

Security Principles

**(as usual, thanks to Dave Wagner and
Vern Paxson)**



TL-15



TL-30



TRTL-30



TXTL-60

“Security is economics”

or, as I’ve been saying,

**“Security is all about risk
analysis”**



This program
can delete any
file you can.

Score: 461
Moves: 39



“Least Privilege”

“Least Privilege”

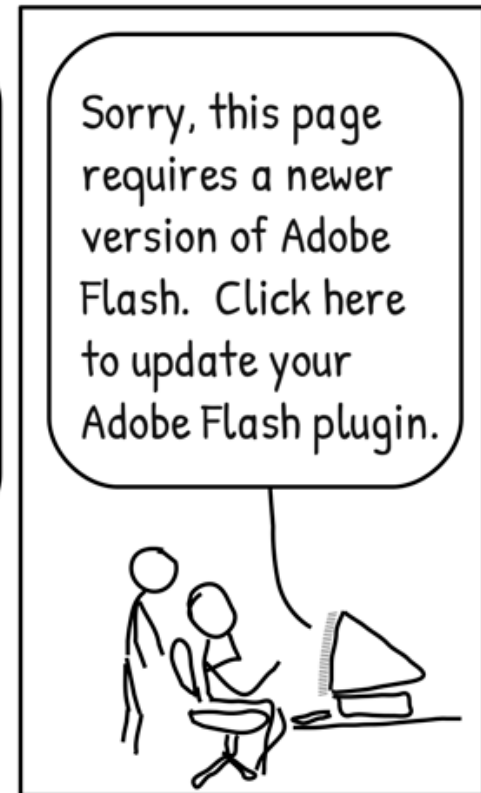
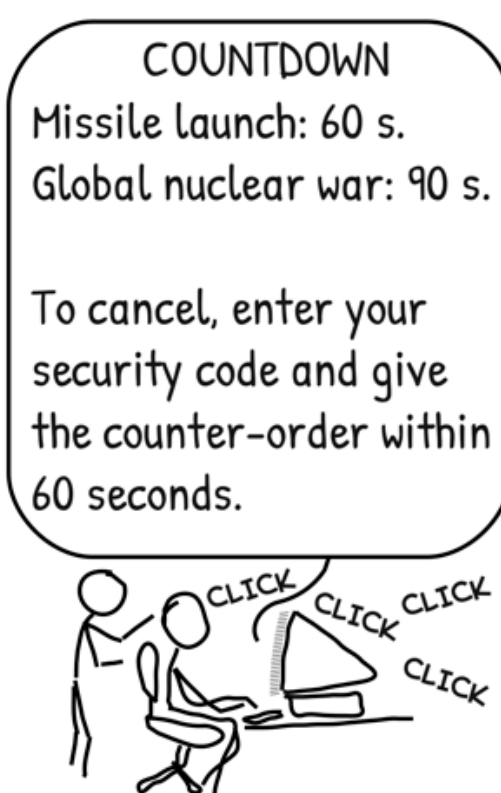
Every entity (process, user, program, etc.) must be able to access only such information and resources necessary for its legitimate purpose



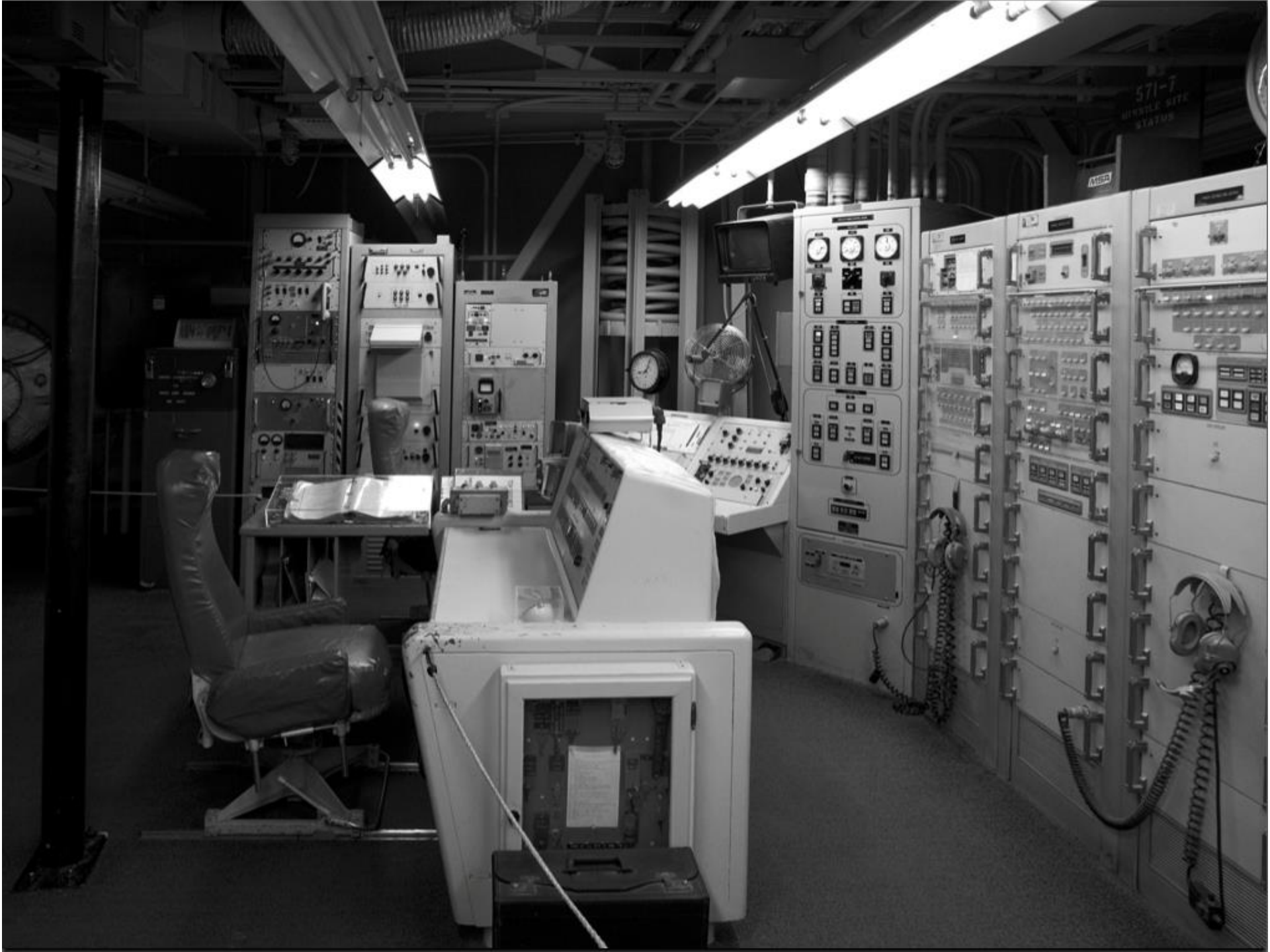
“Use fail-safe defaults”



Fail-Safe.



icanbarelydraw.com CC BY-NC-ND 3.0



571-7
MINI-MITE
STATUS

ATER

571-7
MINI-MITE
STATUS

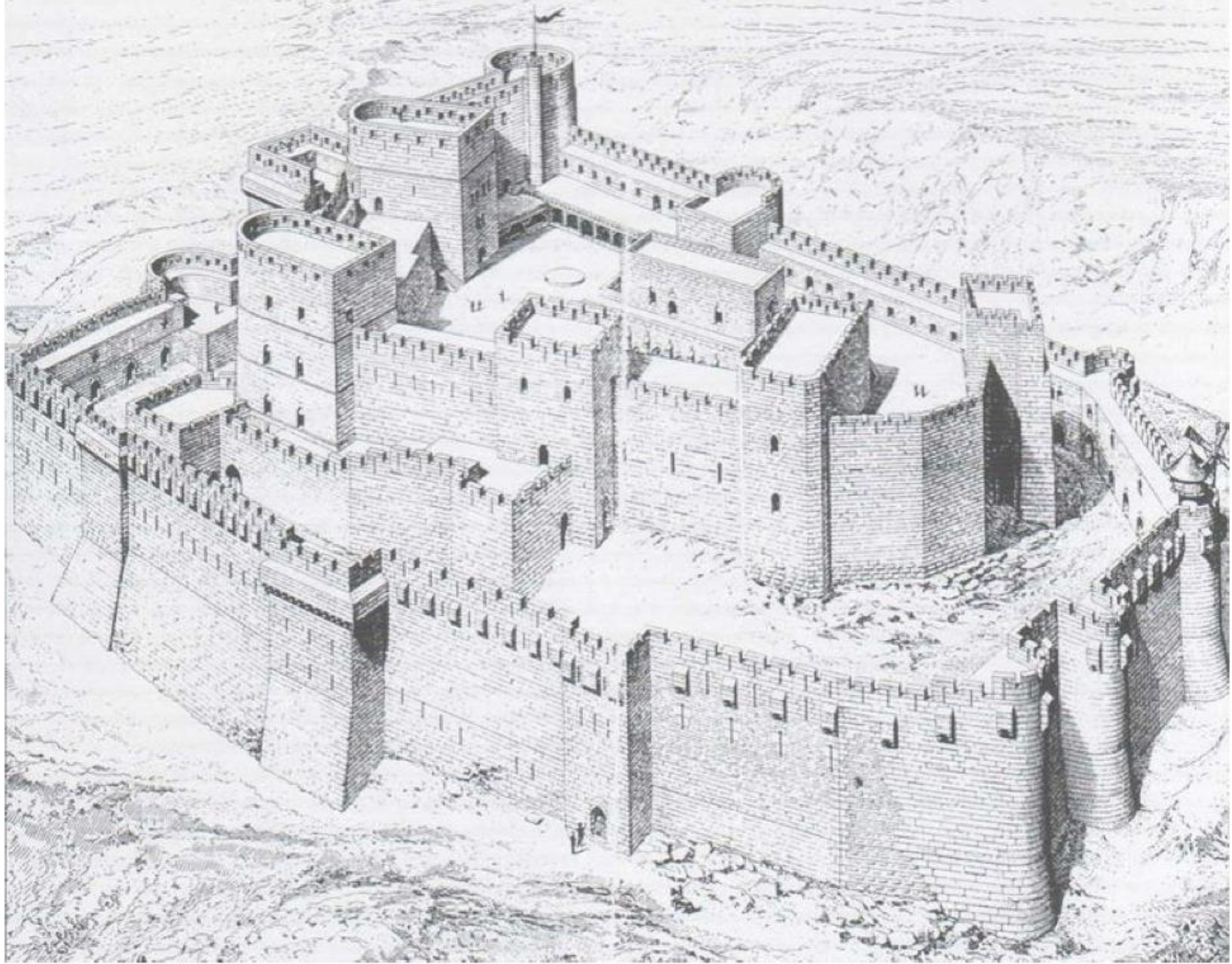
571-7
MINI-MITE
STATUS



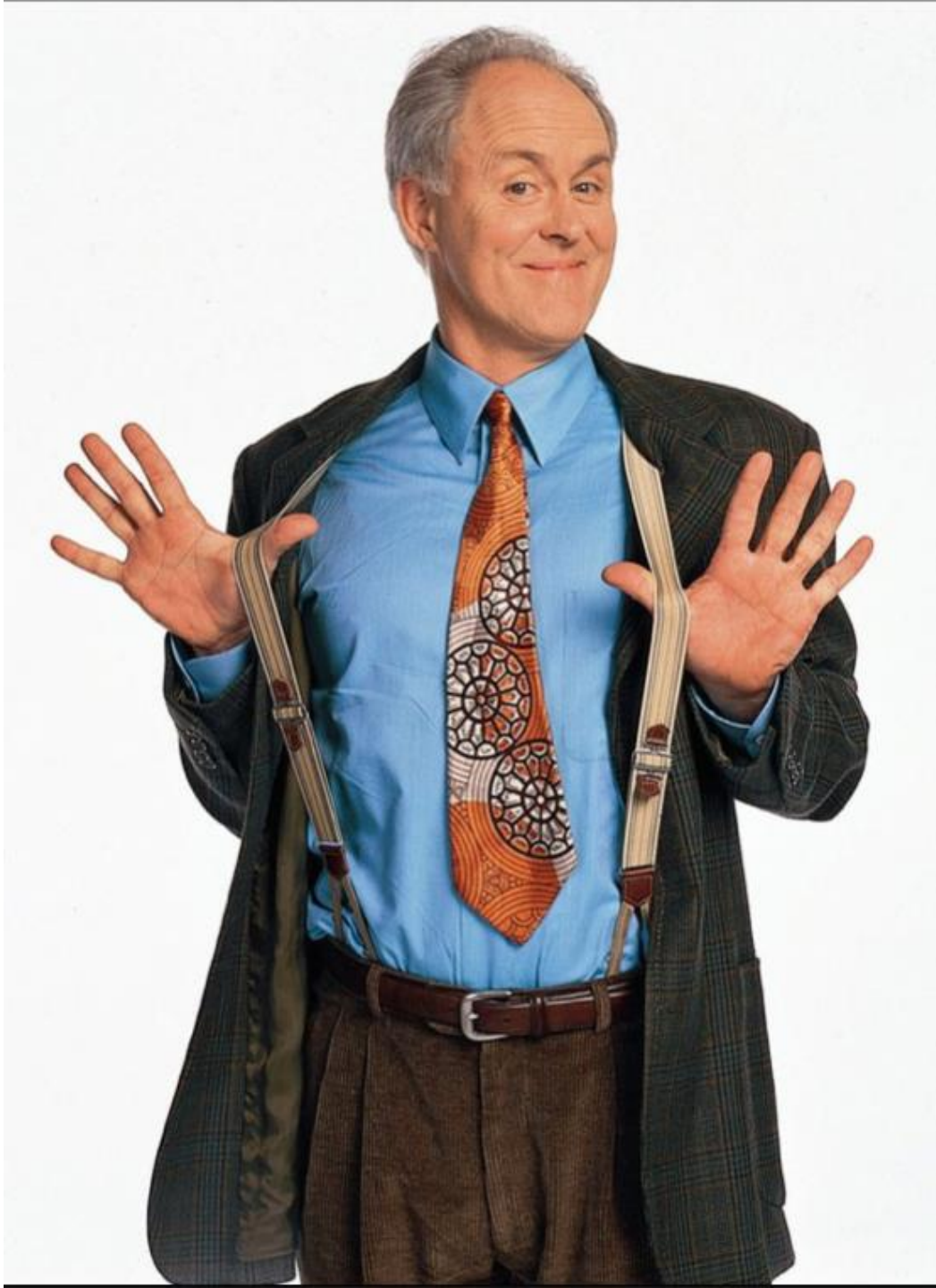
- **Key Security (Access Control):** The launch keys are stored in a secure safe that requires two different, independent keys or combinations to open. No single person has access to the keys necessary to start the launch sequence.
- **Physical Separation of Controls:** The consoles for the commander and deputy commander are positioned, for example, 12 feet apart. This physical distance makes it impossible for one person to turn both launch keys simultaneously.
- **Dual Verification of Orders:** Before initiating a launch, both operators must verify that the launch order (Emergency Action Message) is authentic by comparing authorization codes against a "sealed authenticator". This means both must independently agree the order is legitimate.
- **Simultaneous Action:** The launch sequence requires that both operators turn their keys at the same time. This ensures that both individuals are active participants in the decision to launch.
- **Redundant Command Checks:** For additional protection, another separate launch control center must also concur with the launch, further distributing responsibility beyond just one team.
- **No-Lone Zone Requirement:** Regulations mandate that at least two authorized, vetted individuals are present at all times in "no-lone zones," preventing a single person from being alone with the control systems. 

“Separation of Responsibility”

“Separation of Responsibility”
System should be divided into
entities that overlap in
functionality as little as
possible.



“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.

Your password is case-sensitive and must:

- Be six to twenty characters in length.
- Not use characters other than letters and numbers (e.g. *, &, #, “, etc.).
- Not match your first or last name, or the combination of some or all of your first and last name.
- Not use your date of birth in any combination (e.g. MMDDYYYY)
- Not include the first four to eight digits of your wireless number.
- Not match part or all of your account number.
- Not match your MediaNet User ID
- Not be an e-mail address.
- Not have repeating characters longer than two (e.g. aaa).
- Not have ascending characters longer than three (e.g. abcd).

“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.

(Pfleegeer and Pfleegeer)



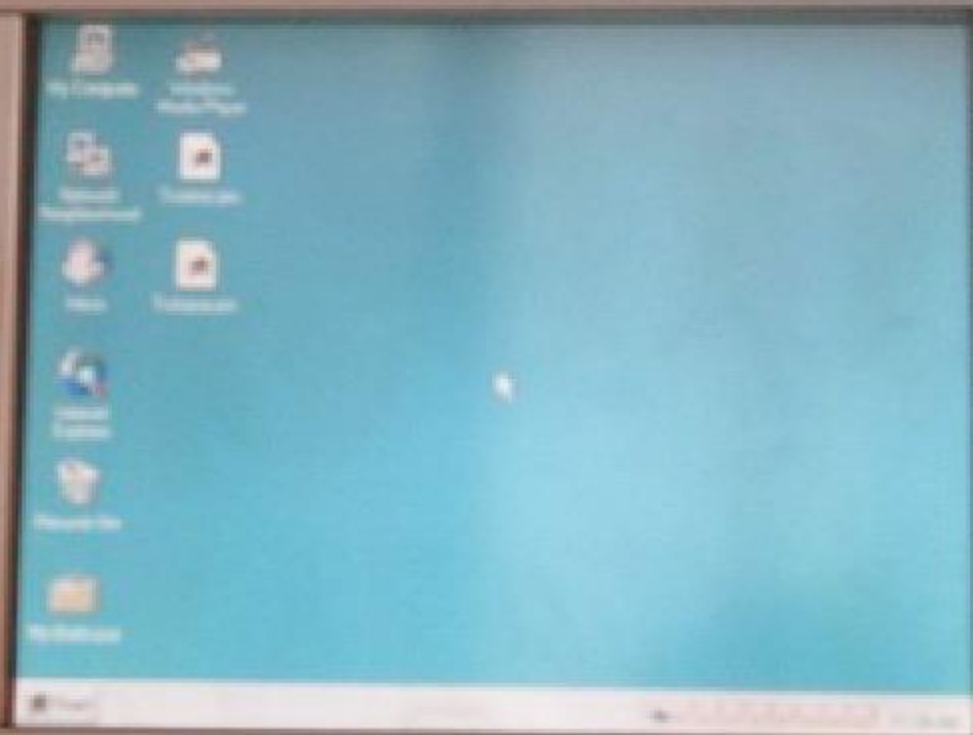


Know your threat model! (They often change over time.)

ATM



ATM







[All Products](#)

[Protect Plans](#)

[Neighbors](#)

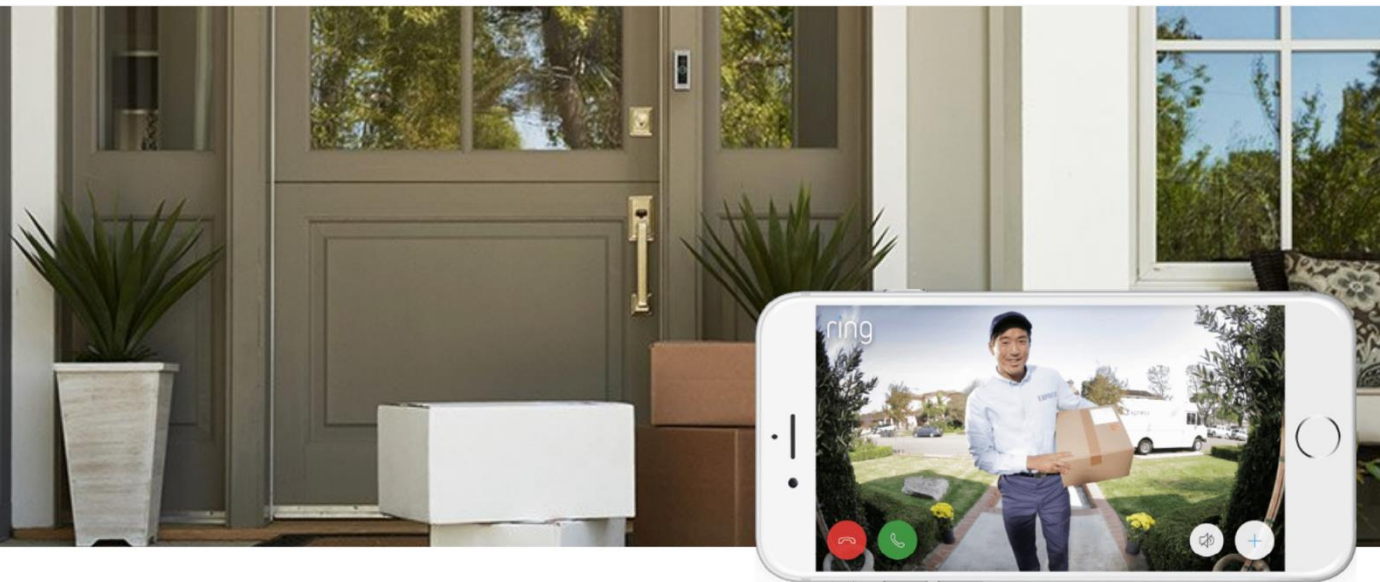
[Help](#)

[Log In](#)

[Cart \(0\)](#)

Video Doorbells

See, hear and speak to people at your door from your phone, tablet and PC.



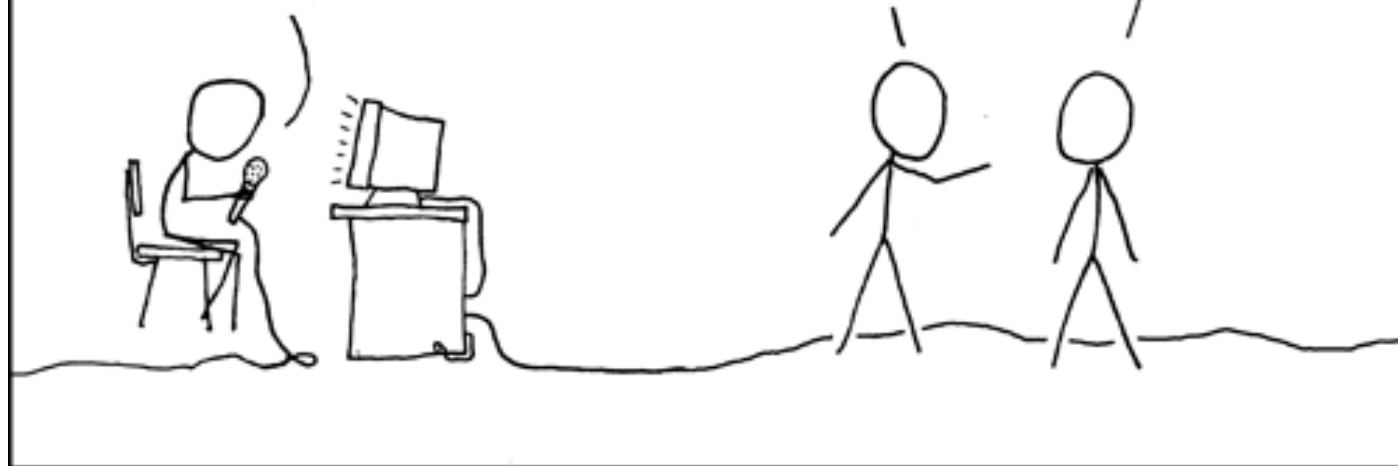
Detect if you can't prevent!

ALA'IH, DO'NEH'LINI,
DO'NEH'LINI, ALA'IH,
ALA'IH, DO'NEH'LINI,
DO'NEH'LINI, DO'NEH'LINI,
ALA'IH, ALA'IH,
DO'NEH'LINI, ALA'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







RAPTORS
AHEAD
CAUTION

RAVENS
CAUTION

MARSH

RAVENS
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!**



Letras de papel de 100g/m² e 120g/m²



Letras de papel de 100g/m² e 120g/m²

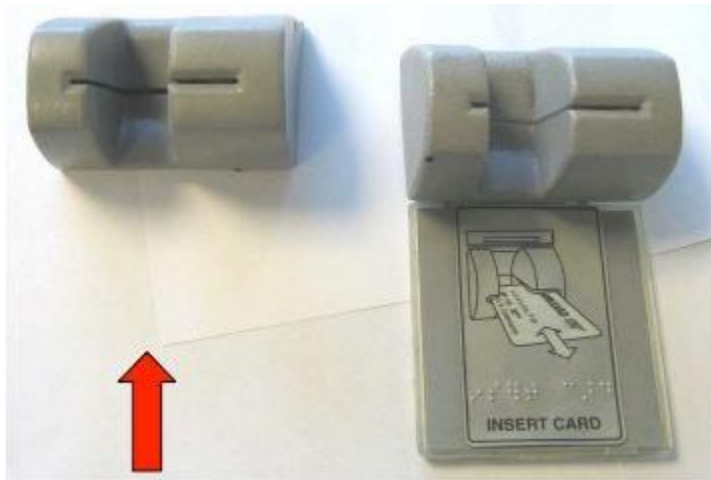
Letras de papel de 100g/m² e 120g/m²

Letras de papel de 100g/m² e 120g/m²



Recycling





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.





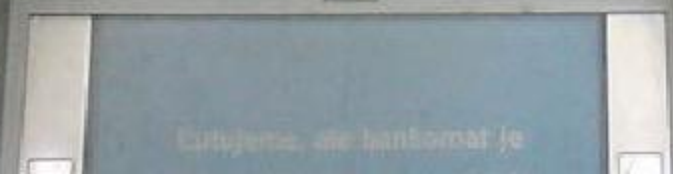


Multi Expresso









100-779(3.5)

Installation time?

About 30 seconds













“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”)**