Ambient posix capabilities

Serge Hallyn

Canonical, Ltd

serge.hallyn@ubuntu.com

August 21, 2015
Capability recalculation

\[ pB' = pB \]
\[ pI' = pI \]
\[ pP' = (pB \& fP) \mid (fI \& pI) \]
\[ pE' = fE \, ? \, pP' : 0 \]
What people thought \( p_I \) should have been

\( p_A \) must be a subset of \( p_I \) and \( p_P \)

Current ways of dropping privilege still work
  
  \( p_A \) cleared for setuid, fcaps, keepcaps
What people thought pI should have been
- pA must be a subset of pI and pP
- Current ways of dropping privilege still work
  - pA cleared for setuid, fcaps, keepcaps

\[
\begin{align*}
pB' &= pB \\
pA' &= (\text{fcaps} | \text{setxid}) \ ? 0 : pA \\
pI' &= pI \\
pP' &= (pB \ & \text{fP}) \ | \ (fI \ & \ pI) \ | \ pA' \\
pE' &= fE \ ? \ pP' : pA'
\end{align*}
\]
Namespaced file capabilities

- File caps cannot be set in user namespace
- Software in container must handle both file caps and setuid-root
- Less complexity → better
- Proposed:
  - sets of file capability sets
  - each tagged with users root k_uid