Lecture 15

Monday, 16 January 2023 18:52

'important'/'interesting' topics: falsifiability of security claims (e.g. change password often)

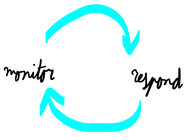
today: monitorability

it is strikingly easy to break into a system

attack symptoms are hard to monitor

supply chain attacks: attack libraries

prevention does not work, because systems will never be perfect



desired aspects intrusion detection systems:

low false negatives / high detection rate → effectiveness

low false positives — high false positives → high usage costs

additional parameters for IDS:

actionability — what should the customer do?

adaptability — costs of adapting to changes in IT systems

scalability — cost increases w.r.t. number of deployments increases (marginal costs)

knowledge-based — blacklisting (actionable, adaptable, scalable) e.g. anti-virus — only detect fraction of attacks

behavior-based — whitelisting e.g. firewall

where do we obtain knowledge?

- give specification → recognize good behavior → if not good, may be bad but not necessarily
  - not adaptable, not scalable
- learn automatically — anomaly-based systems
  - black box — machine learning — inefficient, unstable
  - white box — explain semantics of target system — works, but no specifications only

achieving privacy by unsupervisability is comparable to achieving security by obscurity

suggestion: make software more supervisable