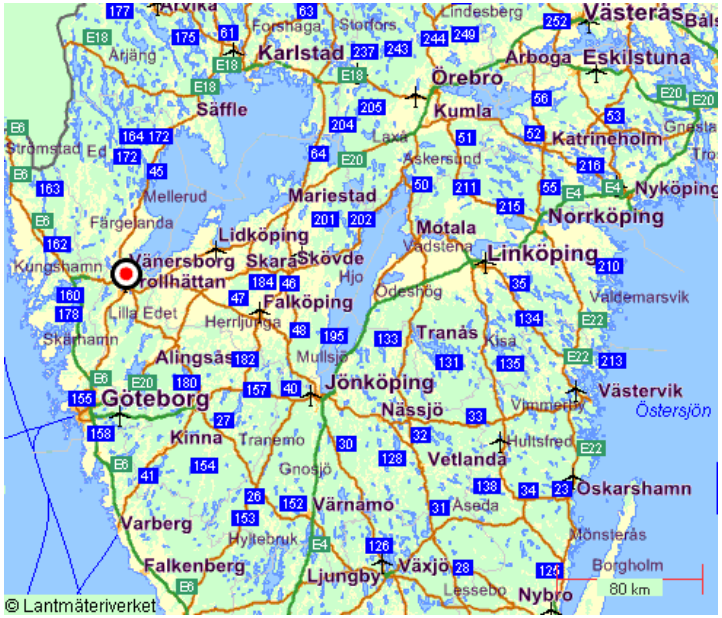
Stochastic Models for Security Evaluation

Karin Sallhammar,
Centre for Quantifiable Quality of Service in Communication Systems (Q2S)
Norwegian University of Science and Technology (NTNU),
Trondheim, Norway
sallhamm@q2s.ntnu.no

Background - personal

- I was born in Vänersborg and went to university in Norrköping (MSc in Media Technology and Engineering).



- I started as a PhD student at Q2S/NTNU in March 2003 and expect to finish in March 2007.

Background - thesis

- Goal: a method to obtain quantitative measures of security
- Idea: apply the dependability paradigm to security
- Dependability models for obtaining quantitative measures are well-known and effective
  - Static models: fault trees, reliability block diagrams, reliability graphs
  - Dynamic models: state diagrams, petri nets
- Quantitative analysis is performed by
  - Mathematical analysis: probabilities, stochastic processes
  - Experimental analysis: simulation

Previous Work

- Applying the dependability paradigm to security
  - Littlewood, et.al.: Towards operational measures of computer security (1993)
  - Jonsson, Strömberg and Lindskog: On the Functional Relation Between Security and Dependability Impairments (1999)
  - Malicious and Accidental Fault Tolerance for Internet Applications - MAFTIA (2001)

- Markov chains / stochastic Petri nets
  - Ortalo, Deswarte: Experimenting with quantitative evaluation tools for monitoring operational security (1999)
  - Stevens, et.al.: Model-based validation of an intrusion-tolerant information system (2004)
  - Madan, et.al.: A method for modeling and quantifying the security attributes of intrusion tolerat systems (2004)

System Failures vs. Security Breaches

- Similar to failures, attacks can be modelled as a series of (intentional) state changes of the system. A successful intrusion will often consist of many subsequent elementary atomic attack actions.

- HOWEVER: Attacks may not always be well characterized by models of random natures; the time/effort an attacker spend may be random, but his decision is not!

- Approaches previously applied on state transition (stochastic) models of security
  - Least cost algorithms (analyses the effort of different paths to the goal)
  - Markov decision processes (choose the transition which maximizes the probability of reaching a success state)

- Drawback: none of these methods include that an attacker may consider the risk of his actions before he acts. Also, they assume that the attacker always has one single goal in mind.

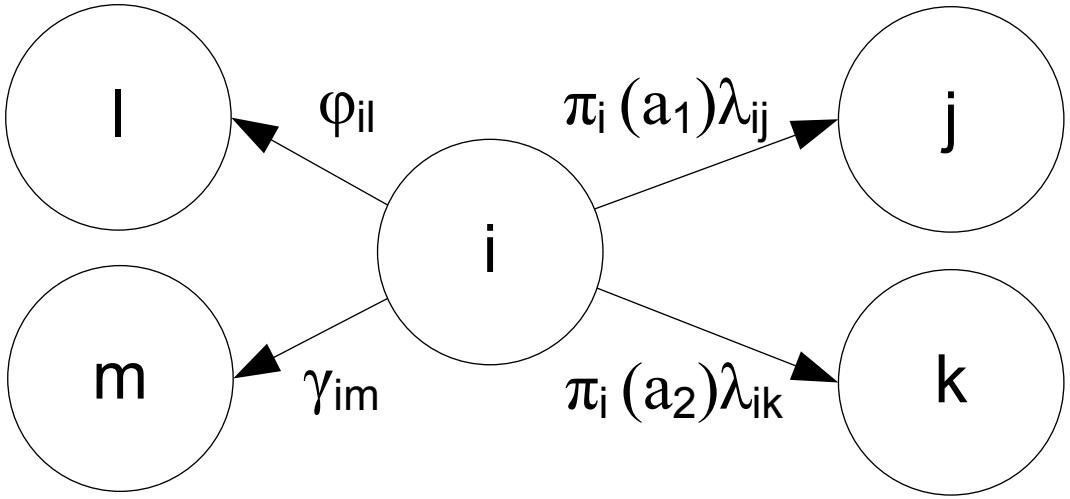
State-based Stochastic Modelling

- Model the security of a system as a CTMC with states $i = 1, \ldots, N$.
- State probabilities $\mathbf{X(t)}=\{X_1(t), X_2(t), \ldots, X_N(t)\}$
- State equation describing system behavior $\frac{d}{dt}\mathbf{X(t)} = \mathbf{X(t)Q}$ where $\mathbf{Q}$ is the $N \times N$ state transition rate matrix of the system. The element $ij (i \neq j)$ of $\mathbf{Q}$, is
  - $q_{ij} = \lim_{dt \to 0} \{\frac{\Pr(\text{system state changes from } i \text{ to } j \text{ in } (t, t+dt))}{dt}\}$
  - $q_{ii} = -\sum_{j \neq i} q_{ij}$
- To find steady state probabilities $X_i = \lim_{t \to \infty} X_i(t), i = 1, \ldots N$, solve the set of N equations given by
  - $N - 1$ of the N equations $\mathbf{XQ} = \mathbf{0}$,
  - the Nth equation $\sum_{l=1}^{N} X_l = 1$.

Incorporate Intentional Attacks

- Idea: represent attacker behavior as a probability distribution over all possible actions in each state

- Example:



$$\pi_i(a_1) + \pi_i(a_2) + \pi_i(\phi) = 1$$

- The attacker strategy $\Pi = \{\pi_i, i = 1 \ldots, z\}$ whereof $\pi_i = \{\pi_i(a), a \in A\}$.

Modelling Attacker Behavior

- Motivation (money, status, entertainment, etc..) and demotivation (conseq. of detection, crimilal offense,...) factors

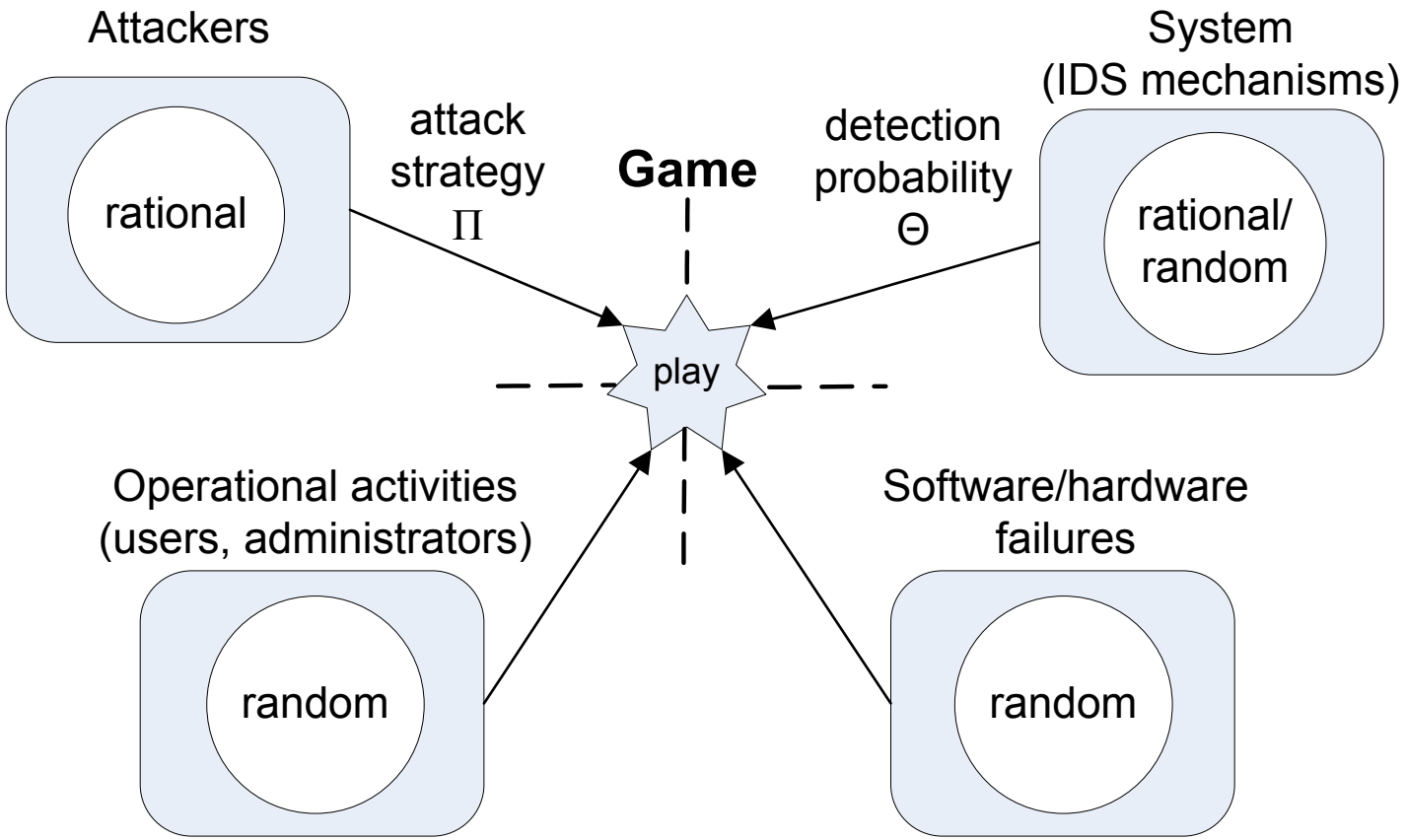
- For each stage (which corresponds to a system security related state) of the attack, the attacker can
  - Attack by performing the next elementary step of the attack
    - If the attacker succeeds the system will be transferred into next state
    - If the attacker fails the system will remain in its current state
  - Resign and interrupt the ongoing attack
    - The system will remain in its current state

  At each intermediate stage of the attack, the attempt may be detected and measures taken by the system owner to interrupt the ongoing attack

- How can we compute the expected attacker strategy Π?

Formalization

A two-player, zero-sum, multistage game $\Gamma = \{\Gamma_i, i = 1, \ldots, z\}$



The Game Model

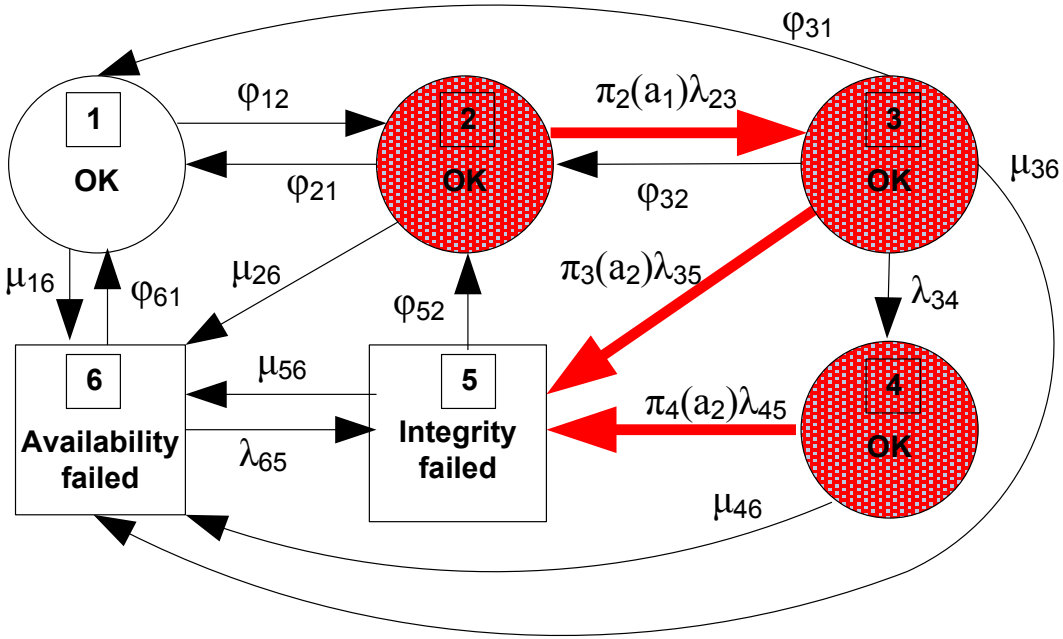
- Each Γ_i is represented by $\Gamma_i = \begin{array}{c} \text{undetected} \quad \text{detected} \\ \begin{pmatrix} \vdots & \vdots \\ \mu_{i1}(a_m) & \mu_{i2}(a_m) \\ \vdots & \vdots \end{pmatrix} \end{array}$ whose entries are
  - $\mu_{i1}(a_m) = r_i(a_m|\text{undetected}) + \sum_{j=1,\ldots,z} p_{ij}(a_m)\Gamma_j$, and
  - $\mu_{i2}(a_m) = r_i(a_m|\text{detected})$

  for which $p_{ij}(a_m) \geq 0$, and $\sum_{j=1,\ldots,z} p_{ij}(a_m) < 1$. The transition probabilities $p_{ij}(a_m)$ is computed from the embedded discrete process of the Markov chain by conditioning of the chosen action

- The expected reward for an attacker in state i under strategy π_i
  - $E(\pi_i, \theta_i) = \sum_{\forall a \in A} \pi_i(a)\Big((1-\theta_i(a))\mu_{i1}(a) + \theta_i(a)\mu_{i2}(a)\Big)$

- Attackers' expected choice of strategy: $\max_{\pi_i} E(\pi_i, \theta_i)$

Example



- Pick out the game elements
- Construct the action set
- Assign reward and cost values
- Compute transition probabilities and solve the game

Conclusions

- Preliminary Results
  - Karin Sallhammar, Bjarne E. Helvik and Svein J. Knapskog, *Incorporating Attacker Behavior in Stochastic Models of Security*. Proceedings of SAM'05, Las Vegas, USA, June 20-23, 2005.
  - Karin Sallhammar, Svein J. Knapskog and Bjarne E. Helvik, *Using Stochastic Game Theory to Compute the Expected Behavior of Attackers*. Proceedings of SAINT2005, Trento, Italy, Jan. 31 - Feb. 4, 2005.
  - Karin Sallhammar and Svein J. Knapskog, *Using Game Theory in Stochastic Models for Quantifying Security*. Proceedings of Nordsec2004, Espoo, Finland, November 4-5, 2004.

- Future work
  - attacker profiles
  - time-dependent success-probabilities
  - the "perfect knowledge" game assumption
  - modelling and simulation of real-world scenarios