Security Principles

(as usual, thanks to Dave Wagner and

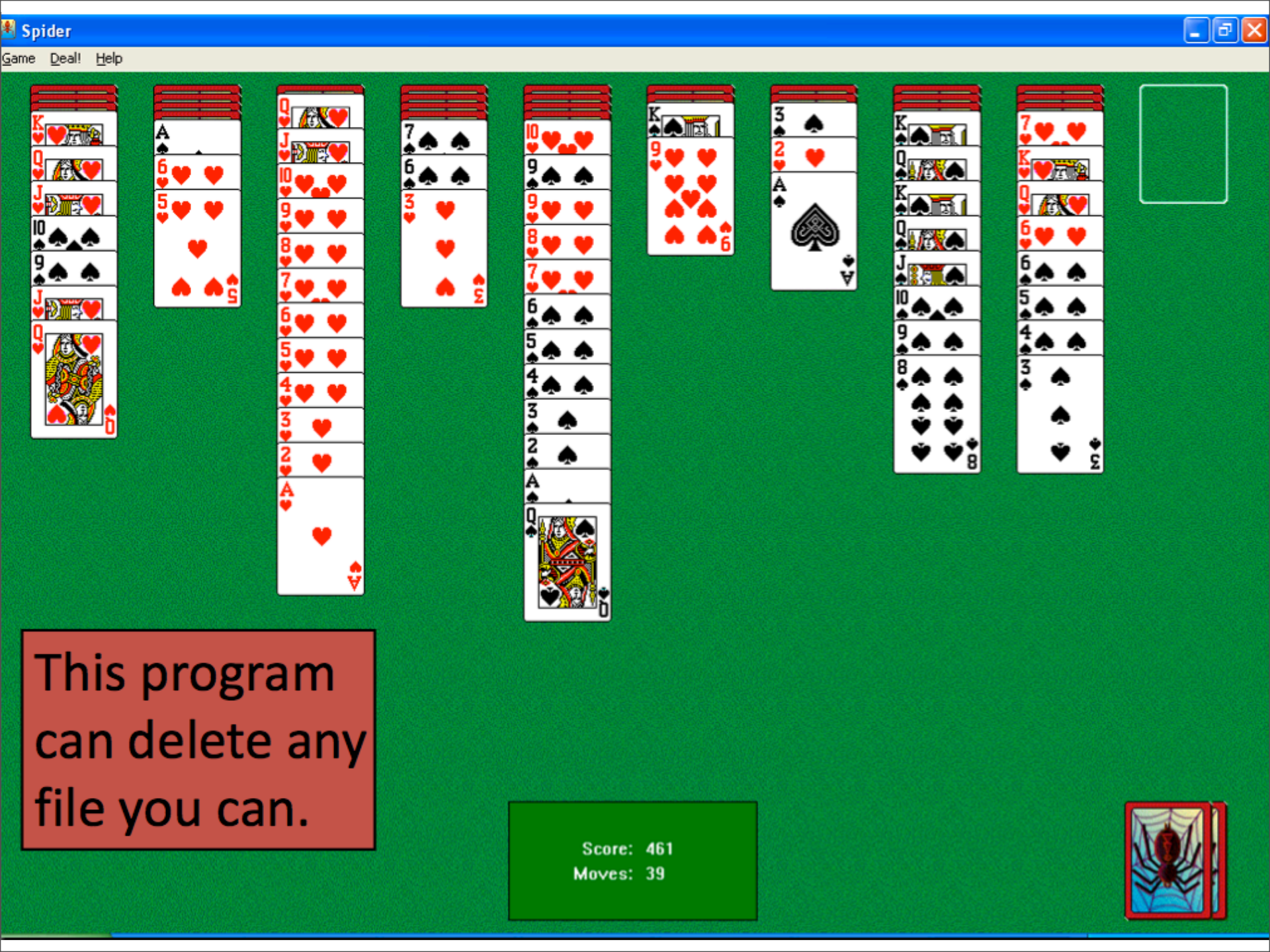
TL-15

TL-30

TRTL-30

TXTL-60

“Security is economics”


Spider
Game
Deal!
Help
This program can delete any file you can.
Score: 461
Moves: 39

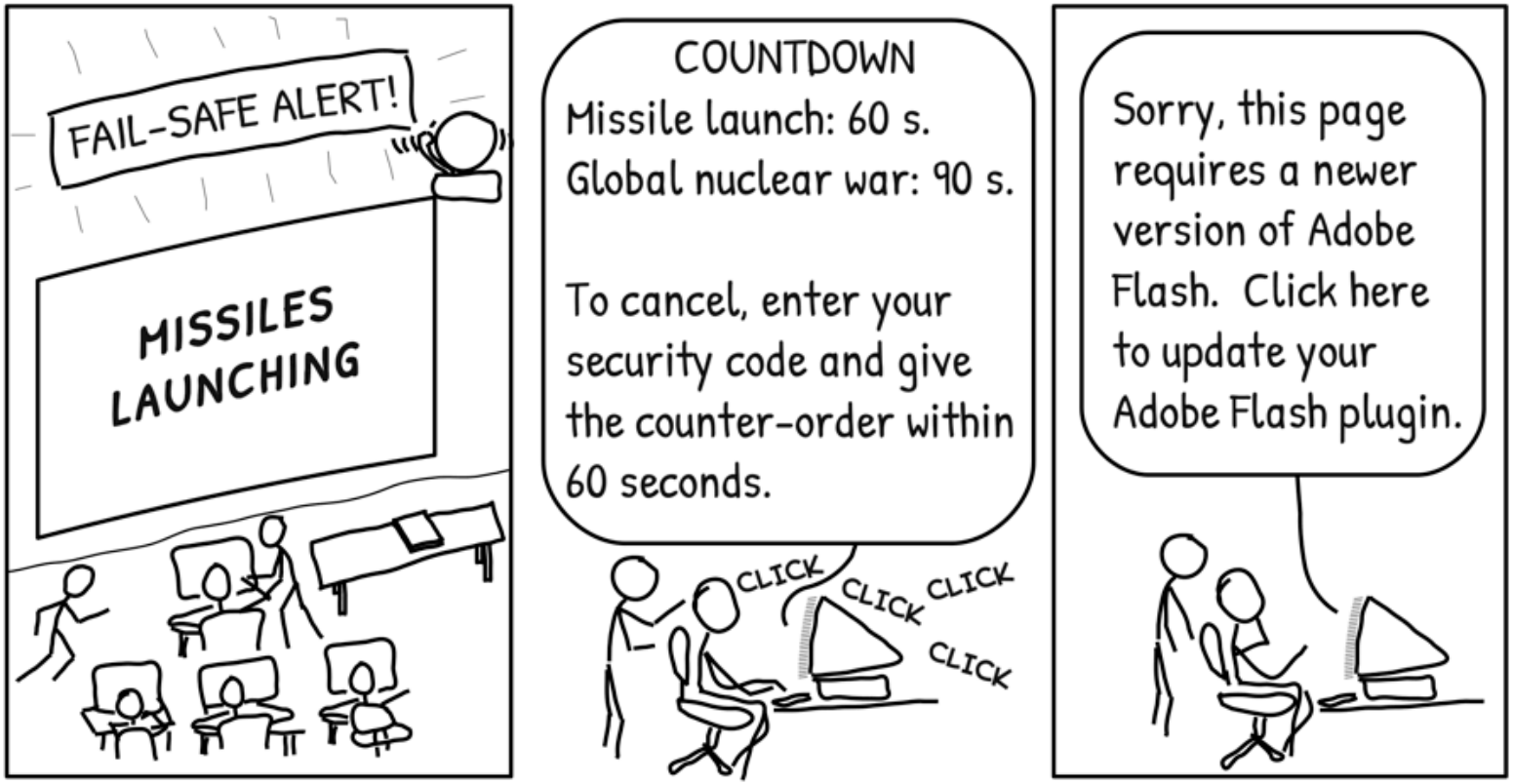
“Least Privilege”

“Least Privilege”

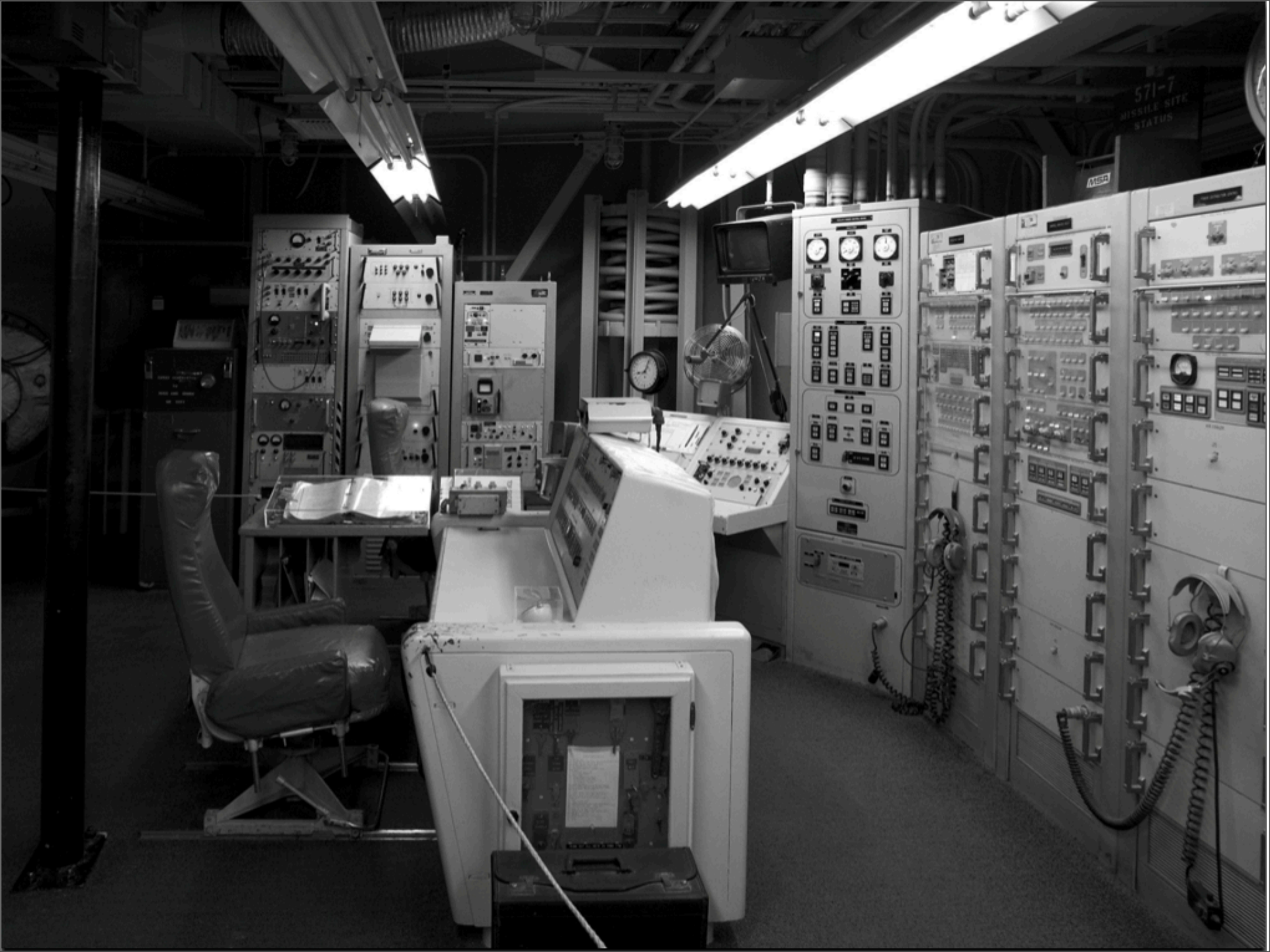
Every entity (process, user, program, etc.) must be able to access only such information and resources necessary for its legitimate purpose

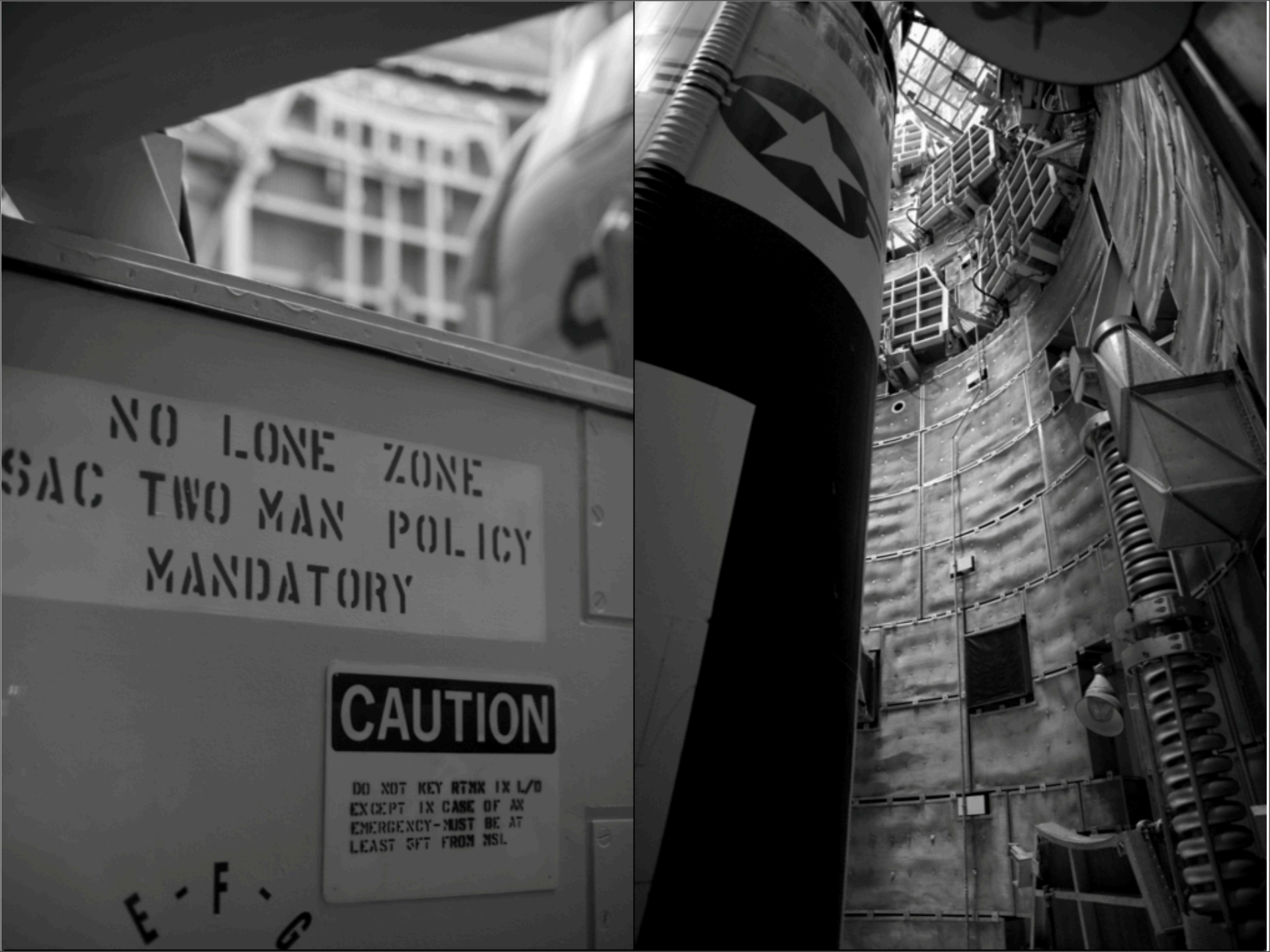
https://www.youtube.com/watch?v=rwgSVhgFm7E

“Use fail-safe defaults”


FAIL-SAFE ALERT!
MISSILES LAUNCHING
COUNTDOWN
Missile launch: 60 s.
Global nuclear war: 90 s.
To cancel, enter your security code and give the counter-order within 60 seconds.
CLICK
CLICK
CLICK
CLICK
Sorry, this page requires a newer version of Adobe Flash. Click here to update your Adobe Flash plugin.
icanbarelydraw.com CC BY-NC-ND 3.0

Fail-Safe.


571-7
MISSILE SITE
STATUS


NO LONE ZONE
SAC TWO MAN POLICY
MANDATORY
CAUTION
DO NOT KEY RTNX IX L/D
EXCEPT IN CASE OF AN
EMERGENCY-MUST BE AT
LEAST 5FT FROM MSL
E-F-G

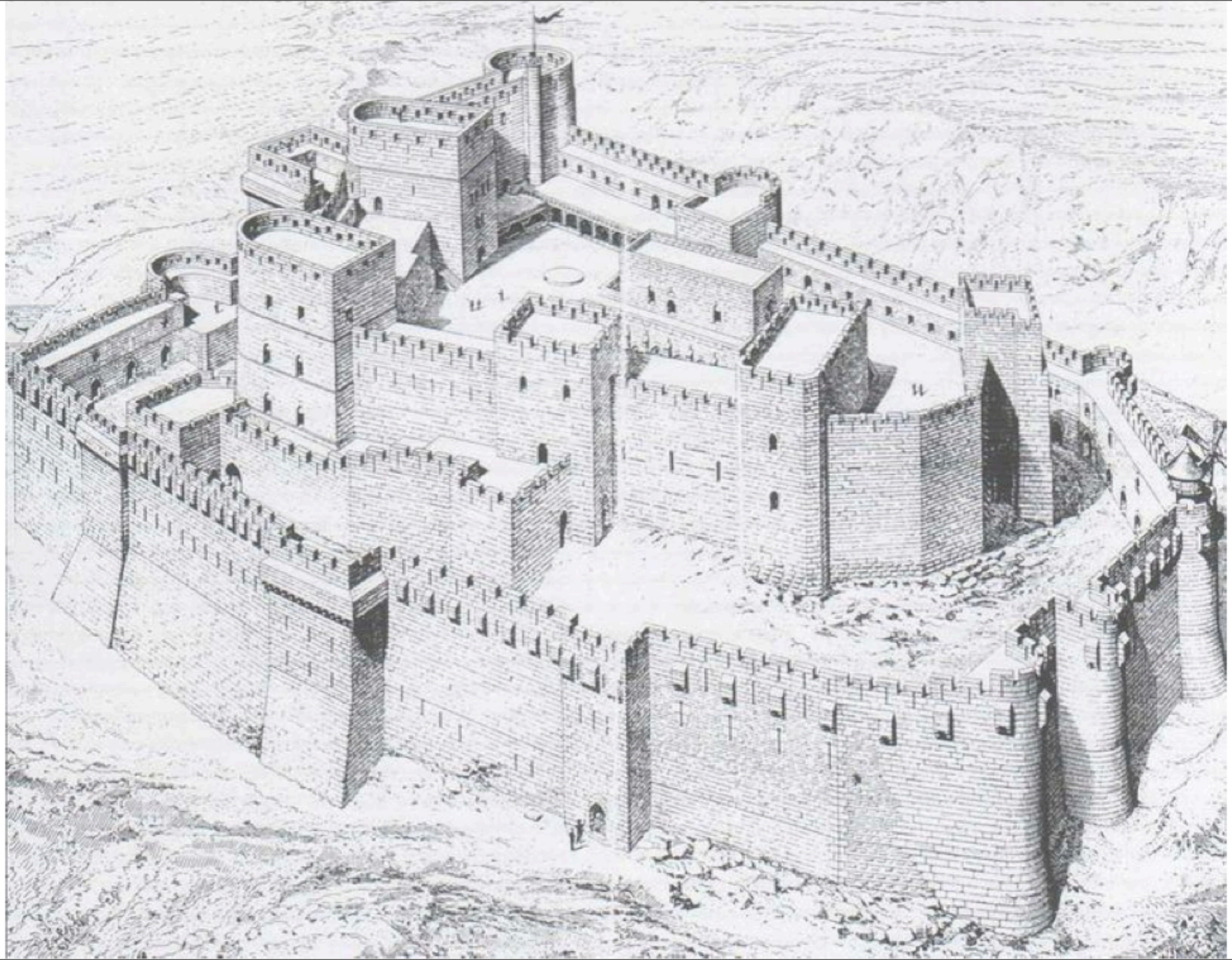
“Separation of Responsibility”

“Separation of Responsibility”

System should be divided into entities that overlap in functionality as little as possible.

Alternative statement: Split up privilege so no one person or program has complete power. Require more than one party to approve before access is granted.


TICKET
356011



“Defense in depth”

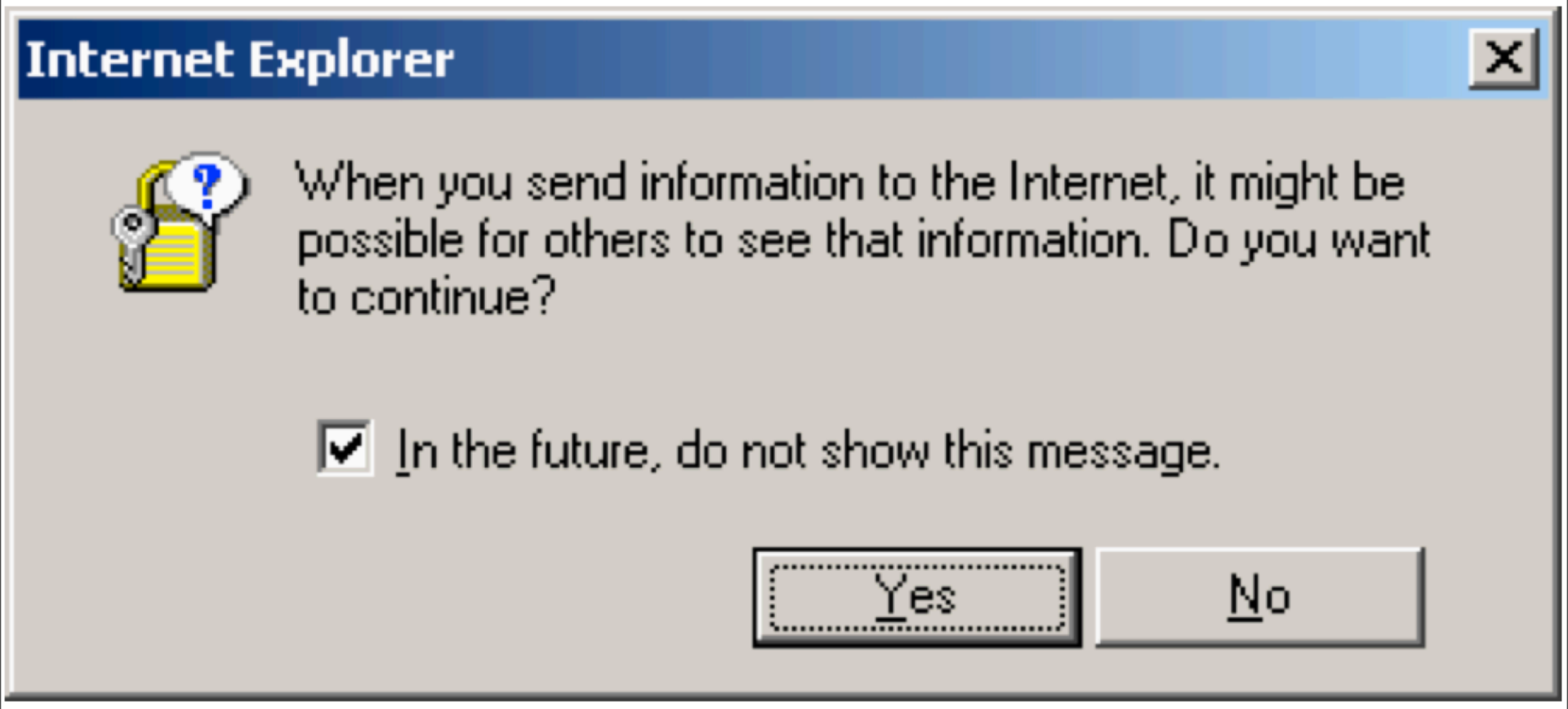
Password selection

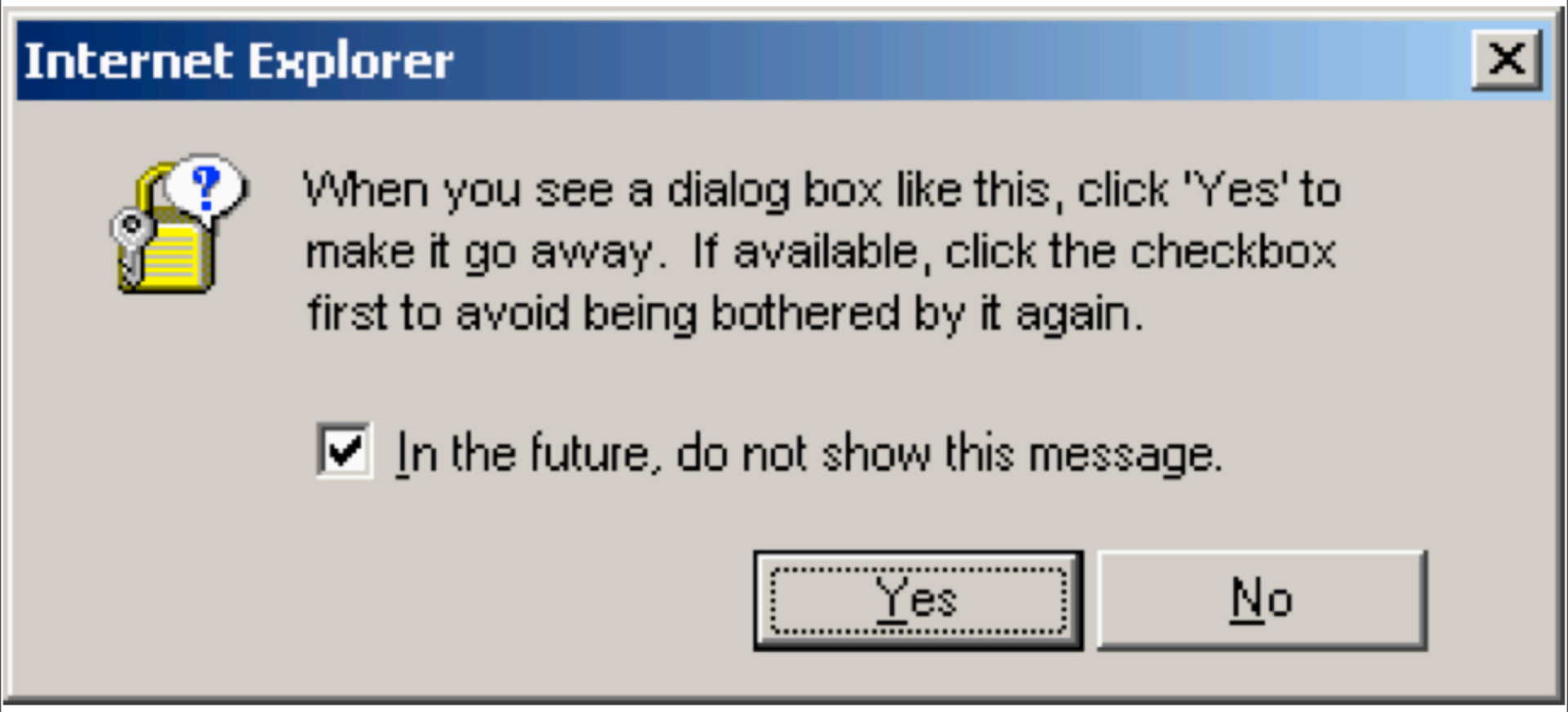
2.6.8. Where passwords are used as the sole authentication method, they **SHOULD**:

a. be a minimum of 7 characters, and
b. consist of at least 3 of the following character sets:
    i) lowercase characters (a-z),
    ii) uppercase characters (A-Z),
    iii) digits (0–9), and
    iv) punctuation and special characters.
    Examples: !@#$%^&*

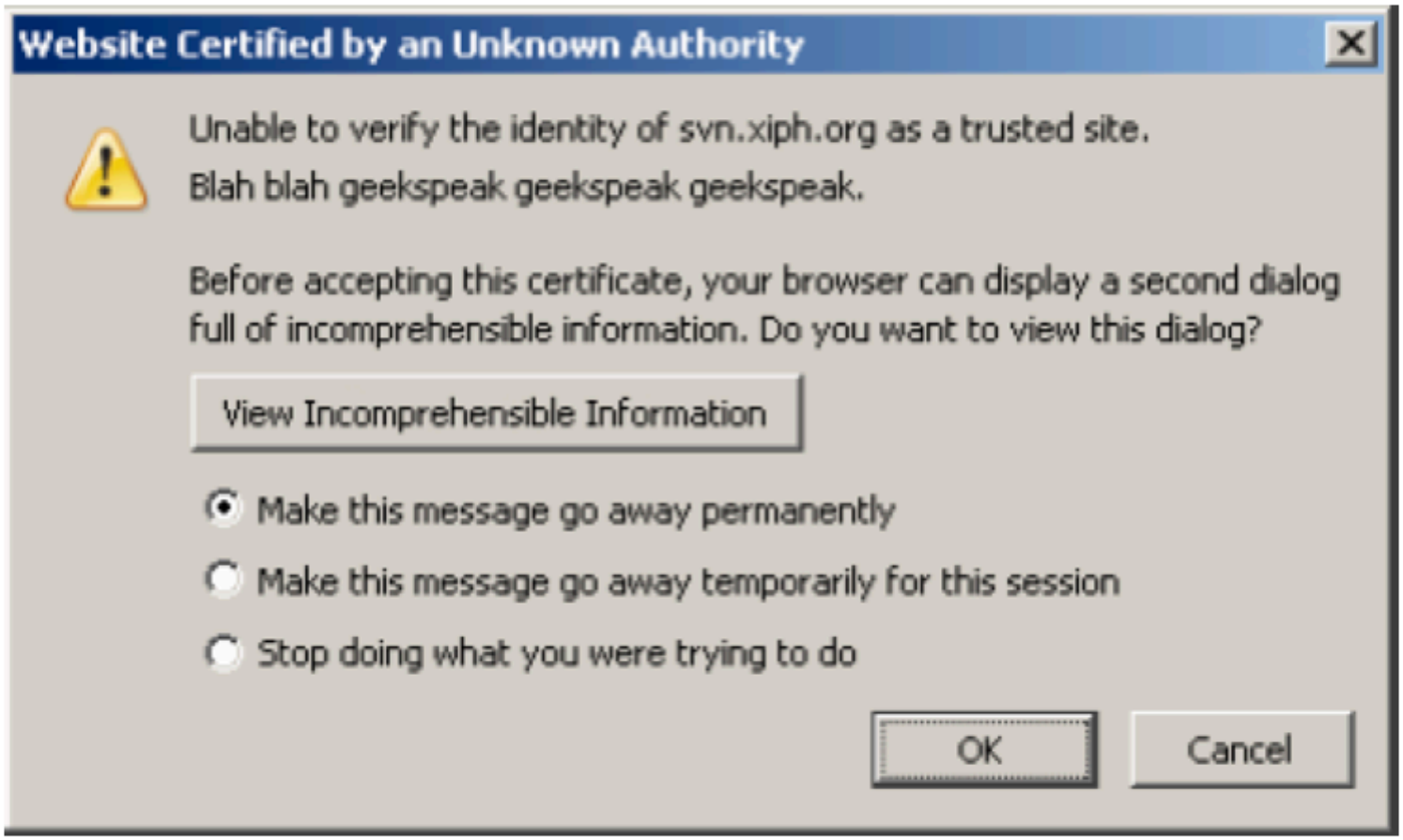
These requirements **SHOULD** be enforced by the system.

“Psychological acceptability”


Internet Explorer
When you send information to the Internet, it might be possible for others to see that information. Do you want to continue?
In the future, do not show this message.
Yes
No


Internet Explorer
When you see a dialog box like this, click 'Yes' to make it go away. If available, click the checkbox first to avoid being bothered by it again.
In the future, do not show this message.
Yes
No


Website Certified by an Unknown Authority
Unable to verify the identity of svn.xiph.org as a trusted site.
Possible reasons for this error:
- Your browser does not recognise the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be svn.xiph.org, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site svn.xiph.org?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this Web site
OK
Cancel


Website Certified by an Unknown Authority
Unable to verify the identity of svn.xiph.org as a trusted site.
Blah blah geekspeak geekspeak geekspeak.
Before accepting this certificate, your browser can display a second dialog full of incomprehensible information. Do you want to view this dialog?
View Incomprehensible Information
Make this message go away permanently
Make this message go away temporarily for this session
Stop doing what you were trying to do
OK
Cancel

“Consider human factors”

“Ensure complete mediation”

“Ensure complete mediation”

Every access attempt must be checked. Both direct access attempts and attempts to circumvent the access checking mechanism should be considered, and the mechanism should be positioned so that it cannot be circumvented.

(Pfleeger and Pfleeger)

Know your threat model! (They often change over time.)


ATM


HARLEY-
DAVIDSON

Detect if you can't prevent!


A'LA'IH, DO'NEH'LINI,
DO'NEH'LINI, A'LA'IH,
A'LA'IH, DO'NEH'LINI,
DO'NEH'LINI, DO'NEH'LINI,
A'LA'IH, A'LA!H,
DO'NEH'LINI, A'LA'IH,
DO'NEH'LINI, DO'NEH'LINI,
DO'NEH'LINI . . .
FOR ADDED SECURITY, AFTER WE ENCRYPT THE DATA STREAM, WE SEND IT THROUGH OUR NAVAJO CODE TALKER.
... IS HE JUST USING NAVAJO WORDS FOR "ZERO" AND "ONE"?
WHOA, HEY, KEEP YOUR VOICE DOWN!


ACCIDENT
ON
MOTORWAY


ACCIDENT
ON
MOTORWAY


CAUTION!
ZOMBIES!
AHEAD!!!
RUN FOR
COLD
CLIMATES
THE END
IS NEAR!
!!!!!!!!!


RAPTORS
AHEAD
CAUTION


TRAPPED
IN SIGN
FACTORY


SEND
HELP!

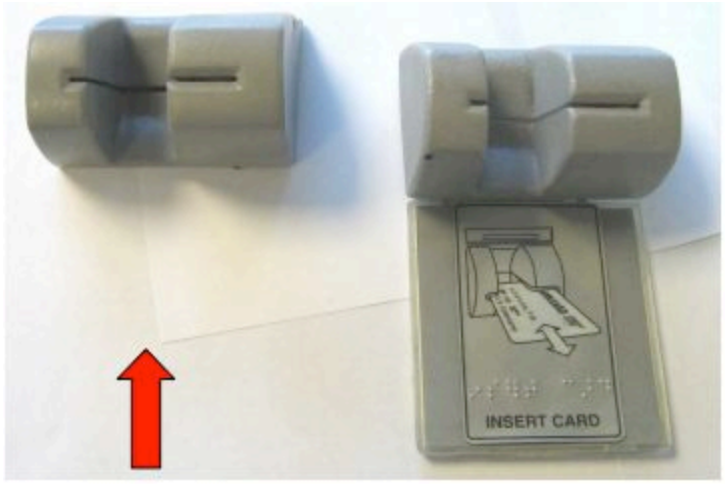
Don’t rely on security through obscurity!

“Don’t rely on security through obscurity.”

The notion that secrecy of design or implementation provides security.

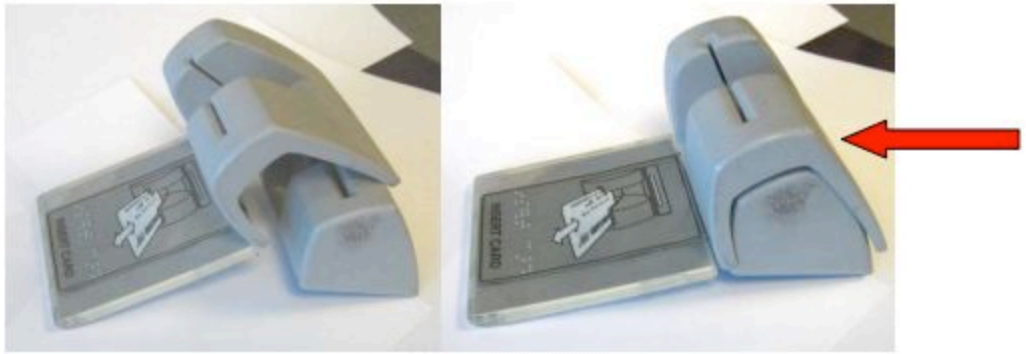
Design security in from the start!


Lectura de código de barras

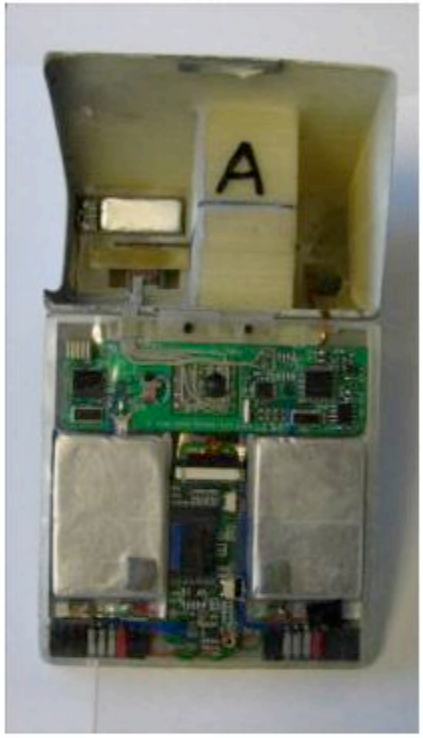


The real card reader slot.

The capture device



The side cut out is not visible when on the ATM.



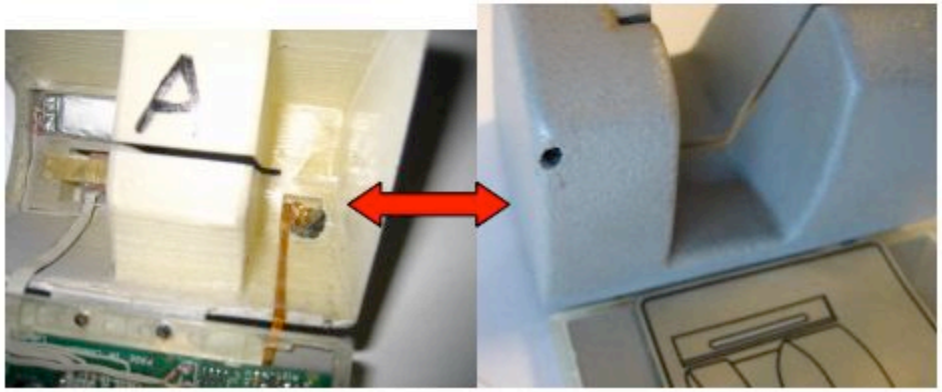
This is the back side of the device.

The card reader is on the left and the camera is tucked into the right side as shown below.

The device may have been constructed with parts from an MP3 Player.

It was attached with several small pieces grey double-sided tape

The part was well made and fit nicely over the original card reader.




Expresso


Bradesco
Tarifas de
Serviços Bancários
Multi Expresso


Bradesco
Tarifas de
Serviços Bancários


Ispričujemo, ale bankomat je

Installation time?

Installation time?


Undergraduate
Admissions 2/2007


ต้องใช้บัตร


1 QZ
2 ABC
3 DEF
CLEAR
4 GHI
5 JKL
6 MNO
CANCEL
7 PRS
8 TUV
9 WXY
ENTER
0


ert Your Card To Begin
favor, inserte su tarjeta.
Enter
Clear
Cancel
VISA


VISA

“Trusted path.”

“Trusted path”

The user must have an unspoofable and incorruptible channel to any entity trusted to manipulate authorities on the user’s behalf.

(Ka-Ping Yee “User Interaction Design for Secure Systems”)

“Trusted path”

The user must have an unspoofable and incorruptible channel to any entity trusted to manipulate authorities on the user’s behalf.

(Ka-Ping Yee “User Interaction Design for Secure Systems”)