

Valuing Security Products and Patches

Rick Wash

`rwash@citi.umich.edu`

CITI - University of Michigan

June 4, 2004

Overview

- ▶ How much is a product worth?
- ▶ How much should be spent on security?
- ▶ Is patching worth it?

Product Value

Currently: Return on Investment / Net Present Value

- ▶ Calculate how much it currently costs
- ▶ Spend up to that on preventing damages

Expert Opinion

Types of Goods

- ▶ Search Goods
- ▶ Experience Goods
- ▶ Credence Goods

Solutions

- ▶ Preview
- ▶ Reputation
- ▶ Expert Opinion

Expert Opinion

Types of Goods

- ▶ Search Goods
- ▶ Experience Goods
- ▶ Credence Goods

Solutions

- ▶ Preview
- ▶ Reputation
- ▶ Expert Opinion

Options Approach

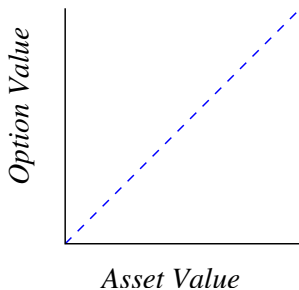
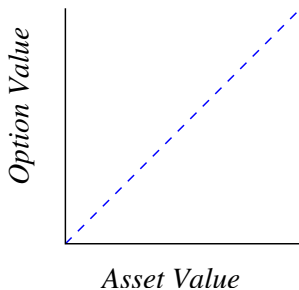
Attackers acquires an option when there exists:

- ▶ Vulnerability
- ▶ Skill
- ▶ Knowledge

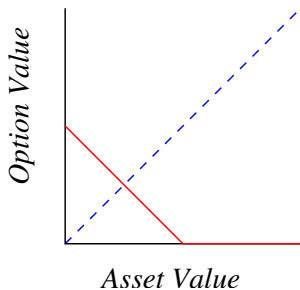
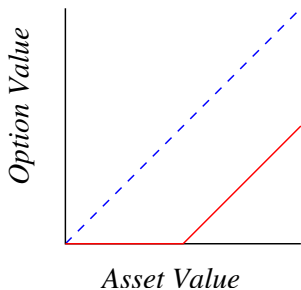
Financial Options Theory

- ▶ Call Options, Put Options
- ▶ Right (not obligation) to Purchase an Asset at a given price
 - ▶ Buy if asset value goes up
 - ▶ Walk away if asset value goes down

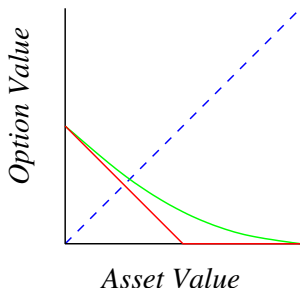
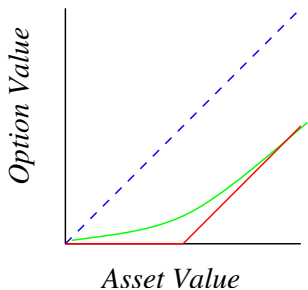
Options Theory (2)



Options Theory (2)



Options Theory (2)



Model

- ▶ Defender has asset, attacker wants it
- ▶ Asset value changes stochastically
- ▶ Geometric Brownian Motion
 - Models asset value over time
- ▶ Geometric Brownian Motion with Poisson Jump
 - Includes the possibility of the vulnerability being patched

Model

- ▶ Defender has asset, attacker wants it
- ▶ Asset value changes stochastically
- ▶ Geometric Brownian Motion
 - ▶ Models asset value over time
- ▶ Geometric Brownian Motion with Poisson Jump
 - ▶ Includes the possibility of the vulnerability being patched

Model

- ▶ Defender has asset, attacker wants it
- ▶ Asset value changes stochastically
- ▶ Geometric Brownian Motion
 - ▶ Models asset value over time
- ▶ Geometric Brownian Motion with Poisson Jump
 - ▶ Includes the possibility of the vulnerability being patched

Model

- ▶ Defender has asset, attacker wants it
- ▶ Asset value changes stochastically
- ▶ Geometric Brownian Motion
 - ▶ Models asset value over time

- ▶ Geometric Brownian Motion with Poisson Jump
 - ▶ Includes the possibility of the vulnerability being patched

Illustrative Example

- ▶ *Jeff*: hacker; *Mike*: defender
- ▶ Mike's credit card database: \$10,000
- ▶ Search Cost: 40 hours at \$20/hour = \$800
- ▶ Exploit Cost: \$25,000
 - ▶ \$50,000 for year in jail
 - ▶ 50/50 probability of being caught
- ▶ 5% annual upward drift, 20% per annum variance, 10% interest rate
- ▶ Option value: \$1970
- ▶ 4 year average lifetime
- ▶ Option value: \$125

Illustrative Example

- ▶ *Jeff*: hacker; *Mike*: defender
- ▶ Mike's credit card database: \$10,000
- ▶ Search Cost: 40 hours at \$20/hour = \$800
- ▶ Exploit Cost: \$25,000
 - ▶ \$50,000 for year in jail
 - ▶ 50/50 probability of being caught
- ▶ 5% annual upward drift, 20% per annum variance, 10% interest rate
- ▶ Option value: \$1970
- ▶ 4 year average lifetime
- ▶ Option value: \$125

Illustrative Example

- ▶ *Jeff*: hacker; *Mike*: defender
- ▶ Mike's credit card database: \$10,000
- ▶ Search Cost: 40 hours at \$20/hour = \$800
- ▶ Exploit Cost: \$25,000
 - ▶ \$50,000 for year in jail
 - ▶ 50/50 probability of being caught
- ▶ 5% annual upward drift, 20% per annum variance, 10% interest rate
- ▶ Option value: **\$1970**
- ▶ 4 year average lifetime
- ▶ Option value: \$125

Illustrative Example

- ▶ *Jeff*: hacker; *Mike*: defender
- ▶ Mike's credit card database: \$10,000
- ▶ Search Cost: 40 hours at \$20/hour = \$800
- ▶ Exploit Cost: \$25,000
 - ▶ \$50,000 for year in jail
 - ▶ 50/50 probability of being caught
- ▶ 5% annual upward drift, 20% per annum variance, 10% interest rate
- ▶ Option value: \$1970
- ▶ 4 year average lifetime
- ▶ Option value: \$125

Illustrative Example

- ▶ *Jeff*: hacker; *Mike*: defender
- ▶ Mike's credit card database: \$10,000
- ▶ Search Cost: 40 hours at \$20/hour = \$800
- ▶ Exploit Cost: \$25,000
 - ▶ \$50,000 for year in jail
 - ▶ 50/50 probability of being caught
- ▶ 5% annual upward drift, 20% per annum variance, 10% interest rate
- ▶ Option value: \$1970
- ▶ 4 year average lifetime
- ▶ Option value: **\$125**

Implications for Defenders

- ▶ Patching a vulnerability removes options from attacker
- ▶ Security should be valued accordingly
- ▶ Attackers might wait till the most opportune time to attack

Implications for Defenders

<i>External Change</i>	<i>Change in Options Value</i>
Information Asset Value Increases	↗
Exploit Cost Increases	↘
Vulnerability Lifetime	↗
Value Volatility	↗

The potential for extremely harmful future damage is what drives security spending!

Implications for Defenders

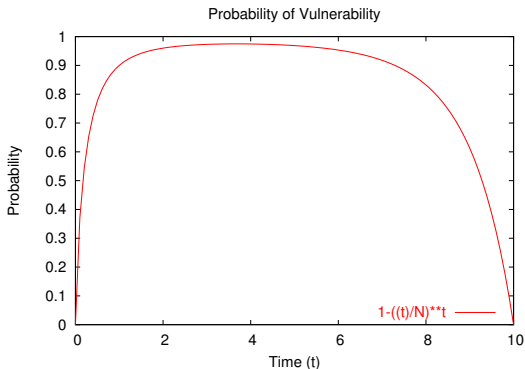
<i>External Change</i>	<i>Change in Options Value</i>
Information Asset Value Increases	↗
Exploit Cost Increases	↘
Vulnerability Lifetime	↗
Value Volatility	↗

The potential for extremely harmful future damage is what drives security spending!

Multiple Vulnerabilities

- ▶ N vulnerabilities
- ▶ Each period research one vulnerability
 - ▶ Defender patches
 - ▶ Attacker holds option

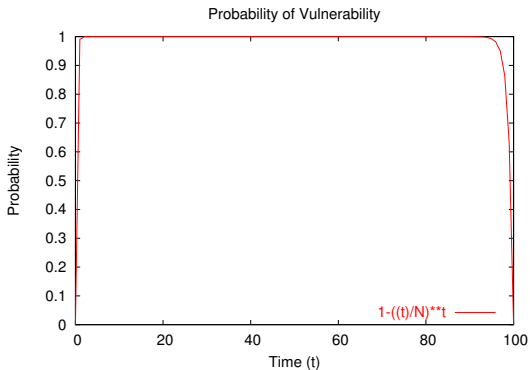
Pre-Patching



Probability of knowing at least one unpatched vulnerability

$$N=10$$

Pre-Patching



Probability of knowing at least one unpatched vulnerability

$$N=100$$

Post-Patching

Assumptions:

- ▶ Cost c to a company to be hacked
- ▶ Patching costs p
- ▶ Unpatched vulnerabilities will be re-exploited

Total Costs:

$$\text{Unpatched } \sum_{t=0}^{\infty} \frac{t \cdot c}{(1.1)^t} = 110c$$

$$\text{Patched } \sum_{t=0}^{\infty} \frac{c + p}{(1.1)^t} = 11(c + p)$$

Post-Patching

Assumptions:

- ▶ Cost c to a company to be hacked
- ▶ Patching costs p
- ▶ Unpatched vulnerabilities will be re-exploited

Total Costs:

$$\text{Unpatched } \sum_{t=0}^{\infty} \frac{t \cdot c}{(1.1)^t} = 110c$$

$$\text{Patched } \sum_{t=0}^{\infty} \frac{c + p}{(1.1)^t} = 11(c + p)$$

Post-Patching

Assumptions:

- ▶ Cost c to a company to be hacked
- ▶ Patching costs p
- ▶ Unpatched vulnerabilities will be re-exploited

Total Costs:

$$\text{Unpatched } \sum_{t=0}^{\infty} \frac{t \cdot c}{(1.1)^t} = 110c$$

$$\text{Patched } \sum_{t=0}^{\infty} \frac{c + p}{(1.1)^t} = 11(c + p)$$

Both Pre and Post Patching

$$\sum_{t=1}^{\infty} \frac{1}{(1.1)^t} \left(\frac{1-t}{N} [c_e + c_p] + c_p \right) =$$
$$11(c_e + 2c_p) - \frac{110}{N}(c_e + c_p)$$

- ▶ Generally not worth pre-patching
- ▶ Closing option valuable, not necessarily patching
 - ▶ Find better ways of closing options?

Future Work

- ▶ Untargeted Attacks
- ▶ Multiple Defenders
 - ▶ Favors attackers
 - ▶ Cooperative defenders?
 - ▶ Externality
- ▶ Multiple Attackers
 - ▶ Cooperation between attackers
- ▶ General Security Technologies
 - ▶ Stop a class of attacks
 - ▶ Stop random attacks
 - ▶ Probably a better investment