

threat landscape gardening

A field guide to examining discrete technology solutions

Neal Wise - Assurance Pty Ltd



Neal Wise - yØ11



@yØ11 = UNIX guy, mac
security zealot, packet
monkey, biz guy

@assurance



Agenda

Talk is about a process not findings

Reaallly vague but I think I'm going somewhere with this

Taking what you know about organised technology to infer hidden components

Also I like taking pictures of busted technology



Discrete Solutions

Yeah. So I made this term up

Focused-purpose solutions that are generally isolated from other solutions (but not always)

Variously connected but many are IP networked or network accessible eventually



Examples I like

CCTV systems

A/D Telephony & VOIP

WiFi

Proximity card access
systems, lifts, etc.

advertising systems &
notice boards

Traffic and transport

Hotel entertainment
systems

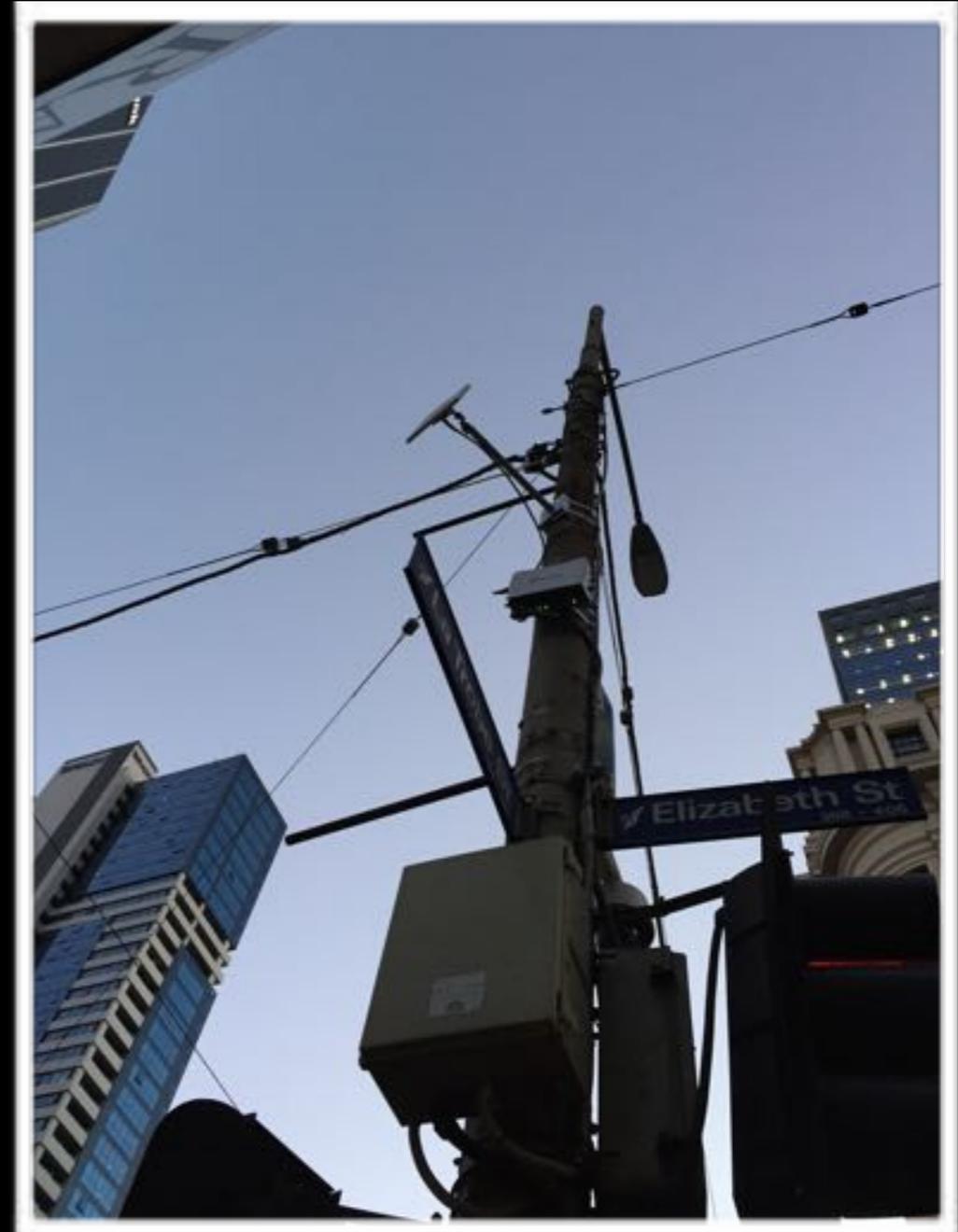
In flight entertainment
systems and data



so many cameras...



so many cameras...



Two endpoints of a point-to-point wireless solution for CCTV in City of Melbourne



Disclosure by observation



SNP Security

Firetide Mesh Routers



Disclosure by Case Study



The image shows a screenshot of a website article. At the top left is the logo for 'security electronics and networks', with 'security electronics' in white and 'and networks' in blue. To the right is a search bar labeled 'Search Articles ...'. Below the logo is a navigation menu with links for HOME, NEWS, PRODUCT REVIEWS, CASE STUDIES (which is highlighted), NEW PRODUCTS, FEATURES, and PRINT MAGAZINE. The breadcrumb trail reads 'Home > Case Studies > SNP Installs Axis, Genetec, Firetide at Footscray >'. The main title of the article is 'SNP Installs Axis, Genetec, Firetide at Footscray'. Below the title, it says 'Submitted on Sun, 01/15/2012 - 19:00'. The main content area features a photograph of a blue police sign with a white checkered pattern and the word 'Police' in white, mounted on a light-colored building wall.

Similar solution in City of Maribyrnong's Footscray CCTV solution



Disclosure by Case Study

FireTide mesh wireless. The work in the field is exemplary. With this much gear, you could excuse a bit of untidiness but the SNP boys have done extremely well in Footscray.



Better angled pics than mine

Visual ID of solution components.

Note the explanation for their technology's ugly urban blight



Disclosure by Case Study

...in the control room and a workstation and large displays in the Watchhouse.

"However, Police IT are currently investigating the creation of an email gateway to enable images to be emailed from within our network, creating an electronic audit trail, and reducing the need for copying to CD or USB."



This really seems like a bad idea



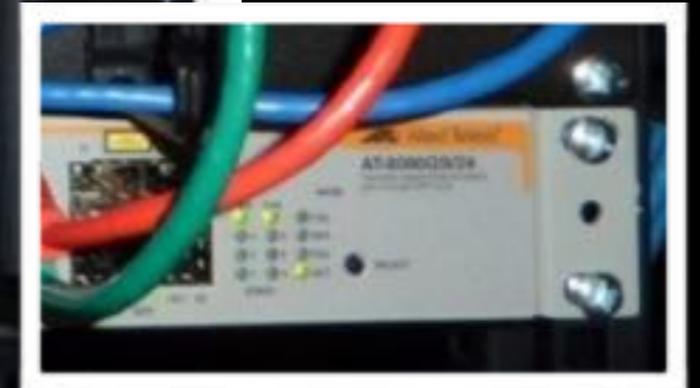
Disclosure by Case Study

significantly expand the capacity of the system in the future. We will continue to use wireless with fibre as the backbone. The wireless mesh is performing extremely well in this system.

"In fact, the original design had a fibre backbone running down to Leeds St and over the railway line but because a major State Government project involves partial demolition of the bridge over which our fibre would have run and the introduction of a whole new railway line we chose to wait."



Really, really unnecessary detail



Disclosure by creepy vendor YouTube vid

<https://www.youtube.com/watch?v=584fjITv-Qw>



The video player shows a street scene in Central Footscray. A white tram with a red roof is moving along the road. A person on a bicycle is riding alongside the tram. The video player interface includes the YouTube logo, a search bar, and playback controls. The video title is "Firetide to Help Prevent Crime in Central Footscray" and the channel is "fretideinc".

YouTube

0:03 / 1:06

Firetide to Help Prevent Crime in Central Footscray

fretideinc

Subscribe 198

284 views

+ Add to Share More

Vendor
solution
enthusiasm
gone
wrong.



Published on Oct 31, 2013

Show how well the zoom works, creeps



The video player shows a surveillance camera view of a shopfront. A red circle highlights a specific area on the right side of the frame, which is then zoomed in to show a person's hand reaching into a yellow bag. The shopfront has a sign that says "SMOOTHIES" and a neon sign that says "OPEN". The video player interface includes a play button, a progress bar at 0:13 / 1:06, and a search icon in the top right corner.

Firetide to Help Prevent Crime in Central Footscray

fretideinc
Subscribe 158

284 views

+ Add to Share More

Published on Oct 31, 2013
Footscray in Melbourne's Inner West is using the Firetide's wireless mesh as a key element in their Public Safety Security Surveillance System.

This video has several examples of zooming the system in on the public.

Who thought this was a good idea to put on YouTube?

How isn't this a violation of the public's privacy?



It is impressive (but creepy)



Firetide to Help Prevent Crime in Central Footscray



fretideinc

Subscribe 158

284 views

+ Add to Share ... More

3 0

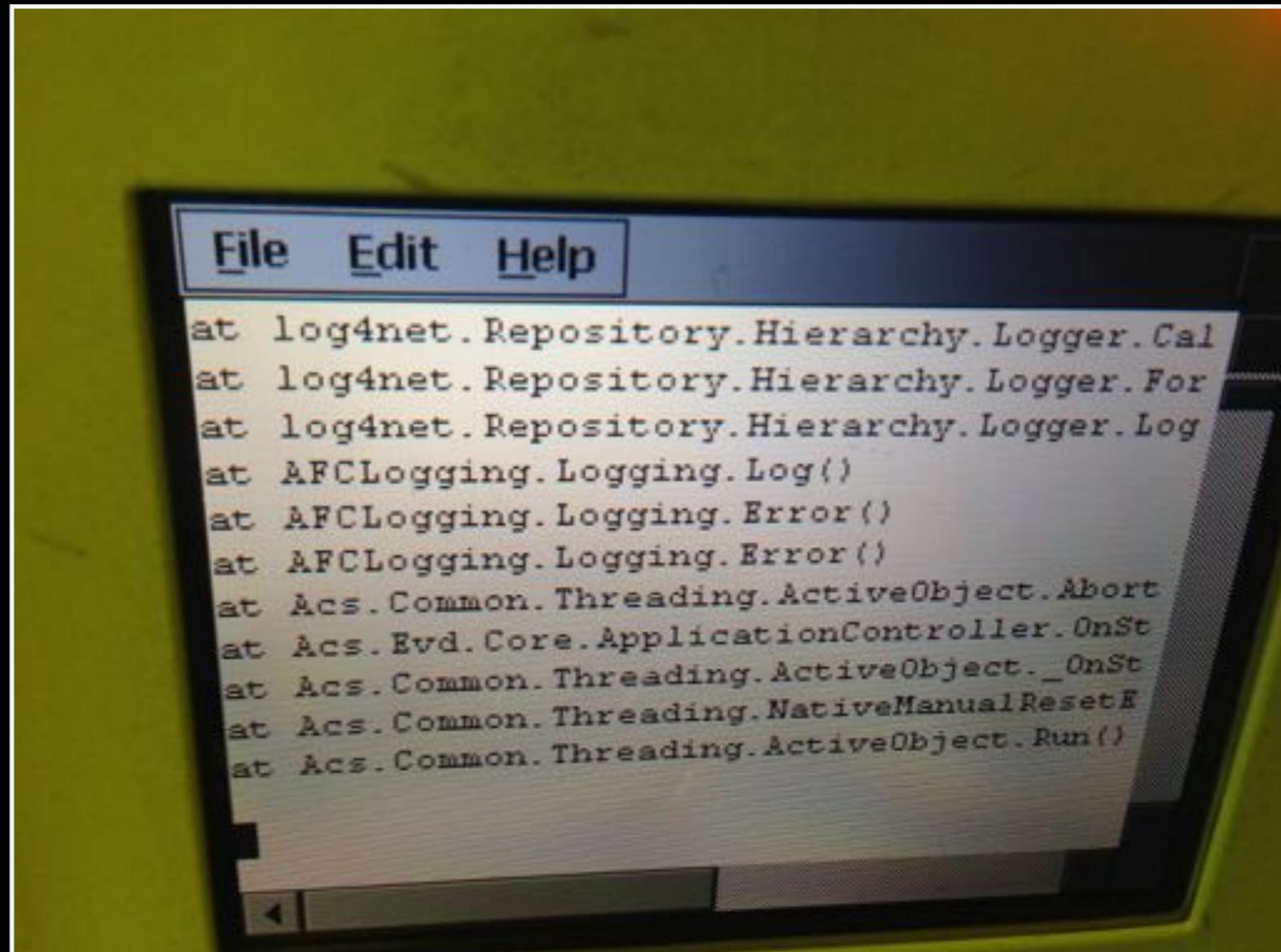


Transport stuff...



ASSURANCE

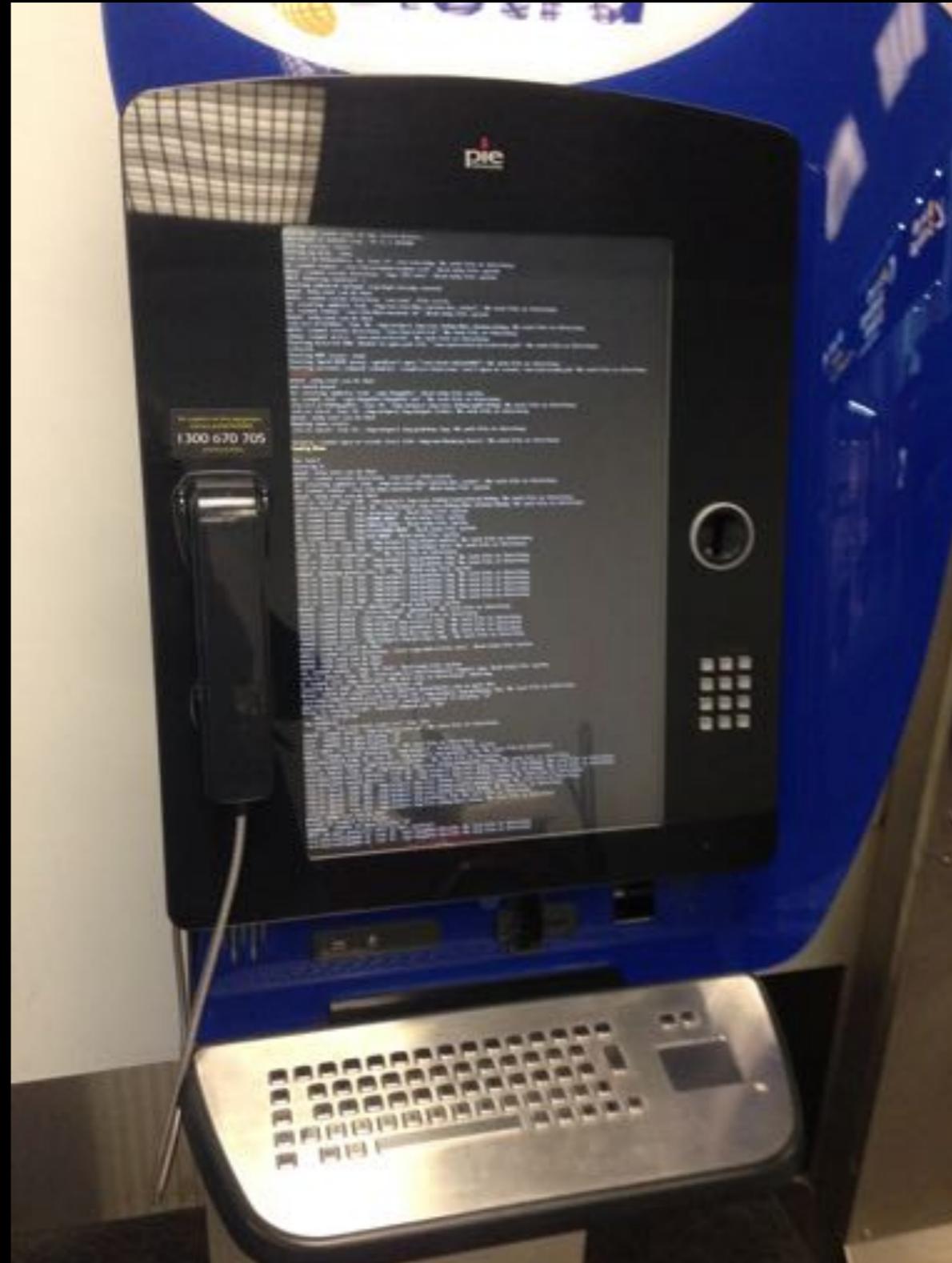
Transport stuff... myki



Transport stuff in Melb



Those PIE terminal things in airports



This one recently disappeared

TRS-80 Model 100 used by City of Hobart to show tidal activity



THE MICRO EXECUTIVE WORKSTATION™



NEW FOR 85

8K Model 100
799⁰⁰

As Low As \$45 Per Month
On OnLine Credit

28K Model 100
999⁰⁰

As Low As \$56 Per Month
On OnLine Credit

- Five Built-In Executive Management Programs
- Weighs Less than 4 lbs.
- Full-Size Typewriter Keyboard
- Self-Contained Direct-Connect Modem
- 8-Line by 40-Character Liquid Crystal Display
- Memory Expands to 32K

TRS-80™ Model 100. So small it'll fit in your in-basket! The Model 100 is a true portable since it runs on batteries or optional AC adapter. And with its five built-in programs, Model 100 is truly revolutionary. Produce connection-free memos, letters and reports with the personal word processing program, TEXT. Editing functions include finding, duplicating, deleting and moving text. With an optional printer, you can print any of your files in selectable widths (up to 132 columns) without spilling words. SCHEDL turns the Model 100 into a mini-database for appointments, expenses, and "to-dos." And file away names, addresses and phone numbers with ADDRESS.

Who is the Model 100 for?

This portable computer provides a convenient workstation for executives, managers, researchers, students—anyone who wants immediate computing power when-

More Built-In Features. With its TELCOM program and built-in auto-dial modem, Model 100 can be used as a terminal for computer-to-computer communications or to access information services like Dow Jones News/Retrieval® or CompuServe®. There's even a program to automatically dial your phone! Programmers will love Model 100's Microsoft® BASIC—an enhanced version of our popular Model III BASIC. You get full string handling, complete file operations, multi-dimension arrays, 14-digit double-precision math operations and more. Separate internal nickel-cadmium batteries retain memory data with power off.

Complete Interface Capability. Connect your Model 100 to any Radio Shack dot-matrix, daisy-wheel or graphics printer via the parallel interface. With the RS-232C interface, Model 100 can be connected to another computer—micro, mini or main-frame. The cassette interface lets you

Use the TRS-80 Model 100



On Your Desk

Or on the Go

Specifications

Microprocessor: 8-bit 80C85 CMOS. **Clock Speed:** 2.4 MHz. **Memory:** 32K ROM, 8 or 24K RAM, expandable to 32K. **Keyboard:** Full-size 58-key typewriter style with embedded 10-key display, plus 8 programmable function keys, 4 command keys and 4 cursor control keys. **Display:** 8x40 Liquid Crystal Display, upper and lower case ASCII characters, 240x64-dot-matrix graphics. **Modem:** Built-in, FCC-regulated direct-connect modem with auto-dialer, 300 baud Originate and answer. **Input/Output:** Parallel printer interface, RS-232C serial communications interface programmable up to 19,200 baud. **Cassette tape interface:** loads at 1500 baud. **Standard two-color water interface.** **Dimensions:**

visualising these things



Take the known to infer the unknown

Inductive reasoning?

Use what I think of as “hacker’s intuition” plus every bit of information you can grab

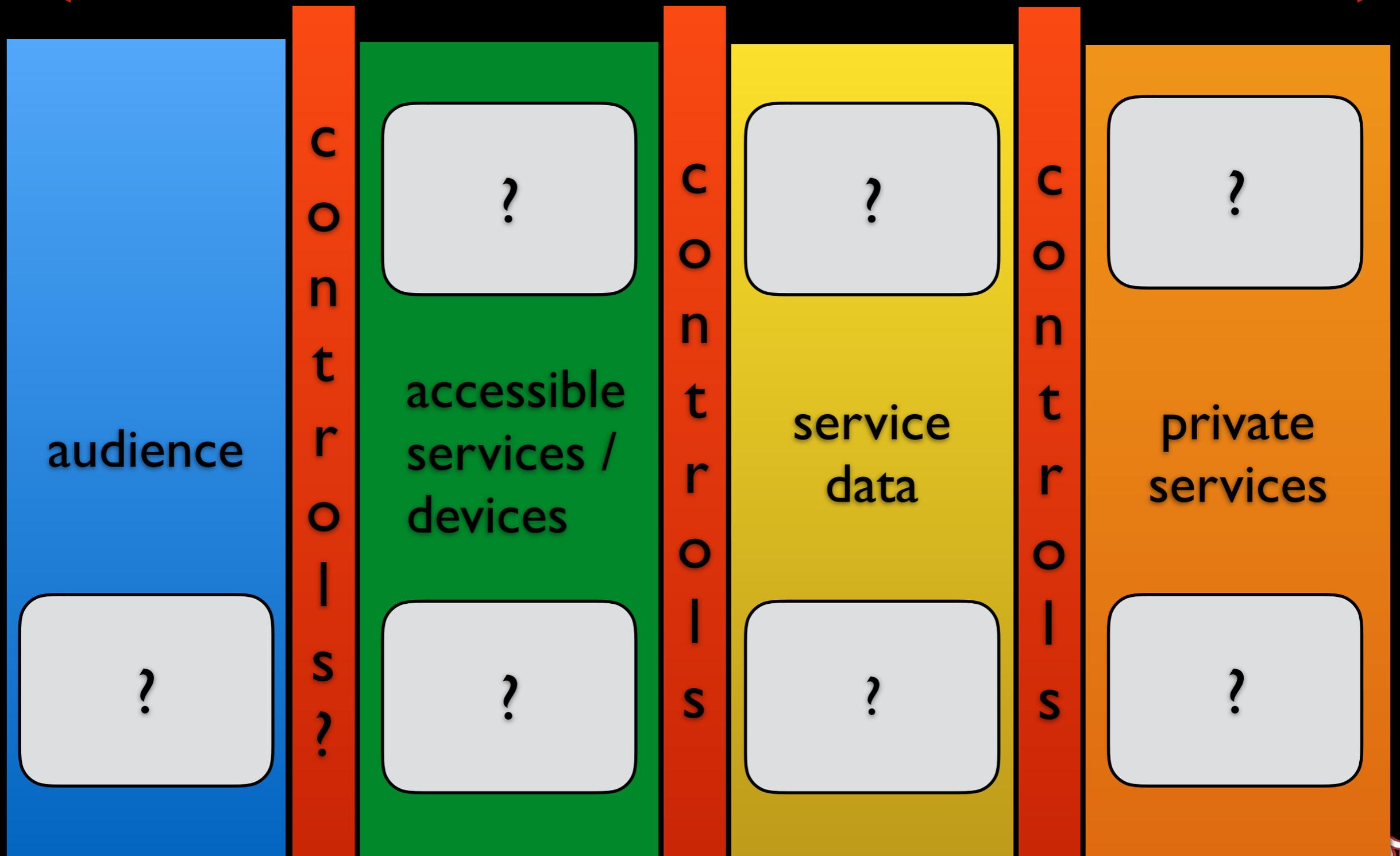
Take parts you can observe + your experience to prove your threat premise



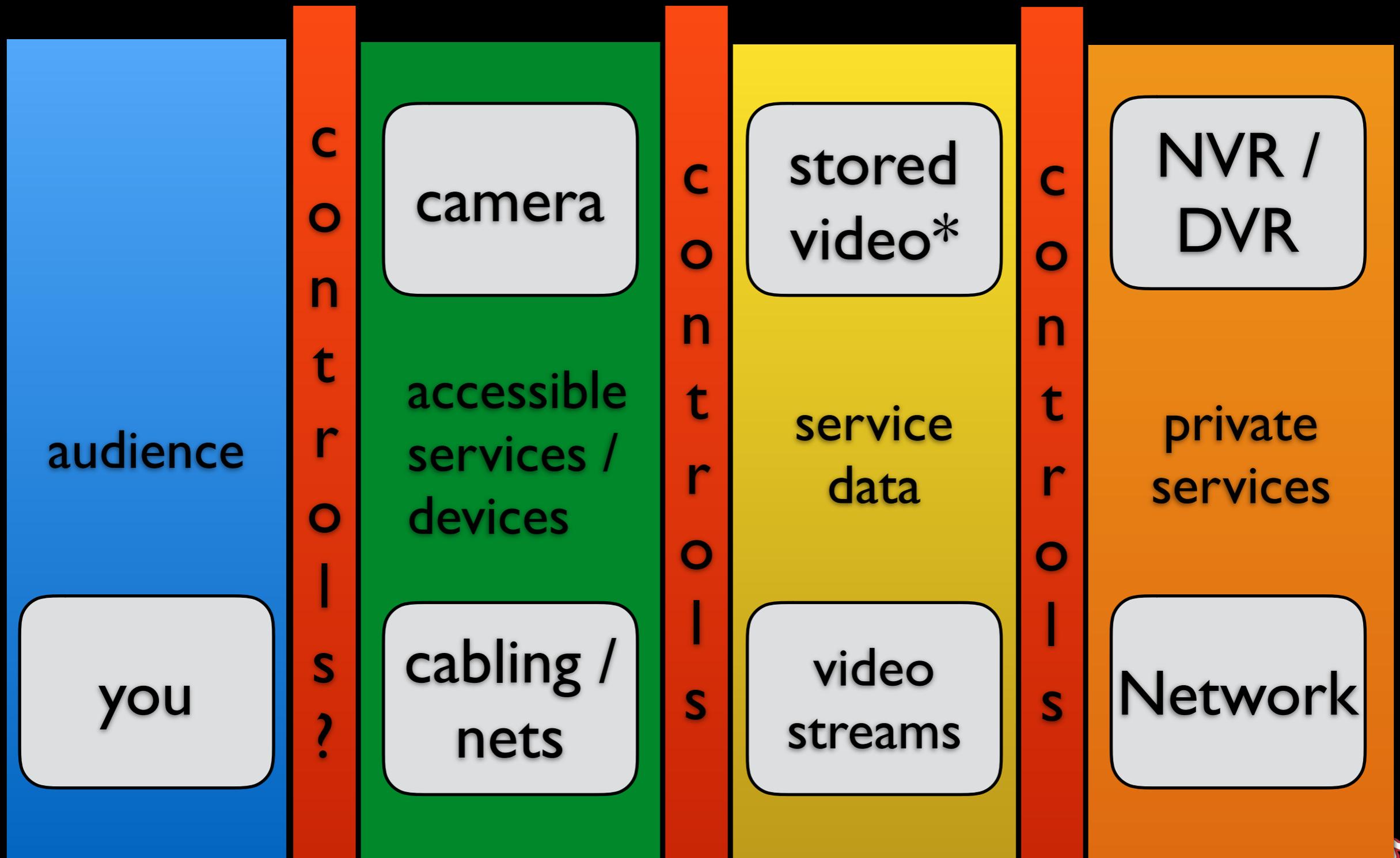
How I look at these

more accessible

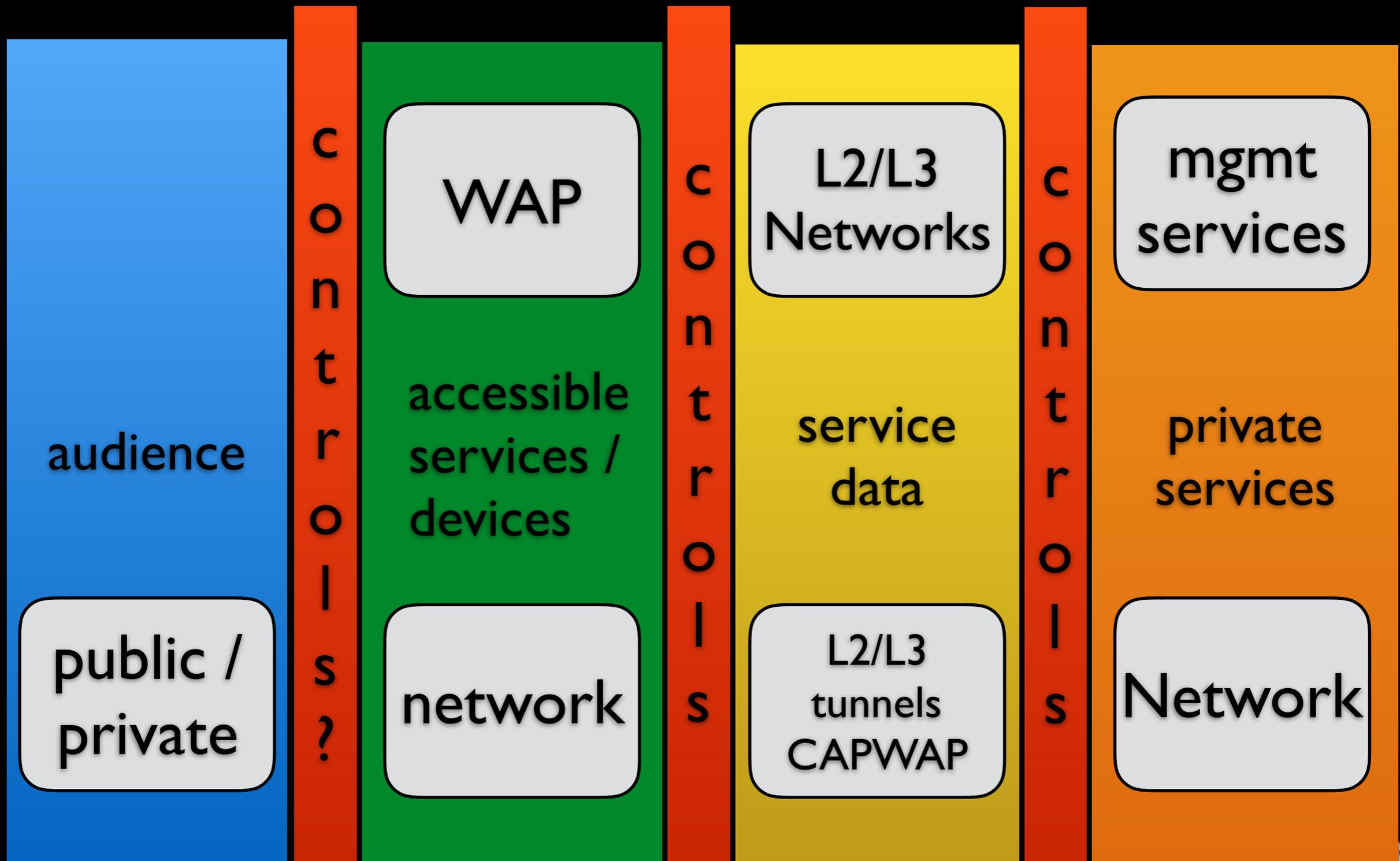
less accessible



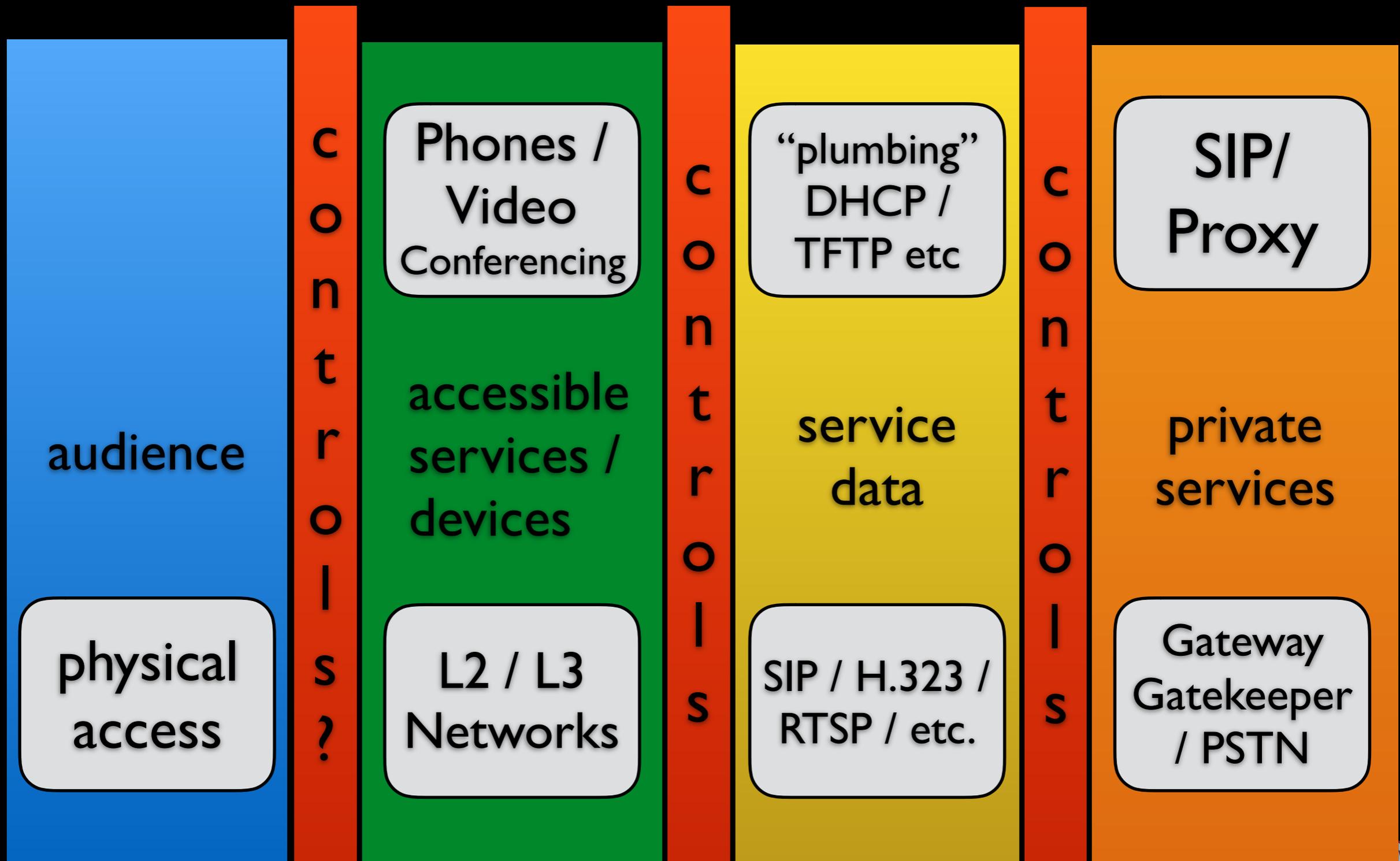
CCTV



802.11



VOIP



Opportunistic attack

Applying this thinking to accessible technology in the course of looking at your life / job / whatever critically



obvious process

Visual observation to collect identifiable details
=> “research”

Passive connection to target to ^^^
=> “research”

Active connection to target to ^^^
=> “research”



toys

Opportunity	Accessible device
Motive	Not enough coffee
Means	Toys like Dualcomm Ethernet “tap” (it’s not exactly a tap); UBNT USB wifi; HackRF



Demo: passive recon on a VoIP solution using a mirror tap

“Passive” port mirror tap using a Dualcomm

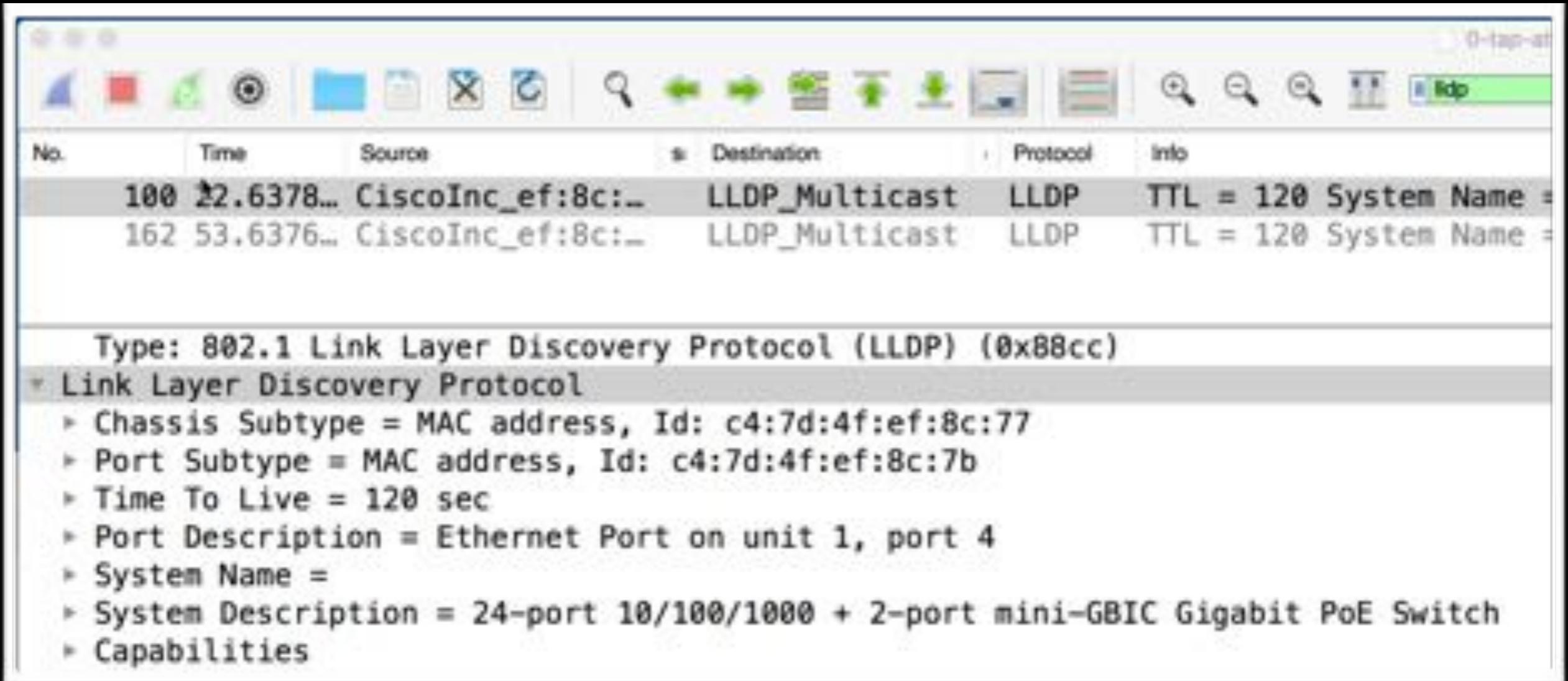
Pass through 802.3af Power over Ethernet from port 1 to port 2

“Mirror” port 1/2 to port 5 for sniffing

Wireshark on an interface configured to not request a DHCP address



CDP/LLDP



The image shows a Wireshark packet capture window. The top toolbar includes various icons for file operations, search, and network analysis. The main display area shows a table of captured packets:

No.	Time	Source	Destination	Protocol	Info
100	22.6378...	CiscoInc_ef:8c:...	LLDP_Multicast	LLDP	TTL = 120 System Name =
162	53.6376...	CiscoInc_ef:8c:...	LLDP_Multicast	LLDP	TTL = 120 System Name =

Below the packet list, the details pane shows the structure of the selected LLDP frame:

- Type: 802.1 Link Layer Discovery Protocol (LLDP) (0x88cc)
- Link Layer Discovery Protocol
 - Chassis Subtype = MAC address, Id: c4:7d:4f:ef:8c:77
 - Port Subtype = MAC address, Id: c4:7d:4f:ef:8c:7b
 - Time To Live = 120 sec
 - Port Description = Ethernet Port on unit 1, port 4
 - System Name =
 - System Description = 24-port 10/100/1000 + 2-port mini-GBIC Gigabit PoE Switch
 - Capabilities



CDP/LLDP

```
▼ Management Address
  0001 000. .... = TLV Type: Management Address (8)
  .... ...0 0000 1100 = TLV Length: 12
  Address String Length: 5
  Address Subtype: IPv4 (1)
  Management Address: 10.1.1.5
  Interface Subtype: ifIndex (2)
  Interface Number: 1001
  OID String Length: 0
```

management IP address

likely in same L3 network available at port



DHCP options

No.	Time	Source	Destination	Protocol	Info
137	88.4919	10.1.1.90	255.255.255.255	DHCP	DHCP Request
138	88.4923	10.1.1.1	255.255.255.255	DHCP	DHCP ACK
141	88.5039	10.1.1.90	255.255.255.255	DHCP	DHCP Request
142	88.5043	10.1.1.1	255.255.255.255	DHCP	DHCP ACK

Length: 4
IP Address Lease Time: (7200s) 2 hours

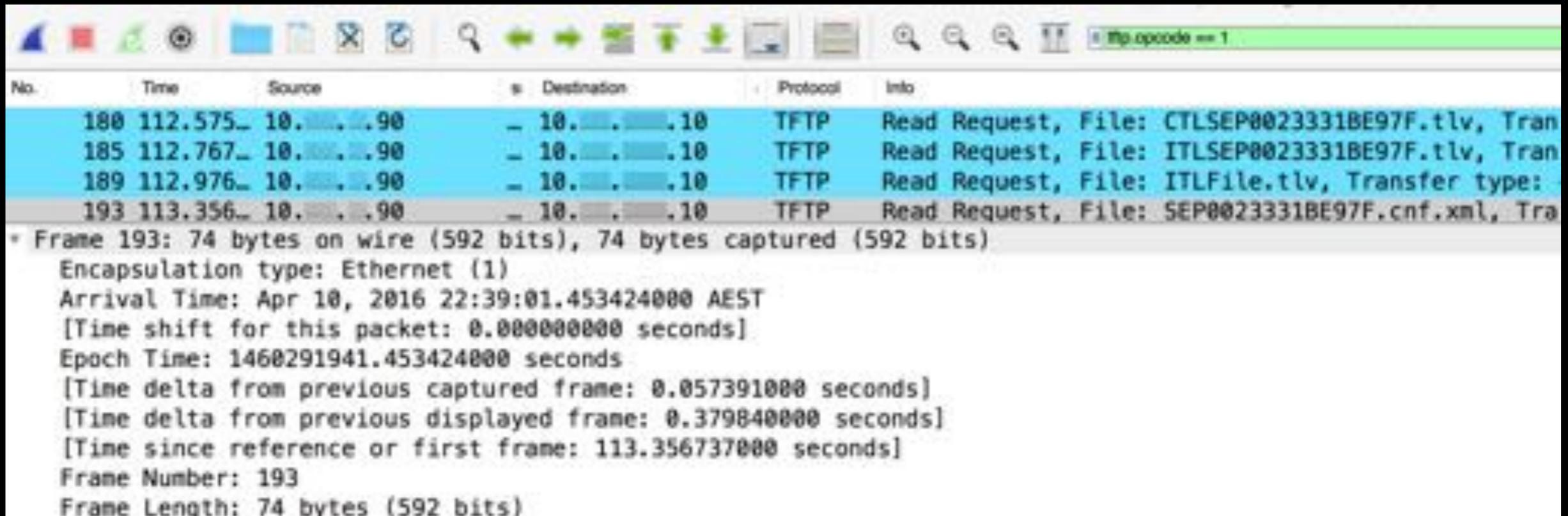
- Option: (1) Subnet Mask
Length: 4
Subnet Mask: 255.255.255.0
- Option: (66) TFTP Server Name
Length: 12
TFTP Server Name: 10.1.1.10
- Option: (6) Domain Name Server
Length: 4

TFTP server specified by DHCP

- common for phone, camera provisioning
- May also be SIP server



TFTP provisioning



The image shows a Wireshark network traffic capture. The top toolbar includes various icons for file operations and search. A filter bar at the top right shows the filter 'tftp.opcode == 1'. The main display area contains a table of captured packets and a detailed view of packet 193.

No.	Time	Source	Destination	Protocol	Info
180	112.575...	10.0.0.90	10.0.0.10	TFTP	Read Request, File: CTLSEP0023331BE97F.tlv, Tran
185	112.767...	10.0.0.90	10.0.0.10	TFTP	Read Request, File: ITLSEP0023331BE97F.tlv, Tran
189	112.976...	10.0.0.90	10.0.0.10	TFTP	Read Request, File: ITLFile.tlv, Transfer type:
193	113.356...	10.0.0.90	10.0.0.10	TFTP	Read Request, File: SEP0023331BE97F.cnf.xml, Tra

* Frame 193: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Apr 10, 2016 22:39:01.453424000 AEST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1460291941.453424000 seconds
[Time delta from previous captured frame: 0.057391000 seconds]
[Time delta from previous displayed frame: 0.379840000 seconds]
[Time since reference or first frame: 113.356737000 seconds]
Frame Number: 193
Frame Length: 74 bytes (592 bits)

TFTP server “Read Request”
-wireshark display tftp.opcode == 1



Passive TFTP collection

The image shows a Wireshark capture of TFTP traffic. The packet list pane at the top shows four packets:

No.	Time	Source	Destination	Protocol	Info
194	113.400...	10.1.1.10	10.1.1.10	TFTP	Data Packet, Block: 1
195	113.400...	10.1.1.10	10.1.1.10	TFTP	Acknowledgement, Block: 1
196	113.445...	10.1.1.10	10.1.1.10	TFTP	Data Packet, Block: 2
197	113.446...	10.1.1.10	10.1.1.10	TFTP	Acknowledgement, Block: 2

The packet details pane shows the XML configuration data for the second data packet (Block 2):

```
....<?xml version="1.0" ?>
<device>
  <deviceProtocol>SIP</deviceProtocol>
  <sshUserId>root</sshUserId>
  <sshPassword>cisco</sshPassword>
  <devicePool>
    <dateTimeSetting>
      <dateTemplate>0/M/Ya</dateTemplate>
      <timeZone>AUS Eastern Standard/Daylight Time</timeZone>
      <ntp>
        <ntp>
          <name>10.1.1.1</name>
          <ntpMode>Unicast</ntpMode>
        </ntp>
      </ntp>
    </dateTimeSetting>
    <callManagerGroup>
      <members>
        <member priority="0">
          <callManager>
            <processNodeName>10.1.1.10</processNodeName>
            <ports>
              <sipPort>5060</sipPort>
            </ports>
          </callManager>
        </member>
      </members>
    </callManagerGroup>
  </devicePool>
</device>
```

The interface at the bottom shows the stream data as ASCII and a search bar.

Phone configuration via TFTP confirms SIP server IP



Passive TFTP collection

```
<line button="1" lineIndex="1">
  <featureID>9</featureID>
  <featureLabel>Extension: 708</featureLabel>
  <proxy>USECALLMANAGER</proxy>
  <port>5060</port>
  <name>====</name>
  <authName>====</authName>
  <authPassword>=====</authPassword>
  <messageWaitingLampPolicy>3</messageWaitingLampPolicy>
  <messagesNumber>+97</messagesNumber>
  <displayName></displayName>
  <contact></contact>
  <autoAnswer>
    <autoAnswerEnabled>2</autoAnswerEnabled>
  </autoAnswer>
  <featureOptionMask>1</featureOptionMask>
  <callWaiting>3</callWaiting>
  <sharedLine>>false</sharedLine>
  <messageWaitingAMWI>1</messageWaitingAMWI>
  <ringSettingIdle>4</ringSettingIdle>
  <ringSettingActive>5</ringSettingActive>
  <forwardCallInfoDisplay>
    <callerName>>true</callerName>
    <callerNumber>>false</callerNumber>
    <redirectedNumber>>false</redirectedNumber>
  <dialNumber>true</dialNumber>
```

SIP server registration details



mitigations

Monitor network-connected device presence - if things reboot, disappear/reappear find the root cause

For devices \leftrightarrow services mutual auth with strong transport encryption but know its limitations - 802.1x/NAC, Locally Significant Certificates / TLS for SRTP/ZRTP, etc.

Where possible apply “port security” or MAC- filter controls to only permit known L2 devices. These are defeat-able but help



Thanks BSides

web:

www.assurance.com.au

twitter:

[@assurance](https://twitter.com/assurance) [@y011](https://twitter.com/y011)

ASSURANCE

