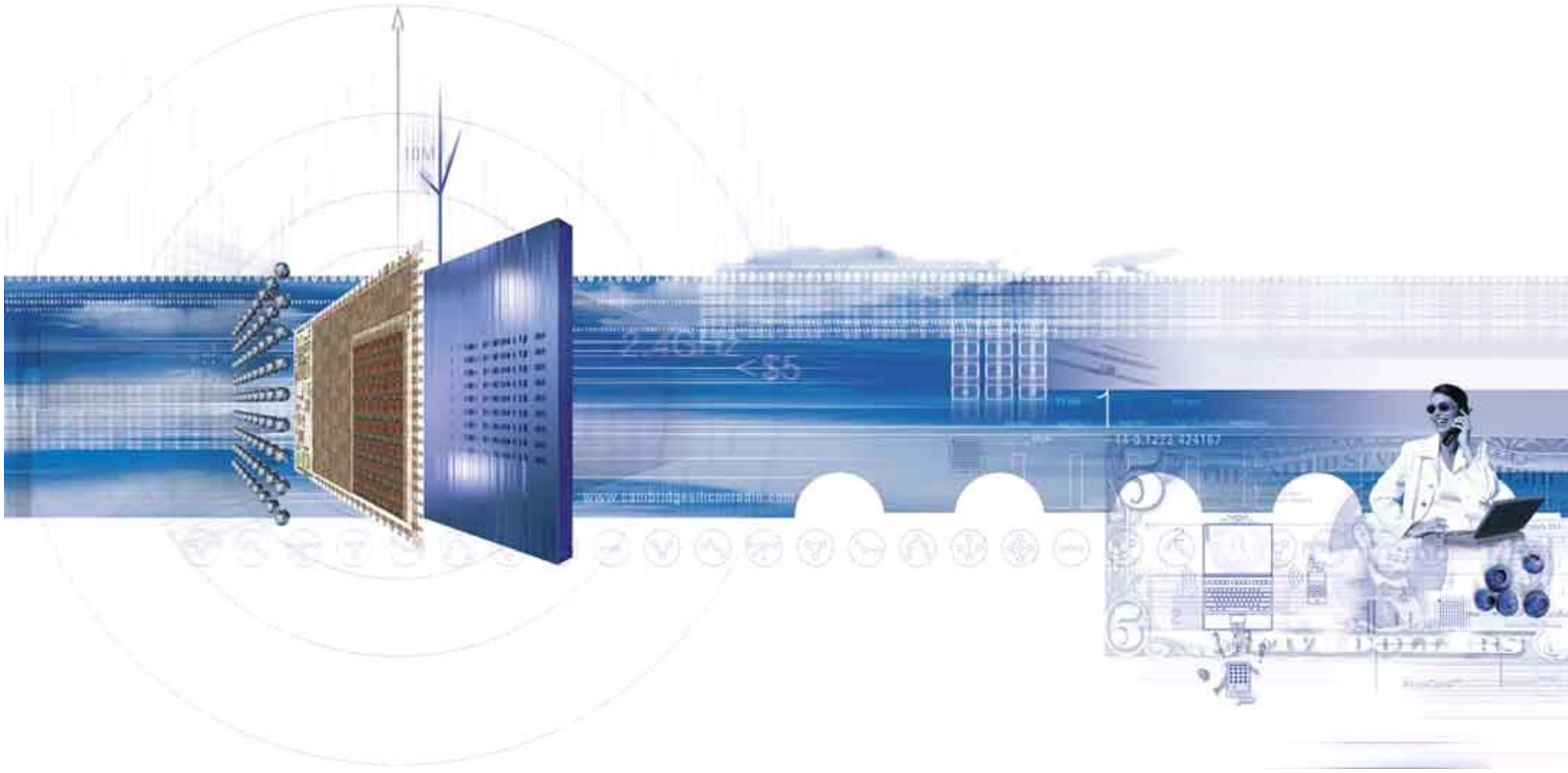
BlueCore™

BCHS Security Note

March 2004



CSR

Cambridge Science Park
Milton Road
Cambridge
CB4 0WH
United Kingdom

Registered in England 3665875

Tel: +44 (0)1223 692000
Fax: +44 (0)1223 692001
www.csr.com

Contents

1 Bluesnarfing and Bluejacking

1.1 Introduction

This note describes the security hazards known as Bluesnarfing and Bluejacking and discusses the robustness of BCHS to these attacks. CSR concludes that devices running BCHS are protected from these methods of attack.

Bluesnarfing attacks are based on the lack of security in some legacy OBEX stacks which allow an unauthenticated attacker to gain access to confidential data by the use of malformed data packets as described in section 1.3.

Bluejacking is when someone (you do not know) tries to push an OBEX card to you. In most phone UI a notification message is shown in the display, for example "Do you wish to store card from XXX?" Bluejacking does not constitute a security risk, it is merely an annoyance; to avoid storing the card, one can always just respond "No", and the card push service can be disabled to avoid Bluejacking.

An additional risk is that certain UI do not actually delete the authentication information of a device if it is deleted from the list of trusted (a.k.a. paired) devices displayed by the UI. Thus, although the user believes the device will no longer be allowed access to his data, in fact that device would still be allowed to connect and access data.

1.2 Bluetooth Security

The link manager security features can be used in different security modes. These are defined in the Bluetooth® Generic Access Profile. Three security modes are defined:

Security mode 1 (non-secure), i.e., a device will not initiate any security procedure. This is normally only used for very specific products that rely on application level security.

Security mode 2 (service-level enforced security) where a device does not initiate security procedures before channel establishment at L2CAP level. This mode allows different and flexible access policies for applications, especially running applications with different security requirements in parallel. This is the security mode used in most products. For RFCOMM based profiles, security policies are individually set for each RFCOMM server channel.(1)

Security mode 3 (link level enforced security). In mode 3 a device initiates security procedures before the link set-up at the link manager level is completed. That is, all connecting devices will be authenticated.

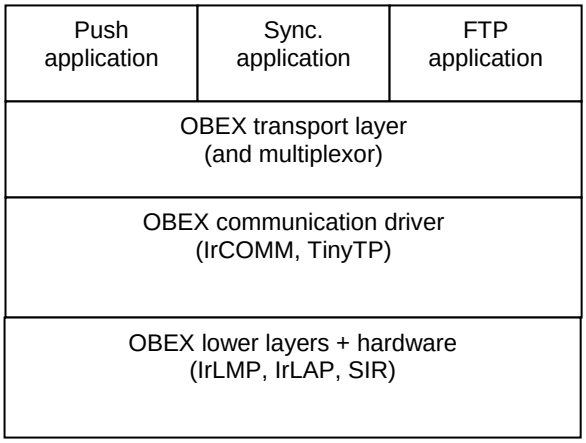
In addition, some Bluetooth profiles allow for application level security although these are rarely implemented.

These security features of Bluetooth provide good security at the link level, supporting both authentication and encryption, and in fact none of the successful attacks discussed in the media have been attacks on the Bluetooth security Itself.

(1) RFCOMM server channel is a logical channel number used to distinguish between different emulated serial ports

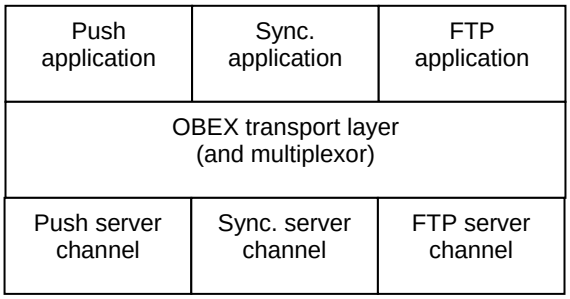
1.3 Bluesnarfing

This is an attack on the legacy layer known as OBEX (OBject EXchange), which was originally devised for Infra-Red communications. A typical OBEX stack has the following layers:



In concurrent OBEX services the OBEX specification has defined a connection identifier (arbitrary number chosen by the server side) that is included in all (except the first from the client) OBEX packets. This connection identifier is used to multiplex between the different services. The multiplexing is normally done in the transport layer. There is no link level security, but application layer security may be enforced.

When a legacy OBEX stack is used above a Bluetooth stack the typical layers are:



The reason for using a separate server channel per service is to enforce Bluetooth service level security into the hitherto insecure OBEX system. Typically there is no security enforced for the Push application but authentication and encryption is mandatory for the Sync. service and optional (but normally enforced) for the FTP service.

The hazard arises because in some implementations the multiplexing, and thus routing, of the traffic through the OBEX transport layer is done solely on the OBEX connection identifier. Thus if an insecure connection is set up to the Push channel and then the packets sent over this channel are deliberately malformed by the attacker so that the OBEX connection identifier is for FTP (or Sync.) rather than for the Push service, the OBEX transport layer will obey this routing directive and serve the FTP (or Sync.) application information.

By this means it is possible to avoid the (robust) Bluetooth service level security mechanism for Sync. and FTP and gain access to the PIM or file transfer services without invoking authentication.

This hazard could have been avoided by using application level security, and indeed support for application level security is mandatory for all Bluetooth OBEX profiles except for the push profile. However few implementations enforce application level security.

1.4 General BCHS Security Features

BCHS supports all mandatory and optional Bluetooth security features and, in addition, the BCHS profiles support application level security. Application layer access to the Bluetooth security features is provided by the BCHS Security Controller API.

1.5 BCHS and Bluesnarfing

BCHS contains an OBEX transport layer written by CSR specifically for use with Bluetooth. It multiplexes on server channel information instead of connection identifiers hence, even if the OBEX connection identifiers are malformed, a Bluetooth connection established to the Push server channel will never be connected to the PIM or file transfer services. Bluesnarfing is not possible with BCHS.

1.6 BCHS and Bluejacking

All BCHS profiles can be activated or deactivated individually; some other implementations force all OBEX services to be on or all to be off.

So it is possible to activate the OBEX Sync. and FTP servers without activating the OBEX Push server. By this means one can avoid the nuisance of Bluejacking without foregoing the services one does want.

1.7 BCHS and Stored Link Keys

When a previously paired device is unpaired, the BCHS Security Controller ensures that link keys are removed from both the persistent storage in the host and in the BlueCore™ chip. This eliminates the third security hazard referred to in section 1.1.

Record of Changes

Date	Revision	Reason for Change
10 MAR 04	a	Original publication of this document. (CSR reference: bcore-me-028Pa)

BCHS Security Note

bcore-me-028Pa

March 2004

BlueCore™ Host Software