Internet考试2020回忆版

> *Isn't it lovely?*

Author list:

- Dong Yibo
- 化名为邓小宇的王力凡同学
- wqx
- 「哈哈同学」

名词解释：

A卷:

- 挑战-应答
- 安全协议
- P believe X

  ~~“P believe X 不就是相信吗！这怎么解释！”~~
- 重放攻击
- 前向无关性

B卷:

- P control X
- 数字信封
- 传输模式
- 前向无关性
- 公钥环

简答

- 时戳和Nonce的区别和联系
- 分析协议过程和目的(A.)（ B卷为D-S协议）

  $1) A \rightarrow B : M, A, B, E(Kas : Na, M, A, B)$

  $2) B \rightarrow S : M, A, B, E(Kas : Na, M, A, B), E(Kbs : Nb, M, A, B)$

  $3) S \rightarrow B : M, E(Kas : Na, Kab), E(Kbs : Nb, Kab)$

  $4) B \rightarrow A : M, E(Kas : Na, Kab)$
- 分析Kerberos协议中Ticketv和认证头的结构和作用

$$\mathbf{C} \rightarrow \mathbf{V} \quad Ticket_v \| Authenticator_c$$

$$\mathbf{V} \rightarrow \mathbf{C} \quad \mathrm{E}(K_{c,v}, [TS_5 + 1]) \text{(for mutual authentication)}$$

$$Ticket_v = \mathrm{E}(\mathrm{K}_v, [\mathrm{K}_{c,v} \| \mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{ID}_v \| \mathrm{TS}_4 \| \mathrm{Lifetime}_4])$$

$$Authenticator_c = \mathrm{E}(\mathrm{K}_{c,v}, [\mathrm{ID}_C \| \mathrm{AD}_C \| \mathrm{TS}_5])$$

- IKE中两个阶段协商SA的联系和区别

综合题

- 分析协议目的，说明可能受到的攻击和加固方法(A.)(B卷为O-R协议)

  1) A→S: A, B

  2) S→A: Certa, Certb

  3) A→B: Certa,Certb,E(Kb:E(Ka^{-1}:Kab,T))

- 根据SET中Preq的图，说明SET协议中的商家(A.) (B. 支付网关)行为。