Threat Modeling Notes

- Are computers ever 100% secure?
- We can't eliminate risk, only mitigate it.
    - Mitigate:
        - verb (used with object), **mitigated, mitigating.**
        - 1. to lessen in force or intensity, as wrath, grief, harshness, or pain; moderate.
        - 2. to make less severe: (e.g., *to mitigate a punishment.*
        - 3. to make (a person, one's state of mind, disposition, etc.) milder or more gentle; mollify; appease.
        - http://www.dictionary.com/browse/mitigate?s=t
- Security is about managing an acceptable level of risk.
- Robert Morris, Sr.: Pioneer of cybersecurity:
    - "The three golden rules to ensure computer security are: do not own a computer; do not power it on; and do not use it" (in *Inside Java 2 Platform Security: Architecture, API Design, and Implementation*, Li Gong, Gary Ellison, and Mary Dageforde, Boston: Addison-Wesley, 2003, 2nd ed.)
    - Obituary: https://www.nytimes.com/2011/06/30/technology/30morris.html
- Security ratings for high security safes are in terms of time to crack and tools:
    - https://standardscatalog.ul.com/standards/en/standard_687_15
    - https://www.nytimes.com/2017/01/08/nyregion/its-right-in-the-name-safes-are-safe-except-for-two-on-new-years-eve.html
- Risk
    - Common definition: Risk = Impact × Probability
    - Better definition: Risk = Asset × Vulnerability × Threat
    - Risk is context dependent: the level of risk changes from one context to another.
    - There is no such thing as secure/insecure. Not a binary property. You are relatively secure to a specific threat.
- *Threat modeling* is about understanding vulnerabilities to specific threats, so that they can be prioritized and mitigated. In other words, prioritizes the most critical weaknesses and make them stronger or more secure.
- Security cards: A Security Brainstorming Toolkit: http://securitycards.cs.washington.edu
- Take for example the modern car. It has lots of features, but could vulnerabilities in any of these features have negative impacts?
    - Cool article about the way-ahead-of-its-time 2010 UCSD hack: https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/
    - 2015 Jeep hack: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
    - 2016 Pwnie awards: http://pwnies.com/winners/
    - https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/
    - Tesla autopilot hack: https://www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles/
    - VM entry and ignition hack: https://www.wired.com/2016/08/oh-good-new-hack-can-unlock-100-million-volkswagens/
    - Semi-truck hack: https://www.wired.com/2016/08/researchers-hack-big-rig-truck-hijack-accelerator-brakes/
    - More recent news articles about car hacking: https://www.wired.com/tag/car-hacking/
- Security is a mindset. It is a way of thinking. Security professionals learn to think like an attacker, or in other words develop "professional paranoia."