
IDS and NAC
TF-Mobility Sept 2007



- Intrusion Detection Systems
- Network Access Control
- ... and where does roaming come into play?

End-user network access



- end-user networks face worries...
 - ❑ infected computers spread spam
 - ❑ may infect others in LAN
 - ❑ deliberate illegal use by end user
 - ❑ AUP breaches (maybe even by accident)
- traditional ways to handle this:
 - ❑ client isolation (port-security)
 - ❑ firewalls or proxies prevent access to shady regions of the internet

Addition: reactive safeguards



- Intrusion Detection Systems
 - monitor network usage
 - supposed to detect malicious activity
 - completely user-transparent
 - some provide contention measures on detection
- widely accepted as a GoodThing(tm)
- plenty of vendors offer plenty of solutions
- interop between vendors not urgent

Addition: proactive safeguards



- relatively new idea: reduce risk of having infected users by scanning before network access – Network Access Control (NAC)
- just like in airports: access permission only after thorough security check
- makes sure that machine is configured according to network policies
 - anti-virus up-to-date?
 - latest patches installed?
 - maybe: no BitTorrent software installed?

downsides



- NOT user-transparent:
 - user needs to install or run piece of network-provided software
 - faces hassle of updating even if the machine may not be threat to network
- some vendors offer it, but interop IS problematic (=non-existent right now)
- can't replace IDSes
 - can not detect deliberate malicious activity
 - tries to sustainably change **user** behaviour (changes mission statement!)
- can be seen as privacy invasion
- “lying endpoint” problem not solved

roaming networks and NAC



- user has no inherent trust to visited network
- installing/running software coming from untrusted third party?
- roaming n times may mean m different NAC scanners?
- how to signal admission decision? (some solutions put it into EAP)
- standardisation could come to the rescue
 - install software once, from (trusted) home network
 - same scanner can report to any backend

What to do?



- Can we really give a cross-the-board answer to the question: should NAC be used or not?
- If yes: what is it?
- If no:
 - it will be a case-by-case decision at the local place
 - then we really should strive to get interop!
- Should we try to influence development of open-source solutions?
- Continue standardisation efforts?