12장 4번

먼저, LKH (Leaf Knockout Hashing) 방식과 OFT (Optimal Full Transitive) 방식은 논리 트리에서 단말 노드에 가입하는 방식을 나타냅니다. 단말 노드에 가입하는 방식에서는 각 사용자는 단말 노드에 직접 가입하게 됩니다.

하지만 가정에서는 단말 노드에 가입하는 방식이 아닌 루트 노드에 가입하는 방식을 사용한다고 가정하였습니다. 이 경우, 중앙서버는 가입한 사용자에게 분배해야 하는 메시지와 해당 메시지를 유니캐스트 또는 멀티캐스트로 전달해야 합니다.

유니캐스트(Unicast): 유니캐스트는 메시지를 하나의 목적지에게만 전송하는 방식입니다. 따라서 중앙서버는 가입한 사용자 1명에게 메시지를 유니캐스트로 전달합니다. 루트 노드에 가입하는 방식에서는 메시지를 유니캐스트로 전송하는 것이 일반적입니다.

멀티캐스트(Multicast): 멀티캐스트는 메시지를 여러 목적지에 동시에 전송하는 방식입니다. 이 방식을 사용하려면, 중앙서버는 메시지를 가입한 사용자들의 그룹에 멀티캐스트로 전달해야 합니다. 루트 노드에 가입하는 방식에서는 멀티캐스트를 사용할 수도 있습니다. 예를 들어, 루트 노드에 가입한 사용자들을 하나의 그룹으로 구성하고, 중앙서버는 그룹에 멀티캐스트로 메시지를 전달할 수 있습니다.

12장 6번

Perrig 등이 제안한 분산형 그룹키 프로토콜과 Ren 등의 OFT(One-way Function Tree) 방식은 키 동의를 위해 Diffie-Hellman 키 동의 프로토콜을 사용하는 방법과 그렇지 않은 방법으로 차이가 있습니다. 이를 구체적으로 비교하겠습니다.

분산형 그룹키 프로토콜 (Perrig 등)

키 동의 과정: 트리의 단말부터 루트까지 올라가면서 Diffie-Hellman 키 동의 프로토콜을 계속 진행합니다.
예시: U1과 U2가 키 동의하여 확립한 키는 K12이고, U3와 U4가 확립한 키는 K34입니다. 이 경우, U2와 U4가 키 K14를 확립하기 위해서는 Diffie-Hellman을 사용하여 상위 노드로 키를 전파해야 합니다.
OFT 방식 (Ren 등)

키 동의 과정: 단말의 조부모 노드부터는 Diffie-Hellman을 할 필요가 없다고 주장합니다. 대신, 단말의 조부모 노드부터는 사전에 확립된 그룹키를

사용하여 키를 전파합니다.
예시: U1과 U2가 키 동의하여 확립한 키는 K12이고, U3와 U4가 확립한 키는 K34입니다. 이 경우, U2와 U4가 키 K14를 확립하기 위해서는 U2와 U4가 공유하는 공통 조상 노드인 루트 노드를 경유하여 키를 전파합니다. Diffie-Hellman을 사용하지 않고 사전에 확립된 그룹키를 이용하여 키를 전파하는 것이 OFT 방식의 특징입니다.
요약하면, 분산형 그룹키 프로토콜은 트리의 단말부터 루트까지 올라가면서 계속 Diffie-Hellman 키 동의 프로토콜을 진행하는 반면에 OFT 방식은 단말의 조부모 노드부터는 Diffie-Hellman을 사용하지 않고 사전에 확립된 그룹키를 이용하여 키를 전파합니다. OFT 방식은 상위 노드에서부터 키를 전파하기 때문에 키 동의에 필요한 계산량을 줄일 수 있고, 효율적인 키 관리를 가능하게 합니다.

12장 8번
CAS(Conditional Access System)는 일방향 통신 환경을 가정하여 만들어진 프로토콜로, 방송국에서 셋톱박스로의 단방향 통신을 지원합니다. 그러나 현재의 IPTV는 양방향 통신이 가능하므로, CAS를 개선하여 보다 효율적이고 안전한 방식으로 구현할 수 있습니다. 이를 위한 몇 가지 개선 방법은 다음과 같습니다:

양방향 통신을 활용한 키 관리: CAS는 일방향 통신 환경에서는 키 관리에 제약이 있을 수 있습니다. 하지만 양방향 통신을 지원하는 IPTV에서는 셋톱박스와 중앙 서버 간의 상호작용이 가능하므로, 보다 강력하고 유연한 키 관리 체계를 구축할 수 있습니다. 예를 들어, 중앙 서버는 동적으로 키를 갱신하거나 셋톱박스에 대한 인증과정을 수행하여 보안성을 강화할 수 있습니다.

개별 인증과 권한 관리: 양방향 통신에서는 개별적인 셋톱박스나 사용자 단말에 대한 인증과 권한 관리가 가능합니다. CAS를 개선하여 IPTV 환경에서는 각 셋톱박스 또는 사용자 단말에 대한 개별적인 인증을 수행하고, 권한 관리를 세밀하게 조정할 수 있습니다. 이를 통해 불법 복제나 해킹 등의 위협으로부터 보다 효과적으로 방어할 수 있습니다.

대화형 서비스 지원: 양방향 통신이 가능한 IPTV에서는 대화형 서비스를 제공할 수 있습니다. CAS를 개선하여 셋톱박스와 중앙 서버 간의 상호작용을 통해 사용자에게 다양한 인터랙티브 기능을 제공할 수 있습니다. 예를 들어, 사용자의 요청에 따라 특정 프로그램을 선택하거나 추가 서비스를 제공하는 등의 기능을 구현할 수 있습니다.

데이터 보안 강화: IPTV 환경에서는 데이터 보안에 대한 요구가 높아집니다. CAS를 개선하여 암호화 기술을 강화하고, 데이터 전송 중의 암호화와

디지털 저작권 관리(DRM) 시스템을 통합할 수 있습니다. 이를 통해 불법 복제 및 저작권 침해를 방지하고, 안전한 콘텐츠 제공을 실현할 수 있습니다.

13장 2 - 1, 2 - 2번

① 방법 1과 방법 2는 AES-CTR 모드로 데이터를 암호화한다고 가정하였을 때, 암호화하지 않은 상태와 암호화한 상태에서 공간 사용의 차이가 있습니다.

방법 1: 데이터마다 새로운 대칭키를 생성하고 이 키를 공개키로 암호화하여 암호화된 데이터와 함께 유지함

암호화된 데이터의 크기: 원본 데이터의 크기와 동일하거나 약간 증가함.
추가 공간 사용: 대칭키를 공개키로 암호화하여 저장해야 하므로, 암호화된 데이터와 함께 대칭키를 저장해야 합니다. 따라서 추가적인 공간이 필요합니다.
방법 2: 하나의 대칭키로 모든 데이터를 암호화하고 해당 대칭키를 로컬에 사용자가 안전하게 유지함

암호화된 데이터의 크기: 원본 데이터의 크기와 동일하거나 약간 증가함.
추가 공간 사용: 대칭키를 로컬에 유지하므로 암호화된 데이터와 함께 대칭키를 저장하는 추가적인 공간은 필요하지 않습니다.
즉, 두 방법 모두 암호화된 데이터의 크기는 원본 데이터의 크기와 비슷하거나 약간 증가하며, 추가적인 공간 사용은 대칭키를 저장하기 위해 필요한 부분입니다.

② 안전성 측면에서 방법 2에는 다음과 같은 문제가 있을 수 있습니다.

대칭키의 보안: 방법 2에서는 하나의 대칭키로 모든 데이터를 암호화합니다. 이 대칭키는 로컬에 사용자가 안전하게 유지해야 합니다. 그러나 대칭키를 유출하거나 노출되면, 해당 키로 암호화된 모든 데이터가 위험에 노출될 수 있습니다. 대칭키의 안전한 관리가 매우 중요하며, 이를 위해 안전한 키 관리 및 보호 메커니즘을 구현해야 합니다.

접근 제어: 방법 2에서는 대칭키를 로컬에 사용자가 유지합니다. 따라서 로컬 환경에 접근할 수 있는 사용자나 시스템에 대한 접근 제어가 중요합니

다. 물리적, 논리적인 접근 제어 및 인증, 감사 로그 등의 보안 메커니즘을 통해 대칭키에 대한 접근을 제한하고 모니터링해야 합니다.

대칭키 갱신과 롤오버: 방법 2에서는 대칭키를 사용하여 모든 데이터를 암호화합니다. 따라서 대칭키의 갱신과 롤오버(전환)를 수행하는 방법과 타이밍을 신중하게 고려해야 합니다. 갱신 및 롤오버 과정에서 데이터의 무결성과 안정성을 유지하며, 중단 없이 원활한 서비스를 제공해야 합니다.