Оглавление

[1 Related Work 2](#__RefHeading___Toc1416_26184610)

[1.1 Related Work in the Area of Taxonomies 2](#__RefHeading___Toc1418_26184610)

[1.2 Input Data Gathering 2](#__RefHeading___Toc1420_26184610)

[1.3 Impact Scores 4](#__RefHeading___Toc1422_26184610)

[1.4 Models of Hackers and Break-ins 5](#__RefHeading___Toc1424_26184610)

# Related Work

## Related Work in the Area of Taxonomies

Howard and Longstaff [2] described attacks as the following process. By using a tool, attackers exploited vulnerabilities in a target and attack for an unauthorized access. They organized a taxonomy of attacks, including five dimensions: attackers, tools used, access, targets chosen, and results achieved. The same idea was later used in Alvarez’s classification of Web attacks[3]. They proposed a taxonomy with eight dimensions: entry point, vulnerability, service, action, input length, target, scope and privileges. We use some of Howard and Alvarez’s ideas in the first and fourth dimensions of our taxonomy. Hansman and Hunt[4] proposed four taxonomies of attacks based on four different dimensions of classification covering network and computer attacks. The four dimensions are: attack vector used to classify the attack, target of the attack, vulnerability base on common vulnerabilities exposures (CVE) or criteria from Howard’s taxonomy, payload or effects involved. They mentioned the need of future research on correlation between attacks within the taxonomy and the utilization of KB.

## Input Data Gathering

The figure (Fig.1) demonstrates how successful attacks penetrate multiple layers of protection.Let us consider the following input data used for the security assessment: topology of the test network (Fig.2), values of the topological metrics, especially Criticality of the hosts (calculated on the previous assessment stage), attack graph, security events.

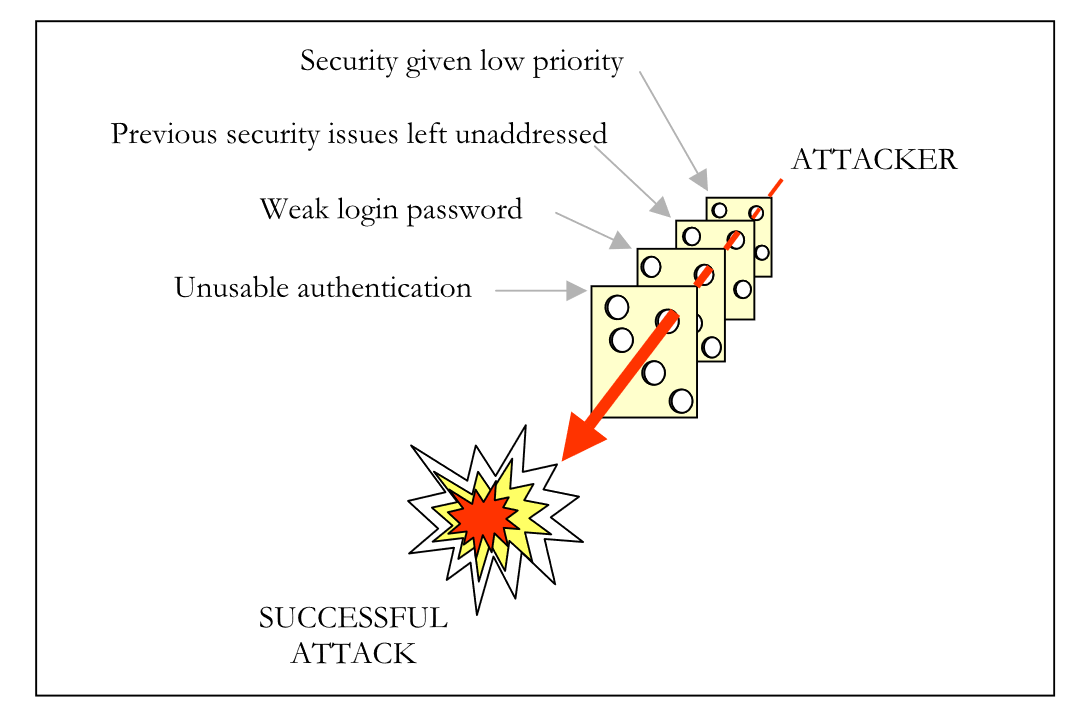


Figure 1 –Successful attacks propagate through several protection layers

Here are the points that we have laid out in this paper:

* Trade-offs are sometimes implemented in a wild, uncontrolled manner.
* Legitimate users sometimes prioritise immediate benefits to the detriment of long-term security.
* Passwords, anti-virus updates, email attachments and shared folders, respectively, raise such issues as memory limitations, risk, trust and practicality.
* Security does not imply protecting everything since some losses are acceptable.
* Trade-offs by legitimate users differ in nature from the ones performed by attackers.
* Computer security is an organisational matter.

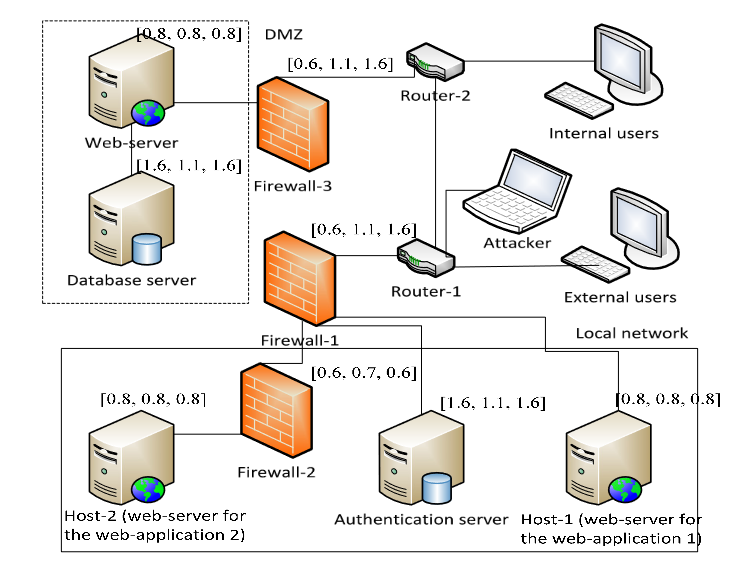


Figure 2 –Topology of the test network and Criticality values

## Impact Scores

There are different interpretations in assessing cyber attacks to users. User impact can be thought as the level of confidence a user can still use the machines he or she has accounts on. In realizing this notion, is defined as a weighted average of for h ∈ H(u) with weights c(h, u).

where is the unknown variable;

is a known variable.

The network impact score will allow an analyst to monitor the health of a subset or of the entire network. Intuitively, the calculation (Formula 1) may be an aggregation of , , or within the subset or the entire network. Consider the target n ∈ N and a set of weights with respect to this target. The impact score can be defined as follows for X = H, S, U.

|  |  |
| --- | --- |
|  | (1) |

The attack effect reflects the impact of exploitation of a potential weakness of the system. The more attack effect on the security property of the system, the more impact caused by exploitation of the vulnerability. Risk calculation is given as

R is the system risk, Pi means the probability of occurrence of ith weakness, and Di means the damage caused by the ith weakness. So the evaluation of attack effect is helpful to risk assessment.

The security assessment technique includes the following stages:

1. Definition of the attacker position on the attack graph on the base of the information from the security event;
2. Determination of the attacker skill level on the base of information from the security event;
3. Calculation of the probabilities of the paths that go through the node that corresponds to the attacker position;

## 1.4 Models of Hackers and Break-ins

Respondents with these models could use them to extrapolate many different situations and use them to make many security-related decisions on their computer. Table 1 summarizes the major differences between the four models

Table 1 – Summary of folk models about viruses, organized by model features

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subjects | Bad Buggy | Software | Mischief | Support Crime |
| Creator | Unspecified | Bad people | Mischievous hackers | Criminals |
| Purpose of viruses | Unspecified | No purpose | Cause mischief; cause annoying problems | Gather information for identity theft |
| Effects of infection | General notion of bad things happening | Same effects as buggy software, but more extreme | Annoying problems with computers | No direct harm to computer; stolen information |
| Method of transmission | “Catch” viruses; miscellaneous methods of catching them | Must be manually downloaded and execute | Passive “catching” by visiting shady websites or opening shady email | Spread automatically, or installed by hackers |

My respondents described four distinct folk models of hackers. These models differed mainly in who they believed these hackers were, what they believed motivated these people, and how they chose which computers to break in to. Table 2 summarizes the four folk models of hackers.

Table 2 – Summary of folk models about hackers, organized by model features

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subjects | Bad Buggy | Software | Mischief | Support Crime |
| Identity of hacker(s) | Young technical geek | Some criminal | Professional criminal hackers | Young technical geek |
| Level of organization | Solo, or to impress friends | Part of a criminal organization | Unspecified | Solo, but a contractor for criminals |
| Reason for break-ins | Cause mischief | Look for financial and personal information | Look for financial and personal information | Look for financial and personal information |
| Effects of break-ins | Lots of computer problems; requires reinstall | Possible harm to computer; exposure of personal information | No harm to computer; exposure of personal information | Exposure of personal information |
| Target(s) | Anyone; doesn’t matter | Opportunistic; could be me | Not me; only looking for rich or important people | Not me; looking for large databases of info |
| Am I a target? | Possibly | Possibly | No | No |