“We don’t need no stinkin’ badges!”

Hacking electronic door access controllers

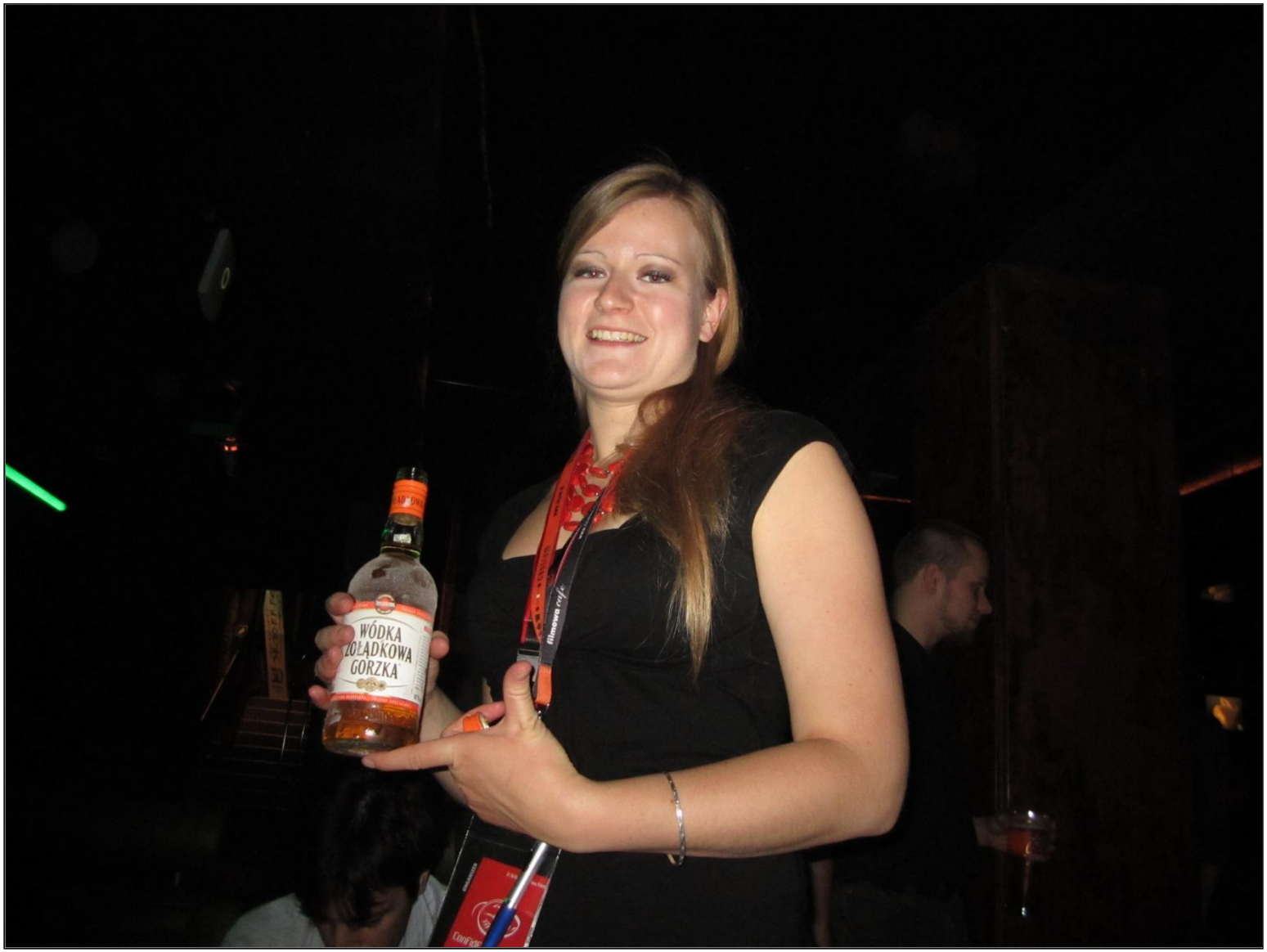
Shawn Merdinger

CONfidence, Krakow, Poland, 2010

Thoughts so far.....

- Fantastic Conference!
- Nice speaker line-up
- Great location – Krakow rocks. Period.
- Speakers very well taken care of at CONfidence
  - Airport meet, hotel, dinner, party
- Special 'Thank You' to CONfidence Staff
  - Anna, Andrej, Arthur

Welcome to Krakow: Drink Tough or Go Home ;)



Outline

- EDAC (Electronic Door Access Controller)
- EDAC technology
  - Trends, landscape
  - Vendors
  - Architecture
- EDAC real-world analysis
  - S2 Security NetBox
    - Research, exposure, vulnerabilities, attacks
    - Countermeasures & recommendations
    - Next steps

Learning Objectives & Outcomes

- Awareness of security issues in EDAC systems
- Trends, major players in this space
- Marketing vs. Reality
- Pen-testing knowledge
- Tangible first stage research and testing methods
- Final paper forthcoming ☺
  - A few more bugs in pipeline with CERT/CC

A Few 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, Volume 14, 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.

US Department of Justice
Weekly Media Briefing, 25 May 2000

EDAC Technology Overview

- Trend is towards IP from proprietary solution
  - Convergence of IP, Video, personnel management
  - Cost savings, integration, increased capabilities
    - Adding building systems (HVAC, elevators, alarms)
    - Power-over-Ethernet door strike = big cost savings
- Most controllers seem to use embedded Linux, or VxWorks
- Wide range of vendors in EDAC space

S2 Security (not picking on them, they're just first)

Honeywell
HID Global Vertx
Ingersoll-Rand
Bosch Security
Reach Systems
Lenel

Cisco Systems (recently Richards Zeta)
Brivo
DSX Access
RS2 Technologies
Synergistics
HID
Etc., Etc.

EDAC Deployment

- Often you'll see
  - Managed by building facilities type of people
  - Stuck in a wiring closet and forgotten
  - Long lifecycles of 5-10 years
- Distanced from organization's IT Security
  - "Physical security is not your domain. It's ours."
  - Patching, upgrades, maintenance? Uhhh, what?
  - Policies regarding passwords, logging?
  - 3rd party Involvement
    - local service contractor adds doors, hardware configuration
    - Management outsourced, not in-house

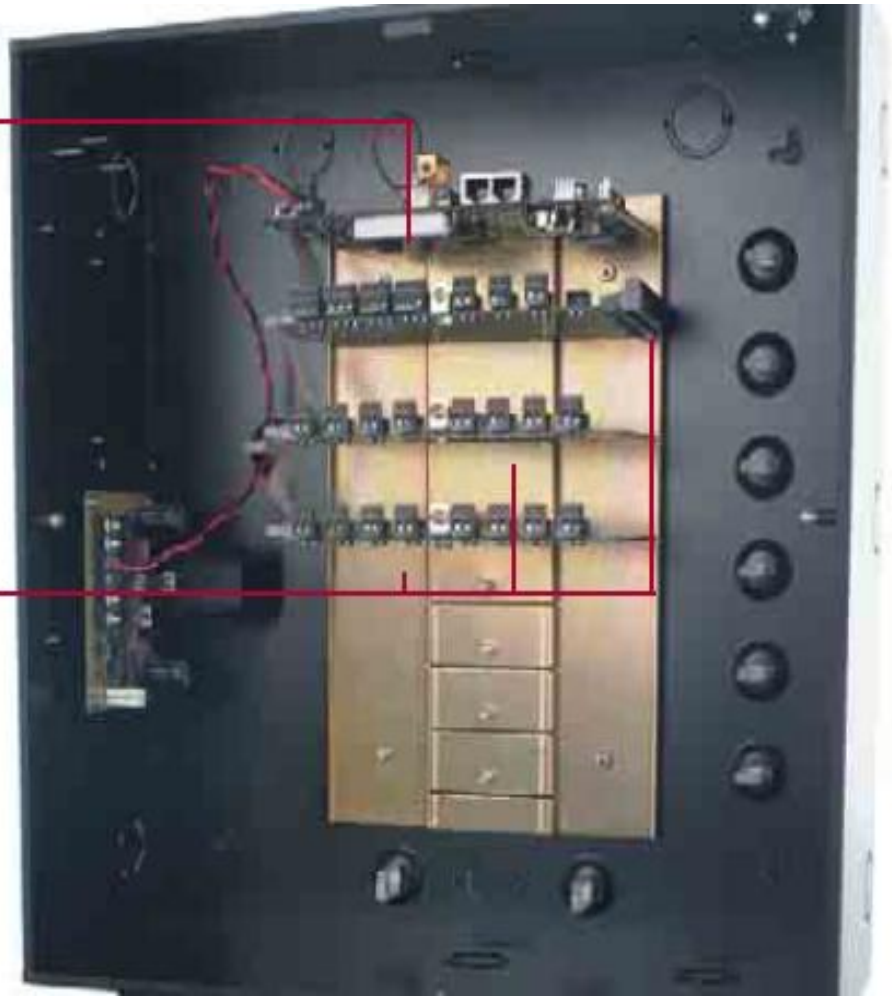
S2 Security NetBox -- “The Brain”

Network Controller

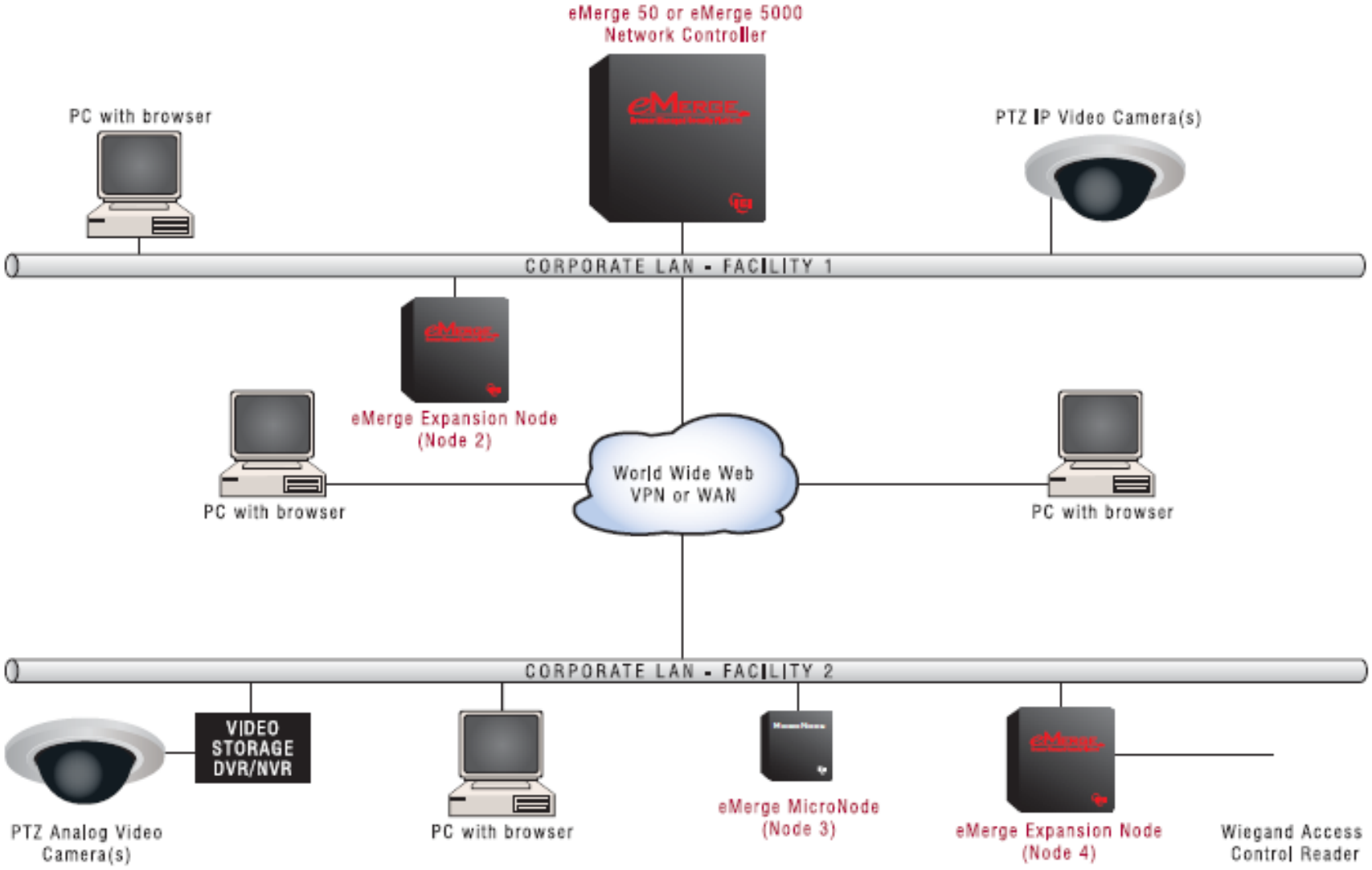
Serving as the central control mechanism of the system, the Network Controller takes the place of a PC-based server on older style systems. It runs a full version of Linux and contains a web server, ODBC-compliant PostgreSQL database server. All software is embedded within the Intel processor. Users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



EDAC Architecture



S2 Security NetBox

- 9000+ systems installed worldwide
  - Schools, hospitals, businesses, LEA (police stations), etc.
- Same box is sold under multiple brand names
  - Built by S2 Security
    - NetBox
  - Distributed by Linear
    - eMerge 50 & 5000
  - Re-re-branded
    - Sonitrol eAccess

eMERGE™ 5000
Browser Managed Security Platform

SONITROL®
eAccess
Powered by IEI

S2 Security: background info

- Preparation and information gathering
  - S2 Security case studies, press releases
  - Google is not good enough
  - Also use commercial databases like Lexis-Nexis, ABI-Inform
- From simple research I'm able to determine
  http://tinyurl.com/s2mysql
  - Samba client, MySQL
  - Lineo Linux distribution (just like Zarus handheld!)
  - **Only 15 months** from design to 1st customer ship
  - "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"

S2 Security: Marketing Statements

- "Data security features built into the software and hardware assure that it is safe to deploy systems across any network, even the public Internet"
- "Remote locations are easily handled"
- **"S2 NetBox can operate for years without maintenance of any kind"**

NetBox Component Review

- HTTP
- MySQL / Postgres
- NmComm
- FTP/Telnet
- Yes, it really is a “Feature”

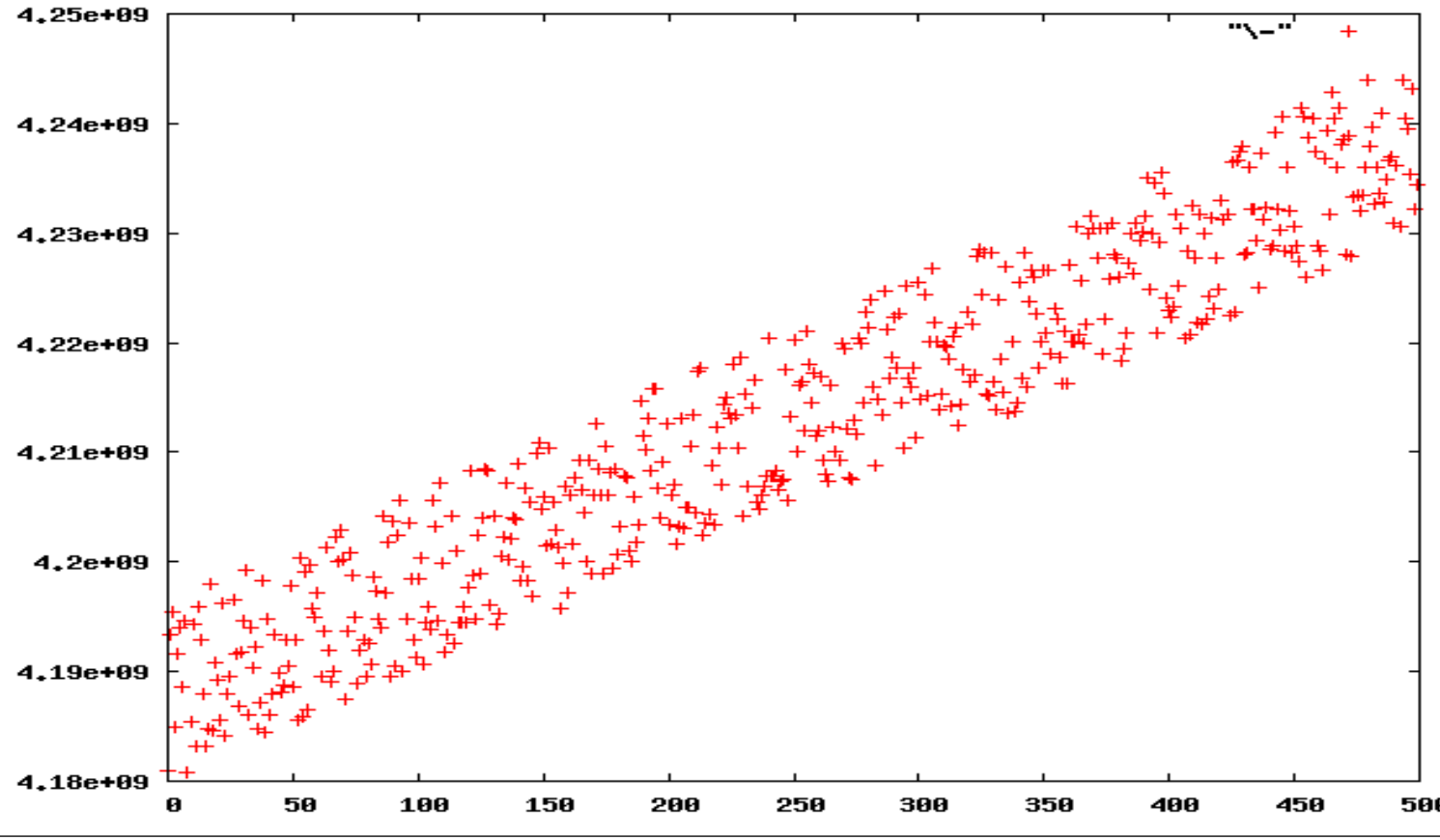
NetBox Component: HTTP Server

- GoAhead Webserver TCP/80
- Bad choice for a webserver!
  - +16 CVEs
    - CVE-2003-1568, CVE-2002-2431, CVE-2002-2430, CVE-2002-2429, CVE-2002-2428, etc.
    - No vendor response, no statements, no obvious fixes
    - Free and opensource – but who maintains it?
    - Typical example: CVE-2002-1951
      - "GoAhead….contacted on three different occasions during the last three months but supplied no meaningful response."

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

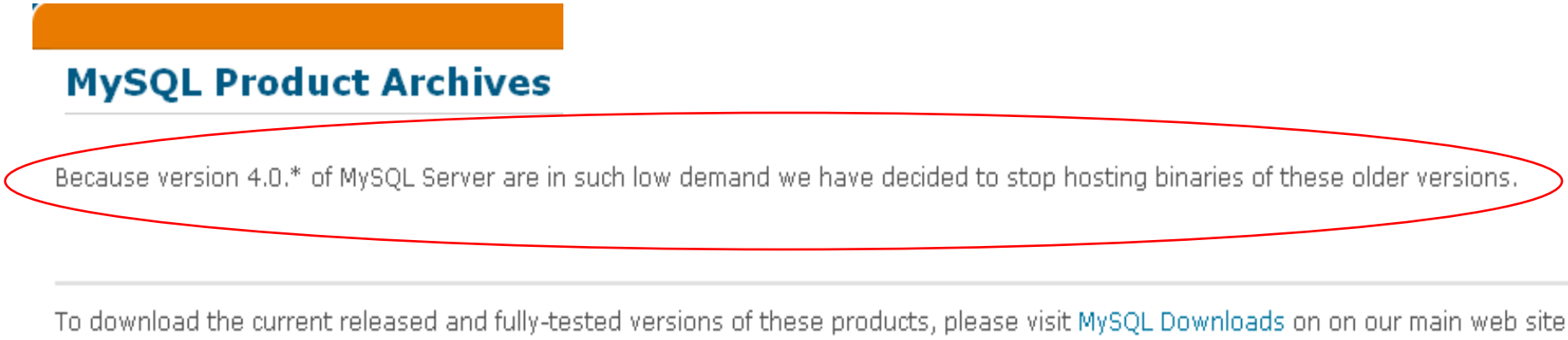
NetBox Component: HTTP Server

- HTTP TCP SYN Initial Sequence Number plots not random
- See Cisco STAT paper **http://tinyurl.com/stackhow2**



NetBox Component: MySQL

- MySQL server listening on TCP/3306
- Outdated SQL
  - Version 2.X uses MySQL version 4.0
    - 3.X uses Postgres
  - MySQL 4.0?
    - Gee, that sounds kind of old…
    - WTF? End of DOWNLOAD? OMG!



NetBox Component: nmComm

- Custom service listening on TCP/7362
- Performs multicast discovery of HID nodes
- Daemon coded by S2 Security
- US Patent issued 15 December, 2009
  - "System and method to configure a network node"
    - http://tinyurl.com/s2patent
    - Details specs, almost like a RFC

"Gentlemen, start your fuzzers!"

NetBox Component: FTP & Telnet

- Cleartext protocols for a critical security device?
  - HTTP by default versus HTTPS
  - Telnet to manage via command-line
  - FTP for device backups
- Poor security-oriented documentation example below

Network Administrator tasks:

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

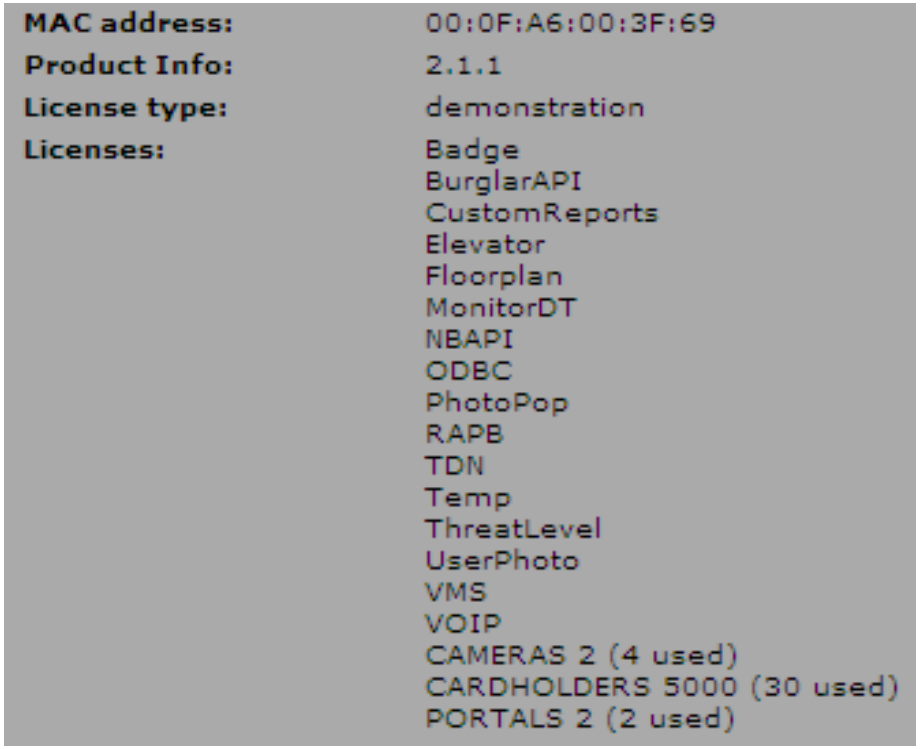
   NOTE: A password is optional. The backup directory must be created at the root level of the FTP server.

"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

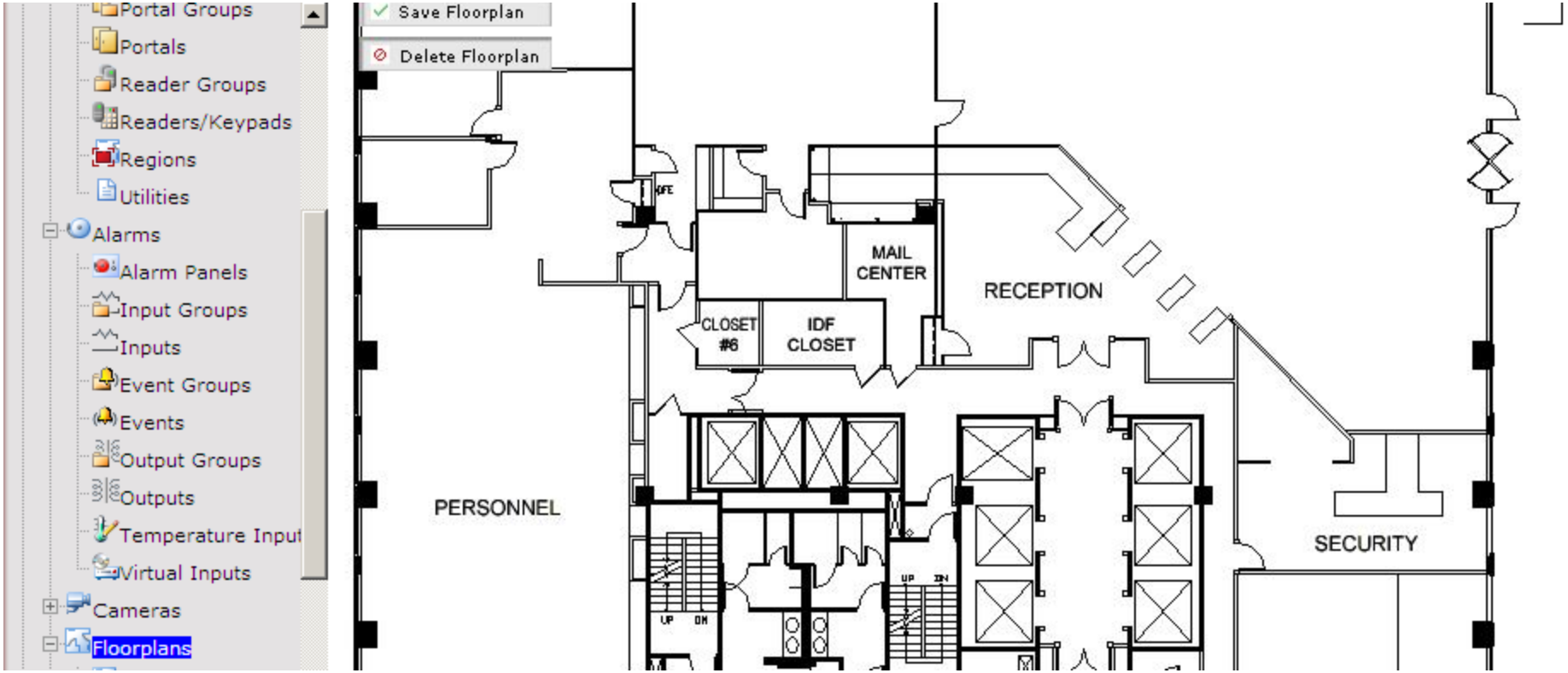
NetBox Components: Features!

- Many extras and license options
  - IP cameras, DVRs
  - Elevators, HVAC, Burglar API
  - VoIP
- Result of feature-creep?
  - Increases complexity
  - More components
  - Expands attack surface



NetBox Components: Building Maps

- View building floorplans – just like in “24”



S2 NetBox Unauthenticated Factory Reset

- US-CERT/CC VU#571629 (public 2010-01-04)
  - Crafted URL allows factory reset
  - Impact is fresh "out-of-box" total wipe of data
- Vendor "communications" poor
  - I was punted between companies kind of games…
    - "Talk to Linear"
    - "Talk to S2"
  - CERT/CC played an invaluable role
    - Gr33tz to Art Manion & Will Dormann
  - 3rd hit on Google search for S2 Security

S2 NetBox Unauthenticated Backup Access

- US-CERT VU#228737 (disclosure in process)
  - Attacker can download DB backups
  - Nightly DB backup is hardcoded CRON
    - 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/"
  - Attacker 0wns backup DB
    - Remember the entire system is in DB!
    - Let's see what we can find….

S2 NetBox: Admin Credentials

- Extraction of administrator MySQL_64bit hash

```
INSERT INTO Person VALUES (1,'Administrator','Sys
L,'admin','43e9a4ab75570f5b',NULL,NULL,0,-3,NULL,
```

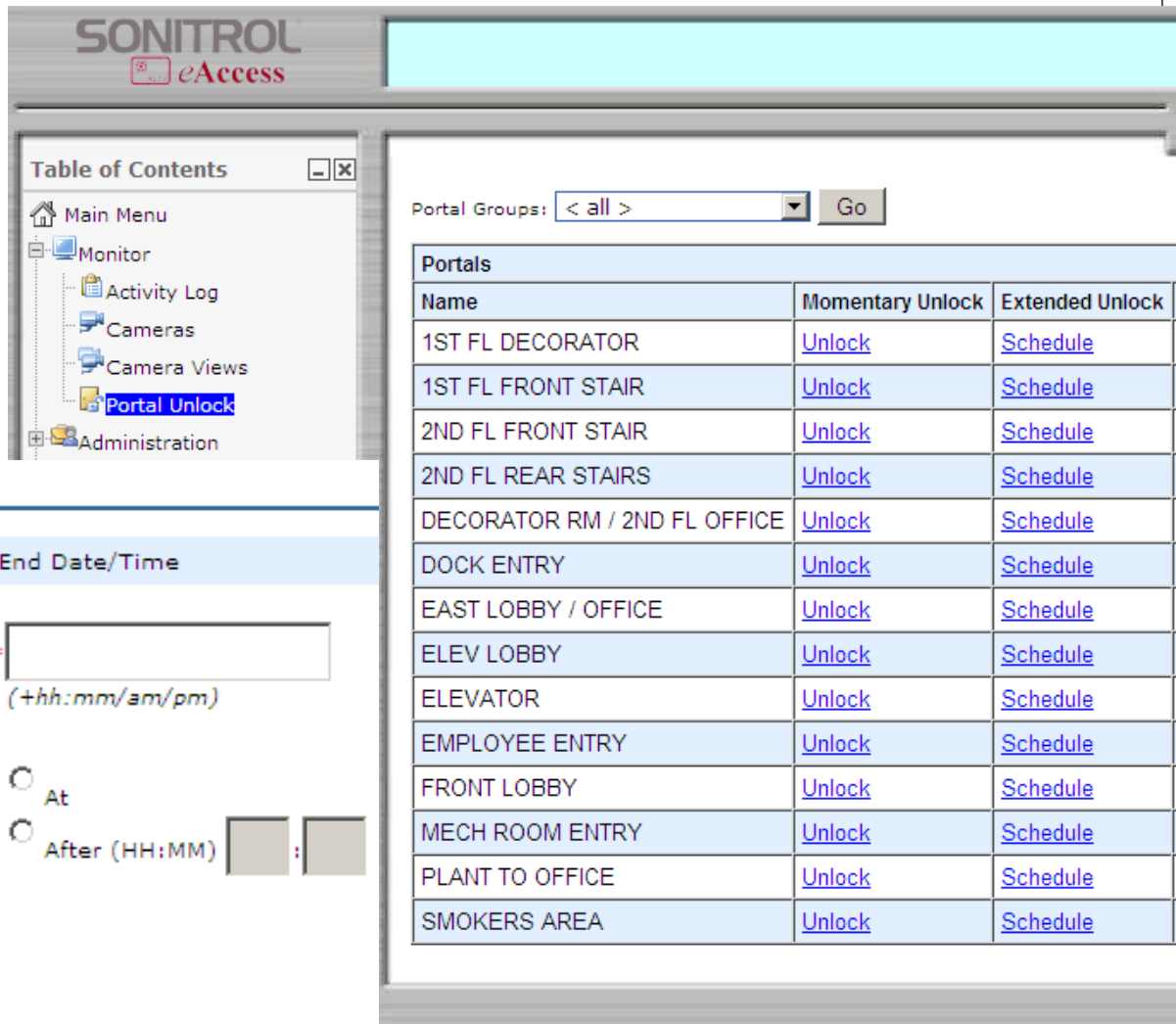
```
Administrator   System          \N
                \\245\\012\\307\\270
  \N      admin   43e9a4ab75570f5b
```

- 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

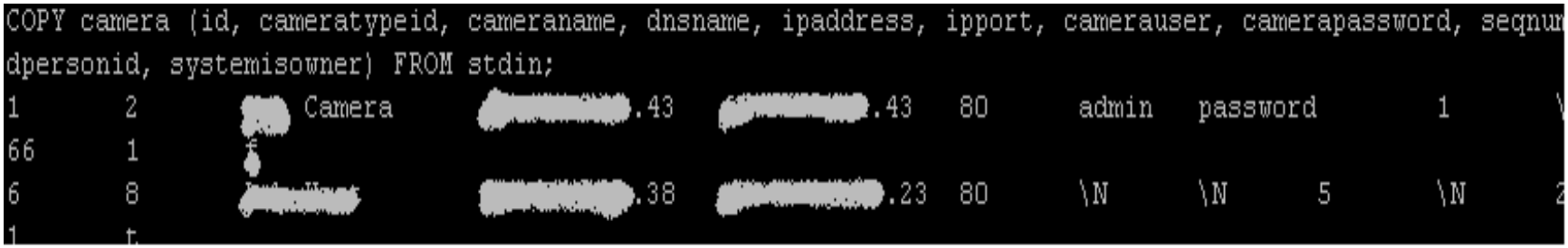
S2 NetBox Pwn3d: “Open Sesame”

- Open any door **right now**
  - Or schedule…
- Privacy concerns
  - Who smokes?
  - Productivity?



S2 NetBox Pwn3d: Control IP Cameras

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



- S2 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

S2 NetBox Pwn3d: Control DVRs

- User/Pass to DVRs in backup DB
- Poor setup guides for DVRs
  - Recommends keeping default user/pass
- 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.

S2 NetBox: Remote Fingerprinting

- Trivial remote identification of MAC
  - 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 to 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/
```

“Shodan Effect” & Fingerprinting

- Me: “Lots of your boxes are on the InterWebs…”
- S2 Security:
  - “Should be behind a firewall, accessible by VPN only”
  - “Typically deep within the corporate network”
- Vendor assumes that S2 NetBoxs are hard to find
- Enter Shodan “Computer Search Engine”
  - Like Google/Rainbow Tables for systems on the Internet
- Crafted search from HTTP fingerprint
  - http://www.shodanhq.com/?q=GoAhead-Webs+login.asp+no-cache%2Cmust-revalidate
  - **+185 S2 NetBox systems on the Internet right now**
- Not much vendor conversation after this…

SHODAN
Computer Search Engine

Search Directory | Help | Blog | Login | Sign Up

GoAhead-Webs login.asp no-cache,must-revalidate

Search

Options

Results **1** - **10** of about **146** for **GoAhead-Webs login.asp no-cache,must-revalidate**

» Top countries matching your search

United States	133
Canada	3
Italy	1

98.237.59.21
Linux recent 2.4
Added on 15.03.2010

c-98-237-59-21.hsd1.pa.comcast.net

```
HTTP/1.0 302 Redirect
Server: GoAhead-Webs
Date: Mon Mar 15 14:37:29 2010
Pragma: no-cache
Cache-Control: no-cache,must-revalidate
Content-Type: text/html
Location: http://98.237.59.21/login.asp
```

68.153.148.20
Linux recent 2.4
Added on 11.03.2010

adsl-068-153-148-020.sip.asm.bellsouth.net

```
HTTP/1.0 302 Redirect
Server: GoAhead-Webs
Date: Thu Mar 11 12:23:46 2010
Pragma: no-cache
Cache-Control: no-cache,must-revalidate
Content-Type: text/html
```

Shodan Effect: Other EDAC Systems?

- iGuard biometric fingerprint reader

Recommendations: Vendor & Reseller

- Conduct security evaluations on your products
- Prepare to work with & not against security researchers
- Provide secure deployment guides, best practices
- Tighten 3rd party device integration
- Improve
  - More log details: changes, auditing
    - VIP for investigations (Yale murder)
  - HTTP
    - Better daemon, HTTPS by default
    - Modify banners, reduce fingerprint
  - FTP / Telnet – no place in security device
    - SSH, SFTP

Recommendations: Customers

- Demand better security from your "security" products
  - From vendor, reseller, and service contractor
  - Expect fixes and patches
- Manage your EDAC like a super critical IT system
  - Patching, change management, security reviews
  - Isolate all eMerge system components
    - VLANs, MAC auth, VPN, restrict IP, etc.

Thank You!

- Questions?
- Contact
  - scm@hush.com
  - www.linkedin.com/in/shawnmerdinger