UNIVERSITY OF
LEICESTER

Guide to Securing Surveillance Camera Devices.

Andrew Gahagan

2nd January 2018

Hardening the IP Cameras (Prior to installation on the network)

Firstly upgrade to latest firmware. We tested the following settings with Bosch common platform CPP4 firmware version 6.42.0021.

The installer should be aware of the IP address assigned to the device however DHCP is still to be utilised.

New deployments must use the IP Camera Password Generator script which generates unpredictable, stable passwords based on devices' IP addresses and meet the minimum password conditions of:-

- Passwords should be between 8 and 12 charters in length.
- Passwords should contain both upper and lower-case letters.
- Passwords should contain at least one special character.
- Passwords should contain at least one digit.

Password stored on the device should be protected as part of the TPM and AES256 encrypted minimum. The device password should never be written in any form, passwords should only be generated by the application issued.

Support secure communication over HTTPS for end to end encryption. Insecure or none required ports and communication protocols (i.e. http, telnet, rcp, RTSP, SNMP, UPnP, SNTPv1 & v2 etc) should be turned off. As well as any cloud services which may be running on the device.

IPv4 address filtering with a minimum of 2 IP address ranges to limit access to the campus network to prevent accidental Internet exposure:

Network -> IPv4 Filter -> 143.210.0.0 mask 255.255.0.0, 10.0.0.0 mask 255.0.0.0

Support TLS-Date Protocol and time servers set to **143.210.16.11**

HTTPS traffic must use TLS 1.2 protocol utilising the AES cipher suite, early TLS and SSLv2 & v3 are not acceptable.

Specific server certificates, client certificates and trusted certificates must be updated and configured on the device.

Any none required user accounts not used should be removed.