The costs and benefits of Honeynets

Maximillian Dornseif with Sascha A. May
Laboratory for Dependable Distributed Systems
RWTH Aachen University

at
The 3. Workshop on Economics of Information Security
(WEIS 2004)
Honeynets

![Diagram of Honeynets]

- Honeywall
- Honeynet
- Honeypots
Motivation
Possible Benefits of Honeynets

• Possible information gain on attacks and attackers.

• Possible increased security by using Honeynets as a decoy.

• Possible increased security by using aggressive Honeynets for redirection (”Bait and Switch”).
Honeynet as a Decoy

Source: Symantec Decoy Server/Mantrap Advertisement
Honeynet Redirection
Honeynet Redirection
Costs of Honeynets

- Deployment
- Operation
- Increased risk
  - To the network
- Legal liability
Building a Model

- We focus on honeypots not aimed at general security research.

- The operator of Honeynets is not interested in all attackers but only in attacks specifically aimed at his systems. We call this type of attacker the “qualified attacker”.
Building a Model

- At $t_0$ the Honeynet starts operation and creates considerable fixed startup costs.
- Every unit of time the Honeynet creates cost for maintenance, housing, power, bandwidth and damages from unqualified attackers.
Building a Model

- At $t_a$, a qualified attacker starts an attack, resulting in information gain for the operator in every unit of time.

- At $t_d$, the attacker detects the “true nature” of the Honeynet and stops its attack.
Building a Model

- There is no way to succeed for the attacker.
- Information gain is independent of privilege escalation.
Building a Model

- Between $t_a$ and $t_d$ additional costs arise.
Building a Model

- By investing in the Honeynet the Operator can make its “true nature” harder to detect thus moving $t_d$ to the right.
Building a Model

- There is a climate of constant attack on the Internet.
- By investing in the Honeynet the frequency of qualified attacks can be increased.
Cost

\[ c(t) = S + Mt \]

- \( S \) : start-up costs.
- \( M \) : Maintenance including forensic analysis, damage repair etc.
Utility

\[ u(t) = Pt \frac{M}{I} \]

- **M**: Maintenance including forensic analysis, damage repair etc.
- **P**: Value of information gained by an attack.
- **I**: Weighting factor coupling higher investment in maintenance to increased frequency and likelihood of prolonged attack.
Are Honeynets profitable?
Are Honeynets profitable?
How Much Maintenance?

![Graph showing the relationship between time to profitability and investment in maintenance. The graph illustrates a decreasing trend, indicating that as time to profitability increases, the investment in maintenance decreases.]
Real World Experiences

• No “qualified attackers” so far.
• Very few sophisticated attackers.
• Some formerly unknown tools captured.
• Very little learned which can’t be found out by more traditional means.

➡ Except catching autonomous malware.
• Problem: redundant attacks.
Open Questions

• Can we more learn about prospective attackers?

• How and when can qualified and unqualified attackers be distinguished?

• What’s about organizations interested in all attackers?

• What is the value of the information gained by a qualified attack (I)?
Open Questions

- How does more investment in maintenance (decoy) relate to more and longer attacks?
- Is the gain by an qualified attack linear with duration of attack?
- Where can results obtained by Honeynet obtained by other possibly cheaper means?
- Get the Numbers!
The costs and benefits of Honeynets

Maximillian Dornseif - md@hudora.de

Slides at
http://md.hudora.de/presentations/#weis2004