Exercise Class December 10, 2020

This is a slightly edited and re-formated transcript of the live notes taken in class.

Exercise Sheet 4

Task: "Are we Missing Something?"

question: is there a protocol that (with FAIL/BREAK rules) is formally secure, but not secure "in real life?"
main challenge: add FAIL constant to right place. E.g., have the FAIL-rule work only for a "specific attack."

cause 1: security goal is "too narrow:"

- example protocol 1 first exchanges N_A, N_B, then example protocol 2 uses these for symmetric encryption: $\mathsf{enc}^{\mathsf{s}}_{[N_A,N_B]}(m)$
- specified goal for protocol 1: "adversary cannot get N_A and N_B"
  $[BREAK, N_A, N_B] \rightarrow \mathsf{FAIL}$
- real goal for protocol 2 : "adversary cannot get plaintext" (decryption of $\mathsf{enc}^{\mathsf{s}}_{[N_A,N_B]}(m)$)

when is this problematic?

- assumption: the only way for ADV to get m is to decrypt $\mathsf{enc}^{\mathsf{s}}_{[N_A,N_B]}(m)$.
- problem: if ADV can get m in another way.

when is this problematic?
example protocol:

- ... steps to exchange N_A and N_B ...
  Alice: $B \rightarrow \mathsf{enc}^{\mathsf{s}}_{[N_A,N_B]}(m)$
  Bob: $y \rightarrow$ ok
  Alice: ok $\rightarrow m$

cause 2: BREAK/FAIL rules are not applicable at some point in the protocol run, making one participant "hang." see example in solution

guidelines for BREAK/FAIL rules to prevent this?

- cause 1: be specific about the goal of the protocol (keep m secret), not the tools (keep N_A, N_B secret)
- cause 2: non-blocking FAIL rule: only have these at end of protocol, **exception**: there might be a blocking rule in real protocol. So, use own instance for FAIL-rule (might need access to (variables), nonces, etc)

Exercise Sheet 5

Task: "Exponential attack size"

Is there a simpler protocol (with more messages) where $\sigma(x)$ will also be exponential, but structure is "simpler?"

Ping-Pong protocol:

$$
\begin{array}{lcl}
x_1 & \rightarrow & \mathsf{enc}_k^{\mathsf{s}}([1,[x_1,x_1]]) \\
\mathsf{enc}_k^{\mathsf{s}}([1,x_2]) & \rightarrow & \mathsf{enc}_k^{\mathsf{s}}([2,[x_2,x_2]]) \\
\mathsf{enc}_k^{\mathsf{s}}([2,x_3]) & \rightarrow & \mathsf{enc}_k^{\mathsf{s}}([3,[x_3,x_3]]) \\
\mathsf{enc}_k^{\mathsf{s}}([3,x_4]) & \rightarrow & \mathsf{enc}_k^{\mathsf{s}}([4,[x_4,x_4]]) \\
\mathsf{enc}_k^{\mathsf{s}}([4,x_5]) & \rightarrow & \mathsf{enc}_k^{\mathsf{s}}([5,[x_5,x_5]]) \\
\vdots & \vdots & \vdots \\
\mathsf{enc}_k^{\mathsf{s}}([n,x_n]) & \rightarrow & \mathsf{FAIL}
\end{array}
$$