Security Design of a Computer-Based Personnel Safety System Logbook

Theo McGuckin

Presentation “Finalization”

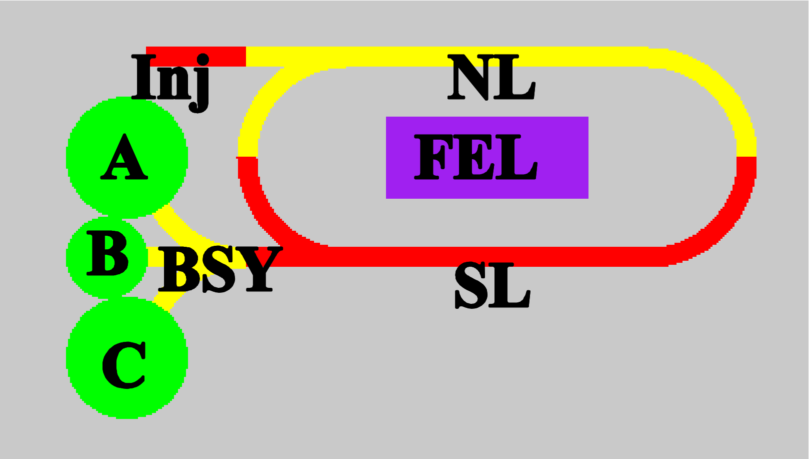
Overview

- Definitions & Background Information
  - Definitions
  - PSS Background Information
  - Paper Logbook
- Requirements & Implementations
  - User Support
  - Security & the User
- User Interface
  - Paper Log Emulation
  - Webpage View
- Conclusions

Definitions

- **PSS** [Personnel Safety System] – the administrative and engineering systems used to protect personnel entering the accelerator
- **SSO** [Safety System Operator] – the individual in charge of performing state changes in the PSS system and allowing accesses under Controlled Access
- **Stamp Entry** – A logbook entry used to record a state change in a segment of the accelerator
- **Access Entry** – A logbook entry used to record information about an individual accessing a segment of the accelerator
- **Autolog** – A logbook entry automatically made by monitoring software to record physical changes in the state of a segment of the accelerator

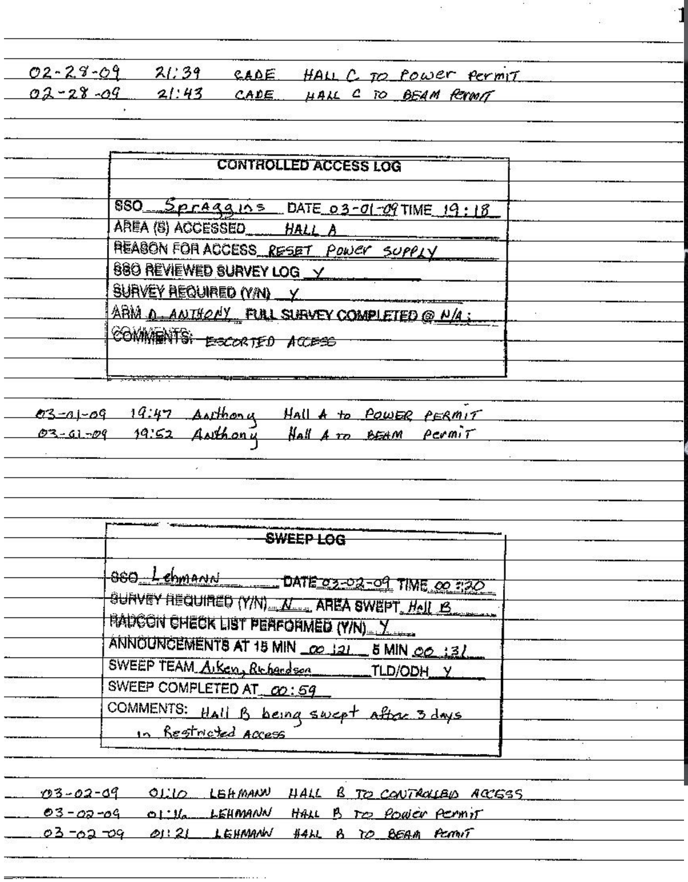
PSS Background Information



- PSS System is divided into eight segments that can each be in different states
- PSS System has five states that are logged:
  - Beam Permit (Purple) - **no access**
  - Power Permit (Red) - **no access**
  - Controlled Access (Yellow) - **logged access**
  - Sweep (Yellow) - **no access** (accept sweepers)
  - Restricted Access (Green) - **unlogged access**

Paper Logbook

Stamps



02-28-09 21:39 CADE HALL C TO Power Permit
02-28-09 21:43 CADE HALL C TO BEAM Permit

CONTROLLED ACCESS LOG

SSO Spraggins DATE 03-01-09 TIME 19:18
AREA (S) ACCESSED HALL A
REASON FOR ACCESS RESET Power SUPPLY
SSO REVIEWED SURVEY LOG Y
SURVEY REQUIRED (Y/N) Y
ARM D. ANTHONY FULL SURVEY COMPLETED @ N/A;
COMMENTS: ESCORTED ACCESS

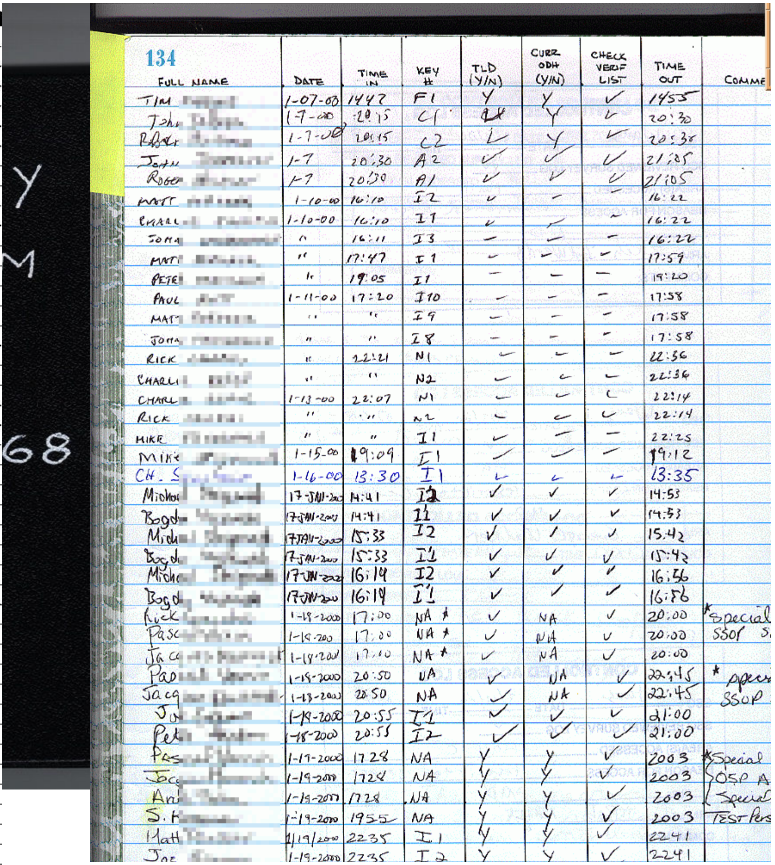
03-01-09 19:47 Anthony Hall A to POWER PERMIT
03-01-09 19:52 Anthony Hall A to BEAM Permit

SWEEP LOG

SSO Lehmann DATE 03-02-09 TIME 00:20
SURVEY REQUIRED (Y/N) N AREA SWEPT Hall B
RADCON CHECK LIST PERFORMED (Y/N) Y
ANNOUNCEMENTS AT 15 MIN 00:21 5 MIN 00:31
SWEEP TEAM Aiken, Richardson TLD/ODH Y
SWEEP COMPLETED AT 00:59
COMMENTS: Hall B being swept after 3 days in Restricted Access

03-02-09 01:10 LEHMANN HALL B TO CONTROLLED ACCESS
03-02-09 01:16 LEHMANN HALL B TO Power Permit
03-02-09 01:21 LEHMANN HALL B TO BEAM Permit

Accesses



134

FULL NAME	DATE	TIME IN	KEY #	TLD (Y/N)	CURR ODH (Y/N)	CHECK VERIF LIST	TIME OUT	COMME
TIM [redacted]	1-07-00	1447	F1	Y	Y	✓	1455	
John [redacted]	1-7-00	20:15	C1	Y	Y	✓	20:30	
Robr [redacted]	1-7-00	20:15	C2	✓	Y	✓	20:38	
John [redacted]	1-7	20:30	A2	✓	✓	✓	21:05	
Roger [redacted]	1-7	20:30	A1	✓	✓	✓	21:05	
MATT [redacted]	1-10-00	16:10	I2	✓	–	–	16:22	
CHARL [redacted]	1-10-00	16:10	I1	✓	✓	–	16:22	
JOHN [redacted]	"	16:11	I3	–	✓	–	16:22	
MATT [redacted]	"	17:47	I1	✓	✓	✓	17:59	
PETE [redacted]	"	19:05	I1	–	–	–	19:20	
PAUL [redacted]	1-11-00	17:20	I10	–	–	–	17:58	
MATT [redacted]	"	"	I9	–	–	–	17:58	
JOHN [redacted]	"	"	I8	–	–	–	17:58	
RICK [redacted]	"	22:21	N1	✓	✓	✓	22:36	
CHARLI [redacted]	"	"	N2	✓	✓	✓	22:36	
CHARL [redacted]	1-13-00	22:07	N1	✓	✓	✓	22:14	
RICK [redacted]	"	"	N2	✓	✓	✓	22:14	
MIKE [redacted]	"	"	I1	✓	–	–	22:25	
MIKE [redacted]	1-15-00	19:09	I1	✓	✓	✓	19:12	
CH. S [redacted]	1-16-00	13:30	I1	✓	✓	✓	13:35	
Micha [redacted]	17-JAN-2000	14:41	I2	✓	✓	✓	14:53	
Bogd [redacted]	17-JAN-2000	14:41	I1	✓	✓	✓	14:53	
Mich [redacted]	17JAN-2000	15:33	I2	✓	✓	✓	15:42	
Bogd [redacted]	17-JAN-2000	15:33	I1	✓	✓	✓	15:42	
Mich [redacted]	17-JAN-2000	16:14	I2	✓	✓	✓	16:36	
Bogd [redacted]	17-JAN-2000	16:14	I1	✓	✓	✓	16:56	
Rick [redacted]	1-18-2000	17:00	NA *	✓	NA	✓	20:00	*Special
Pasc [redacted]	1-18-200	17:00	NA *	✓	NA	✓	20:00	SSOP S.
Jac [redacted]	1-18-2000	17:10	NA *	✓	NA	✓	20:00	
Pa [redacted]	1-18-2000	20:50	NA	✓	NA	✓	22:45	* Special
Jacq [redacted]	1-18-2000	20:50	NA	✓	NA	✓	22:45	SSOP
J [redacted]	1-18-2000	20:55	I1	✓	✓	✓	21:00	
Pet [redacted]	1-18-2000	20:55	I2	✓	✓	✓	21:00	
Pas [redacted]	1-19-2000	1728	NA	Y	Y	✓	2003	*Special
Jac [redacted]	1-19-2000	1728	NA	Y	Y	✓	2003	OSP A
An [redacted]	1-19-2000	1728	NA	Y	Y	✓	2003	Special
S. K [redacted]	1-19-2000	1955	NA	Y	Y	✓	2003	TEST Pers
Matt [redacted]	1/19/2000	2235	I1	Y	Y	✓	2241	
Joe [redacted]	1-19-2000	2235	I2	Y	Y	✓	2241	

REQUIREMENTS AND IMPLEMENTATIONS

Requirements

- 68 page Requirements Document
- Will not be going over entire document (of course)
- The requirements were published in ~2001 but the project didn’t make much progress for several years
- The project was restarted last year with broader input from user groups
- Talk will focus on security and design elements that were chosen to minimize negative impact on the users

User Support

- The Safety System Group and Accelerator Operations were primary customers for the new logbook
- Without their support, the project would not move forward
- Security features therefore, while essential, could not adversely impact operation of the user-interface
- **A core philosophy of the design was then to mask security from the user as much as possible and, where possible, use security features to enhance the user-interface**

Site Security

Computer Security

PSS elog computer must be resistant to network interruptions and tampering

- Dell Workstation running Redhat Enterprise Linux OS
- RF card reader connected through standard USB port for user authentication (with ID badge)
- Stand-alone system with minimal dependencies
  - No NFS participation
  - No NIS participation
  - Only local (auto-login) and admin account
  - Connection to database machine required
  - NTP to keep SSO entries and Autologs in time-sync

Computer Security (Cont.)

Source of each entry must be unique and recorded

Only two machines have required permissions to make entries to the PSS database:

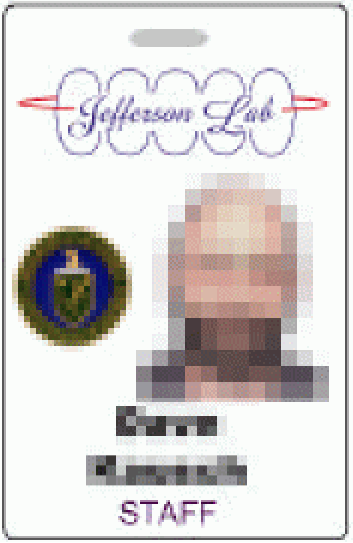
- A local workstation running Linux in kiosk-mode
- A network server running a daemon to autolog state changes in the PSS-system

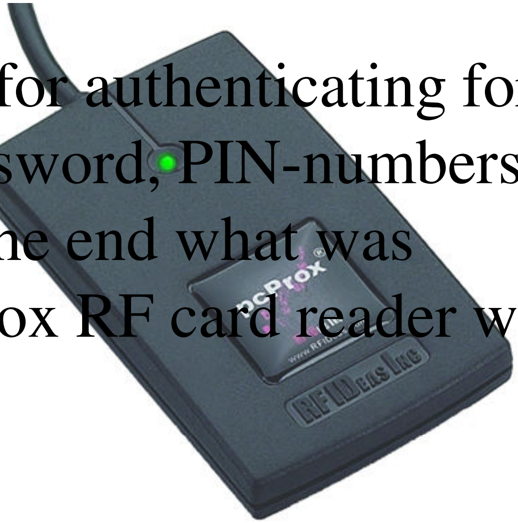
Benefits to user:

- Kiosk-mode on PSS workstation means using the SSO workstation is simpler.
- Autologs track state-changes in the machine with no input necessary from SSO.

Computer Security (Cont.)

SSO must be identified for each entry submitted to the database





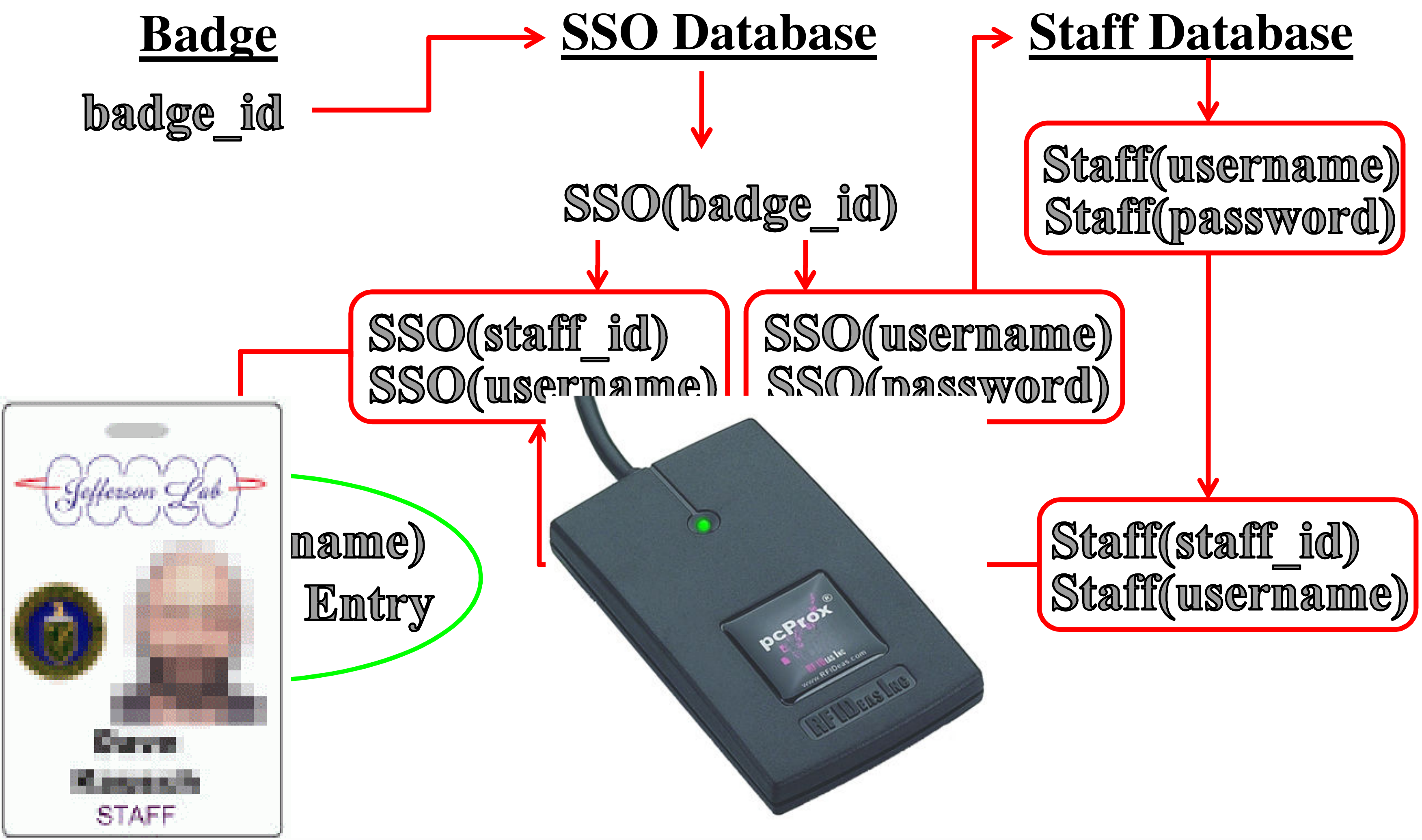
Sever were suggested for authenticating for each ng username/password, PIN-numbers and e nt scanning. In the end what was decid n RF Ideas pcProx RF card reader with the S D badge.

Benefits to user:

- SSO's can make dozens of entries in an hour. Having to type username/password for each would be onerous
- Using existing technology (Jlab badges) means using an existing system (users already "swipe their badge" to get on site, access buildings, etc.)
- No additional PII (finger-prints) needed to be recorded/stored

Login & Badge Security

SSO must be identified for each entry submitted to database



Badge

badge_id

SSO Database

SSO(badge_id)

SSO(staff_id)
SSO(username)

SSO(username)
SSO(password)

Staff Database

Staff(username)
Staff(password)

Staff(staff_id)
Staff(username)

name)
Entry

Program Security

No data can be lost due to suspension/halting of the application

/var/tmp

All data being en is automatically logged to to several r periodically. If a e data is automatically ret emp-file or the database when the is restarted.

Benefits to user:

- Data that an SSO is entering cannot be lost due to simple user-error, computer-failure or other problems.
- SSO does not have to figure out where temp-data is stored or how to retrieve it in the event of a crash. Data retrieval is automatic on application launch.
- An audit log of all changes to open entries is maintained and can be referred back to if necessary (more on this later).

Program Security (Cont.)

Access entries must be able to track multiple SSO’s

Access Entries have separate time_in and time_out fields that can be filled in by different SSO’s (recorded in corresponding SSO_IN and SSO_OUT fields).

Benefits to user:

- Multiple SSO’s routinely trade duties during a shift or between shifts. Making the user track which SSO made which entry would be almost impossible. All the tracking is handled, instead behind the scenes automatically.
- An Access can last for hours and/or span multiple work shifts. Having to keep a single SSO for extended durations would be unreasonable, separating the SSO field into SSO_IN and SSO_OUT alleviates this problem.

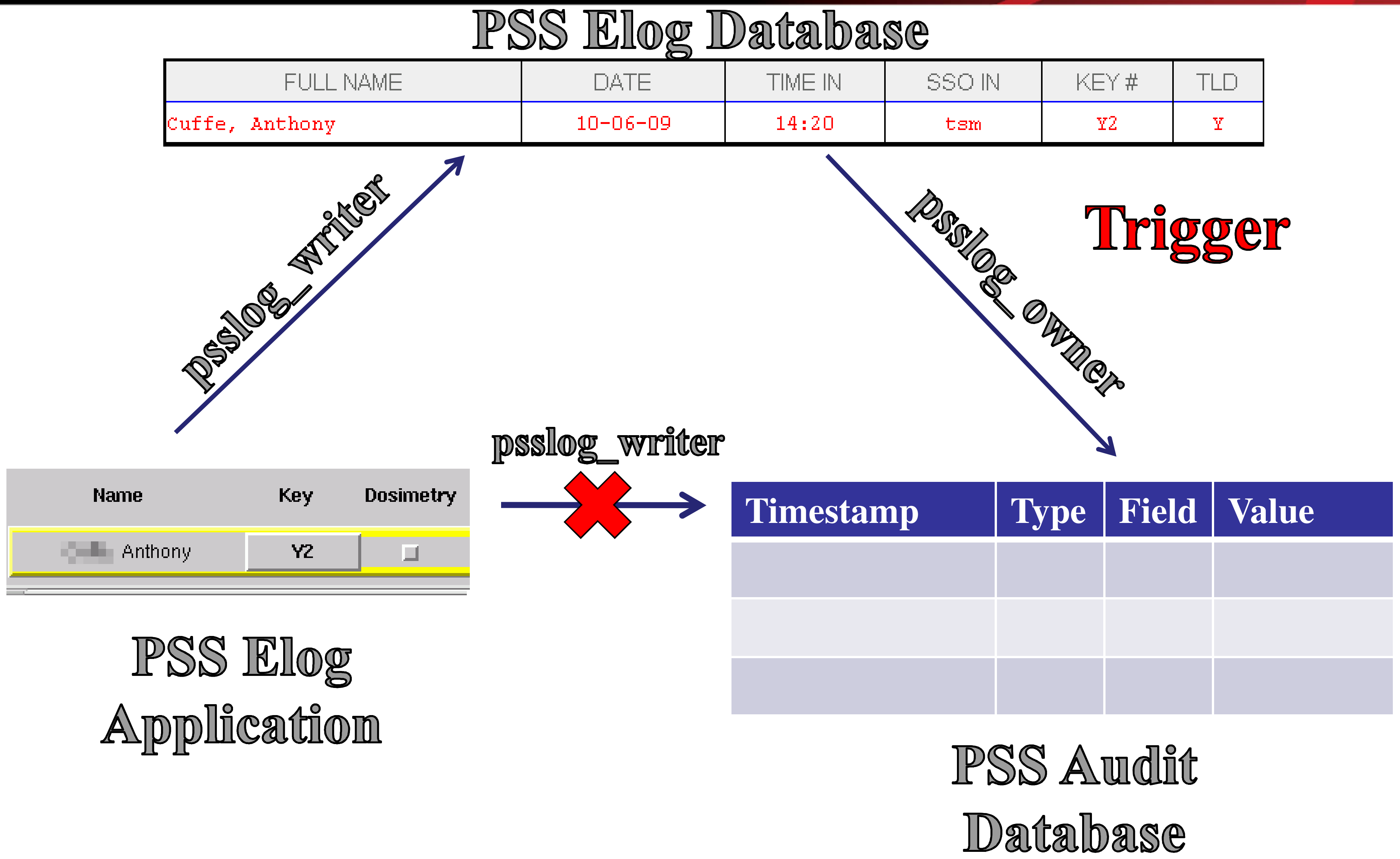
Database Security

Any changes to an entry prior to submission must be recorded

The underlying PSS database was built with two layers.

- The database table itself is writable by user psslog_writer, and data in this table can be modified until the final entry is submitted
- There is also an Audit log that is writable only by user psslog_owner, whenever the database table is written-to a trigger event automatically writes to the Audit log, recording the data change

Database Security (Cont.)



PSS Elog Database

FULL NAME	DATE	TIME IN	SSO IN	KEY #	TLD
Cuffe, Anthony	10-06-09	14:20	tsm	Y2	Y

Name	Key	Dosimetry
[redacted] Anthony	Y2	☐

PSS Elog Application

Timestamp	Type	Field	Value

PSS Audit Database

Database Security (Cont.)

- **Benefits to user:**
  - Simple errors (like typing mistakes) can be corrected by SSO (prior to submission) without complicated verification procedures or additional logging of information
  - At the same time, any corrections are recorded and no data is lost thanks to the Audit table
  - The interface remains simple to use while still satisfying a requirement that ALL data changes be recorded

Database Security (Cont.)

An entry cannot be alterable after submission to the database

By not allowing **psslog_writer** to access the Audit Database a clear step-by-step log of events is maintained.

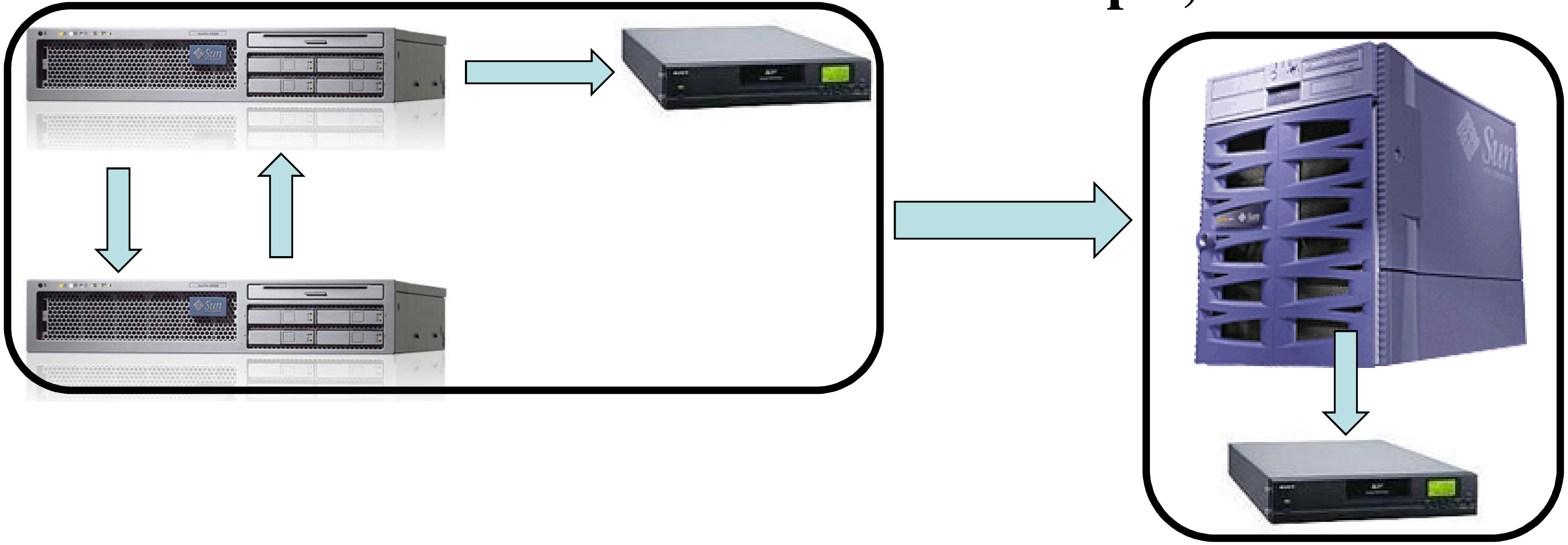
Likewise, once an entry has been submitted to the PSS Database and finalized, it can no longer be modified by **psslog_writer** or **psslog_owner**.

Benefits to user:

- Primary benefit is that all this processing occurs in the background on the database server. To the SSO/user an open entry can be created, modified and submitted without any knowledge of the underlying processes.

Database Security (Cont.)

Database records must be retained in multiple, secure locations



Database records are also stored in multiple formats:

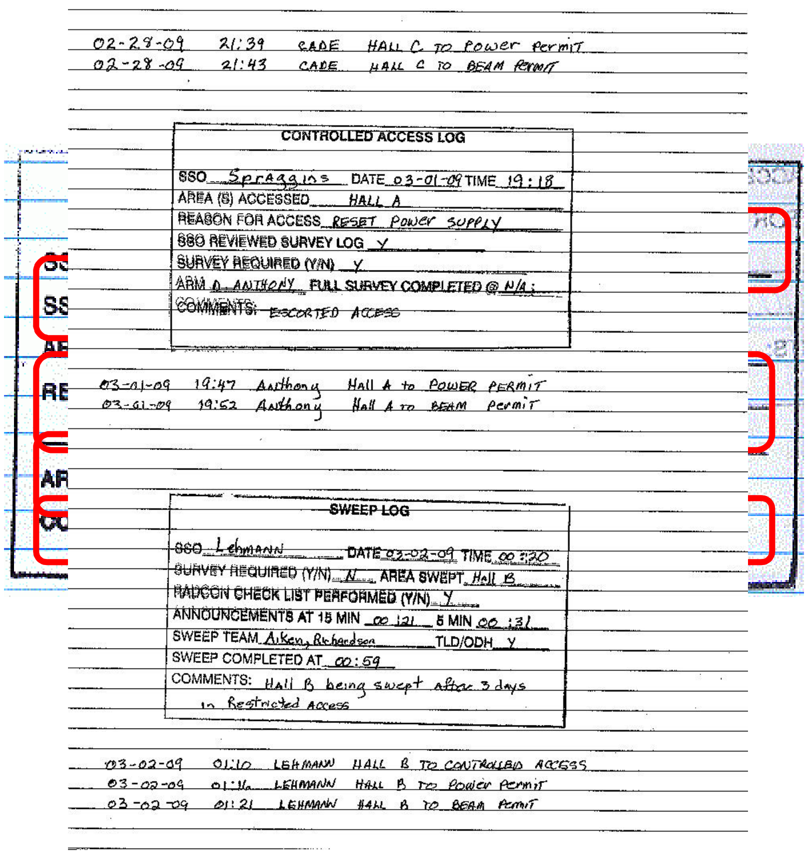
- Oracle database records
- Xml-format text file
- And a flat text file

This means all three file-types in all locations would have to changed for information to be altered maliciously.

USER INTERFACE

Paper Logbook Emulation

Stamp Entry



02-28-09 21:39 CADE HALL C TO Power Permit
02-28-09 21:43 CADE HALL C TO BEAM Permit

CONTROLLED ACCESS LOG

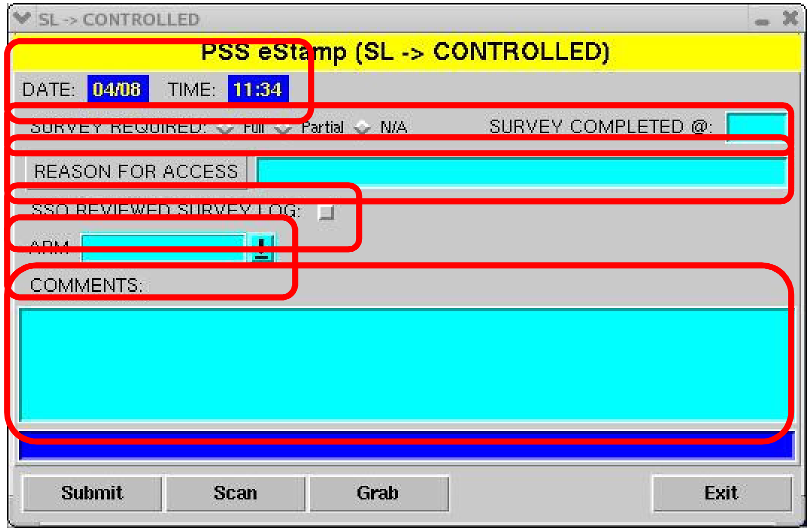
SSO Spraggins DATE 03-01-09 TIME 19:18
AREA (S) ACCESSED HALL A
REASON FOR ACCESS RESET Power SUPPLY
SSO REVIEWED SURVEY LOG Y
SURVEY REQUIRED (Y/N) Y
ARM D. ANTHONY FULL SURVEY COMPLETED @ N/A :
COMMENTS: ESCORTED ACCESS

03-01-09 19:47 Anthony Hall A to POWER PERMIT
03-01-09 19:52 Anthony Hall A TO BEAM Permit

SWEEP LOG

SSO Lehmann DATE 03-02-09 TIME 00:20
SURVEY REQUIRED (Y/N) N AREA SWEPT Hall B
RADCON CHECK LIST PERFORMED (Y/N) Y
ANNOUNCEMENTS AT 15 MIN 00:21 5 MIN 00:31
SWEEP TEAM Aiken, Richardson TLD/ODH Y
SWEEP COMPLETED AT 00:59
COMMENTS: Hall B being swept after 3 days in Restricted Access

03-02-09 01:10 LEHMANN HALL B TO CONTROLLED ACCESS
03-02-09 01:16 LEHMANN HALL B TO Power Permit
03-02-09 01:21 LEHMANN HALL B TO BEAM Permit



SL -> CONTROLLED

PSS eStamp (SL -> CONTROLLED)

DATE: 04/08 TIME: 11:34

SURVEY REQUIRED: ◇ Full ◇ Partial ◇ N/A SURVEY COMPLETED @:

REASON FOR ACCESS

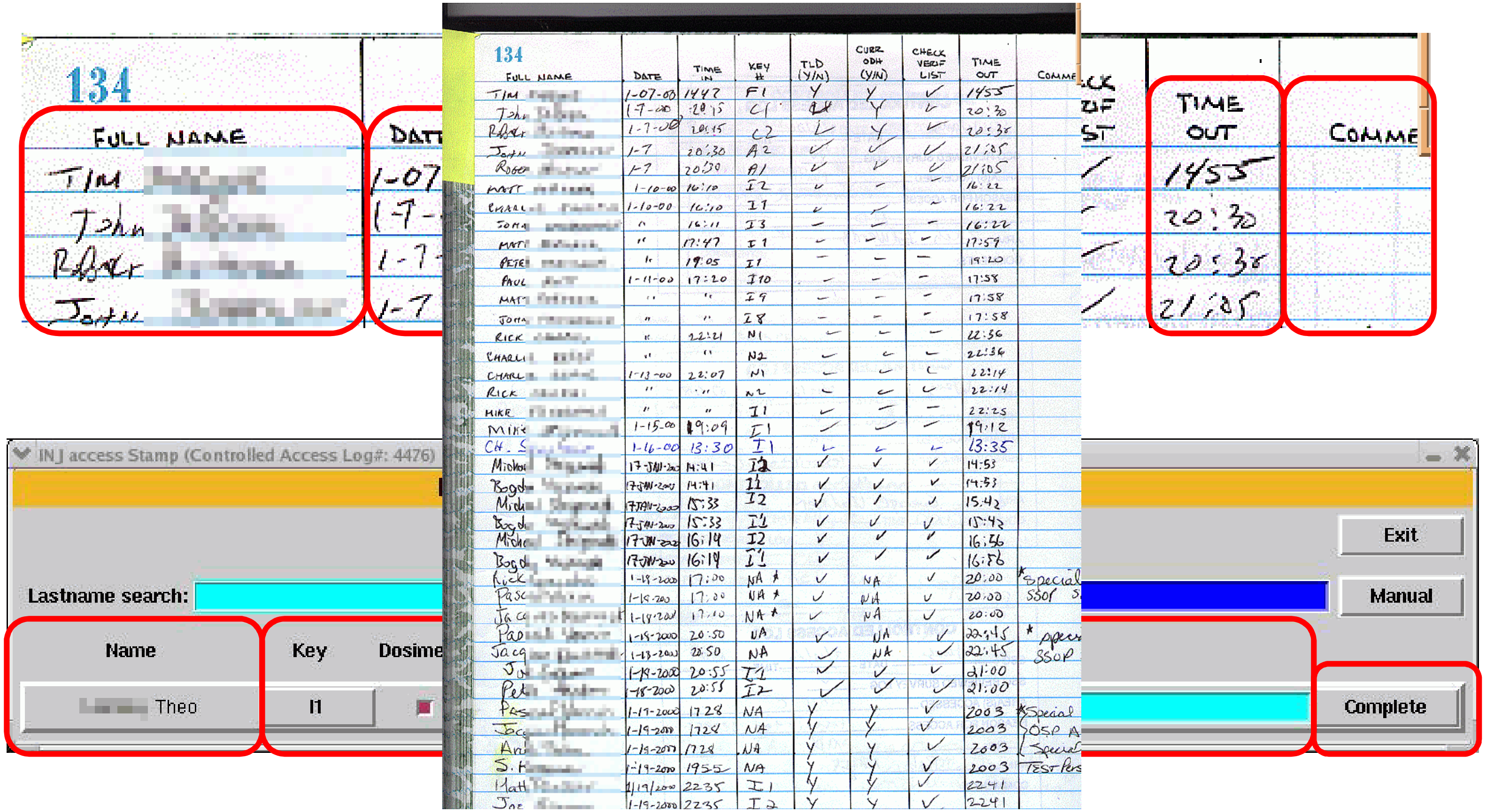
SSO REVIEWED SURVEY LOG: □

ARM:

COMMENTS:

Paper Logbook Emulation (Cont.)

Access Entry


FULL NAME
DATE
TIME OUT
COMME

134

FULL NAME	DATE	TIME IN	KEY #	TLD (Y/N)	CURR ODH (Y/N)	CHECK VERIF LIST	TIME OUT	COMME
TIM [redacted]	1-07-00	1447	F1	Y	Y	✓	1455	
John [redacted]	1-7-00	20:15	C1	Y	Y	✓	20:30	
Rbbr [redacted]	1-7-00	20:15	C2	✓	Y	✓	20:38	
John [redacted]	1-7	20:30	A2	✓	✓	✓	21:05	
Roger [redacted]	1-7	20:30	A1	✓	✓	✓	21:05	
MATT [redacted]	1-10-00	16:10	I2	✓	–	–	16:22	
CHARL [redacted]	1-10-00	16:10	I1	✓	✓	–	16:22	
JOHN [redacted]	"	16:11	I3	–	–	–	16:22	
MATT [redacted]	"	17:47	I1	–	–	–	17:59	
PETE [redacted]	"	19:05	I1	–	–	–	19:20	
PAUL [redacted]	1-11-00	17:20	I10	–	–	–	17:58	
MATT [redacted]	"	"	I9	–	–	–	17:58	
JOHN [redacted]	"	"	I8	–	–	–	17:58	
RICK [redacted]	"	22:21	N1	✓	–	–	22:36	
CHARLI [redacted]	"	"	N2	✓	✓	–	22:36	
CHARL [redacted]	1-13-00	22:07	N1	✓	✓	✓	22:14	
RICK [redacted]	"	"	N2	✓	✓	✓	22:14	
MIKE [redacted]	"	"	I1	✓	–	–	22:25	
MIKE [redacted]	1-15-00	19:09	I1	✓	✓	–	19:12	
CH. S [redacted]	1-16-00	13:30	I1	✓	✓	✓	13:35	
Michael [redacted]	17-JAN-2000	14:41	I2	✓	✓	✓	14:53	
Bogd [redacted]	17-JAN-2000	14:41	I1	✓	✓	✓	14:53	
Michael [redacted]	17-JAN-2000	15:33	I2	✓	/	✓	15:42	
Bogd [redacted]	17-JAN-2000	15:33	I1	✓	✓	✓	15:42	
Michael [redacted]	17-JAN-2000	16:19	I2	✓	✓	✓	16:36	
Bogd [redacted]	17-JAN-2000	16:19	I1	✓	✓	✓	16:56	
Rick [redacted]	1-18-2000	17:00	NA *	✓	NA	✓	20:00	*special
Pasc [redacted]	1-18-200	17:00	NA *	✓	NA	✓	20:00	SSOP S
Jac [redacted]	1-18-2000	17:00	NA *	✓	NA	✓	20:00	
Pa [redacted]	1-18-2000	20:50	NA	✓	NA	✓	22:45	* Spec
Jacq [redacted]	1-18-2000	20:50	NA	✓	NA	✓	22:45	SSOP
J [redacted]	1-18-2000	20:55	I1	✓	✓	✓	21:00	
Pet [redacted]	1-18-2000	20:55	I2	✓	✓	✓	21:00	
Pas [redacted]	1-19-2000	1728	NA	Y	Y	✓	2003	*Special
Jac [redacted]	1-19-2000	1728	NA	Y	Y	✓	2003	OSP A
An [redacted]	1-19-2000	1728	NA	Y	Y	✓	2003	Special
S. K [redacted]	1-19-2000	1955	NA	Y	Y	✓	2003	TEST Pers
Matt [redacted]	1/19/2000	2235	I1	Y	Y	✓	2241	
Joe [redacted]	1-19-2000	2235	I2	Y	Y	✓	2241	

INJ access Stamp (Controlled Access Log#: 4476)

Lastname search:

Name	Key	Dosime
[redacted] Theo	I1	

Exit

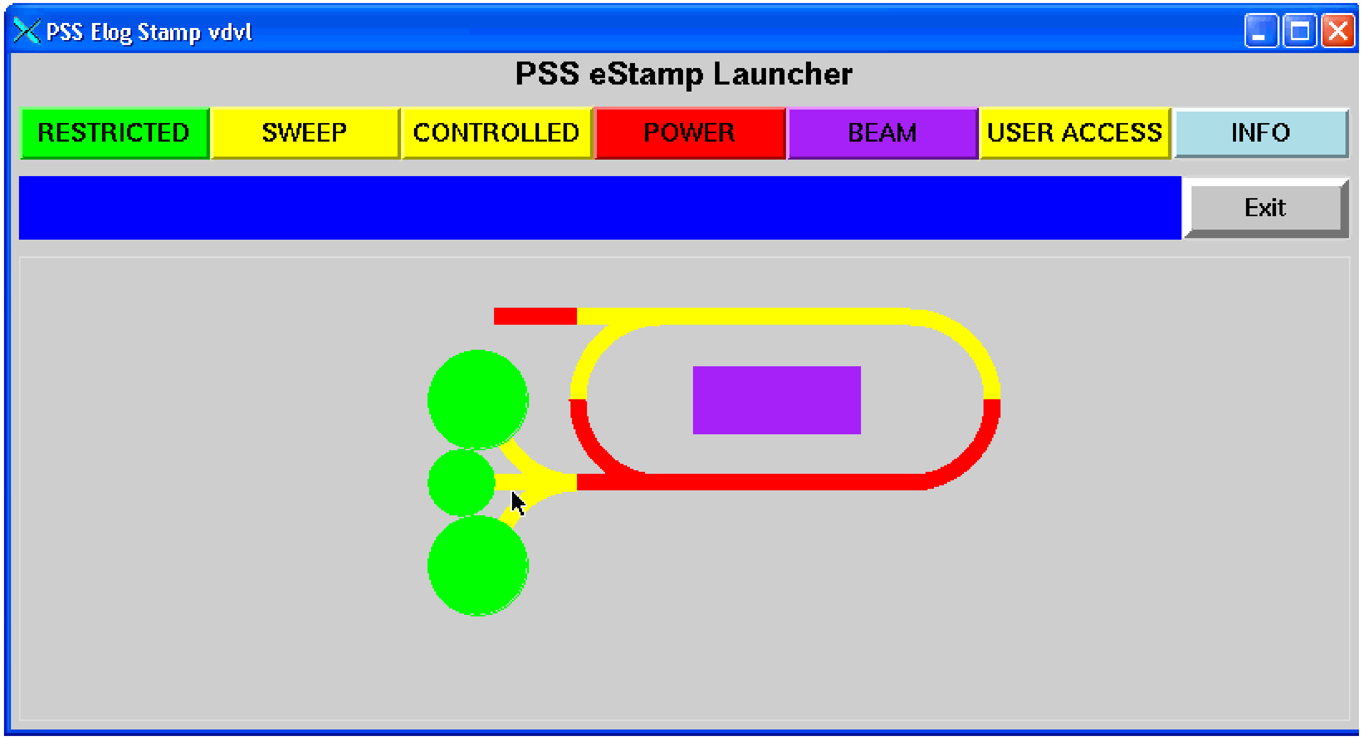
Manual

Complete

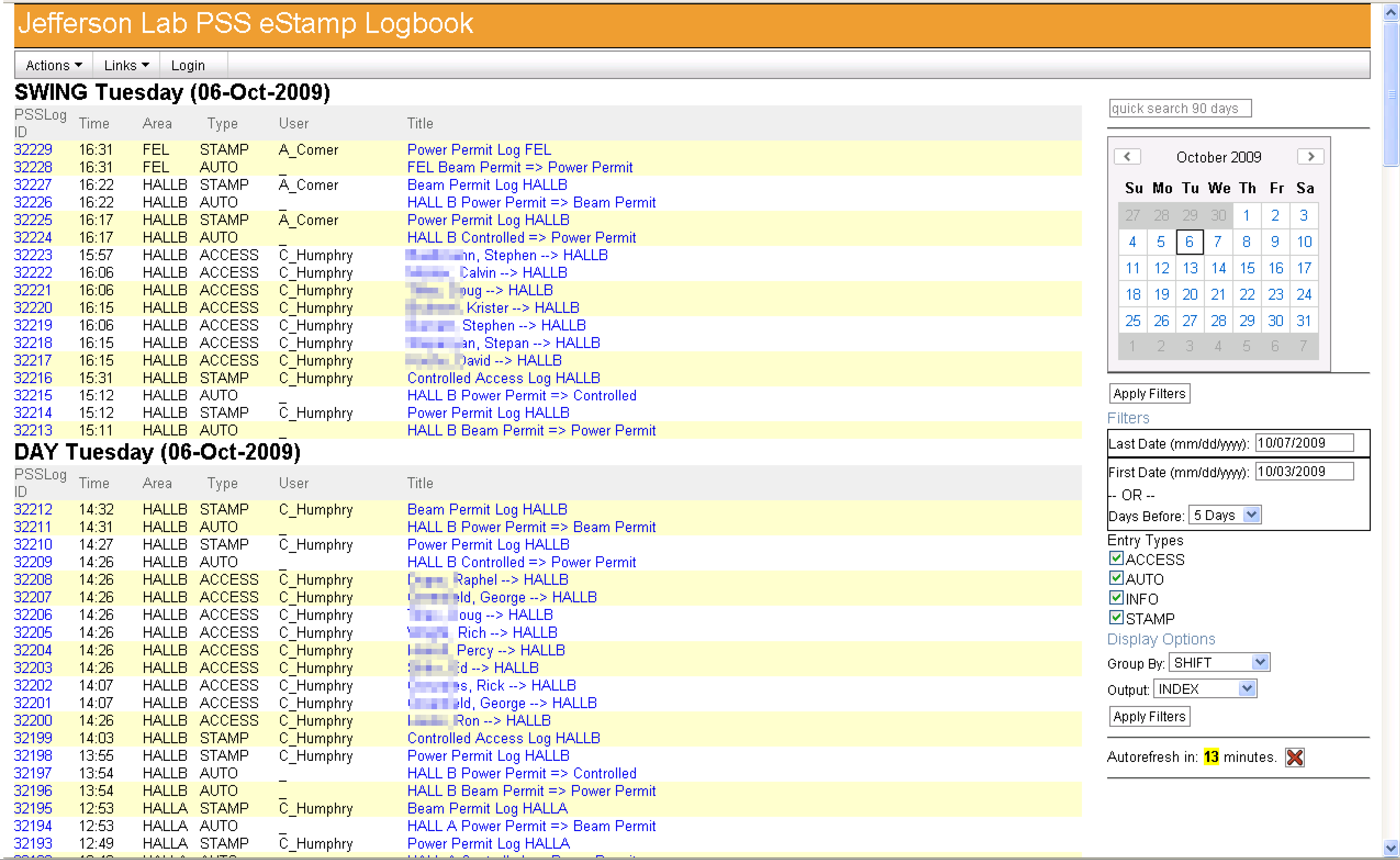
Authentication Procedure

- When SSO submits an entry, they must swipe their badge
- If more than eight hours (one complete shift) have passed since they last submitted an entry then their badge has timed out and they must enter their username and password
- They are now authenticated for the next eight hours (their badge is linked to their user account in the elog database), so they won’t have to type their username/password again for the duration of the shift
- Multiple SSOs can access the PSS system in a single shift, so multiple users can be authenticated at the same time

Step-by-Step Entry Example



Web Interface (View-only)



Jefferson Lab PSS eStamp Logbook

SWING Tuesday (06-Oct-2009)

PSSLog ID	Time	Area	Type	User	Title
32229	16:31	FEL	STAMP	A_Comer	Power Permit Log FEL
32228	16:31	FEL	AUTO	_	FEL Beam Permit => Power Permit
32227	16:22	HALLB	STAMP	A_Comer	Beam Permit Log HALLB
32226	16:22	HALLB	AUTO	_	HALL B Power Permit => Beam Permit
32225	16:17	HALLB	STAMP	A_Comer	Power Permit Log HALLB
32224	16:17	HALLB	AUTO	_	HALL B Controlled => Power Permit
32223	15:57	HALLB	ACCESS	C_Humphry	[redacted]n, Stephen --> HALLB
32222	16:06	HALLB	ACCESS	C_Humphry	[redacted]Calvin --> HALLB
32221	16:06	HALLB	ACCESS	C_Humphry	[redacted]ug --> HALLB
32220	16:15	HALLB	ACCESS	C_Humphry	[redacted] Krister --> HALLB
32219	16:06	HALLB	ACCESS	C_Humphry	[redacted] Stephen --> HALLB
32218	16:15	HALLB	ACCESS	C_Humphry	[redacted]an, Stepan --> HALLB
32217	16:15	HALLB	ACCESS	C_Humphry	[redacted]avid --> HALLB
32216	15:31	HALLB	STAMP	C_Humphry	Controlled Access Log HALLB
32215	15:12	HALLB	AUTO	_	HALL B Power Permit => Controlled
32214	15:12	HALLB	STAMP	C_Humphry	Power Permit Log HALLB
32213	15:11	HALLB	AUTO	_	HALL B Beam Permit => Power Permit

DAY Tuesday (06-Oct-2009)

PSSLog ID	Time	Area	Type	User	Title
32212	14:32	HALLB	STAMP	C_Humphry	Beam Permit Log HALLB
32211	14:31	HALLB	AUTO	_	HALL B Power Permit => Beam Permit
32210	14:27	HALLB	STAMP	C_Humphry	Power Permit Log HALLB
32209	14:26	HALLB	AUTO	_	HALL B Controlled => Power Permit
32208	14:26	HALLB	ACCESS	C_Humphry	[redacted] Raphel --> HALLB
32207	14:26	HALLB	ACCESS	C_Humphry	[redacted]ld, George --> HALLB
32206	14:26	HALLB	ACCESS	C_Humphry	[redacted]oug --> HALLB
32205	14:26	HALLB	ACCESS	C_Humphry	[redacted] Rich --> HALLB
32204	14:26	HALLB	ACCESS	C_Humphry	[redacted] Percy --> HALLB
32203	14:26	HALLB	ACCESS	C_Humphry	[redacted]d --> HALLB
32202	14:07	HALLB	ACCESS	C_Humphry	[redacted]s, Rick --> HALLB
32201	14:07	HALLB	ACCESS	C_Humphry	[redacted]ld, George --> HALLB
32200	14:26	HALLB	ACCESS	C_Humphry	[redacted] Ron --> HALLB
32199	14:03	HALLB	STAMP	C_Humphry	Controlled Access Log HALLB
32198	13:55	HALLB	STAMP	C_Humphry	Power Permit Log HALLB
32197	13:54	HALLB	AUTO	_	HALL B Power Permit => Controlled
32196	13:54	HALLB	AUTO	_	HALL B Beam Permit => Power Permit
32195	12:53	HALLA	STAMP	C_Humphry	Beam Permit Log HALLA
32194	12:53	HALLA	AUTO	_	HALL A Power Permit => Beam Permit
32193	12:49	HALLA	STAMP	C_Humphry	Power Permit Log HALLA

quick search 90 days

October 2009

Su	Mo	Tu	We	Th	Fr	Sa
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Apply Filters

Filters

Last Date (mm/dd/yyyy): 10/07/2009

First Date (mm/dd/yyyy): 10/03/2009

-- OR --

Days Before: 5 Days

Entry Types

☑ ACCESS
☑ AUTO
☑ INFO
☑ STAMP

Display Options

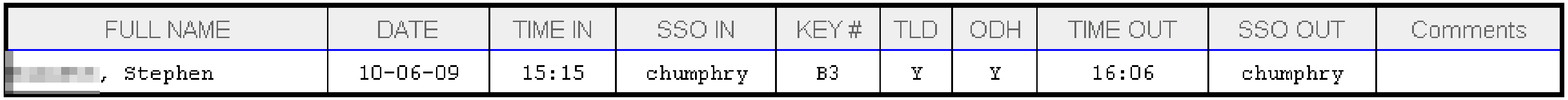
Group By: SHIFT

Output: INDEX

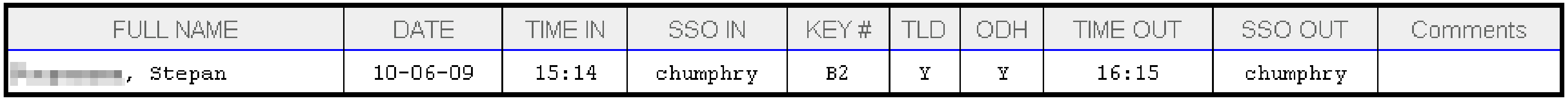
Apply Filters

Autorefresh in: 13 minutes. ☒

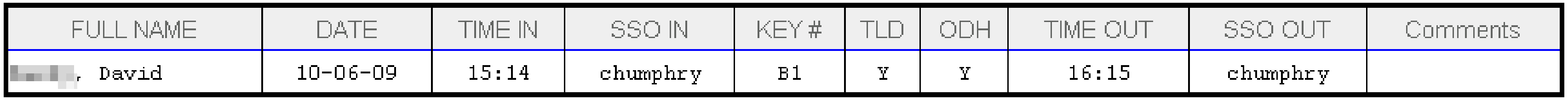
Web Interface (View-only, Cont.)



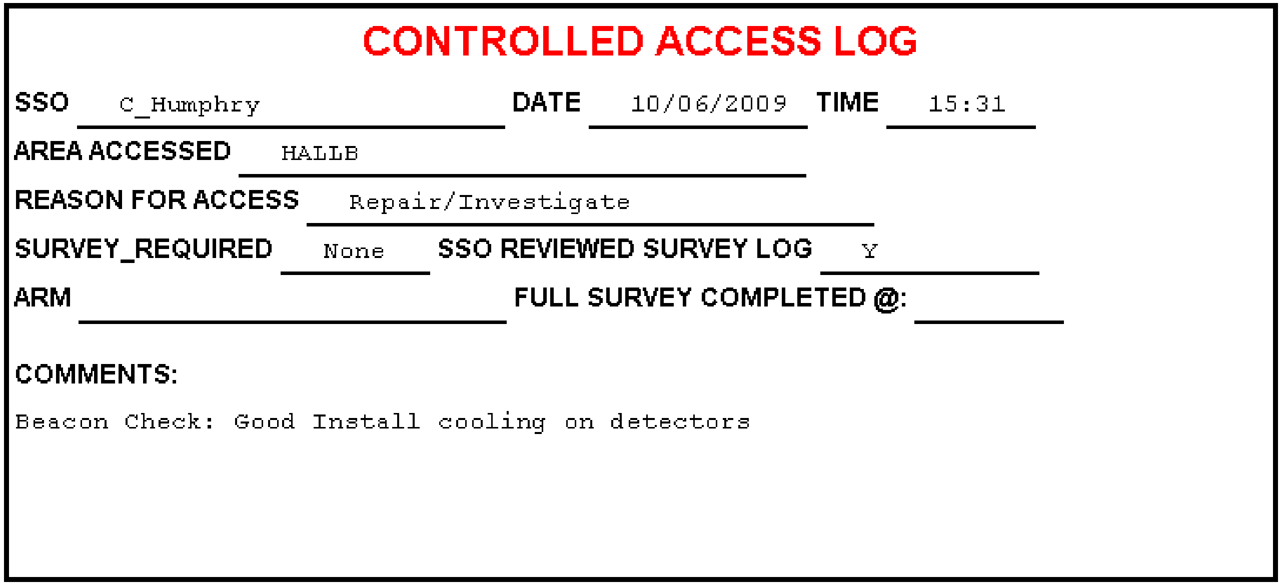
FULL NAME	DATE	TIME IN	SSO IN	KEY #	TLD	ODH	TIME OUT	SSO OUT	Comments
[redacted], Stephen	10-06-09	15:15	chumphry	B3	Y	Y	16:06	chumphry	



FULL NAME	DATE	TIME IN	SSO IN	KEY #	TLD	ODH	TIME OUT	SSO OUT	Comments
[redacted], Stepan	10-06-09	15:14	chumphry	B2	Y	Y	16:15	chumphry	



FULL NAME	DATE	TIME IN	SSO IN	KEY #	TLD	ODH	TIME OUT	SSO OUT	Comments
[redacted], David	10-06-09	15:14	chumphry	B1	Y	Y	16:15	chumphry	



CONTROLLED ACCESS LOG

SSO C_Humphry DATE 10/06/2009 TIME 15:31

AREA ACCESSED HALLB

REASON FOR ACCESS Repair/Investigate

SURVEY_REQUIRED None SSO REVIEWED SURVEY LOG Y

ARM ______ FULL SURVEY COMPLETED @: ______

COMMENTS:

Beacon Check: Good Install cooling on detectors

CONCLUSIONS

Conclusions

- Security requirements may be designed and implemented with very little concern for accessibility of the application.
- However if this is done when designing a new system that requires user-support to implement, a difficult security design can result in slow or no progress on the development, adoption, and update cycle.
- By implementing as much security to be invisible to the user, or by implementing security features to make the application easier to use (RF card reader, information recovery, etc.) it is possible to present security features to outside groups in a that encourages rapid development and deployment, rather than delaying the development and adoption cycle.

Questions?

- Future upgrades and additions?
  - Expanded user-tools
  - Expanded admin-tools
  - Training-mode
- Code?
  - Languages
  - Methodology
- Hotfixes – making minor changes to the code while it's in service
- How's It going so far?
- Testing and Versioning control