Bluetooth Security

Syed Jebran[1], Yashpal Singh[2]
[1,2]Department of Computer Science &Engineering,
Ganga Institute of Technology and Management,
Kablana, Jhajjar, Haryana, India

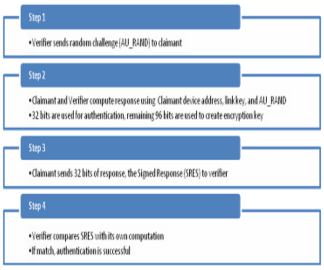
***Abstract*— Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Bluetooth technology unplugs our digital peripherals and makes a cable clutter a thing of the past. In short, it is a wireless replacement for many of the cables we currently use to transmit voice and data signals. It is the result of the joint achievements of nine leading companies: 3COM, Lucent Technologies, IBM, Intel, Microsoft, Motorola, Nokia, Toshiba, and Ericsson, altogether known as the Blue Tooth Special Interest Group (SIG). The idea is to create a single wireless protocol to address the end-user problems arising from proliferation of various mobile devices.**

Fig 1

I. INTRODUCTION

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the **ISM band** from 2.4 to 2.485 GHz) from fixed and mobile devices, and building **personal area networks** (PANs). Invent. It was originally conceived as a wireless alternative to **RS-232** data cables. It can connect several devices, overcoming problems of synchronization.Bluetooth is managed by the **Bluetooth Special Interest Group** (SIG), which has more than 20,000 member companies' telecommunication, computing, networking, and consumer electronics. Bluetooth was standardized as **IEEE 802.15.1**, but the standard is no longer maintained. The SIG oversees the development of the specification, manages the qualification program, and protects the trademarks. To be marketed as a Bluetooth device, it must be qualified to standards defined by the SIG. A network of patents is required to implement the technology, which is licensed only for that qualifying device.

II. BLUETOOTH SECURITY MECHANISM



Step 1
- Verifier sends random challenge (AU_RAND) to claimant

Step 2
- Claimant and Verifier compute response using Claimant device address, link key, and AU_RAND
- 32 bits are used for authentication, remaining 96 bits are used to create encryption key

Step 3
- Claimant sends 32 bits of response, the Signed Response (SRES) to verifier

Step 4
- Verifier compares SRES with its own computation
- If match, authentication is successful

Fig 2

ea

Fig 3

III. BLUETOOTH VULNERABILITIES

The text will be continuously completed with pictures and links for download. Bluetooth is a great technology that is Implemented in several mobile device. For communication with other device no cable is necessary and there is a lot of applications dedicated directly for Bluetooth. As well as in the case with Wi-Fi there is not necessary a cable for connecting two devices. Expansion of Zambian based mobile phones will probably bring into this sector many new possibilities. This technology has a lot of advantages but has as well a great potential to deprive the mobile phone owner of his data. Most of the mobile phones today need to activate the Bluetooth interface and to confirm the data acceptance.

But there is also a lot of people who consciously or unconsciously use Bluetooth without Hidden mode.

Blue Jacking is commonly known as a term for sending data (vCard, picture) to a random person with a focus on the humor. Someone uses this opportunity for promotion. But there are also a lot of other activities connected to Bluetooth technology. This is an overview of applications for blue jacking, blue snaring and Blue Bugging.

IV. BLUETOOTH APPLICATIONS

1. Wireless networking between laptops and desktop computers, or desktops that are in a confined space and little bandwidth is needed.

2. Peripherals such as mice, keyboards, and printers. 3. Cell phones with Bluetooth technology have been sold in large numbers, as they are able to connect to computers, PDAs (Personal Data Assistant), and various other devices. The standard also includes the support for more powerful and longer range devices.

4. The transfer of files, images and MP3, between mobile phones.

5. Certain MP3 players and digital cameras to transfer files to and from computers.

6. Bluetooth technology headsets for smart phones and cell phones.

7. Data logging equipment that transmits data to a computer via Bluetooth technology.

8. Sony Play station 3 and Nintendo Revolution will both use Bluetooth technology for their wireless controllers.

For Bluetooth, there are literally hundreds of different applications and devices available for you to use or purchase. As you may already know. Bluetooth is the most popular wireless technology in the world. It’s very reliable, very dependable, and very hard to crack into.

There are many other applications for Bluetooth in development now, many of which plan to take the wireless age to the next level. Video game systems are using Bluetooth technology as well, for their wireless controllers. This is great news for gaming fans, as Bluetooth offers the best in wireless data transmission. If you’re curious about applications for Bluetooth that are still in development, you can search on the internet. You can find all sorts of information, especially when it comes to Bluetooth. As the future arrives, you can expect Bluetooth to bring bigger and better things.

Fig 4

V. FUTURE BLUETOOTH TECHNOLOGY

A new core specification positions Bluetooth technology for an explosion of wireless applications in the home. The most recent core specification, Bluetooth v4.0, extends wireless capabilities to products that require low energy consumption, such as smart watches, in-home medical monitoring devices and energy-efficiency sensors. It also allows high speed data transfer, which is useful for moving ever larger volumes of electronic data such as videos and music playlists among devices. This means Bluetooth enabled devices will be ready for the ever-increasing power usage and bandwidth demands from the growing number of connected homes.

Home automation is coming, with the required Bluetooth profiles close to completion. "You should see (new) products being demonstrated at the beginning of the year (2011)," says. "That's a major step for the heating and air conditioning industry, because up to now they have been (using) proprietary products."

Asian countries are showing particular interest in home automation and energy efficiency – especially China. "China is deploying smart energy meters at an amazing rate, something like 25 million meters per year," says Drake. Hun says governments also are pushing home applications like these in Europe. "There's increasing government pressure driving the industry into interoperability," he says. "Going to a standard wireless profile makes it much, much easier for people to control their energy usage at home." Compare that with, for example, the cost of retrofitting a home for the many new hard-wired connections that would be needed for a comprehensive wired home automation system.

In the United States, the National Institute of Standards and Technology has sponsored a group called the Smart Grid Interoperability Panel. "Bluetooth technology is now represented in that forum, trying to define how smart energy will work (especially) in the home.

Manufacturers can plug into the existing base of billions of Bluetooth wireless chips. Whether someone is using their cell phone as a remote control, using a Bluetooth enabled headset for a Skype application running on their TV, streaming songs from a cell phone or music player to their home entertainment system, or pushing pictures to their TV to view them on a big screen, Bluetooth technology enables existing products to be used in new ways for home entertainment.

Usability is an ongoing challenge. Bluetooth technology works well – once it's enabled. The process of pairing devices is designed to be easy, but consumers need clear product instructions and simple user interfaces that get them to the pairing process in the first place.

Fig 5

VI. CONCLUSION

The version of this template is V2. Most of the formatting instructions in this document have been compiled by

Causal Productions from the IEEE Latex style files. Causal Productions offers both A4 templates and US Letter templates for Latex and Microsoft Word. The Latex templates depend on the official IEEEtran.cls and IEEEtran.bst files, whereas the Microsoft Word templates are self-contained. Causal Productions has used its best efforts to ensure that the templates have the same appearance.

ACKNOWLEDGMENT

The heading of the Acknowledgment section and the References section must not be numbered.

Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE Latex style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE Latex distribution.

REFERENCES

[1] SECURITY BREACHES.TDA John Huffman

[2] DATA COMMUNICATION Fourazan

[3] NETWORK SECURITY AND FUNDAMENTALS William Stallings

[4] https://www.google.co.in/webhp?sourceid=chrome-instant&ion=1&espv=2&es_th= 1&ie= UTF-8#q=proliferation

[5] http://www.garykessler.net/library/steganography.html

[6] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.

[7] www.google.com/security/wireless/infrared.