CO331: Network and Web Security

Tutorial 3: Threat Modeling for Networks*

February 2, 2018

Describe a threat posed by the given network attacker in each of the following scenarios. Assign a STRIDE category (**S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of service, **E**levation of privilege) to each threat you identify, then propose a way of addressing each threat.

A reminder of the network attacker types:

Eavesdropper: a passive attacker capable of reading packets sent on the network; e.g. wiretapper, wifi sniffer.

Off-path attacker: an active attacker, but not necessarily positioned between the two victims; can create arbitrary packets and inject them into the network, can act as a legitimate participant in a protocol.

Man in the middle: an active attacker positioned directly on the network path between the two victims; capable of intercepting traffic and reading/modifying/creating/deleting packets. It can also act like an off-path attacker if needed.

1. Describe a threat posed by an eavesdropper to a web application served over HTTP.
2. Describe a threat posed by an eavesdropper to a web application served over HTTPS.
3. Describe a threat posed by an off-path attacker to a web application served over HTTP.
4. Describe a threat posed by an off-path attacker to a web application served over HTTPS.
5. Describe a threat posed by a man in the middle to a web application served over HTTP.
6. Describe a threat posed by a man in the middle to a web application served over HTTPS.

*Thanks to Chris Novakovic `c.novakovic@imperial.ac.uk` for preparing this material.