AGILE case study: Discussion on performance and security analysis of a mobile computing example

Stephen Gilmore
(plus contributions from project members)

DEGAS Workshop, 2nd September 2004

Purpose of the AGILE case study

- Represent a mobile object system.
- Mobility should be about acquiring (and losing) capabilities.
- There are different kinds of mobility.
  - Some things move themselves (Hubert)
  - Some things are moved (Hubert's laptop)
  - Some things do not move (Charles de Gaule airport)
- Use the existing DEGAS tools.
- Performance measures: *utilisation* of Hubert's laptop (maximise this), plus trip-time (minimise this).

PEPA model of the laptop

$$
\begin{aligned}
LaptopOff &= (powerUp, r_{pU}).LaptopOn \\
LaptopOn &= (compute, r_c).LaptopOn \\
&+ (crash, r_{cr}).LaptopDown \\
&+ (powerDown, r_{pD}).LaptopOff \\
LaptopDown &= (reboot, r_r).LaptopOn
\end{aligned}
$$

The laptop is utilised when it is on (and not utilised when it is off, or down).

PEPA model of Hubert (Outward journey)

$$
\begin{aligned}
&Hubert_{MUN} = \\
&\quad (compute, \top).Hubert_{MUN} \\
&+(called, \top).(powerDown, \top).(board, \top).Hubert_{LH123}
\end{aligned}
$$

$$
\begin{aligned}
&Hubert_{LH123} = \\
&\quad (compute, \top).Hubert_{LH123} \\
&+(signOff, \top).(powerUp, \top).Hubert_{LH123} \\
&+(signOn, \top).(powerDown, \top).Hubert_{LH123} \\
&+(deplane, \top).Hubert_{CDG}
\end{aligned}
$$

PEPA model of Hubert (Return journey)

$$
\begin{aligned}
&Hubert_{CDG} = \\
&\quad (compute, \top).Hubert_{CDG} \\
&+(called, \top).(powerDown, \top).(board, \top).Hubert_{AF123}
\end{aligned}
$$

$$
\begin{aligned}
&Hubert_{AF123} = \\
&\quad (compute, \top).Hubert_{AF123} \\
&+(signOff, \top).(powerUp, \top).Hubert_{AF123} \\
&+(signOn, \top).(powerDown, \top).Hubert_{AF123} \\
&+(deplane, \top).Hubert_{MUN}
\end{aligned}
$$

PEPA model of a plane

$$LH123_{MUN} = (called, r_{ca}).(board, r_b).(takeOff, r_{tO}).LH123_{air}$$

$$LH123_{air} = (signOff, r_{s_{off}}).(signOn, r_{s_{on}}).(land, r_l).LH123_{CDG}$$

$$LH123_{CDG} = (deplane, r_d).LH124_{CDG}$$

Alternative models

Alternative scenarios:

- Hubert flies to Schipol with KLM, then to CdG
- Hubert takes the TGV to Frankfurt, then flies to CdG
- Hubert takes the TGV to CdG

Different results for the same measure

Additional details:

- Some airports offer WiFi access points.
- Some airplanes offer WiFi.

Different performance measure which is an aggregate of connected utilisation plus disconnected utilisation

Discussion of security issues

- Boarding the plane requires *authentication*.
- The laptop connects to server, requiring secure protocol.
- During the journey, the plane crosses different administrative boudaries, requiring handover protocol.
- Regulations: require well-behaved passengers (like Hubert) who obey the rule to switch off electronic equipment. Prevent non-well-behaved passengers from boarding the plane?
- Idea: acquire token (permissions) when boarding which is used to permit computing or network access.
- Planes with WiFi: shut down Internet server when signs are lit.

Conclusions

- For the AGILE case study we can compute some simple or some more complex quantitative measures.
- For the case study we can *identify* points where a security analysis is needed, which are places in the story where a secure communication is established. Then, the existing DEGAS tools have already been used for the analysis of the protocols which would be used here (Diffie-Helmann, Needham-Schroeder, Kerberos, etc).