



Leaking Beeps:

Unencrypted Pager Messages in Industrial Environments

Stephen Hilt and Philippe Lin

Trend Micro Forward-Looking Threat Research

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents

4

Pagers in the Age of Smartphones

6

Analysis of Leaked Protocols

7

Systems Used in Industrial Environments

9

Passive Intelligence

20


Spoofing Pages

21

Possible Attack Scenarios

22

Conclusion



When it comes to mobile communication, the smartphone is king. Despite that, there are still several industries using pager technology for communication. Unfortunately, we discovered that communication through pagers is not secure at all. Since pager messages are typically unencrypted, attackers can view pager messages even at a distance—the only thing attackers need is a combination of some know-how on software-defined radio (SDR) and US\$20 for a dongle.

Passive intelligence or passive information gathering pertains to the discovery of information unintentionally leaked by networked or connected organizations. While a significant amount of the effort to protect high-value assets is spent on protecting against or detecting active attacks or probing and exploiting security vulnerabilities, it is equally important to look at how much and what kind of information organizations are unwittingly offering attackers for “free”.

In the course of our research, we found that a disturbing amount of information that enterprises typically consider confidential can easily be obtained through unencrypted pager messages. Some of the information that were transmitted pertained to alarm/event notifications, diagnostics information and facility-related status updates—information that can help an attacker get familiar with a plant’s operation.

Aside from that, we also saw personal information being transmitted in the clear, such as email addresses, project codes, and employee names. Any motivated attacker can craft extremely effective social engineering attacks using these information. Thus any organization is at risk of suffering the repercussions of successful targeted attacks, which could mean anything from industrial espionage, loss of customer loyalty and trust to fatal real-world sabotage of public service systems, as in terrorism.

“Leaking Beeps” is a series of studies that aims to highlight certain weaknesses in pager technology and how those weaknesses could put critical activities of affected companies at risk. To identify such weaknesses, we will take a look at different industries that are still using pagers for everyday operations and how security comes into play. In this paper, we studied the implications of compromised security in industrial environments like nuclear power plants, substations, power generation plants, chemical plants, defense contractors, semiconductor and commercial manufacturers, and heating, ventilation and air conditioning (HVAC) companies.

Organizations that are still using pagers are advised to switch to an encrypted paging system with asymmetric keys. They should also have a process in place to authenticate any received paging messages. Finally, when using an email-to-pager gateway, organizations must audit possible leakage.

A more technically comprehensive version of this paper is available upon request.

Pagers in the Age of Smartphones

According to the National Institute of Standards and Technology (NIST), an Industrial Control System (ICS) is a general term for various types of control systems including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures.¹

To ensure optimal generation, production, and distribution of raw materials, ICS enables tight control of systems in industrial process plants through data-gathering, reporting, supervisory and local controls, timers, actuators, and self-corrector functions. Because of the nature of the materials processed, timely notifications regarding events or deviations and regular updates on remote diagnostics are crucial in the upkeep of facilities. For some organizations, pagers are still capable of addressing such a purpose.

While cellular coverage has widened over the years, some sectors still find it useful to maintain pager technology as a reliable means of communication—especially in areas where cellular frequencies are weak or nonexistent. In Japan, for instance, pagers or emergency radios using paging protocol are legally adopted as backup communication lines in cases of disasters.

Since the 1950s, physicians have been using pagers that can receive pager messages (pages) up to 25 miles away from a single transmitter tower.² In the 1960s, the technologies used in walkie-talkies and automobile radios were combined to create the first transistorized pagers. It wasn't until the 1990s that the general public began using pager technology. However, its wider adoption was cut short when it was replaced by current cellular technologies such as text messages or Short Message Service (SMS).

Pagers are still utilized today in different sectors, mostly because they need at least one communication device to alert and inform an end user in a consistently straightforward and reliable way. IT departments, industrial automation, restaurants, and big hotels, for instance, use pagers to deliver messages in a closed system within a limited distance. Eventually, different pager gateways were developed so that organizations can send messages across different platforms. For instance, short emails or SMS messages can be transmitted to pagers and vice versa.

Furthermore, it doesn't take much power to transmit pages over long distances. Since it only requires a pre-defined wattage to be sent, pages can be received even from tens of kilometers away from their transmitting facilities.

In the course of our research, we were surprised to find a lot of unencrypted pager messages from what we could consider critical industries. In the next section, we will discuss what we saw in these unencrypted pager messages.

Analysis of Leaked Information

Pagers were designed before security was even a concern and privacy standards were just coming about. Since pagers rarely use any type of encryption, paging messages are usually sent over the airwaves unencrypted and vulnerable to abuse.

Since pagers rarely use any type of encryption, paging messages are usually sent over the airwaves unencrypted and vulnerable to abuse. Through technical means, we were able to decode pager messages using software-defined radio (SDR) and a USB dongle as cheap as US\$20.

After setting up our equipment and software to observe pager messages, we began analyzing what types of information are being passed along in the clear. We did this to determine how well the pager technology—a relatively outdated means of communication—stands against today’s attackers, who have easy access to decoding tools as well.

The pager contents themselves are varied in form. This pie chart shows the distribution of data types seen in this research:

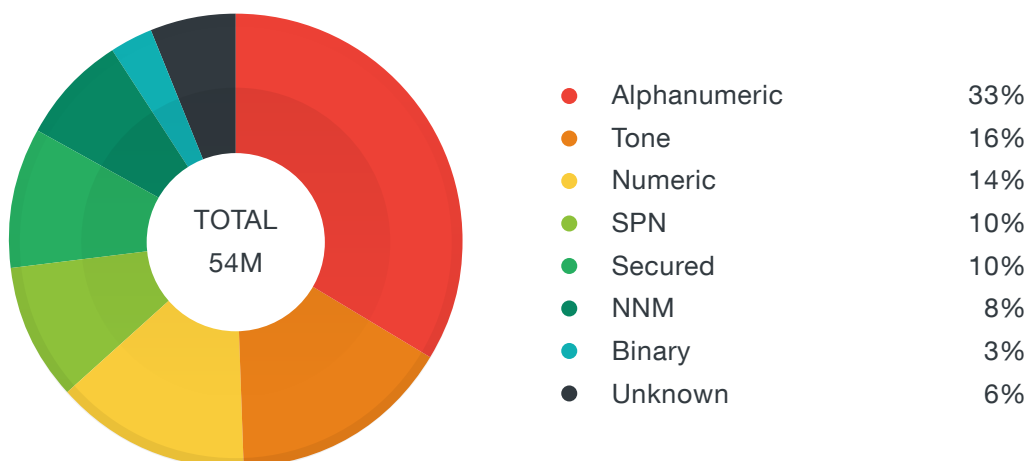


Figure 1. Data type distribution

While identifying the frequencies used in countries from around the world, we noticed that unencrypted pages are a systemic problem affecting several states in the U.S., and even other countries like Canada. The period of our observation is from 25 January 2016 to 25 April 2016. During the four months of study, we have monitored 54,976,553 records of pages, among which 18,368,210 (33%) are alphanumeric.

Systems Used in Industrial Environments

Industrial environments are becoming increasingly modern. Both ICS's and building automation systems (BAS) are used by industrial sectors to automate various plant and peripheral operations. ICS's are built with more robust systems that can handle industrial processes that directly impacts manufacture or operations. BAS, on the other hand, have simpler controls that manage some aspects of a facility such as heating or ventilation. However, both are capable of sending out notifications which we will see in the case studies in the Passive Intelligence section.

Industrial Control Systems

An ICS is made up of devices, systems, networks, and controls that are used to operate and/or automate industrial processes. These devices, which are specific to an industry, are often found in almost every industry today—from the vehicle manufacturing and transportation segment to the energy and water treatment segment.

In our paper titled, “Towards a More Secure Posture for ICS Networks” and “Who’s Really Attacking Your ICS Equipment?”, we discussed ICS in length. In this paper, however, we will focus on what happens when ICS is set up to notify people-in-charge about plant emergencies or updates via pager technology. Most of the examples in the Passive Intelligence section were evidences of this capability.

Building Automation Systems

Building Automation is a centralized system which allows the automatic control of certain parts of a building’s heating, ventilation, and air conditioning or HVAC. Other components such as lighting can also be controlled from a centralized system. Building Automation Systems (BAS) are complex systems that are made up of sensors, controllers, output devices, communications protocols, and a user interface.

BACnet is the most popular communications protocol. But just like most industrial control system protocols, it is not secure, meaning that it’s an unauthenticated protocol that’s not encrypted.

Unlike typical control systems, BAS’s rarely have someone to monitor every activity 24/7. Due to this,

remote alarms can be set up. A common way is to send alarms over SNMP to a monitoring system to alert the appropriate people. During the course of this project, we saw multiple systems utilizing pagers for alarm functions. These alarms can leak out information about the buildings' layout, products in use, as well as other company-specific information that should not be seen by anyone outside the company.

Potential abuse of this information leaking out would involve malicious actors who want to break into a facility. To get in, they could monitor the building's temperature settings, lighting settings, and other sensors and then alter those settings when no one is inside the building.

WebCTRL System

Automated Logic WebCTRL® System is a building automation system that gathers, analyzes, and visualizes the data collected from sensors and controllers. Some of its features include colored floor plans, scheduling, alarming, logging, and reporting. It also sends an email to engineers and administrators when an alert is triggered, which is then forwarded via an email-to-pager gateway. We were able to observe this through a pager's radio signal.

Email-to-pager gateway is a service, usually provided by a third-party company that pushes emails sent to a specific address to predefined paging numbers. People sometimes have a false assumption that emails are private and confidential. Emails, however, are usually transmitted in plain text through the internet. Forwarding the emails to pagers makes them transmitted in the clean air, thus being even more vulnerable to unexpected readers since encryption in paging systems is uncommon.

Despite WebCTRL being designed for building automation, we have seen its extended use as an ICS with a fancy interface. We observed the extensive use of WebCTRL in an important defense partner, where there were conventional controls over humidity, ventilation, particle counts, as well as non-conventional controls like generators, boilers, and chillers.

METASYS

METASYS® is a building automation system (BAS) from Johnson Controls, designed for energy efficiency, HVAC, lightning, security and protection system. With field equipment controllers, input/output modules, network engines, thermostats, application and data server (ADS), METASYS makes a complete ecosystem that allows users to manage the BAS on computers, tablets, and smart phones. Just like WebCTRL, we also observed the alerts sent to engineers via email-to-pager gateways.

METASYS has a special identifier on its HVAC systems, called Fully Qualified Reference. By analyzing the fully qualified reference (FQR), we know which checkpoints in a particular facility have raised an alarm or have returned to normal states. It is relatively easy to figure out that the prefix is usually related to the abbreviation of the facility.

Passive Intelligence

Passive intelligence is information gathering as opposed to active intelligence, which requires an attacker to make some kind of contact with the target's network. Instead of using ping and port scanning to find open ports on servers or calling someone to social engineer required information, that might risk alerting people of the attack, attackers relying on passive intelligence would instead wait and listen to whatever information they can collect on the internet and other sources and then carefully analyze them before a real penetration test or attack takes place.

Pages, it turns out, are considered a source of high quality passive intelligence. During four months of observation, we saw messages containing information on contact persons, locations inside manufacturers and electricity plants, thresholds set in industrial control systems, field engineers who were flooded by too many messages, possible unreported restricted events, intranet IP address, intranet hostnames, Structured Query Language (SQL) table names and queries. Information such as phone numbers and contact persons' names can be used in social engineering attacks, while intranet IP and hostnames are very useful for lateral movement.

We are going to discuss the observations we had for every case in the following sections, in order to estimate the potential damage unencrypted paging messages might cause to organizations. The cases include nuclear plants, power administrations, chemical plants, defense contractors, and semiconductor manufacturers. In addition to English pages, we will also inspect pages in French.

Note that any mention of specific ICS or BAS software in this research does not suggest any issue with the software themselves but only that they use the legacy protocols that pager vendors had set to communicate with pagers, which is the subject of this paper.

Nuclear Plants

The first paging messages in the industrial sector that caught our attention came from several nuclear plants scattered among different states. Most of the messages were not generated by automated systems, but were written by a real person and then sent to people via an email-to-pager gateway.

These are a few examples of incidents that took place inside the nuclear plants:

- Reduced pumping flow rate
- Water leak, steam leak, radiant coolant service (RCS) leak, electrohydraulic control (EHC) oil leak
- Fire accidents in an unrestricted area³ and in an administration building
- Loss of redundancy
- People requiring off-site medical attention (*Note: This is a reportable event according to regulations*)
- A control rod losing its position indication due to data fault
- Nuclear contamination without personal damage

The United States is the only country wherein nuclear plants continue to send paging messages. We did not check if all the incidents were reported but such events are usually found in the US Nuclear Regulatory Commission website.⁴

Substations

Power substations within the United States have a lot of regulations and security controls that are supposed to be followed. These rules, also known as North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), provide a basic framework by which all communication channels are supposed to be evaluated. Because of this we were surprised to see some information coming from substations via pager systems. An example follows below:

```
From: [EMAIL] Subject: Alert - Alarm: [SUBSTATION NAME] Control House N.E.  
Door Held. [SUBSTATION NAME] Sub. Control House RTU Cabinet (NERC) [26]
```

Based on these pages there is a fair amount of information that can be collected about the surrounding infrastructure. The potential impact could also be properly assessed by looking at the number of customers that were affected. In all of the incidents, the locations and times only showed small amounts of affected customers. Information about critical incidents, such as the ones listed above, can be used as leverage by attackers and other utility companies who wish to gain competitive advantage.

In the United States, power traders usually have no access to information concerning real-time operations of running a power grid since they may use that information to price fix power. Some of the information that we saw could be considered real-time operations information that could also be utilized by traders for inside information or to increase trading power.

Power Plants and Generation Stations

Just like the substations identified in this research, power generation stations, despite the existence of NERC CIP's guidelines regarding communications, were also transmitting pages in the clear. Most of the pages seen from power-producing facilities were notifications and alerts that were sent through SMS- or email-to-pager gateways.

```
From: [EMAIL]- Due to storm, we lost the steam plant momentarily, there  
are downed trees and lines are down. Generators are running for bldgs.  
that lost power. [31]
```

Some of this information could be used to determine the location of issues, the amount of generation that was lost, the potential response, and the names of employees who were responding to the issues. Most of these information may not be useful to an attacker but would definitely be useful for groups that are monitoring facilities.

Chemical Companies

Chemical companies deal with sensitive raw material so it was also interesting to find several pages pertaining to their operations. In the course of our research we were able to see at least two chemical plants that transmitted pages.

Chemical Company A

We saw an abundant quantity of paging messages sent by the SCADA system of one of the world's largest chemical companies. These paging messages can be used to compose a list with site, checkpoint, and threshold. Although the pages might contribute little to industrial espionage, they somehow give a snapshot of the plants' current status.

Unlike what most people think, figuring out the format of the paging messages is easy. With enough patience, an attacker can easily have a clear view of the ICS devices in a plant and use that information to compose fake messages. Threat actors with in-depth knowledge of ICS may be able to figure out the systems in use based on the naming scheme, and then use that information to check if there are any vulnerabilities.

We also found a very interesting message which contained a complete stack dump of some unknown device sent over pagers. It took about 20 minutes to finish the dump.

We also noticed that the service team had probably received too many messages in a day. The average number is 30 pages per cap code (a code similar to IMSI or phone number of a pager) per day. However, in an extremely busy day, there were a maximum of 550 pages per day, (or 90 pages per cap code per day) which is similar to a denial of service. Such a situation might cause some delays or inconvenience on the plant's notification and monitoring process.

Chemical Company B

We saw several paging messages about a specific dam with a name that suggests it might have been located in Florida. The messages also contained information about this dam (i.e., TS-1B, river, and KP_INPUT_levels). However, the domain name in the "From" field suggests that the pages came from a chemical company located in Delaware instead.

At first all those information did not make sense. But when we verified the location of the chemical company through the Google Maps™ application, we understood why the chemical company had to send information about a particular dam.

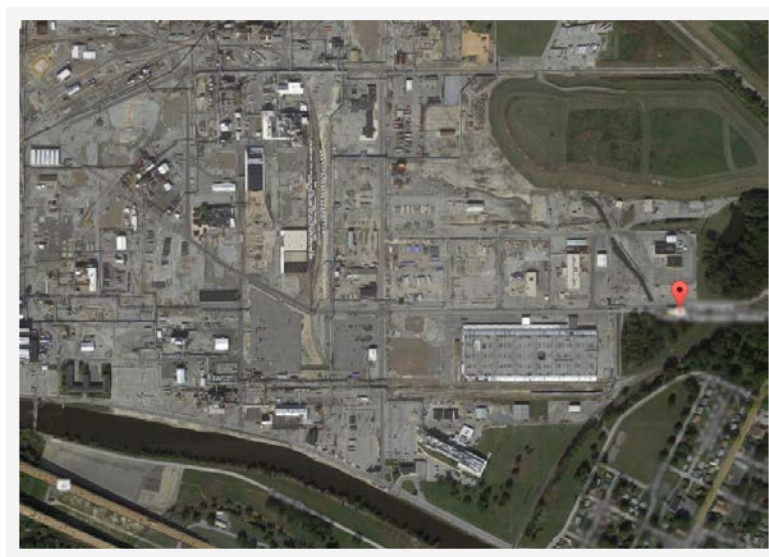


Figure 2. Map of the plant's surrounding area using Google's mapping service, Google Maps

By looking at the chemical company's location through Google Maps, we discovered that the chemical company referred to in the pages was right beside a canal. According to a report by the National Dam Safety Program, there is only one dam located near the said canal, which is the dam that was identified in the pages. With this, we figured that the dam's activities had an effect on the chemical company's operations one way or the other.

Defense Contractor

The researchers noted more than 1,380 email addresses from the email-to-pager gateway of one of the largest defense contractors in the world. However, there were only a dozen active users that gave more information. Two of the most active users were the WebCTRL® and Niagara Tridium accounts, both of which are automation systems.⁵

WebCTRL

There were two test pages that were sent to two cap codes every day. We observed a list of events along with the abbreviation codes by checking the cap codes. The list is only an excerpt of 77 types of events we were able to determine using these pages.

Abbreviation	Description
--	Steam Boiler 1 is in alarm
!PC_HI2	High Space Particle Count Level 2
!ZH_LO1	Low Zone Humidity Level 1
!ZT_HI1	The zone temperature is too warm
A2	[BRAND] ACU #2 (Server Room) is in alarm
CCT_LO	The cooling coil air temperature is too cool
CH18_COMM	Chiller 18 Bacnet communication is offline
CHST_HI	The chilled water supply/return temperature is too warm
CWRT_HI	The condenser water return temperature is too warm
DIA4	General DI Alarm Input is on
EF_FAIL	Kitchen Exhaust Fan status is OFF when it should be ON
FANA_HAND	Cell 1 fan status is ON when it should be OFF
FRZ_HI	Freezer temperature is too warm
GEN_HAND	Generator is running in hand
MAT_HI	The mixed air temperature is too warm
P1_FAULT	Pump 1 VFD fault is ON
PCST_LO	The process cooling loop chilled water supply temperature is too cool

Abbreviation	Description
PHP_HAND	The preheat coil pump status is ON when it should be OFF
PH_HIGH	pH is too high
PH_LOW	pH is too low
RAFLO_LO	The return airflow is too low below set point
SAH_LO	The discharge air humidity is too low
SSP_LO	The static pressure is too low below set point
SUMP_HI	The cooling tower sump water level is too high
TS-SCHS	Tertiary CHW Loop Supply Temperature is too warm

Table 1. Excerpt of list of events

Despite that, we were not certain where or how the WebCTRL events will be applied.

In addition to the event codes, we were also able to identify the sites where the events took place. Below is part of the list of sites:

Site
E625 Lab
I052 Server Room Temp/Hum
MSAT AHU-1 (High Bay)
MSAT AHU-2 (Airlock)
SAF II/III Chiller Monitoring
SAF III Hum Alm
SRACU-7 S109A / S116 SIG-1F-1B Freezer
Sigma Chem. Storage SIG-1F-1A Freezer High Temp: Alarm
WebCTRL AHU Alarm (AHU 15-18 Static Pressure)
WebCTRL Alarm (B-Base Acid Pit: Alarm)
WebCTRL Alarm (B-Base Sewage Pit: Alarm)
WebCTRL Alarm (B105 Focalplane Zone Humidity: Alarm)
WebCTRL Alarm (C-Mod Acid Tank: Alarm)
WebCTRL Alarm (CO VAV J-28 (J213A Server Room): Alarm)
WebCTRL Alarm (G-Mod Generators: Alarm)
WebCTRL Alarm (I052 [Brand] ACUs: Alarm)
WebCTRL Alarm (K-Mod Freezer Temp: Alarm)
WebCTRL Alarm (K-Mod Perimeter Htg. / KREF-5: Alarm)
WebCTRL Alarm (Plant Air Pressure: Normal)
WebCTRL Alarm (Plant-Air Moisture: Normal)
WebCTRL Alarm (SP High pH: Alarm)
WebCTRL Alarm: DUV Photo Area Humidity
WebCTRL CHW System Alarm (C-Base CHW Loop Temp)
WebCTRL CHW System Alarm (C-Base CHW Pumps)

Site
WebCTRL CHW System Alarm (CRMF Chiller BACnet)
WebCTRL CHW System Alarm (Tower 3)
WebCTRL HW System Alarm (C-Bsmt Boiler Room FCU)
WebCTRL HW System Alarm (Sigma HW Valve)

Table 2. An excerpt from the list of sites where the events took place

Niagara Tridium

Tridium's Niagara Framework® is a solution for building integration and enterprise connectivity. We have observed 371 normal events and 333 off-normal events. We also noticed that the thresholds can be deduced from the paging messages, like the sample that follows:

```
From: tridium@[DOMAIN]Subject: Alarm From 66_Boiler_2_Supply_Temp -
State: Normal Text: 66_Boiler_2_Supply_Temp has returned to normal!
Timestamp: 22-Mar-16 3:58:47 AM PDT
```

Site	LO Threshold	HI Threshold
66_Boiler_1_Supply_Temp	120 DEG	
66_Boiler_2_Supply_Temp	100 DEG	
66_Chiller_1_Supply_Temp		58 DEG
66_Chiller_2_Supply_Temp		56 DEG
905_Chiller#1 Leaving_Temp		50 DEG
M1_Chiller CHWS_T		50 DEG
M4_HB_AH5_Dungeon SF-S	OFF	
M7_Boiler PLHWS_T	125 DEG	
R3_RDC_1171_East_Zn_Temp		78 DEG
R3_RDC_1171_East_Zn_Temp#2		80 DEG
R5_CTF Norht_Water_A	Leak	
R5_CTF Y10X13_ZnTemp		78 DEG
R5_CTF_[Brand]_RAT		
R11_2354A_Data_Room SpaceTemp		75 DEG
R11_CRAC10_Rm1905 SpaceTemp		75 DEG
R11_CRAC11_Rm1210J SpaceTemp		75 DEG
R11_CRAC14_Rm1210G SpaceTemp		75 DEG

Table 3. List of thresholds by site based on pages

Semiconductor Companies

Information that leaks via paging messages are not limited to information about critical infrastructure and military contractors. During the course of our research, we saw one particular case wherein TopView® (FMS-Monitoring), which is used in the civil sector, had messages forwarded to pagers as well.

TopView is an alarm management and notification system which was developed by Exele Information Systems. It is featured with the integration of audible alarms, email, SMS, voice notifications, SNMP traps and pagers.⁶

We also saw messages sent by an unknown system with more than 350 checkpoints and a hundred types of events—including various alarms and even a notification about a NaOH (sodium hydroxide) leak. Actual sensor values are sent to InfraEES-sasrelay@mail.[DOMAIN].com, and most messages are sent to five cap codes.

The paging message is composed of a FAB unit (gas, scrubber, chiller, pump, etc.), timestamp, a checkpoint (INMS13/12_a), alarm message, and event (high or low process cy, etc.). As for FAB units, we saw FAB1_GAS, CU_FAB1_CHILLER, CU_FAB1_SCRUBBER, CU_FAB1_PUMP, FAB2_GAS, FAB2_CHILLER, FAB2_CHILLER_M2, FAB2_PUMP_M1, FAB2_PUMP_M2, FAB2_SCRUBBER, and FAB2_SCRUBBER_M2. However, we do not know how to decode the checkpoints, like SDEMS4MS01S_A or S-DCS-203A/B-D. A list of frequent events follows.

- | | | |
|--------------------|----------------------|---------------------|
| • LOW CYL WEIGH | • EMERGENCY STO | • BULK FILL TIMEOU |
| • NO COM | • LOW BRANCH DEL 1/ | • BULK RES OVERFUL |
| • LOW PROCESS CY | • BRANCH 2 EPO ALAR | • BULK SCALE BROKEN |
| • BULK RES LO | • OPERATOR INPUT TI | WIR |
| • LOW PURGE DEL PT | • POWER U | • BULK VENT FAILE |
| • BULK EMPT | • BRNCH 1/A SHUTDOWN | • RES OVERFUL |
| • LOW EXHAUS | • COAX LEAK 7/ | • SOLVENT OVERFUL |
| • LEAK TEST FAILUR | • HARDWIR | |

In addition to these fairly readable events, there are events in plain English, for example, “Waste Gas Valve1 Bypass” or “Dry pump body temperature Control Limit Alarm”.

We noticed that part of the factory uses another monitoring system, labeled as SAS_CHEMICAL. The messages are similar to the aforementioned ones.

```
SAS_CHEMICAL: F2M2_SAHFAB1-02, Measuring Bath Level Sensor Trouble
```

```
SAS_CHEMICAL: F2M2_SAHFAB1-02, Mixing Tank B Mixing Fail
```

```
SAS_CHEMICAL: FAB1_CBAHOD-01, Drum A Empty
```

```
SAS_CHEMICAL: FAB1_CBAHOD-01, Unit Door Open (Drum Zone
```

```
SAS_CHEMICAL: FAB1_CSNBAD-01, Day Tank Level Low Alarm
```

```
SAS_CHEMICAL: FAB1_CSNBAD-01, Distribution Outlet Pressure High - PT-30
```

```
SAS_CHEMICAL: FAB1_F1-PECT230-C10-01D, Unit End Point Pressure High
```

Sometimes, human-readable messages with an extension number are sent. For example, a NaOH leak was reported and a person using a specific extension number was contacted. It seemed like that person was the appropriate party to contact about the incident.

HVAC

HVAC systems are mainly used for building automation. Most alerts are about ventilation, temperature, humidity, and steam boilers, hence are not mission-critical and should be irrelevant to be considered part of a company's manufacturing secrets. We only saw one exception where a sewage high water alert was sent to a hospital. HVAC messages are sent via email-to-pager gateways, like most of the aforementioned cases, and from the email addresses alone we can tell which facilities are running HVAC systems. We saw a few universities, a chemical manufacturer, a semiconductor company, and an energy provider using HVAC, among others.

Email Address	Company Description
metasys@[DOMAIN].com	A solution provider
hvac-alarm@[DOMAIN].org	A healthcare alliance organization
METASYS@[DOMAIN].net	A healthcare network
ADX@[DOMAIN].org	A center for cancer study
ADS@[DOMAIN].com	A medical center
Metasys@[DOMAIN].com	A major solution provider
hvacalarms@[DOMAIN].com	A healthcare alliance organization
piadmin@[DOMAIN].com	A chemicals manufacturer
HVAC@[DOMAIN].com	A power management solutions provider
[NAME]@[DOMAIN].com	An energy provider
SiteScan@[DOMAIN].com	A clothes manufacturer
METASYS@[DOMAIN].EDU	A state university
bms@[DOMAIN].com	A steel and metals manufacturer
NoReply@[DOMAIN].net	A parish in California
noreply@[DOMAIN].com	A hospital integration solution provider
mt0100055@[DOMAIN].com	A grocery store in Texas
Bldg10@[DOMAIN].com	A telecommunications solutions company
[NAME]@[DOMAIN].com	A defense contractor
[NAME]@[DOMAIN].com	An interior design company
[NAME]@[DOMAIN].com	A real estate services company
TMSException@[DOMAIN].org	A healthcare delivery system company
2way@[DOMAIN].com	A call center company

Table 4. An excerpt from the list of identified HVAC users

Most HVAC paging messages are plain alerts about running and failing fans and room temperature going below or above preset thresholds. However, we noticed that pages from a cancer research center in Texas, for instance, contained information such as an unknown code, a particular event type, a building number, a contact person's name and phone number, actual values of items monitored, and their corresponding descriptions

Although we weren't able to find a map of the university that housed the said cancer research center on the internet, it was interesting that we were able to identify several buildings inside the university by simply reading through the paging messages. This, we believe, is a good case of passive intelligence. Here are some of the university buildings that were described in the messages we viewed:

- BLDG [NUMBER] ADMIN
- MAIN BLDG [NUMBER]
- SERVICE BLDG [NUMBER]
- LARGE ANIMAL BLDG [NUMBER]
- CHIMP EXPANSION BLDG [NUMBER]
- CHIMP LONG TERM BLDG [NUMBER]
- WATER STORAGE BLDG

A certain medical school in Houston, Texas had been using a paging system a lot. In addition to patients' personally identifiable information (PII), they have HVAC messages about outlet filter pressure, boilers, freezer farm, condenser water pump, condenser head suction pressure, SAT acid circulating water pump, and variable air volume (VAV) box.

We also saw several cases where BACnet was used as the industrial control system.

Commercial Printing

During our study, we also found a company engaged in commercial printing. Through the pages we observed it was interesting to find that several issues concerning the manufacturing process were reported to engineers. The system that the company used looks quite innovative—since most of the systems we observed did not have the same look and feel of this particular system.

Non-English Cases

Apart from the English-language pages, we saw several pages used by ICS and HVAC in French. Identical to the English messages, there are alarms for temperature, boilers, tanks, doors, and fans. An example follows:

```
Su.:Friday, 04/29/2016 at 13:56:57. The Point A301A.ALERTE is Normal..
```

```
Alarm Message: VENTILATION SYSTEME A301A EN PROBLEME
```

```
Trans.: Ventilation system A301A in trouble
```

Once passive intelligence is collected, a malicious attacker might proceed to perform social engineering tactics by actively looking for more weaknesses, sending fraudulent paging messages, or even carrying out a real intrusion. We will describe several attack scenarios in the following section.

Spoofing Pages

Lots of information can be seen from sniffing pager messages. However, it is also possible to inject your own pages if you have basic information about the systems in use. Without encryption and authentication, pager messages are easy to spoof as there is no way to verify that the messages are sent from trusted and known sources.

To test these theories, we bought some pagers to simulate the sending of pager messages. The goal was to send pages that were created by the researchers and prove that valid pagers would receive crafted messages from SDR. The simulation was done in a secure environment so it would not affect any existing pager systems.

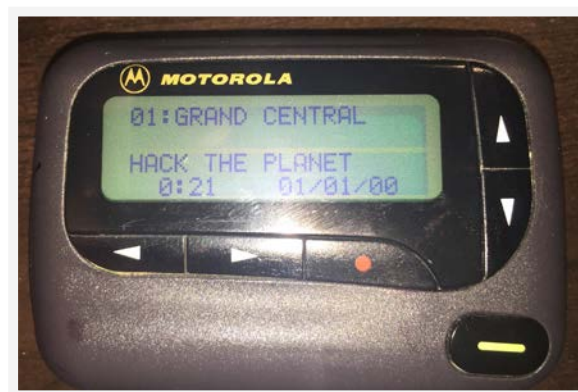


Figure 3. Test pager receiving test messages

Multiple tests were conducted to see the type of pager message formats sent and the cloning of these types. The messages were successfully sent and decoded by a couple of popular paging decoder software.

Based on the results, we were able to prove that messages can be sent to any pager with the same protocol, as long as the transmitting power of the radio and antenna can support the distance needed to successfully spoof messages. In this case, we tested the POCSAG (Post Office Code Standardization Advisory Group) protocol, which is one of just two protocols typically used by pagers, the other one being FLEX.

Our experiment proves that systems relying on pager technology can be easily compromised.

Possible Attack Scenarios

In summary, most of the notifications we observed from unencrypted pager messages were alarm/event notifications, diagnostics information, and status updates across the different sectors. These include information on leaks, deviations, sensor values, which can also be used to identify what ICS was used inside the facility and what SCADA devices are located in the plant.

Additionally, pages received via email-to-pager or SMS-to-pager gateways also gave out the email addresses of an organization's employees, including C-level officers. We were also able to view information such as employee names, delivery tracking numbers, project names and other code that may be meaningless to casual observers, but valuable for the well-versed.

As mentioned earlier, passive intelligence plays an incredibly large and underrated role in the crafting of attacks in each of the following hypothetical scenarios:

1. Knowledge of issues within the plant, like minor mechanical failures, etc. can be creatively used by determined attackers to craft social engineering attacks that will appear highly believable because of prior reconnaissance. Depending on the attacker's goal, one possible way for an attacker to get in is by scheduling a delivery that is timed with the scheduled arrival of a replacement part. Another way is to simply send an email containing a remote access Trojan to the maintenance department with relevant word tokens.
2. Information about a company's high-ranking employees, like names, email addresses and phone numbers, can be used to directly craft social engineering attacks.
3. While some information types are the same across more than one sector, the possible applications of a planned attack may be different depending on the nature of the sector involved. Less likely but also plausible, would be for highly skilled attackers to make use of the specific issues inside, for instance, a nuclear plant, to trigger some form of sabotage, after they have gained physical access.

Apart from the above scenarios, our findings also emphasize the importance of protecting privacy, not only from threat actors but also from outside parties in general, including competitors or other interested entities. Any company, especially the ones who are transmitting vital information through pagers, must be concerned once they realize that they are unknowingly transmitting vital information about their facility operations.

Conclusion

Our research on unencrypted pager messages led us to discover which sectors are still using pager technologies in this age of smartphones and the internet. We were surprised to see unencrypted pages coming from industrial sectors like nuclear power plants, substations, power generation plants, chemical plants, defense contractors, semiconductor and commercial manufacturers, and HVAC.

These unencrypted pager messages are a valuable source of passive intelligence, the gathering of information that is unintentionally leaked by networked or connected organizations. We also saw different readable types of pages including alarm or event notifications and diagnostic or status updates, names, email addresses, phone numbers, and other coded terminologies.

Taken together, threat actors can do heavy reconnaissance on targets by making sense of the acquired information through paging messages. Though we are not well-versed with the terms and information used in some of the sectors in our research, we were able to determine what the pages mean, including how attackers would make use of them in an elaborate targeted attack or how industry competitors would take advantage of such information.

The power generation sector is overseen by regulating bodies like the North American Electric Reliability Corporation (NERC). The NERC can impose significant fines on companies that violate critical infrastructure protection requirements, such as ensuring that communications are encrypted. Other similar regulations also exist for the chemical manufacturing sector.

For companies using pager technologies, we strongly recommend the following:

1. **Encrypt the communication.** Even a simple pre-shared key (PSK) encryption can raise the bar for the attacker. More sophisticated encryption methods mean more secure communication. Given the current development in embedded hardware, asymmetric encryption is possible without much impact on cost.
2. **Authenticate the source.** To prevent spoofed messages from being accepted by the system, there should be authentication designed in the firmware. When in doubt of weird information, make a phone call or meet with the person to verify the information.
3. **Audit possible leakage when using an email-to-pager gateway.**

References

1. Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams and Adam Hahn. (May 2015) *National Institute of Standards and Technology*. "Guide to Industrial Control Systems (ICS) Security." Last accessed on 30 August 2016, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>.
2. Wikipedia. (Unknown). *Wikimedia Foundation*. "Pager." Last accessed on 10 August 2016, <https://en.wikipedia.org/wiki/Pager>.
3. Gavin Rozzi. (20 February 2016). *The Lacey Reporter*. "Minor Damage After Oyster Creek Brush Fire." Last accessed on 6 September 2016, <https://laceyreporter.com/minor-damage-after-oyster-creek-brush-fire/>.
4. U.S. Nuclear Regulatory Commission. (Updated daily). *U.S. Nuclear Regulatory Commission*. "Current Event Notification Report." Last accessed on 6 September 2016. <http://www.nrc.gov/reading-rm/doc-collections/event-status/event/en.html>.
5. Tridium. (Unknown). *Tridium, Inc.* "Building Automation." Last accessed on 6 September 2016, <https://www.tridium.com/en/products-services/building-automation>.
6. Exele. (Unknown). *Exele Information Systems, Inc.* "TopView." Last accessed on 6 September 2016, <http://www.exele.com/software-products/topview/>.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.



Securing Your Journey
to the Cloud

www.trendmicro.com