Vulnerability of networks and data

Dmitry Kryukov
What is risk?

Vulnerability + Threat = Risk
Vulnerabilities

- You can't eliminate all potential vulnerabilities on a computer unless you disconnect it from the network and lock it in a closet.
- Any input mechanism is a potential security hole.
- Outside of a complete lockdown, the goal is to minimize the most substantial risks.
- The first step is to understand how vulnerabilities occur.
Example of an emergency plan
People

- Security stands and falls with people
  - Habits
  - Attitude
  - Lack of initiative
  - Routines
  - Understanding
  - Training (or the lack of training)
  - Reporting
People

- Security stands and falls with people

**Panel 1: My keyboard is broken. It only types asterisks for passwords.**

**Panel 2: Dogbert's Tech Support**

- Try changing your password to five asterisks.

**Panel 3: I hope I can remember it.**

Copyright © 2001 United Feature Syndicate, Inc.
Organization

- Sets the framework for ALL security work
  - Priorities
  - Responsibility
  - Delegation
  - Follow-up
  - Documentation

A Security Policy is no stronger than the organization's intent of following it.
Technology

- Information Technology (IT) is the base for most of today's information handling

- IT security is often (wrongly) thought of as information security

- Lack of understanding the technical problems
Technology: 5 foundations of IT security:

- Availability
- Audit
- Object security
- Quality of Code
- Perimeter Security
Threat metrics

- Remember all three areas:
  - People
  - Organization
  - Technology

- Remember: No chain is stronger than the weakest link!
Understanding how vulnerabilities occur

Mostly vulnerabilities happen because of

- Software bugs
- Malware
- Poor patch management
- Misconfiguration
- Security policy weaknesses
- Social engineering
Software bugs

- Ultimately, many vulnerabilities wouldn't happen if the software was coded better.
- But perfectly coded software is a theoretical concept that doesn't exist in the real world.
- Code flaws are measured in bugs per thousand lines of code. It's claimed** that the average commercial software program contains 15 bugs per 1000 lines of code.

Malware

Malware lets hackers quickly find and exploit vulnerabilities.

For example, if a buffer overflow is found in an exposed service, it's usually only weeks to months before a malicious coder automates the process. If a hacker can trick a user into executing malware, the hacker can create a vulnerability where none existed before.

Most malware programs come in the form of a virus, worm, Trojan, buffer overflow, or other type of hybrid.

The natural defense against malware is proactive and reactive malware scanning tools. The former prevents recognized malware from being installed and executed in the first place, and the latter passively warns the user of the malware's existence.
Poor patch management

- Most security vulnerabilities have available patches to close the exploitable holes for weeks to months before the malware is released!

- Unfortunately, patching can be difficult to manage — administrators must test each patch and apply it with rollback strategies in case it unduly affects legitimate operations.
Misconfiguration

- A hacker can exploit a fully patched system with no known vulnerabilities if that system isn't properly configured!

- These types of vulnerabilities can only be fought by educating administrators and support staff in appropriate configuration settings and in change management.

- Many organizations, such as the Center for Internet Security (http://www.cisecurity.org) and the National Institute of Standards and Technology (http://csrc.nist.gov) contain excellent baseline recommendation documents.
Security policy weaknesses

- All employees should follow the security policies and procedures in regard to covered assets!

- Because technology is always evolving security policies quickly become dated after their approval.

- A policy must be audited to ensure that it's being consistently and appropriately applied!
Social engineering

- It as an attempt by a computer hacker to persuade a legitimate system user to reveal information, allowing the hacker to break through the system security.
- The most common way hackers break into systems.
- The most common attack through the telephone.
- “If you give me your logon ID and password, I can fix it in a few minutes, you can change your password when I’m done!”
- Hacker takes advantage of the organization size – people do not know each other.
- If you receive a suspicious phone call, ask for a phone number and call the person back.
Social engineering (cont.)

- No amount of technology can defeat a correctly implemented social engineering attack. If someone can persuade a user to reveal his or her password, even a legitimate complex password won't help.

- Administrators can only defeat social engineering by providing end-user education and enforcing good security policies.

- Social engineering subverts all mechanisms by gaining privileged information from unknowing privileged insiders.
Classes of threat

- Natural Phenomenon (acts of God)
- Other physical acts
- Murphys law
- Competition
- Disgruntled / demoralized earlier employees
- Disgruntled / demoralized employees
- Hackers
- Virus writers
- Industrial spies
- (Foreign) Governments
- Terrorists
- Organized Crime
Risk prioritizing

- What would the consequences be if the risk came true?
- What is the probability for it to happen?
- Very low, low, average, high or very high?
The "Square of Risk":

<table>
<thead>
<tr>
<th>Probability</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Low</td>
<td>Very Low</td>
</tr>
<tr>
<td>Average</td>
<td>Average</td>
</tr>
<tr>
<td>Low</td>
<td>Average</td>
</tr>
<tr>
<td>Very Low</td>
<td>Very Low</td>
</tr>
</tbody>
</table>

Probability: Very High, High, Average, Low, Very Low
Consequence: Very High, High, Average, Low, Very Low
Example 1: Virus attack

Computer virus via e-mail:

**Probability:** Very High
(Happens every day)

**Consequence:** Very Low
(We have a fully working Anti-Virus protection)
Example 2: Server Disk Crash

Server disk crashes:

**Probability**: High  
(happens annually, at least)

**Consequence**: High  
Existing back-up is inadequate. If we lose data, the organization will suffer.
Example 3: Unwanted visit in the server room

Intrusion in the server room:

**Probability:** Low
(We have strong access routines)

**Consequence:** Very High
(unauthorized people in the server room can kill the organization)
Developing a Security Plan

The top right quadrant contains the most prioritized items:
Developing a plan

Often, too much time and resources are spent in the bottom left quadrant.

*Diagram showing a risk matrix with quadrants for Probability and Consequence.*

- **Probability**
  - Very High
  - High
  - Average
  - Very Low

- **Consequence**
  - Very High
  - High
  - Average
  - Very Low

*Legend or key for risk levels.*
What do you do when you detect something?

A lot of people have no idea what to do when the alarm goes off

- Observe the attacker?
- Scare them away and lock up?
- Catch the attacker?
- Prosecute?

If you don’t know, it’s hard to take the right action
Legal problems

It’s not a good idea to use the hackers tools against him

What is the difference between logging and eaves drop?

Laws for information gathering are confusing

Logs might be unavailable
  • ISP

The attacker might not be prosecutable
  • Too young
  • No laws against hacking/virus writing in his home land
Thank you!

Questions?