Threat Modelling

Dr Rob Hegarty

Aims and Objectives

- Upon completion of this lecture you will be able to:
  - Describe the purpose of threat modelling
  - Categorise different types of threat
  - Propose proportional responses to a variety of threats
  - Demonstrate your understanding of threat modelling, by developing a personal threat model

- Note – In order to preserve operational security, and encourage discussion and debate, this lecture focuses on personal threat modelling

Risk Appetite

- Risk appetite defines our tolerance to risk, and is typically derived from two main attributes

- Risk / Likelihood – What is the probability of a threat being realised?
- Impact – What are the potential consequences of a threat

Risk Appetite

- Individuals and organisations fit into a spectrum:
  - Risk Hungry – risk taker, likes innovation, prepared to gamble
  - Risk Averse – Avoid risks at all costs

- Risk appetite changes, and is influenced by outside factors, consider the current trend of home assistants:
  - Open microphone + Internet connection + Proven privacy failing
  - = MASS MAINSTREAM ADOPTION ☹
- Always consider the motivation behind a product, or risk becoming the product yourself.

Classifying Threats

- Threats to the principles of security

- Confidentiality – Eavesdropping, unauthorised access
- Integrity – Unauthorised modification
- Availability – Denial of Service

Threat Consequences

- Confidentiality – Loss of privacy
- Integrity – Compromise of assets, increased vulnerability to other threats
- Availability – Disruption to services

- Also
  - Compliance, Reputational, Financial, Operational, Legal

Countermeasures (Recap)

- Consider both data at rest and data in transit:
  - Encryption
  - Cryptographic checksums
- Technical/Architectural countermeasures:
  - Firewalls, VPNs, Proxies, etc
- Access Control
- Policy
- Training

OpSec – Operational Security

- Thinking holistically about security
- Considering how information may be used by an adversary
- Reducing the data footprint
- Recognising the threat/power of data aggregation and AI
- Asserting some control over digital assets

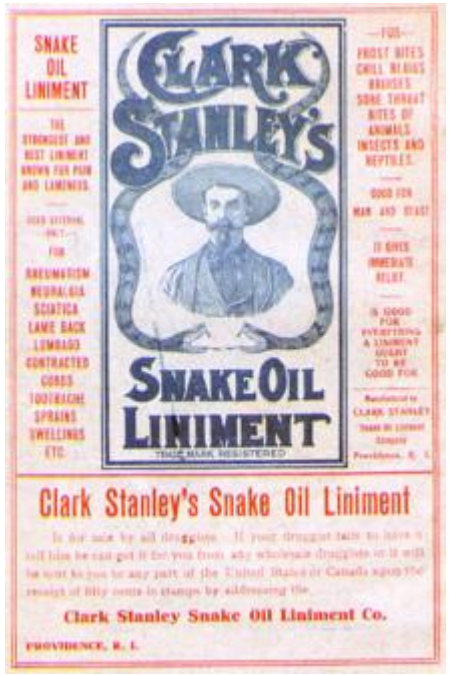
Threat Modelling

- Analysing threats from our environment, and preparing appropriate responses.

- We do it all the time in our everyday lives;
  - Crossing the road
  - Booking a holiday

- It involves:
  - Identifying threats
  - Rationalising risks
  - Proposing proportional responses

Threat Modelling Challenges



Personal Threat Modelling

- What do I want to protect?
- Who do I want to protect it from?
- How bad are the consequences if I fail?
- How likely is it that I will need to protect it?
- How much effort am I willing to expend to prevent the potential consequence?

- https://ssd.eff.org/en/module/your-security-plan

What do I want to protect?

- Assets, typically data:
  - Email
  - Contacts
  - Photographs
  - Online accounts
  - Browsing habits
  - Personal location / movements
- Where is it kept?
- Who has access to it?
- What prevents unauthorised access?
- Make a list of your most important assets

Who do I want to protect it from?

- Who is your adversary?
- Example adversaries:
  - Hacker
  - Friends / Enemies
  - Business competitor
  - Government
  - Data platform (Facebook, Google, Amazon, Microsoft, et al)
- Make a list ranked on importance to you, the order may vary for each of the assets you wish to protect

How bad are the consequences if I fail?

- What are the motives of your adversary?
- Potential motives:
  - Degrade ability to communicate (censorship)
  - Damage reputation
  - Gain access to secrets
  - Profiling
    - E.g. Impact on elections
  - Impairment of free will
    - E.g. advertising bias, exclusions in search results, ranking of results
- Make a list ranked by severity

How likely is it that I will need to protect it?

- Risk is the likelihood of a threat being realised, it must be balanced against your adversary's ability
- Assessing risks is subjective (consider air travel, and how it polarises people)
- Make a list of the threats you consider to be serious, and also make a list of risks that are; rare, harmless, or too difficult to combat.

How much effort am I willing to expend to prevent the potential consequences?

- Security is never 100%, and priorities and concerns vary from person to person over time.
- Consider the lists you have made, and plan a strategy to balance:
  - Privacy
  - Cost
  - Convenience
- Reflect on your responses (or lack of responses) to the threats you identified, are they proportionate to the risk and consequences?
- Guidance - https://ssd.eff.org/en/module/your-security-plan

Reflection

- The primary goal of creating your own personal threat model, is to improve your awareness of threats, and allow you to make informed decisions about how you interact with technology.
- Hopefully there will be a knock-on affect in the way you recognise and rationalise threats in the workplace.
- As cyber security experts you play an important role in society, steering decisions that safeguard our privacy and security.
- It is your responsibility shape the world you interact with, be it by advising on security issues at work, or giving advice to friends and family.
  - Beyond; Use strong passwords, Don’t post your holiday photographs publicly on Facebook, Update your operating system, etc

Summary

- Threat modelling is something we do instinctively in our everyday lives.
- The complexity of computer systems, makes threat modelling a challenging endeavour.
- By taking a structured pragmatic approach, it is possible to develop robust threat models, that balance security, privacy, cost, and convenience
- Our risk appetite, circumstances, and the technology which we interact with is continually changing, therefore we must continue to evolve our threat models to accommodate change.

Resources

- EFF https://ssd.eff.org/en/module/your-security-plan
- ArsTechnica https://arstechnica.com/information-technology/2017/07/how-i-learned-to-stop-worrying-mostly-and-love-my-threat-model/
- Security Innovation https://blog.securityinnovation.com/creating-your-own-personal-threat-model