Multicast Security

- a *multicast message* is a message that has many designated receivers, i.e., one-to-many communication as opposed to one-to-one communication
- a *multicast network* is a network of users in which it is possible to send messages simultanously to all of the users
- two "benchmark scenarios" for multicast security:

single source broadcast

a single entity broadcasts information to a long-lived, possibly dynamic, *group* (consisting of some or all of the users in the network)

virtual conference

a subset of the network users wish to form a small virtual conference, i.e., a short-lived, static, group

Possible Goals

- in a single source broadcast, we might want to achieve one or more of the following goals:
  - confidentiality, data integrity
  - key revocation, key updating
  - source authentication
  - copyright protection
- in a virtual conference, we might want to achieve one or more of the following goals:
  - establishment of a group session key (which enables confidentiality and data integrity within the group)
  - source or group authentication
  - anonymity
  - shared access control

Cryptographic Tools

New cryptographic tools are required to enable multicast security:

secret sharing schemes

distributing shares of a "secret" in such a way that a specified threshold of shares is required to reconstruct the secret; used as a building block in more complicated protocols

group key predistribution schemes

KPS in whick keys are associated with groups of users of a certain size; secure against coalitions of a certain size

broadcast encryption/exclusion

broadcasting an encrypted message in such a way that only users in a specified group can decrypt the message; secure against coalitions of a certain size; used for group session key distribution and key updating

Cryptographic Tools (cont.)

tracing schemes

also called fingerprinting schemes; they comprise techniques and algorithms to facilitate tracing of illegally redistributed keys and/or content back to the owners

interactive group KAS

KAS in which a session key is established for a specified group of users

multireceiver authentication codes

a MAC in which all the users in a specified group can validate the authenticity and/or the source of data transmitted by one of the group members

Secret Sharing (overview)

- various types of shared control schemes depend on a cryptographic primitive called a (t, n)-*threshold scheme*
- let t and n be positive integers, $t \leq n$
- we have a trusted authority, denoted TA, and n users, denoted $U_1, \ldots, U_n$
- the TA has a secret value $K \in \mathcal{K}$, called a *secret* or a *key*, where $\mathcal{K}$ is a specified finite set

Secret Sharing (overview)

- the *TA* uses a *share generation algorithm* to split K into n *shares*, denoted $s_1, \ldots, s_n$
- each share $s_i \in \mathcal{S}$, where $\mathcal{S}$ is a specified finite set
- for every i, $1 \leq i \leq n$, the share s_i is transmitted by the *TA* to user U_i using a secure channel
- the following two properties should hold:
  1. a *reconstruction algorithm* can be used to reconstruct the secret, given any t of the n shares,
  2. no $t - 1$ shares reveal any information as to the value of the secret

An (n, n)-Threshold Scheme

- suppose $K \in \mathbb{Z}_m$ is the secret
- let $s_1, \ldots, s_{n-1}$ be chosen independently and uniformly at random from $\mathbb{Z}_m$
- let

$$s_n = K - \sum_{i=1}^{n-1} s_i \bmod m$$

- $s_1, \ldots, s_n$ are shares of an (n, n)-threshold scheme:
  1. $K = \sum s_i \bmod m$
  2. given all the shares except s_j, K could take on any value, depending on the value of the share s_j

Shamir Threshold Scheme

- in 1979, Shamir showed how to construct a (t, n)-threshold scheme based on polynomial interpolation over $\mathbb{Z}_p$, where p is prime
- let $p \geq n + 1$ be a prime
- let $\mathcal{K} = \mathcal{S} = \mathbb{Z}_p$
- in an initialization phase, $x_1, x_2, \ldots, x_n$ are defined to be n distinct non-zero elements of $\mathbb{Z}_p$
- the TA gives x_i to U_i, for all i, $1 \leq i \leq n$
- the x_i's are public information

Share Generation for the Shamir Scheme

- given a secret $K \in \mathbb{Z}_p$, the share generation algorithm is as follows:
  1. the TA chooses $a_1, \ldots, a_{t-1}$ independently and uniformly at random from $\mathbb{Z}_p$
  2. the TA defines
     $$a(x) = K + \sum_{j=1}^{t-1} a_j \, x^j$$
     (note that $a(x) \in \mathbb{Z}_p[x]$ is a random polynomial of degree at most $t-1$, such that the constant term is the secret, K)
  3. for $1 \leq i \leq n$, the TA constructs the share $s_i = a(x_i)$

Reconstruction Algorithm for the Shamir Scheme

- suppose users $U_{i_1}, \ldots, U_{i_t}$ want to determine K
- they know that $s_{i_j} = a(x_{i_j})$, $1 \leq j \leq t$
- since $a(x)$ is a polynomial of degree at most $t-1$, they can determine $a(x)$ by Lagrange interpolation; then $K = a(0)$
- recall the Lagrange interpolation formula:

$$a(x) = \sum_{j=1}^{t} s_{i_j} \prod_{1 \leq k \leq t, k \neq j} \frac{x - x_{i_k}}{x_{i_j} - x_{i_k}}$$

- set $x = 0$:

$$K = \sum_{j=1}^{t} s_{i_j} \prod_{1 \leq k \leq t, k \neq j} \frac{-x_{i_k}}{x_{i_j} - x_{i_k}} = \sum_{j=1}^{t} s_{i_j} \prod_{1 \leq k \leq t, k \neq j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}}$$

Reconstruction Algorithm for the Shamir Scheme (cont.)

- for $1 \leq j \leq t$, define

$$b_j = \prod_{1 \leq k \leq t, k \neq j} \frac{x_{i_k}}{x_{i_k} - x_{i_j}}$$

- the b_j's do not depend on the shares, so they can be precomputed (for a given subset of t users)
- then K can be computed from the formula

$$K = \sum_{j=1}^{t} b_j \, s_{i_j}$$

Example

- suppose that $p = 17$, $t = 3$, and $n = 5$; and the public x-co-ordinates are $x_i = i$, $1 \leq i \leq 5$
- suppose that the group $G = \{U_1, U_3, U_5\}$ wishes to compute K, given their shares $8, 10$, and 11, respectively
- it is possible to (pre)compute b_1, b_2, and b_3:

$$\begin{aligned} b_1 &= \frac{x_3 x_5}{(x_3 - x_1)(x_5 - x_1)} \bmod 17 \\ &= 3 \times 5 \times (-2)^{-1} \times (-4)^{-1} \bmod 17 \\ &= 4, \\ b_2 &= 3, \quad \text{and} \\ b_3 &= 11 \end{aligned}$$

- then the users in G can (collectively) compute K as follows:

$$K = 4 \times 8 + 3 \times 10 + 11 \times 11 \bmod 17 = 13$$

Security of the Shamir Scheme

- suppose users $U_{i_1}, \ldots, U_{i_{t-1}}$ want to determine K
- they know that $s_{i_j} = a(x_{i_j})$, $1 \leq j \leq t-1$
- let K_0 be arbitrary
- by Lagrange interpolation, there is a unique polynomial $a_0(x)$ such that $s_{i_j} = a_0(x_{i_j})$ for $1 \leq j \leq t-1$ and such that $K_0 = a_0(0)$
- hence no value of K can be ruled out, given the shares held by $t-1$ users