Security Managment (security engineering)

By

Hafez Barghouthi

Agenda Today

- Attack.
- Security policy.
- Measuring Security.
- Standard.
- Assets.
- Vulnerabilities.
- Threats.
- Risk and Risk Mitigation.

Attack

- A basic definition is exploiting a vulnerability in a system attach a specific threat to a vulnerability.
- A lot of scenarios

❑Social engineering .

❑Identity theft.

❑Denial of service.

❑Uncountable ☹.

Classifications and Motivations

- Organized crime to gain Money.
- Terrorists (critical infrastructure).
- Governments.(inside and outside)
- The competition.(commercial)
- Hacktivists: This class of attackers tries to break into your systems to make a political point or demonstrate regarding social issues(political)
- For fun ☺
- **Attacker Skill Levels: From Script Kiddies to the Elite**

Main objectives for Managment

- Security policy.
- Security awareness should be organized.
  - Why security is important for them and for organization.
  - What is expected from each member.
  - Which good practices they should follow
  - Comply with rules rather than looking to workaround

(Adams and Sasse,1999).

Of course secretary is different than developer .

Security Policy

- A statment of intent to protect an identified resource from unauthorized use.
- Organizational level(organizational security Policy)
  - Laws,rules and practices regulate how an organization manages,protects and distribute resources to achieve security aspects(CIA).
- Technical level (Automated security Policy)
  - How this will be achieved using computer system.
  - Access controls, firewalls,security protocols … etc

Measuring Security

- We are searching for quantitative not qualitative (or not).????????
- Security level is good ????????
- Security is 99% (from 1000 employees 10 attackers).
- Product is 100%secure (definitly you are a lier) but can be deployed in an insecure manner (default password).
- Then How????
- Actually there is no simple answer

Ways

- Number of bugs (statistical approach)
- Software security
  - Product surface (number of interfaces).
  - Dangerous instructions
  - 1 bug is better than 50 bug ????????
- Again quality or what. (it is good believe me I swear)
- Number of acccounts with week passwords(system).
- Number of open ports or nodes connectivity (Network).
- Good measurments or not ?????????

Another Way (Attack point of view)

- The time an attacker has to invest.
- The expenses .(how many computers to calculate)
- The knowledge necessary to conduct an attack
- ☹cost of discovering an attack for first time >> the cost of mounting an attack(war games).
- Assets measurment drive us to risk and threat analysis.
- Lost so search for a standard .

Standard (ISO 27002)

- Security policy
- Organization of Information Security.
- Asset Managment
- Human resources security
- Physical and environmental security
- Communication and operations managment
- Access control , remote access.
- Information system acquisition, development and maintinance.
- Information security incidents managment
- Business continuity managment
- Compliance

Risk Analysis

- The possibility that an attack cause damage to your enterprise.
- Risk = Assets ×Threats ×Vulnerabilities.
- To have a quantitive values are taken from mathmatical domain (asset replacment, propability of threat.)
- Qualitative we will mention some principles later

Assets

- Hardware.
- Software.
- Data and information.
- Reputation.
- Money+customer+competition(how much you will survive)
- Much better to sell potato ☺

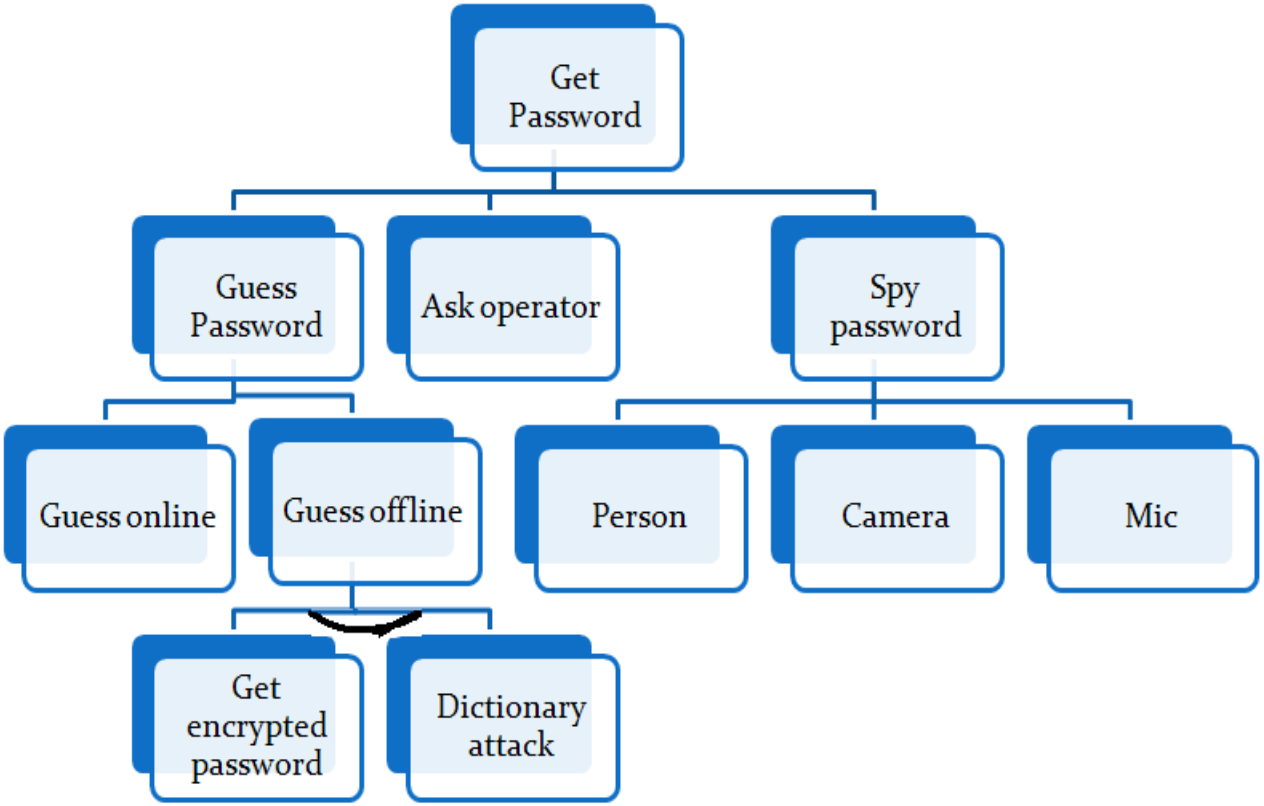
Vulnerabilities

- Accounts with a privileges where the default password for ”Manager” has not been changed.
- Programs with known flows or unnecessary privileges.
- Weak access control.
- Weak firewall configurations.
- How much is critical.????(admin than guest).
- Scanners or risk analysis tool.

Threats

- An action by an attacker who try to exploit vulnerabilities to damage the assets.
  - Spoofing identity.
  - Tampering data.
  - Gain a privilege.
  - Denial of service.
  - Repudiation.
  - Disclosure.
  - (Howard and Leblanc,2002).

Attack Tree



Risk (Quantitative vs Qualititative)-1

- Quantitative
  - Value of asset.
  - Critically of vulnerability
  - Likelihood of Threat
  - Other words statistics and data mining.

Risk (Quantitative vs Qualitative)-2

- Qualitative
  - scale of asset(very important,important,not imp).
  - Critically of vulnerability(fixed soon,should be fixed,fix if convenient).
  - Likelihood of Threat(very likely, likely, not likely)

  e.g numerical scale from 1 to 10 guidance on how to assign rating like in war games

Countermeasures

- Risk analysis takes a time so concentrate more on security.(Baseline protection approach).
- Full risk analysis is Hard to achieve therfore concentrate on defence measurments in similar cases.