



Wireless USB Association Models

Preston Hunt
Intel Corp.

Chair, WUSB Association Model Working Group

preston.hunt@intel.com



Presentation Objective

- **Introduce** the problem we are trying to solve
- Discuss available **solutions**
- Explain **requirements** for products
 - **Now** is the time to give your feedback!



What's Association?

- Scenario
 - Buy a new wireless digital camera
 - Want to connect to laptop for the first time
- How?

Association Models define how this is done in Wireless USB

What's At Stake?



RFID Kills.com
Death by Passport.
 The State Department wants to turn all US passports into terrorist beacons.

SC
MAGAZINE
 for IT security professionals

- Home
- News
- Products
- Features

Go to **SC** M...

News

Mobile virus infects Lexus cars
 by David Quainton

Lexus cars may be vulnerable to viruses that in mobile phones. Landcruiser 100 models LX470 a


 **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.

Slashdot

It is what IT is.

 **Car RFID Security System Cracked**



Wireless & USB

- Wireless inherently more complex than wired
- But it is being marketed as a simplification
- USB is extremely easy to use
- Must not mess this up
- Security mandatory for Wireless USB



Association Issues

Issue	Example
Accidental connection	Neighbor
Conditioning	Getting things started
Passive attack	Eavesdropping
Active attack	Impersonator/Man-in-the-middle
User intent	Identifying right device



Association Issues Scorecard

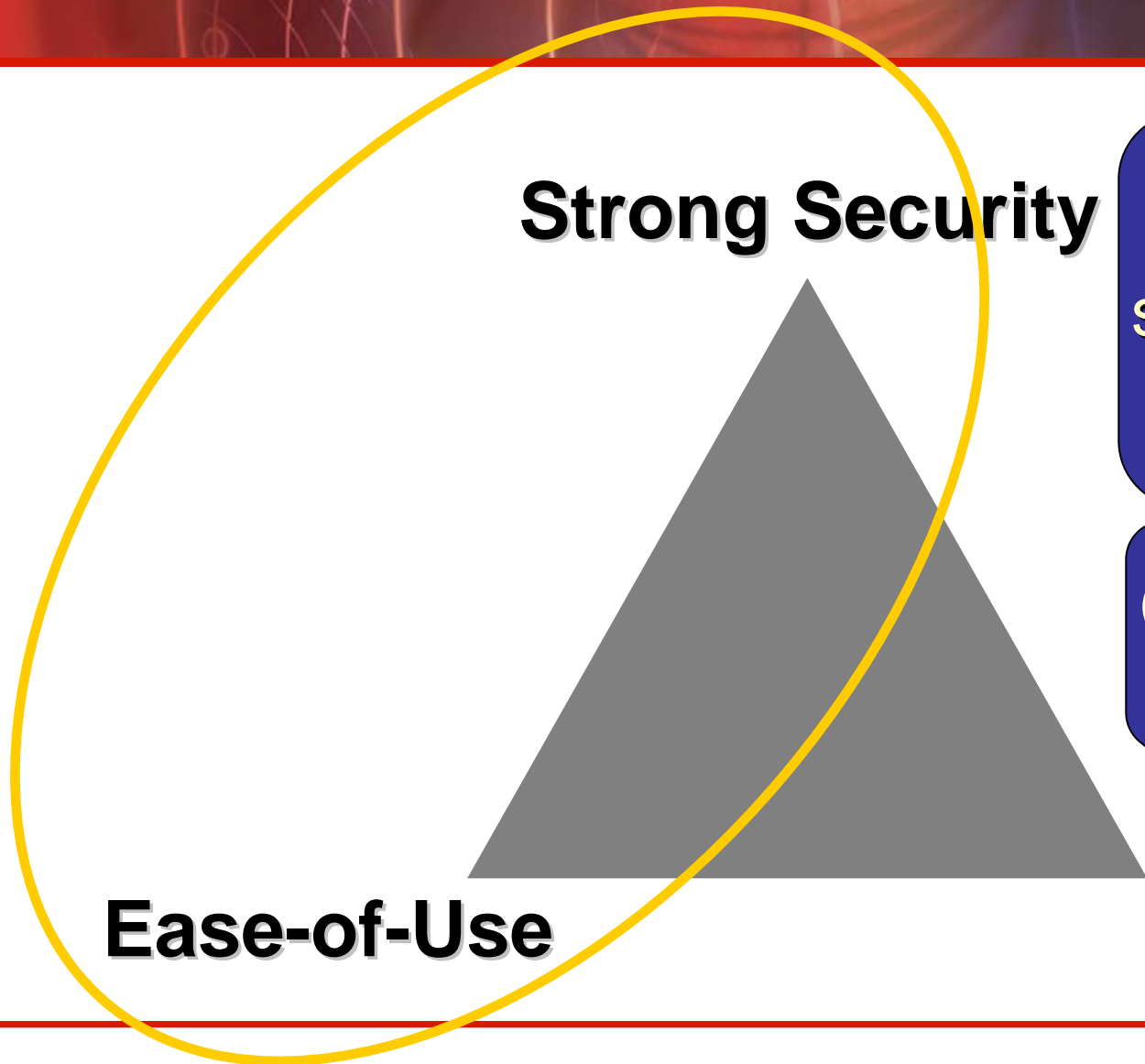
Wired vs. Wireless

Issue	Wired	Wireless
Accidental connection	Impossible	Easy
Conditioning	Easy	Can be difficult
Passive attack	Very hard	Easy
Active attack	Impossible	Unknown
User intent	Obvious	Can be difficult

The Association Models Specification will address these issues for Wireless USB



Tough Decision



Must not sacrifice security or usability!

(But obviously can't cost **too** much.)

No Extra Cost

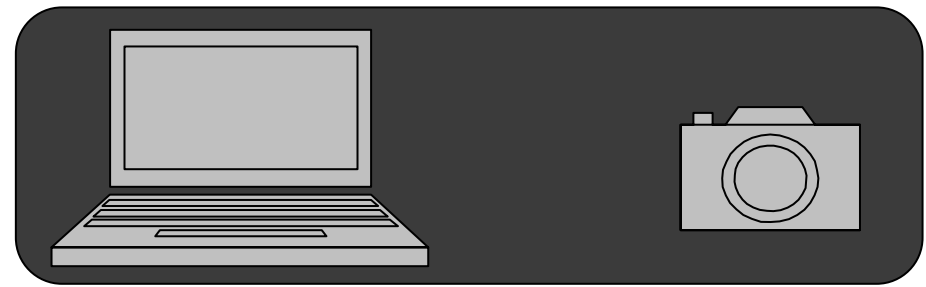


Three Models

- Viable for launch
 - Cable
 - Numeric
- Investigating for future use
 - Near Field Communication

All three models meet the security requirements for Wireless USB

Cable Model Overview



You bring the device into the vicinity of the host.

You plug a cable into the host.

Then you plug the cable into the device.

After the cable has been plugged into both the host and the device, the host will display a message that says:

*“Success!
You may now use this device wirelessly.”*

You can now remove the cable – it was only needed for the first time connection.

The host and device communicate wirelessly from now on.



Cable Model Analysis

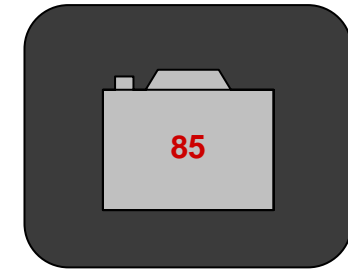
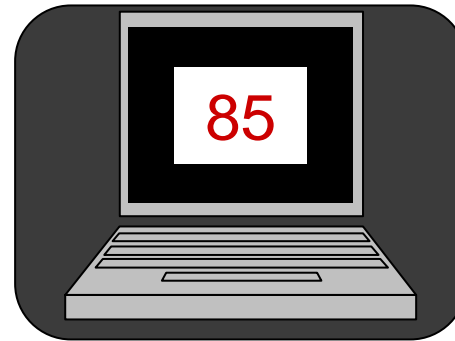
PRO

- Simple
- Cheap
- Secure by nature
- Many devices need to charge anyway
- 2+ billion existing ports
- “Gold standard”

CON

- Users dislike it
- Bad image (“I thought this was wireless!”)
- May need “introducer”

Numeric Model Overview



You bring the device into the vicinity of the host.

From a menu on the host, you select the option to “add a new device.”
On the device, you select from a menu that says “connect to new host.”

The host screen displays a two-digit code.
The device screen displays the same code.

You compare the codes and see they are the same, so you select “accept” on the host **and** then select “accept” on the device.

The host will display a message that says:
“Success! You may now use this device wirelessly.”
Now the host and the device know it is ok to communicate with one another. They will communicate wirelessly from now on.



Numeric Model Security

- Unlike cable, numeric is not secure by nature
- Can be eavesdropped
 - Diffie-Hellman solves this
 - D-H requires gates or CPU power
- D-H doesn't protect against impersonators
 - Need to verify the identity of the host/device
 - Need a display on the device to do this



Diffie-Hellman

- Cryptographic protocol
- Allows two parties to agree upon a shared secret
 - Over an insecure medium
 - Without any prior secrets
- Vulnerable to man-in-the-middle attacks
 - Requires verification of host and device identities
- Requires big math and a fair amount of RAM
 - E.g., $\langle 3072 \text{ bit number} \rangle^{\langle 256 \text{ bit} \rangle} \text{ mod } \langle 3072 \text{ bit} \rangle$
- Patent free and extremely well understood (and approved of) by the crypto community



Numeric Model Analysis

PRO

- No cable needed
- Users like it
- Works in many scenarios (heavy, far away devices)

CON

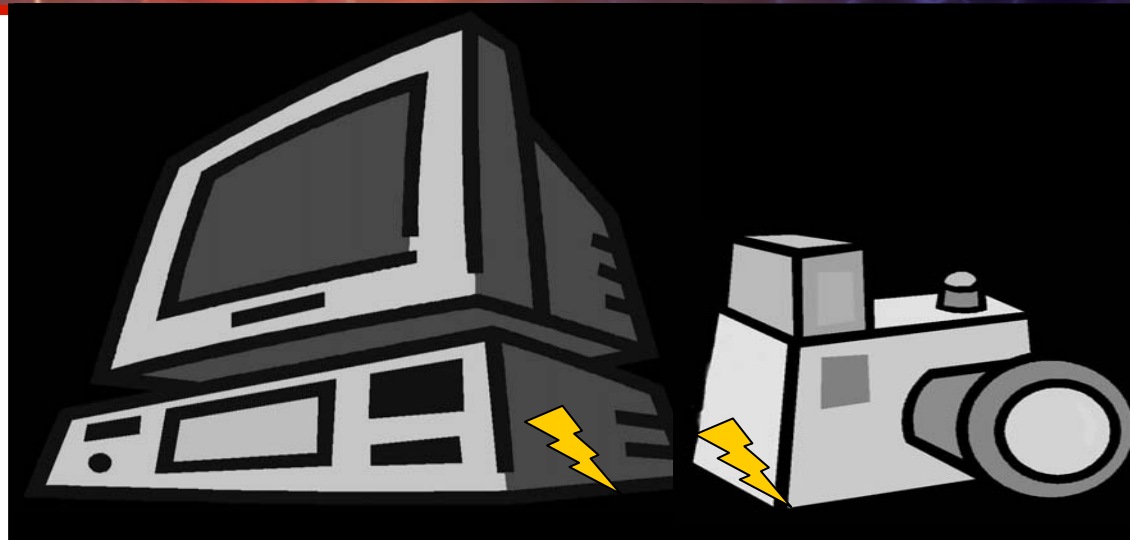
- Display required on device
- More user effort to start the process
- Requires Diffie-Hellman



NFC

- Near Field Communication
- 13.56MHz RF technology
- Very short range (5-10cm)
- In theory, active attack impossible
- Readers: Powered, more expensive
- Tags: Passive, cheap

NFC Model Overview



You bring the device into the vicinity of the host.

Both have an NFC logo.

When the products are placed close to one another (i.e., with the logos touching), they will automatically communicate with one another.

The host will display a message that says:
"Success! You may now use this device wirelessly."
Now the host and the device know it is ok to communicate with one another. They will communicate wirelessly from now on.



NFC Model Security

- In theory, NFC is resistant to impersonation
 - Because passive tag is charged by the reader
- Eavesdropping would be difficult, but possible
 - Magnetic fields fall off very quickly
 - RFID passports will require add'l security
 - May need Diffie-Hellman to be sure



NFC Model Analysis

PRO

- No cable needed
- Users love it
- Industry momentum

CON

- Cost unknown
- Deployment unknown
- Possible schedule risk
- May need introducer
- May require D-H crypto



Focus Group Study

- Conducted May 2005 in 2 markets
- 5 groups, 6 participants each
- Professionally moderated
- Goal was to assess perceived usability, security of 5 models



Focus Group Results

Wireless Expectations – Emphasis on Ease of Use

- Consumers have extremely high expectations
- Should be simple & easy
- Consumers hope/expect security will be there

Connection Scenarios – Most Popular: NFC and Number

- NFC has the biggest “wow” factor
 - “This is the ease I’m looking for!”
 - Some worried that it was insecure because it was too easy
- Number variants seen as all-around strong performer
 - Easy, reassuring, secure.
- Cable more of a disappointment than a deal-breaker
 - Redeemed itself in the security category
 - Less sophisticated users thought it was just fine



Focus Group Results

Purchase Motivator or Deterrent?

	Numeric	PIN	NFC	Cable	LED
Motivator 😊	13	14	17	10	1
Neutral 😐	16	15	8	12	8
Deterrent ☹️	1	1	5	8	21

Most/Least Favorite

	Numeric	PIN	NFC	Cable	LED
Ranked #1 😊	10	5	13	0	0
Ranked #2-4 😐	20	22	14	24	16
Ranked #5 ☹️	0	3	3	6	14



Association Model Specification

- Association Model Specification 1.0
 - Definitive source for all association information
 - Full technical, implementation details
 - Everything you need to build WUSB devices
- Association not included in core WUSB spec
 - Necessary core spec functionality already there
- Association will be enforced through compliance testing and logo certification



WUSB AM 1.0 Proposal

- Cable model is sufficient, but not required
 - Product with a port must support cable model
- Hosts: **must** support numeric model
- Devices: **should** support numeric model
 - Diffie-Hellman required for numeric model
 - Display required for numeric model
- Will investigate NFC for future adoption



Outstanding Issues

- Should numeric be required (all products)?
 - Put another way: cable is **not** sufficient
- How much does D-H really cost?
- How about the display cost for devices?

Need your feedback on these ASAP



Summary

- Association must be secure and easy
- Cable & Numeric models at launch
- Investigate NFC as future model
- Association Model Spec 1.0
 - Definitive source for all technical details
 - Full info on how to implement models
 - Available for review in June

Questions, Feedback, Discussion

Backup



Bluetooth Association Example: Motorola BT headset to Nokia 6820 Phone



1. Press two buttons on headset → light flashes
2. Navigate menu structure on phone, select "discover new devices"
3. Phone searches for 5-10 seconds, then displays list of discovered devices.
4. Select headset on phone UI → Prompted for PIN
5. Look up PIN in headset owner's manual (0000)
6. Enter PIN on phone
7. Association complete
8. Still need to enable headset mode to use it



Cable Model Implementation

- What happens when the device is plugged in?
 - Host enumerates the WUSB device just like any other USB device
 - Device has a specific interface that identifies it as wireless capable
 - When the host detects this interface, it will load a Wireless USB Association Class device driver
- Association class device driver sets up the device's security using class-specific requests
 - **GetConnection** to get current security settings from the device
 - **SetConnection** to set or modify security settings on device
- Full details will be in the Association Model Specification
 - Will include device, configuration, and interface descriptors
 - Will use default endpoint only, no endpoint descriptor required



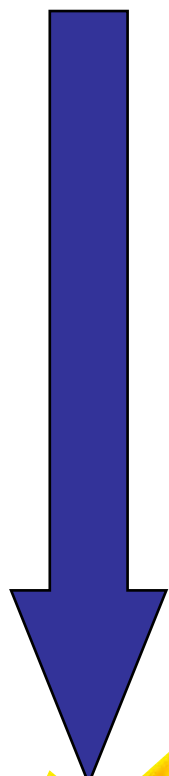
Cabled Devices

Wireless USB products with upstream USB Ports

- **Should** behave as a regular wired USB product while plugged in
 - **Should** enumerate at least 1 class in addition to association class
- **Must** support cable association
 - **Must** enumerate as association class
- **Should not** enumerate with the same host wirelessly while connected via a wire



WUSB AM Timeline



- 11/2002 WUSB Marketing Requirements
- 09/2003 End-user focus groups
WUSB working group meetings
WUSB developer F2F meetings
- 11/2004 Industry Update (SF)
- 01/2005 Industry Update (Milpitas)
Hardware prototypes, cost analysis
Second focus group study
Alignment with other wireless specs
- 05/2005 San Jose DevCon
- 06/2004 Version 0.9
Final review
- 07/2005 Version 1.0RC

**WUSB AM
1.0**

