“We don’t need no stinkin’ badges!”

Hacking electronic door access controllers

Shawn Merdinger
security researcher
DEFCON 18

Outline

- EDAC technology
  - Trends, landscape
  - Vendors
  - Architecture
- EDAC real-world analysis
  - S2 Security NetBox
    - Research, exposure, vulnerabilities, attacks
    - Countermeasures & recommendations

Learning outcomes

- Awareness of security issues in EDAC systems
- Major players, vendors, resellers
- Pen-testing knowledge
- Research and testing methods

Choice quotations

“When hackers put viruses on your home computer it's a nuisance; when they unlock doors at your facility it's a nightmare.”

John L. Moss, S2 Security CEO
STAD, Volume14, Issue 1. 1 January, 2004

Q . About security of buildings around town….what was your response?

ATTY GEN. RENO: “Let's do something about it.”

Q. Is this a good thing that has happened?

ATTY GEN. RENO: I think any time you expose vulnerabilities, it's a good thing.

Department of Justice
Weekly Media Briefing, 25 May 2000

EDAC Technology Overview

- Trend is towards IP from proprietary solution
  - Convergence of IP, Video
  - Adding other building systems (HVAC, elevators, alarms)
  - Cost savings, integration, increased capabilities
- Most controllers use embedded Linux
- Wide range of vendors in EDAC space

S2 Security

Honeywell

HID Global Vertx

Ingersoll-Rand

Bosch Security

Reach Systems

Cisco Systems (Richards Zeta)

Brivo

DSX Access

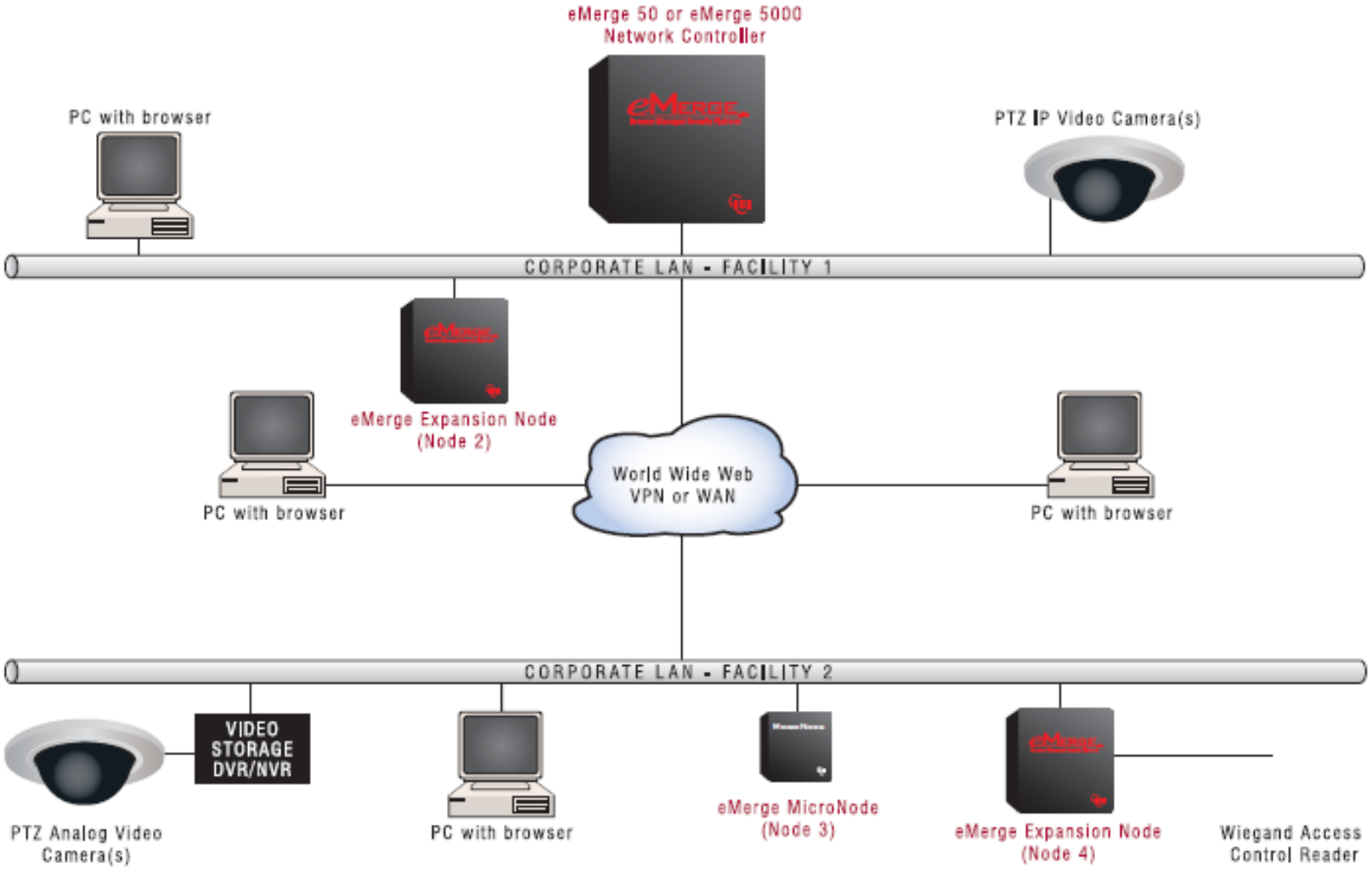
RS2 Technologies

Synergistics

EDAC Deployment

- Often you'll see
  - Managed by building facilities people
  - Stuck in a closet and forgotten
  - Long lifecycles of 5-10 years
- Distanced from IT Security
  - Physical security is not your domain. It's ours.
  - Patching, upgrades, maintenance. What? Huh?
  - Policies regarding passwords, logging don't apply
  - 3rd party local service contractor adds doors, hardware configuration

EDAC Architecture



S2 Security NetBox

- Built by S2 Security
- 9000+ systems installed worldwide
  - Schools, hospitals, businesses, LEA facilities, etc.
- Same box is sold under multiple brand names
  - Built by S2 Security
    - NetBox
  - Distributed by Linear
    - eMerge 50 & 5000
  - Resellers' re-branding
    - Sonitrol eAccess

eMERGE™ 5000
Browser Managed Security Platform

SONITROL®
eAccess
Powered by IEI

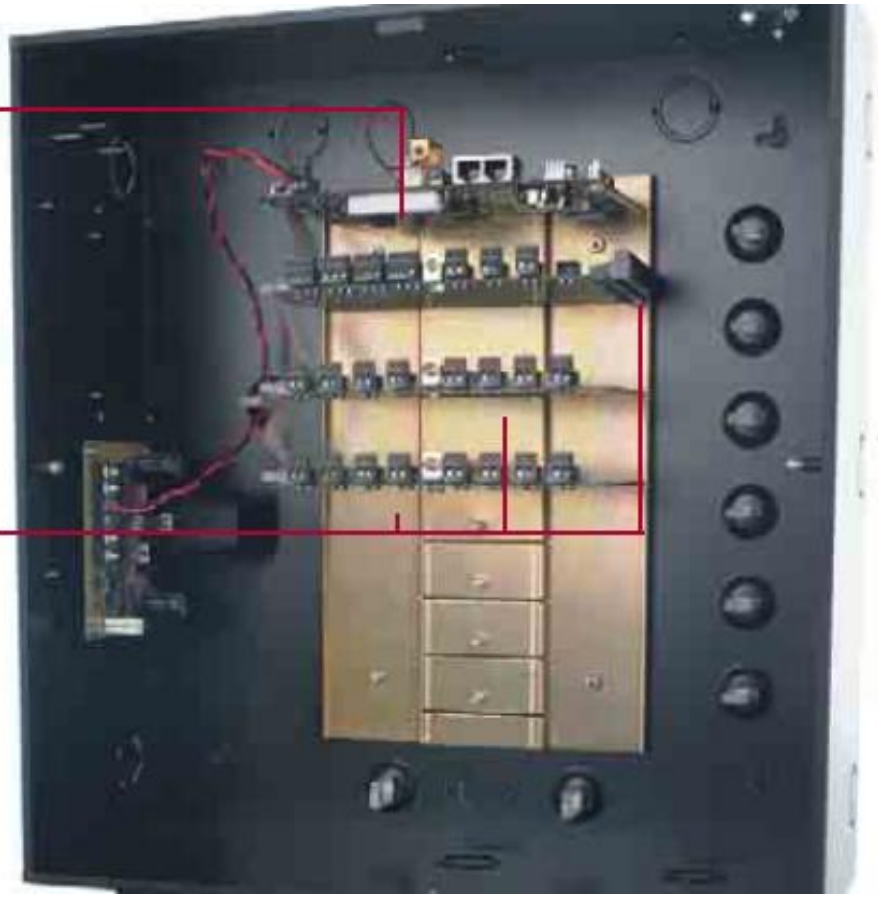
S2 Security NetBox

Network Controller

Serving as the central control mechanism of the system, the Network Controller takes the place of a PC-based server on older style systems. It runs a full version of Linux and contains a web server, ODBC-compliant PostgreSQL database server. All software is embedded within the Intel processor. Users access the software by using a web browser anywhere on the network, or anywhere the Internet is available.

Application Modules

Allow you to build a custom security panel containing exactly the components you want, where you need them. Up to 7 application modules can be mounted within a Node. Application modules include: Access Control Modules with Wiegand protocol card reader inputs, Supervised Input Modules, Relay Output Modules and Temperature Monitoring Modules.



S2 Security: Reading up

- Preparation and information gathering
  - S2 Security case studies, press releases
  - "The Google"
  - Lexis-Nexis Academic Universe, ABI-Inform, etc.

- Example: able to determine from http://tinyurl.com/s2mysql
  - Samba client
  - MySQL, MyISAM
  - Lineo Linux distribution (just like Zarus!)
  - Processor is ARM Core IXP 425 chip @ 533 MHz
  - Only 15 months from design to 1st customer shipping
  - "S2 did not have much prior experience with open source"
  - "MySQL is used to store everything from reports, user information, customized features, facility diagrams, and more"

NetBox Components

- HTTP
- MySQL / Postgres
- NmComm
- FTP/Telnet
- Features!

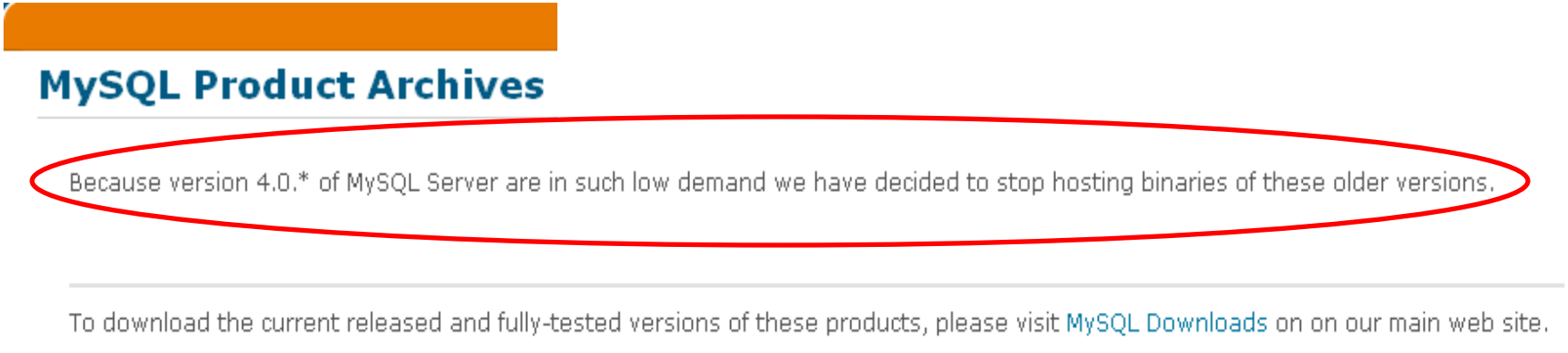
NetBox Component: HTTP Server

- GoAhead Webserver TCP/80
- Poor choice
  - Sixteen CVEs
    - CVE-2003-1568, CVE-2002-2431, CVE-2002-2430, CVE-2002-2429, CVE-2002-2428, etc.
    - No vendor response
      - Typical example in CVE-2002-1951
        - Vendor response:
          GoAhead….contacted on three different occasions during the last three months but supplied no meaningful response.

"Data security is a challenge, and unfortunately, not everyone has risen to it.“
John L. Moss, S2 Security CEO

NetBox Component: MySQL

- MySQL server listening on 3306
- Outdated SQL
  - Version 2.X uses MySQL version 4.0
    - 3.X uses Postgres
  - Just how old is MySQL 4.0?
    - WTF? End of DOWNLOAD?



NetBox Component: NmComm

- Service listening on TCP/7362
- Performs multicast discovery of nodes
- Daemon coded by S2 Security
- Patent issued 15 December, 2009
  - "System and method to configure a network node"
    - http://tinyurl.com/s2patent

"Gentlemen, start your fuzzers!"

NetBox Component: FTP & telnet

- Cleartext protocols for a security device
  - Telnet to manage
  - FTP for DB backups
- Poor security-oriented documentation

Network Administrator tasks:

1. On the FTP Server create a user name, password, and directory for the security system FTP Backups.

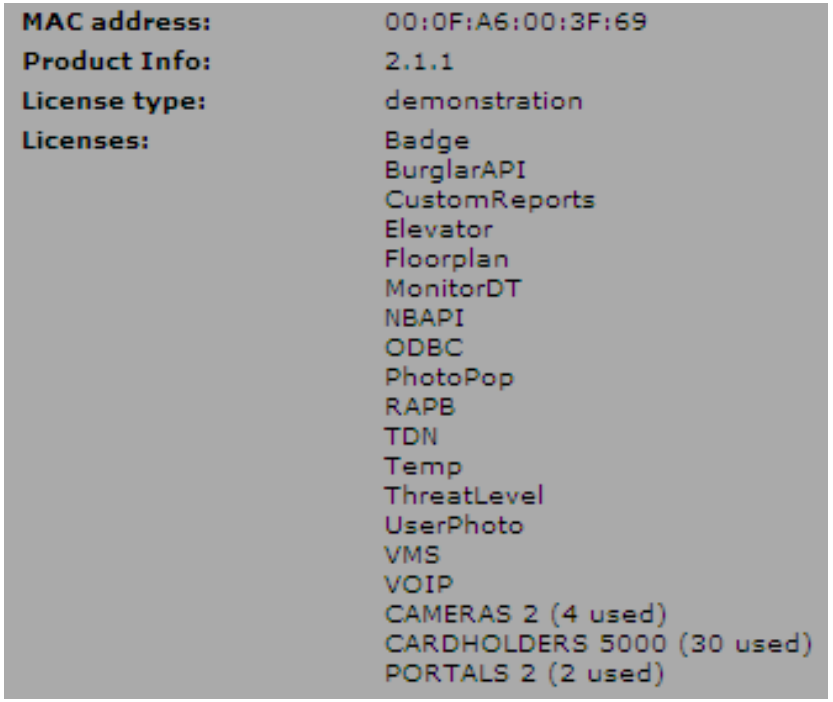
   NOTE: A password is optional. The backup directory must be created at the root level of the FTP server.

"We see some vendors fitting their serial devices with Telnet adapters, which simply sit on the network transmitting unsecured serial data."

John L. Moss, S2 Security CEO

NetBox Components: Features!

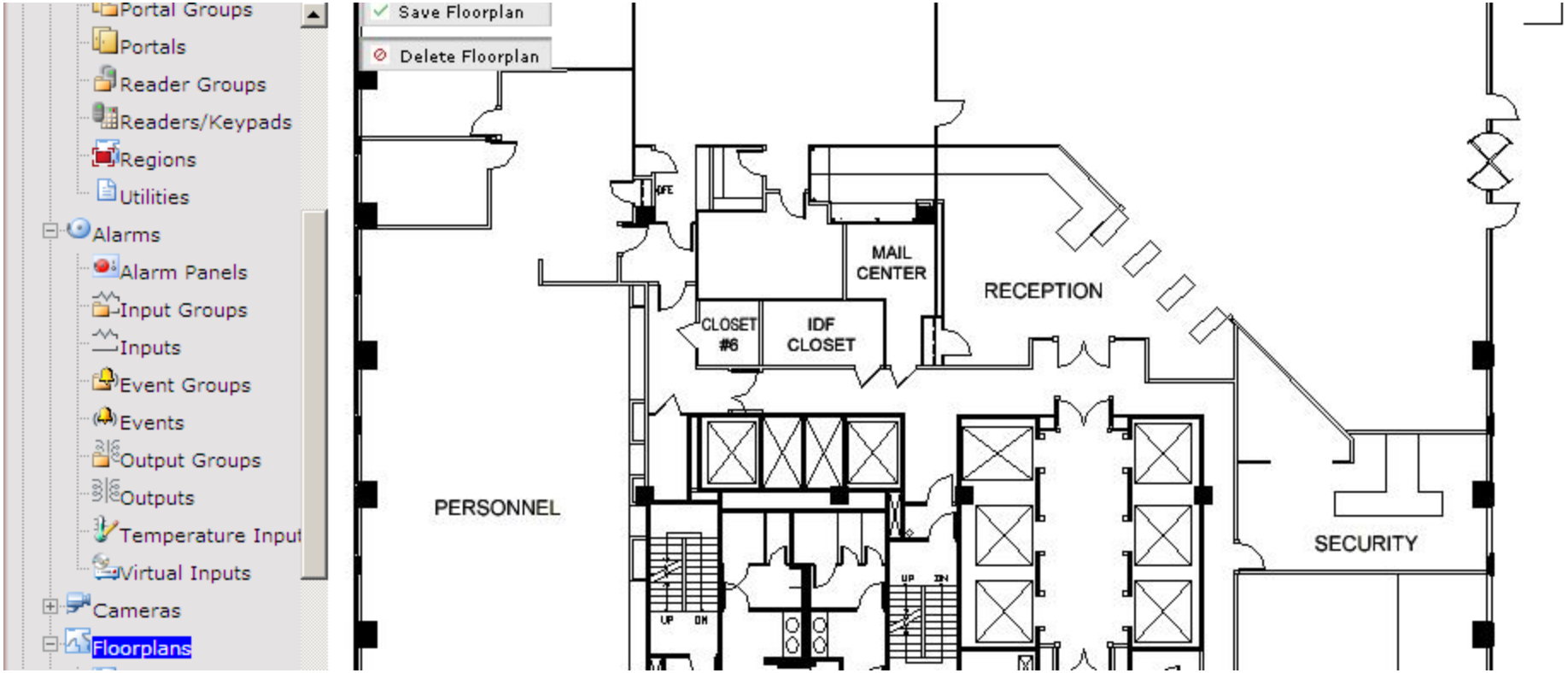
- Lots of extras and licenses options
  - Elevators, HVAC, Burglar
  - VoIP
- Increases complexity
- Expands attack surface
  - Daemons
  - Libraries



MAC address:	00:0F:A6:00:3F:69
Product Info:	2.1.1
License type:	demonstration
Licenses:	Badge BurglarAPI CustomReports Elevator Floorplan MonitorDT NBAPI ODBC PhotoPop RAPB TDN Temp ThreatLevel UserPhoto VMS VOIP CAMERAS 2 (4 used) CARDHOLDERS 5000 (30 used) PORTALS 2 (2 used)

NetBox Components: Features!

- View floorplans



NetBox unauthenticated reset

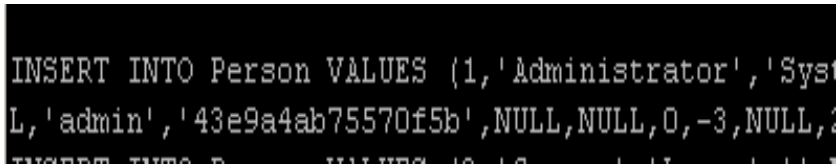
- VU#571629
- Remote, unauthenticated factory reset via crafted URL

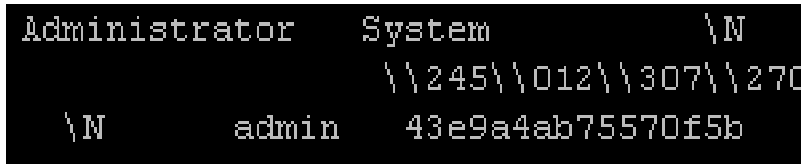
NetBox Unauth Access to Backup

- VU#228737
  - Unauth attacker can dload DB backups
  - Nightly DB backup is hardcoded CRONJOB
    - File name is “full_YYYYMMDD_HHMMSS.1.dar”
    - Predictable naming convention with timestamp
    - Uncompress the.dar format
      - Backup DB is in “var/db/s2/tmp/backup/all.dmp”
  - Attacker gets backup DB = Game Over
    - Entire system data in DB!

NetBox Unauth Access to Backup

- Extraction of administrator MySQL_64bit hash





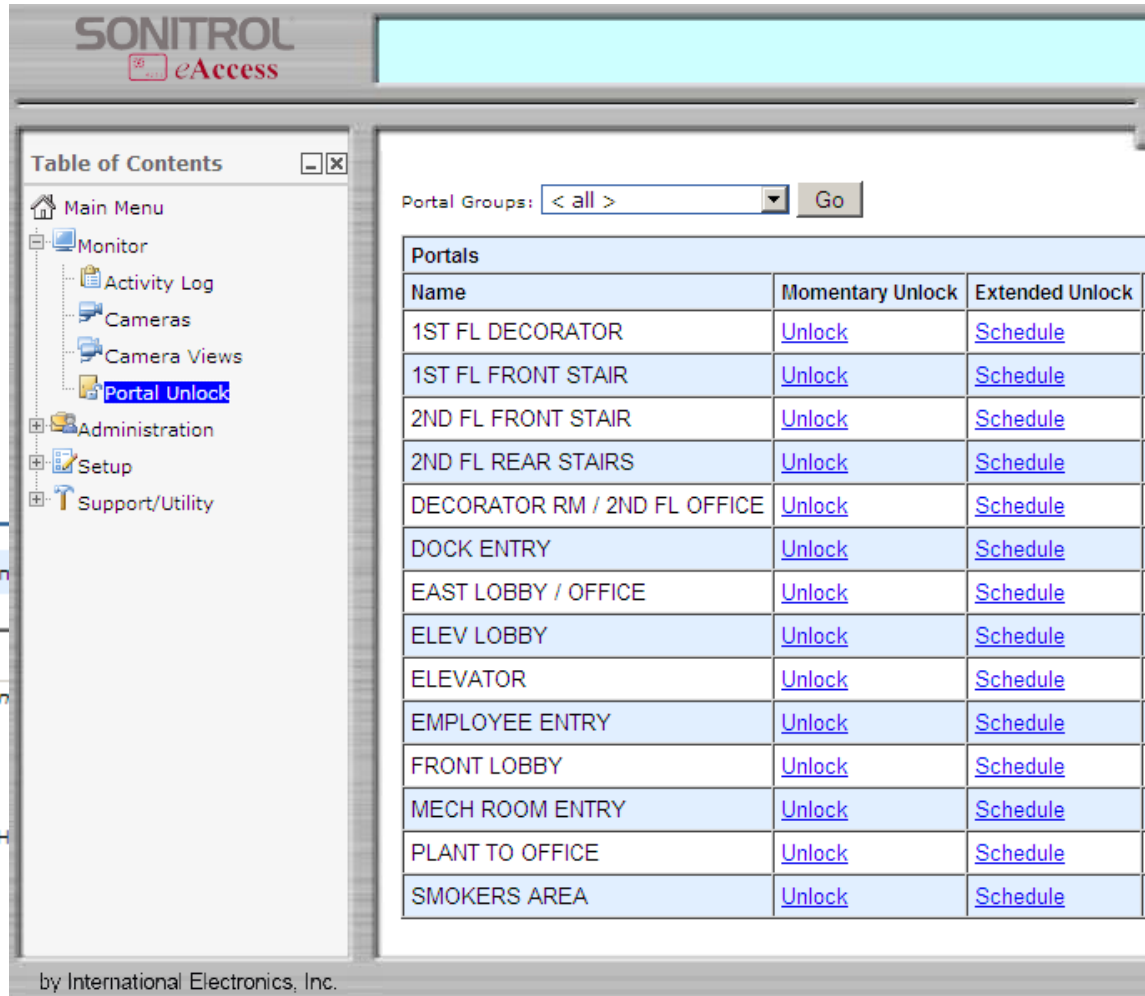
- Affects NetBox 2.X (mysql) and 3.X (postgres)
- Hash is trivial to crack

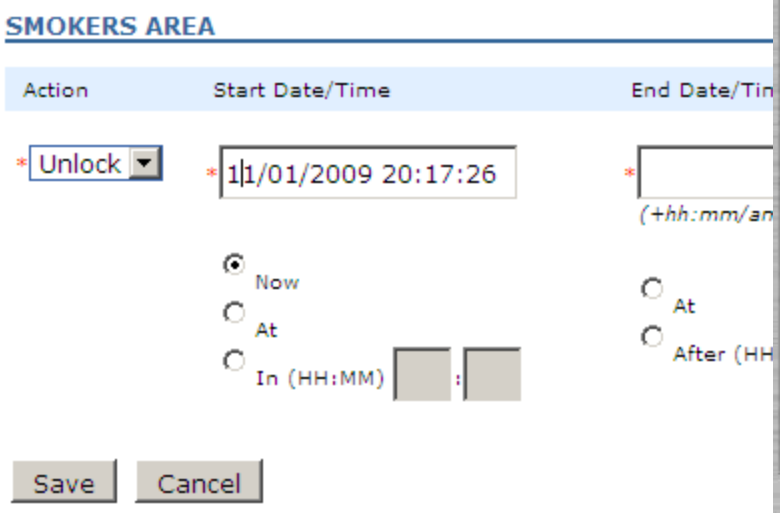
id	type	hash	pass	hex
339	MySQL_64bit	43e9a4ab75570f5b	admin	61646D696E
16017513	MySQL_64bit	43e9a4ab75570f5b	admin	2061646D696E
16115746	MySQL_64bit	43e9a4ab75570f5b	admin	2061646D696E20
16168230	MySQL_64bit	43e9a4ab75570f5b	admin	61646D696E20

- Attacker now has admin access

NetBox Pwnage: Doors

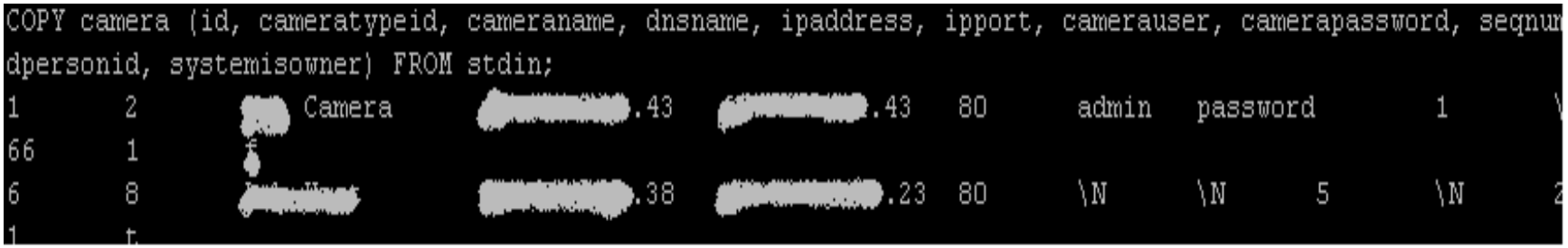
- Open any door
  - Right now
  - Or schedule





NetBox Pwnage: Cameras

- Backup file contains IP camera information
  - Name, IP address, admin username and password



- NetBox 2.X and 3.X systems vulnerable
- Attacker now owns IP cameras

"Most hackers don't care about watching your lobby. If they gain access to the network, they're going to go after financial data and trade secrets."

Justin Lott, Bosch security marketing

NetBox Pwnage: DVRs

- User/Pass to DVRs in backup DB
- Poor setup guides for DVRs
  - Recommends keeping default user/pass
    - On-Net Surveillance Systems Network Video Recorder document

Complete the NetDVMS Setup

1. If you have not already done so create a User and Password with the **Image Server Administrator**.
2. Click the **User Setup** button and create a user. The eMerge defaults to the user name "IEleMerge" and the password "eMerge." We recommend that you use these defaults.

NetBox Fingerprinting

- Remote Identification
  - MAC OID registered to S2 Security

00-0F-A6	(hex)	**S2 Security** Corporation
000FA6	(base 16)	**S2 Security** Corporation 6 Abbott Road Wellesley MA 02481 UNITED STATES

  - Nmap service fingerprint submitted (nmap 5.20)

```
root@vc157:~/nmap-5.20# cat nmap-service-probes |grep -i sonitrol
match http m|^HTTP/1\.0 302 Redirect\r\nServer: GoAhead-Webs\r\n.*Location: http://([\w._
-]+)/login\.asp\r\n|s p/GoAhead-Webs/ i/Sonitrol building access control system http conf
ig/ h/$1/
```

Recommendations: Vendor

- Vendor
  - Conduct security evaluations on your products
  - Provide secure deployment guides
  - Tighten-up 3rd party integration
  - Improve
    - Logging
      - More details: changes, auditing, debug levels
      - Ability to send to log server
    - HTTP
      - Use a “better” HTTP daemon
      - Enable HTTPS by default
      - Modify banners, reduce footprint, etc.
    - FTP
      - Change to SFTP
    - Telnet
      - Change to SSH

Recommendations: Customers

- Demand better security!
  - From vendor, reseller, and service contractor
  - Expect fixes and patches
- Manage your EDAC like any other IT system
  - Patching, change management, security reviews
- Technical
  - Isolate eMerge system components
    - VLANs, MAC auth, VPN, restrict IP, etc.

Questions?

- Contact
  - Follow-up questions
  - Security evaluations

scm@hush.com

http://www.linkedin.com/in/shawnmerdinger