A Hacker's Top 10 Guide to Protecting Enterprise Systems

SearchEnterpriseLinux.com

Monday, March 1, 2004, 3pm EST

Joe Grand

President & CEO, Grand Idea Studio, Inc.

joe@grandideastudio.com

© 2004 Grand Idea Studio, Inc.

Agenda

- Goals
- Hacker v. Attacker
- "The Ten Immutable Laws of Security"

© 2004 Grand Idea Studio, Inc.

Goals

- Learn the basic security maxims
- Understand that nothing is 100% secure
- Accept that properly implemented security is difficult
  - **Most companies have a false sense of security**

© 2004 Grand Idea Studio, Inc.

Hacker v. Attacker

- Hacker: Somebody involved in the exploration of technology
- Attacker: Malicious goals of theft or illegitimately breaking into a system
- Terms often confused and hyped (intentionally) by media
- Contrary to popular belief, hacking does not have to be illegal

© 2004 Grand Idea Studio, Inc.

The True Hacking Philosophy

- Build upon an existing idea to create something better
- Do something that has never been done before
- Create something extraordinary
- Harm nobody in the process
- Education a motivating factor

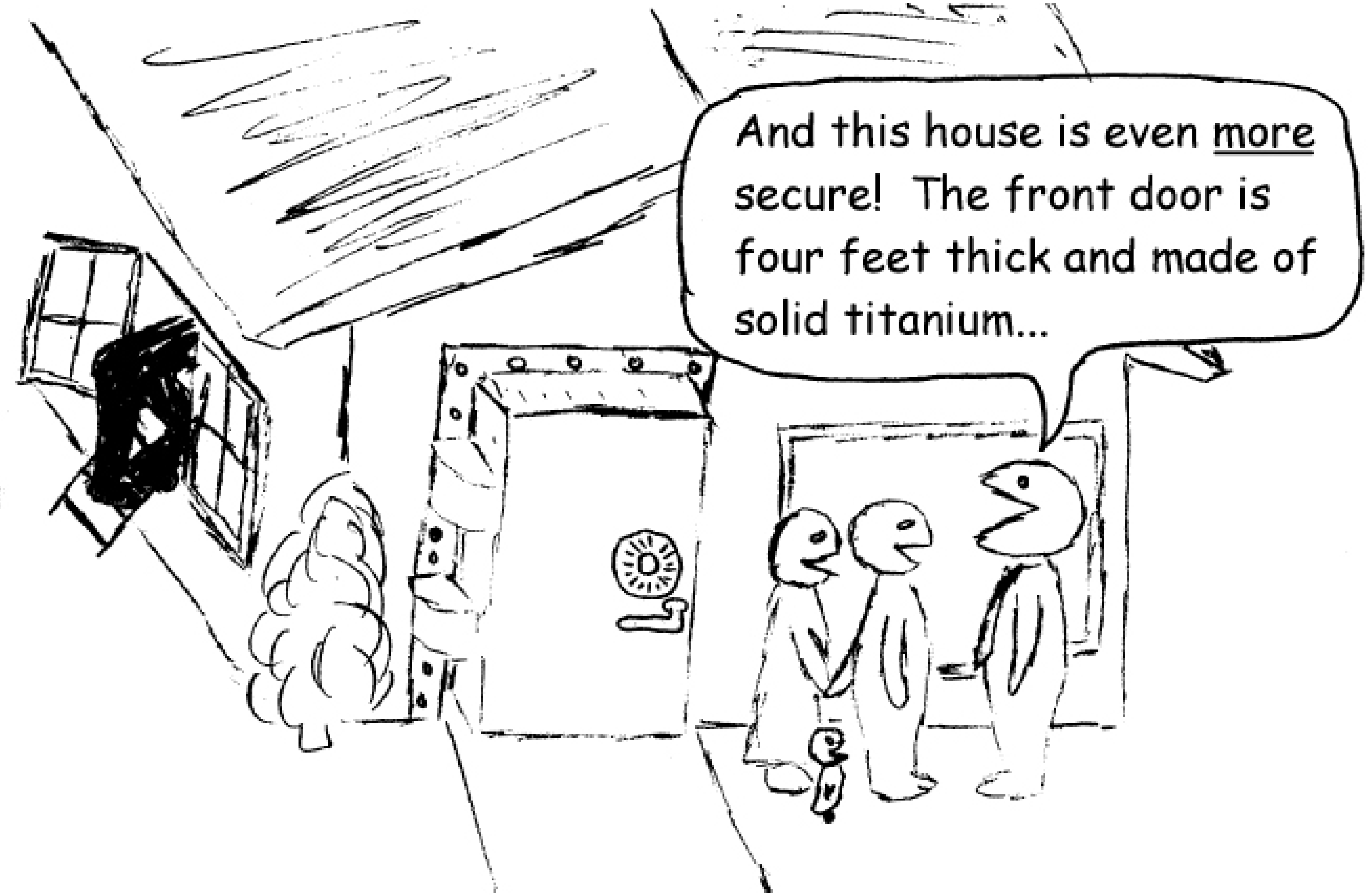
© 2004 Grand Idea Studio, Inc.

Law #1

- You must understand your risk before you can protect yourself
- What needs to be protected
- Why it is being protected
- Who you are protecting against
  - **Define the enemy**
- One size does **not** fit all

© 2004 Grand Idea Studio, Inc.

Law #1


And this house is even more secure! The front door is four feet thick and made of solid titanium...

© 2002 by Paul Kocher

Law #1

- Nothing is 100% secure
  - **Reduce risk to an acceptable level**
  - **Given enough time, resources, and motivation, an attack can break any system**
- Security is a process
  - **Constantly changing to reflect "state of the art"**

© 2004 Grand Idea Studio, Inc.

Law #2

- If a bad guy can persuade you to run his program on your computer, it's not your computer anymore
- Never run a program from an untrusted source
  - **Beware of worms that use address book**
- Lack of education
  - **"Click on the link to play the game!"**

© 2004 Grand Idea Studio, Inc.

Law #3

- If a bad guy can alter the operating system on your computer, it's not your computer anymore
- OS is the most trusted part of the computer
  - **Handles user accounts, manage passwords, access control**
- Administrator and registry access must be protected at all costs

© 2004 Grand Idea Studio, Inc.

Law #4

- If a bad guy has unrestricted physical access to your computer, it's not your computer anymore
  - **Physical destruction, bypass password mechanisms, image hard drive, add keystroke logger, etc.**
- Ensure physical protection of systems in a secure facility
- Use encrypted file system
  - **EFS, TCFS, CompuSec**

© 2004 Grand Idea Studio, Inc.

Law #5

- If you allow a bad guy to upload programs to your web site, it's not your web site anymore
- Lockdown server controls
- Beware of shared server
  - **If one web site compromised, chances are yours is, too**

© 2004 Grand Idea Studio, Inc.

Law #6

- Weak passwords trump strong security
- If password is easy to guess or obtain, any security mechanism is irrelevant
- Avoid commonly used passwords
  - **Dictionary words, husband/wife/pet's name, "money", "sex", "password"**
- Implement two-factor authentication
  - **SecurID, smartcards, biometrics**

© 2004 Grand Idea Studio, Inc.

Law #7

- A machine is only as secure as the administrator is trustworthy
- Internal attacks are most common type against corporations
  - **Disgruntled employee, tempted w/ $$$**
- Use separate accounts and enable logging for accountability

© 2004 Grand Idea Studio, Inc.

Law #8

- Encrypted data is only as secure as the decryption key
- Strength of the crypto relies on the secrecy of the key, not the algorithm
- Obfuscation (to hide encryption keys) does **not** work
- Store in secure location or secure hardware

© 2004 Grand Idea Studio, Inc.

Law #9

- An out-of-date virus scanner is only marginally better than no virus scanner at all
- Helps against known malicious code attacks
  - **Does not necessarily protect you immediately from 0-day attacks**
- Run auto-updates and keep up to patch level

© 2004 Grand Idea Studio, Inc.

Law #10

- Technology is not a panacea
- Don’t expect technology to solve all your security problems
  - **One size does not fit all**
- Do not implement unnecessary security mechanisms
  - **Strive for simplicity**
  - **Each product/tool should support a defined goal**

© 2004 Grand Idea Studio, Inc.

Quick Fixes

- Educate the whole company about security
  - **Responsibility does not fall on one single person**
- Frequently perform internal security audits
  - **In laboratory or test network**
  - **Don't let an attacker find problems first**
- Stay up-to-date on software patches

© 2004 Grand Idea Studio, Inc.

Conclusions

- The only way to stop a hacker is to think like one
  - **Do not be afraid to look for security vulnerabilities on your own network**
- Many attackers take advantage of the "low hanging fruit"
- Nothing is 100% secure
  - **Though many steps exist to "raise the bar"**

© 2004 Grand Idea Studio, Inc.