

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





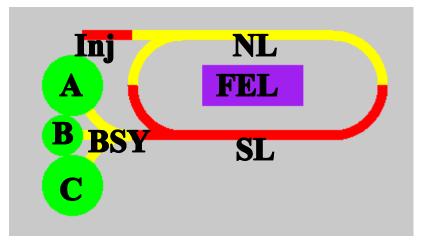
Definitions

- **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

Accesses

		(a) A second s second second s Second second secon second second sec
		134
02-29-09 21:39 CADE HALL C. TO POWER PERMIT_		FULL NAME
32-28-09 21:43 CADE HALL C TO BEAM FORM		TIM
		T-h.
		Phar
CONTROLLED ACCESS LOG	>/	Jortu
	— У	Rober
\$50 5prAggins DATE 03-01-09 TIME 19:18	/	MOT
AREA (S) ACCESSED HALL A		H CHARL
REASON FOR ACCESS RESET POWER SUPPLY		JOHA
880 REVIEWED SURVEY LOG	\sim	MATI
SURVEY REQUIRED (Y/N)		PETE
		PAUL
ABM D. ANTHONY FULL SURVEY COMPLETED @ N/A :		MAT
COMMENTS: - ESCORTED ACCESS		TOMA
		RICK
		CHARLI
		CHARL
03-11-09 19:47 Authony Hall A to POWER PERMIT		RICK
03-01-09 19:47 Authony Hall A to POWER PERMIT 03-01-09 19:62 Authony Hall A to BEAM PORMIT		MIKE
03-01-09 19:47 Aathony Hall A to POWER PERMIT 03-01-09 19:62 Aathony Hall A to BEAM PORMIT	68	MIKE
03-01-09 19:47 Aarthony Hall & to POWER PERMIT 03-01-09 19:62 Aarthony Hall & to BEAM PORMIT	68	MIKE MIKK CH.S
03-01-09 19:47 Authony Hall A to POWER PERMIT 03-01-09 19:62 Authony Hall A to BEAM Permit	68	Mike Mike CH.S Midka
03-61-09 19:62 Authony Hall A ro office Permit	68	Mike Mike CH.S Miokou Bogd
03-01-09 19:47 Authony Hall A to POWER PERMIT 03-01-09 19:62 Authony Hall A to BEAM PORMIT SWEEPLOG	68	Mike Mike CH.S Mioka Bogd Mida
03-61-09 19:62 Asthony Hall A ro BEAM Permit 	68	Mike Mikk CH _ S Mitoboo Bogdo Mitobo Mitobo
03-61-09 19:62 Authony Hall A ro BEAM Permit SWEEPLOG 060_Lebmann	68	Mike CH-S Mitolas Bogdy Mita Bogdy Mita
83-01-09 19:62 Aathony Hall A to BEAM Permit SWEEPLOG 600 Lehmanni DATE 02:02-09 TIME 00 7:20 OUNTEY HEQUIRED (YN) A. AREA SWEET HALL B.	68	Mire DA III' CH - S Mirobu Bogd Mirobu Bogd Mirobu Bogd
B3-61-09 19:52 Asthony Hall A to BEAM Permit SWEEP LOG 660 Lehmanin DATE 22-02-09 TIME 00 520 OURVEY HEQUIRED (Y/N) M. AREA SWEPT HALL B. MADCON CHECK LIST PERFORMED (Y/N) Y	68	Mike NA IKK CH . S Mitokau Bogol Mitoka Bogol Mitoka Bogol (Luck
B3-61-09 19:52 Asthony Hall A to BEAM Permit SWEEP LOG 660 Lehmanin DATE 22-02-09 TIME 00 520 OURVEY HEQUIRED (Y/N) M. AREA SWEPT HALL B. MADCON CHECK LIST PERFORMED (Y/N) Y	68	Hire CM.S Mister Bogd Mister Bogd Mister Bogd Mister Bogd Lizz
B3-61-09 19:52 Asthony Hall A ro BEAM Permit SWEEP LOG 600_Lebmann DATE 02-02-09 TIME 00 520 6UNVEY HEQUIRED (YN)_A_ AREA SWEPT HALL 5 RADCON CHECK LIST PERFORMED (YN)_Y ANNOUNCEMENTS AT 18 MIN 00 121 5 MIN 00 131	68	нике Mirike CH - S Mirike Bogd Mirke Bogd Mirke Bogd Mirke Bogd Mirke Bogd Jac
B3-61-09 19:52 Aathony Hall A ro BEAM Permit SWEEP LOG BCO_Lebranni DATE 03-02-09 TIME 00 7:20 BURVEY REQUIRED (Y/N)_XAREA SWEPT_HALL B NADCON CHECK LIST PERFORMED (Y/N)_Y ANNOUNCEMENTS AT 18 MIN _00 .121_ 5 MIN _00 .121_ SWEEP TEAM_ALKON_Reference	68	Mike Mike CH - S Mitobel Bogd Mitobe Bogd Mitobe Bogd Lick Pasc Hap
B3-61-29 19:62 Asthony Hall A to BEAM Permit SWEEP LOG BCO_L SWIANN DATE 02:02:09 TIME 00 T20 GUAVEY HEQUIRED (Y/N)_N_A AREA SWEPT HALL B NANCON CHECK LIST PERFORMED (Y/N)_Y ANNOUNCEMENTS AT 15 MIN _02 12. 5 MIN 20 131 SWEEP TEAM_ALKON, Reformed on SWEEP COMPLETED AT _02:59	68	Mike Mike CH . S Michae Bogd- Michae Bogd Michae Bogd Nucle Pase Jace Hae Jace Jace Jace
B3-61-09 19:52 Asthony Hall A to BEAM Permit SWEEP LOG BSO L. CAMANAN DATE 02-02-09 TIME 02 730 BURVEY HEQUIRED (Y/N) X. AREA SWEPT Hall B. NANCON CHECK LIST PERFORMED (Y/N) Y. ANNOUNCEMENTS AT 18 MIN	68	Mire CN.S Mirobu Bogd Mirobu Mirobu Bogd Mirobu Bogd Mirobu Bogd Mirobu Bogd Mirobu Bogd Mirobu Bogd Mirobu Bogd Mirobu Mir
B3-61-29 19:62 Asthony Hall A to BEAM Permit SWEEP LOG BCO_L SWIANN DATE 02:02:09 TIME 00 T20 GUAVEY HEQUIRED (Y/N)_N_A AREA SWEPT HALL B NANCON CHECK LIST PERFORMED (Y/N)_Y ANNOUNCEMENTS AT 15 MIN _02 12. 5 MIN _02 131 SWEEP TEAM_ALKAN, Reformed on SWEEP COMPLETED AT _02:59	68	Mire CH.S Michen Bogd Michen Bogd Michen Bogd Michen Bogd Michen Bogd Michen Bogd Michen Bogd Michen Bogd Michen Bogd Jacq Jacq Jacq Jacq Jacq
B3-61-09 19:52 Asthony Hall A to BEAM Permit SWEEP LOG BSO L. CAMANAN DATE 02-02-09 TIME 02 730 BURVEY HEQUIRED (Y/N) X. AREA SWEPT Hall B. NANCON CHECK LIST PERFORMED (Y/N) Y. ANNOUNCEMENTS AT 18 MIN	68	Mire M. Irs CH.S Mirober Bogd Micher Bogd Guck Pase Jacq Jacq Jacq Jacq Jacq Jacq Jacq
B3-61-09 19:52 Asthony Hall A to BEAM Permit SWEEP LOG BOO_L.chmanniDATE 02:02-09, TIME 00:520 BURNEY HEQUIRED (Y/N)_NAREA SWEET_HALL IS MADCON CHECK LIST PERFORMED (Y/N)_Y ANNOUNCEMENTS AT 15 MIN 20:12. 5 MIN 20:121 SWEEP TEAM (Jian Jacoba Jaco	68	Hire Miris Griss Mirisher Bogd Mirsher Bogd Mirsher Bogd Mirsher Bogd Jacq Jacq Jacq Jacq Jacq Jacq Jacq Jacq
B3-61-09 19:62 Anthony Hall A to BEAM Permit SWEEPLOG GOO L. CHMANN DATE 03-02-09 TIME 02 7320 GUAVEY HEQUIRED (Y/N) X. AREA SWEPT, Hall B. NADCON CHECK LIST PERFORMED (Y/N) Y. ANNOUNCEMENTS AT 18 MIN 02 121 B MIN 02 131 SWEEP TEAM Alken, Rebaden TLD/ODH Y SWEEP TEAM Alken, Rebaden TLD/ODH Y SWEEP COMMENTS: Hall B, being swicht after 3 days 10 Restricted Access	68	Hike Mike CH.S Mitober Bogd Mitole Bogd Mitole Bogd Mitole Bog Mitole Bog Lace Jace Jace Jace Jace Jace Jace Jace J
B3-61-09 19:52 Asthony Hall A to BEAM Permit SWEEP LOG BOO_L.chmanniDATE 02:02-09, TIME 00:520 BURNEY HEQUIRED (Y/N)_NAREA SWEET_HALL IS MADCON CHECK LIST PERFORMED (Y/N)_Y ANNOUNCEMENTS AT 15 MIN 20:12. 5 MIN 20:121 SWEEP TEAM (Jian Jacoba Jaco	68	HIRE MIRE CH.S. Misber Bogd- Misber Bogd- Misber Bogd Misber Bogd Pase Jacq Jacq Jacq Jacq Jacq Jacq Jacq Jacq

1.1				an Real and Solar					-
	134 FULL NAME	DATE	TIME	# Kea	TLD (Y/N)	CURE ODH (Y/N)	CHECK VERSF	TIME OUT	COMME
	TIM MAL	1-07-03	1447	FI	Y	Y	V	1455	
	Tohy	1-7-00	20.15	C(.	28	Y	V	20:30	
	RAX	1-7-00	201.15	12	V	Y,	V	20:30	
	John Domand	1-7	20,30	AZ	V	V	V	21:05	
	Rober	1-7	20:30	AI	V	V	V	21:05	
DUAL	MATT	1-10-00	16:10	I2	v			16:22	
	EMALL	1-10-00	16:10	11	V		1030 <u>2</u> ×8	16:22	1990 Constant
P	JOHA .	0	16:11	I3	·····		and the second	16:22	
	MAT	11 1	17:47	T 1	and the second	2.5717	1-6-2	17:59	
	PETE	e le j	19:05	I1	- 1	-	- T.	19:20	1. San (2)
	FAUL	1-11-00	17:20	I10	and the second	and the second	- Easter	17:58	and the second
	MAT	e traine		<i>I9</i>		-	-	17:58	and the second
	Jona	Same Sec.	S 20. 1	18	and the second			17:58	
	RICK	R. Sec. 1	22:21	N	-		-	22:36	A. S.
110	CHARLI	10.00	e e	NZ	-	c	-	22:36	
	CHARL	1-13-00	22:07	2	1000		S. S. Conne	22:14	
	RICK	11	1.11	NL	1000	v	V	22:14	
	HIKE	11		II	-	-	-	22:25	10 10 A
	Mike	1-15-00	19:09	E1 II	1	/	-	19:12	141.202
and a	CH.S	1-16-00	13:30		4	4	4	13:35	
	Michael	17-JAN-200	14:41	ī2	1	1	1	14:53	
<u>e</u> k	Bogd	17541-2003	14:41	11	V	1	V	14:53	
US.	Mide	17JAN-2000		12	V	1 1300	7	15,42	
	togd	7-511-200	12:33	T1	V	V.	V.	15:42	2010 - 1993
	Miche	17-111-202		I2	1	V	1	16:56	
	Bogd	17-711-200	16:19	11	~	1	1	16:56	1
-	fuck	1-19-2000	17:00	NA #	V	NA	1	20:00	Special
L.	Pasc	1-19.200	17:00	NA +	V	NA	V	20.00	stor s
ip.	Jaco	1-18-2001	17,10	NAA	V	NA		00:05	
-	Pao	1-19-2000	20:50	UA	V	NA	V	22:45	* ppec
Sel.	Jacque	1-13-200	20:50	NA	1	NK	1	22:45	SSOP
4	Jo	1-19-200		I1		V,	V	21:00	
Air	Pet	1-18-2000	20:55	I2		1		21:00	
an.	Passer	1-17-2002	1728	NA	Y	y	V	2003	Special
	Teq	1-19-2000	1724	NA	1 1	Y Y	BAYODA	2003	YOSP A
	Ani	1-19-2000	1728	NA	y y	Y	V	2003	(Special
	SH	1-19-2000	1955	NA	Y.	17.	V	2003	TEST Per
-	Matt Matt	1/19/200	2235	II	4	14	V	2241	12 Jan 19
D.J	JAE	1-19-2000	2235	IJ	ΙY	Y	IV.	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





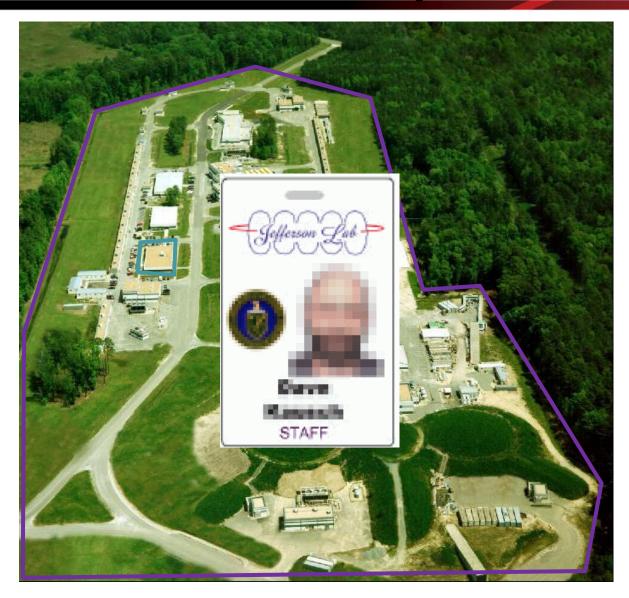
User Support

- 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:

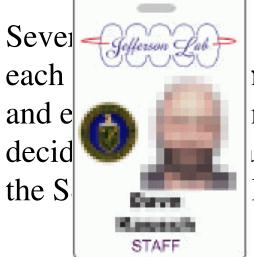
- Kiosk-mode on PSS workstation means using the SSO workstation is simpler.
- Autologs track state-changes in the machine with no input necessary from SSO.





Computer Security (Cont.)

SSO must be identified for each entry submitted to the database



were suggested for authenticating for 1g username/password, PIN-numbers nt scanning. In the end what was In RF Ideas pcProx RF card reader with D badge.

Benefits to user:

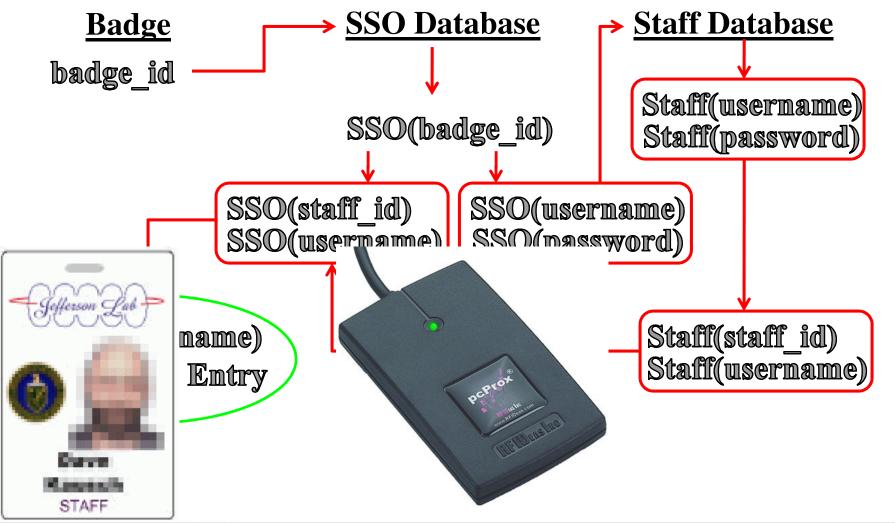
- SSO's can make dozens of entries in an hour. Having to type username/password for each would be onerous
- Using existing technology (Jlab badges) means using an existing system (users already "swipe their badge" to get on site, access buildings, etc.)
- No additional PII (finger-prints) needed to be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





Login & Badge Security

SSO must be identified for each entry submitted to database







Program Security

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



Benefits to user:

- Data that an SSO is entering cannot be lost due to simple usererror, 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

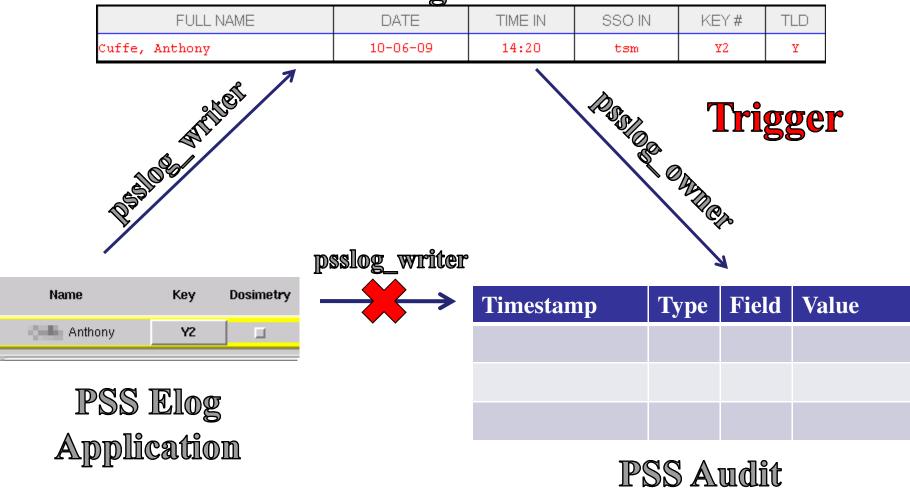
The underlying PSS database was built with two layers.

- 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





- 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





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**.

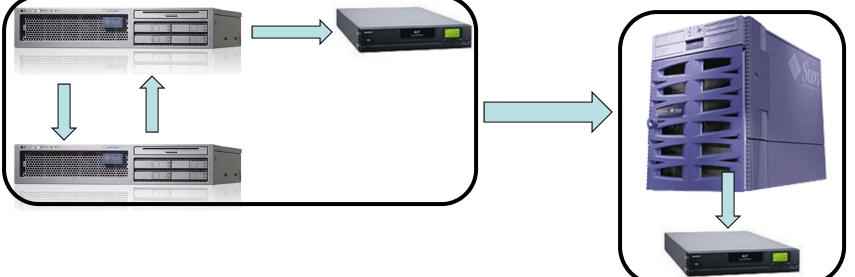
Benefits to user:

- 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 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



02-23-09 21:39 CADE HALL C. TO POWER PERMIT. 02-28-09 21:43 CADE HALL C. TO BEAM PERMIT.

	CONTROLLED ACCESS LOG	
	SSO SPRAGUES PATE 22 AL ACTUS 10.12	
<u>11.</u>	SSO Spragens DATE 03-01-09 TIME 19:18 AREA (S) ACCESSED HALL A	
	REASON FOR ACCESS RESET POWER SUPPLY	
<u></u>	SSO REVIEWED SURVEY LOG	
	SURVEY AEQUIRED (Y/N)	
	ABM D. ANTHONY FULL SURVEY COMPLETED @ N/A;	C
38	CONTRACTS: ESCORTED ACCESS	
	ALL ALL ENCONTED AUDED	
A F		
	· · · · · · · · · · · · · · · · · · ·	
	21-09 19:47 Aarthony Hall A to POWER PERMIT	3
03-	al-09 19:52 Anthony Hall A to BEAM Permit	
-08		
NF I		
NF		
AF X	SWEEP LOG	
993 993		
993 993	860 Lebmann DATE 03-02-09 TIME 00 220	
993 993	SEO_LehmanniDATE 22.02-09 TIME @ 120_ SURVEY REQUIRED (YN)_LAREA SWEPT HALL B	
993 993	060 Lehmann DATE 23-02-09 TIME @ 120 OURVEY REQUIRED (Y/N) AL AREA SWEPT HALL S	
993 993	SEC. Lehmann DATE 22-02-09 TIME @ 120 SURVEY HEQUIRED (YN) AREA SWEPT_HOLLES RADCON CHECK LIST PERFORMED (YN) ANNOUNCEMENTS AT 15 MIN 212 5 MIN cc 13/	
993 993	SEC Lemann DATE 23-02-09 TIME 20 1220 SURVEY HEQUIRED (Y/N), <u>M</u> AREA SWEPT_HALLE RADCON CHECK LIST PERFORMED (Y/N), <u>Y</u> ANNOUNCEMENTS AT 15 MIN _20 121_5 MIN _20 131 SWEEP TEAM. <u>Alkena, Reference</u> TLD/ODHY	
993 993	SEC. LEMANN DATE 22-02-09 TIME 00 :200 OURVEY REQUIRED (Y/N) <u>M</u> AREA SWEPT <u>Holl 15</u> ANNOUNCEMENTS AT 15 MIN <u>co 121</u> 5 MIN <u>co 131</u> SWEEP TEAM <u>Alken, Refactore</u> TLD/ODH <u>y</u> SWEEP COMPLETED AT <u>co :59</u>	
993 993	SEC_LEMMANNDATE 22-02-09 TIME 00 720 OURVEY REQUIRED (Y/N) AREA SWEPT HALL 3 MADCON CHECK LIST PERFORMED (Y/N) _Y ANNOUNCEMENTS AT 15 MIN _00 121 5 MIN _00 : 31 SWEEP TEAM <u>Alsen</u> , <u>Referderen</u> TLD/ODH Y SWEEP COMPLETED AT _00:59 COMMENTS: HALL 6 being sweet after 2 days	
993 993	SEC. LEMANN DATE 22-02-09 TIME 00 :200 OURVEY REQUIRED (Y/N) <u>M</u> AREA SWEPT <u>Holl 15</u> ANNOUNCEMENTS AT 15 MIN <u>co 121</u> 5 MIN <u>co 131</u> SWEEP TEAM <u>Alken, Refactore</u> TLD/ODH <u>y</u> SWEEP COMPLETED AT <u>co :59</u>	
993 993	SEC_LEMMANNDATE 22-02-09 TIME 00 720 OURVEY REQUIRED (Y/N) AREA SWEPT HALL 3 MADCON CHECK LIST PERFORMED (Y/N) _Y ANNOUNCEMENTS AT 15 MIN _00 121 5 MIN _00 : 31 SWEEP TEAM <u>Alsen</u> , <u>Referderen</u> TLD/ODH Y SWEEP COMPLETED AT _00:59 COMMENTS: HALL 6 being sweet after 2 days	
	SEC. LEMANN DATE 03-02-09 TIME 00 120 OURVEY HEQUIRED (Y/M), <u>M</u> AREA SWEPT, <u>HOLL B</u> RADCON CHECK LIST PERFORMED (Y/N), <u>Y</u> ANNOUNCEMENTS AT 15 MIN	
	SEC_LEMMANNDATE 22-02-09 TIME 00 720 OURVEY ABOURDED (Y/N) AREA SWEPT HALL 3 MADCON CHECK LIST PERFORMED (Y/N) _Y ANNOUNCEMENTS AT 15 MIN _00 121 5 MIN _00 : 31 SWEEP TEAM <u>Alsen</u> , <u>Referderen</u> TLD/ODH Y SWEEP COMPLETED AT _00:59 COMMENTS: HALL 6 being sweet after 2 days	

SL-> CONTROLL		CONTROL LEDY	-
	and the second	-> CONTROLLED)	
DATE: 04/08 T	IME: 11:34		
SURVEY REQUIN	ED: 👽 Full 👽 Partial 🐟 NA	A SURVEY COMPLETED @:	
REASON FOR A	CCESS		
SSOREWED			
COMMENTS:			
Submit	Scan Grab	Ex	100





Paper Logbook Emulation (Cont.)

Access Entry

134	ann a'		134 FULL MAME TIM	DATE 1-07-00 1-7-00	TIME IN 1447 :2015	KEY H		CURE ODH (Y/N)	CHECK VERAF LIST	TIME OUT 1453	COMME	TIME	
FULL NAME		DATI	Tohi Politi	1-7-00	20:15	c2	L	Y	V	20:30	57	OUT	COMME
TIM		1-07	Joyn Rober	1-7 1-7	20:30	A2 A1 IZ	V	V	V	21:05 21:05 16:22	1	1455	
		1-7-	MATT CHARL JOHA	1-10-00	16:10	11 11 13	<i>v</i> <i>v</i>		8830 <u>0</u> A A	16:22	200	20:30	
Rader		1-7-	MWT PETE	rt i i te i	17:47 19:05	I1 I1	-	1 1		17:59 19:20	a sta	20:30	
John RASAR Joyu	in her	1-7	PRUL MAT JOHA	1-11-00	17:20	110 19 28		in an		17:58	_/	21:05	
-off-t		1	RICK CHARLI	et et	22:21	N(N2	-	ب د	- -	22:36	211112		CARL CARAGE
			CHARL	1-13-00	22:07	NI	-	י ני	L V	22:14			
			Mike Mike	1. 1-15-00		II El		-		22:25			
J access Stamp (Contro	lled Access L	og#: 4476)	<u>CH.S</u> Miohou	1-16-00 17-5111-200	M:41	11 12 11	V	L V	1- 1- 1- 1-	13:35			ł
			Bogd Midu	175711-2003 175711-2003	15:33	11 12 11			J	15:42			
			Bogoli Miche Rogol	7-541-2000 17-541-2020 17-541-2020	16:19	11 12 11	V			16:56			Exit
stname search:			Pasc	1-19-2000	17:00	NA A NA A	V	NA	V	20:00	special ssor s		Manua
Name	Key	Dosime	Jac Pao Jacq	1-19-2000	17:10 20:50 28:50	NA A NA NA	~ ~ /	NA NA NK	<i>y</i>	adi TJ	* ppers SSOP		
Theo			Pet	1-18-2000	20:55	T1 12		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		21:00			Complete
Theo			Pas Jec An	1-19-2000	1724	NA NA NA	¥	Ý	V	2003	Special 205,P A Special		Complete
		1	S.F. Matt	1-19-2000	1955	NA	12	14	V		TEST Res		





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

SWEEP	PSS e	Stamp Laun POWER	cher BEAM	USER ACCESS	
SWEEP	CONTROLLED	POWER	BEAM	LISER ACCESS	
				USER AUCESS	INFO
					Exit
		8			





Web Interface (View-only)

Jefferson Lab PSS eStamp Logbook

Actions	s 🔻 🛛 Link	s▼ Log	jin			
SWIN	lG Tue	esday	(06-Oct	-2009)		
PSSLog		Area	Түре	User	Title	quick search 90 days
ID 32229	16:31	FEL	STAMP	A_Comer	Power Permit Log FEL	Coctober 2009
32228	16:31	FEL	AUTO	_	FEL Beam Permit => Power Permit	Cotober 2009
32227	16:22	HALLB	STAMP	Ā_Comer	Beam Permit Log HALLB	Su Mo Tu We Th Fr Sa
32226	16:22	HALLB		_	HALL B Power Permit => Beam Permit	
32225	16:17		STAMP	A_Comer	Power Permit Log HALLB	27 28 29 30 1 2 3
32224	16:17	HALLB		_	HALL B Controlled => Power Permit	4 5 6 7 8 9 10
32223	15:57		ACCESS	C_Humphry	n, Stephen> HALLB	11 12 13 14 15 16 17
32222	16:06		ACCESS	C_Humphry	Calvin> HALLB	
32221	16:06		ACCESS	C_Humphry	pug> HALLB	18 19 20 21 22 23 24
32220	16:15		ACCESS	C_Humphry	Krister> HALLB	25 26 27 28 29 30 31
32219 32218	16:06 16:15		ACCESS ACCESS	C_Humphry	Stephen> HALLB	
32218	16:15		ACCESS	C_Humphry	an, Stepan> HALLB David> HALLB	1 2 3 4 5 6 7
32217	15:31		STAMP	C_Humphry C_Humphry	Controlled Access Log HALLB	
32215	15:12	HALLB		C_numprity	HALL B Power Permit => Controlled	Apply Filters
32213	15:12		STAMP	C_Humphry	Power Permit Log HALLB	
32213	15:12	HALLB		o_nampiny	HALL B Beam Permit => Power Permit	Filters
			-Oct-20	ก้อง		Last Date (mm/dd/yyyy): 10/07/2009
PSSLog	Tuesu	ау (оо	-001-20	v v)		First Date (mm/dd/yyyy): 10/03/2009
PSSLUg ID	Time	Area	Туре	User	Title	OR
32212	14:32	HALLB	STAMP	C_Humphry	Beam Permit Log HALLB	Days Before: 5 Days 💌
32211	14:31	HALLB	AUTO		HALL B Power Permit => Beam Permit	
32210	14:27	HALLB	STAMP	C_Humphry	Power Permit Log HALLB	Entry Types
32209	14:26	HALLB		_	HALL B Controlled => Power Permit	ACCESS
32208	14:26		ACCESS	C_Humphry	Raphel> HALLB	☑ AUTO
32207	14:26		ACCESS	C_Humphry	lenge eld, George> HALLB	✓INFO
32206	14:26		ACCESS	C_Humphry	oug> HALLB	STAMP
32205	14:26		ACCESS	C_Humphry	Rich> HALLB	Display Options
32204	14:26		ACCESS	C_Humphry	Percy> HALLB	Group By: SHIFT
32203	14:26		ACCESS	C_Humphry	id> HALLB	
32202	14:07		ACCESS	C_Humphry	Contraction State> HALLB	Output: INDEX 💌
32201 32200	14:07 14:26		ACCESS ACCESS	C_Humphry	led, George> HALLB Ron> HALLB	Apply Filters
32200	14:26 14:03		STAMP	C_Humphry C Humphry	Controlled Access Log HALLB	
32199	13:55		STAMP	C Humphry	Power Permit Log HALLB	Autorefresh in: 13 minutes. 🔀
32190	13:55	HALLB		C_unuhury	HALL B Power Permit => Controlled	Autorenesn m. 13 minutes. 👗
32197	13:54	HALLB		-	HALL B Power Permit => Power Permit	
32195	12:53		STAMP	C_Humphry	Beam Permit Log HALLA	
32194	12:53	HALLA		o_nampiny	HALL A Power Permit => Beam Permit	
32193	12:49		STAMP	C Humphry	Power Permit Log HALLA	
	10.10	110110				





Web Interface (View-only, Cont.)

FULL NAME	DATE	TIME IN	SSO IN	KEY #	TLD	ODH	TIME OUT	SSO OUT	Comments
, Stephen	10-06-09	15:15	chumphry	в3	Y	Y	16:06	chumphry	

FULL NAME	DATE	TIME IN	SSO IN	KEY #	TLD	ODH	TIME OUT	SSO OUT	Comments
, Stepan	10-06-09	15:14	chumphry	в2	Y	Y	16:15	chumphry	

FULL NAME	DATE	TIME IN	SSO IN	KEY #	TLD	ODH	TIME OUT	SSO OUT	Comments
, David	10-06-09	15:14	chumphry	В1	Y	Y	16:15	chumphry	

	CONTROLLE	ED ACCESS	S LOG	;
SSO C_Humphry	DATE	10/06/2009		15:31
AREA ACCESSED HAL	JLB			
REASON FOR ACCESS	Repair/Investiga	te		
SURVEY_REQUIRED	None SSO REVIEW	ED SURVEY LOG	Y	
ARM	FULL S	URVEY COMPLE	TED @:	
COMMENTS: Beacon Check: Good I	install cooling on	detectors		





CONCLUSIONS





Conclusions

- Security requirements <u>may</u> 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



