Good Wireless Personal Area Network (WPAN) Protection: Don't Forget to Brush Your Bluetooth

3112 M Street NW
Washington, DC 20007
202.337.5600
www.TDISecurity.com

Paul Innella, CISSP
PaulInnella@TDISecurity.com

WPANs

Definition: **Short distance wireless networks.**

Alternate Definition: **A computer network used for communication among computer devices (e.g. telephones, PDAs, etc.) close to one person. PANs can be used for communication among the personal devices themselves, or for connecting to a higher level network.**

WPAN technology differs from WLAN/WAN technology:

- Maximum data throughput is much smaller. WPAN is meant for information transmission that does not require huge flows of data.
- WPAN is strictly close range (less than 30 feet) applications.
- Unlike infrared networks, it doesn't require alignment of objects for communication.

Examples:

- Technology that uses the natural electrical conductivity of the human body to transmit digital data between wearable computer devices.
- Bluetooth: small-form factor, low-cost, short range radio links between mobile PCs and other portable devices.

Tetrad Digital Integrity

Knowing Bluetooth Has Security Vulnerabilities, Why Talk About It?

Every technology has vulnerabilities

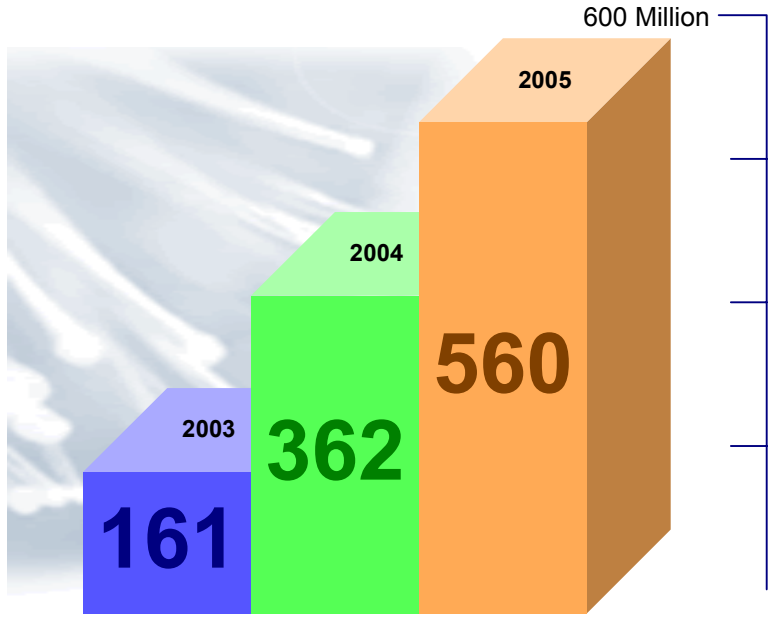
- Take for example AOL's IM, pcAnywhere, or NetMeeting.

This is our job/role, to secure technology solutions, regardless of their inherent security features – or lack of

- Far easier to implement or endorse security features of 802.11i, AES, or WPA.

Bluetooth is here to stay, so we'd better figure out how to securely integrate it Into the IT infrastructure

- More than 700 Bluetooth-equipped products and over 50 vendors exist.



Projected Number of Shipped Bluetooth Devices

Tetrad Digital Integrity

Overview: Bluetooth Security

Bluetooth Security Features

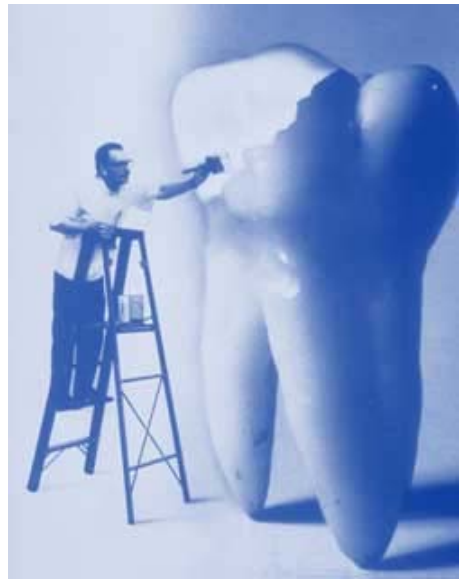
- Transmission occurs on a heavily used frequency, so Bluetooth uses “frequency hopping”, skipping around within the band. This reduces eavesdropping by only allowing synchronized devices to communicate.
- Each Bluetooth device has a unique address, helping to differentiate and authenticate devices.
- Secure transactions between devices are handled by a link key. The key is used for authorization and for deriving the encryption key. Authentication is based on shared-key (secret key) technology.
- An initialization key is needed when two devices engage in communication for the first time.
- The initialization key is based in part on a user-determined PIN. The PIN can be entered manually or stored by the device in memory.

Tetrad Digital Integrity

Overview: Bluetooth Security

Bluetooth Security Features

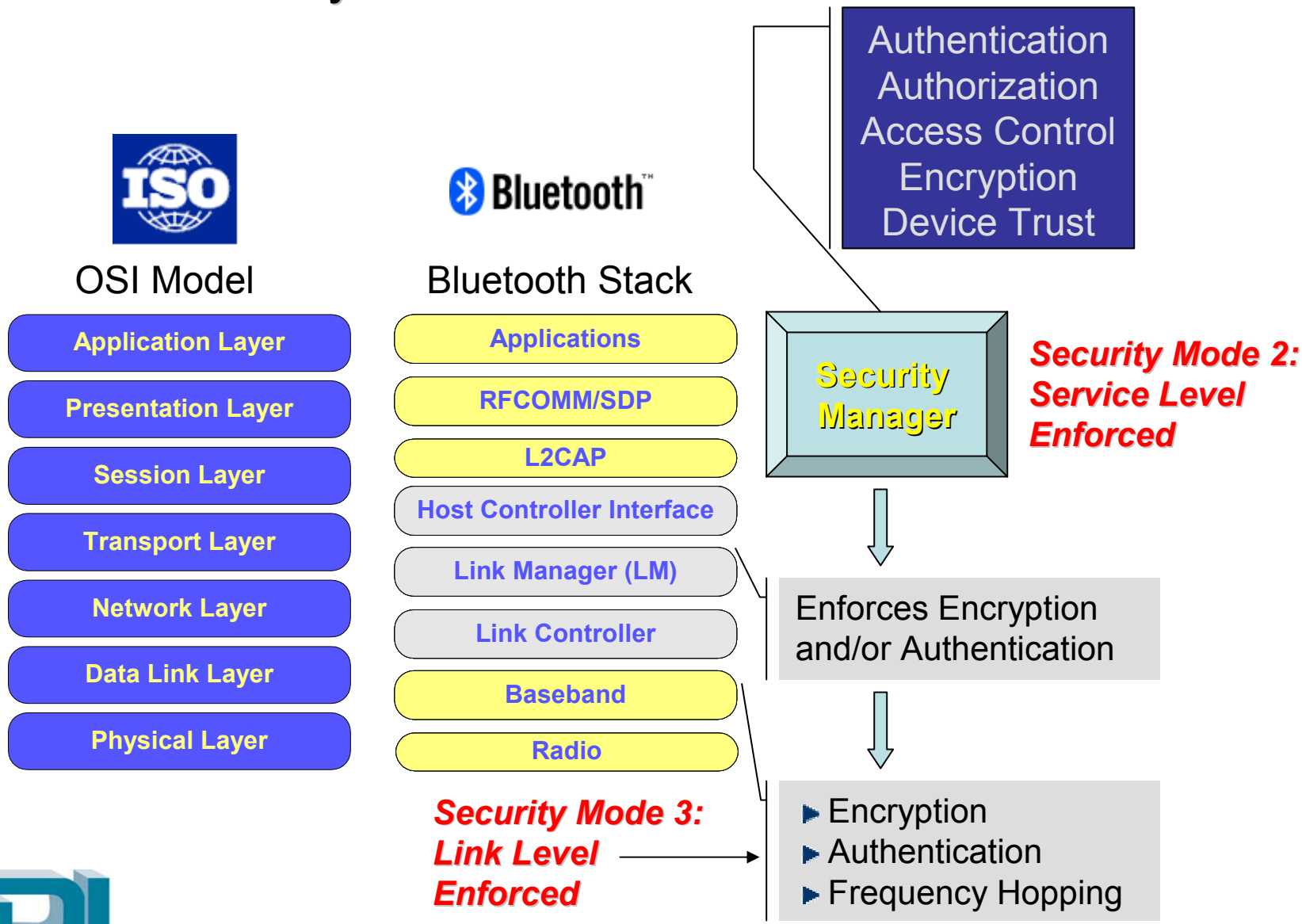
- All packet payloads are encrypted using a stream cipher called E0.
- Three Bluetooth security modes: non-secure, security after connection establishment, and security before connection initiation.
- Two trust levels for devices: trusted and non-trusted.
- Three security levels for services: open, authentication only, and both authentication and authorization required. Defined by attributes: authentication, authorization, and encryption required.



Tetrad Digital Integrity

Overview: Bluetooth Security

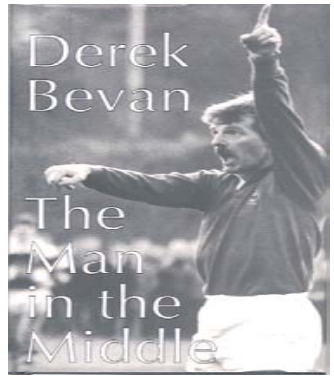
Bluetooth Security Architecture



Tetrad Digital Integrity

Source: Wireless Security Nichols, Lekkas

Overview: Bluetooth Security Vulnerabilities



Man-In-The-Middle Attack

Takes advantage of shared key authentication. Attacker steals a key before the start of a session and uses it to impersonate and/or eavesdrop on further communications.

Encryption Crack

The E0 stream cipher, relying on a key size of 128-bits, can be broken into its smaller linear feedback shift register (LFSR) components and used with the summation register. The smaller size is easier for intruders to decipher. This cipher is used because it is more efficient than other industry-standard ciphers.

NOTE: This attack is hard to carry out because each frame is encrypted separately with a different key segment, making data capture impractical.

Initialization key generation

When two Bluetooth devices engage in communication, the authentication key is generated from a combination of the BD_ADDR, PIN code, the PIN length, and a random number that is transmitted in the clear. The only secret is the PIN, which is often a 4-digit number providing only 10^4 different possibilities.

Tetrad Digital Integrity

Overview: Bluetooth Security Vulnerabilities

Individual Tracking

Each device has a unique ID, or Bluetooth Device Address (BD_ADDR), associated with it. An unscrambled header containing the ID is sent with every message. If an attacker connects an ID with an individual, they can track, monitor, and log all the Bluetooth activities of the individual.

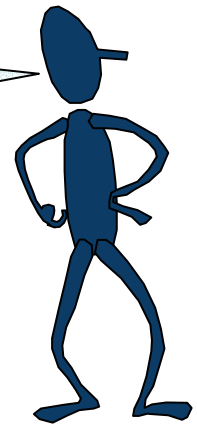
PIN Storage

Bluetooth devices offer the option of storing a PIN in the device's memory. While convenient (don't have to enter PIN for every connection), this makes authentication/encryption security non-existent.

No User Authentication

The Bluetooth protocol handles device authentication, but lacks user authentication.

"Bluetooth is adequate for small applications, but any sensitive data should not be sent with Bluetooth, " concluded Helsinki University of Technology's Jula Vainio.



Tetrad Digital Integrity

Overview: Bluetooth Security Vulnerabilities

Jamming

Bluetooth is susceptible to jamming if the hopping sequence is identified and the jamming equipment synchronizes with the hops; otherwise, the entire band would have to be jammed.

Security Disablement

Various Bluetooth-equipped devices do not, by default, enable the inherent security features of Bluetooth. Implications are of course serious, including the ability to perform:

War-phoning

Allows other Bluetooth-equipped devices to read data such as personal contacts and appointments and even make calls using the security-disabled device's identity.

Tetrad Digital Integrity

So Why All of the Negativity?

After all, look how Bluetooth measures up to 802.11b

- Different encryption and authentication keys are employed with Bluetooth but not in 802.11b.
- WEP RC4 coupled with the use of an IV, and an ICV are less secure than Bluetooth's E0.
- Neither technologies deal with Non-repudiation or instantiate a mechanism for auditing.
- Both 802.11b and Bluetooth rely on hardware and software solutions to augment their security weaknesses.

In truth, these technologies are complementary.

Tetrad Digital Integrity

Bluetooth Security Measures

Use What Bluetooth Has to Offer

- Rely on combination keys as opposed to unit keys. Unit keys are globally shared whereas combination keys are only for communication between Bluetooth device pairs. Group keys are a new alternative as well, pairing a unit to a service instead of another unit.
- Use security mode 2 at a minimum.
- Define trust relationships between devices.
- Perform the pairing procedure in an isolated environment.
- Properly define policies, especially those governing which device may assume the role of master versus slave.

Institute PIN Policies

- Require minimum PIN length longer than 4-digits. This will make brute force attacks harder and increase the complexity of the initialization key.
- Forbid storage of PIN on device. While it makes life more convenient by cutting down on manual entry of PINs, storing the PIN on the device is a potential security hole. If the device carries or connects with sensitive information, cut down on storage of the PIN as much as possible.

Tetrad Digital Integrity

Bluetooth Security Measures

Incorporate Additional Security Solutions

When using Bluetooth to connect with secured corporate networks, use extra authentication and encryption products. These include:

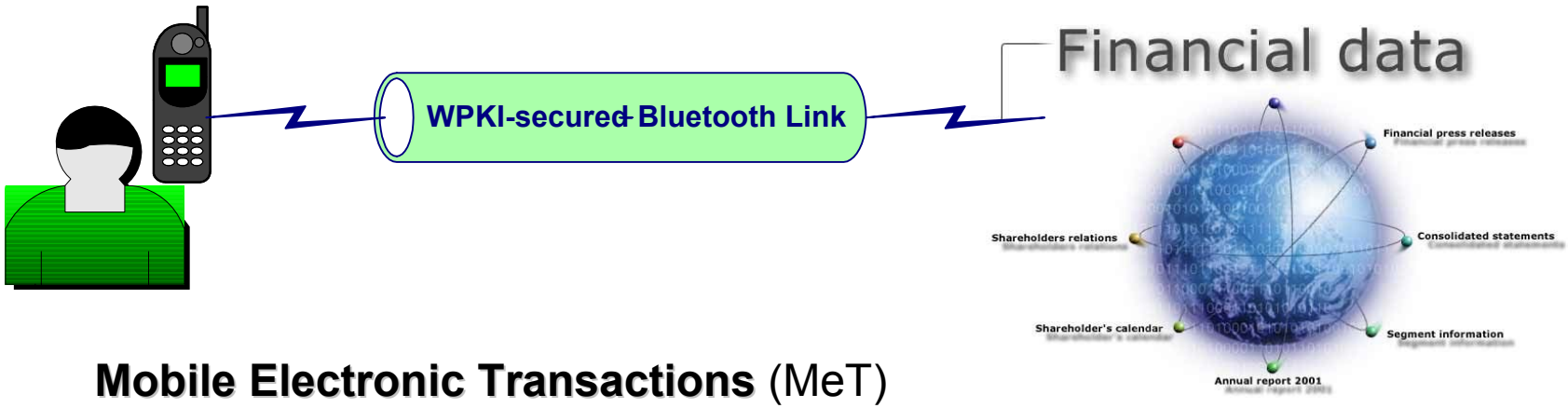
- Digital certificate based systems (such as Diffie-Hellman key agreement) for authentication. This limits the shared key vulnerability and prevents from Man-in-the-middle.
- Software-based gateway, such as Bluseocket, that resides on a PC between wireless clients and protected servers. This provides an extra authentication layer.
- A firewall that controls individual wireless users' access and data flows around secured network services.
- Incorporate application-level security such as VPN/IPSec/SSL/TLS to provide encryption and build secure tunnels between the Bluetooth device and the network.
- Physical protection such as Faraday's cage.
- Biometrics and voice authentication on the Bluetooth device.

Tetrad Digital Integrity

Current Example

AU-System Deployment

- Wireless PKI (WPKI)
- Bluetooth-equipped phones and PDAs
- WAP
- Provided secure access to financial data.



Mobile Electronic Transactions (MeT)

- Working on solutions to integrate WAP for WTLS (Wireless Transport Layer Security), WIM (Wireless Identity Module), and WPKI (Wireless Public Key Infrastructure). As a transmission medium, MeT also embraces Bluetooth.

Tetrad Digital Integrity

Future Example

USMC Public Key-Enabling (PK-E) Program

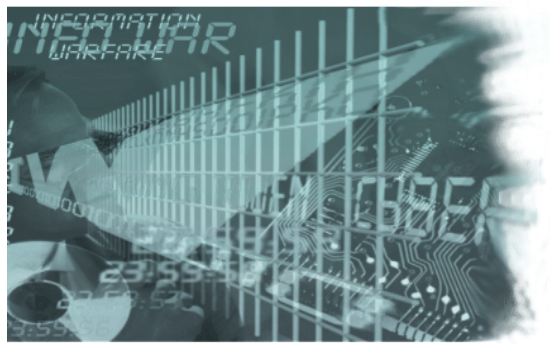
- Currently in progress and aimed at allowing applications to use services provided by the US Department of Defense (DoD) PKI; namely confidentiality, authentication, integrity, access control, and non-repudiation.

Common Access Card (CAC)

- DoD-wide Smart Card that serves as:
  - Identification card for military personnel.
  - Access control mechanism to network assets and physical entities.
  - Primary platform for PKI authentication token.

Numerous Technological Combinations Possible:

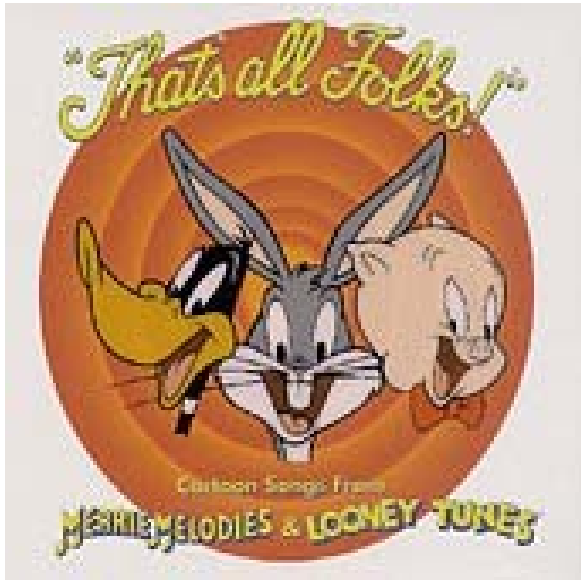
- PKI or WPKI coupled with:
  - Bluetooth-equipped devices.
  - Bluetooth chip embedded on the CAC.
  - Card reader can equally use Bluetooth links.



Tetrad Digital Integrity

Conclusion

- We know that Bluetooth has inherent security vulnerabilities.
- The technology is nonetheless viable.
- It thus behooves us to understand how to secure it.



Tetrad Digital Integrity