Access Control and Privacy Policies (4)

Email: christian.urban at kcl.ac.uk
Office: S1.27 (1st floor Strand Building)
Slides: KEATS (also homework is there)

Unix-Style Access Control

- Q: "I am using Windows. Why should I care?"
  A: In Windows you have:

  administrators group
  (has complete control over the machine)
  authenticated users
  server operators
  power users
  network configuration operators

- Modern versions of Windows have more fine-grained AC; they do not have a setuid bit, but have `runas` (asks for a password).

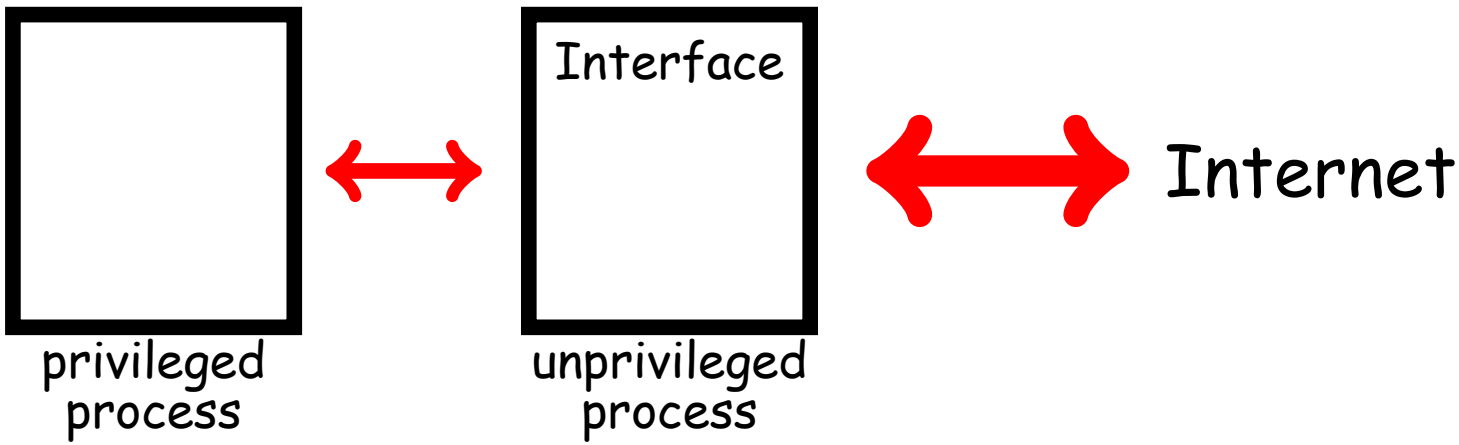
Unix-Style Access Control

- Q: "I am using Windows. Why should I care?"
  A: In Windows you have:

  administrators group
  (has complete control over the machine)
  authenticated users
  server operators
  power users
  network configuration operators

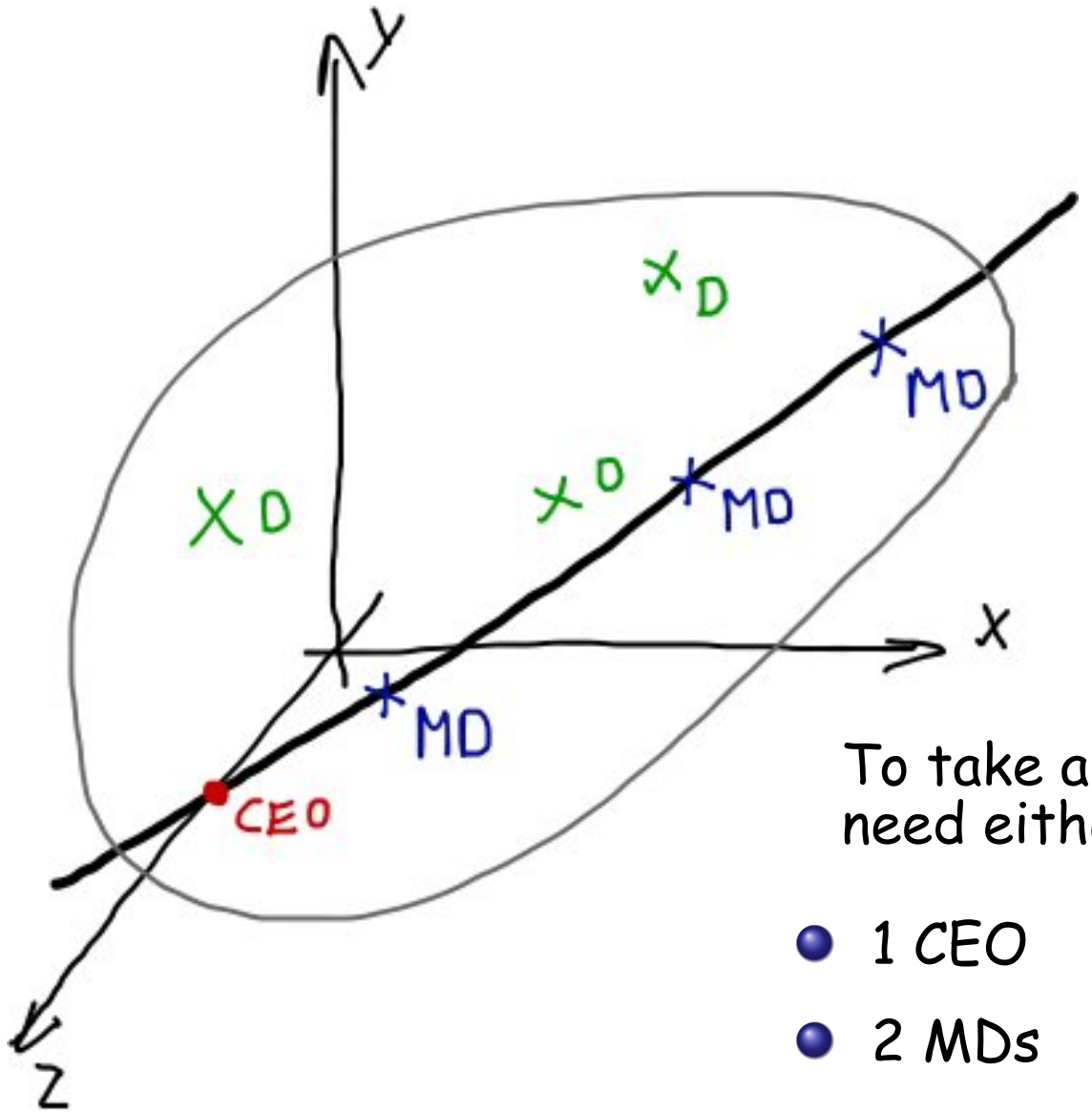
- Modern versions of Windows have more fine-grained AC; they do not have a setuid bit, but have `runas` (asks for a password).
- OS provided access control can add to your security.

Network Applications: Privilege Separation



- the idea is make the attack surface smaller and mitigate the consequences of an attack

Shared Access Control



To take an action you need either:

- 1 CEO
- 2 MDs
- 3 Ds

Lessons from Access Control

- if you have too many roles (i.e. too finegrained AC), then hierarchy is too complex
  you invite situations like. . . let's be root

- you can still abuse the system. . .

A "Cron"-Attack

The idea is to trick a privileged person to do something on your behalf:

- root:

```
rm /tmp/*/*
```

A "Cron"-Attack

The idea is to trick a privileged person to do something on your behalf:

- root:

  ```
  rm /tmp/*/*
  ```

  the shell behind the scenes:

  $\texttt{rm /tmp/dir}_1\texttt{/file}_1\ \texttt{/tmp/dir}_1\texttt{/file}_2\ \texttt{/tmp/dir}_2\texttt{/file}_1\ \ldots$

  this takes time

A "Cron"-Attack

1. attacker (creates a fake passwd file)
   `mkdir /tmp/a; cat > /tmp/a/passwd`
2. root (does the daily cleaning)
   `rm /tmp/*/*`

   records that `/tmp/a/passwd`

   should be deleted, but does not do it yet
3. attacker (meanwhile deletes the fake passwd file, and establishes a link to the real passwd file)
   `rm /tmp/a/passwd; rmdir /tmp/a;`
   `ln -s /etc /tmp/a`
4. root now deletes the real passwd file

A "Cron"-Attack

1. attacker (creates a fake passwd file)
   `mkdir /tmp/a; cat > /tmp/a/passwd`
2. ro
   rr

To prevent this kind of attack, you need additional policies.

records that `/tmp/a/passwd`
should be deleted, but does not do it yet

3. attacker (meanwhile deletes the fake passwd file, and establishes a link to the real passwd file)
   `rm /tmp/a/passwd; rmdir /tmp/a;`
   `ln -s /etc /tmp/a`
4. root now deletes the real passwd file

Schneier Analysis

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

There is no absolutely secure system and security almost never comes for free.

Example: Credit Cards

You might have the policy of not typing in your credit card online. Worthwhile or not?

Example: Credit Cards

You might have the policy of not typing in your credit card online. Worthwhile or not?

- What assets are you trying to protect?
  your credit card number

Example: Credit Cards

You might have the policy of not typing in your credit card online. Worthwhile or not?

- What assets are you trying to protect?
- What are the risks to these assets?

  With credit cards you loose a fixed amount £50. Amazon £50.

Example: Credit Cards

You might have the policy of not typing in your credit card online. Worthwhile or not?

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?

  Well, hackers steal credit cards from databases. They usually do not attack you individually.

Example: Credit Cards

You might have the policy of not typing in your credit card online. Worthwhile or not?

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?

  None (?)

Example: Credit Cards

You might have the policy of not typing in your credit card online. Worthwhile or not?

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

  Internet shopping is convenient and sometimes cheaper.

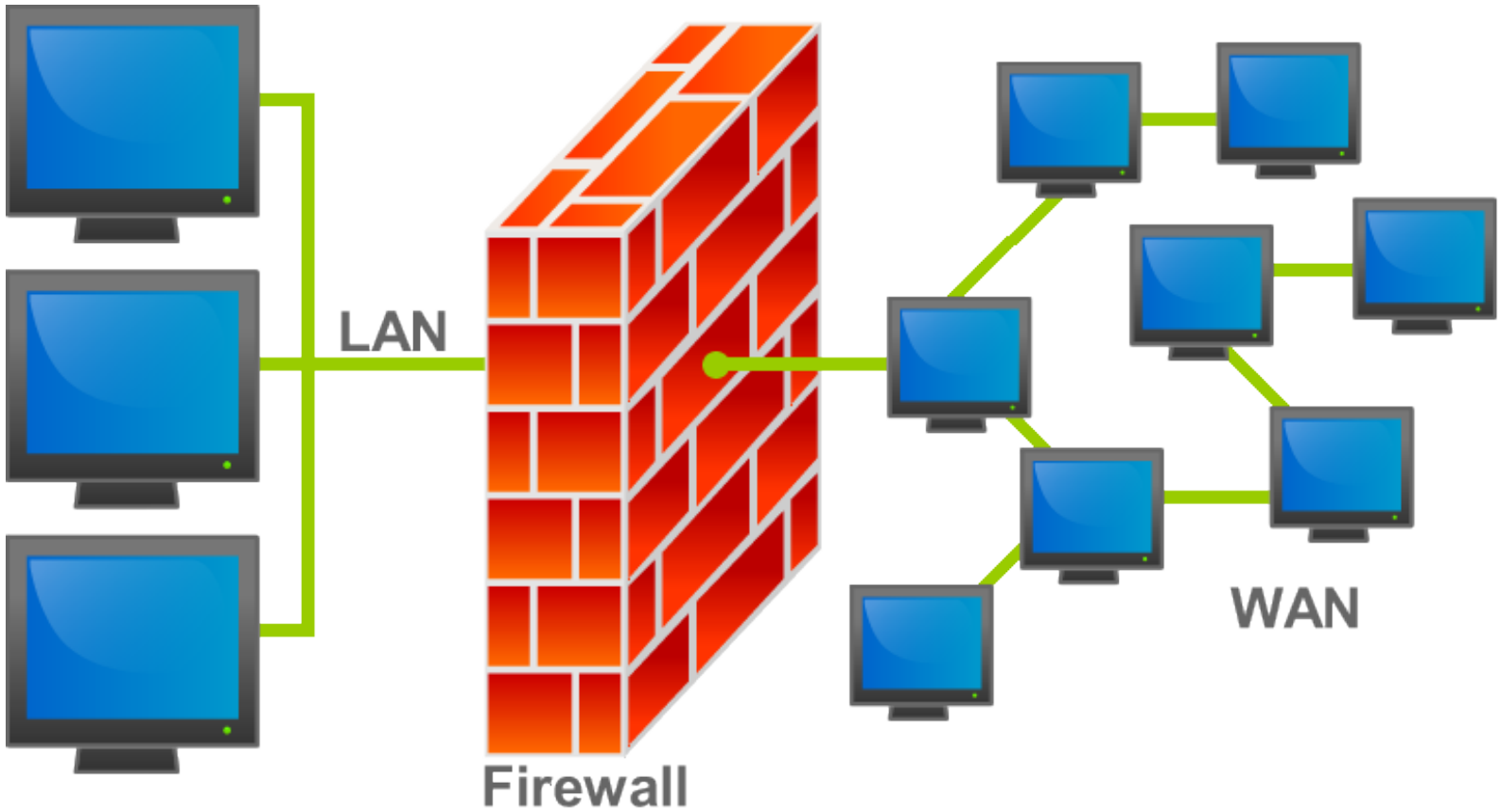
Example: Credit Cards

You might have the policy of not typing in your credit card online. Worthwhile or not?

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

No!

Example: Firewall



A firewall is a piece of software that controls incoming and outgoing traffic according to some rules.

Example: Firewall

- What assets are you trying to protect?

  Whatever is behind the firewall (credit cards, passwords, blueprints, ...)

Example: Firewall

- What assets are you trying to protect?
- What are the risks to these assets?

  With a small online shop you are already at risk. Pentagon, definitely.

Example: Firewall

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?

  Well, at home so not much. Everywhere else, if properly configurated then it does.

Example: Firewall

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?

  There might be backdoors or bugs in the firewall, but generally they are secure. You choose to prevent certain traffic.

Example: Firewall

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

  Minimal to modest. Firewalls are part of free software. You need a knowledgeable person to set them up.

Example: Firewall

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

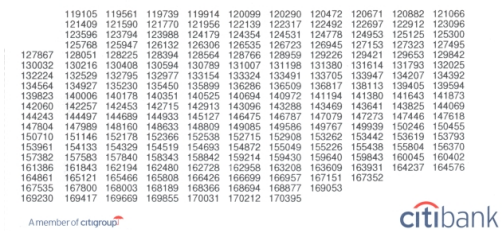
Example: Firewall

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

  Yes!

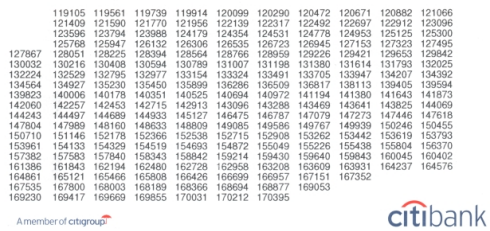
Ex: Two-Factor Authentication

Google uses nowadays two-factor authentication. But it is an old(er) idea. It is used for example in Germany and Netherlands for online transactions.



Ex: Two-Factor Authentication

Google uses nowadays two-factor authentication. But it is an old(er) idea. It is used for example in Germany and Netherlands for online transactions.



Or nowadays by SMS (restricts the validity of the numbers) or with a secure generator

Ex: Two-Factor Authentication

- What assets are you trying to protect?

  Your bank account.

Ex: Two-Factor Authentication

- What assets are you trying to protect?
- What are the risks to these assets?

  Nowadays pretty high risk.

Ex: Two-Factor Authentication

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?

  It prevents problems when passwords are stolen. Man-in-the-middle attacks still possible.

Ex: Two-Factor Authentication

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?

  Your mobile phone or creditcard/pin might be stolen. SIM card become valuable.

Ex: Two-Factor Authentication

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

  Banks need to establish an infrastructure.

  For you it might be inconvenient.

Ex: Two-Factor Authentication

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

Ex: Two-Factor Authentication

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

  Yes!

Security Seals

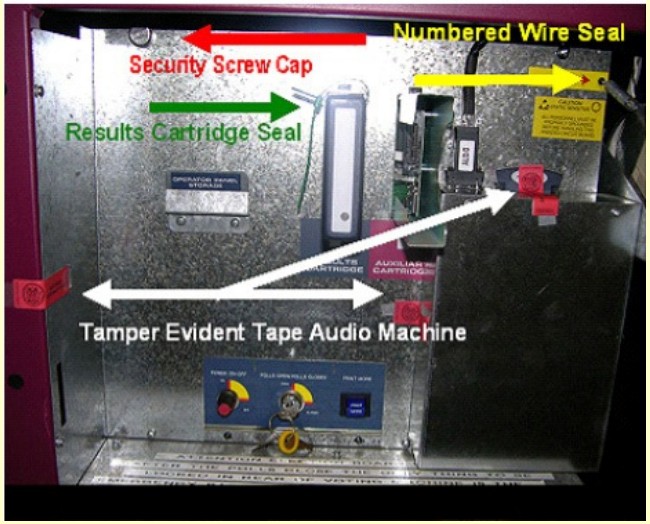
According to Ross Anderson: "... is a tamper-indicating device designed to leave non-erasable, unambiguous evidence of unauthorized entry or tampering."

They also need some quite sophisticated policies (seal regiment).

Security Seals (2)

- at the Argonne National Laboratory they tested 244 different security seals (including 19% that were used for safeguard of nuclear material)
  - mean time to break the seals for a trained person: 100 s
- Andrew Appel defeated all security seals which were supposed to keep voting machines safe.

Security Seals (2)



- The tamper-indicating tape can be lifted using a heat gun.
- The security screw cap can be removed using a screwdriver, then the serial-numbered top can be replaced (undamaged) onto a fresh (unnumbered) base.
- The wire seal can be defeated using a #4 wood screw.
- The plastic strap seal can be picked using a jeweler's screwdriver.

Ex: Security Seals

- What assets are you trying to protect?

  Voting machines, doors.

Ex: Security Seals

- What assets are you trying to protect?
- What are the risks to these assets?

  Casual thiefs, insider attacks.

Ex: Security Seals

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?

  Needs a quite complicated security regiment.

Ex: Security Seals

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?

  You might not notice tampering.

Ex: Security Seals

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

  The "hardware" is cheap, but indirect costs can be quite high.

Ex: Security Seals

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

Ex: Security Seals

- What assets are you trying to protect?
- What are the risks to these assets?
- How well does the security solution mitigate those risks?
- What other risks does the security solution cause?
- What costs and trade-offs does the security solution impose?

  No! Though in some areas they work: airport.