

Security analysis of videoconferencing systems

TuX++

Matěj Plch, Lukáš Toldy, Maroš Valter

PB173 Tematicky zaměřený vývoj aplikací v jazyce C/C++

1 Robin Knaur's team (team name missing)

- Problem identification: `A_BadKeyUsage`
 - Severity: High
 - Description of the problem: On page 2 there is said that some message will be encrypted by the private key of the sender.
 - Proposed solution: Never encrypt messages using private key.
- Problem identification: `C_DangerousStrings`
 - Severity: Medium
 - Description of the problem: For strings basic `char*` is used.
 - Proposed solution: Use safer alternatives such as `std::string` or `QString`.
- Problem identification: `C_NotEnoughConsts`
 - Severity: Low
 - Description of the problem: Parameters, which obviously won't be changed, are not accepted as constants.
 - Proposed solution: Declare function/method parameters as `const` wherever it is possible.
- Problem identification: `A_InsufficientKeyLength`
 - Severity: Medium
 - Description of the problem: It is said that key length is 1024-bits, which is considered insufficient nowadays.
 - Proposed solution: Use longer keys instead, e.g. 2048-bits.
- Problem identification: `A_MissingTimeStamp`
 - Severity: Medium
 - Description of the problem: Attacker can record packets and try to resend them later to cause unexpected behaviour of the system.
 - Proposed solution: Add timestamps to verify freshness of the messages.

2 Hrochokobry

1.
 - Problem identification: A_Client-ServerCommunicationUnencrypted
 - Severity: high
 - Practicability: easy
 - Description of the problem: Communication between server and client is not protected by encryption or integrity control.
 - Proposed solution: Use authentication and encryption.
2. C_DangerousStrings
3. A_MissingTimeStamp

3 Sapiens

1. A_MissingTimeStamp