

Time left 0:03:05

Question 6

Not yet answered

Marked out of 2.00

Trong một giờ học ATTT, thầy Lâm giới thiệu 1 giao thức đơn giản cơ bản PRT_AU (xem dưới đây) và yêu cầu sinh viên bàn luận nhóm để phân tích mục đích & phê bình ưu-nhược; từ đó thử thiết kế một giao thức làm tốt hơn hoặc có lợi ích hơn về một phương diện nào đó.

PRT_AU: (thầy Lâm nêu đầu giờ)

- 1) $A \rightarrow S: ID_A$
- 2) $S \rightarrow A: \text{Password Request}$
- 3) $A \rightarrow S: H(PW_A)||T$

Trong đó một số ký hiệu sử dụng ở trên có ý nghĩa như sau:

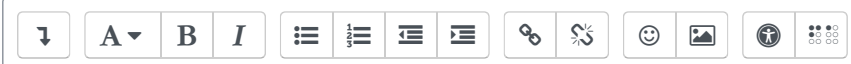
ID_A – là ID (danh tính) của A; R là 1 số ngẫu nhiên; T là một nhãn thời gian (Timestamp) tại thời điểm hiện thời (có thể sử dụng computer clock)

PW_A là chuỗi ký tự mật khẩu của A; p_A là giá trị băm của mật khẩu của A, tức là $p_A = H(PW_A)$ và với H là một hàm băm xác định công bố trước.

Sinh viên Dũng phân tích ra một nhược điểm của giao thức này và đề xuất bản sửa có thêm điểm mới:

- 1) $A \rightarrow S: ID_A$
- 2) $S \rightarrow A: R$
- 3) $A \rightarrow S: \{R+1\}p_A$
- 4) $S \rightarrow A: \{k_s\}p_A$

Hãy cho biết bạn Dũng đã có những ý kiến gì?



[← Announcements](#)

Jump to...

