ECE 716, Fall 2005, Handout 4, G. Gong

Encryption in Wireless Systems

1 Secure Tunnels

As there are no physical boundaries to prevent intruders from intercepting data in free space, wireless communication security is to protect the packets of data being transmitted; ensuring that only those for whom they are intended can read them. This is accomplished through secure tunnels. There are many ways to create wireless secure tunnels. In order to do so, the following crypto operations are basic building blocks of creating a secure tunnel.

1. User Authentication: Determining that the network users are whom they claim to be. Authentication allows access to users based on certain credentials, and verifies that a third party has not altered data sent between two users.

2. Encryption: Encrypt data before it is transmitted and delivering it in a way that can be efficiently deciphered by the authenticated receiver. Encryption allows sensitive information to travel over a public network without compromising confidentiality.

3. Message Authentication: A proof that messages have not been tampered with or replayed (sent multiple times) between the sender and receiver.

4. Access Control: Blocking unwanted user access to an internal network or service. This restricts the user to the privileges that are designated only for them. Access control is typically achieved through authentication.

In the following, we will describe several stream ciphers that proposed for encryption in WLANs and Bluetooth standard, and block ciphers implemented as stream cipher mode for UMTS (or W-CDMA) and CDMA 2000 in 3G.

2 Security of Encryption in WEP: RC4

A. WEP Description

The 802.11 standard describes the communication that occurs in wireless local area networks (LANs). The Wired Equivalent Privacy (WEP) algorithm is used to protect wireless

[0]

communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network; this function is not an explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP.

WEP relies on a secret key that is shared between a mobile station (e.g. a laptop with a wireless ethernet card) and an access point (i.e., a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks.

B. Encryption Algorithm RC4 in WEP

WEP uses the RC4 encryption algorithm, which is a stream cipher. The description of RC4 is provided in the slides. In the following, we list two weaknesses of WEP setting:

1. If an attacker flips a bit in the ciphertext, then upon decryption, the corresponding bit in the plaintext will be flipped.

2. If an eavesdropper intercepts two ciphertexts encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts. Knowledge of this XOR can enable statistical attacks to recover the plaintexts. This attack can be extended to the case the two ciphertexts are encrypted by two different key streams which are strongly correlated, i.e., the autocorrelation of the key stream sequences are bad.

To prevent this type of attacks, WEP uses an Initialization Vector (IV) to augment the shared secret key and to produce a different RC4 key for each packet.

However, the initialization vector in WEP is a 24-bit field, which is sent in the cleartext part of a message. Such a small space of initialization vectors guarantees the reuse of the same key stream. A busy access point, which constantly sends 1500 byte packets at 11Mbps, will exhaust the space of IVs after $1500 \cdot 8/(11 \cdot 10^6) \cdot 2^24 \approx 18000$ seconds, or 5 hours. (The amount of time may be even smaller, since many packets are smaller than 1500 bytes.) This allows an attacker to collect two ciphertexts that are encrypted with the same key stream and perform statistical attacks to recover the plaintext. So, the usage of RC4 in WEP is not secure.

3 E_0 Encryption Algorithm in Bluetooth

Bluetooth is a way of connecting machines to each other without cables or any other physical medium. It uses radio waves to transfer information, so it is very susceptible to attacks. In the following, we first give some background information about Bluetooth system, and then the algorithm.

A. Description

Bluetooth is the new emerging technology for wireless communication. It was developed by a group called Bluetooth Special Interest Group (SIG), formed in May 1998. The founding members were Ericsson, Nokia, Intel, IBM and Toshiba. Since then, almost all of the biggest companies in the telecommunications business (e.g. 3Com, Microsoft, Motorola) have joined the Bluetooth SIG and the number of the participating companies is now over 1,500. The version 1.0 of the Bluetooth specification was approved in the summer of 1999, and the latest version (at the time of writing) 1.0B in December 1999.

Bluetooth can be used to connect almost any device to another device. The traditional example is to link a Personal Digital Assistant (PDA) or a laptop to a mobile phone. In that way you can easily take remote connections with your PDA or laptop without getting your mobile phone from your pocket or messing around with cables. Bluetooth can also be used to form ad hoc networks of several (up to eight) devices, called *piconets*. This can be useful for example in a meeting, where all participants have their own Bluetooth-compatible laptops, and want to share files with each other.

B. Bluetooth Encryption

The Bluetooth encryption system encrypts the payloads of the packets using a stream cipher E0, which is re-synchronized for every payload. The E0 stream cipher consists of the payload key generator, the key stream generator and the encryption/decryption part. A block diagram of E0 is shown in the slides.

The payload key generator combines the input bits in an appropriate order and shifts them to the four Linear Feedback Shift Registers (LSFR) of the key stream generator. The key stream bits are generated by a method derived from the summation stream cipher generator by Massey and Rueppel [**?**].

Depending on whether a device uses a semi-permanent link key or a master key, there are several encryption modes available. If a unit key or a combination key is used, broadcast traffic is not encrypted. Individually addressed traffic can be either encrypted or not. If a master key is used, there are three possible modes. In encryption mode 1, nothing is encrypted. In encryption mode 2, broadcast traffic is not encrypted, but the individually addressed traffic is encrypted with the master key. And in encryption mode 3, all traffic is encrypted with the master key.

As the encryption key size varies from 8 bits to 128 bits, the size of the encryption key used between two devices must be negotiated. In each device, there is a parameter defining the maximum allowed key length. In the key size negotiation, the master sends its suggestion for the encryption key size to the slave. The slave can either accept and acknowledge it, or send another suggestion. This is continous, until a consensus is reached or one of the devices aborts the negotiation. The abortion of the negotiation is done by the used application. In every application, there is defined a minimum acceptable key size, and if the requirement is not met by either of the participants, the application aborts the negotiation and the encryption cannot be used. This is necessary to avoid the situation where a malicious device forces the encryption to be low in order to do some harm.

The encryption algorithm uses four LFSRs of lengths 25, 31, 33 and 39, with the total length of 128. The initial 128-bit value of the four LFSRs is derived from the key stream generator itself using the encryption key, a 128-bit random number, the Bluetooth device address of the device and the 26-bit value of the master clock. The feedback polynomials used by the LFSRs are all primitive, with the Hamming weight of 5. The polynomials used are (25, 20, 12, 8, 0), (31, 24, 16, 12, 0), (33, 28, 24, 4, 0) and (39, 36, 28, 4, 0).

Note that the encryption algorithm E_0 is vulnerable to the algebraic attack. It has been proposed to implement AES, introduced in Chapter 7, as a stream cipher mode to replaced both algorithms.

4 Encryption for Wireless W-CDMA and CDMA Systems

For cellular communications, there are two types of existing systems in the world before developments of 3G. In 2G and 2.5G, there are GSM and GPRS, which are used in Europe and the multiplexing method is time division multiplexing access (TDMA), and IS-95 and IS-98 which employed code division multiplexing access (CDMA) as the multiplexing method, and these CDMA systems are used in the North America. Later on, the European systems are extended to the so-called UWTS and its modification in the physical layer, wideband CDMA (W-CDMA) which uses CDMA for access methods and adopted the original network structure of GSM. IS-95 and IS-98 are extended to CDMA2000 (or called IS-2000). In the original GSM, it employed $A_5/1$, introduced in Chapter 7, as the encryption algorithm to protect the voice message over air. In W-CDMA, it proposed to implement a block cipher Kusumi in a stream cipher mode as an encryption algorithm to protect both voice and data information. For CDMA2000, it proposed three different LFSR based stream cipher algorithms to protect voice, data, and signaling, respectively. However, they all suffered varieties of attacks. Currently, it proposed to implement AES Rijndael in stream cipher mode to provide a stream cipher encryption in CDMA2000.

A. CDMA: A General Description

Code-Division Multiple Access (CDMA) is a digital cellular technology that uses spread-spectrum techniques. It allows multiple uses to share a common channel. In a CDMA system, individual conversations are spreaded with a pseudo-random sequence. CDMA consistently provides better capacity for voice and data communications than other commercial mobile technologies, allowing more subscribers to connect at any given time, and it is the common platform on which 3G technologies are built.

Originally, CDMA is a military technology first used during World War II by English allies to foil German attempts at jamming transmissions. The allies decided to transmit over several frequencies, instead of one, making it difficult for the Germans to pick up the complete signal. Qualcomm created communications chips for CDMA technology starting in the middle of 80's, which became the first to commercialize it.

B. Encryption in W-CDMA

The encryption in W-CDMA (or UMTS) is a stream cipher implemented using the block cipher Kasumi. The description of this stream cipher and block cipher Kasumi is provided in the slides.

C. CDMA2000 Encryption

Originally, CDMA2000 systems proposed to employ three different encryption algorithms, which are Cellular Authentication and Voice Encryption (CAVE), Cellular Message Encryption Algorithm (CMEA - for signaling), ORYX (for data) on the CDMA channel. All are LFSRs based stream ciphers. The private Authentication Key (A-key) and the mobile handset Electronic Serial Number (ESN) serve as inputs to the algorithms in both the mobile handset and the network (HLR/AC) for signature authentication and encryption/decryption of voice, data and signaling messages. However, none of these ciphers is secure. The newly proposed scheme is similar to that of W-CDMA system, in which AES Rijndael will be implemented as a stream cipher mode for providing stream cipher encryption in CDMA2000. See the slides for details.