Expertise

Adversary's Resources

Expertise

Adversary's Resources

What levels of expertise does the adversary have (or have access to)? How do different kinds of expertise allow the adversary to execute a broader range of attacks on your system?

Example Related Concepts

Example Expertise: novice at network penetration · expert at picking locks · proficient con artist

Example Contributors: hobbyist adversary · government adversary

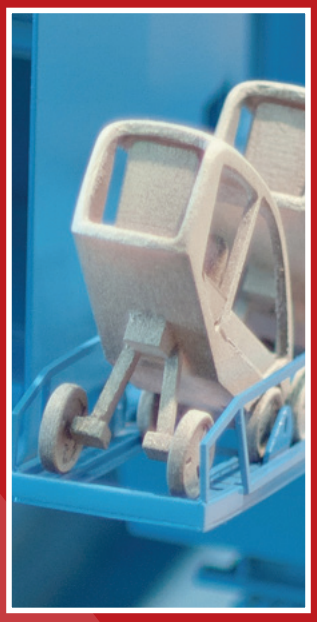
A Future World

Adversary's Resources

A Future World

Adversary's Resources

What kinds of new opportunities might be available to the adversary in the future? How might future changes to the technology, its usage, or the surrounding world affect the abilities of the adversary to attack your system?



Example Related Concepts

Example Contributors: cyber-physical or sensor-rich systems · increased technology adoption or reliance · increasing connectivity

Example Outcomes: new potential victims · new potential harms to victims · cheaper or more efficient attacks

Impunity

Adversary's Resources

Impunity

Adversary's Resources

What kinds of impunity might the adversary have? How might impunity for their actions make adversaries free to execute more frequent, longer-lasting, or more obvious attacks on your system?

Example Related Concepts

Example Causes: unafraid of incarceration · government sponsorship · utilizing network proxies and redirection

Example Contributors: geo-political diversity · anonymity

Inside Capabilities

Adversary's Resources

Inside Capabilities

Adversary's Resources

What kinds of inside capabilities might the adversary have (or gain) access to? How might inside access or influence allow the adversary to execute new or more effective attacks on your system?

Example Related Concepts

Example Capabilities: physical access · user or admin account · system backdoors · affect system design

Example Sources: a collaborating insider · blackmail · bribery · counterfeit hardware

Inside Knowledge

Adversary's Resources

Inside Knowledge

Adversary's Resources

What kinds of inside knowledge might the adversary have (or gain) access to? How might inside knowledge allow the adversary to execute new or more effective attacks on your system?

Example Related Concepts

Example Knowledge: design documents · system usage or maintenance patterns · implementation details · bureaucratic processes

Example Sources: employment · a collaborating insider · discarded documents

Money

Adversary's Resources

Money

Adversary's Resources

What kinds of liquid assets might the adversary have access to? How might different levels of liquid assets amplify or enable attacks on your system?

Example Related Concepts

Example Contributors: organized crime adversary · corporate adversary

Example Uses: pay bribes · purchase equipment · hire help

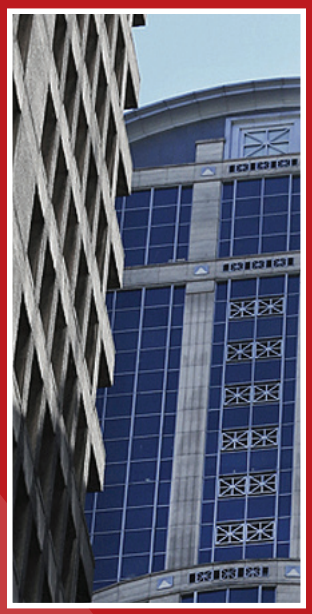
Power or Influence

Adversary's Resources

Power or Influence

Adversary's Resources

What kinds of power or influence does the adversary have? How can the adversary leverage them to amplify or enable attacks on your system?



Example Related Concepts

Example Uses: mobilize large volunteer force · affect laws or regulations · coerce employees

Example Contributors: government adversary · religious or movement leader

Time

Adversary's Resources

Time

Adversary's Resources

What kinds of time limits does the adversary have (or not have) on attacks? How do different timeframes allow the adversary to execute different kinds of attacks or cause more damage to your system?

Example Related Concepts

Example Timeframes: seconds · hours · decades

Example Contributors: a current or upcoming event (e.g. election) · ability to execute a time-independent attack · scheduled system maintenance

Tools

Adversary's Resources

Tools

Adversary's Resources

What kinds of specialized or generic hardware, software, or other equipment might the adversary have access to? How might different kinds of tools allow the adversary to execute new or more effective attacks on your system?

Example Related Concepts

Example Tools: cryptographic key crackers · reverse engineering tools · helicopters

Example Contributors: hobbyist adversary · government adversary · corporate adversary

Unusual Resources

Adversary's Resources

Unusual Resources

Adversary's Resources

What kinds of unexpected or uncommon resources might the adversary have access to? How might unusual resources enable or amplify attacks on your system?