Some Considerations for Mitigating IoT Risk in Institutions
HELUG

June 2019

Chuck Benson
Director of IoT Risk Mitigation Strategy
University of Washington

Some background

Why IT Matters to Higher Education
EDUCAUSEreview

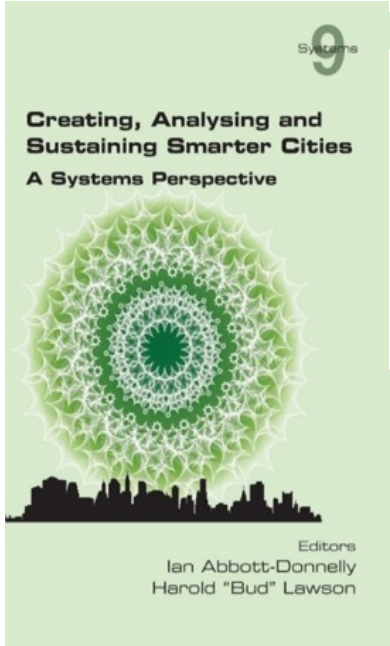
CAMPUS TECHNOLOGY

'Smart' Campuses Invest in the Internet of Things

Forward-thinking CIOs are exploring the potential of IoT technologies in higher education and heading off challenges along the way.

By David Raths | 08/24/17

At Sun Devil Stadium on the campus of Arizona State University in Tempe, sensors connected to the WiFi and cellular network collect temperature, humidity and noise data for use by facilities staff. As part of a longstanding cheering contest, the noise data analysis identifies the section of the stadium that is making the most noise and puts the results on a big screen. Sensors can identify if a faucet anywhere in the stadium is left running after a football game is over, to help cut water usage. ASU also is exploring providing information through a mobile app on the availability of parking and wait time estimations for concession lines and restrooms.



Chpt 4 – "IoT Systems – Systems Seams & Systems Socialization"

U.S.-CHINA
ECONOMIC and SECURITY REVIEW COMMISSION

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

Increasing the Manageability & Measurability of IoT/Cyberphysical System Implementations in Institutions & Cities

Northwest Institute of Advanced Computing
Pacific Northwest National Labs Workshop
University of Washington

Chuck Benson
June 2017

Long Tail Risk

Internet of Things systems risk management

HOME DOWNLOADS ABOUT

Creating IoT Systems Manageability – A Risk-Managed Set of Networked Things

ystems ROI and to ensure non-degradation of an institution's existing cyber-risk
ems must be manageable. In turn, in order to build IoT Systems manageability,
need to manage their IoT Systems risk with non- traditional approaches that
ng IoT endpoints (the 'things' in IoT) to risk categories that can be independent

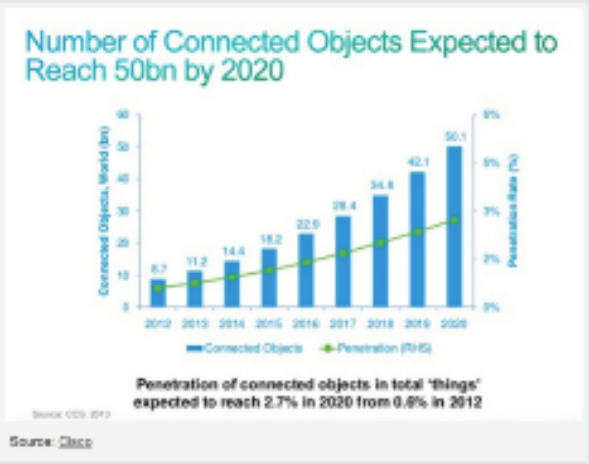
http://longtailrisk.com

Taylor & Francis Group
an informa business

Book Release July 2019: Managing IoT Systems for Institutions & Cities

IoT Systems are different from traditional enterprise IT -- 6 differences

1. Scale
   a. Raw number of networked, computing devices
   b. Rate of growth of number of these devices

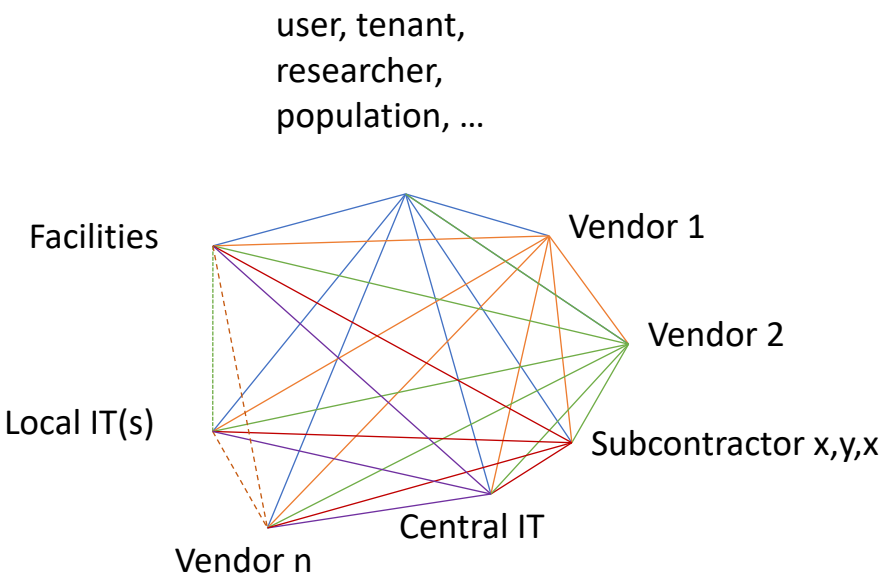


2. Variation Many types of devices. Difficult to categorize & classify
   a. Many types of devices – non-obvious risk buckets
   b. Many types of components within devices

3. Lack of language to discuss these systems with institutional leadership
   a. Both ROI & Cybersecurity / cyber risk

IoT Systems are different from traditional enterprise IT -- 6 differences

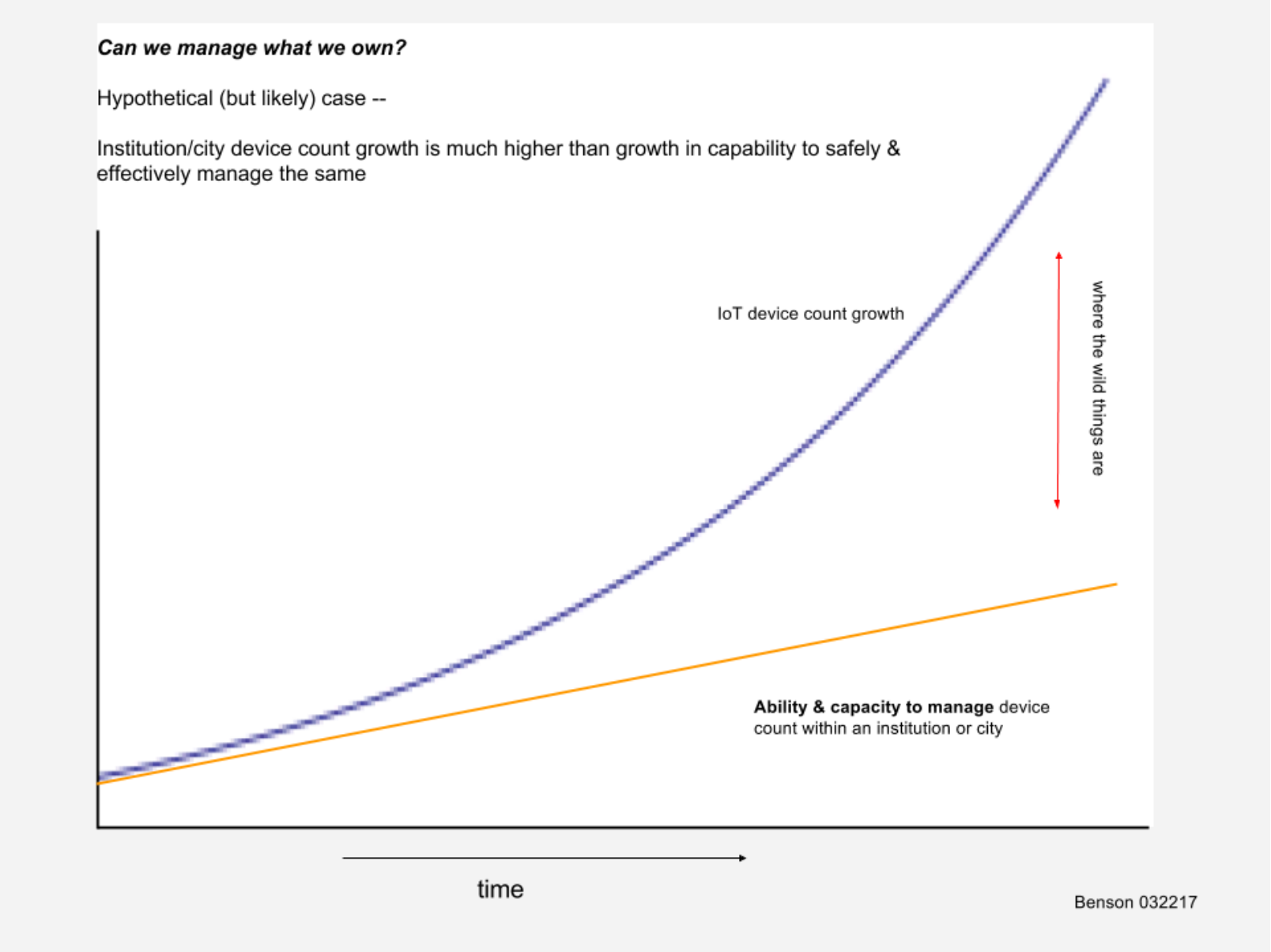
4. IoT Systems span multiple organizations within an institution



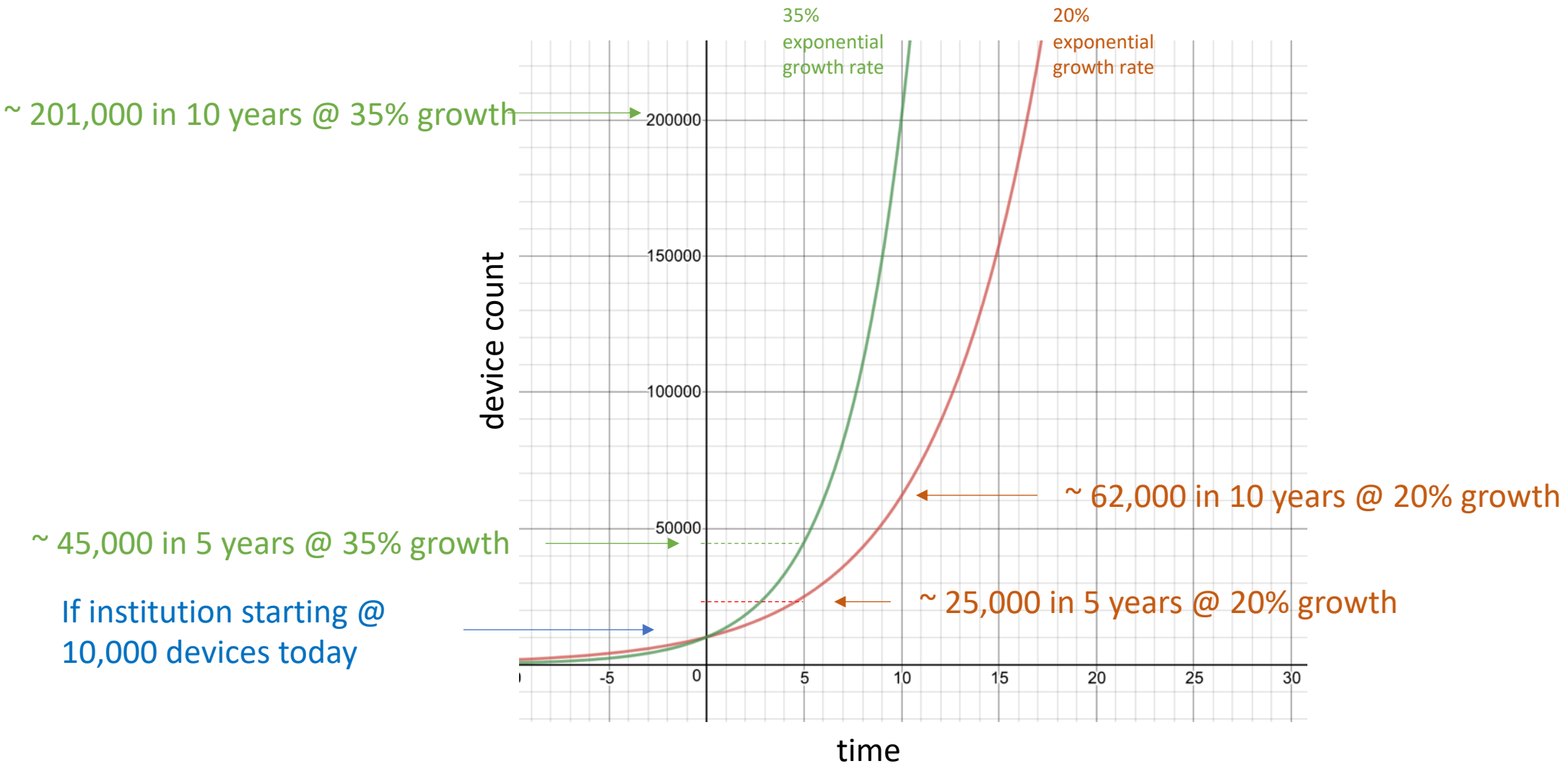
5. Devices can be out of sight, out of mind

6. Lack of precedent for implementation
   a. As an industry/sector, we’re not good at it

Can we manage what we own?

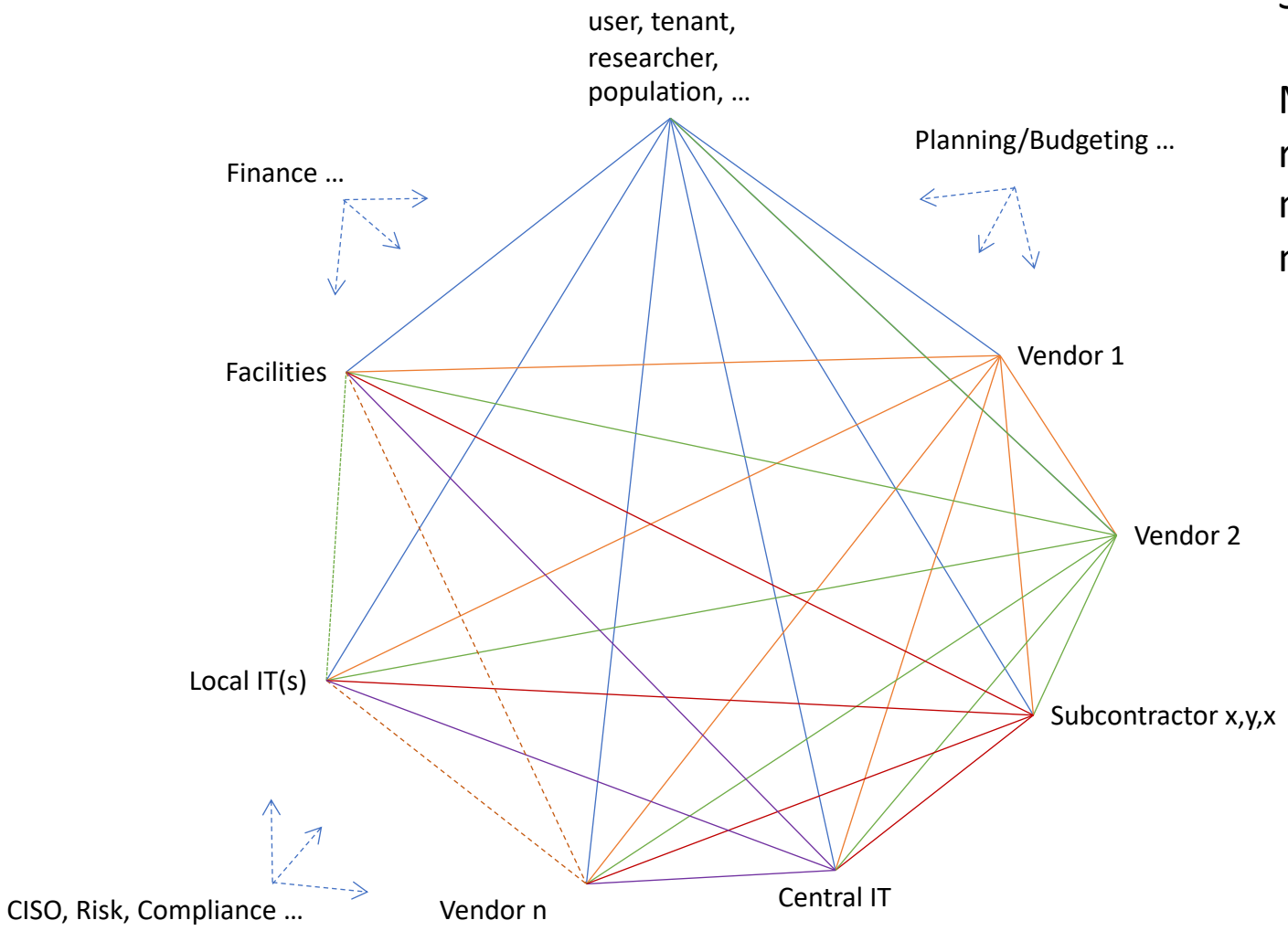


Reminding ourselves of what exponential growth looks like --



Chuck Benson | 031119

Organizational spanning

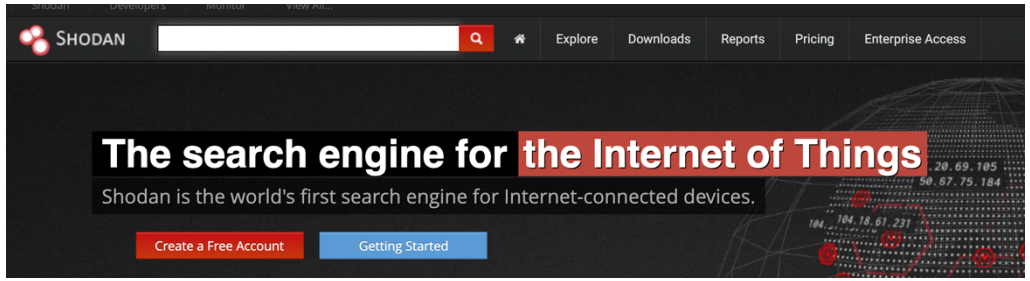


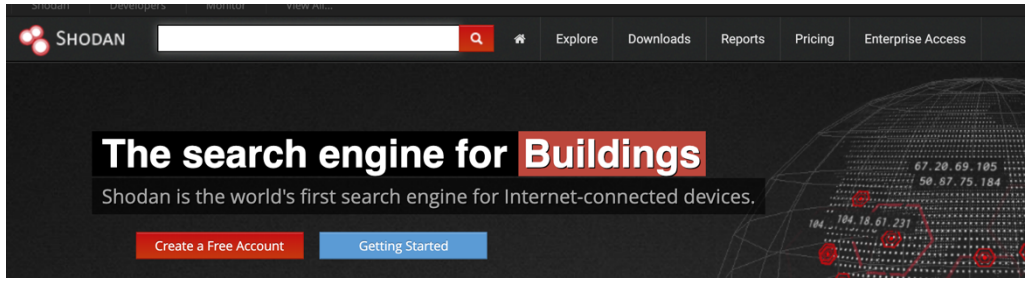
Many different orgs/departments, vendors/contractors involved in IoT Systems …

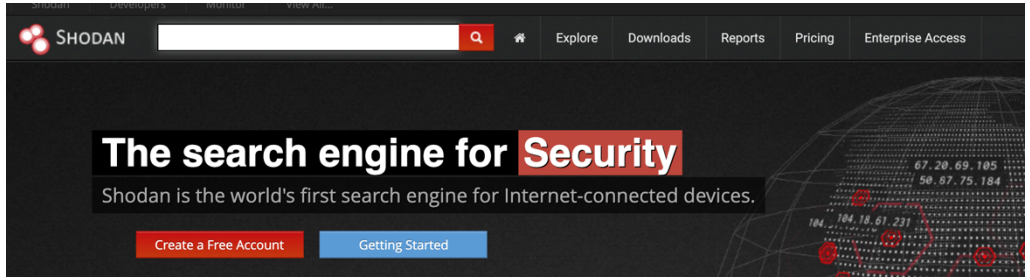
Means even higher number of relationships between them to be managed (or costs/consequences of not managing them)

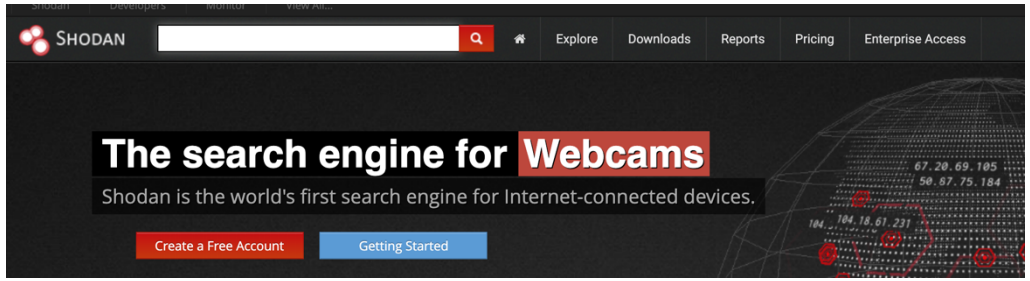
# of orgs/vendors	# of relationships
2	1
3	3
4	6
5	10
6	15
7	21
…	…

Shodan.io

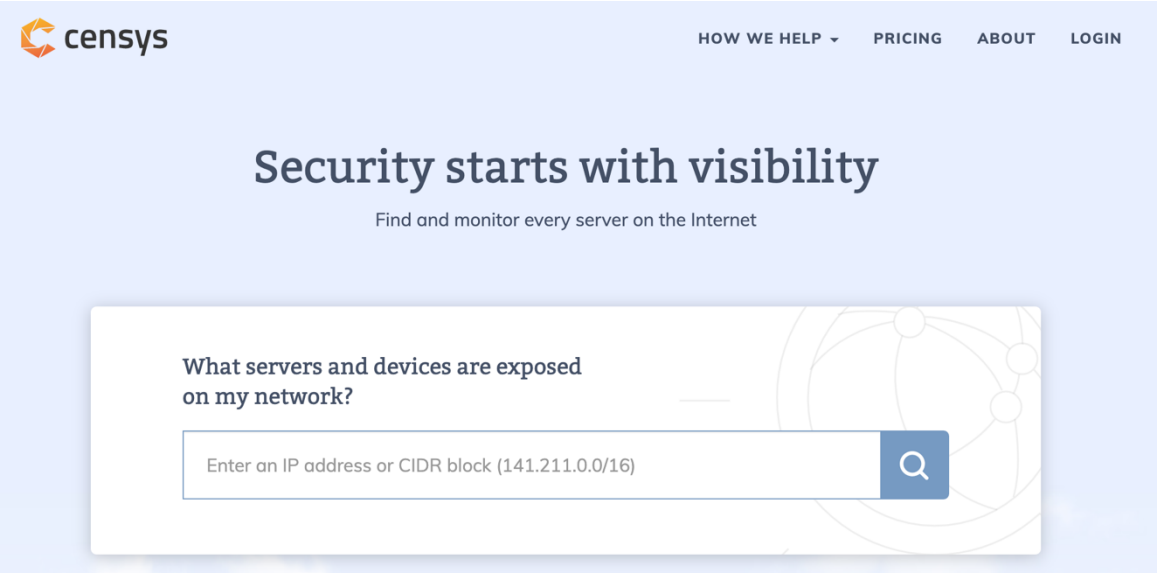








Censys.io



Sort of typical return from Shodan query

Some location info:

[redacted] View Raw Data

City	Seattle
Country	United States
Organization	[redacted]
ISP	[redacted]
Last Update	2019-06-02T10:32:59.311205
ASN	[redacted]

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2014-2532	sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.

Ports

22 80 443

Services

22
tcp
ssh

OpenSSH Version: 6.5

```
SSH-2.0-OpenSSH_6.5
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQC7V3dBai+EAYXl1sPVGWGvwUTCotEM2wHfmK/ZkMcpAyZs
6dz4LJEvVSYgE8I1aAg8t+CyKfuBYWXH7tEjtGVbYL2Zk81APlol9Xprx3TqhD3ufAQqzuNr23j/
FSofaeUPWwychEM3kVEV57VawEjRuG3qZxUXFTM0D/FrCecAWCVDHmZ/QdIKIj+778sv4RX+8cPg
gVnmI9KI1bNNwFYrZGtVWXsWyf74YPwxTKliZfxsKIRWgLE5LyDomlVXIssaB7igg8cgyJOjdRTH
eRn5d61Q9iEPCJddmS4sf1RdzHzVBGuebbCICct91VQiuvDNkcEfJvEuDFWqfRlR64uf
Fingerprint: 6e:33:ba:0d:33:d4:b0:81:17:37:a0:fa:86:d2:3f:b9
```

Some open ports & services – SSH & 2 web ports, in this case

(vulnerability list cropped off here)

(additional port/service information cropped off here)

https://www.shodan.io/search?query=lenel

Shodan | Developers | Monitor | View All...

SHODAN lenel

Explore | Downloads | Reports | Pricing | Enterprise Access

Exploits | Maps | Share Search | Download Results | Create Report

search term "lenel"

TOTAL RESULTS

81

TOP COUNTRIES

United States	80
Germany	1

TOP SERVICES

8032	80
8081	1

TOP ORGANIZATIONS

[redacted] Stores, LLC	80
[redacted] GmbH	1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

[redacted].83.33.220
[redacted]
Added on 2019-06-04 04:28:05 GMT
United States, Stow

```
HTTP/1.0 200 OK
date: x
content-type: text/html
connection: close
server: Lenel Embedded Web Server/8373
```

[redacted].83.32.114
[redacted]
Added on 2019-06-04 01:09:10 GMT
United States, Stow

```
HTTP/1.0 200 OK
date: x
content-type: text/html
connection: close
server: Lenel Embedded Web Server/8373
```

[redacted].83.34.64
[redacted]
Added on 2019-06-04 19:32:12 GMT
United States

```
HTTP/1.0 200 OK
date: x
content-type: text/html
connection: close
server: Lenel Embedded Web Server/8373
```

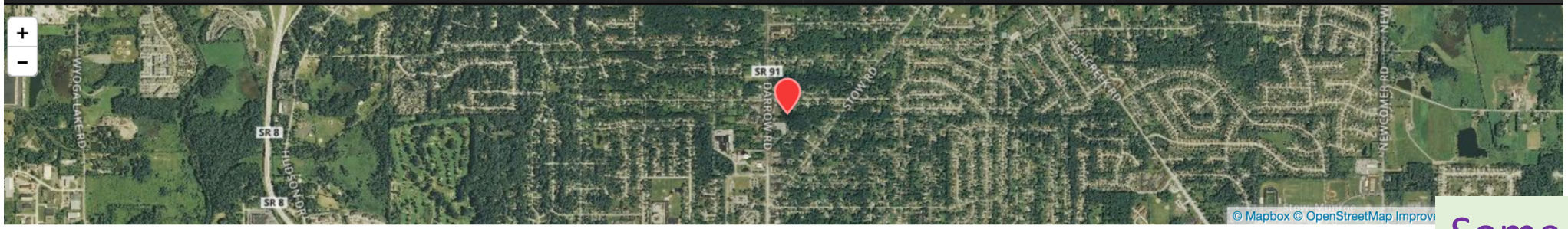
[redacted].83.34.179
[redacted]
Added on 2019-06-01 21:21:28 GMT
United States

```
HTTP/1.0 200 OK
date: x
content-type: text/html
```

approx 50 of these

Some instances & ports returned with search term “lenel”

SHODAN | Explore | Downloads | Reports | Pricing | Enterprise Access | My Account



[redacted].83.32.114 [redacted] View Raw Data

videogame

City	Stow
Country	United States
Organization	[redacted]
ISP	
Last Update	2019-06-05T02:35:23.304659
Hostnames	[redacted]
ASN	AS20164

Ports

15	19	26	37	82	88	113	389	444	587	777
873	1604	1991	2000	2056	2095	2455	3388	3542	3780	4001
4063	4848	5269	6379	6666	7777	8000	8002	8032	8060	8095
8554	8889	9000	9869	9943	9944	12345	17000	20256	27015	33338
54984										

Services

Some open ports & services – 1000+

IP address

Business: [redacted] Stores

Approx 50 of these addresses

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

[redacted].83.32.53
[redacted]
Added on 2019-05-24 12:04:27 GMT
United States, Stow

```
HTTP/1.0 200 OK
date: x
content-type: text/html
connection: close
server: Lenel Embedded Web Server/8373
```

[redacted].83.33.18
[redacted]
Added on 2019-05-24 07:45:38 GMT
United States, Stow

```
HTTP/1.0 200 OK
date: x
content-type: text/html
connection: close
server: Lenel Embedded Web Server/8373
```

[redacted].83.33.155
[redacted]
Added on 2019-05-23 11:18:18 GMT
United States, Stow

```
HTTP/1.0 200 OK
date: x
content-type: text/html
connection: close
server: Lenel Embedded Web Server/8373
```

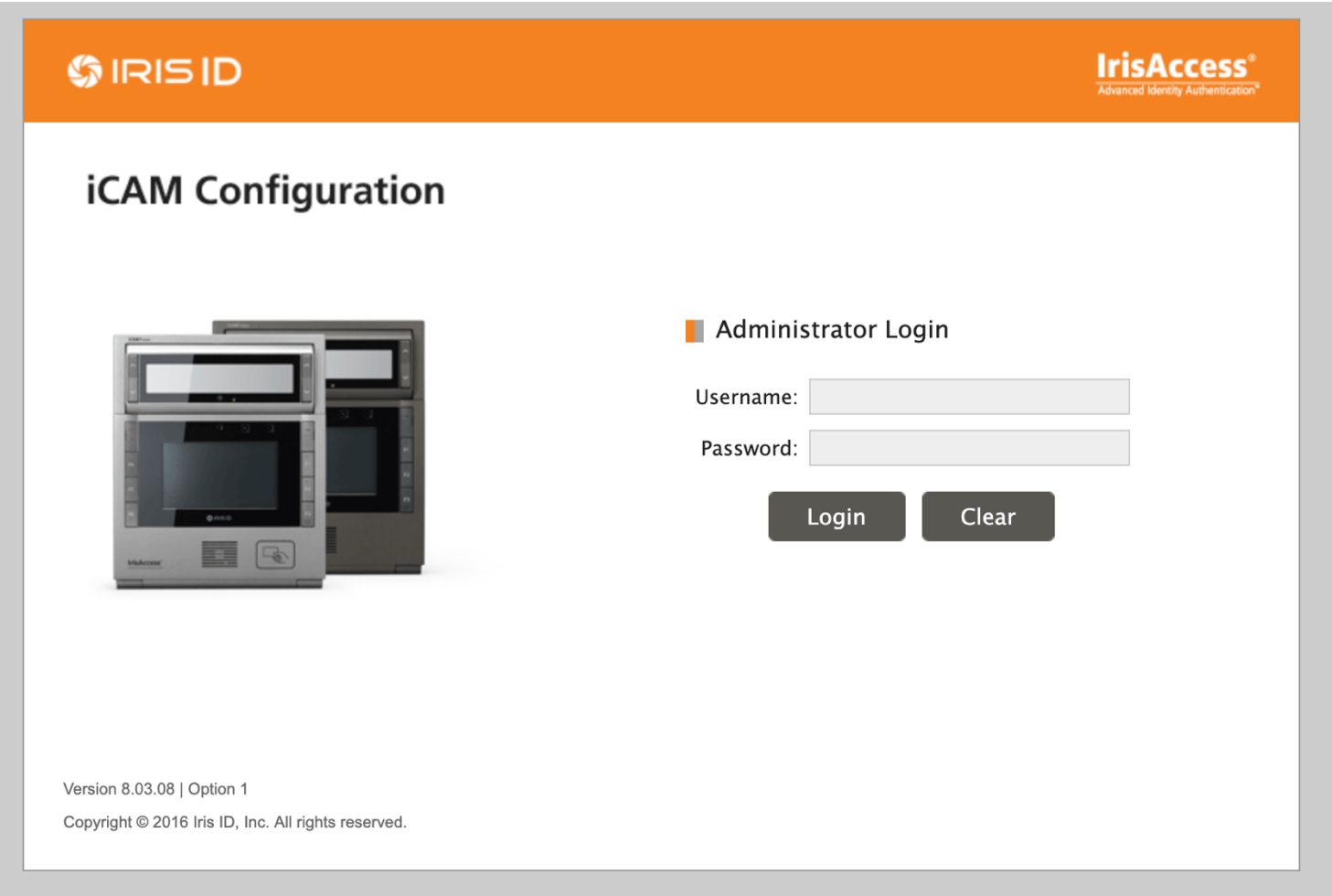
?

server: Lenel Embedded Web Server/8373

- This is what the service is reporting – don't know if Lenel or not
- But even if Lenel, could have been configured poorly
  - By client/customer or
  - 3rd party integrator

Benson | 060419

Another example



icam 7000 default password

All | Shopping | News | Images | Maps | More | Settings | Tools

About 32,000 results (0.39 seconds)

[PDF] iCAM7100S_Hardware_Guide_160215_ver 1.1 - Iris ID

https://www.irisid.com/.../iCAM7100S_Hardware_Guide_160215_ver%201.1.pdf

For example, if the IP address of an **iCAM** is 192.168.5.100 (**default** IP), you would access the configuration web interface by typing http://192.168.5.100 from an internet browser. To login, the User ID required when prompted is iCAM7000. The **Password** is iris7000.

"To login, the User ID required when prompted is iCAM7000. The Password is iris7000"

IRISACCESS ICAM7000

Iris Recognition Biometric Access Control System

$2,199.00

Usually ships within 2-3 business days

1

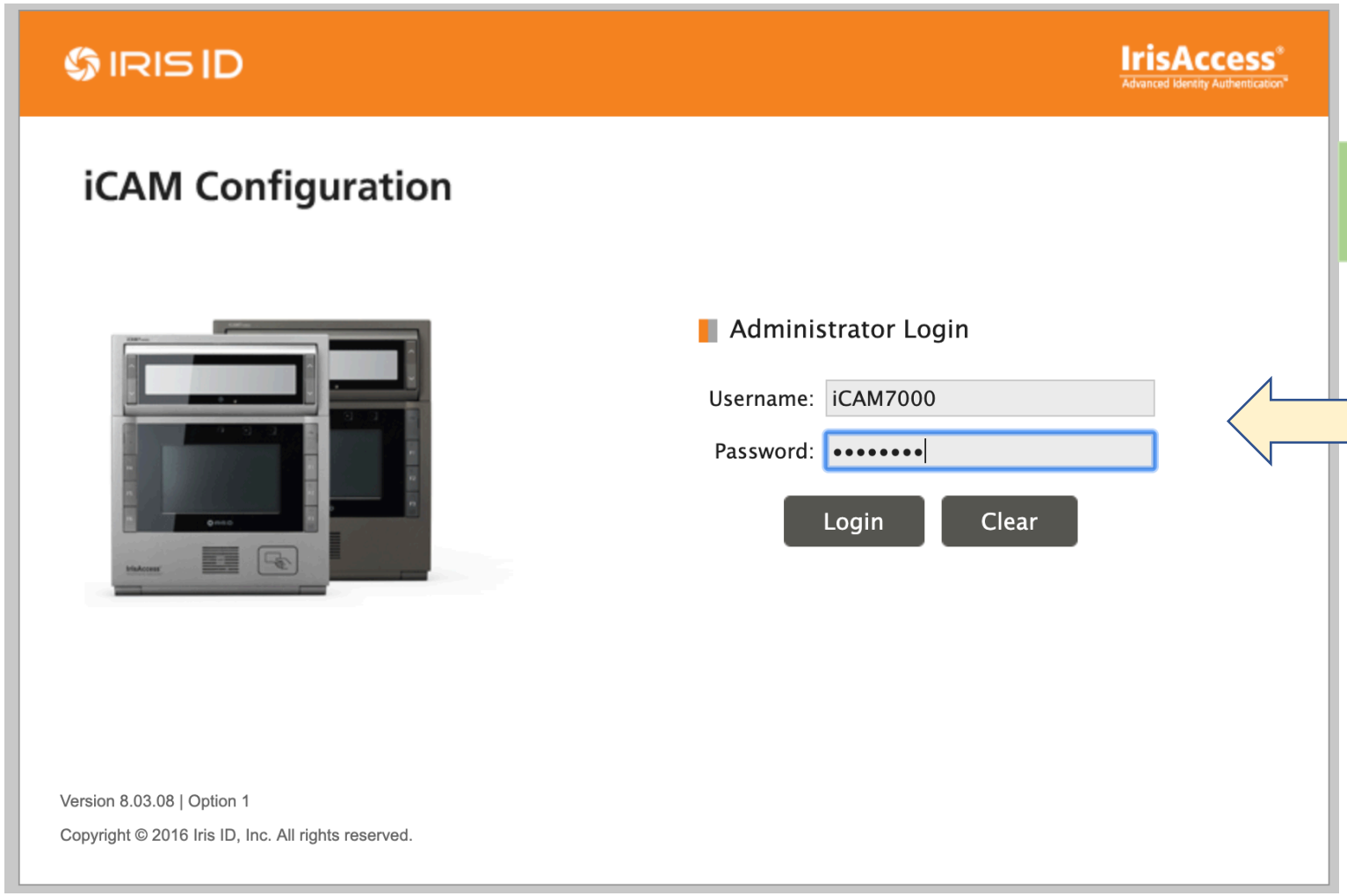
ADD TO CART

SKU: iCAM7000

SAFE AND SECURE

100% Price & Performance Guarantee

Benson | 060419



Default username & password from Google

IRIS ID

IrisAccess®
Advanced Identity Authentication®

Logout

iCAM Configuration

- Configuration Summary
- Network Settings
- iCAM Settings
- Wiegand Settings
- Smart Card Settings
- LCD & PIN Pad Settings (LCD Models Only)
- LCD Custom Image Upload (LCD Models Only)
- Voice Message Upload
- Custom Certificate Upload
- Change Username/Password
- Operational Mode Selection
- Reboot

Version 8.03.08 | Option 1

Logout

iCAM Configuration

Configuration Summary

Operational Mode:	Option 1
Display initial start-up screen:	Disabled
Voice Language:	English
Network Configuration:	Static
IP Address:	[redacted]
Subnet Mask:	
Default Gateway:	
IP announcement:	Enabled
Communication on Port 80:	Enabled
Smart Card Type:	HID iClass
Tilt Assist:	
By Card/PIN:	Enabled
On Approach:	Disabled
Power Save:	Never
IrisCapture Guiding Voice Messages:	Play all
Shutter Sound:	Disabled
Wiegand In Interface Type:	Enabled
PIN pass-through from an external PIN PAD device:	Disabled
Wiegand Out Interface Type:	Enabled
LCD Display:	ON
LCD Brightness:	5
Date and Time Display:	Enabled
Time Format:	12-hour
Custom Image Display:	Disabled
IrisCapture Guiding Display Messages:	Enabled
Keypad Popup:	Enabled
PIN Mode:	8bit Burst
PIN Pad Timeout :	5 sec

IRIS ID

IrisAccess
Advanced Identity Authentication

Logout

iCAM Configuration

- Configuration Summary
- Network Settings
- iCAM Settings
- Wiegand Settings
- Smart Card Settings
- LCD & PIN Pad Settings (LCD Models Only)
- LCD Custom Image Upload (LCD Models Only)
- Voice Message Upload
- Custom Certificate Upload
- Change Username/Password
- Operational Mode Selection
- Reboot

Version 8.03.08 | Option 1

IRIS ID

IrisAccess
Advanced Identity Authentication

Logout

iCAM Configuration

Smart Card Settings

Smart Card Type: HID iClass

Communication: Plain

Authentication Key (hexadecimal): ••••••••••••••••

Set to Default

OK Cancel

Back To Main

Version 8.03.08 | Option 1

IRIS ID

IrisAccess
Advanced Identity Authentication

Logout

iCAM Configuration

Operational Mode

Option 1: Networked iCAM Control / Iris Matching Mode See Diagram

For iris enrollment (EAC IrisEnroll) or for use with an ICU, or with iData iCAM7000 Series Device Control SDK Software. No built-in database or iris matching.

Option 2: Smart Card On-Device Verification Mode (See Option 3 settings)

Option 3: On-Device iCAM Control and Iris Matching Mode See Diagram

iCAM is controlled and iris matched inside iCAM. Provides input and output function within the iCAM.
Use with IrisAccess EAC software. Can match iris in 1:1 (with PIN or Prox), 1 to Many (Iris Only), and match iris on Smart Card, or prox card only.

IrisServer IP:
(IP Address of the computer running IrisServer)

Security ID:
(Note: The security ID must match security ID entered in IrisManager/Creation/Remote Units for this unit.)

Upon failure to synchronize with the IrisServer:
- Use the local copy of the DB and continue operation.
- Put iCAM into an error state and wait for reconnection to IrisServer.

Iris template MUST BE Encoded onto SmartCard: Stand-alone mode for 1:1 verification only. No EAC IrisServer connection.(Previously Option2)

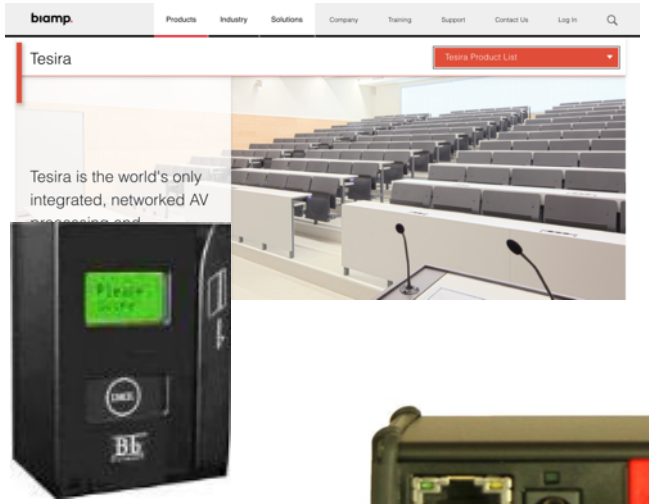
iCAM Setting Recognition Mode must be set to "Smart Card + Iris".

iCAM Manager:

iCAM is controlled and iris matched inside the iCAM. Use to provide services to iCAM Manager SDK client applications.

Security ID:

Examples of other devices found on some Higher Ed networks



Lab automation & environmental control

DM-DGE-200-C

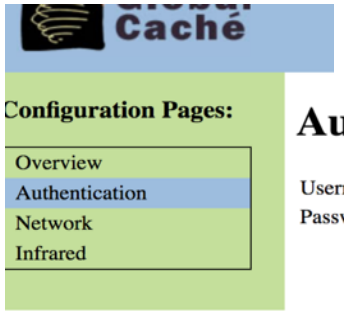
Digital Graphics Engine 200 w/PinPoint™ UX & 4K DM 8G+® Input

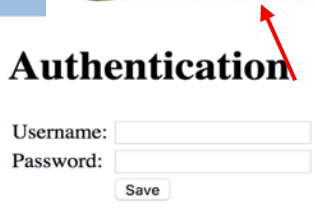
Provides a high-performance graphics engine for the Crestron® TSD-2220 and third-party touch screen displays. Supports advanced Smart Graphics™ with dual-window video from HDMI®, DM®, and streaming sources. Its low-profile, surface-mountable design fits virtually anywhere.

Built-in PinPoint™ UX app leverages any room display to create an intelligent meeting space seamlessly integrated with Crestron Fusion® Cloud. Offers an enhanced

Classroom AV – no password, unencrypted access – able to configure device, download logs, …

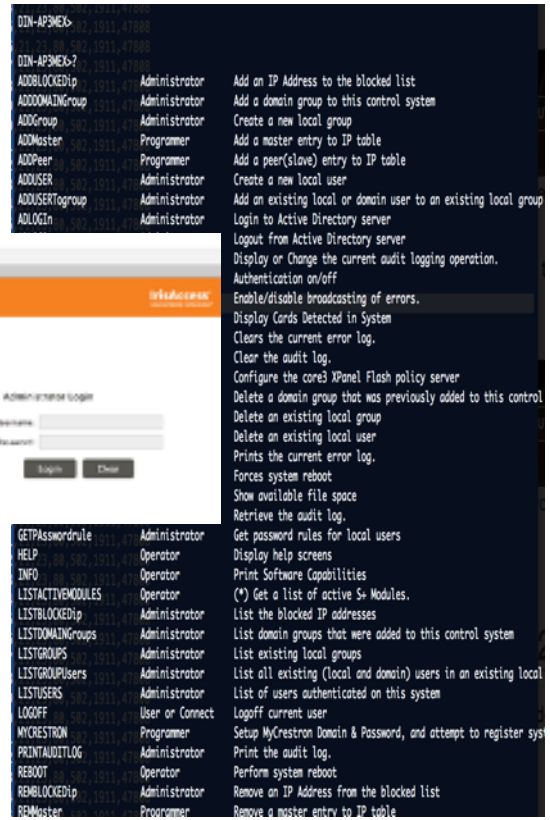
[PDF] XPort AR User Guide - Lantronix
www.lantronix.com/wp-content/uploads/pdf/XPort-AR_UG.pdf
Dec 10, 2010 - 19. Accessing **XPort** AR Using DeviceInstaller ..... The factory-**default** username is "admin" and the factory- **default password** is "PASS.





Open for configuration -- Remotely controls infrared devices over internet – no password – infrared control of what … ?

Remote power switching unit – open for configuration



+ many printers …

SMA CLUSTER CONTROLLER

Professional monitoring and controlling for decentralized large-scale PV plants

SMA Cluster Controller for medium-sized plants up to 25 devices

Hue White and color ambiance Beyond table lamp

- LED integrated
- White
- Smart control with Hue bridge*
- Control with your voice*

71202/31/48 $199.99

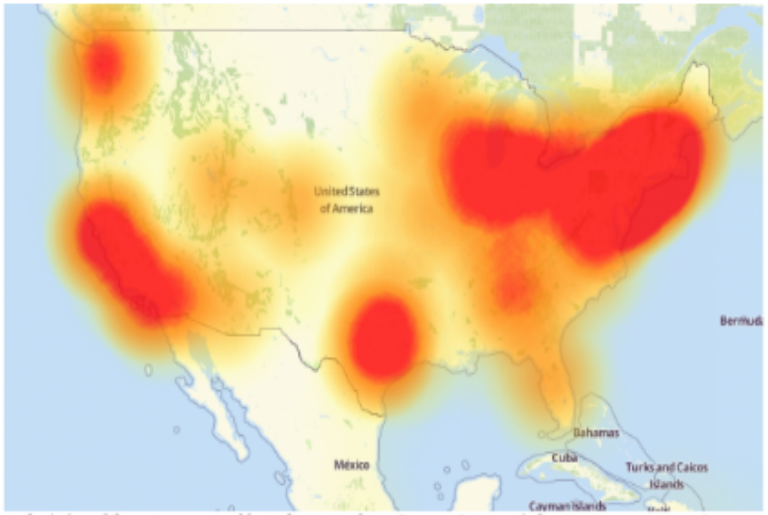
Some historical outcomes …

21 Hacked Cameras, DVRs Powered Today's Massive Internet Outage

OCT 16

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.

'Mirai' 2016
(krebsonsecurity.com)

2008 Turkish pipeline hack (via network video cameras)

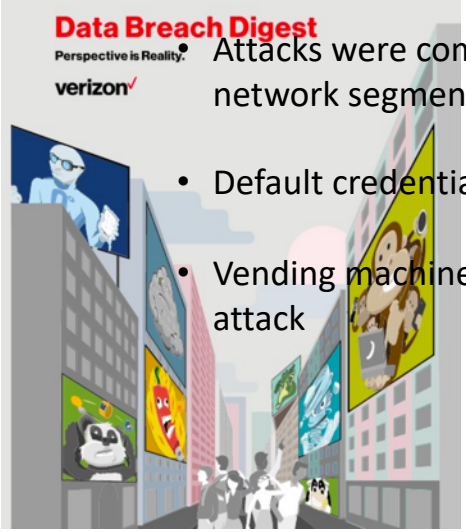
2015 Jeep hack

465,000 devices needed in place firmware update

Unnamed University attacked via on campus IoT devices
(from Verizon Data Breach Digest 2017)

- Campus domain name servers (DNS) attacked causing slowdowns & outages
- Over 5,000 devices used to attack
- Malware had full device control
- Malware changed passwords so that IT support was locked out

- *"We had known repeatable processes and procedures for replacing infrastructure and application servers, <u>but nothing for an IoT outbreak</u>."*



- Attacks were coming from the university's IoT network segments

- Default credentials were on many of the devices

- Vending machines, light bulbs, other used in attack

Evaluating IoT system implementation success by measuring --

- ROI
  - Does the system do what we thought it would for the actual incurred & ongoing cost?
  - Did we underestimate the work required to manage?

- Cyber risk profile
  - Did we make things worse in the course of implementing the system?
  - Did we increase the attack surface?
  - Did we underestimate the work required to manage?

-- Desired state --

Higher Ed client/customer –

has high expectations for thorough & thoughtful system deployment

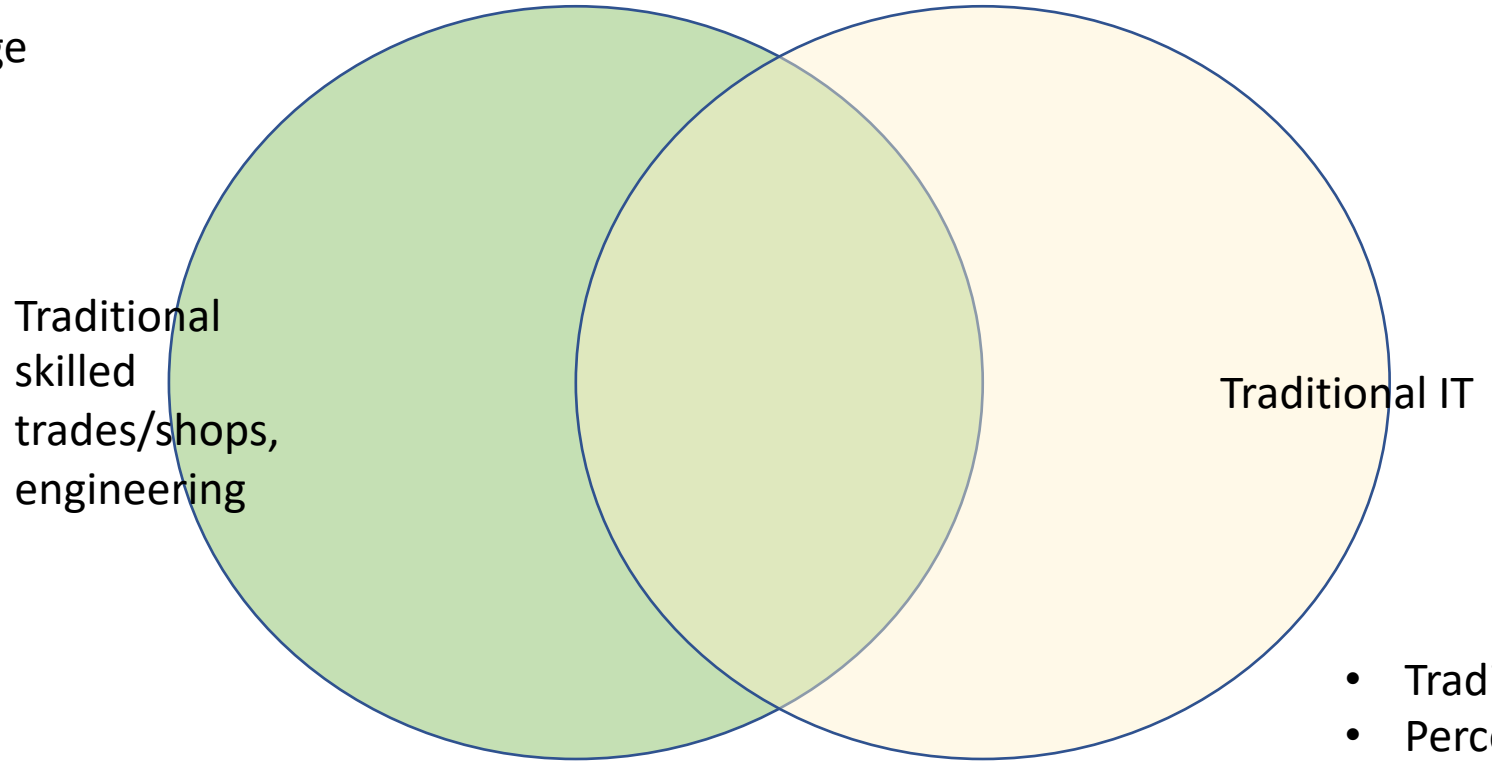
Vendor/provider –

has high expectations for thorough & thoughtful system deployment

Both have expectations for thorough & thoughtful system deployment

Cultures in Collision – Creates Opportunity

- Tradition/history
- Perceptions of time
- Perceptions of change
- Language



- Tradition/history
- Perceptions of time
- Perceptions of change
- Language

"Culture eats strategy for breakfast"

Peter Drucker

IoT Systems on Campus

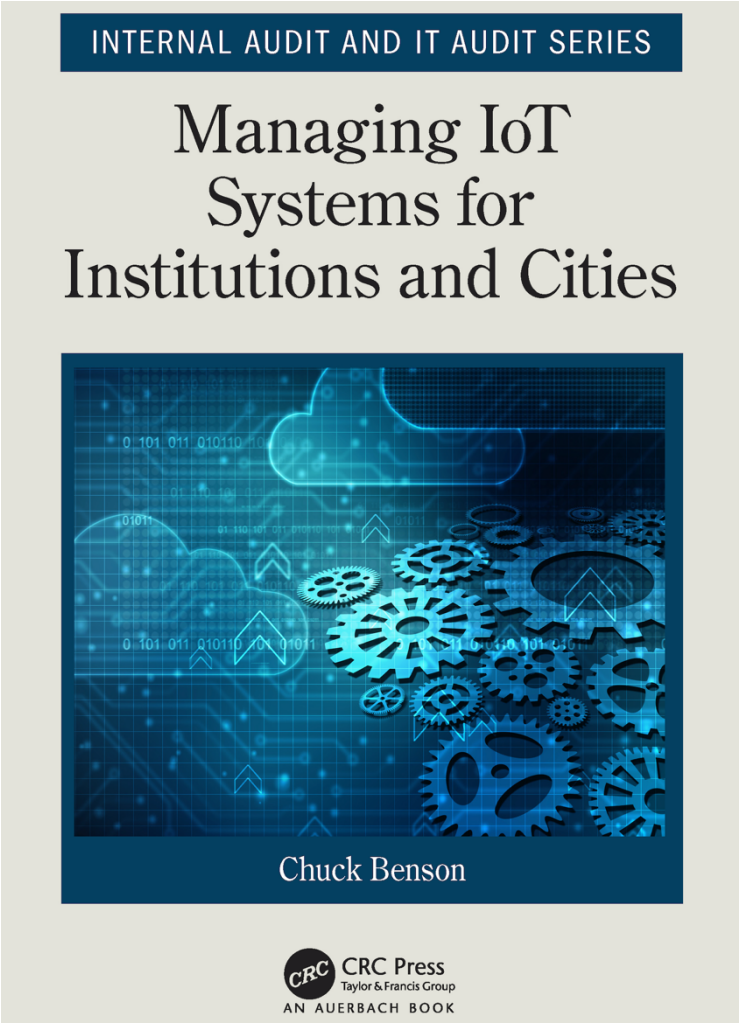
Partnerships essential. Some current examples include:

-- Advanced metering team with Facilities
-- Central IT Reporting & Analytics
-- Facilities Critical Infrastructure
-- Network Segmentation
-- Procurement
-- Research
-- More coming up

Questions/Comments ?

cabenson@uw.edu
cabenson361@gmail.com
http://longtailrisk.com

@cabenson361



(Scheduled publication data 7/15/19)