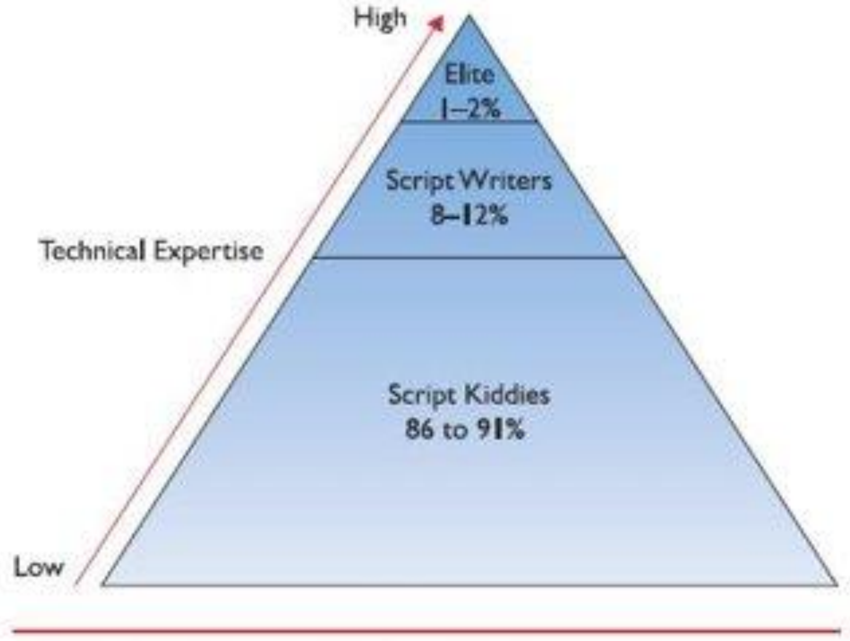
# Threat Agents and Hacking

- White Hat
  - Hired to discover security vulnerabilities in a system. Also known as ethical hackers.
- Gray Hat
  - Illegally access a system, but generally do not exploit the discovered vulnerabilities.
- Black Hat
  - Criminals - use their skills to conduct malicious activities.

Hacking
Positive
Negative
WHITE HAT
GRAY HAT
BLACK HAT

# Threat Agents and Hacking

- Hacker is a person that conducts a deliberate software attack.
  - Elite hackers: Individuals capable of discovering new vulnerabilities and writing scripts that exploit those vulnerabilities.
  - Script Writers: Individuals capable of writing scripts to exploit known vulnerabilities.
  - Script Kiddies: Individuals with (only) enough understanding of computer systems to be able to download and run scripts that others have developed. Vast majority of attack activity on the Internet is carried out by these individuals.



• Figure 1.1 Distribution of attacker skill levels

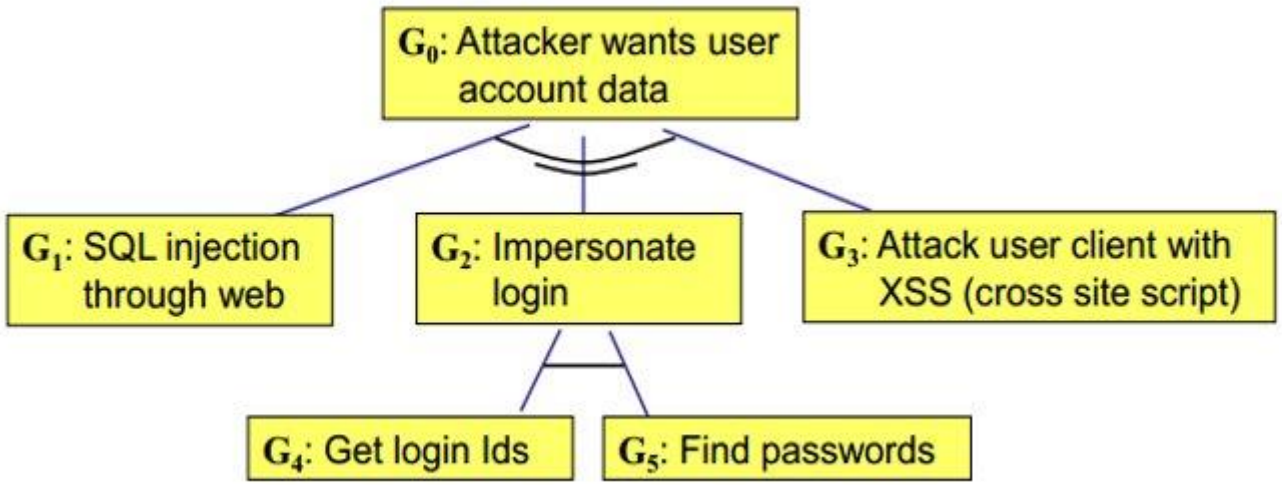
# Threat Modelling

- Understanding the potential threats to a system is the essential starting point in order to bake solid defenses and mitigations into your software designs.
- Thread modeling provides a perspective with which to guide any decisions that impact security through the software development process.
  - You must adopt and see things from “the adversary perspective!”

- Threat Modelling: practice of building an abstract model of how an attack may proceed and cause damage [ attacker-, system-, or asset- centric]

# Threat Modelling – cont’d

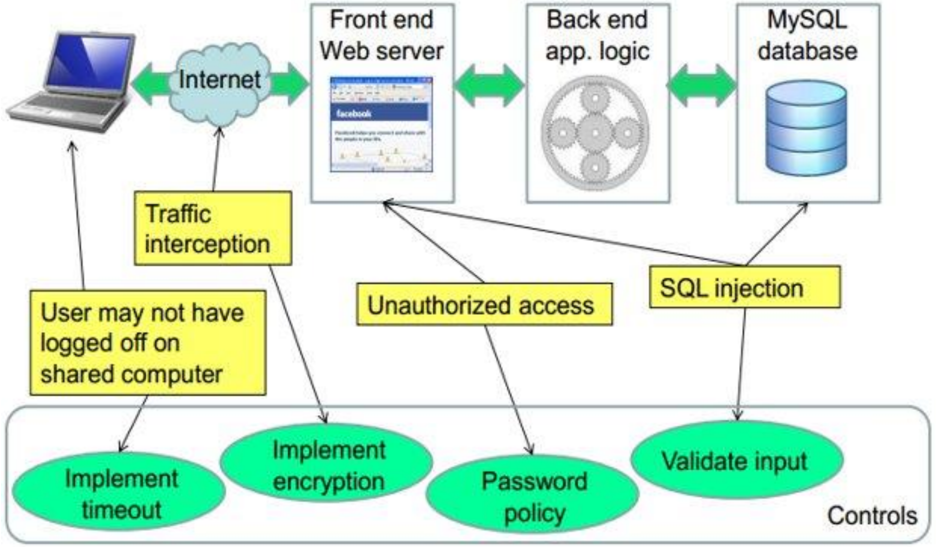
- Attacker-centric: starts from attackers, evaluates their motivation and goals, and how they might achieve them through attack tree.


$G_0$: Attacker wants user account data
$G_1$: SQL injection through web
$G_2$: Impersonate login
$G_3$: Attack user client with XSS (cross site script)
$G_4$: Get login Ids
$G_5$: Find passwords

http://www.uio.no/studier/emner/matnat/ifi/INF3510/v12/learningdocs/INF3510-2012-L03.pdf

# Threat Modelling – cont’d

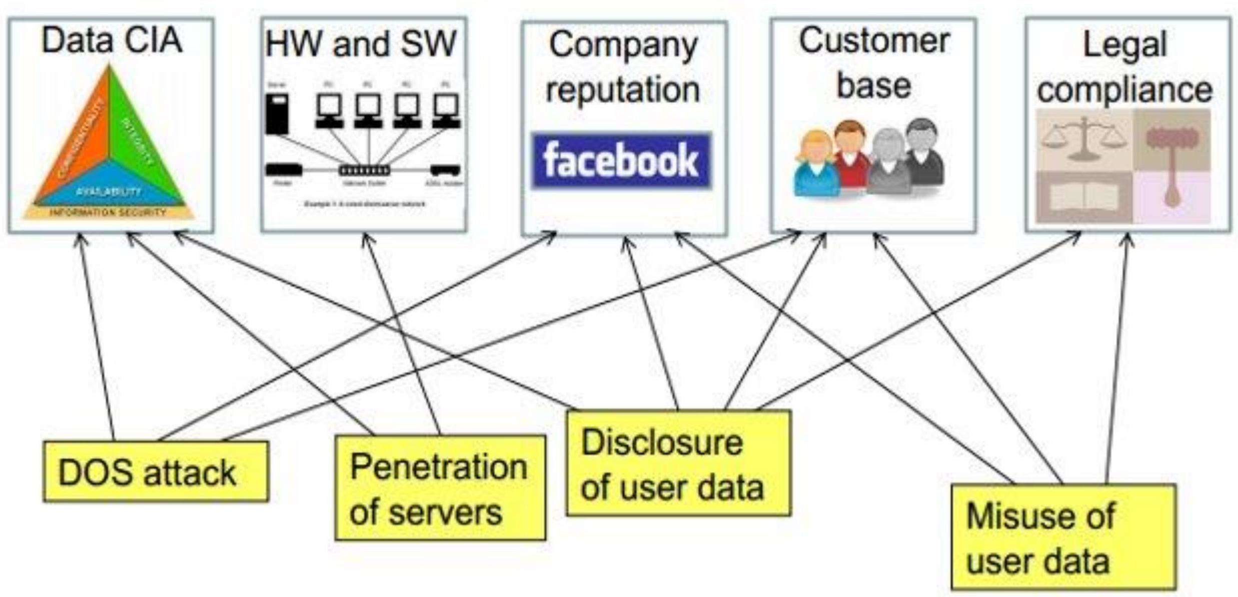
- System-Centric: starts from model of system, and attempts to follow model dynamics and logic, looking for types of attacks against each element of the model.



http://www.uio.no/studier/emner/matnat/ifi/INF3510/v12/learningdocs/INF3510-2012-L03.pdf

# Threat Modelling – cont’d

- Asset-Centric: starts from assets entrusted to a system, such as collection of sensitive personal information, and attempts to identify how CIA security breaches can happen.



http://www.uio.no/studier/emner/matnat/ifi/INF3510/v12/learningdocs/INF3510-2012-L03.pdf