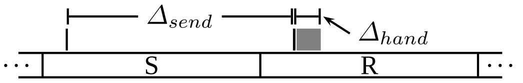
This document contains an appendix to the article *Information-Theoretic Modeling and Analysis of Interrupt-Related Covert Channels* by Heiko Mantel and Henning Sudbrock. The article appears at the Workshop on Formal Aspects in Security and Trust 2008.

A Probabilistic System Behavior

To integrate probabilistic behavior of the system into the model, we define the probabilities $P_C[i, o]$ based on two random variables, $\varDelta_{send}$ and $\varDelta_{hand}$. The value of $\varDelta_{send}$ represents the time that passes between a transmission request and the corresponding interrupt request, while the value of $\varDelta_{hand}$ represents the amount of time that it takes to handle the interrupt request caused by a given transmission request. We assume that the probability distributions of these random variables are independent. This assumption is supported by experiments we performed on a real system. The values of the random variables $\varDelta_{send}$ and $\varDelta_{hand}$ are depicted in the following diagram:



For the following definition of the probabilities $P_C[i, o]$, we assume that, whenever the sending process performs transmission requests, the order of the corresponding interrupt requests is unchanged. We confirmed this assumption on a system running a Linux kernel (version 2.6.20.7), using an Intel 82573L Ethernet controller. On this system, the random variable $\varDelta_{send}$ took values between approximately 89 and 98 microseconds, while a transmission request took approximately 17 microseconds. We furthermore assume that transmission requests in the sending process' time-slot do not cause interrupt requests after the subsequent time-slot of the receiving process (i.e., $\varDelta_{send} < l$), which we also confirmed in experiments.

To define the probabilities $P_C[i, o]$, let $i = [t_1, \dots, t_j] \in I''_C$ as well as $o = [(s_1, d_1), \dots, (s_k, d_k)] \in O_C$. We distinguish the three different cases $j < k$, $j = k$, and $j > k$, where j is the number of transmission requests represented by i, and k is the number of interrupt requests represented by o.

We assume throughout this section that all interrupt requests are caused by transmission requests of the sending process.

In the case that $j < k$, we define $P_C[i, o] = 0$, because j transmission requests do not cause more than j interrupt requests.

If $j = k$, each transmission request represented by the input symbol must cause an interrupt request represented by the output symbol. Since the order of the interrupt requests is the same as the order of the transmission requests, the transmission request at time t_m causes the interrupt request at time s_m for all m. The probability that this is the fact is given by

$$\prod_{m=1}^{k} p(\varDelta_{send} = s_m + l - t_m). \qquad (1)$$

Moreover, the probability that the respective execution times of the interrupt handler are given by the list $[d_1, \ldots, d_k]$ equals

$$\prod_{m=1}^{k} p(\mathit{\Delta}_{hand} = d_m). \tag{2}$$

Therefore, for $j = k$ we define the probability $P_C[i, o]$ as the value obtained by multiplying the Products (1) and (2), resulting in

$$P_C[i, o] = \prod_{m=1}^{k} \bigl[p(\mathit{\Delta}_{send} = s_m + l - t_m) * p(\mathit{\Delta}_{hand} = d_m)\bigr]. \tag{3}$$

If $j > k$, the k interrupt requests are caused by the last k transmission requests, because the assumption $\mathit{\Delta}_{send} < l$ implies that the interrupt requests caused by the transmission requests do not occur after the receiving process' time-slot. The first $j - k$ transmission requests do not cause interrupt requests represented in the output symbol. We compute the probabilities for these two statements separately, the probability $P_C[i, o]$ is then defined as their product. The probability that the k interrupt requests are caused by the last k transmission requests equals $P_C[[t_{j-k+1}, \ldots, t_j], [s_1, \ldots, s_k]]$ and can be computed with Formula (3) in the case for $j = k$.

Transmission requests only cause an interrupt request handled in $\mathit{\Delta}_{hand}$ time units that is not represented in the output symbol if it is requested $\mathit{\Delta}_{hand}$ time units before the receiving process' time-slot or earlier. Using the assumption that the order of interrupt requests corresponds to the order of transmission requests, the probability that the first $j - k$ transmission requests do not cause interrupt requests represented in the output symbol is therefore given by $p(t_{j-k} + \mathit{\Delta}_{send} \leq l - \mathit{\Delta}_{hand})$. In summary, in the case $j > k$ the probability $P_C[i, o]$ is defined as

$$p(t_{j-k} + \mathit{\Delta}_{send} \leq l - \mathit{\Delta}_{hand}) * P_C[[t_{j-k+1}, \ldots, t_j], o].$$