Chapter 9

Always A Pioneer, Always Ahead

Physical and Logical Access Control

Dr Zaheera Zainal Abidin

zaheera@utem.edu.my

MyUTeM

By the end of the lesson, the student will be able to:

- Understand the application of physical and logical access control system
- Understand the challenges in physical and logical access control system

OVERVIEW

- Introduction
- Physical and Logical Access Control Methods
- Physical and Logical Access Control Types
- Physical and Logical Access Control Systems
- Doors : Keri systems
- Physical Access Control Log Format
- From logs to ESM
- Challenges: Piggybacking, Ingress, Egress, Corporate Structure, Correlation Issues
- Detection through convergence: Physical + VPN access

INTRODUCTION

INTRODUCTION

- The combination of physical and logical authentication events are the essence of convergence in physical access control.
- Two authentication method considered as strong authentication due to combination of two element (userid+password and physical object).
- The integration of physical and logical system produce logs, challenges and one of the solution is to detect the convergence through physical device and VPN access.

THE PHYSICAL AND LOGICAL ACCESS CONTROL METHODS

THE METHODS

Technical Control

- Controls using systems - for instance permission controls
- Operating system controls
- Hardware usage control

Administrative Control

- Controls that determine people behavior – the insiders, absentee and missing in action
- Security policies
- Standard operating procedures

THE PHYSICAL AND LOGICAL ACCESS CONTROL TYPES

THE TYPES

1) **Transaction Authorization**
   - To ensure employees are carrying out only authorized transactions.
   - Example: one-time passwords, Radius Server, AAA.
2) **Segregation of Duties**
   - To separate the custody of asset, separation between program coding, processing and maintenance.
   - Example: one task is shared by one or more employee to control against fraud and error.
3) **Supervision**
   - To compensation for lack of segregation in computer system.
   - Example: The process of monitoring the activity done by other person to sustain safety, quality and progressing as scheduled.

THE TYPES

4) Accounting Records

- To produce audit trails.
- Example: Ledger accounts or ISO documents need to be labeled, cataloged or tagged with RFID or QR code for document tracking.

5) Access Controls

- To assist in protecting the assets by restricting physical access to them.
- Example: Direct (assets), Indirect (ISO document), Fraud, Disaster Recovery.

6) Independent Verification

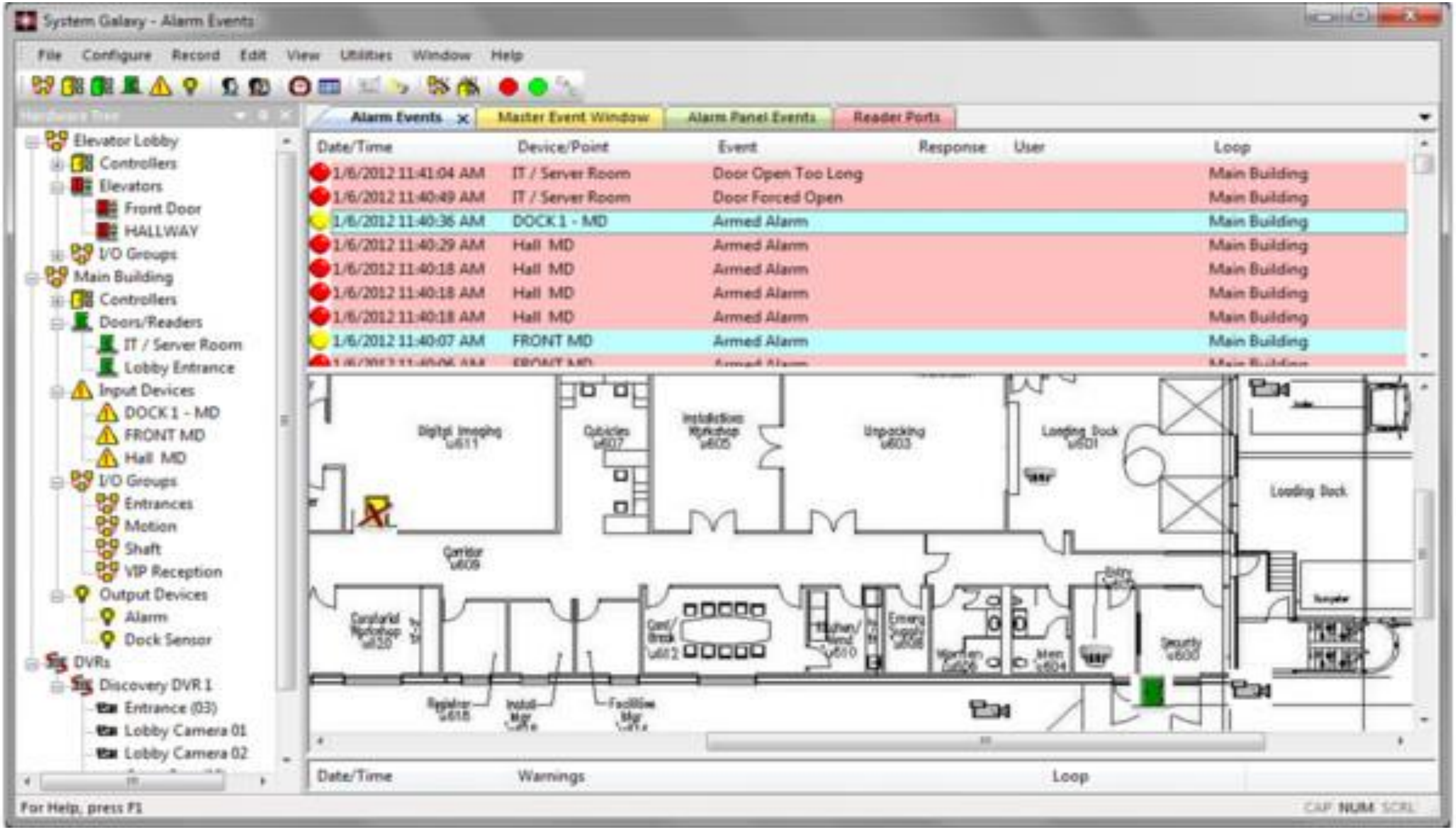
- To review a batch of subsidiary accounts with control accounts.
- Example: Management can assess:
- The individual performance
- The integrity of data in records

THE PHYSICAL ACCESS CONTROL SYSTEM (PACS)

PACS

- Physical access control systems (PACS) are systems that are installed in areas that need to be supervised and user access control is necessary. Existing commercial applications require a dedicated communication infrastructure and special hardware requirements comprising a compact system not flexible to user customization.
- PACS come in all shapes and sizes and from many different vendors, but they all accomplish similar task and mission
- Some of common systems:
  - Swipe card systems
  - Proximity reader (key fob)
  - Centralized management platform to put updated configurations to handle actual authentication

EXAMPLE OF PACS



Date/Time	Device/Point	Event	Response	User	Loop
1/6/2012 11:41:04 AM	IT / Server Room	Door Open Too Long			Main Building
1/6/2012 11:40:49 AM	IT / Server Room	Door Forced Open			Main Building
1/6/2012 11:40:36 AM	DOCK 1 - MD	Armed Alarm			Main Building
1/6/2012 11:40:29 AM	Hall MD	Armed Alarm			Main Building
1/6/2012 11:40:18 AM	Hall MD	Armed Alarm			Main Building
1/6/2012 11:40:18 AM	Hall MD	Armed Alarm			Main Building
1/6/2012 11:40:18 AM	Hall MD	Armed Alarm			Main Building
1/6/2012 11:40:07 AM	FRONT MD	Armed Alarm			Main Building
1/6/2012 11:40:06 AM	FRONT MD	Armed Alarm			Main Building

DOOR : KERI SYSTEMS

https://www.keri-kb.com/

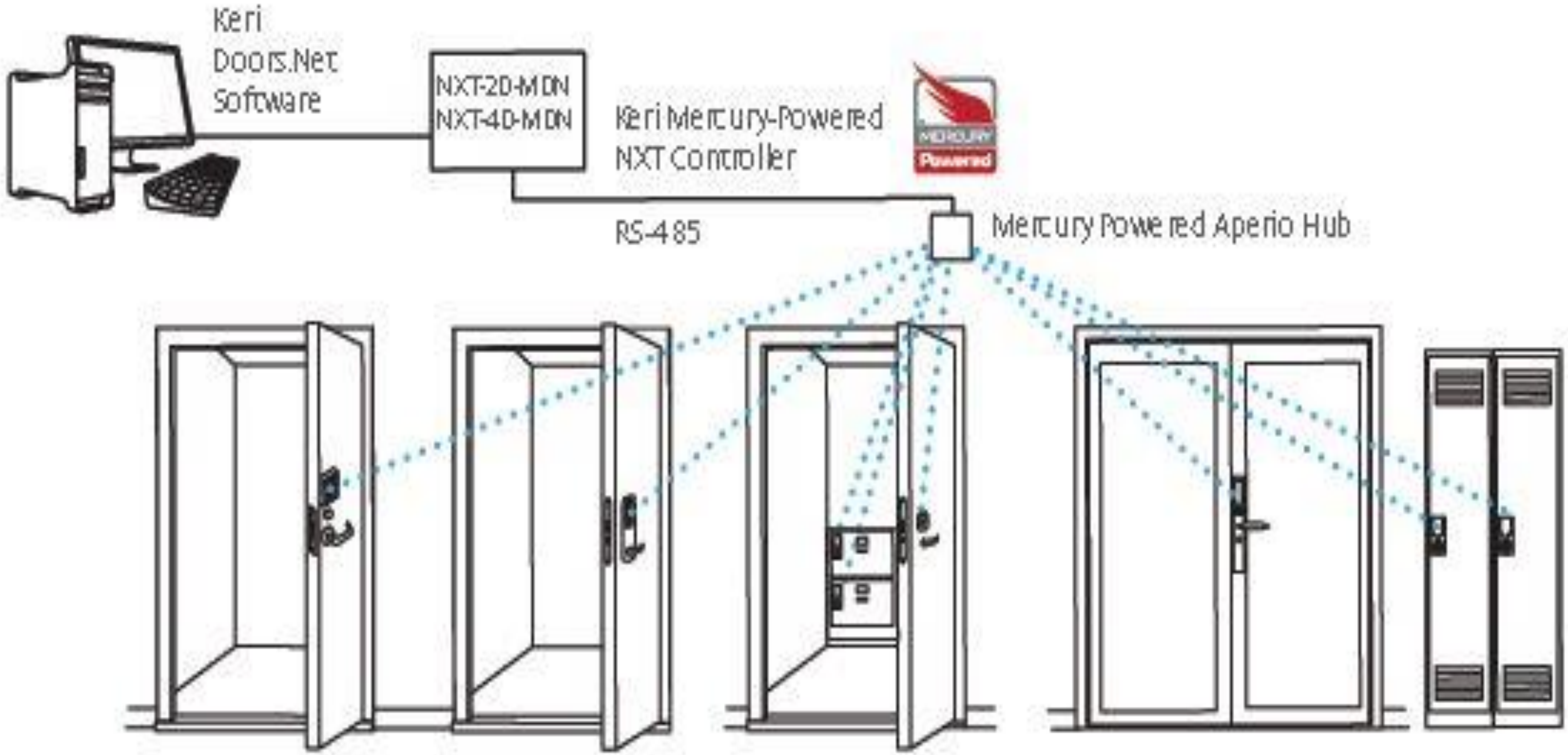
Door: Keri Systems

- It is a system that is usable to configure and manage Keri’s physical access controllers
- Runs on Windows via TCP/IP
- All of the functionality expected from PACS
- Provide multiple site administrators with different levels of control, and it accommodates holiday schedules and times when actual doors should open or locks
- Includes built-in monitoring and logging capabilities
- Includes an option either collect or not collect the logs from the readers

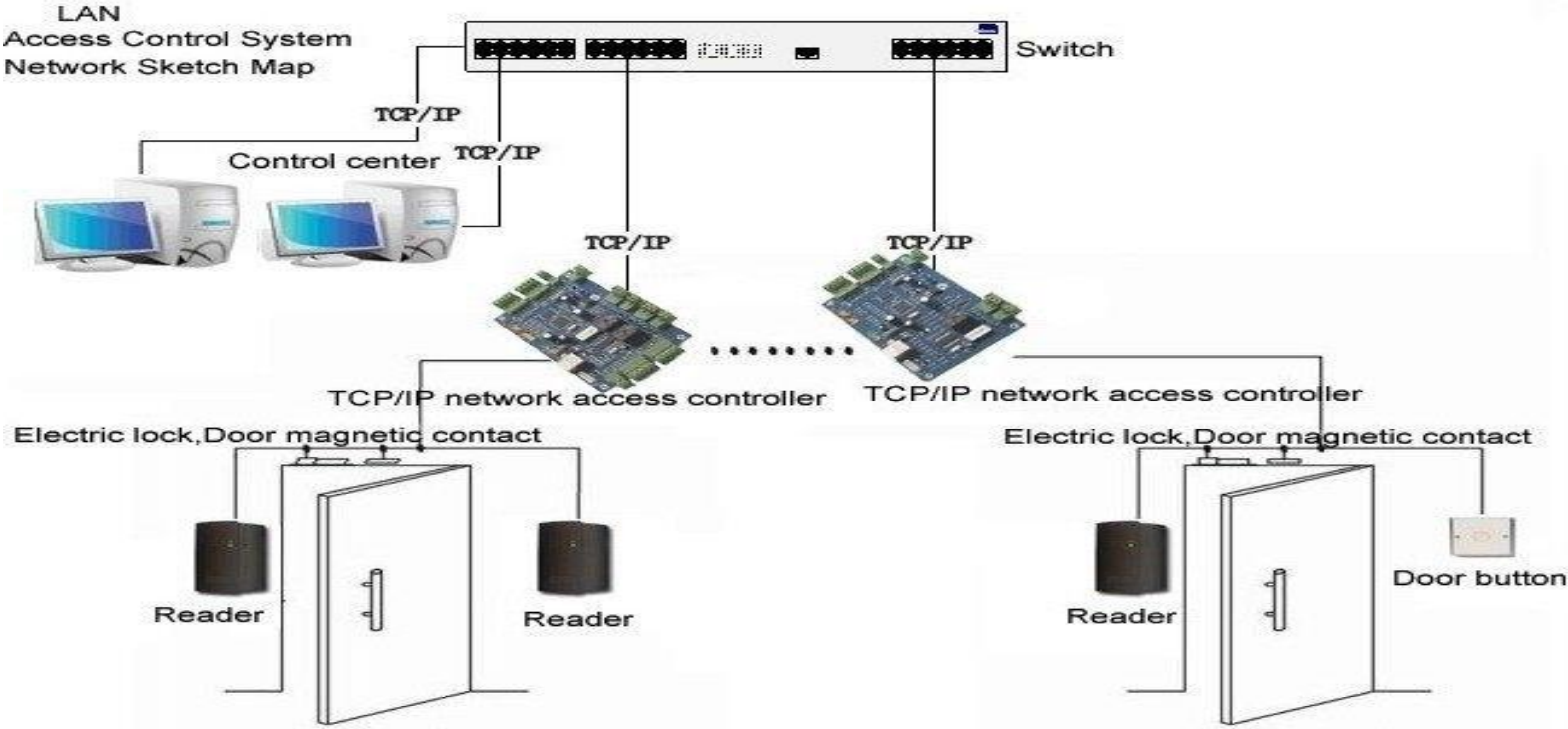
EXAMPLE OF KERI DOOR SYSTEM

Keytag Access Control

KERI DOOR SYSTEM ARCHITECTURE

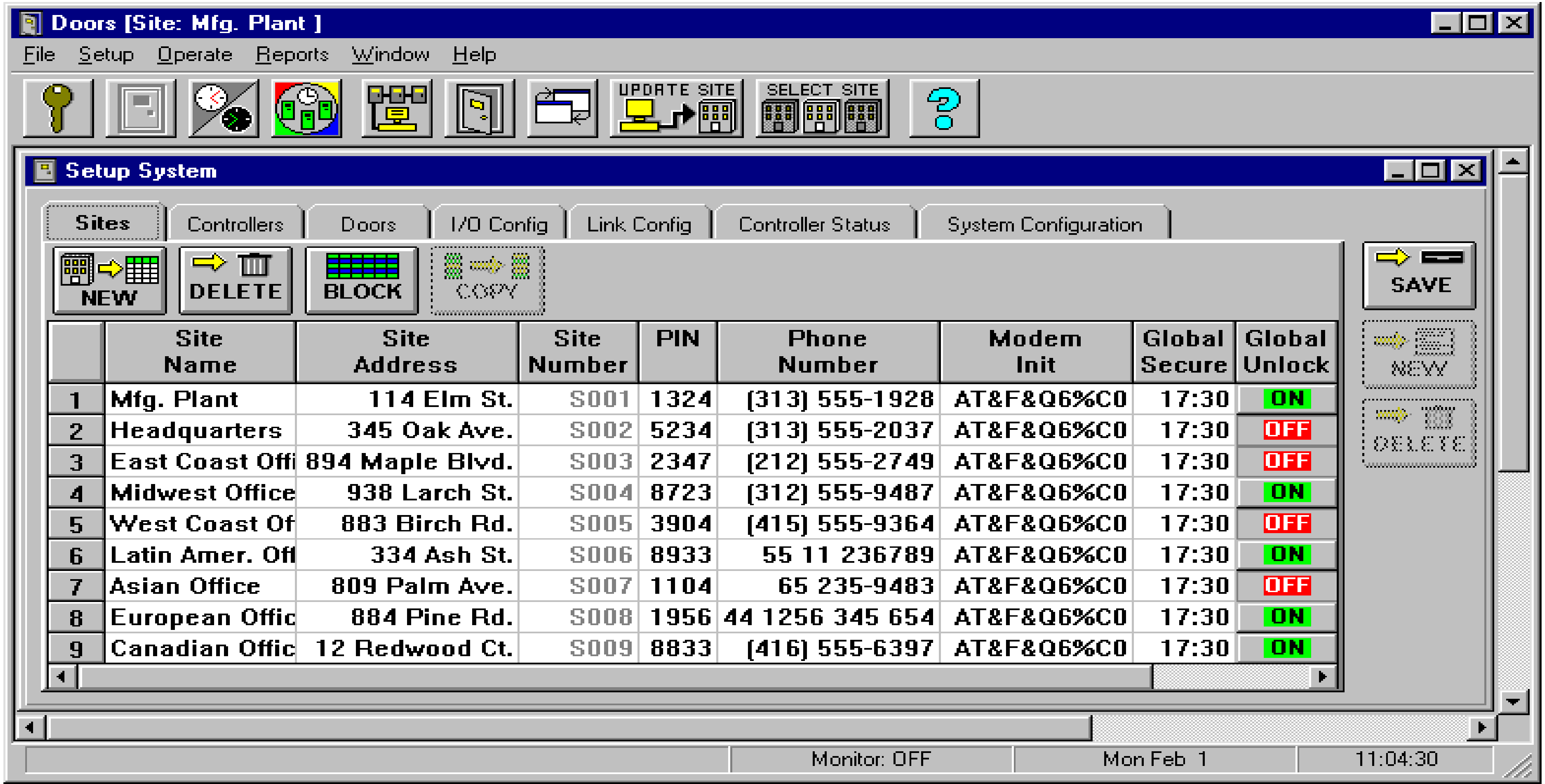


TOPOLOGY DOOR SYSTEM


LAN
Access Control System
Network Sketch Map
Switch
TCP/IP
TCP/IP
Control center
TCP/IP
TCP/IP
TCP/IP network access controller
TCP/IP network access controller
Electric lock,Door magnetic contact
Electric lock,Door magnetic contact
Reader
Reader
Reader
Door button

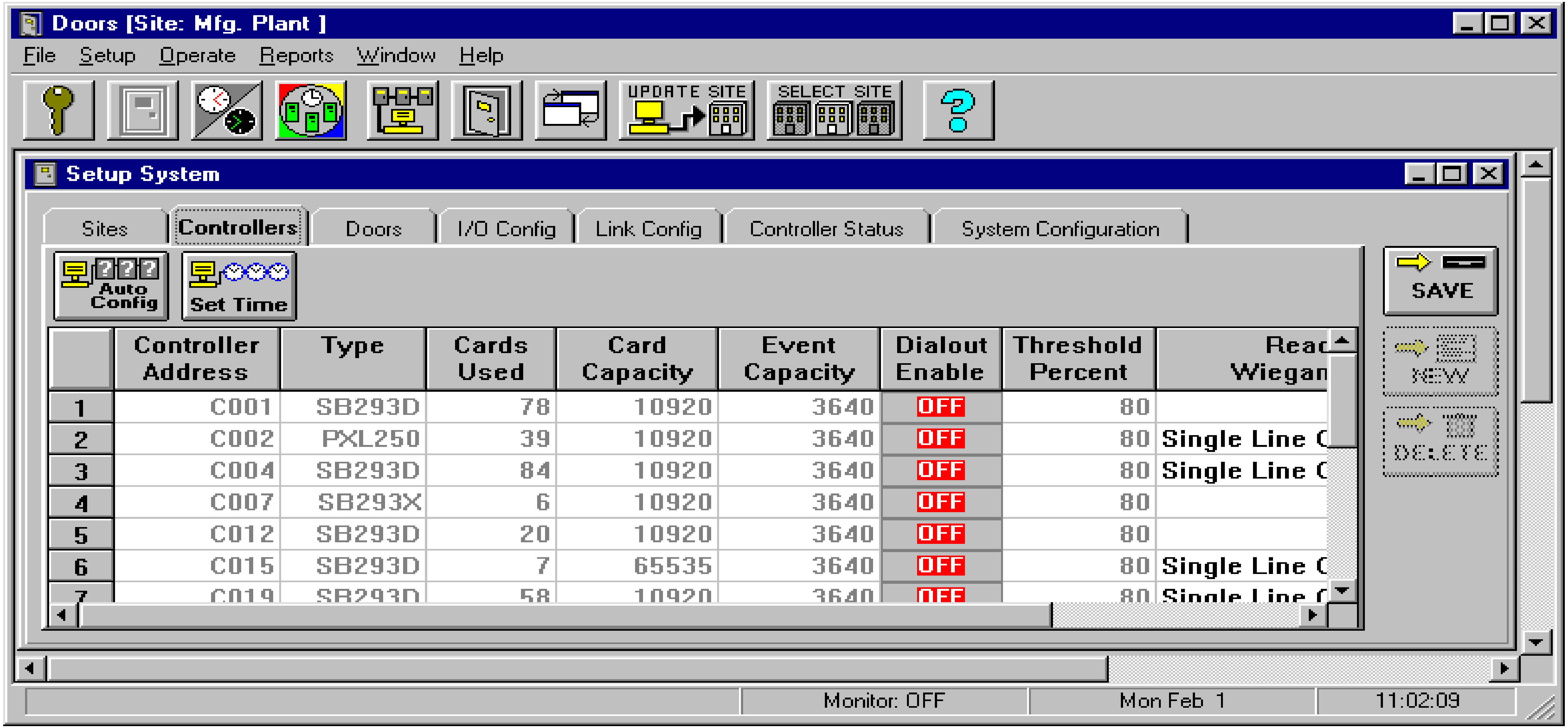
PHYSICAL ACCESS CONTROL LOG FORMAT

The Log Format



	Site Name	Site Address	Site Number	PIN	Phone Number	Modem Init	Global Secure	Global Unlock
1	Mfg. Plant	114 Elm St.	S001	1324	(313) 555-1928	AT&F&Q6%C0	17:30	ON
2	Headquarters	345 Oak Ave.	S002	5234	(313) 555-2037	AT&F&Q6%C0	17:30	OFF
3	East Coast Offi	894 Maple Blvd.	S003	2347	(212) 555-2749	AT&F&Q6%C0	17:30	OFF
4	Midwest Office	938 Larch St.	S004	8723	(312) 555-9487	AT&F&Q6%C0	17:30	ON
5	West Coast Of	883 Birch Rd.	S005	3904	(415) 555-9364	AT&F&Q6%C0	17:30	OFF
6	Latin Amer. Off	334 Ash St.	S006	8933	55 11 236789	AT&F&Q6%C0	17:30	ON
7	Asian Office	809 Palm Ave.	S007	1104	65 235-9483	AT&F&Q6%C0	17:30	OFF
8	European Offic	884 Pine Rd.	S008	1956	44 1256 345 654	AT&F&Q6%C0	17:30	ON
9	Canadian Offic	12 Redwood Ct.	S009	8833	(416) 555-6397	AT&F&Q6%C0	17:30	ON

The Log Format



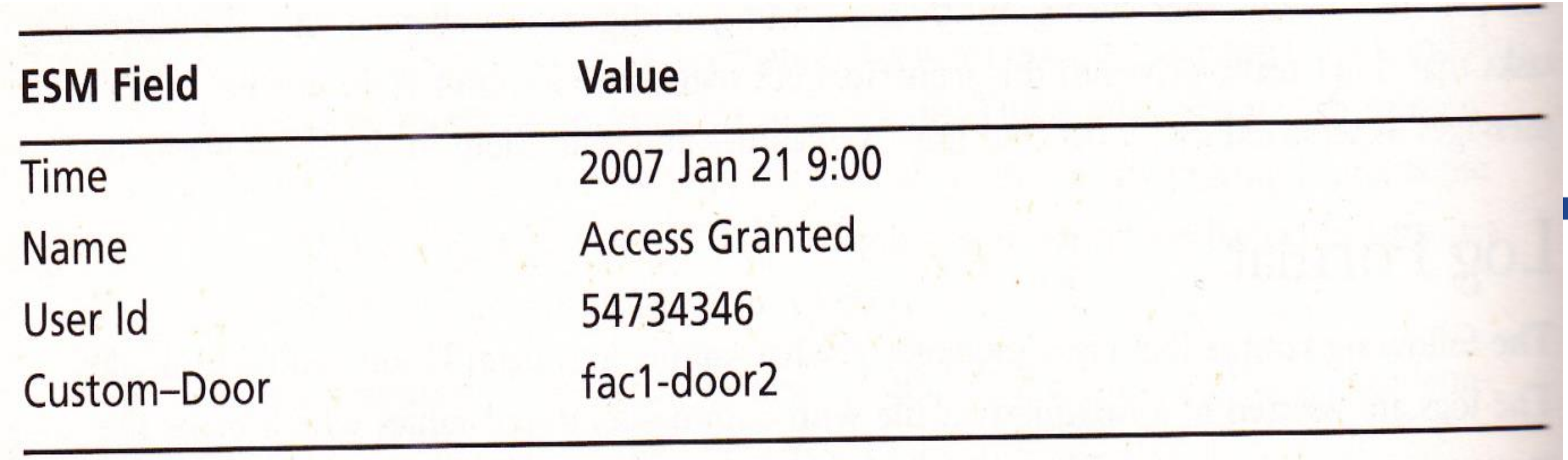
	Controller Address	Type	Cards Used	Card Capacity	Event Capacity	Dialout Enable	Threshold Percent	Reac Wiegan
1	C001	SB293D	78	10920	3640	OFF	80	
2	C002	PXL250	39	10920	3640	OFF	80	Single Line C
3	C004	SB293D	84	10920	3640	OFF	80	Single Line C
4	C007	SB293X	6	10920	3640	OFF	80	
5	C012	SB293D	20	10920	3640	OFF	80	
6	C015	SB293D	7	65535	3640	OFF	80	Single Line C
7	C019	SB293D	58	10920	3640	OFF	80	Single Line C

FROM LOGS TO ESM

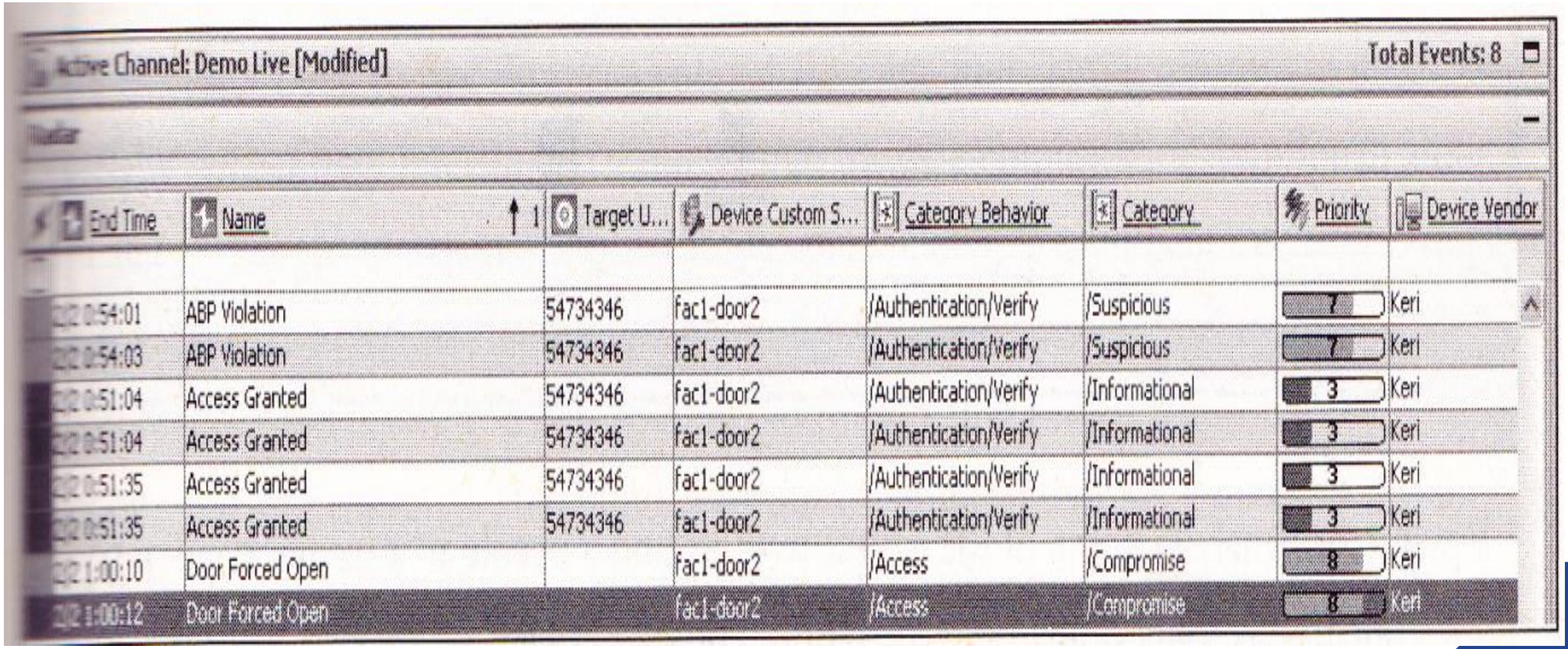
The Log Format

- Logs are written in a rotating text file with comma-delimited values
- General idea is between each comma there is a field with a value in it to be parsed and mapped to field in ESM schema

```
2019 Jan 21 9:00, Access Granted, 54734346,
fac1-door2
2019 Jan 21 9:00, ABP Violation, 54734346,
fac1-door2
2019 Jan 21 9:00, Access Denied (Access Group
Violation), 54734346, fac3-door3
2019 Jan 21 9:00, Door Forced Open, fac3-door3
```



ESM Field	Value
Time	2007 Jan 21 9:00
Name	Access Granted
User Id	54734346
Custom–Door	fac1-door2

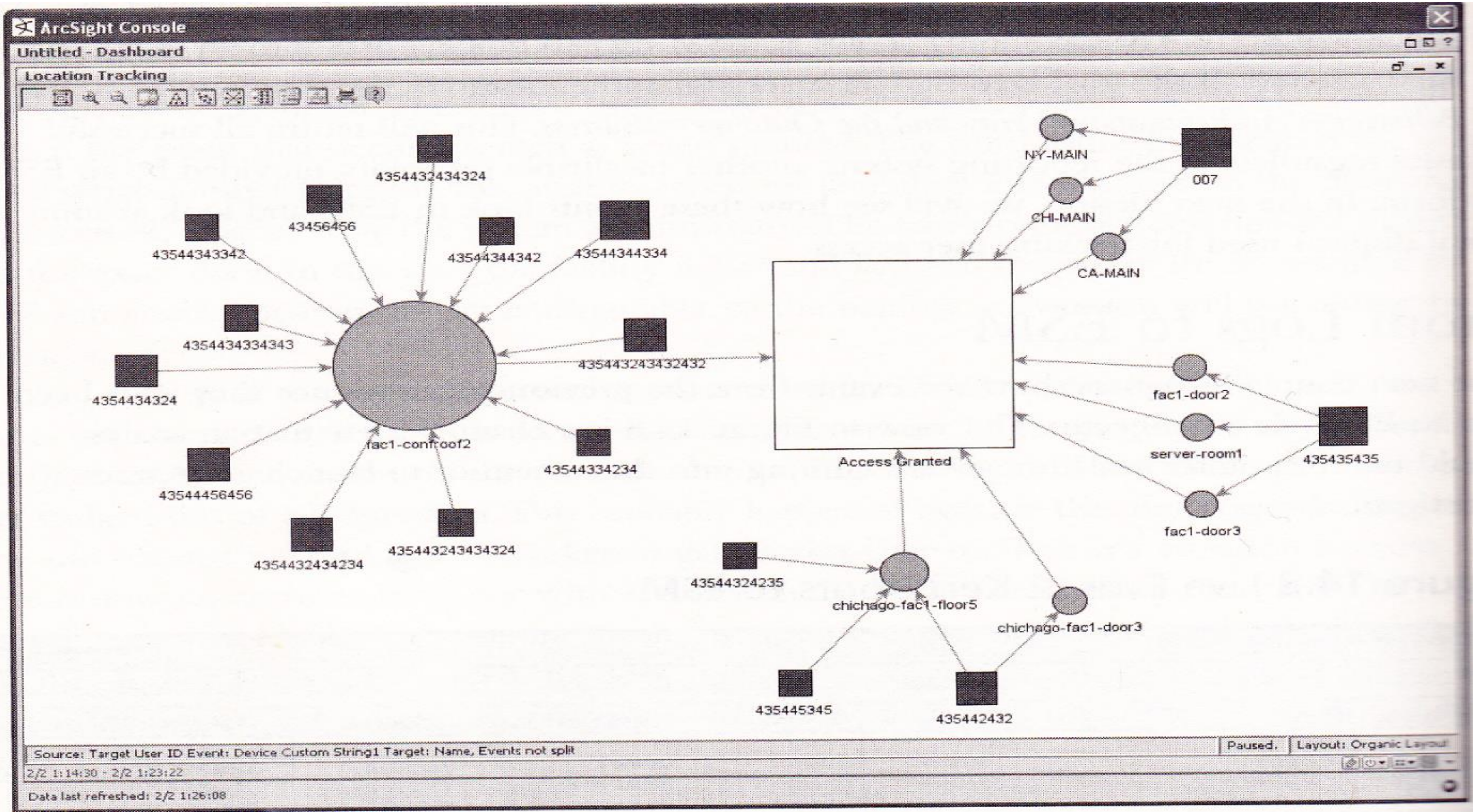


Active Channel: Demo Live [Modified]

Total Events: 8

End Time	Name	Target U...	Device Custom S...	Category Behavior	Category	Priority	Device Vendor
2/2 0:54:01	ABP Violation	54734346	fac1-door2	/Authentication/Verify	/Suspicious	7	Keri
2/2 0:54:03	ABP Violation	54734346	fac1-door2	/Authentication/Verify	/Suspicious	7	Keri
2/2 0:51:04	Access Granted	54734346	fac1-door2	/Authentication/Verify	/Informational	3	Keri
2/2 0:51:04	Access Granted	54734346	fac1-door2	/Authentication/Verify	/Informational	3	Keri
2/2 0:51:35	Access Granted	54734346	fac1-door2	/Authentication/Verify	/Informational	3	Keri
2/2 0:51:35	Access Granted	54734346	fac1-door2	/Authentication/Verify	/Informational	3	Keri
2/2 1:00:10	Door Forced Open		fac1-door2	/Access	/Compromise	8	Keri
2/2 1:00:12	Door Forced Open		fac1-door2	/Access	/Compromise	8	Keri

The syslog shows that at 9:00 a.m., on 21 Jan 2007, there was an incident of access granted with user id of 54734346 has occurred at fac1-door2. However, a violation of access has happened at fac3-door3 at the same time.



Source: Target User ID Event: Device Custom String1 Target: Name, Events not split

2/2 1:14:30 - 2/2 1:23:22

Data last refreshed: 2/2 1:26:08

CHALLENGES

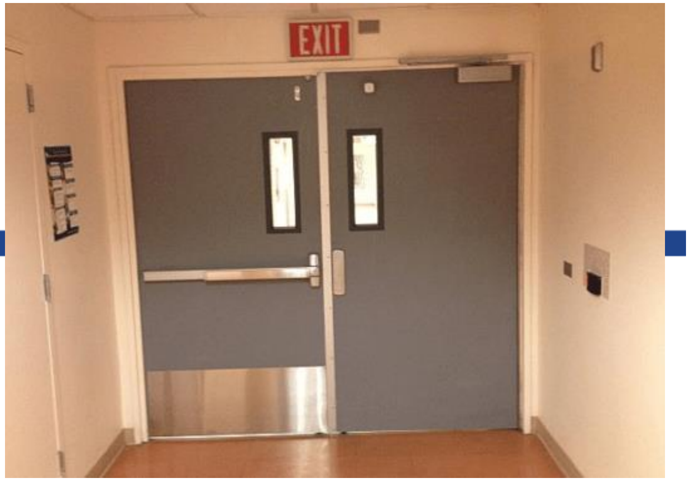
PIGGYBACKING

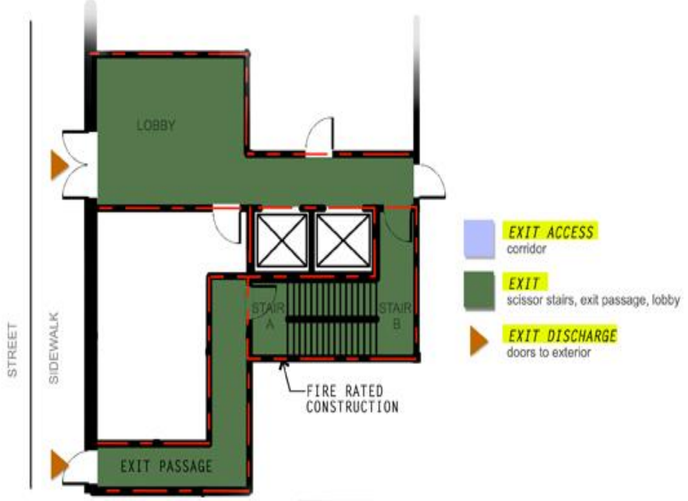
- Piggybacking means someone is carry by someone with his or her consent.
- Describes the situation in which one user authenticates but holds the door open in permission to another user so that another user can enter at the same time
- Challenge when trying to determine who is in the building
- Very difficult problem to address to ensure only one person at a time passes through an entryway
- Solution:
  - Airlock system: passageway with two doors and calculate weight, deployed only in extremely secure area
  - Concept of turnstiles: authenticate at individual section

TAILGATING

- Tailgating is when another person, whether an employee or not, passes through a secure door without the knowledge of the person who has gained legitimate access through the secure door.
- This is a similar concept to when there is a car following closely behind you on the freeway without your permission.
- You are being tailgated!

EGRESS





- The meaning of egress is ……
  - to go out or “to exit” (i.e.: jump or run away)
  - the action or method of going out of (i.e.: use stairs)
  - a safe place to exit (i.e.: area of gathering when emergency)
  - A continuous way of leaving form any point in a premise to a public area (i.e.: hallway)
  - The design of exits and other safeguards that reliance for safety to life (i.e.: fire drill training)

EGRESS

- Describe IP traffic that leaving a network or protected environment
- Typically done in border routers or firewalls
- Refers to physical access system that require users to badge out of a protected locations as well as in.
- If user doesn't swipe his badge on the way out, he will not be allowed back into the building when he returns.

INGRESS

- The meaning of Ingress is….
  - The act of going in or entering a building
  - Someone has a permission to enter
  - Example : a kitchen has an ingress door and egress door in the restaurant to provide easy movement for the chef and waiter.
  - Example: Highway

CORPORATE STRUCTURE

- The challenge is due to manager interferes with the imperatives criteria in business planning.
- Open source versus proprietary software used in business that usually not similar
- Group that controls and manages the PACS is typically not under the same organization, which these group need to know each other with top-down approach.

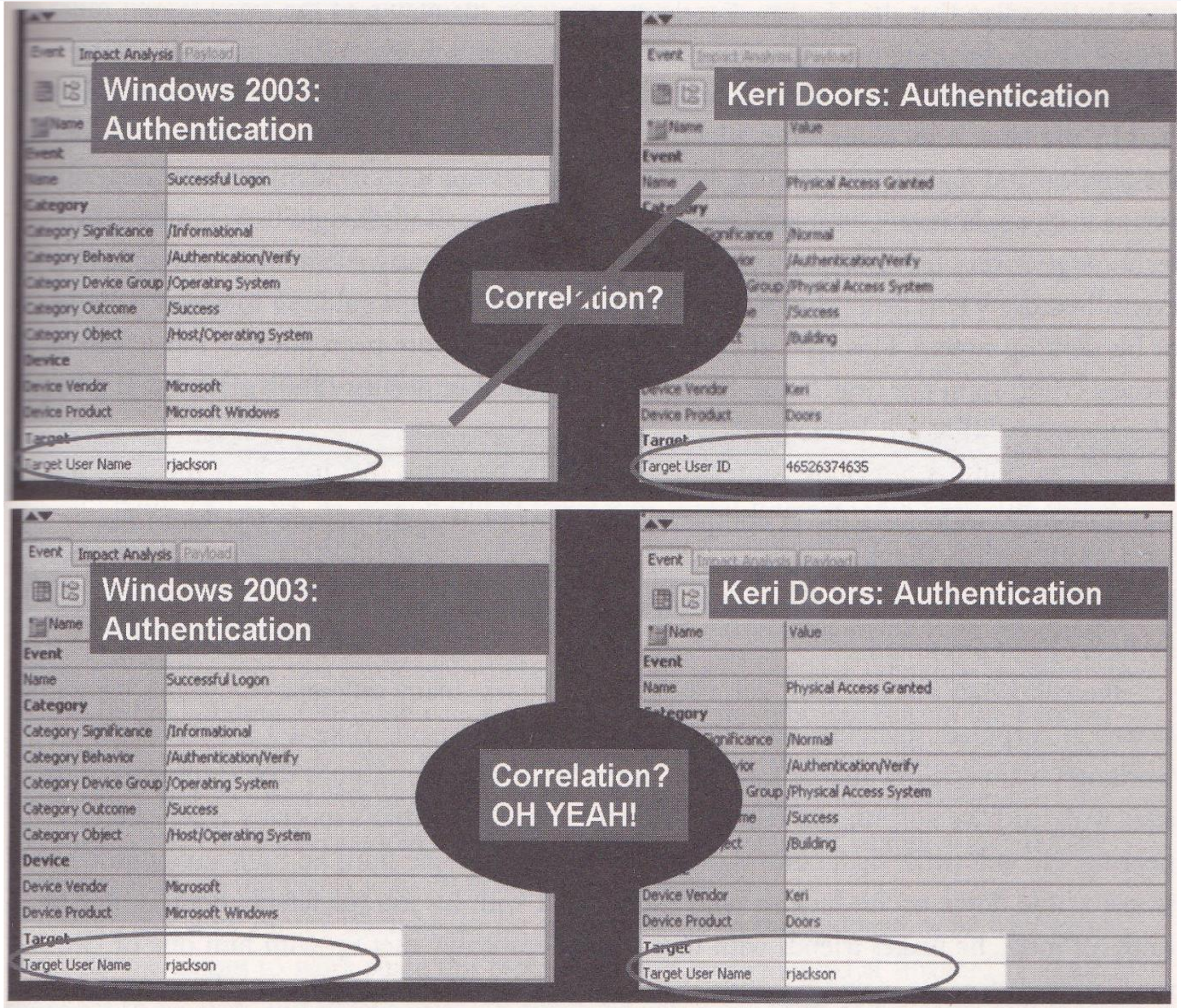
CORRELATION ISSUE

- Event correlation means a technique of capturing the application logs or host logs or system logs and analyzes the data to identify the relationships.
- Moreover, event correlation simplifies and speeds the monitoring of events by consolidating alerts or notification into short and easy-to-understand message.
- Example of application logs – error, warnings, failure from devices, firewalls deemed suspicious and SNMP traps.

CORRELATION – TIME DELAY AND BATCH LOADING

- When event batched, they are stored on end device and not sent to the collection point until a buffer is filled – problems for real time correlation
- Trying correlate an event from OS within milliseconds from when it actually happens
- Solution : provides real-time logging capabilities

CORRELATION – IDs and usr



Windows 2003: Authentication

Name	
Event	
Name	Successful Logon
Category	
Category Significance	/Informational
Category Behavior	/Authentication/Verify
Category Device Group	/Operating System
Category Outcome	/Success
Category Object	/Host/Operating System
Device	
Device Vendor	Microsoft
Device Product	Microsoft Windows
Target	
Target User Name	rjackson

Keri Doors: Authentication

Name	Value
Event	
Name	Physical Access Granted
Category	
Significance	/Normal
ior	/Authentication/Verify
Group	/Physical Access System
e	/Success
t	/Building
Device Vendor	Keri
Device Product	Doors
Target	
Target User ID	46526374635

Windows 2003: Authentication

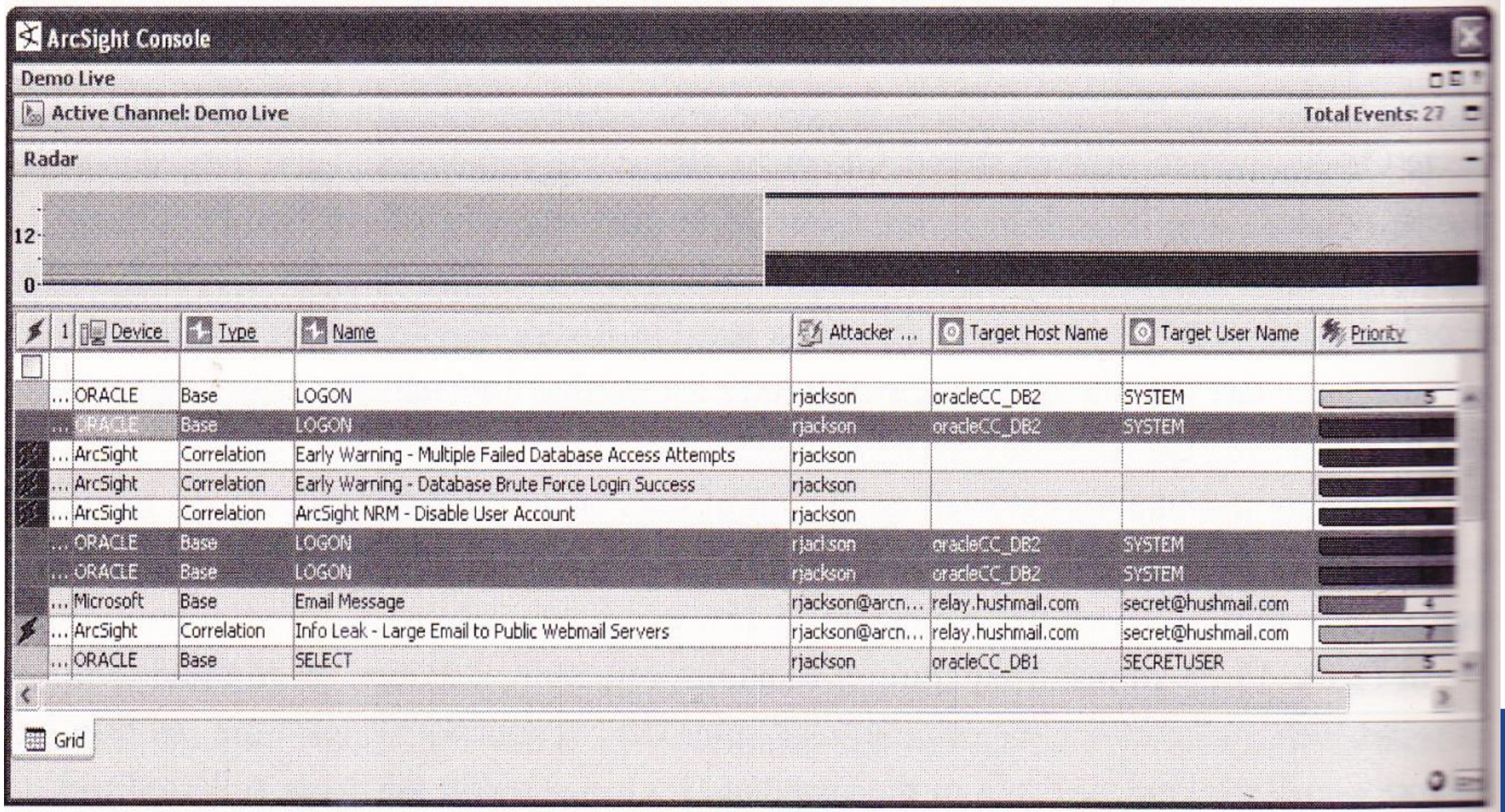
Name	
Event	
Name	Successful Logon
Category	
Category Significance	/Informational
Category Behavior	/Authentication/Verify
Category Device Group	/Operating System
Category Outcome	/Success
Category Object	/Host/Operating System
Device	
Device Vendor	Microsoft
Device Product	Microsoft Windows
Target	
Target User Name	rjackson

Keri Doors: Authentication

Name	Value
Event	
Name	Physical Access Granted
Category	
Significance	/Normal
ior	/Authentication/Verify
Group	/Physical Access System
me	/Success
ect	/Building
Device Vendor	Keri
Device Product	Doors
Target	
Target User Name	rjackson

CONVERGENCE DETECTION – PHYSICAL + VPN ACCESS

- Setup to detect malicious and non-malicious violations



ArcSight Console

Demo Live

Active Channel: Demo Live — Total Events: 27

Radar

⚡	1	Device	Type	Name	Attacker ...	Target Host Name	Target User Name	Priority
☐								
	...	ORACLE	Base	LOGON	rjackson	oracleCC_DB2	SYSTEM	5
	...	ORACLE	Base	LOGON	rjackson	oracleCC_DB2	SYSTEM	
	...	ArcSight	Correlation	Early Warning - Multiple Failed Database Access Attempts	rjackson			
	...	ArcSight	Correlation	Early Warning - Database Brute Force Login Success	rjackson			
	...	ArcSight	Correlation	ArcSight NRM - Disable User Account	rjackson			
	...	ORACLE	Base	LOGON	rjackson	oracleCC_DB2	SYSTEM	
	...	ORACLE	Base	LOGON	rjackson	oracleCC_DB2	SYSTEM	
	...	Microsoft	Base	Email Message	rjackson@arcn...	relay.hushmail.com	secret@hushmail.com	4
⚡	...	ArcSight	Correlation	Info Leak - Large Email to Public Webmail Servers	rjackson@arcn...	relay.hushmail.com	secret@hushmail.com	7
	...	ORACLE	Base	SELECT	rjackson	oracleCC_DB1	SECRETUSER	5

CONCLUSION

Conclusion

- Physical and logical access control is a mechanical form of physical items (such as key, door knob, or physical door) that controlled by software to verify or identify the identity of the respective person.
- With the use of physical and logical access control help the security administrator to secure the data and to be creative person to obtain the log from the evidence

Thank You

MyUTeM

www.utem.edu.my