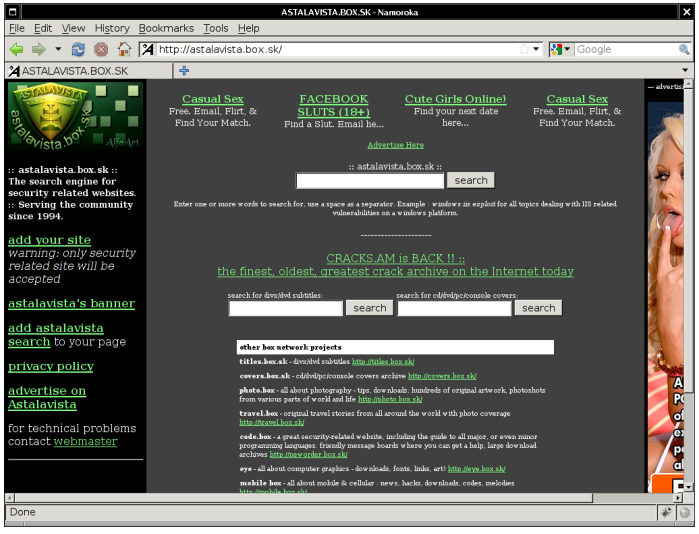
Security when applications become web sites

Andrea Bittau, Arti Gupta, and David Mazières

April 30, 2010

Web and apps perceived differently

- Users know software can do bad things.
- Conservative: only install “trusted” software.



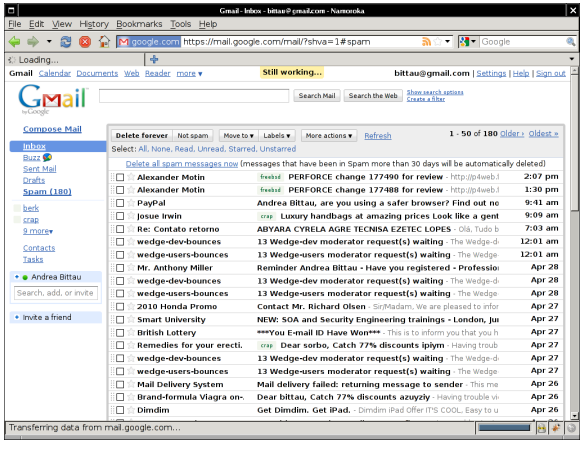
- Users believe web sites cannot do “bad” things to system.
- Liberal about visiting dubious web sites.

Web and apps converging

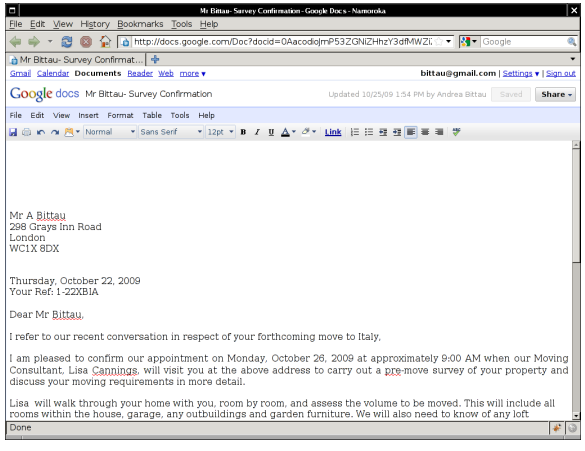
The Web's evolution: rich apps (*e.g.*, Gmail, games)

- Ever increasing functionality and performance demand.
- Security problems will only get worse.

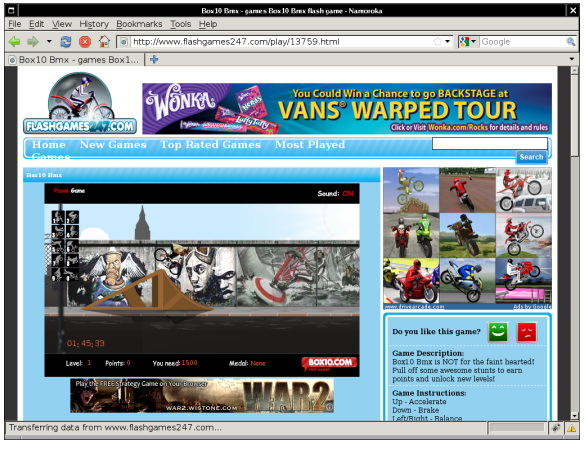
Browser becoming platform for running applications



Gmail



Google Docs

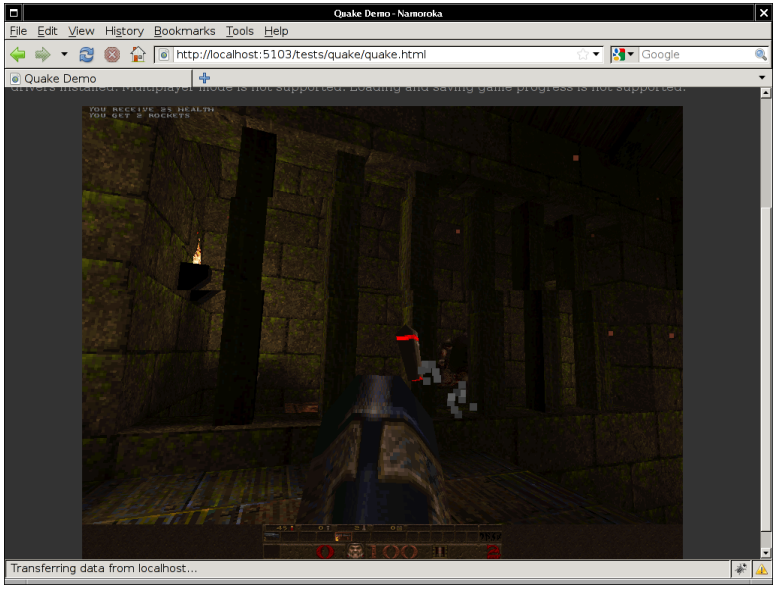


Flash game

NaCl: run x86 in browser

Google Native Client—run x86 code in browser:

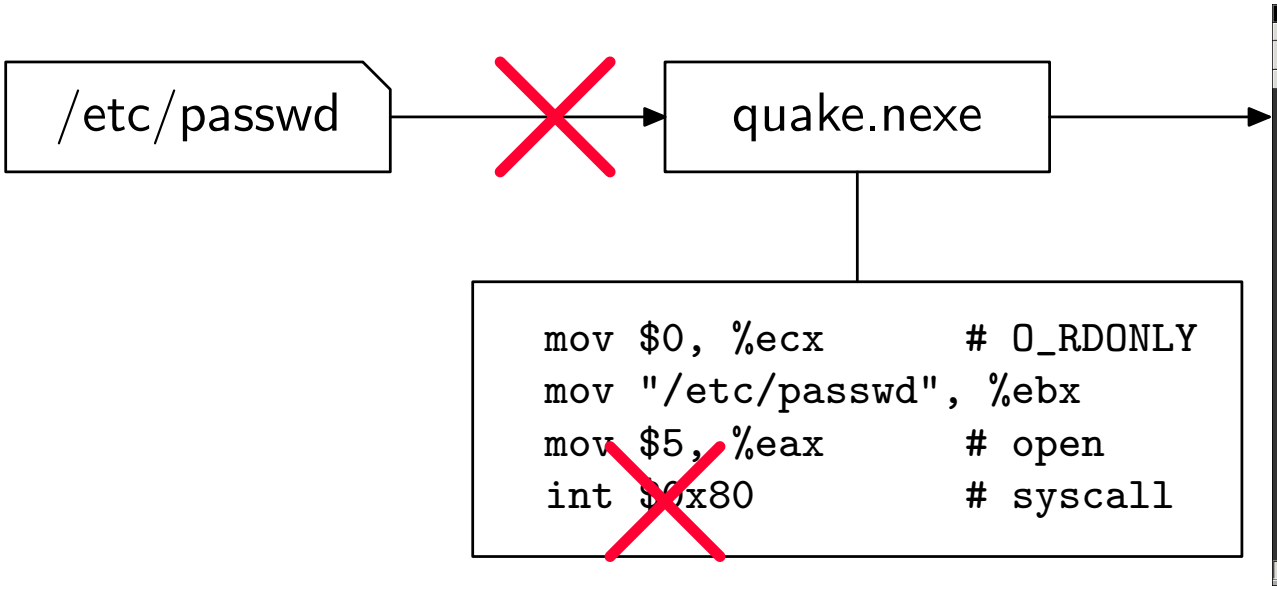
- High performance.
- Easy porting of legacy code.

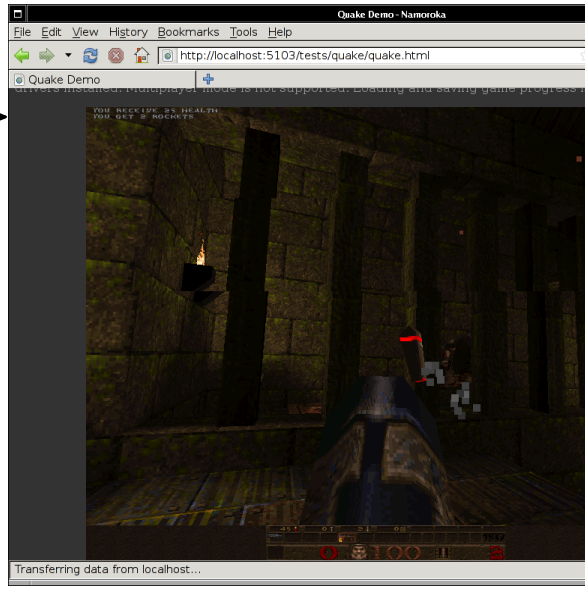


Quake
91,582 LoC

NaCl: run x86 in browser, securely

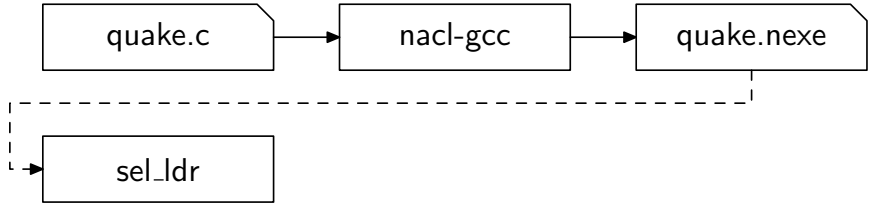
Problem: how to sandbox x86 code?





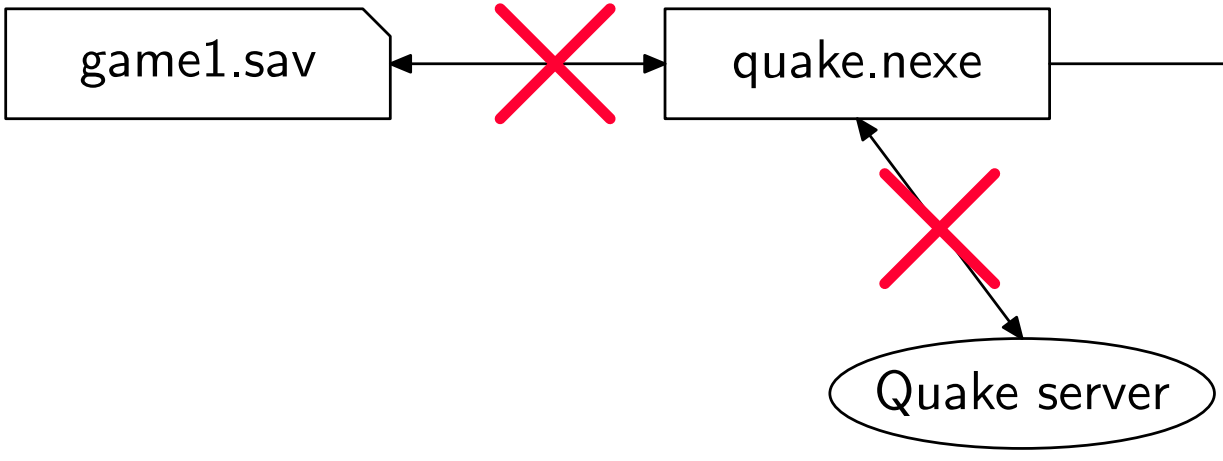
Solution:

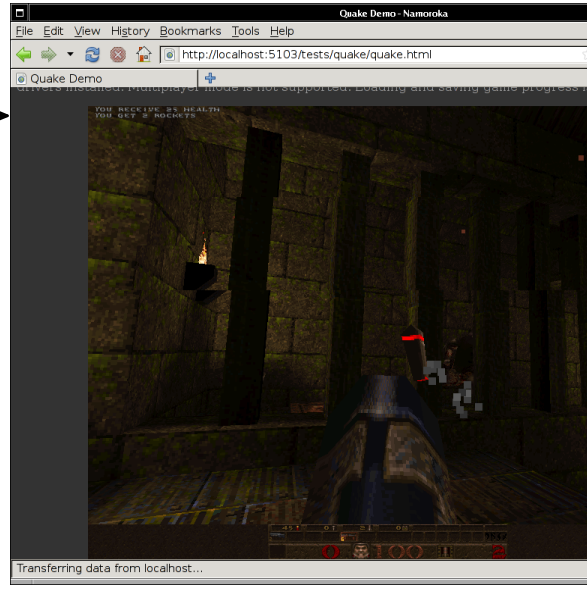
1. Compile code to verifiable form.
2. Verify code prior to launch.



Our work: add syscalls, securely

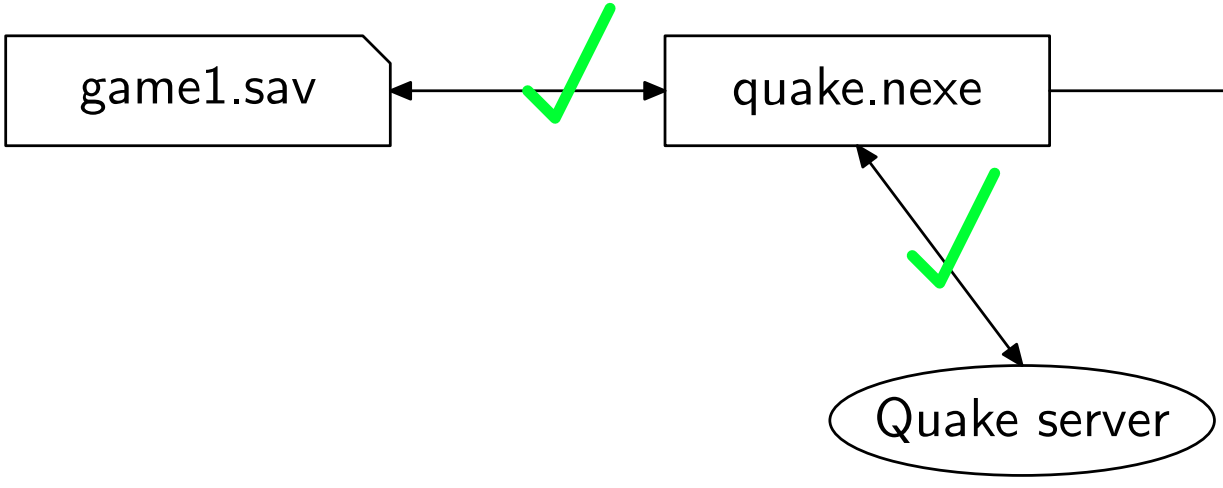
Problem: how to securely allow syscalls?

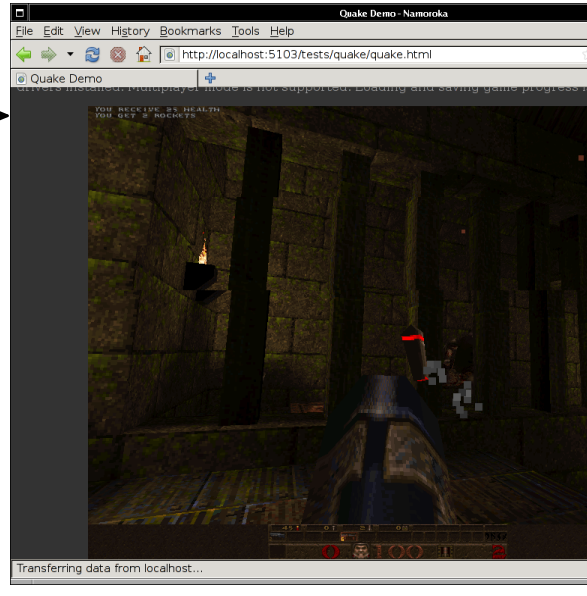




Our work: add syscalls, securely

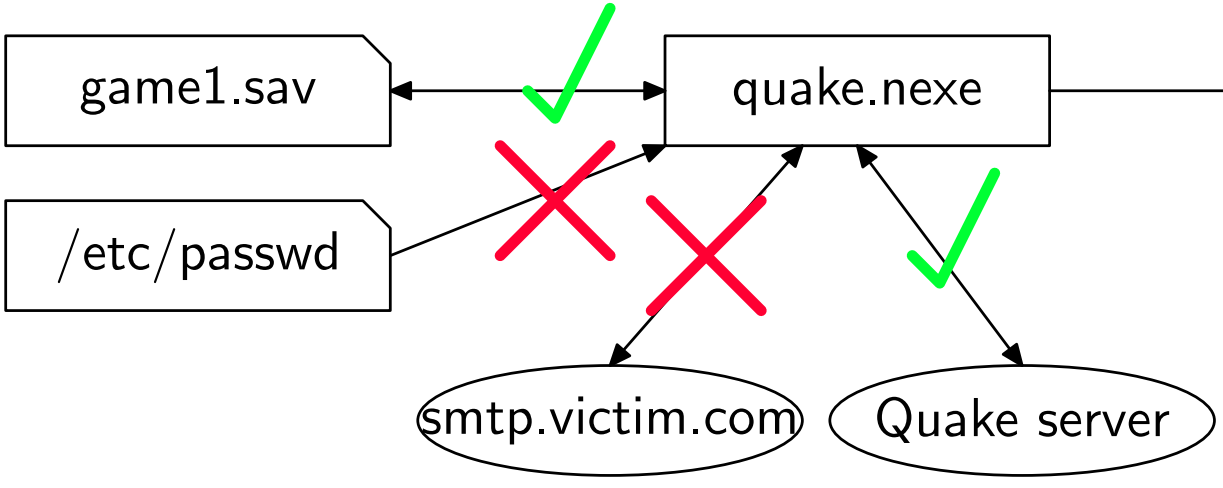
Problem: how to securely allow syscalls?

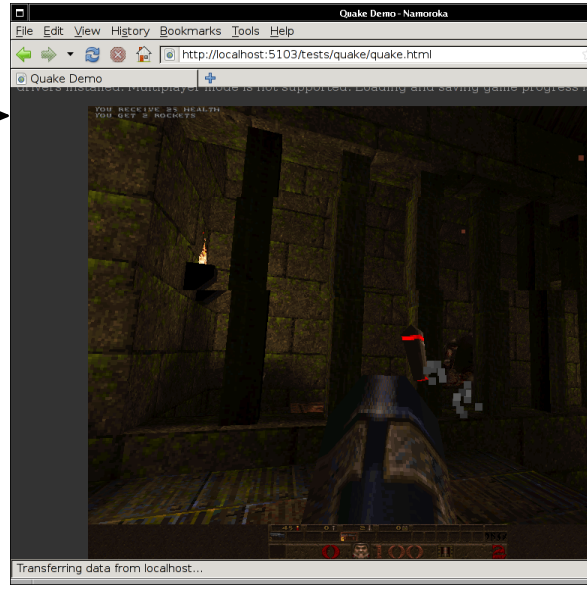




Our work: add syscalls, securely

Problem: how to securely allow syscalls?



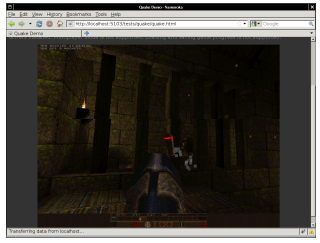


Challenge: figure out policy and enforce it

Motivating examples

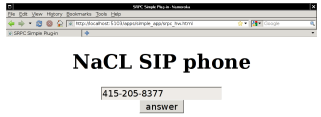
Quake

- Online gaming.



VOIP client

- Live support while shopping online.



Peer-to-peer streaming video player

- No need for server bandwidth.

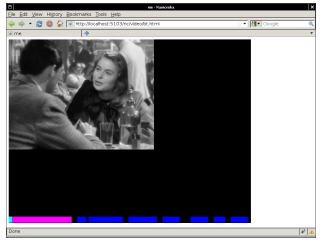
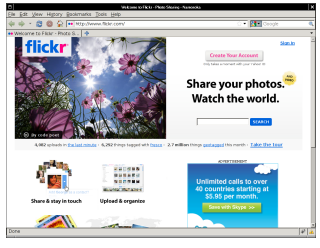


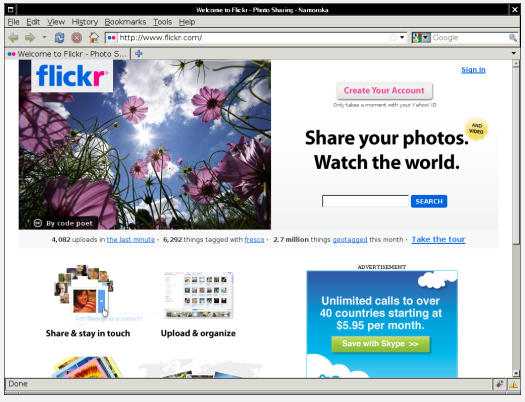
Photo editor and publisher

- No need for server CPU expense.

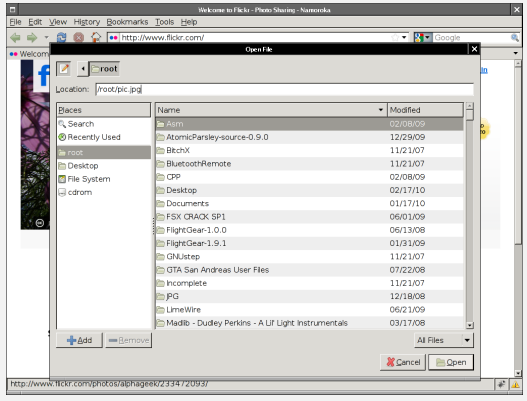


Example: Hypothetical Flickr

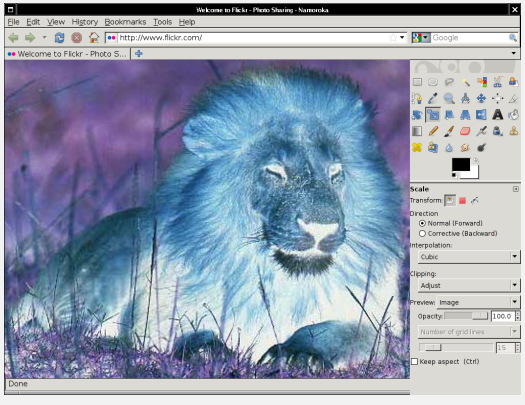
1. Visit Flickr's NaCl web site



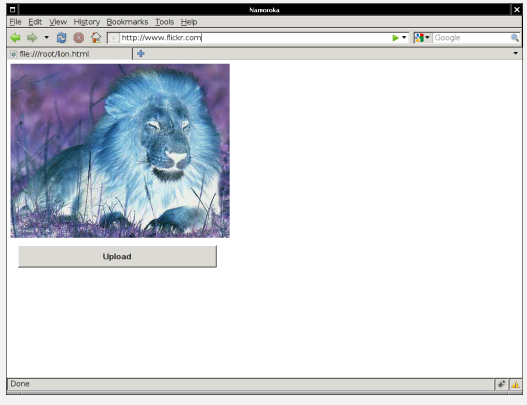
2. Choose file to upload



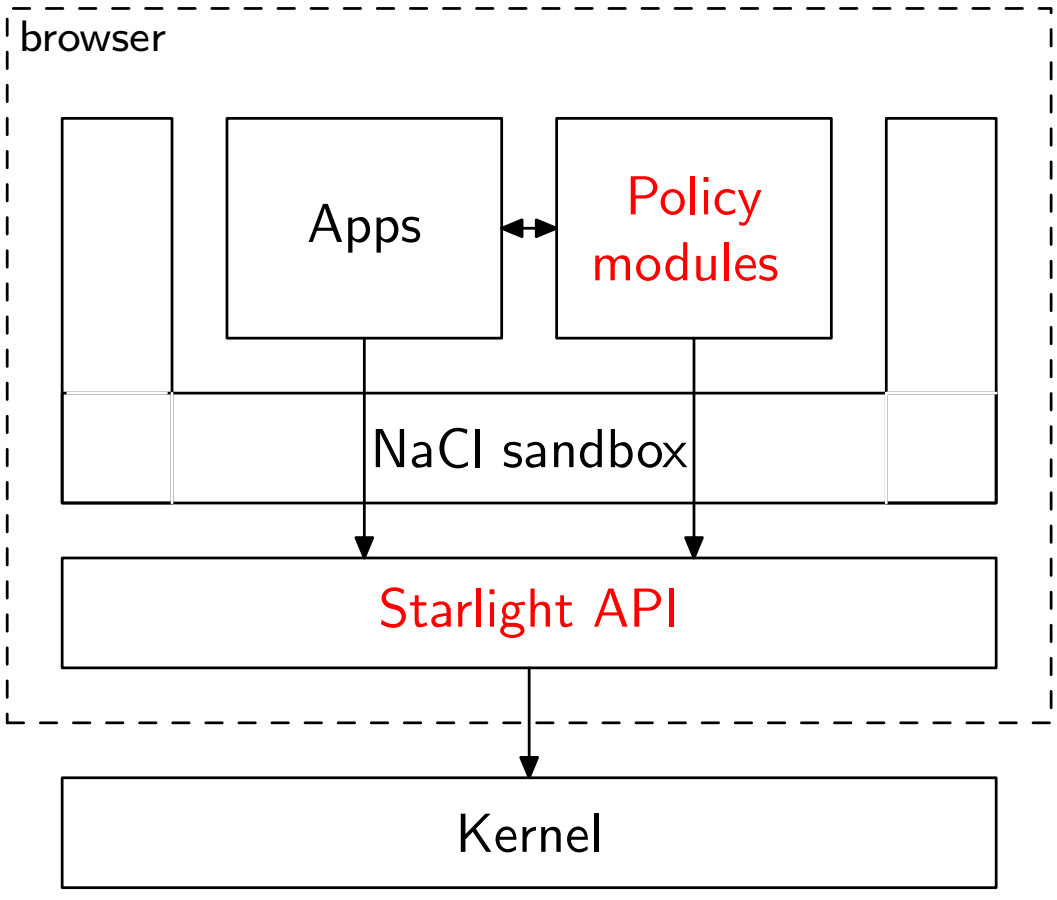
3. Edit picture



4. Upload!

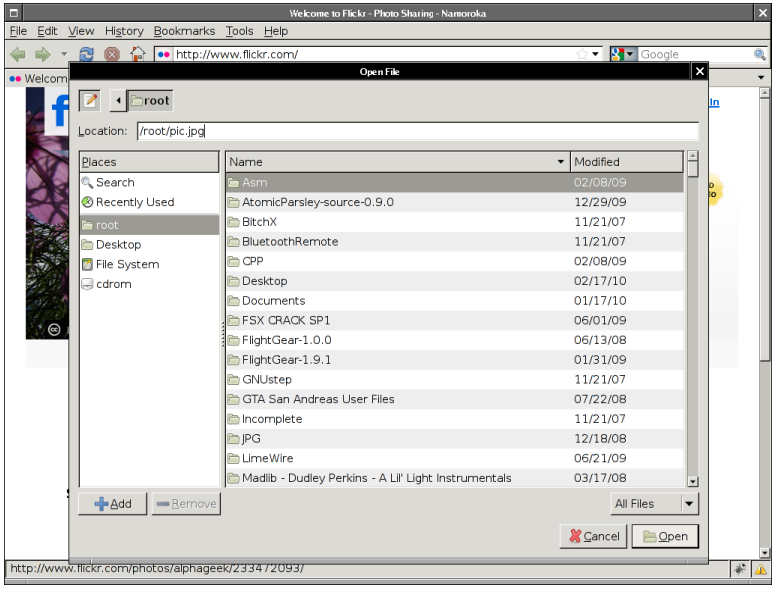


Architecture



User actions specify user's intent

Security: carry out user intentions and nothing more.

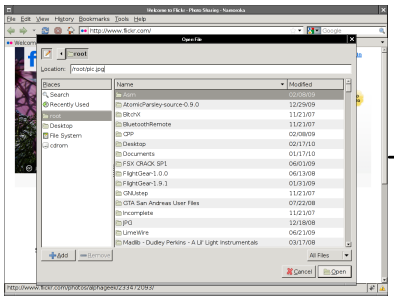


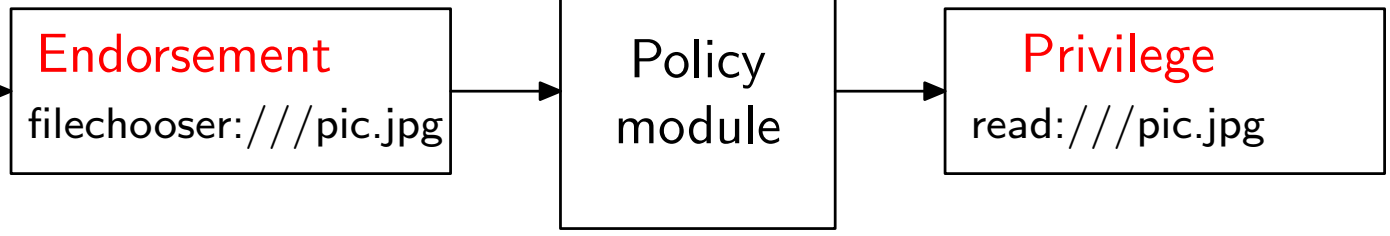
- User wants to open pic.jpg
- User expects app will read pic.jpg

User action: select pic.jpg via file chooser.

User actions grant privileges

Give applications privileges based on user actions [Karp06]





User action	Example of possible capability granted
File chooser	Read file
Textbox	Allow connection to host
Link text	Allow connection to peers specified in torrent file obtained from link
Button	Allow microphone access

Policy modules: generic and small (*e.g.*, bittorrent 100 LoC)

Trusted UI gives user action proof

Code

```
add_trusted(TEXTBOX, "SMTP server");
```

User interface displayed

SMTP server | smtp.com

Endorsements (→ privileges)

textbox://SMTP server/smtp.com → tcp://smtp.com:25

Trusted UI gives user action proof

Code

```
add_trusted(TEXTBOX, "SMTP server");
add_trusted(TEXTBOX, "Type warez.com to continue");
```

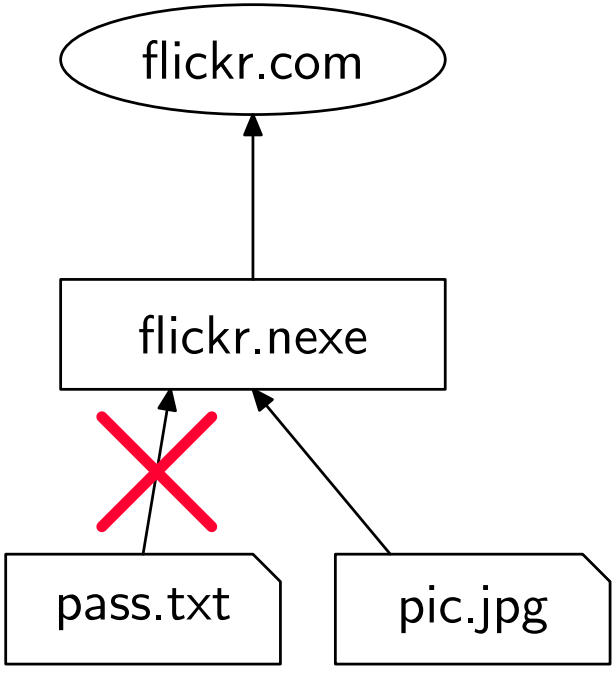
User interface displayed

SMTP server	smtp.com
Type warez.com to continue	warez.com

Endorsements (→ privileges)

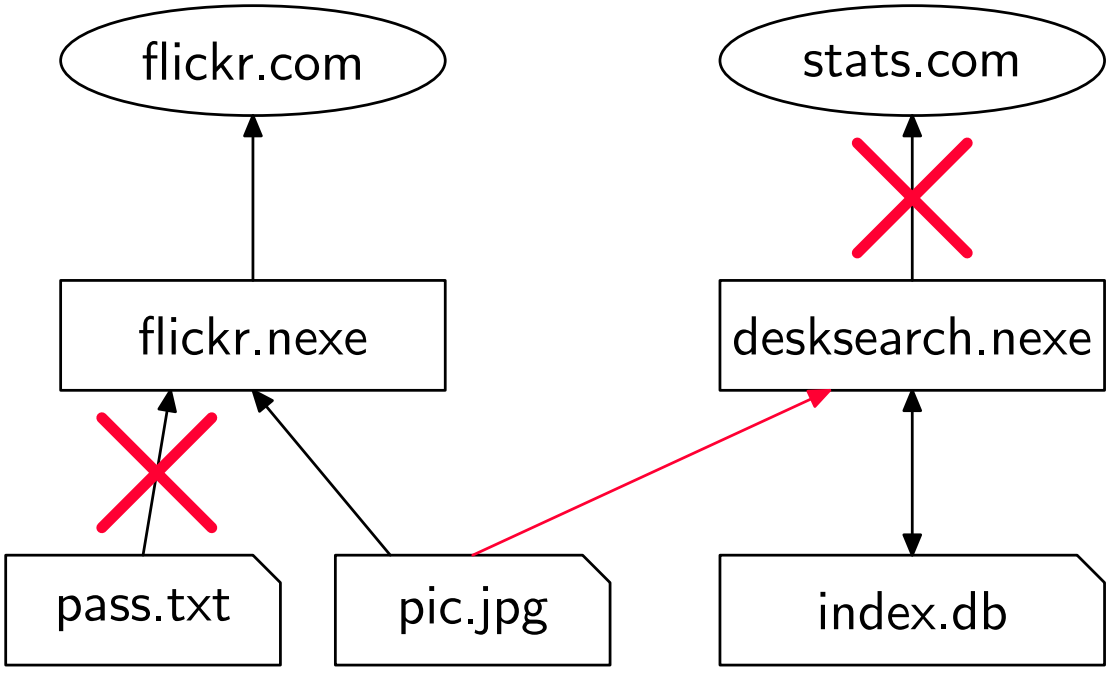
textbox://SMTP server/smtp.com → tcp://smtp.com:25
textbox://Type warez.com to continue/warez.com

Allow controlled sharing using IFC



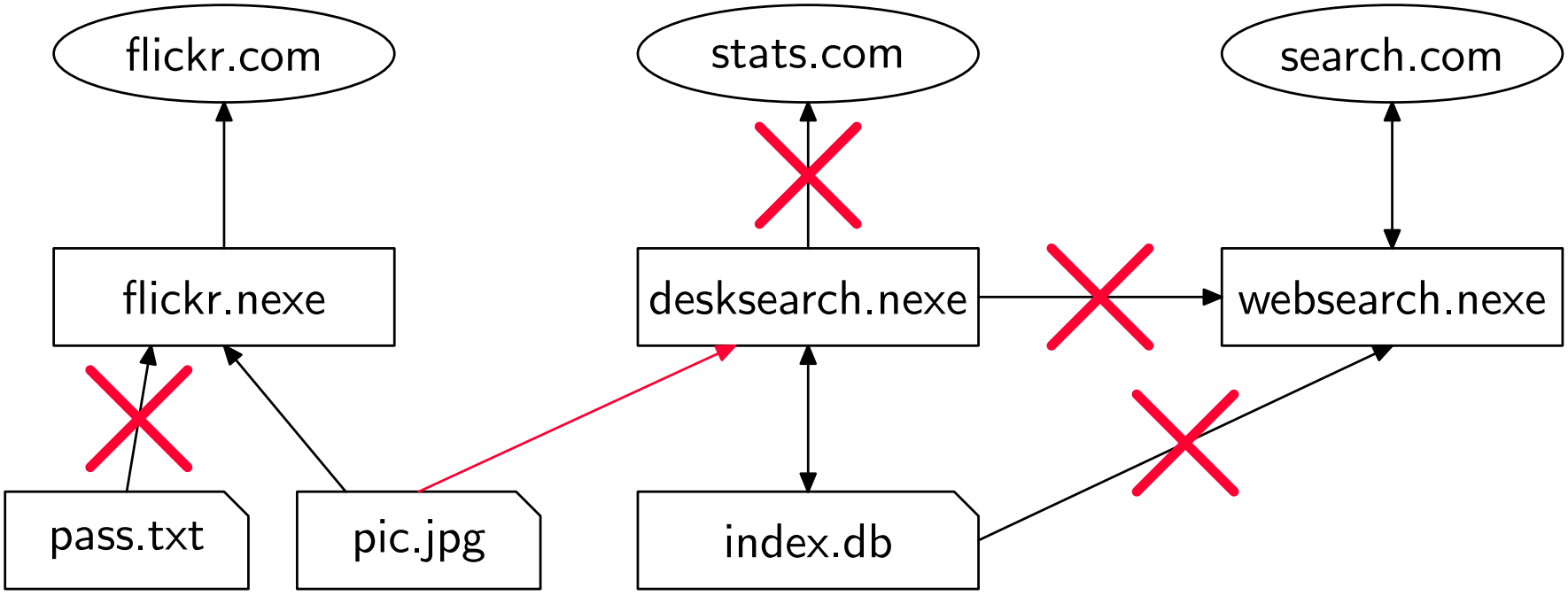
Allow controlled sharing using IFC

How to allow sharing data, and avoid exfiltration?



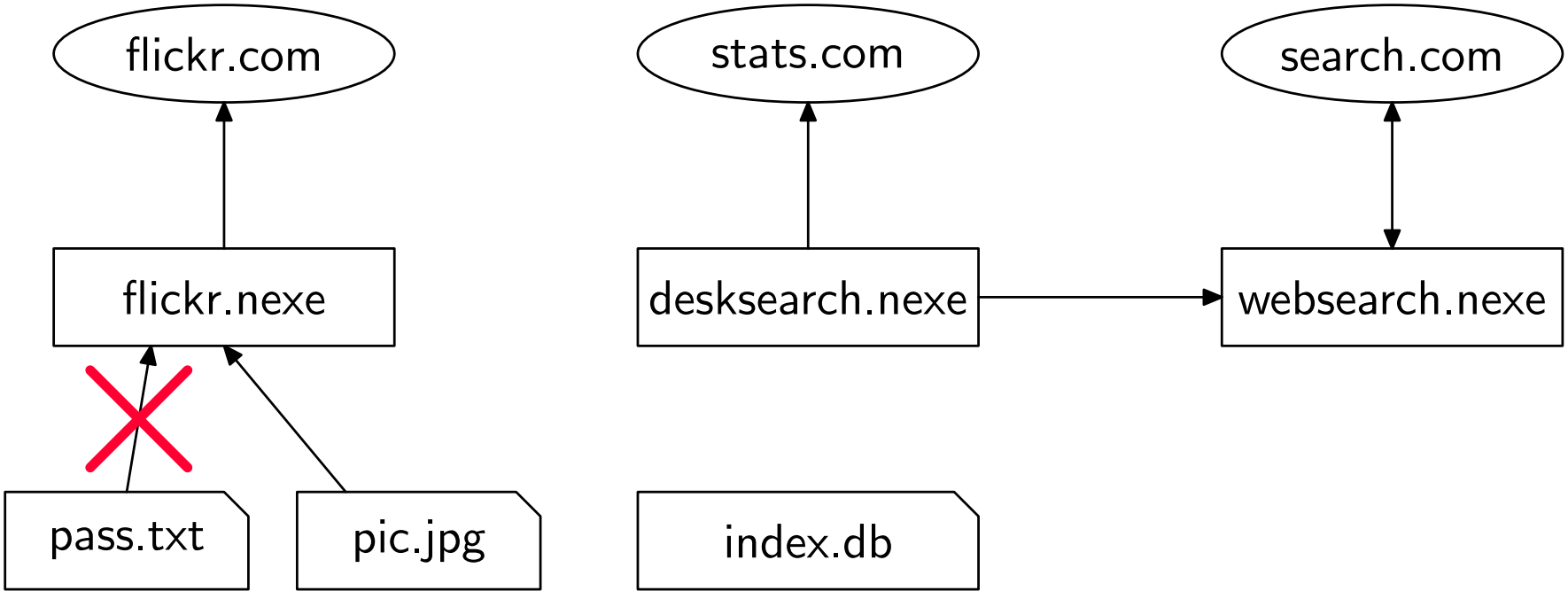
Allow controlled sharing using IFC

How to allow sharing data, and avoid exfiltration?



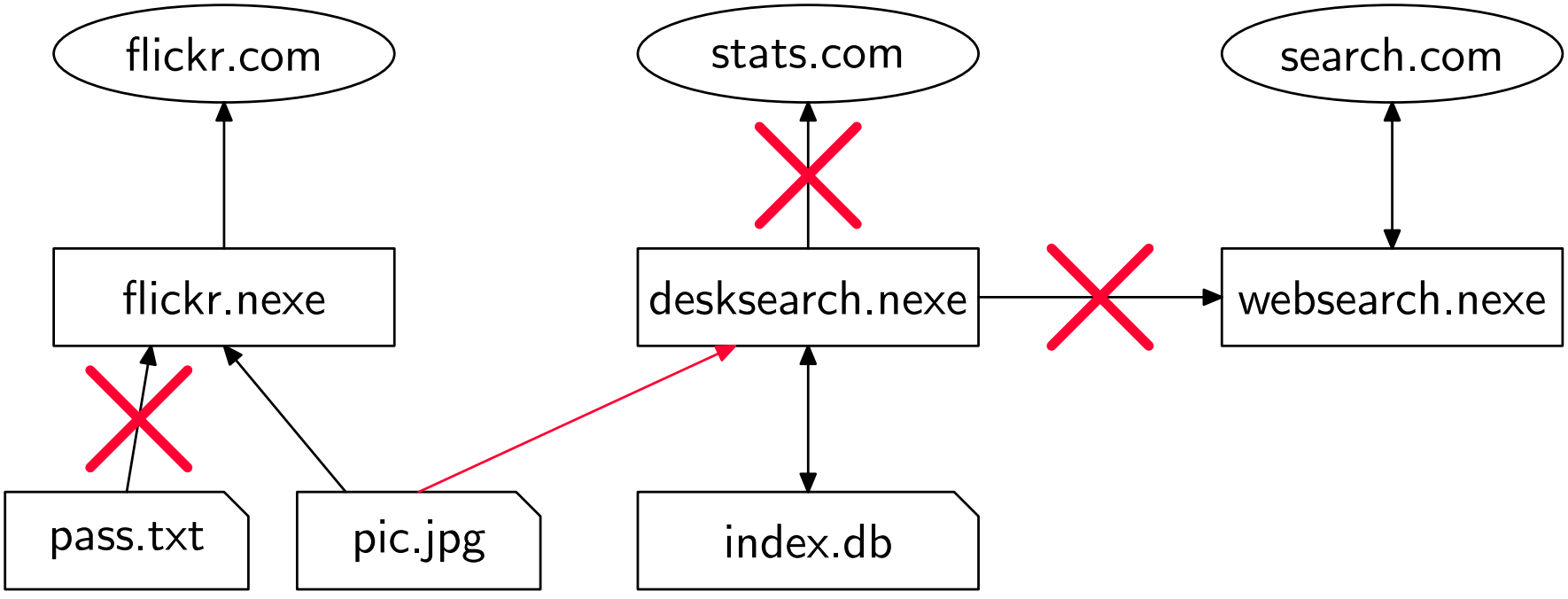
Allow controlled sharing using IFC

How to allow sharing data, and avoid exfiltration?



Allow controlled sharing using IFC

How to allow sharing data, and avoid exfiltration?

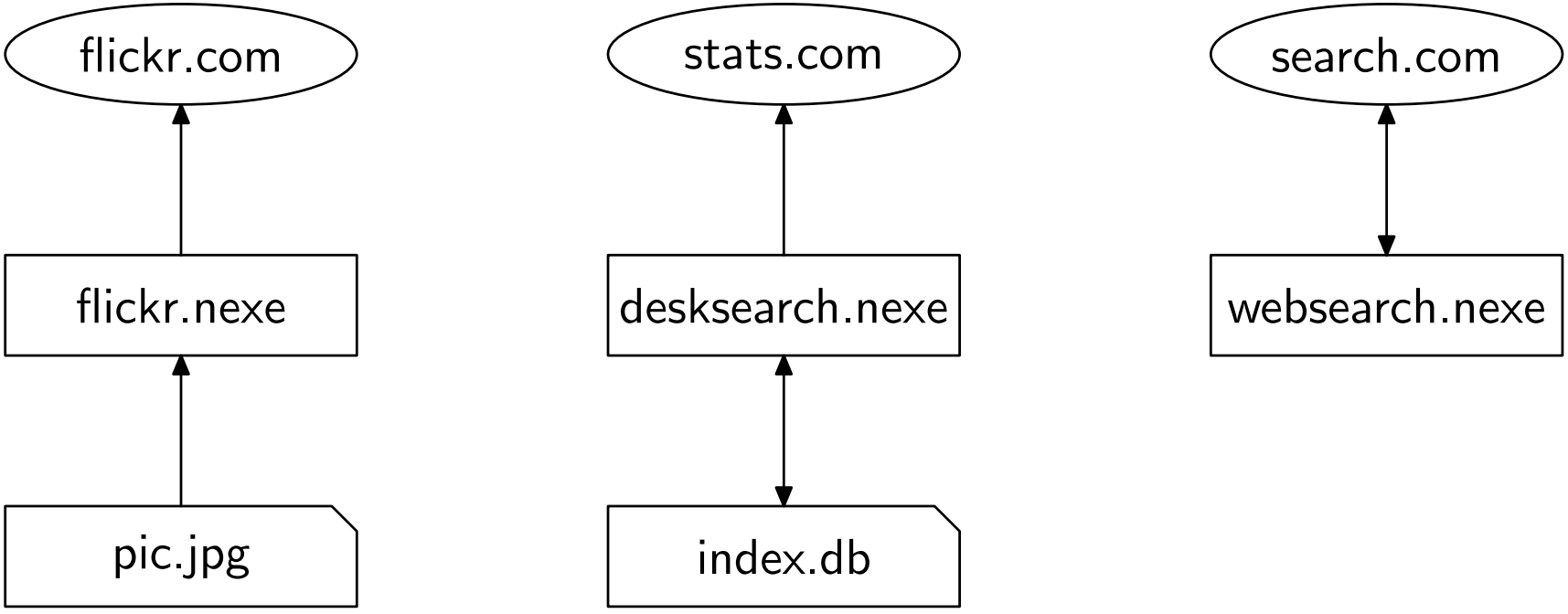


Need Information Flow Control (IFC).

Track data and control export

To prevent data disclosure:

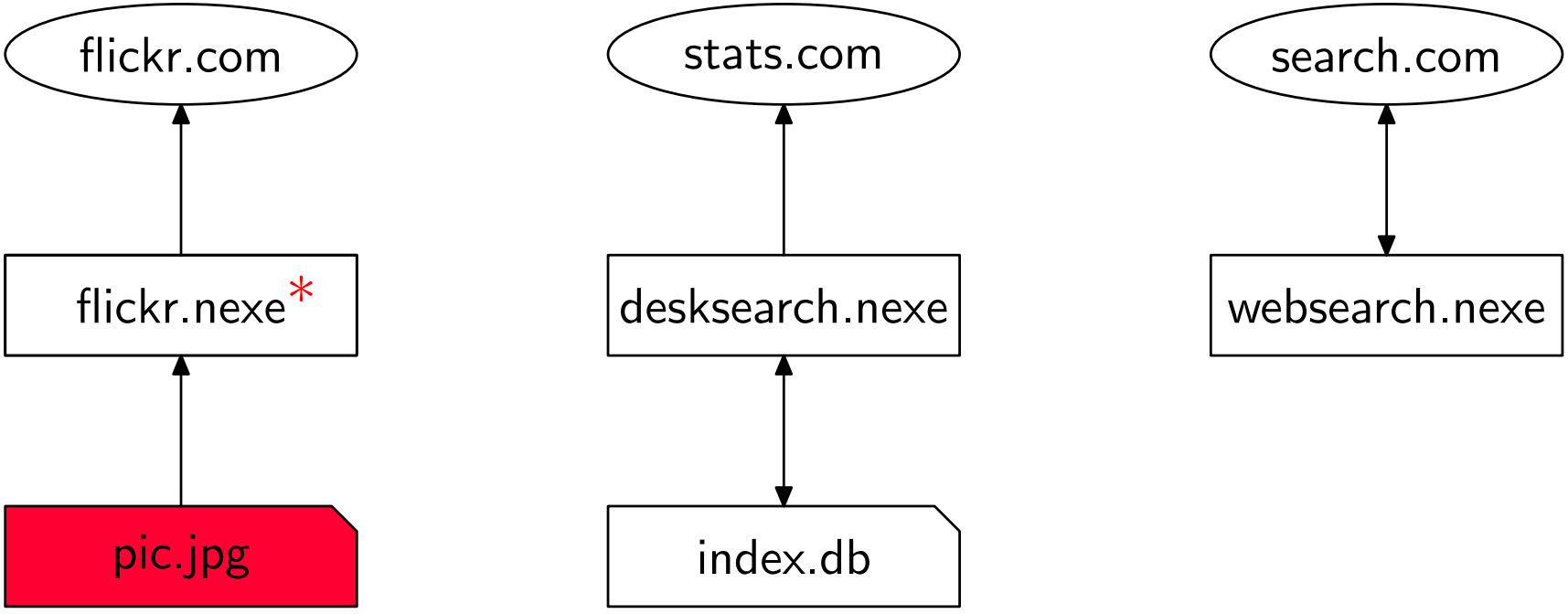
1. Label data.
2. Taint processes that hold labeled data.
3. Deny tainted processes from talking to network.



Track data and control export

To prevent data disclosure:

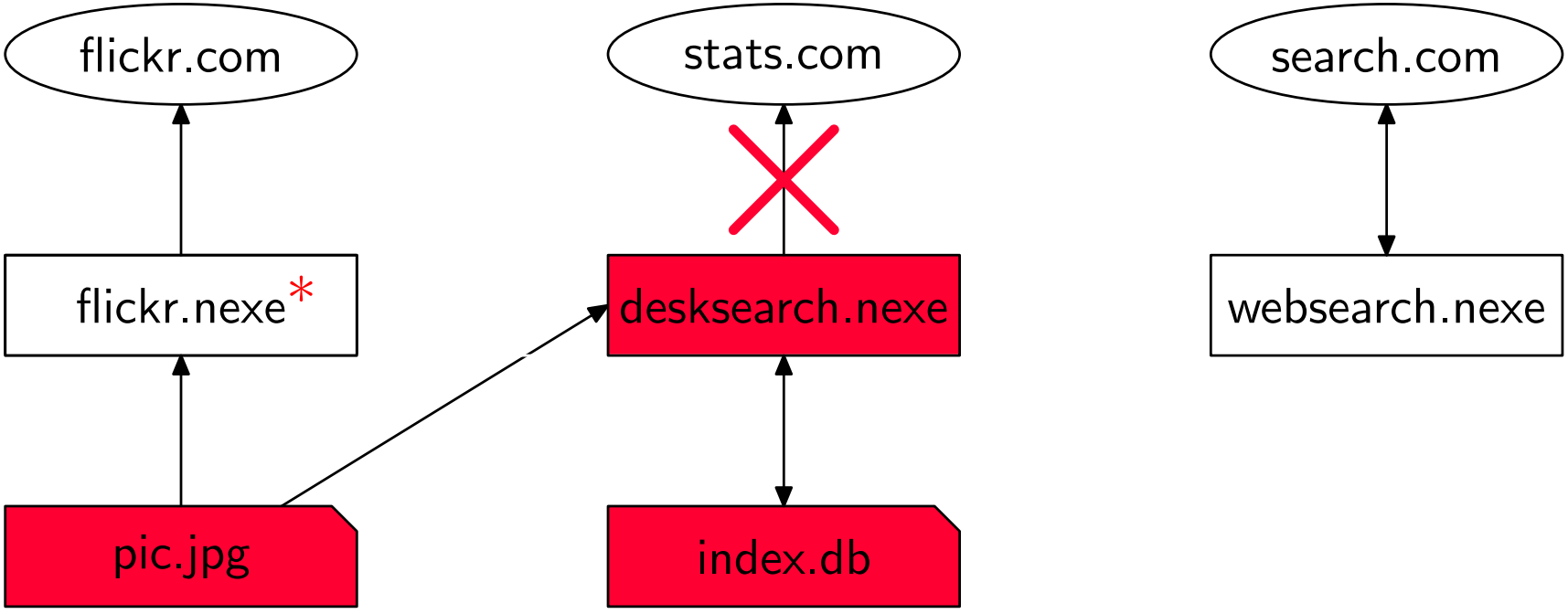
1. Label data.
2. Taint processes that hold labeled data.
3. Deny tainted processes from talking to network.



Track data and control export

To prevent data disclosure:

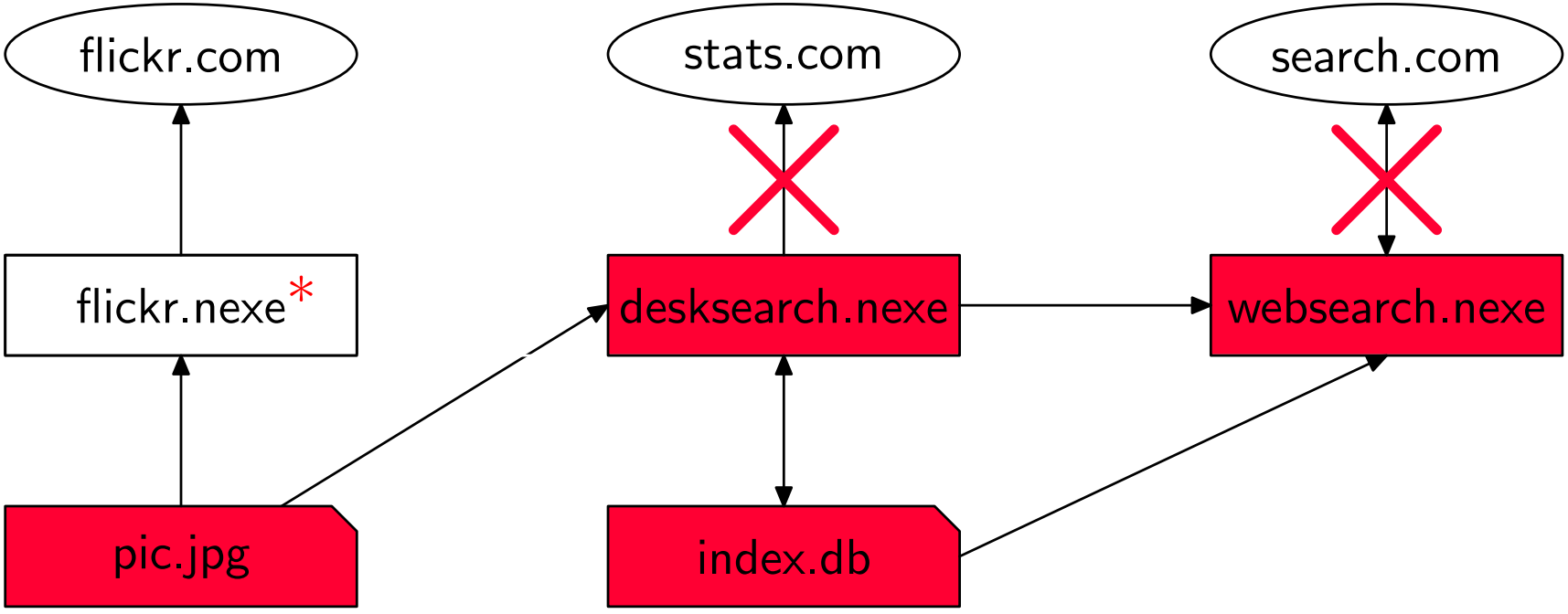
1. Label data.
2. Taint processes that hold labeled data.
3. Deny tainted processes from talking to network.



Track data and control export

To prevent data disclosure:

1. Label data.
2. Taint processes that hold labeled data.
3. Deny tainted processes from talking to network.

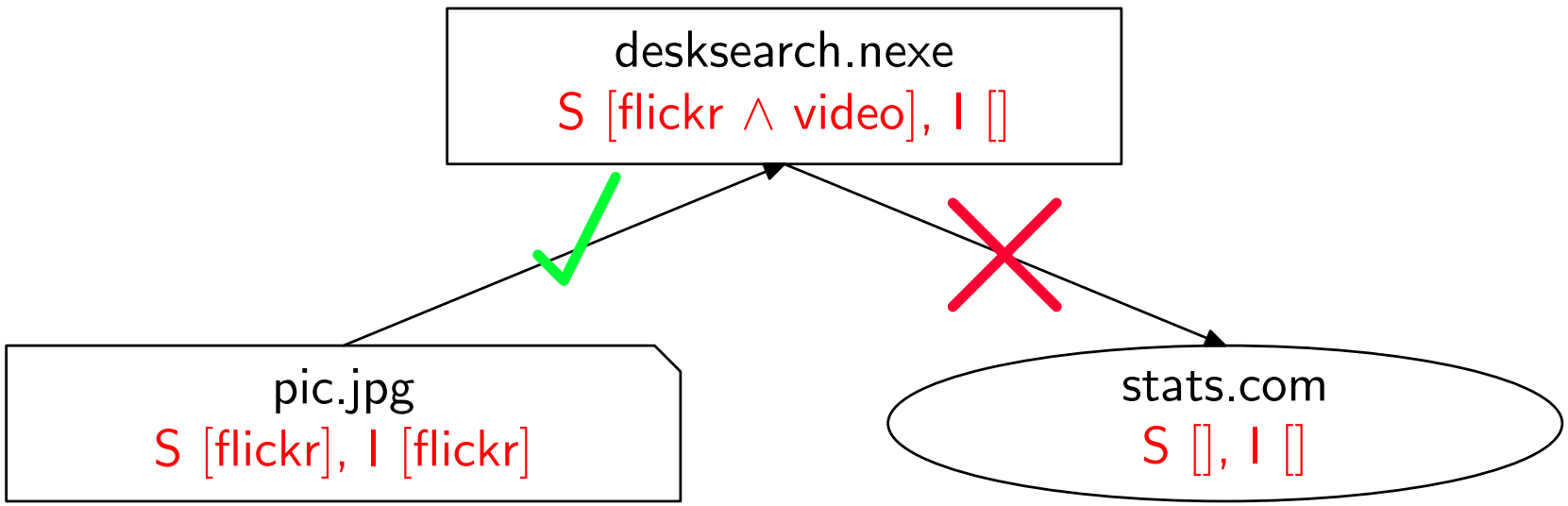


Labels control information flow

- Red on previous slide represents a category of taint.

Category An arbitrary string, *e.g.*, "secret".

Label A set of integrity and secrecy categories.



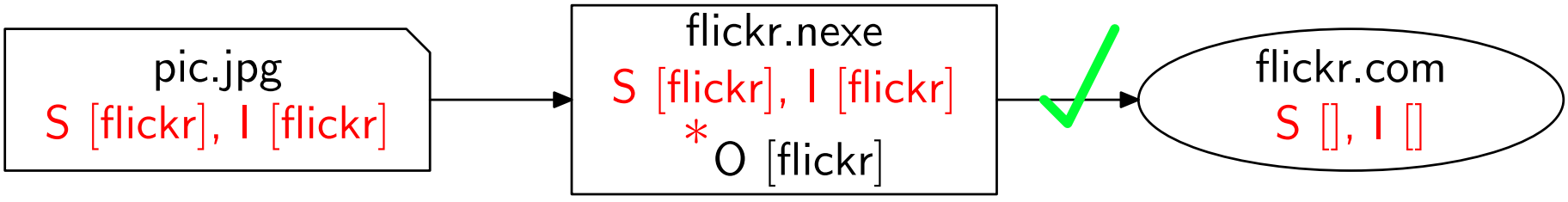
Information can flow from x to y if:

- Secrecy categories of $x \subset y$.
- Integrity categories of $y \subset x$.

Category owners control data export

Category owners can export data.

- They can remove owned categories from their label.



NaCl applications own the following categories:

Category	Allows sharing between
HTTP origin	Applications in same page
Hash of app binary	Instances of same application
Certificate that signed app	Applications from same vendor

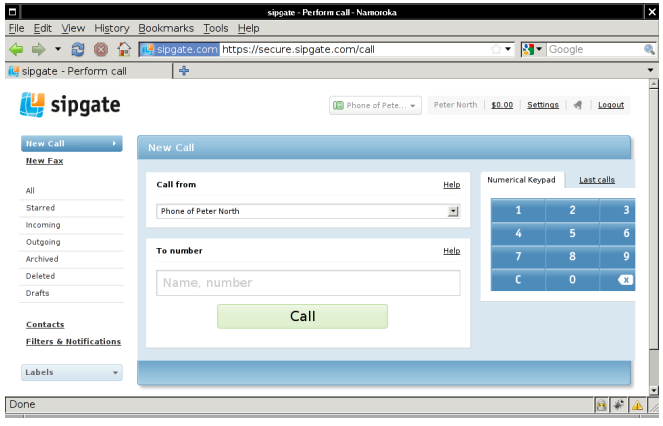
Telephoning from your browser

Make and receive calls from your browser:

- Live phone support while shopping online.
- Sales callbacks.

NaCl benefits:

- Can reuse SIP libraries: 347,501 LoC.
- Need performance for audio codecs.



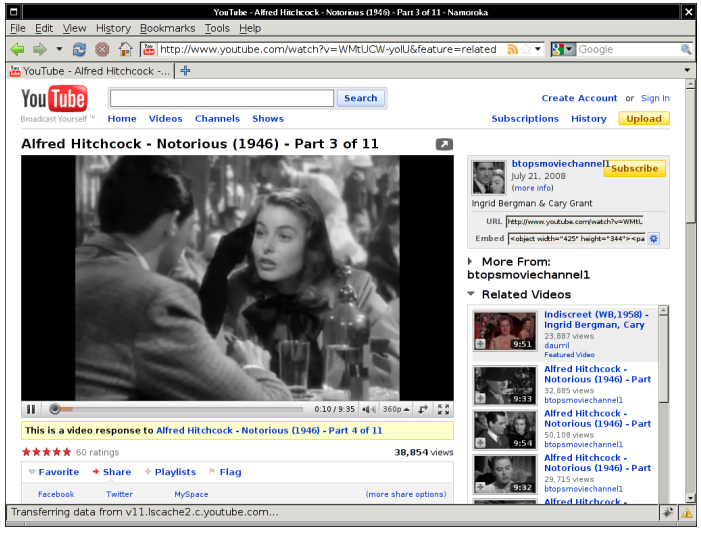
Client-based video streaming

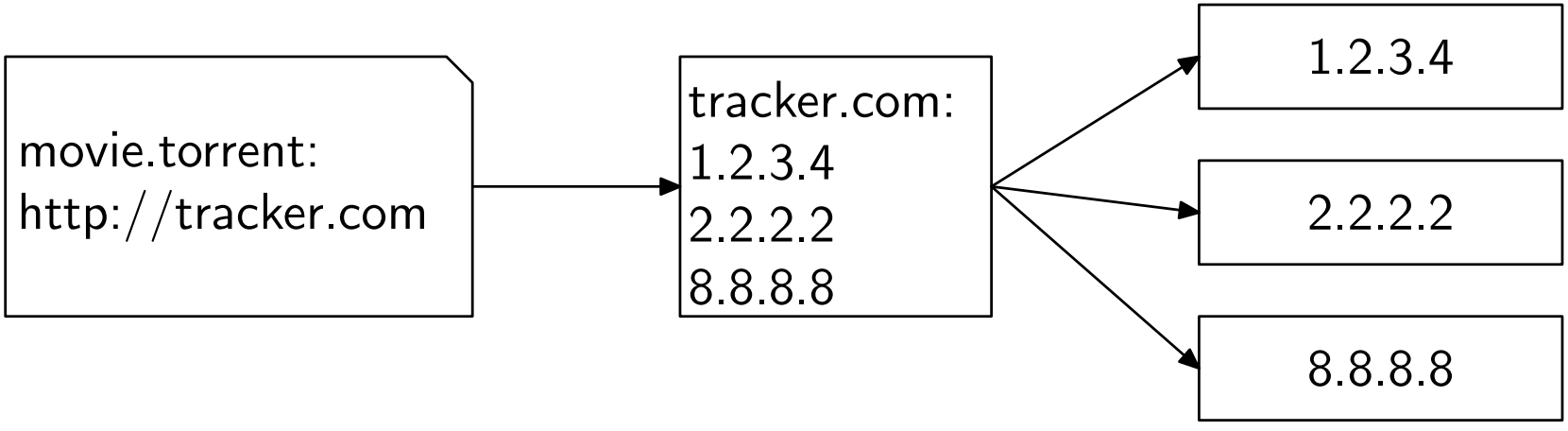
Watch and stream videos using bittorrent.

- No need for server bandwidth.
- High performance for video codecs.

Security requirements:

- Restrict network traffic to bittorrent peers.
- Restrict disk access to bittorrent files.

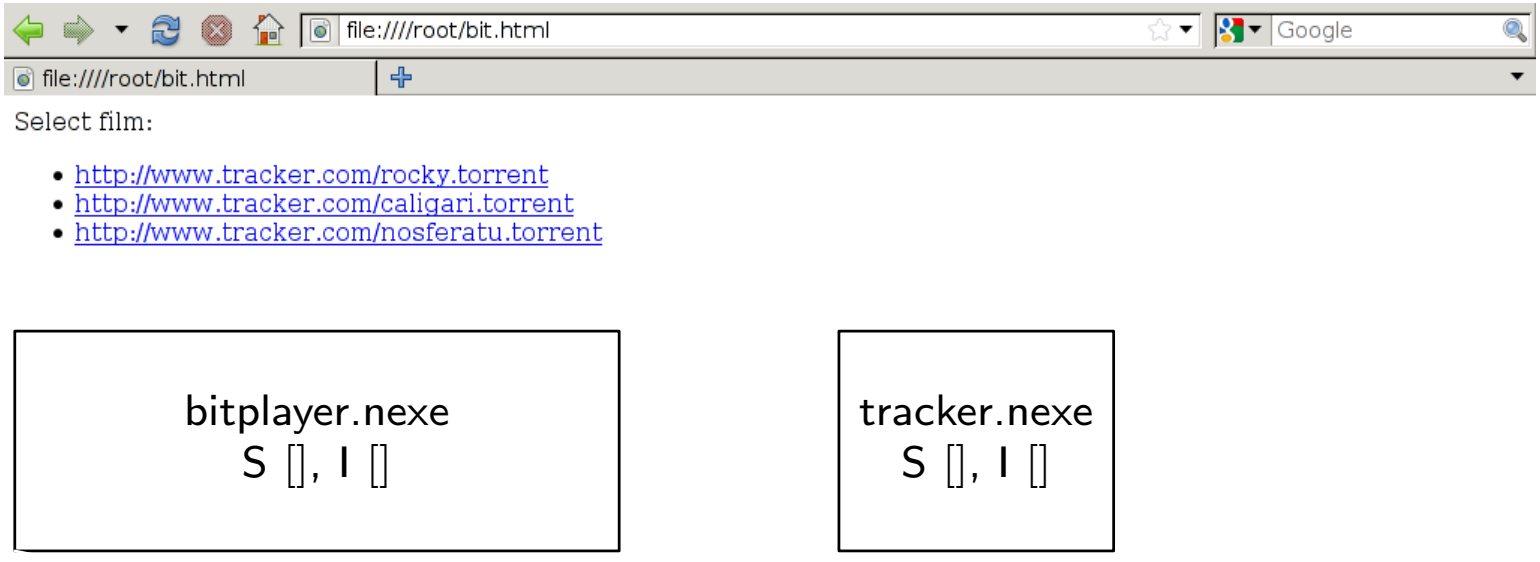




NaCl bittaurent player

Policy module tracker.nexe (100 LoC; *cf.* 327,000 untrusted):

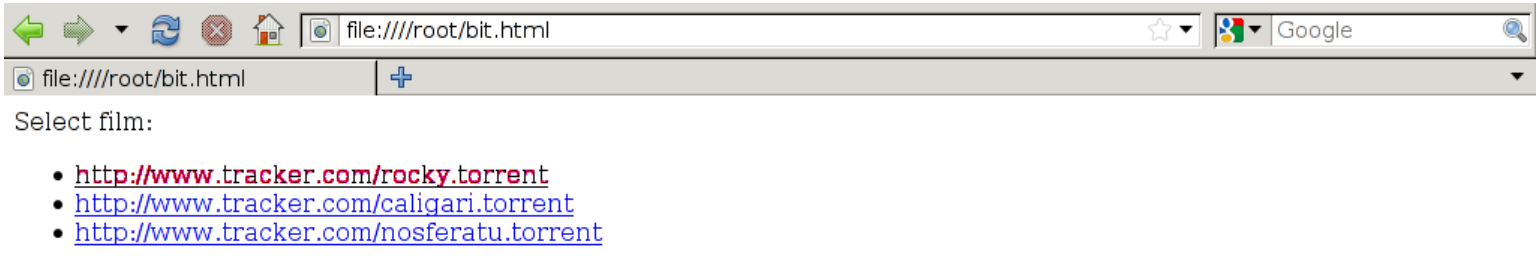
- Connects only to trackers authorized by user.
- Grants privileges only for IPs returned by tracker.

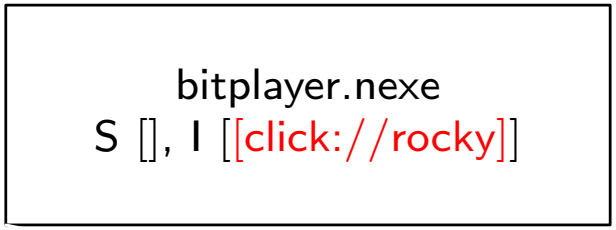


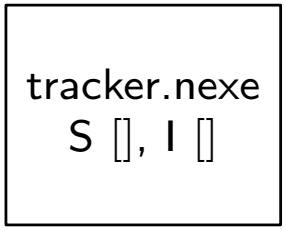
NaCl bittaurent player

Policy module tracker.nexe (100 LoC; *cf.* 327,000 untrusted):

- Connects only to trackers authorized by user.
- Grants privileges only for IPs returned by tracker.



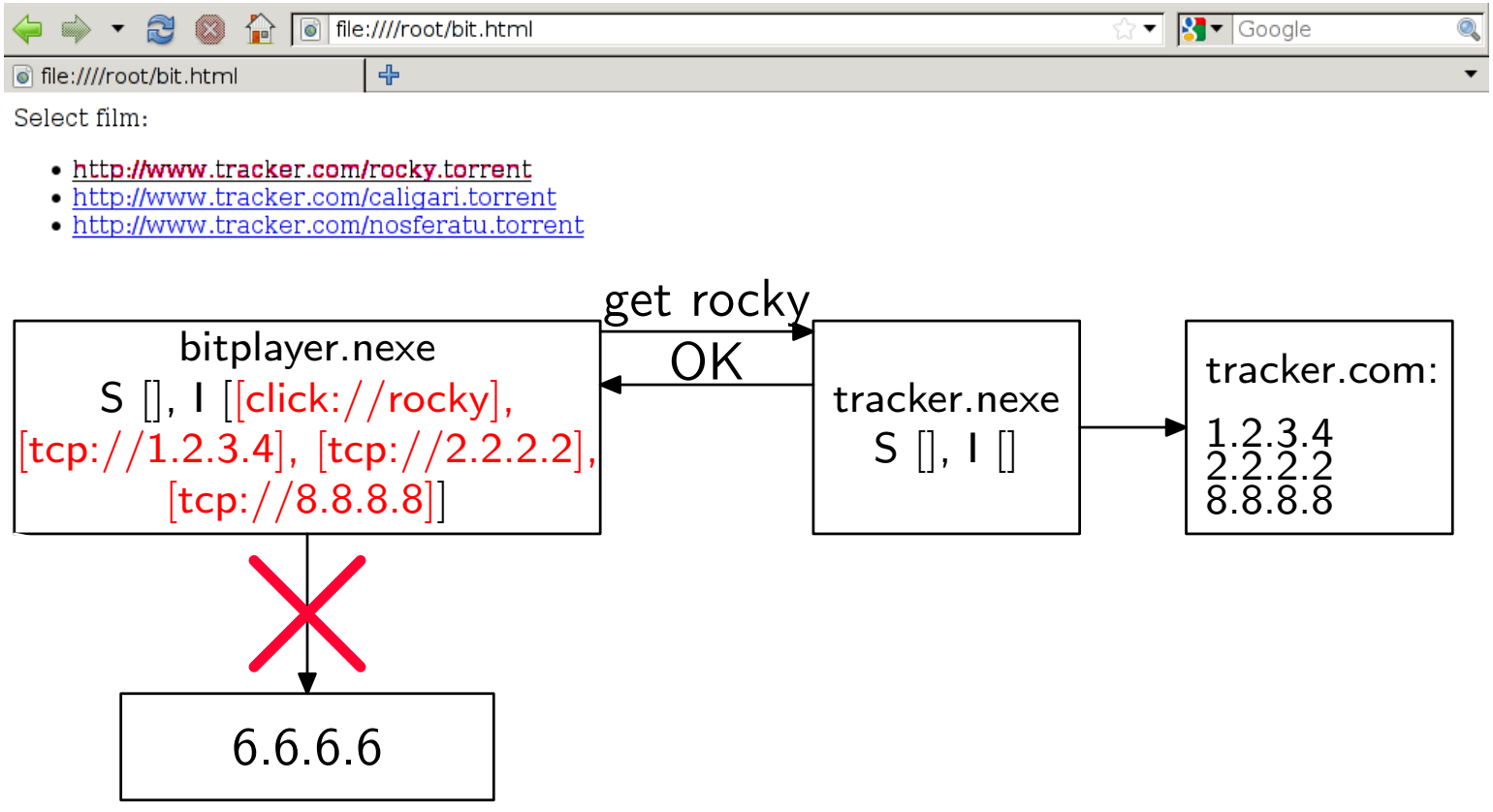




NaCl bittaurent player

Policy module tracker.nexe (100 LoC; *cf.* 327,000 untrusted):

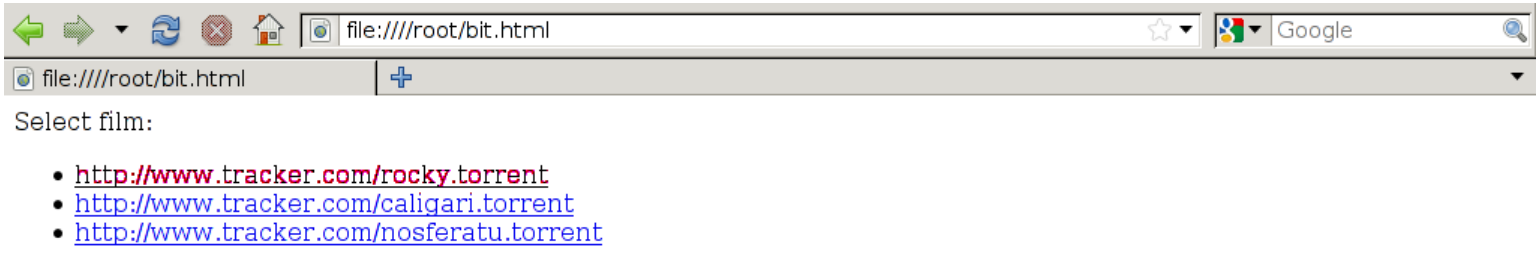
- Connects only to trackers authorized by user.
- Grants privileges only for IPs returned by tracker.

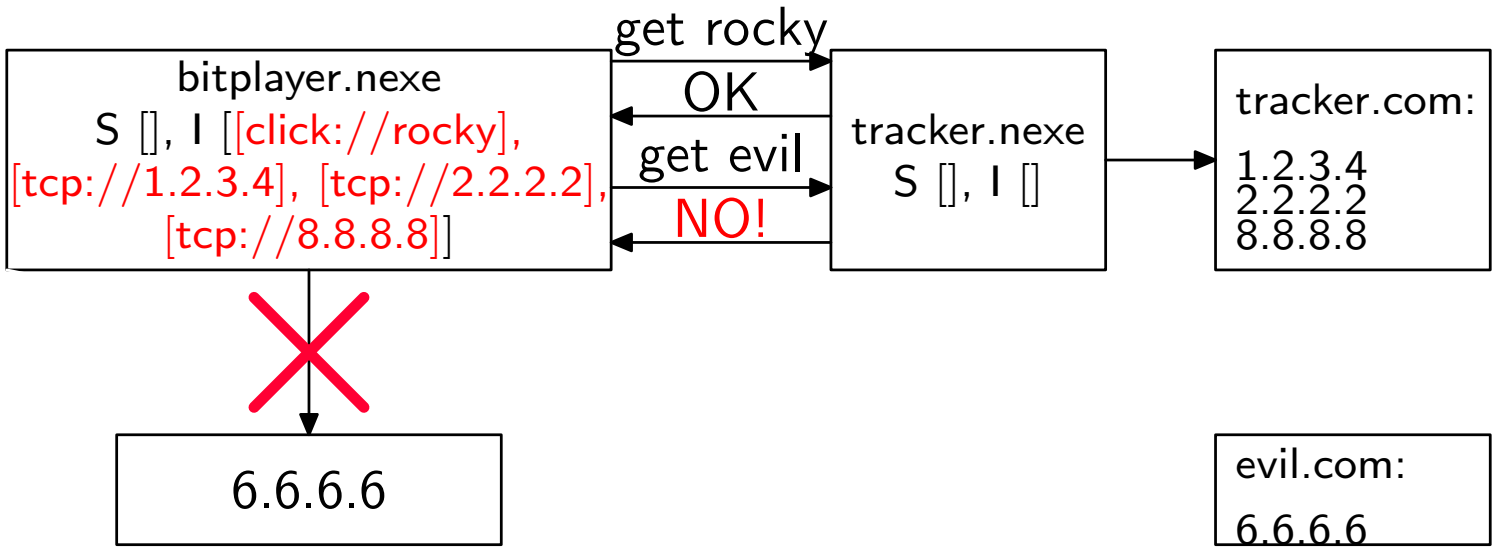


NaCl bittaurent player

Policy module tracker.nexe (100 LoC; *cf.* 327,000 untrusted):

- Connects only to trackers authorized by user.
- Grants privileges only for IPs returned by tracker.





Summary

- Convergence of applications and web sites is inevitable.
  - Web apps need more performance and functionality.
  - Threatens to undermine already tenuous browser security.
- Information flow control transcends complex module interactions.
- Infer user's intent from actions.
  1. User action generates endorsement.
  2. Policy modules translate endorsements to privileges.