Modeling Security with Graphs, etc.

IARPA/NSA/NSF Workshop: Sciences of Security

Joshua D. Guttman

The MITRE Corporation

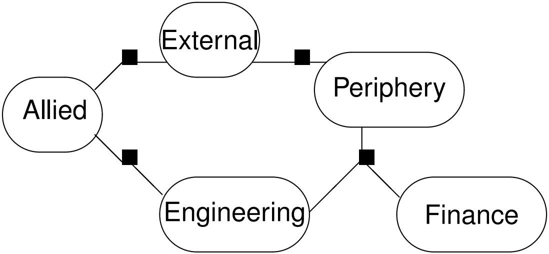
17 Nov. 2008

Sciences of Information Security

- Science requires simple models
- Models are inaccurate
- Science requires ways to appraise:
  - When is this model good enough?
  - Which questions can I answer with this model?

Packets and Trajectories

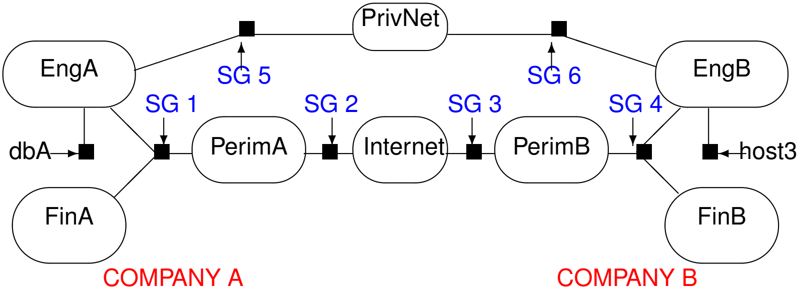
Filtering routers (example 1)



What's it good for?

- Clarifies:
  - Security goals: Which packets permitted on which paths
  - Localization choices to enforce goals
  - Matches well-defined mechanism
- Leaves in shadows:
  - Connections, routing
  - Mechanisms that transform packets
  - Authentication, confidentiality
  - Application-level proxies
  - Which vulnerabilities are actually present

IPSec protocols



What’s it good for?

- Clarifies:
  - Security goals: Packets with state along paths
  - Localization choices to enforce goals
  - Matches well-defined mechanism
  - Some mechanisms that transform packets
  - Authentication, confidentiality
- Leaves in shadows:
  - Connections, routing, application-level proxies
  - Other mechanisms that transform packets
  - Which vulnerabilities are actually present

Crypto protocols

$$\begin{tikzcd}
\bullet \arrow[r, "\{\!|Q,\, N_a,\, Y_a,\, A|\!\}_B"] \arrow[d, Rightarrow] & {} \arrow[r, phantom, "\prec"] & {} \arrow[r, "\{\!|Q,\, N_a,\, Y_a,\, A|\!\}_B"] & \bullet \arrow[d, Rightarrow] \\
\bullet \arrow[d, Rightarrow] & {} \arrow[l, "\{\!|Y_a,\, K,\, B|\!\}_A"'] \arrow[r, phantom, "\succ"] & {} & \bullet \arrow[l, "\{\!|Y_a,\, K',\, B|\!\}_A"'] \\
\bullet \arrow[r, "\{\!|Q|\!\}_K"] & {} & &
\end{tikzcd}$$

Does $K' = K$?

Maybe not

Questions about applicability

of a given model

- What sort of adversary is expected?
- What outcomes benefit adversaries?
  . . . harm us?
- What actions are available in real system, but not represented in model?
- Do unrepresented actions affect properties the model represents?