

CS615 - Aspects of System Administration

System Security

Department of Computer Science
Stevens Institute of Technology
Jan Schaumann

`jschauma@cs.stevens.edu`

`http://www.cs.stevens.edu/~jschauma/615A/`

When is a computer system secure?



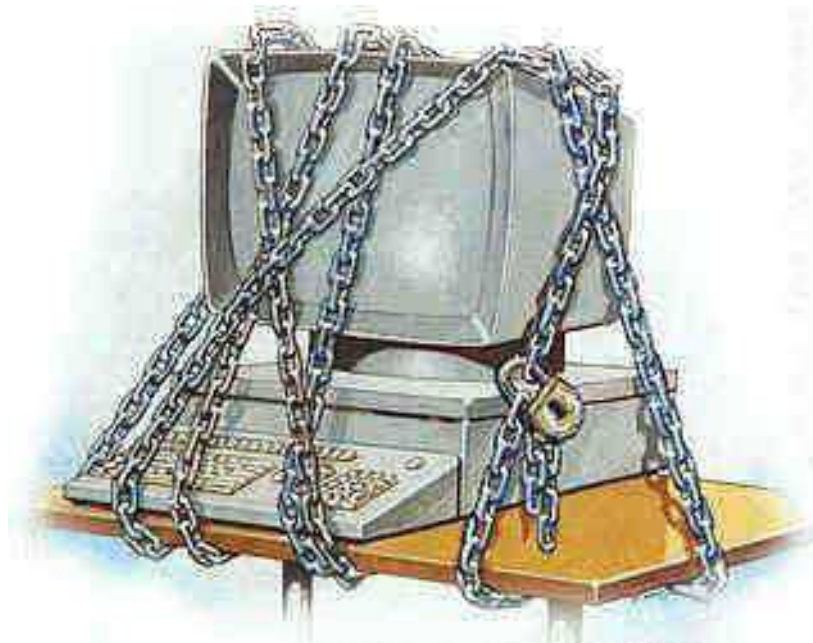
When is a computer system secure?



When is a computer system secure?



When is a computer system secure?



When is a computer system secure?



When is a computer system secure?



What is security?

security

NOUN:

Freedom from risk or danger; safety.

What is risk?

risk

NOUN:

The possibility of suffering harm or loss; danger.

What danger are you facing?

Suffering harm or loss of *what*?

What danger are you facing?

Suffering harm or loss of *what*?

- access to data

What danger are you facing?

Suffering harm or loss of *what*?

- access to data
- integrity of data

What danger are you facing?

Suffering harm or loss of *what*?

- access to data
- integrity of data
- availability of services

What danger are you facing?

Suffering harm or loss of *what*?

- access to data
- integrity of data
- availability of services
- reputation

What danger are you facing?

Suffering harm or loss of *what*?

- access to data
- integrity of data
- availability of services
- reputation
- monetary loss due to any of the above

What danger are you facing?

Suffering harm or loss of *what*?

- access to data
- integrity of data
- availability of services
- reputation
- monetary loss due to any of the above
- monetary loss due to physical items of actual value

How to determine *risk*

“Risk Assessment”

- identify *assets*

How to determine *risk*

“Risk Assessment”

- identify *assets*
- identify *threats*

How to determine *risk*

“Risk Assessment”

- identify *assets*
- identify *threats*
- identify *vulnerabilities*

How to determine *risk*

“Risk Assessment”

- identify *assets*
- identify *threats*
- identify *vulnerabilities*
- determine *likelihood of damage*

How to determine *risk*

“Risk Assessment”

- identify *assets*
- identify *threats*
- identify *vulnerabilities*
- determine *likelihood of damage*
- estimate *cost of recovery*

How to determine *risk*

“Risk Assessment”

- identify *assets*
- identify *threats*
- identify *vulnerabilities*
- determine *likelihood of damage*
- estimate *cost of recovery*
- estimate *cost of defense*

How to determine *risk*

“Risk Assessment”

- identify *assets*
- identify *threats*
- identify *vulnerabilities*
- determine *likelihood of damage*
- estimate *cost of recovery*
- estimate *cost of defense*

A *risk* is the *likelihood* of a *threat* successfully exploiting a *vulnerability* and the *estimated cost* (or potential damage) both in the short and long term you may incur as a result.

It's not just 1s and 0s

System security is not restricted to *software* security.

Physical Security

Remember that who has physical access to a machine can control the machine!

Consider:

- tamper-proof, locking cases
- door locks, window bars
- biometric identification
- security cameras, motion detectors etc.

Various People's Words of Wisdom

Thursday, April 23th, 2009

Words of Wisdom

Hanlon's Razor:

Never attribute to malice that which can be adequately explained by stupidity.

Words of Wisdom

Sturgeon's Law (first adage):

Nothing is always absolutely so.

Words of Wisdom

Sturgeon's Law (second adage):

Ninety percent of everything is crap.

Types of Vulnerabilities

- Denial of Service

Types of Vulnerabilities

- Denial of Service
- Privilege Escalation

Types of Vulnerabilities

- Denial of Service
- Privilege Escalation
- Backdoor

Types of Vulnerabilities

- Denial of Service
- Privilege Escalation
- Backdoor
- Direct Access

Types of Vulnerabilities

- Denial of Service
- Privilege Escalation
- Backdoor
- Direct Access
- Privacy Leak

Types of Vulnerabilities

- Denial of Service
- Privilege Escalation
- Backdoor
- Direct Access
- Privacy Leak
- Social Engineering

Types of Vulnerabilities

- Denial of Service
- Privilege Escalation
- Backdoor
- Direct Access
- Privacy Leak
- Social Engineering
- ...

Types of Vulnerabilities



Encryption

Encryption can help mitigate *some* of the risks *sometimes*.

Encryption

Encryption can help mitigate *some* of the risks *sometimes*.

It may provide security in the areas of:

- Secrecy or Confidentiality

Encryption

Encryption can help mitigate *some* of the risks *sometimes*.

It may provide security in the areas of:

- Secrecy or Confidentiality
- Accuracy or Integrity

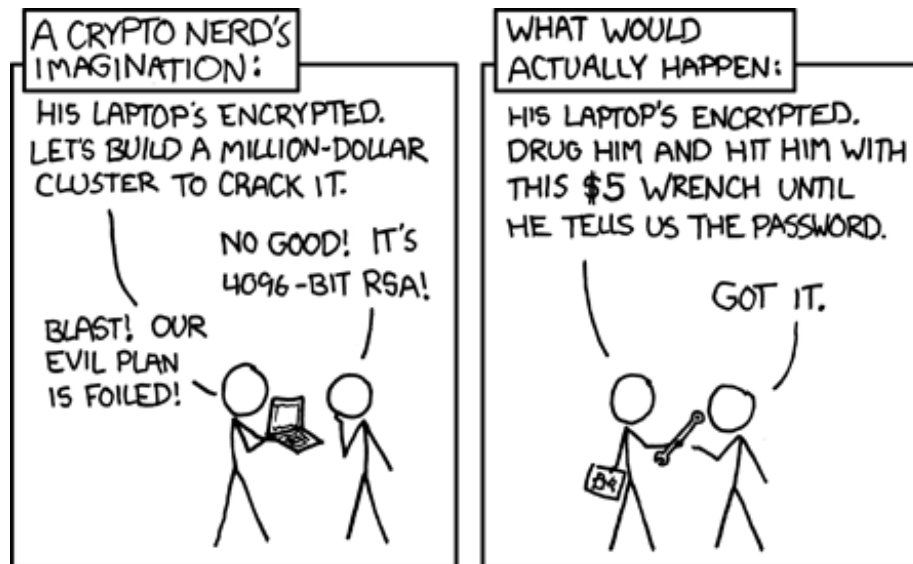
Encryption

Encryption can help mitigate *some* of the risks *sometimes*.

It may provide security in the areas of:

- Secrecy or Confidentiality
- Accuracy or Integrity
- Authenticity

Understanding your realistic threats



Practical System Security

- Authentication, Passwords and Permissions
- System Integrity
- Data and Network Traffic Encryption

All of the above are subject to your, your users and other peoples

- ignorance
- laziness
- malice

Another Word of Wisdom

Bruce Schneier:

Complexity is the worst enemy of security.

Whom do you trust?



What to do in the case of an emergency

As usual, this *depends*. Some the smarter things to do if you detect an intrusion include:

- keep system online to monitor what the attacker does or how she gained access,
or
- take system offline, possible entirely into single user mode
- take a complete snapshot of the system to separate media
- keep system offline while you investigate
- reinstall

Remember that you can't trust *any* data on the compromised system!

Miscellaneous

Things probably mentioned before, but worth repeating:

- subscribe to your vendors security alert mailinglist
- subscribe to independent security alert mailinglists
- checksum and verify any and all packages and patches
- regularly audit the installed software
- require strong passwords
- inform your users on security issues
- guard against threats from outside as well as inside the network

Be Paranoid!



Reading

Helpful Tools:

- `mtree(1)`
- `gpg(1)`

Helpful Information:

- CSRC NIST <http://csrc.nist.gov/>
- SecurityFocus <http://www.securityfocus.com/>
- CryptoGram <http://www.counterpane.com/crypto-gram.html>

Misc:

- <http://archive.cert.uni-stuttgart.de/isn/2006/01/msg00055.html>