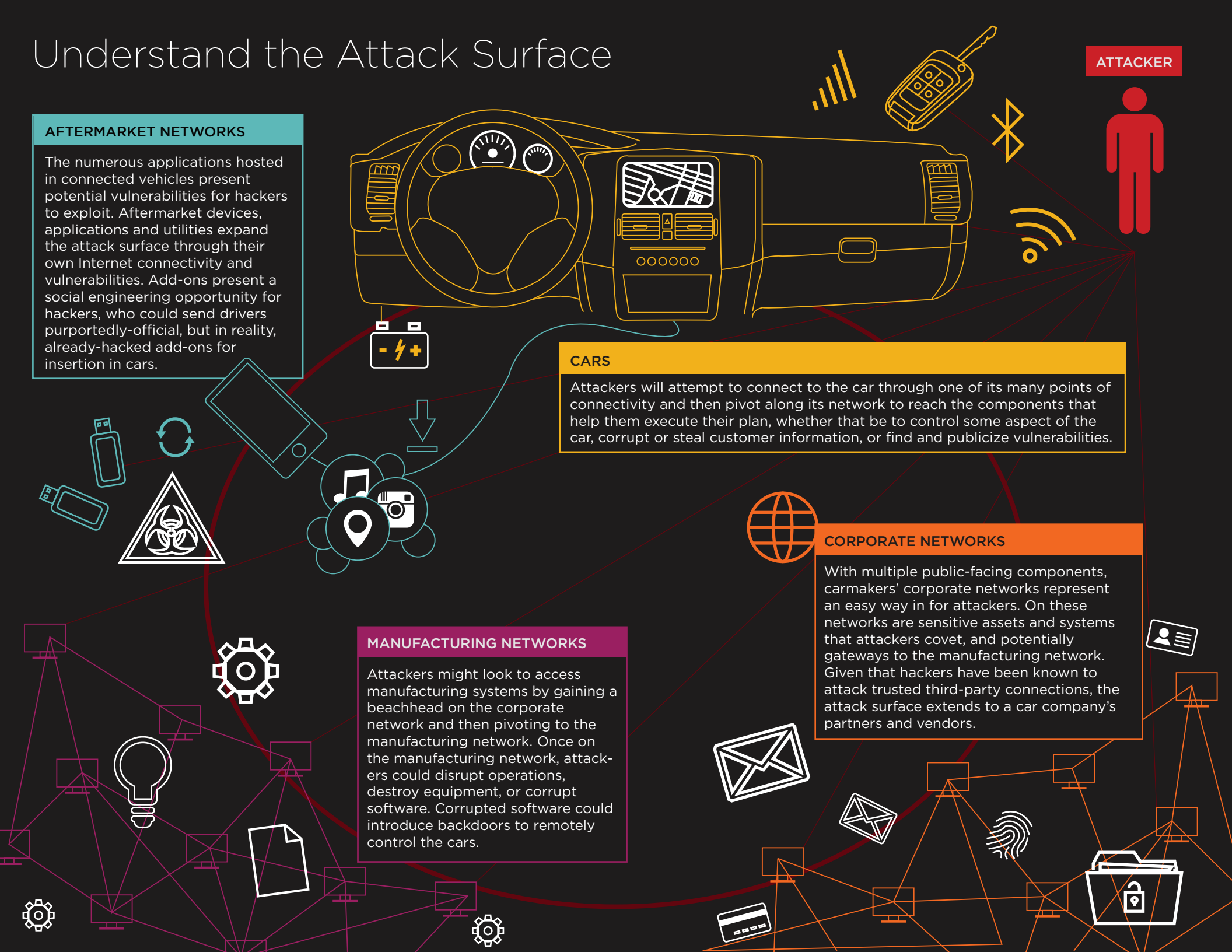
Understand the Attack Surface



AFTERMARKET NETWORKS

The numerous applications hosted in connected vehicles present potential vulnerabilities for hackers to exploit. Aftermarket devices, applications and utilities expand the attack surface through their own Internet connectivity and vulnerabilities. Add-ons present a social engineering opportunity for hackers, who could send drivers purportedly-official, but in reality, already-hacked add-ons for insertion in cars.

CARS

Attackers will attempt to connect to the car through one of its many points of connectivity and then pivot along its network to reach the components that help them execute their plan, whether that be to control some aspect of the car, corrupt or steal customer information, or find and publicize vulnerabilities.

CORPORATE NETWORKS

With multiple public-facing components, carmakers' corporate networks represent an easy way in for attackers. On these networks are sensitive assets and systems that attackers covet, and potentially gateways to the manufacturing network. Given that hackers have been known to attack trusted third-party connections, the attack surface extends to a car company's partners and vendors.

MANUFACTURING NETWORKS

Attackers might look to access manufacturing systems by gaining a beachhead on the corporate network and then pivoting to the manufacturing network. Once on the manufacturing network, attackers could disrupt operations, destroy equipment, or corrupt software. Corrupted software could introduce backdoors to remotely control the cars.