Example (2): Patching

- **Correcting problems** such as **default or empty passwords poses problems when the vendor distributes the correction**. As an example, for many years, Microsoft's SQL Server was distributed with an **empty password on its administrator account.**
- **A patch is an update to a program or system designed to enhance its functionality or to solve an existing problem. In the context of security, it is a mechanism used to fix a security problem by updating the system**. The patch, embodied in a program or script, is placed on the system to be patched, and then executed. The execution causes the system to be updated.

STUDENTS-HUB.com
Uploaded By: anonymous

Patching: Detailed Description

- Ideally, **patching should never be necessary**. **Systems should be correct and secure** when delivered. But in practice, even if such systems could be created, their **deployment into various environments would mean that the systems would need to be changed to meet the needs of the specific environment** in which they are used. So, **patching will not go away**. However, **it should be minimal, and as invisible as possible**. Specifically, the principle of psychological acceptability implies that patching systems should require little to no intervention by the system administrator or user.

STUDENTS-HUB.com
Uploaded By: anonymous

Why is it difficult to make patching invisible?

- Collecting all of the necessary patches.
- The second difficulty is **system-specific conflicts**. When vendors write and test a patch, they do so for their current distribution. **But customers tailor the systems to meet their needs**. If the tailoring **conflicts with the patch**, the patch may inhibit the system from functioning correctly.
- The third difficulty with automating the patching process is understanding the **trustworthiness of the source**.

STUDENTS-HUB.com
Uploaded By: anonymous

Configuration

Building a secure system does not assure its security: **the system must also be installed and operated securely**. **Configuration is a key component of secure installation and operation**, because it constrains **what users and the system processes can do in the particular environment where the system is used**. For example, a computer configured to be secure in a university research environment (in which information is accessible to everyone inside the research group) would be considered nonsecure in a military environment (in which information is accessible only to those with a demonstrated need to know). **Different configurations allow a system to be used securely in different environments.**

STUDENTS-HUB.com
Uploaded By: anonymous

Configuration: Example

This example first arose from a system that was designed for academic research. One version was widely distributed with **file permissions set by default to allow any user on the system to read, write, and execute files on the system**. Once the system was installed, the file permissions could be reset to allow accesses appropriate to the site. This approach **violated the principle of fail-safe defaults**, because the system was distributed with access control permissions set to allow all accesses. It also required all system administrators to take action to protect the system.

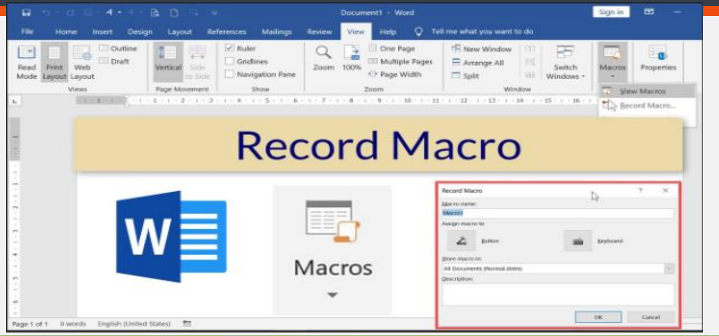
STUDENTS-HUB.com
Uploaded By: anonymous

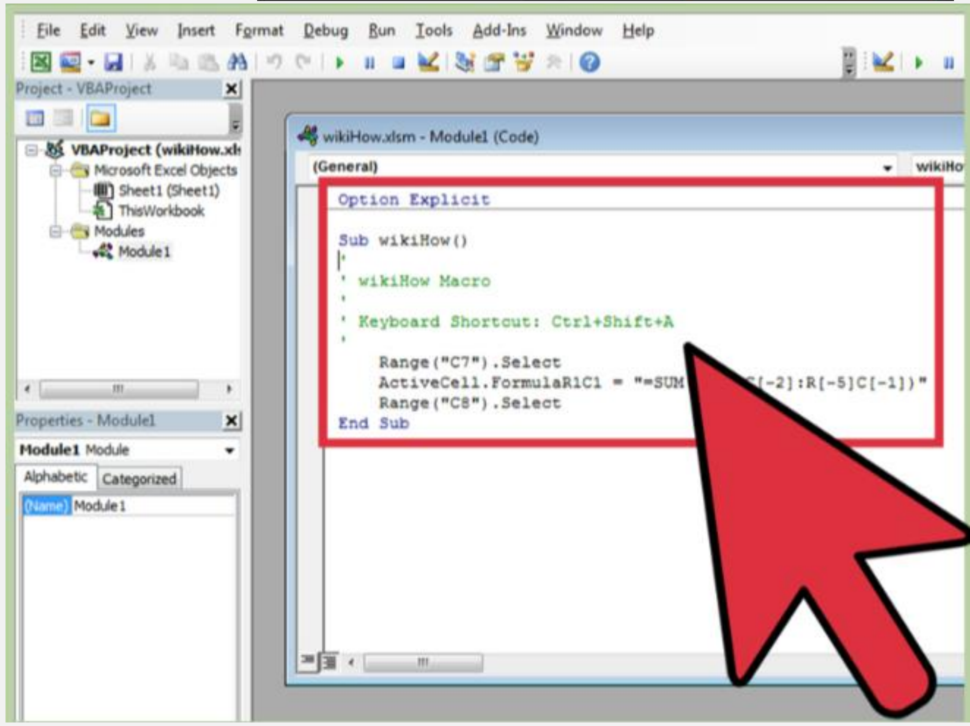
Configuration: Example

- Microsoft Word allows the user to take special actions upon opening a file. These actions **are programmed using a powerful macro language**.

  - ➢ This language allows special-purpose documents to be constructed, text to be inserted into documents, and other useful functions.

  - ➢ **Attackers can use this language to write computer viruses and worms and then embed what they wrote in word documents.**





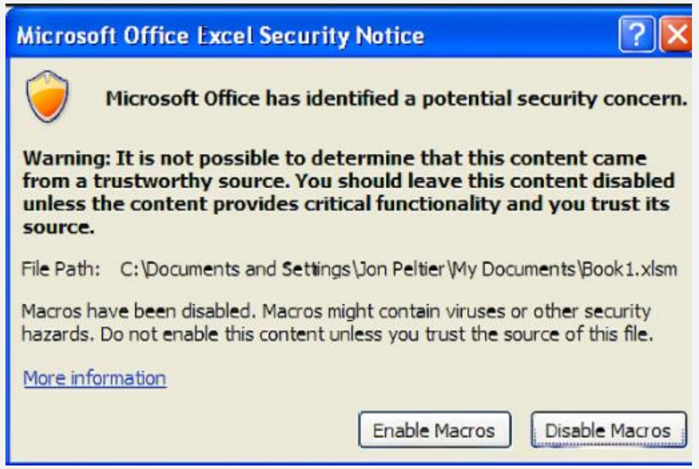
```
Option Explicit

Sub wikiHow()
'
' wikiHow Macro
'
' Keyboard Shortcut: Ctrl+Shift+A
'
    Range("C7").Select
    ActiveCell.FormulaR1C1 = "=SUM [illegible]C[-2]:R[-5]C[-1])"
    Range("C8").Select
End Sub
```

STUDENTS-HUB.com
Uploaded By: anonymous

Configuration: Example

The solution was **to allow the user to configure Microsoft Word to display a warning box before executing a macro. This box would ask the user if macros were to be enabled or disabled**. **Whether this solution works depends upon the user's understanding that macros pose a threat, and the user being able to assess whether the macro is likely to be malicious given the particular file being opened**. The wording and context of the warning, and the amount and quality of information it gives, is critical to help a naive user make this assessment. If macro languages must be supported, and a user can make the indicated assessment, this solution is as unobtrusive as possible and yet protects the user against macro viruses. It is an attempt **to apply the principle of psychological acceptability.**



Microsoft Office Excel Security Notice

Microsoft Office has identified a potential security concern.

Warning: It is not possible to determine that this content came from a trustworthy source. You should leave this content disabled unless the content provides critical functionality and you trust its source.

File Path: C:\Documents and Settings\Jon Peltier\My Documents\Book1.xlsm

Macros have been disabled. Macros might contain viruses or other security hazards. Do not enable this content unless you trust the source of this file.

STUDENTS-HUB.com
Uploaded By: anonymous

In Short

- The solution to the problem of developing psychologically acceptable security mechanisms **depends upon the context** in which those mechanisms are to be used.
- In an environment in which only **trusted users have access to a system, simple passwords are sufficient**; but **in a more public environment, more complex passwords or alternate authentication mechanisms become necessary**.
- Patches **designed for a known environment can modify the system with little or no user action**; patches applied **in an environment different from the one for which they are designed risk** creating security problems.
- **Complex configurations lead to errors**, and the less computer-savvy the users are, the worse the security problems will be.

STUDENTS-HUB.com
Uploaded By: anonymous

References

- Security and Usability: Designing Secure Systems that People Can Use by Lorrie Cranor.

STUDENTS-HUB.com
Uploaded By: anonymous