



Developers Conference 2007

Amsterdam, The Netherlands



Certified Wireless USB Security & Association Models

Preston Hunt

Chair & Editor, Association Model Working Group
Intel Corporation

Agenda



- Why security and association matter
- Basics review
- Errata
- Common implementation questions
- Future enhancements for Wireless USB 1.1

Why Security Matters



Go to SC M



News

Mobile virus infects Lexus cars

by David Quainton

Lexus cars may be vulnerable to viruses that infect mobile phones. Landcruiser 100 models LX470 and LX570 are affected.



tom's networking

How To: Building a BlueSniper Rifle – Part 1

A Toronto Man faces charges after being arrested for "War-Driving" around Toronto neighborhoods, using unsecured networks to download child-pornography.



It is what IT is.

Car RFID Security System Cracked



Association and Security

- **Association** defines first time setup for Wireless USB products
 - Association is the interface with the user
 - Ease of use is very important
 - Security is equally important – most attacks are during setup
- Once products are associated, **security** defines operational encryption
 - Crypto specifics: handshakes, encryption algorithms, message authentication, key rotation, etc.
 - Users don't see any of this
- **Connection context**
 - Tuple [CHID, CDID, CK]
 - Association sets it up, security uses it



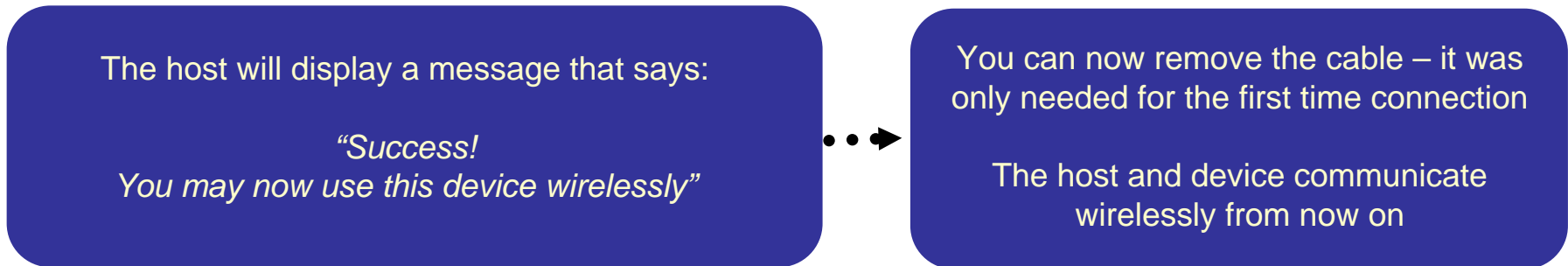
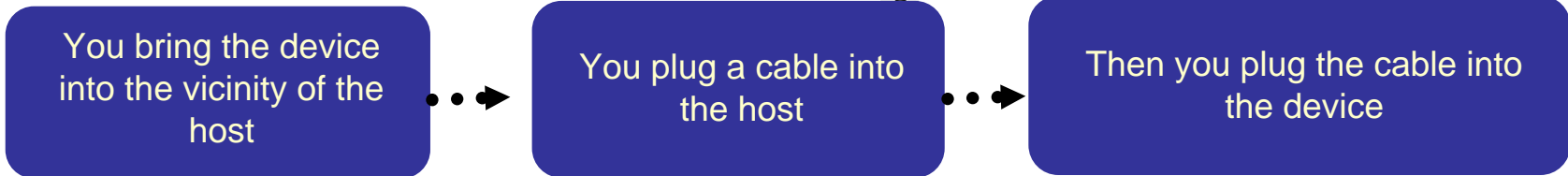
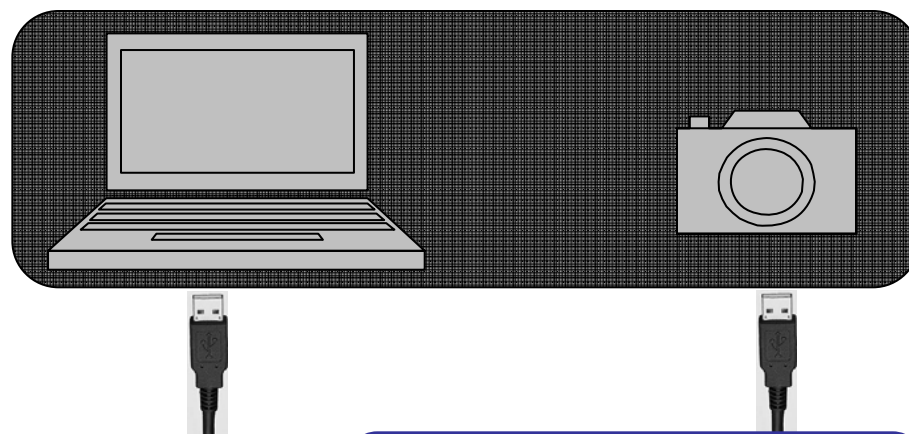
Wireless USB 1.0 Logo Requirements

- Two models: Cable and Numeric
- Hosts **must** support cable and numeric
 - Limited hosts/DRDs need only support TPL list
- Devices with USB ports **must** support cable model
- Devices with displays **must** support numeric model
 - Diffie-Hellman also required
- Devices **must** use at least one of the above

Basics review: association

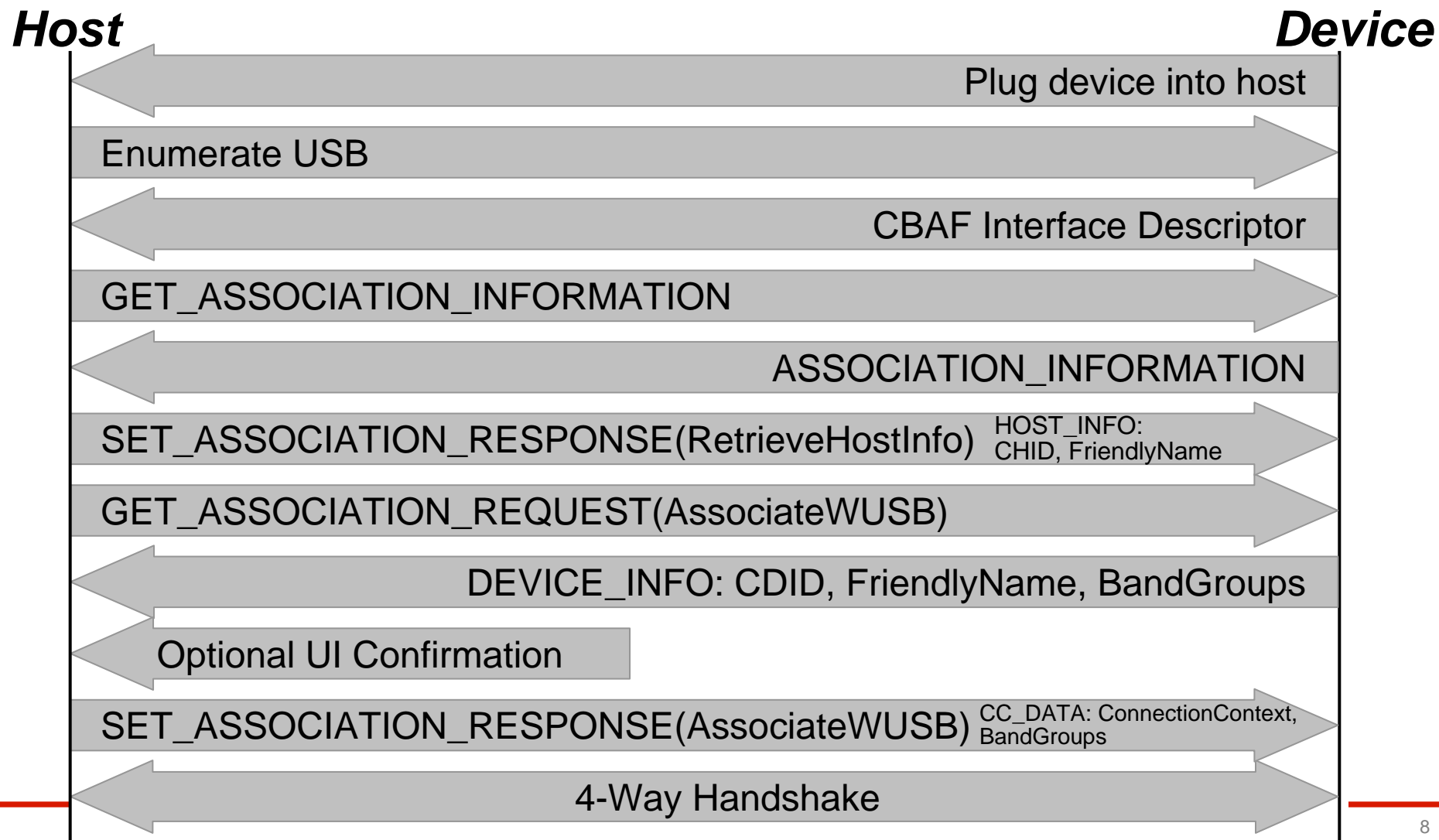


Cable Model User Experience



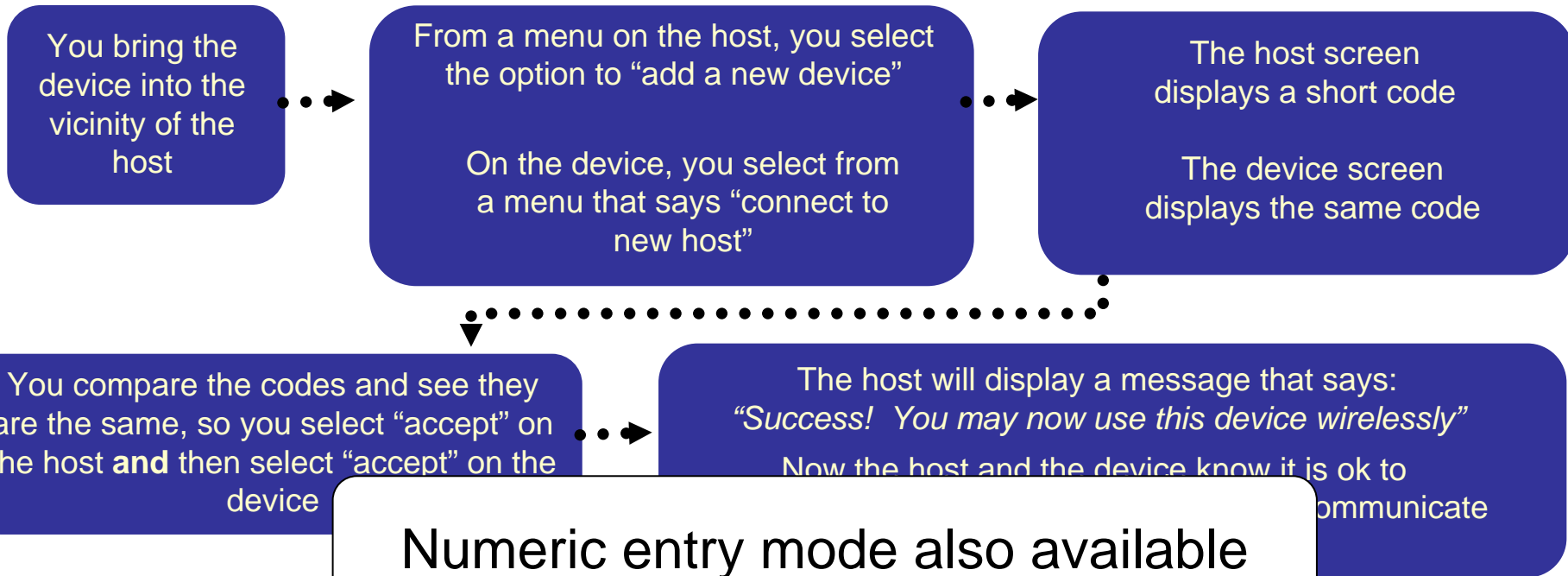
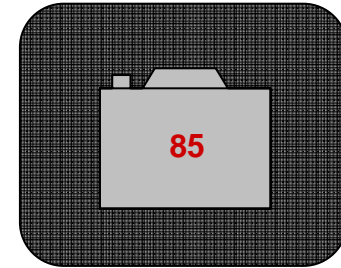
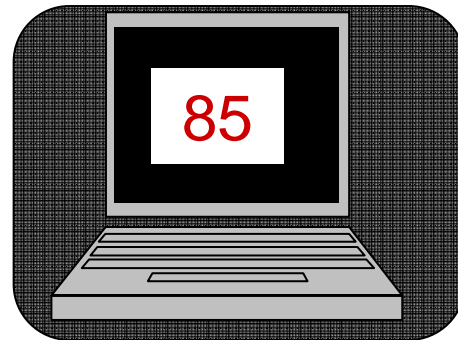


Cable Model Process





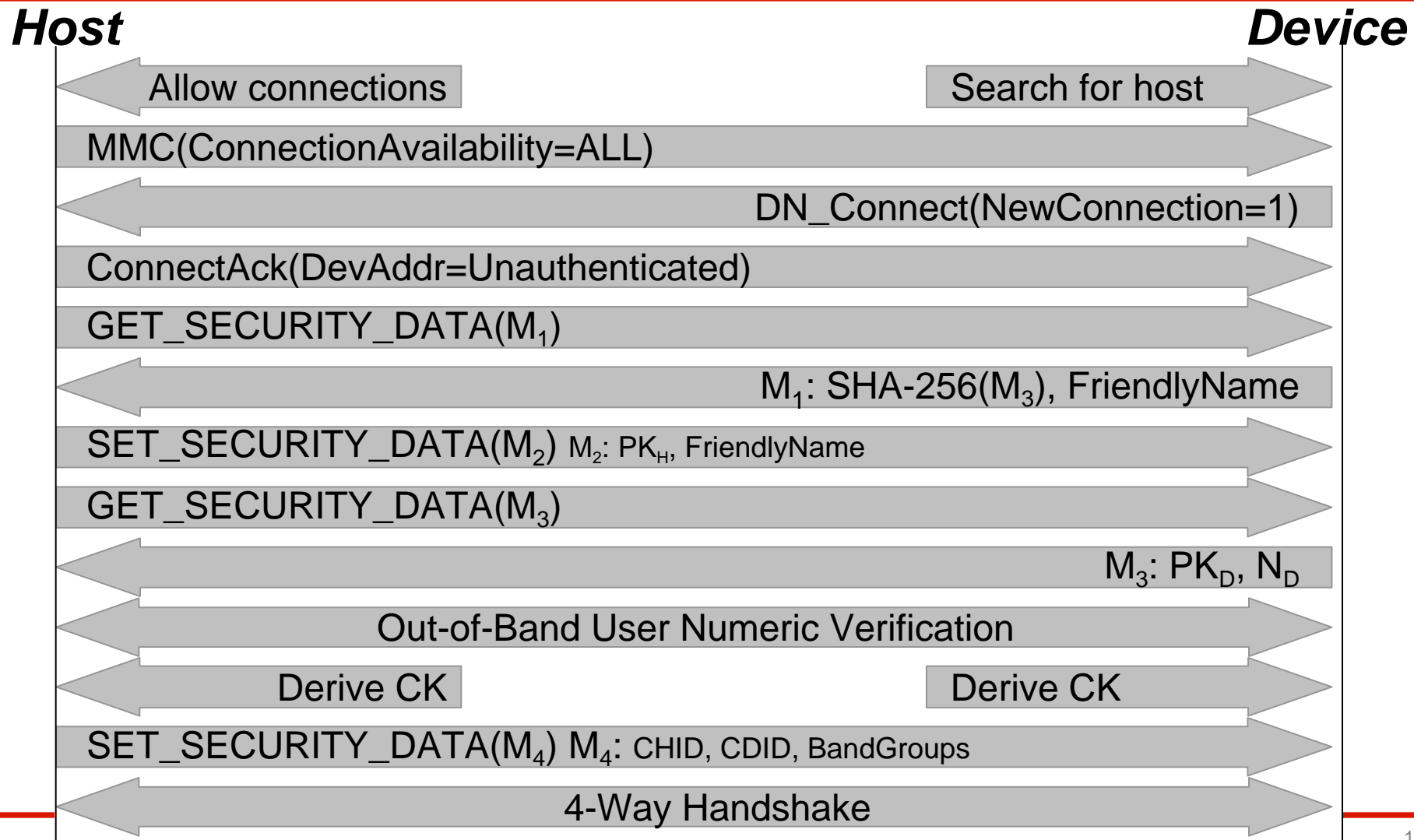
Numeric Model User Experience



Numeric entry mode also available

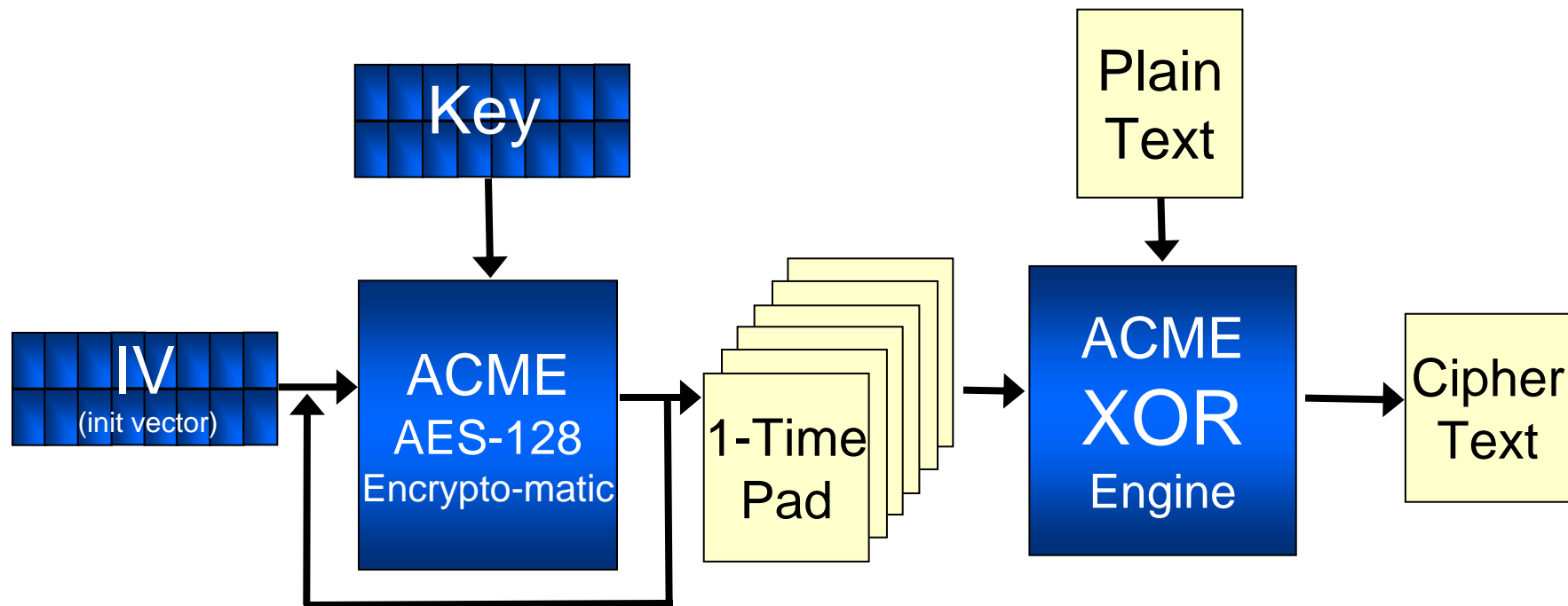


Numeric Model Process





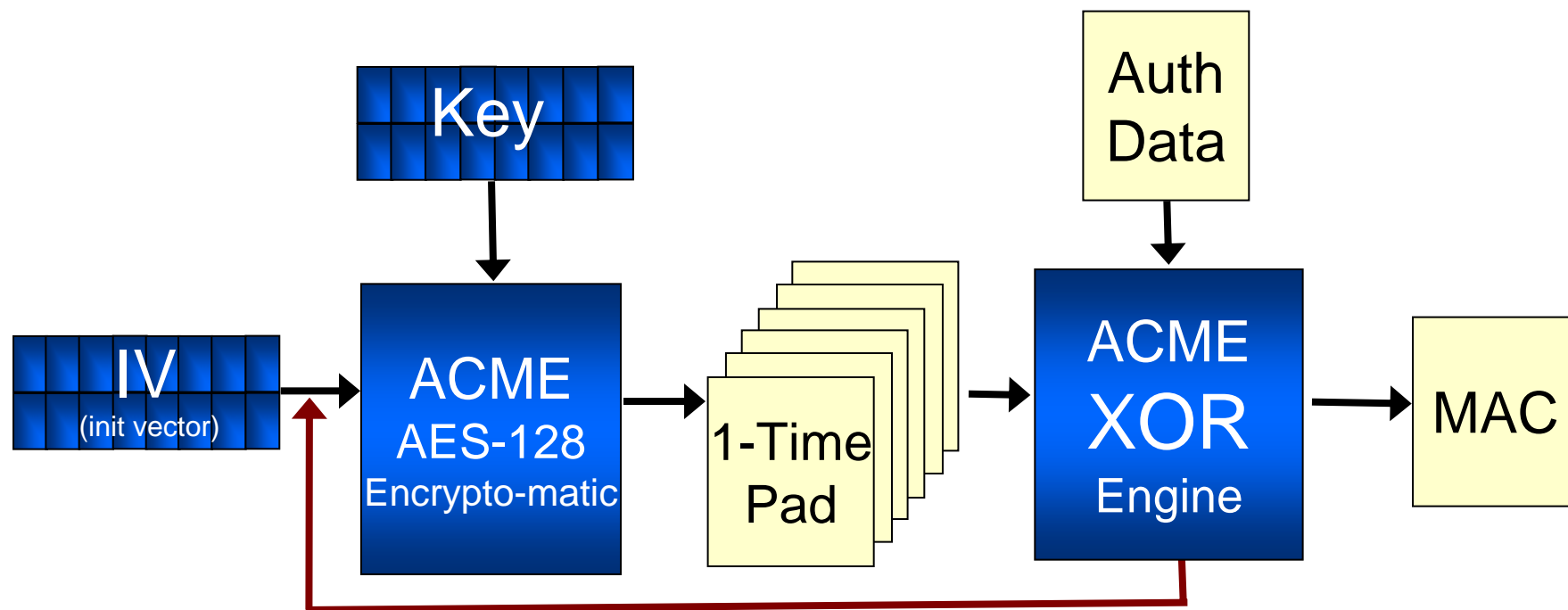
CCM Encryption/Decryption



Encryption/Decryption Identical: $PT \text{ XOR } n = CT$, $CT \text{ XOR } n = PT$



CCM Authentication





Connections: Host Startup

- Beginning of time – Host Starts Up
 - Creates GTK and gives to host controller
 - Enables host controller security
 - Starts sending MMCs with HostInfo IE
- Why secure with no connections?
 - Eliminates special “first-time” case



Secure MMC

Secure MMC

Secure MMC



Connections: Device Startup

Secure MMC → 

(Host is sending secured, plain-text MMCs)

- Device scans for MMCs
 - Security not enabled
 - MMC received as “raw packet”, security info is present, but not processed. Device must know how to parse
 - If device finds HostInfo IE of interest, device makes unsecured Connect Request



CONNECT →





Connections: Back to Host



(Device is sending unsecured Connect Requests)

- Incoming unsecured DNs are accepted
- Connect ACK sent in subsequent secured MMC



- Host queries security info descriptors
- Host starts 4-way handshake





Connections: Handshake

- All Handshake setup data delivered inside secured MMCs (not encrypted)
- All device responses delivered inside unsecured data packets. Receipt by host is legal
- Handshake payload data protected out-of-band as per command definitions





Connections: HS Completion

- Host – Install derived PTK, enable security for device



- Device – Install derived PTK, but defer enabling of security. Wait for next operation, SetKey(GTK)





Connections: SetKey(GTK)

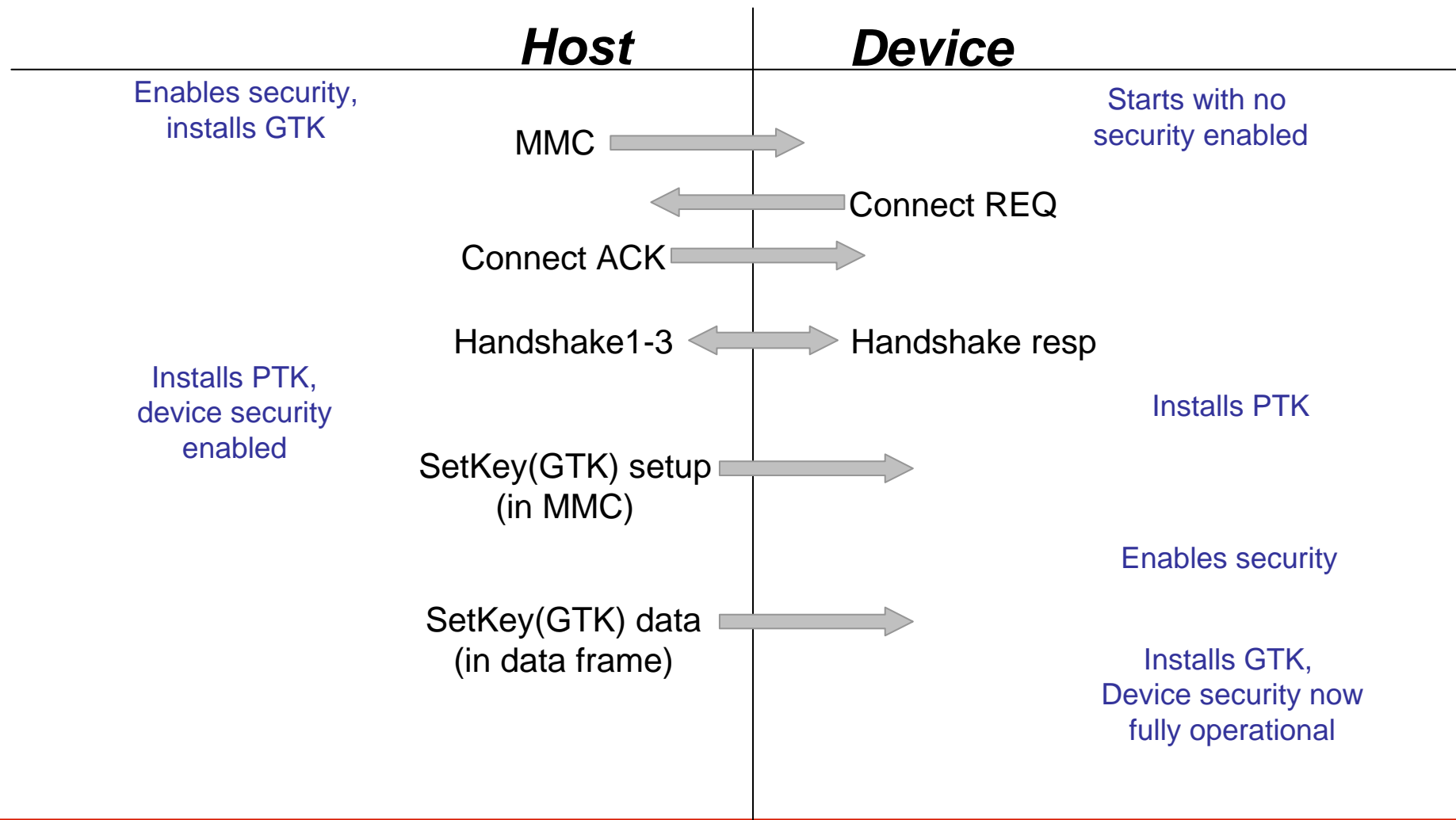
- Host – security for device fully enabled, sends SetKey(GTK) to device: MMC and secured data packet
- Device – receives MMC first:
 - Notes SetKey(GTK) setup
 - Latches SFN from MMC
 - Enables security
- Device – receives GTK key data
 - Unencrypted with PTK (part of receive processing)
 - Installs GTK with SFN from MMC as replay counter

Device and Host now both fully operational





Connections: Message Chart





Association Errata

- Internationalization
 - Microsoft Locale ID instead of UNICODE language ID
 - UNICODE UTF-16LE instead of UTF8
 - Removed redundant null termination
- Numeric model
 - Added DeviceFriendlyName to M1
 - Added HostFriendlyName to M2
- Some other minor typos/corrections



Security Errata

- Vestigial public key information removed from section 6 of Wireless USB 1.0 spec
- Cleared up ambiguity of handshake 3
- Added physical entropy requirement for random numbers
- Corrected typos and clarified examples



Endianness

- Association spec is correct! (multiple verifications)
- Any field ≤ 64 bits is a number
 - USB rules apply: Transmit little endian
- Any field > 64 bits is a byte array
 - Must be transmitted from left to right
 - Must be stored in memory from left to right, where the left-most byte is stored in the lowest memory address location
 - Applies to all UNICODE strings as well
- Use the test vectors!
- Debug traces of valid exchanges will be published



Diffie-Hellman

- Use the test vectors!
- Arnold Reinhold's Big Number Calculator is a useful tool
- ARM implementation optimized for speed is ~16KB code size
- Philip Zimmermann's bnlb is an SDK for big number arithmetic (GNU and non-GNU licenses available)

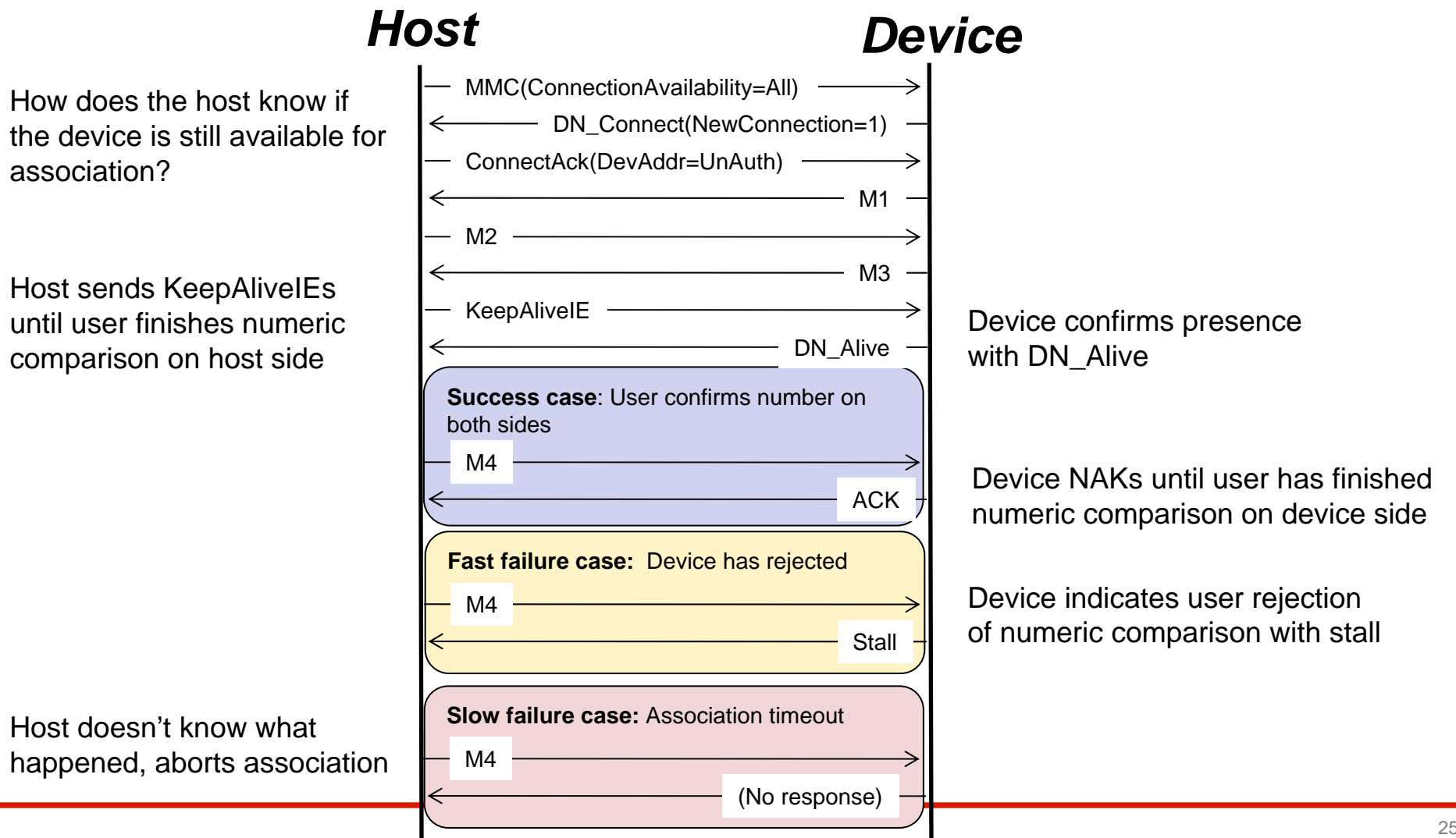


Comparison with Other Wireless Technologies

- Wireless USB, WLP, Bluetooth, WiFi all share a common user experience
 - Wireless USB, BT, and WLP have numeric comparison
 - All protocols listed have numeric entry
 - Cable model is only implemented by Wireless USB at this time, but is extensible
- Implementations are different
- Very similar from a user perspective



Device Presence Detection



Device confirms presence with DN_Alive

Device NAKs until user has finished numeric comparison on device side

Device indicates user rejection of numeric comparison with stall

Future Enhancements



- NFC (see the demo at the NXP booth)
- Discovery enhancements for association
 - Additional information provided to help provide a richer user experience



Summary

- Association and security specifications are stable
- Multiple products have passed certification
- Keep up-to-date on errata and frequently asked questions (www.usb.org/wusb)
- Implement association models and security in your products now!

**See association in action
in the demo showcase!**



Developers Conference 2007

Amsterdam, The Netherlands