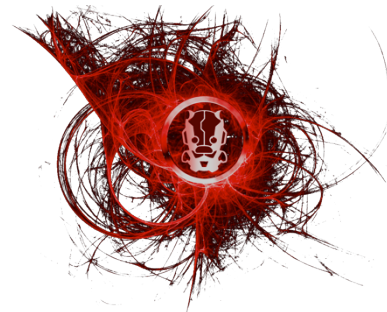


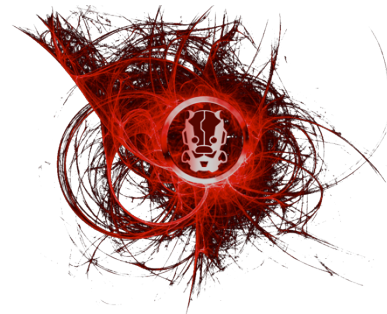
Boiler Plate Code: Building Management Systems

Common Security Issues

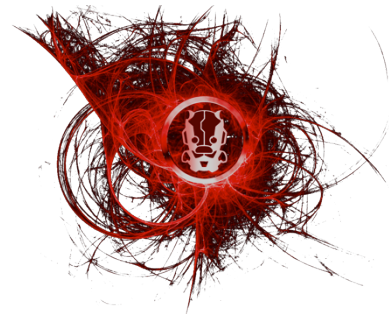


House Keeping

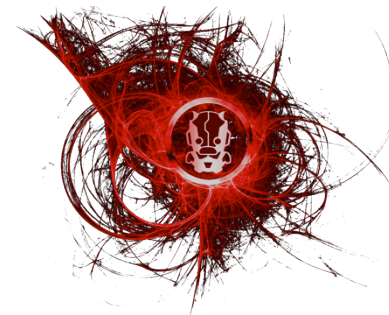
- If your phone goes off, I'll answer it.
- You can ask questions during the presentation.
- Rants can happen over a glass of red wine.
- If the fire alarm goes off, it was me.



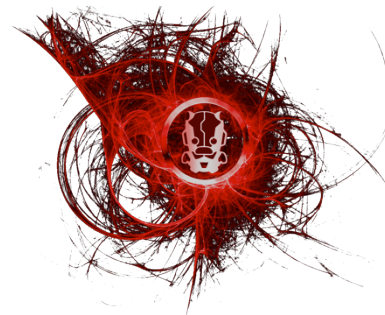
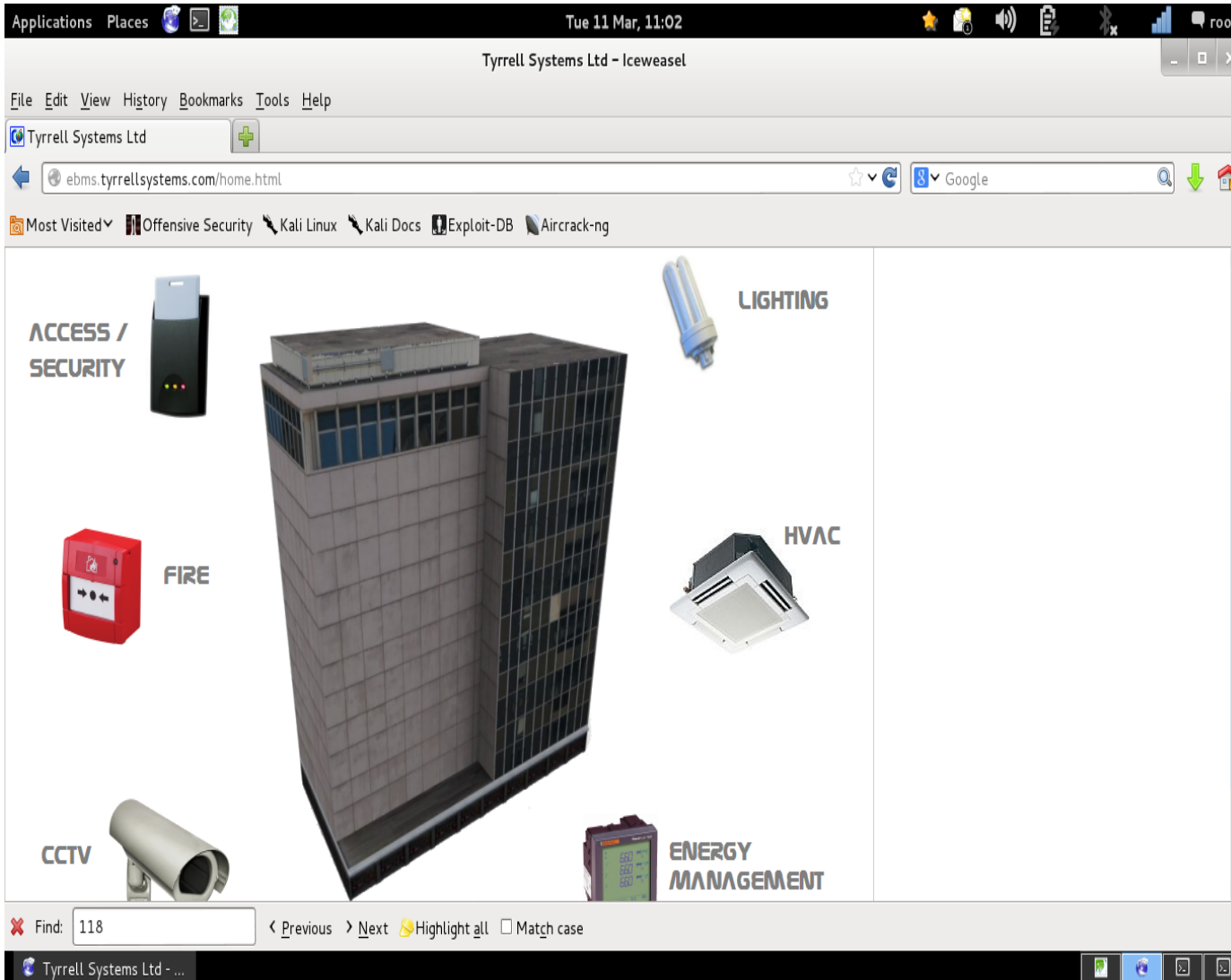
Some people think I do this...



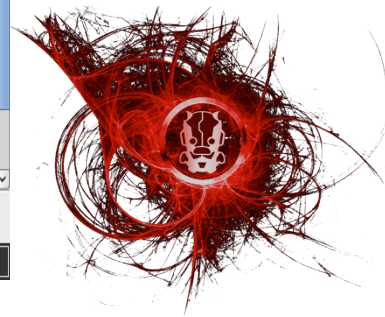
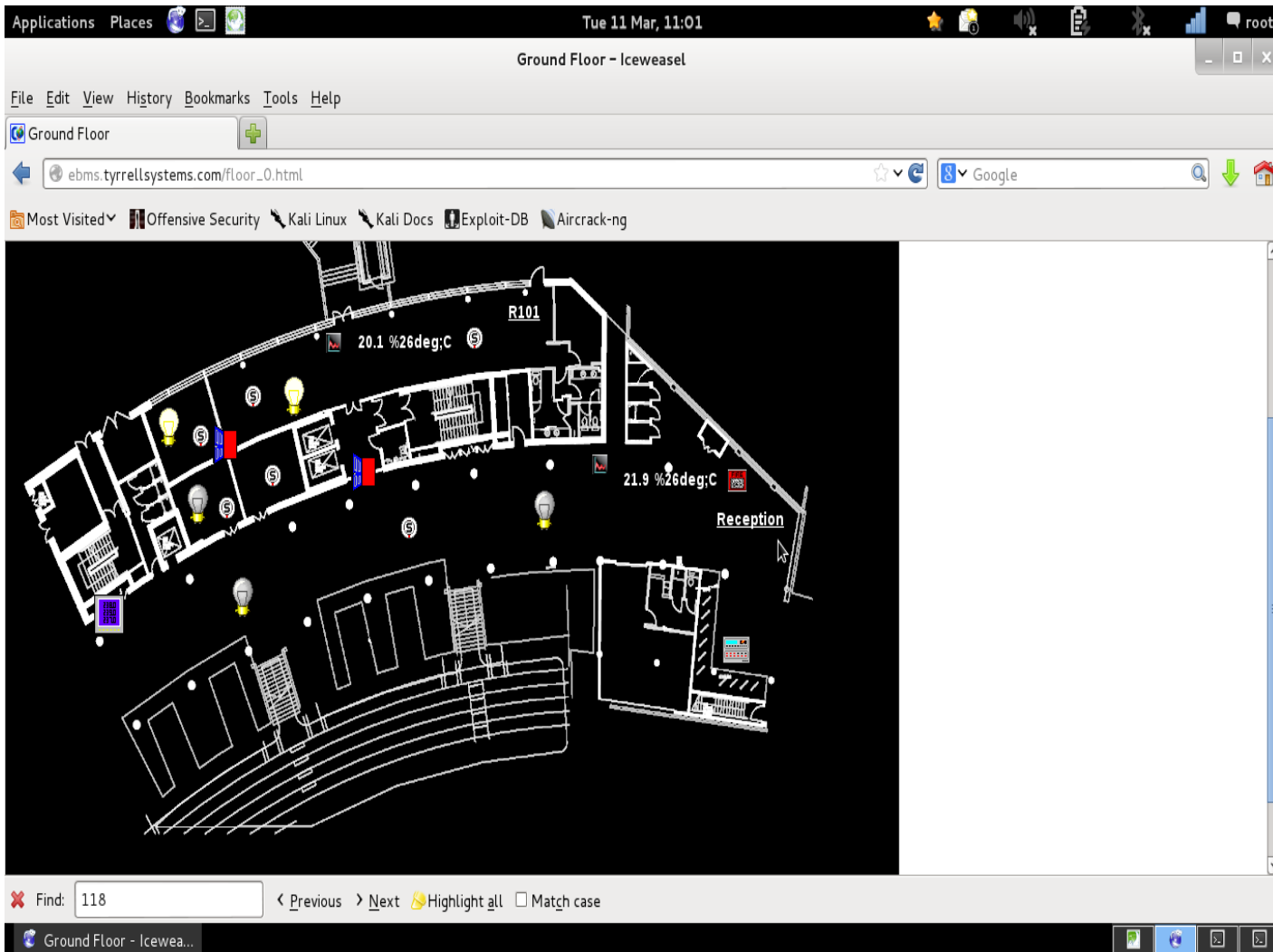
...it's really more like this!



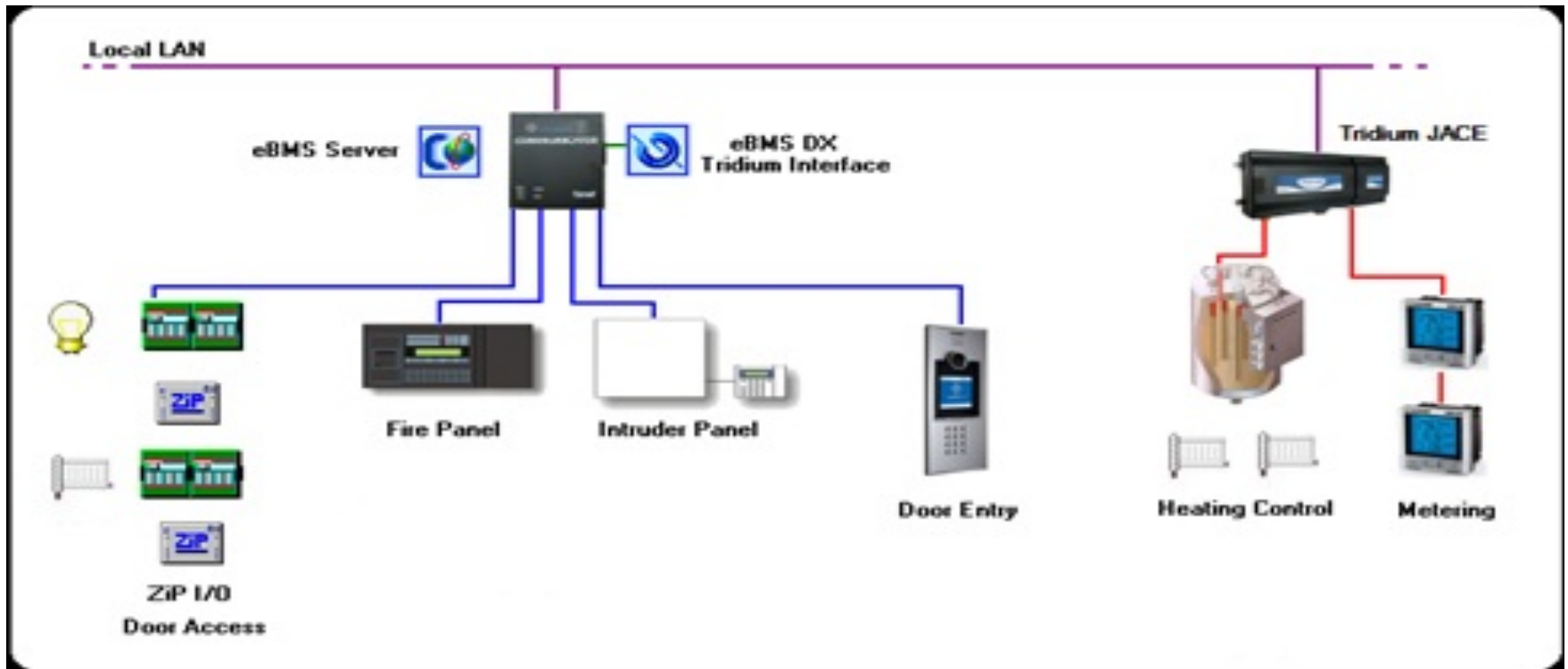
Brief intro to building management



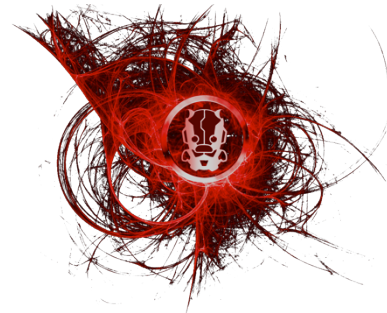
Why do they get attacked?



BMS is a network of cheap devices

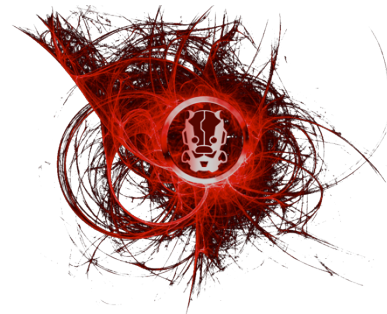


Access control device usually cache credentials
Updated by batch scripts
By design physically accessible



Common Security Issues

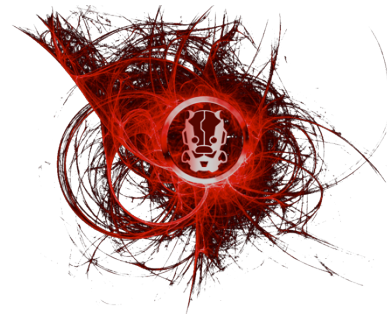
- All usual web app issues –
 - Auth
 - Dir trav
 - XSS
 - XXE
 - SQLi
- Protocols are spoofable, unauthed, insecure
- Vendor Maint Accounts *cough* backdoors *cough*
- Poor network segregation
- Incomplete network stacks
- Some components physically accessible



Lonworks

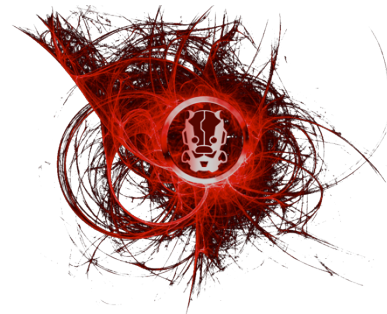
More than one addressing mechanism

- Neuron ID (phy address)
- Can have up to 15 groups per address
- Logical addresses (up to 2) bootstrapped Neuron ID
 - Domain ID 0-6 Bytes (Optional)
 - Subnet ID
 - Node ID
 - It's possible to do SENDER auth, but OPTIONAL
 - Often not done because challenge response increases network traffic x2



LonTalk Jargon

- SNVTs (“snivets”)
 - Network variables to you and me
 - Over 100 types
 - Temperature
 - Relative Humidity
 - Switch state
 - ASCII
 - Voltage
 - Messages may be ack’d or unack’ed



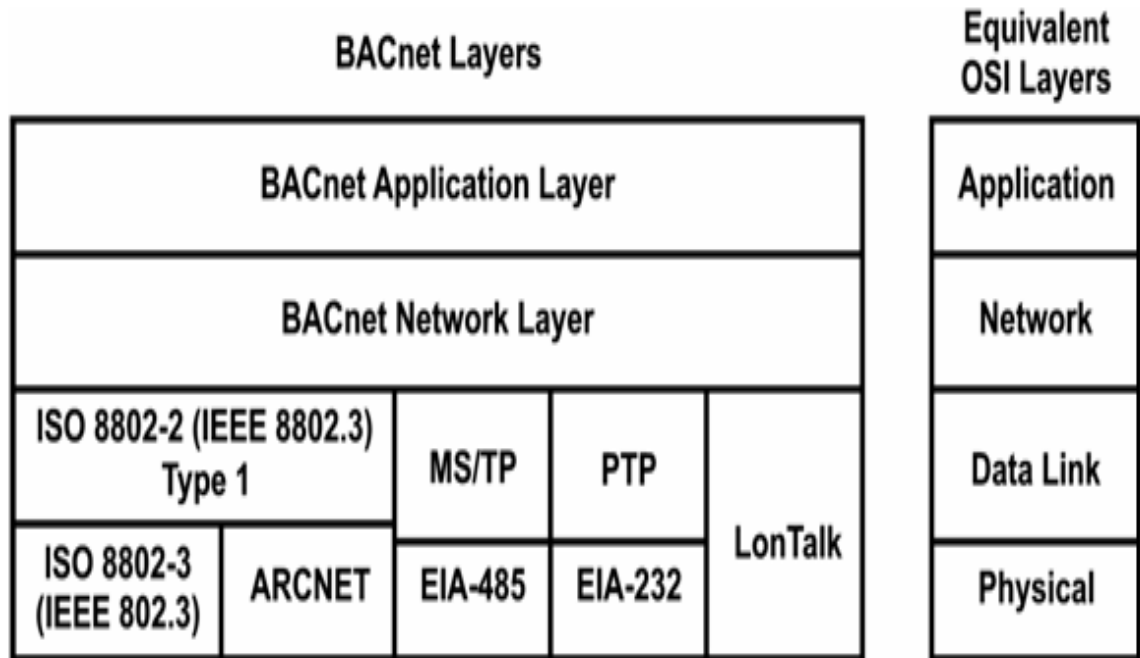
BACnet

Can traverse IP network:

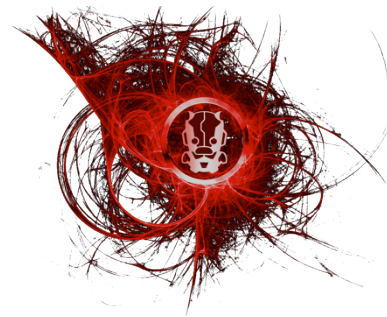
1. IP Tunnelling
2. BACnet/IP

“Foreign Devices” can join via
SLIP or PPP

Allows reception of forwarded
Broadcast messages


























“Wouldn't it be great if you could access a particular BACnet network over the phone from anywhere? That is the purpose behind "foreign device registration" which can be carried out through any internet connection, static or dynamic.” –BACNet tutorial

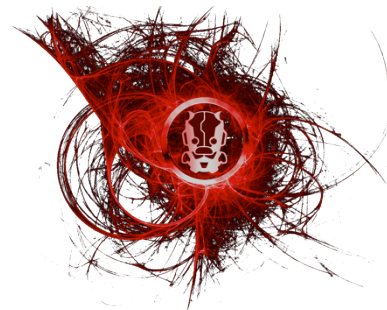


Mixing Binary and Analog in protocols? Simples.

Objects

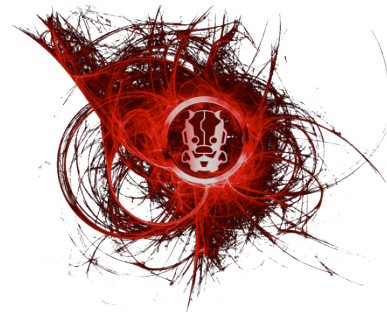
BACnet defines a collection of 23 standard object types

 Binary Input	 Multi-state Input	 File
 Binary Output	 Multi-state Output	 Program
 Binary Value	 Multi-state Value	 Schedule
 Analog Input	 Loop	 Trend Log
 Analog Output	 Calendar	 Group
 Analog Value	 Notification Class	 Event Enrollment
 Averaging	 Command	 Device
 LifeSafetyZone	 LifeSafetyPoint	

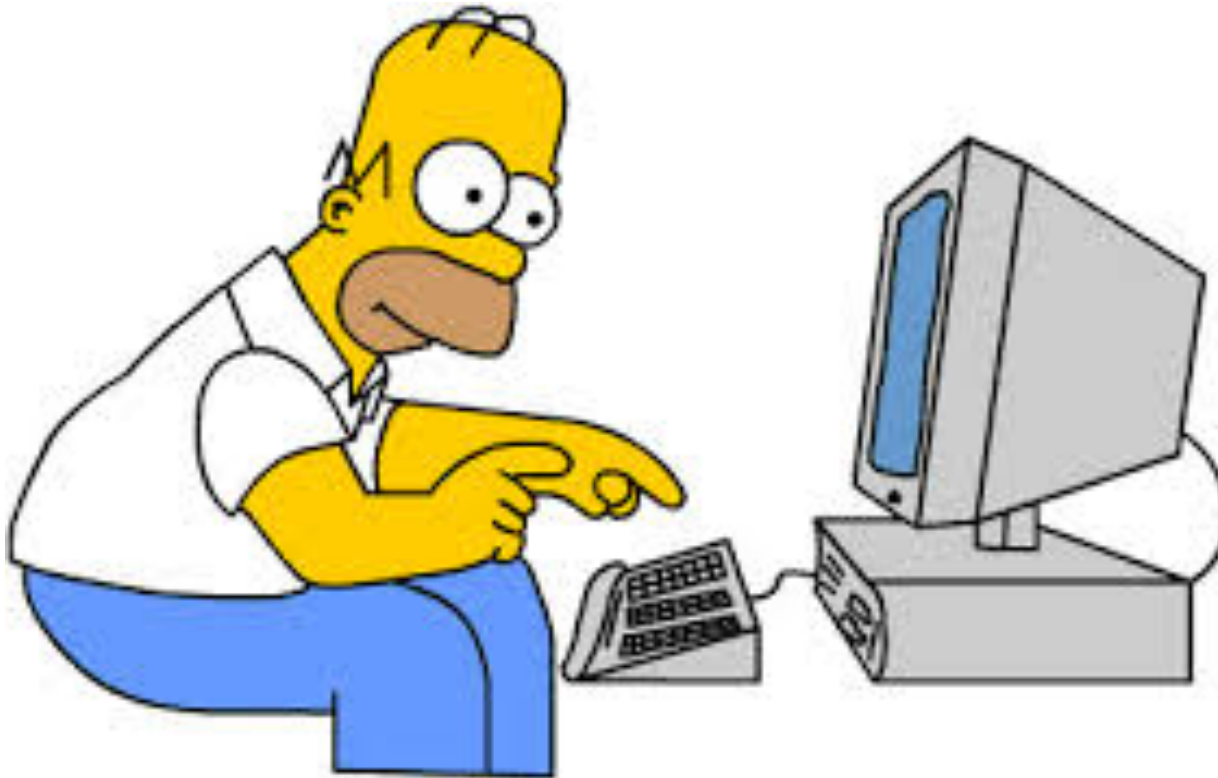


Bacnet NSE (NMAP) script

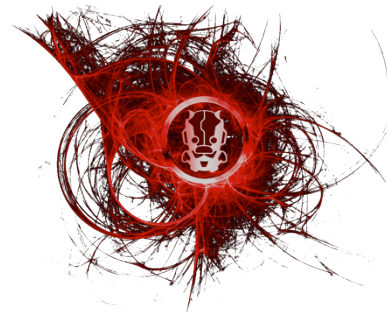
- Developed by Stephen Hilt @ DigitalBond
- Enumerates BACnet devices
- Error means it is old BACnet
- Details mean it is new BACnet
- Now get out there and look at your networks.



The Homer Problem



- ☐ Facilities Management are not comp-scis, neither should the be.
- ☐ Security is a lock right?
- ☐ No concept of how this opens an attack surface of your org
- ☐ Trusts the vendor
- ☐ Threatened by your suggestion of security review



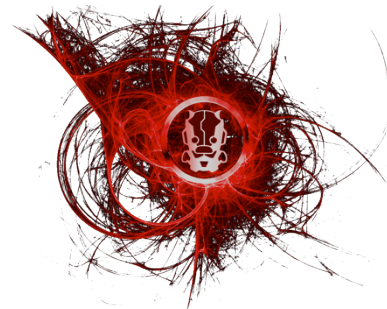
Scalance – X200 Switches

- Used MD5 over HTTP for credentials
- Session ID's completely predictable
- XSRF in FIRMWARE UPLOAD function

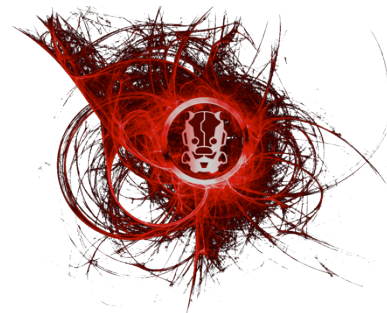
I worked with Siemens to get these fixed...
BUT WHO CARES?

NO ONE PATCHES SWITCHES.

Now consider that these are passing
packets for the protocols we just
described...

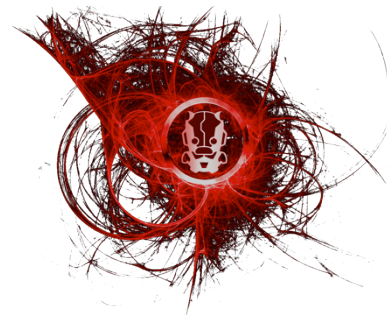


Remember this!



Mitigations

- Segregate the BMS network:
 - Ideally separate LAN
 - At least VLAN
- Disable external access || two factor
- Test web interface
 - Don't need to be great penetration tester
 - But do need to be careful
 - brittle BMS is the problem
 - Scanning device can cause problems



Summary

- ❖ Facilities Management couldn't have imagined, so be gentle with them
- ❖ Protocols offer little to no protection, and are aids to attackers
- ❖ At the very least segregate the network
- ❖ Worth penetration testing to push vendor improvements

When budgeting for the above tasks, you REALLY CAN use a flooded building, or fire engine call-out, or every door being unlocked as a cost of compromise!



Thank you for your time

Eireann.leverett(at)ioactive(dot)co(dot)uk

@blackswanburst

38D157B8

