	User acceptance	Required security level	Long-term stability
Fingerprints	High	Dryness, dirt, age	High	Medium	High	High
Hand Geometry	High	Hand injury, age	High	Medium	Medium	Medium
Retina	Low	Glasses	Very High	Medium	High	High
Iris	Medium	Poor Lighting	Very High	Medium	Very High	High
Face	Medium	Lighting, age, glasses, hair	High	Medium	Medium	Medium
Signature	High	Changing signatures	High	Medium	Medium	Medium
Voice	High	Noise, colds, weather	High	High	Medium	Medium

Fig. 2

3. IMPLEMENTATION

The Iris Access networks at RHIC consist of six remote scanners and an enrollment system (see fig. 3).

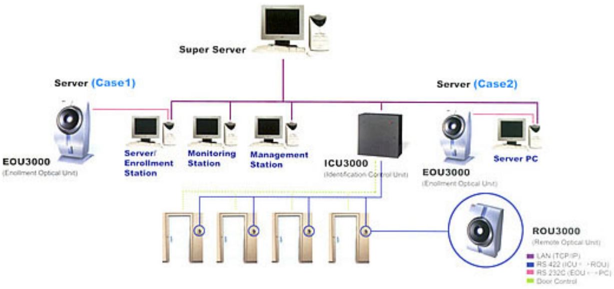


Fig. 3, typical configuration.

Using transaction-encrypted, TCP/IP communication, the Iris Access system can control access to a primary area using the outreach of the organization's Intranet, and up to 254 remote doors over the Internet.

A typical iris access system at a RHIC access gate consists of a key tree box (five keys), a remote iris camera and engine (see fig. 4).

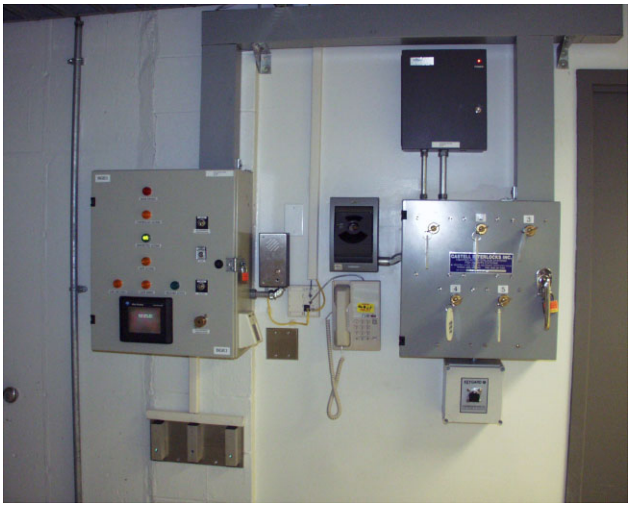
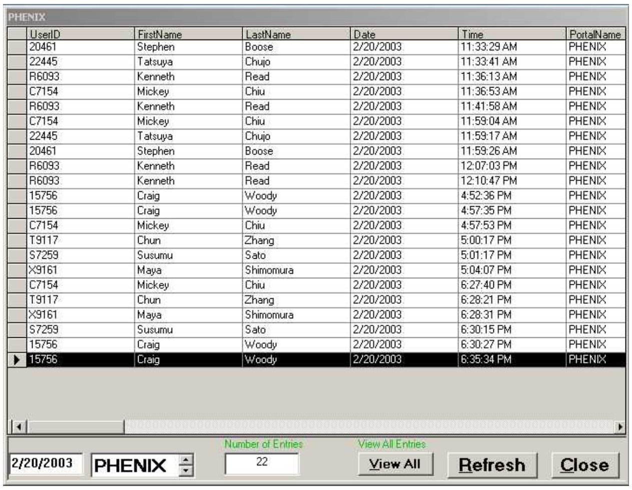


Fig. 4

The server's software has two major elements — a data component, which stores IrisCode® records, and a processing engine that enrolls IrisCode records and performs real-time matching. The server enrolls the image into the database while establishing links to the enrollment information database. During recognition, the KnoWho Authentication Server accepts an iris image and performs a high speed, real-time, exhaustive search to match the IrisCode templates. The MCR operator reviews the record, which is logged (see Fig. 5).



PHENIX

UserID	FirstName	LastName	Date	Time	PortalName
20461	Stephen	Boose	2/20/2003	11:33:29 AM	PHENIX
22445	Tatsuya	Chujo	2/20/2003	11:33:41 AM	PHENIX
R6093	Kenneth	Read	2/20/2003	11:36:13 AM	PHENIX
C7154	Mickey	Chiu	2/20/2003	11:36:53 AM	PHENIX
R6093	Kenneth	Read	2/20/2003	11:41:58 AM	PHENIX
C7154	Mickey	Chiu	2/20/2003	11:59:04 AM	PHENIX
22445	Tatsuya	Chujo	2/20/2003	11:59:17 AM	PHENIX
20461	Stephen	Boose	2/20/2003	11:59:26 AM	PHENIX
R6093	Kenneth	Read	2/20/2003	12:07:03 PM	PHENIX
R6093	Kenneth	Read	2/20/2003	12:10:47 PM	PHENIX
15756	Craig	Woody	2/20/2003	4:52:36 PM	PHENIX
15756	Craig	Woody	2/20/2003	4:57:35 PM	PHENIX
C7154	Mickey	Chiu	2/20/2003	4:57:53 PM	PHENIX
T9117	Chun	Zhang	2/20/2003	5:00:17 PM	PHENIX
S7259	Susumu	Sato	2/20/2003	5:01:17 PM	PHENIX
X9161	Maya	Shimomura	2/20/2003	5:04:07 PM	PHENIX
C7154	Mickey	Chiu	2/20/2003	6:27:40 PM	PHENIX
T9117	Chun	Zhang	2/20/2003	6:28:21 PM	PHENIX
X9161	Maya	Shimomura	2/20/2003	6:28:31 PM	PHENIX
S7259	Susumu	Sato	2/20/2003	6:30:15 PM	PHENIX
15756	Craig	Woody	2/20/2003	6:30:27 PM	PHENIX
15756	Craig	Woody	2/20/2003	6:35:34 PM	PHENIX

2/20/2003 PHENIX

Number of Entries: 22

View All Entries

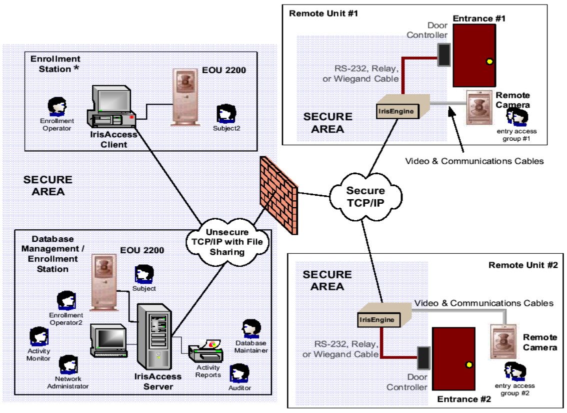
Fig. 5

The C-AD training section administers the enrollment database. Prior to being enrolled, a user's C-AD access training is verified. Figure 6 shows an enrollment activity being executed in MCR.

Fig. 6

4 CYBER SECURITY

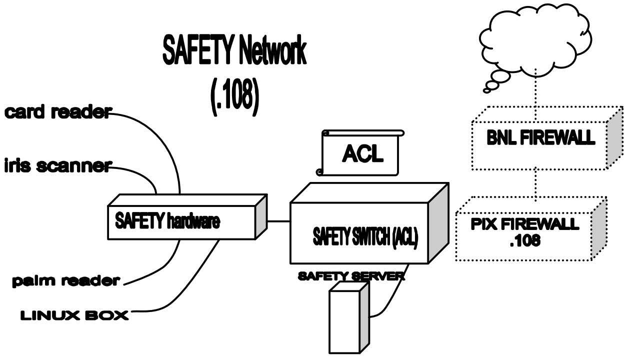
In addition to the native security measures implemented in the iris access software, a network configuration employing multiple layers of firewalls was installed. A dedicated firewall consisting of a Cisco PIX 500 Series firewall with standards-based IPsec Virtual Private Networking (VPN). This is located between a department level firewall with ACL network switches and PC server.



* All Client/Enrollment Station functions may be handled by the Server.

Figure 1: An IrisAccess Network

Fig. 7



5 ADVANTAGES/DISADVANTAGES FOR USING IRIS SCANNERS

Advantages

Some of the benefits for using the iris scanner include:

- Reduction of the turn around time for user access into the experimental areas. Since the access keys are located at the counting houses, access that used to take an hour has been reduced to 15 - 20 minutes. This is very important to the users since it resulted in more beam time.
- Verification that a user’s access training is valid prior to releasing a token. Each user is required to take annual department specific training before they are allowed to use the facility. The training group administers this training and enrolls users into the iris access database.
- Highest user acceptance of all the biometric technologies. Iris scanners are very accurate with a false acceptance rate of 1 in 10^{78}.
- Minimal training to configure the IrisAccess software since it is Windows based. Automatic logging of scanned personnel during access provides accurate tracking and archiving.
- No known health effects. Users were initially concerned about the health effects from using iris recognition system. The iris scanner takes a video picture of your iris, unlike a retinal scanner that uses a laser to map the retina.
- Identification occurs in 2 seconds.
- CCD Camera is auto focus.
- No password or PIN to remember.

Disadvantages

Some of the disadvantages for using iris scanners include:

- Significant administration to create and maintain the iris access database. As users come in, they must enroll into the iris access database. When users’ training expire, they are manually removed from the system and re-entered when they receive training once again.
- The initial cost to implement the iris access system at BNL is high. To date we have spent a total of ~$60K on hardware and installation. The incremental cost to install more remote iris units is ~$5K per location.
- To our surprise, the political aspect of using iris scanners is the highest hurdle. Of ~ 1000 RHIC users, 25% refused to enroll in the Iris Access system. We had to provide legal assurance that BNL would not release iris records to external authorities (Homeland Security, etc.).

6 CONCLUSION

Using iris scanners in the C-AD access control system has resulted in ensuring that only users with valid training gain access into beam enclosures. From the user’s perspective, iris scanners have increased the beam time availability for physics due to shortened access time. This has also improved the ability for MCR to track users during entries.

7 REFERENCE

[1] IrisAccess v10 Entry Access Control System, Iridian Technologies Document Number: 101903, Iridian Technology, March 18th, 2002

[2] How Iris Recognition Works, John Daugman, PhD University of Cambridge, Cambridge CB2 3QG, U.K.

[3] Various internal documents, C-AD BNL