Risk Assessment for Integrated Cyber and Physical Attacks on Stadiums and Transportation Systems

Fred S. Roberts
Rutgers University
froberts@dimacs.rutgers.edu

November 14, 2024

Manchester arena after attack
Credit: en.wikipedia.org BBC picture

Credit: Wikimedia commons, Jiří Karlík from Studénka, Czech Republic, no changes

So What? Who Cares?

- Mission: Protect stadiums & transit systems from terrorist attacks
- Problem:
  - For stadiums & transit systems: Long-term interest in physical security, increasing interest in cyber security
  - ***But more sophisticated attacks could be multi-modal - integrated***
  - Cyber attack as precursor to physical attack, or vice versa ***Precursor attack not the end goal; aims to increase impact of following attack***
- Solution Needed: Risk assessment
  - There is literature on RA for cyber attacks & for physical attacks
  - Large literature on RA for attacks on cyber-physical systems
  - ***Virtually nothing on RA for integrated attacks***
    - Some work by FEMA, EU's SAURON project, SANDIA
- **RISK = threat x vulnerability x consequence**, but may only be able to calculate this qualitatively for integrated attacks
- Examples will show qualitative approach is feasible
- TRL = 2

Integrated Cyber & Physical Attacks

- **Example: Hacking into the Stadium Jumbotron**
  - Attack at Ariana Grande concert, Manchester, UK 2017
  - People attacked leaving
  - Could cyber attack on message board draw people out into a physical attack?
  - AFC Championship 2017: hack leads to message on Jumbotron

- **Variant: Attack on Train Message Board** telling passengers to go to track A
  - Hack on message board happened in Iran in 2021
- **Example: Car Hacking on Stadium Roadway**
  - Bad actor controls car remotely, causes crash
  - Remote control of Prius demo in 2013
  - Chaos on roadway makes it ripe for physical attack

Image credits, Wikimedia commons, m01229 from USA; ctvnews.ca

Integrated Cyber & Physical Attacks

- **Example: Rail Tunnel Attack**
  - Rail tunnels require pumping after storm
  - Cyber attack disables pumping system; train gets stuck
  - Physical attack on train follows

Image credit:Amtrak

- **Risk Assessment**: *How would a bad actor compare a standard physical attack to an integrated one?*
  - Not many examples (as yet) of successful cyber attacks on stadiums and train systems, making ***threat*** hard to estimate
  - Estimates of probability attack will succeed (***vulnerability***) are essentially speculation
  - ***Consequences*** could be large, so important to be able to estimate probabilities accurately, which is difficult
- *Since assessment of threat & vulnerability is qualitative, it makes sense to approach the RA problem qualitatively at least to begin*

RA: Hacking into the Jumbotron

- Attack *A*: Hack into Jumbotron, tell people to leave
- Attack *B*: Physically attack people leaving as result of *A*
- **Integrated Attack *I***: *A* followed by *B*
- **Attack *X***: Attack people leaving after event
- *Vulnerability*: ***Success probability*** P_A is high since Attack *A* seems feasible.
- For success probabilities: $P_{B/A} > P_X$: that is whole point of joint attack. If P_A sufficiently large, then $P_I > P_X$ and **system is more vulnerable to *I* than to *X***
- *Threat* ***(measured by cost)***: Cost of *A* is fairly small, so costs of *I* and *X* are close. So, **threats of *I* and *X* are close**
- *Consequence*: Almost surely **consequences of *I* are higher than consequences of *X***
- ***Reasonable to conclude that I is of higher risk than X***

RA: Vehicle Hacking at Stadium

- Attack *A*: Hack into vehicle causing chaos on stadium road
- Attack *B*; Physical attack while cars are stuck.
- **Integrated Attack *I***: *A* followed by *B*
- **Attack *X***: Physical attack *R* by a car ramming another car, causing chaos in road, followed by attack *B*
- *Vulnerability*: Success probabilities $P_{B/A}$ and $P_{B/R}$ are similar. Success probability P_A is lower than success probability P_R. So, **system more vulnerable to attack *X* than attack *I***
- *Threat* ***(measured by cost)***: Cost of *I* might be higher than cost of *X* if driver isn't afraid of death or arrest, so **threat of *X* is higher than threat of *I***
- *Consequence*: **Consequences for *I* & *X* likely to be similar**
- ***This suggests that the risk of an integrated cyber and physical attack I is lower, and maybe considerably lower, than the risk of the two-part physical attack X***

RA: Rail Tunnel Example

- Attack *A*: Hack into tunnel pump leads to train stuck
- Attack *B*: Following physical attack on train
- **Integrated Attack *I***: *A* followed by *B*
- **Attack *X*:** Physical attack *R* on pump, leads to train stuck, followed by attack *B*
- *Vulnerability*: Hacking into pump may be much more likely to succeed than physically destroying it, so $P_A > P_R$. Also, $P_{B/A}$ is close to $P_{B/R}$
- So, $P_I > P_X$. **System is more vulnerable to *I* than to *X***
- *Threat (measured by cost)*: Cost of *A* is likely lower than cost of *R;* cyber attack is easier than physical one.
- So, cost of *I* is less than cost of *X*, and **threat of *I* is higher than threat of *X***
- *Consequence*: **Likely that consequences are similar**
- ***Reasonable to conclude that I is of higher risk than X***