Security Architecture for Broadway

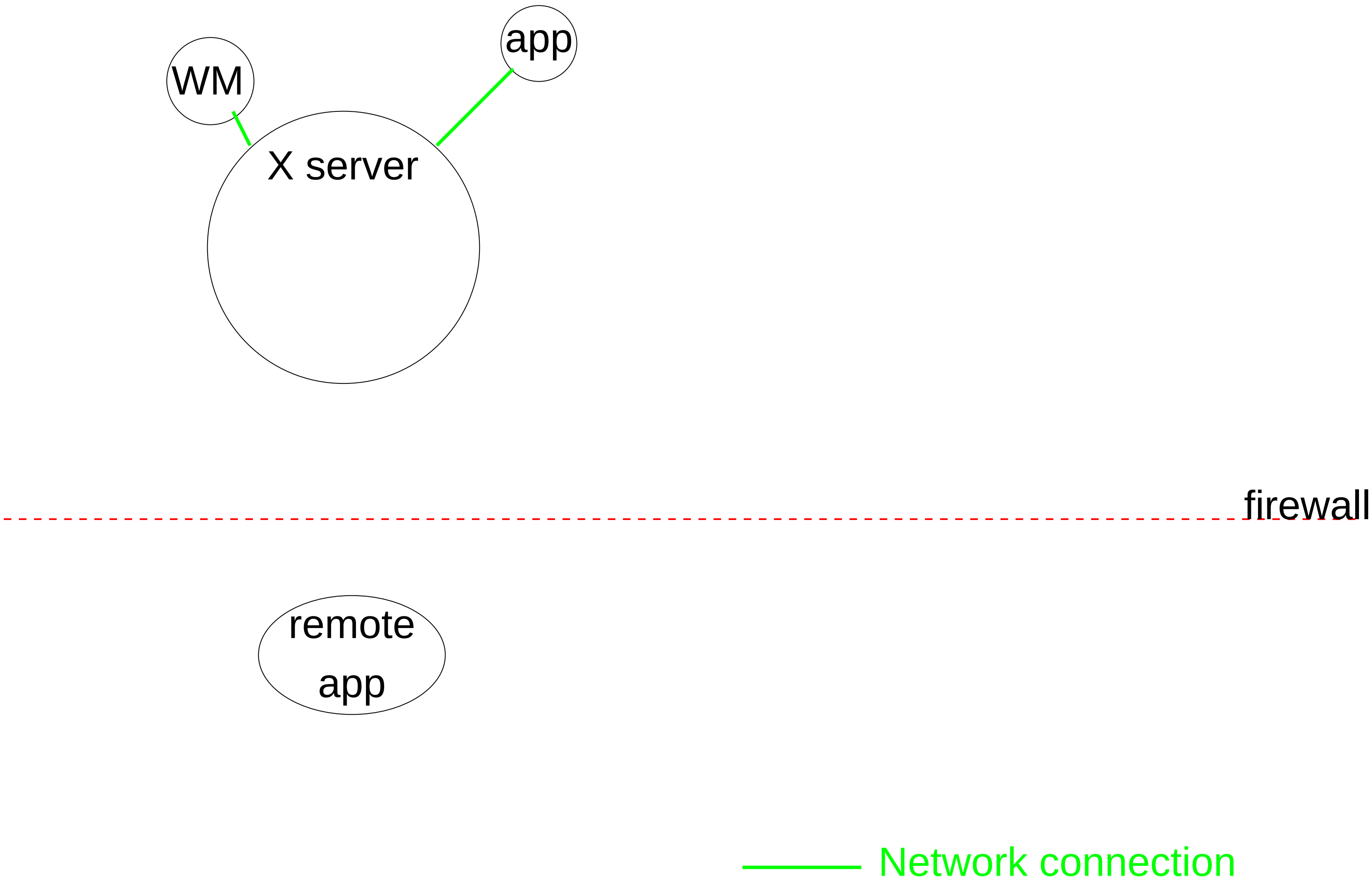
Stephen Gildea

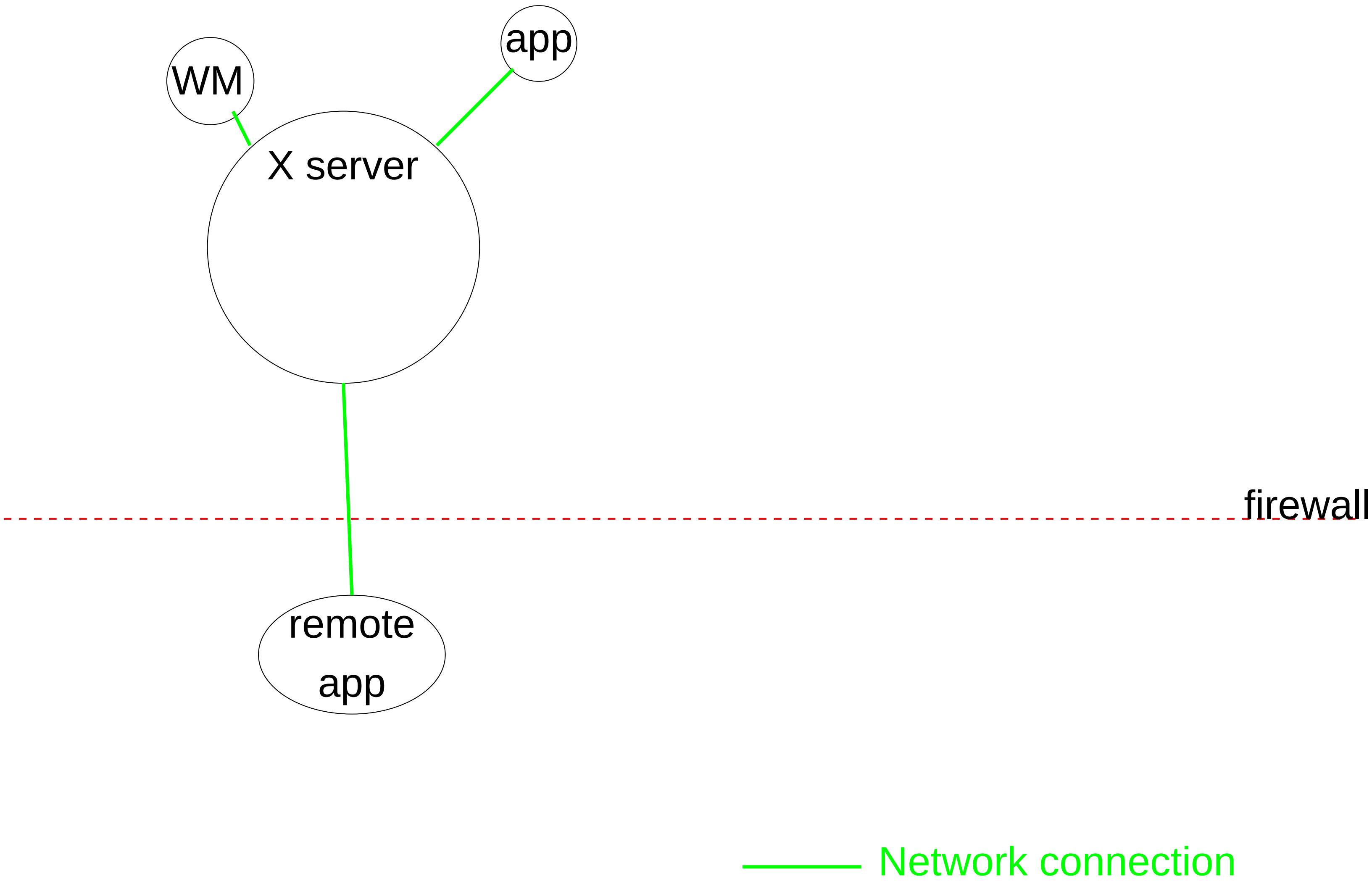
gildea@x.org

General Goal:
To make Broadway secure

. . . even in the presence of

- insecure communication path
- unknown application


WM
app
X server
firewall
remote app
Network connection

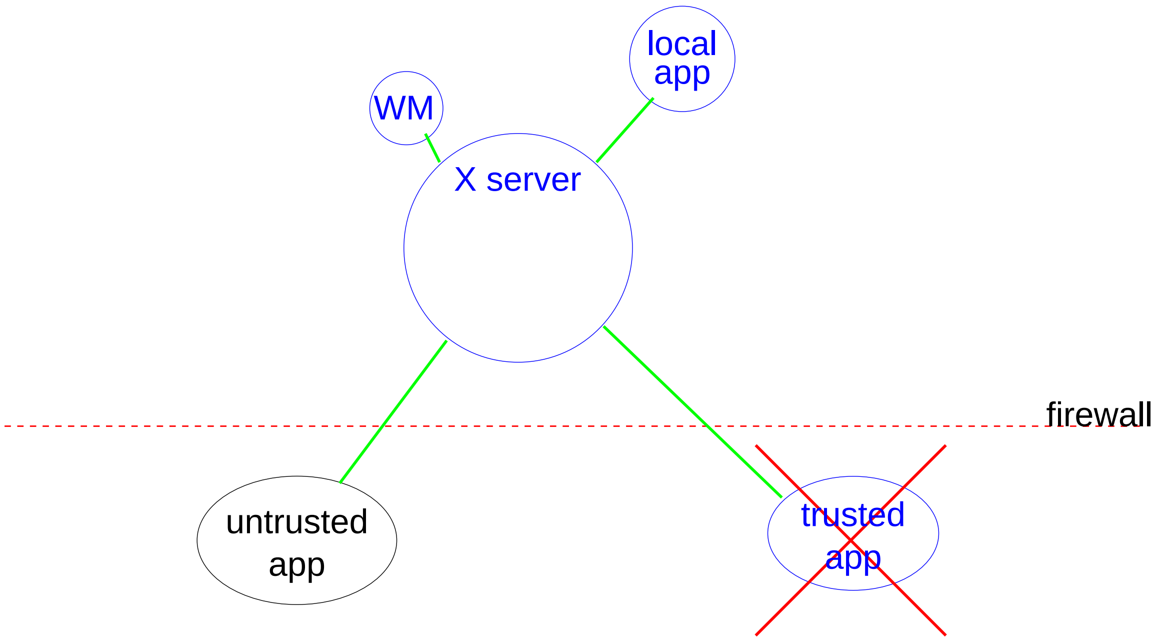

WM
app
X server
firewall
remote
app
Network connection

Non-Goals:

Compartmented Mode Workstation

Non-Goals:

trusted applications over insecure networks



Specific Goals

- Prevent untrusted applications stealing, modifying, or destroying data of trusted applications.
- Control who can connect to your servers and whether they are regarded as trusted or untrusted.
- Be able to revoke access to applications.

More Goals

- Make it easy to configure Broadway securely.
- Not require changes to existing applications.

Threats *not* countered

all classes of denial-of-service attacks

covert channels

Outline:

- Security in X11R6
- Additional Functionality Needed
- Broadway Security

Security in X11R6

- authorization at connection time
- full run of server after connection

What R6 Doesn't Let You Do

- all applications must be trusted
- all communication paths must be secure

Hence, remote execution over the Internet uncommon.

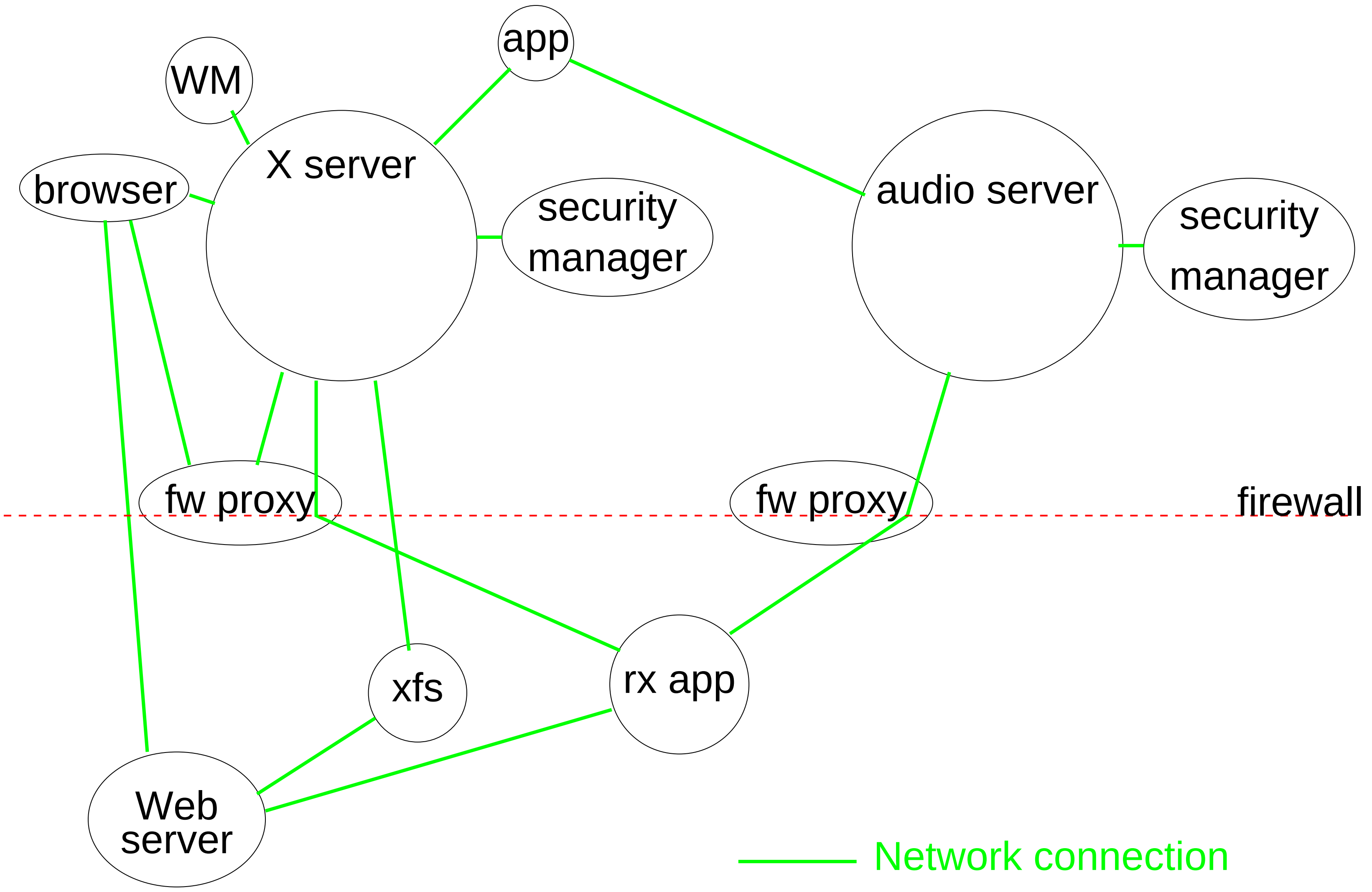
Basic strategy:

Connected $\neq$ Trusted

Broadway Security

Components

- security-aware X server and audio server
- security manager (new)
- firewall proxy (new)


WM
app
X server
browser
security
manager
audio server
security
manager
fw proxy
fw proxy
firewall
xfs
rx app
Web
server
Network connection

X Server

- recognizes trusted and untrusted clients
- policy determined by a security manager
- allows breaking grabs

Security Manager

- determines what actions are acceptable
- may query the user

Firewall Proxy

- gets remote applications through a corporate firewall
- verifies that the X server is security-aware

Firewall Proxy does *not* implement security

- no duplicated code
- no tracking extensions
- keeps firewall small

X Server: connection of untrusted clients

identified by authorization presented

- by key presented
- by source host

can be disconnected if authorization revoked

X Server and Untrusted Clients: Resources

limited access to resources of trusted clients

limited access to server global resources

X Server and Untrusted Clients: Protocol

core requests: access control handled per-operation

extensions: access control handled per-extension

X Server: extensions

insecure extensions are

- not advertised to untrusted clients
- not executed on behalf of untrusted clients

(extensions do not need to be re-written)

Security Manager: Selections

allows access according to its policy

acts as intermediary

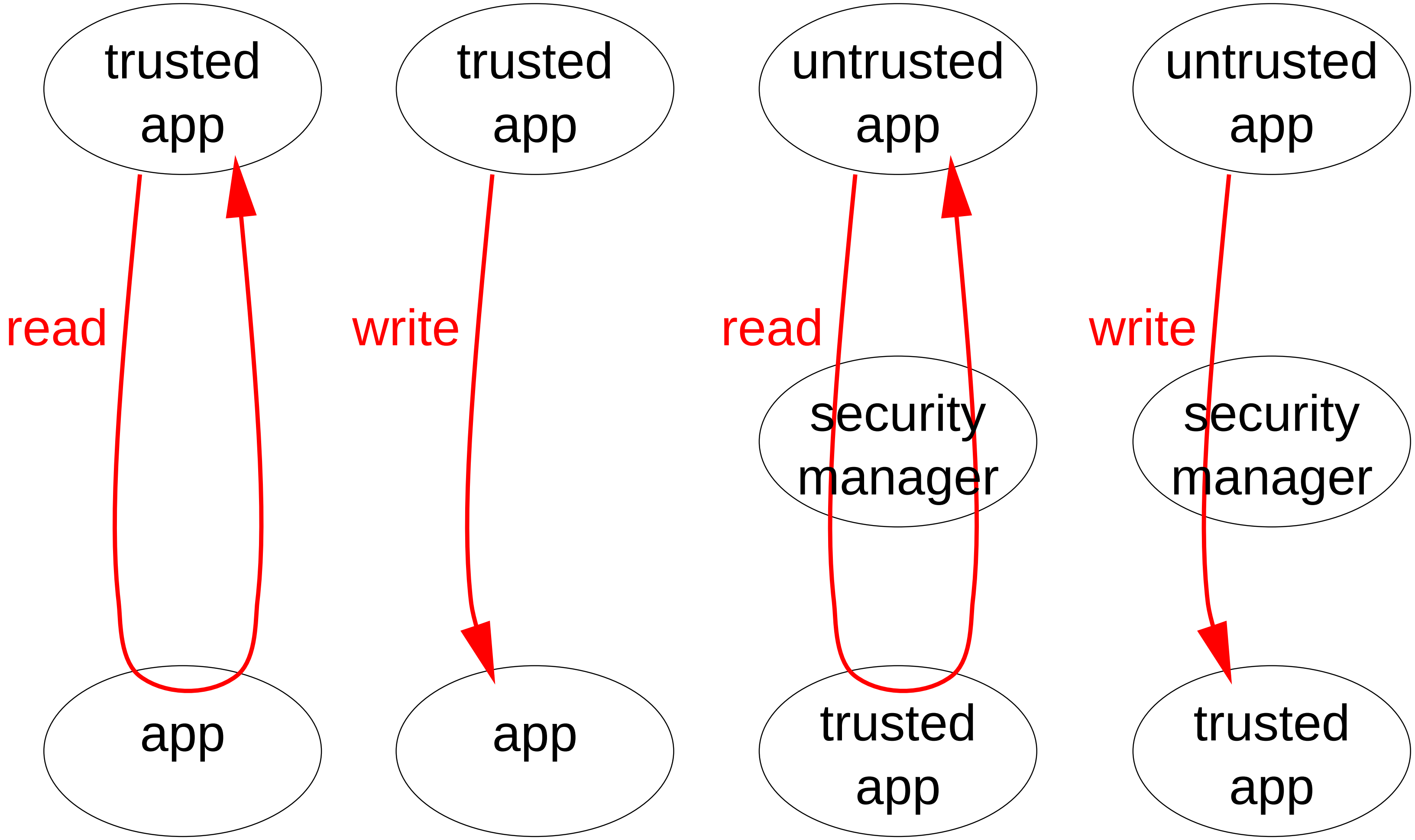
Security Manager: Cut Buffers

trusted $\rightarrow$ untrusted: query user

trusted $\rightarrow$ trusted: ok

untrusted $\rightarrow$ untrusted: ok

Security Manager



Other X Server Global Data

unreadable:

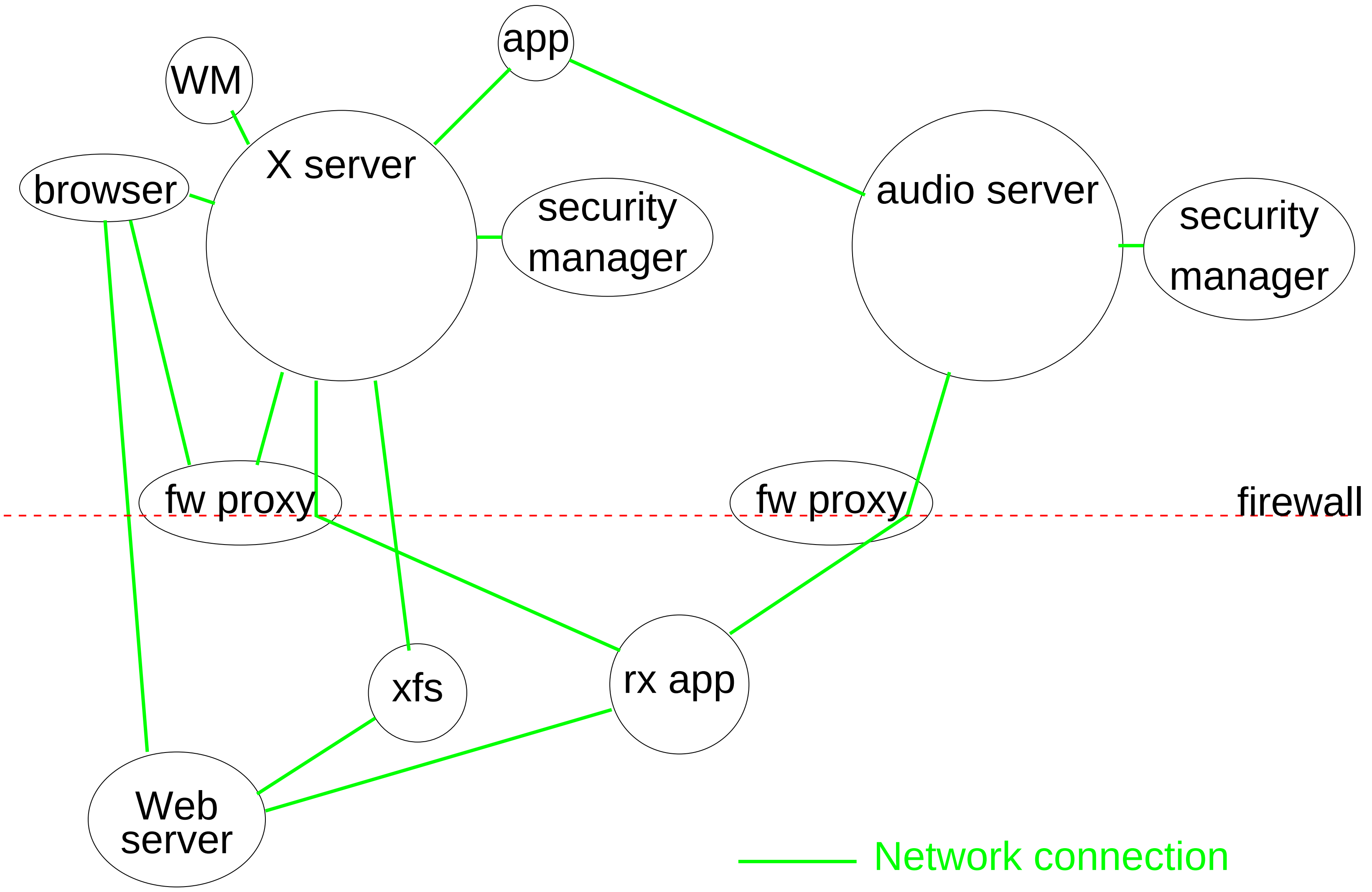
- keyboard state

unwritable:

- root properties, e.g., `RESOURCE_MANAGER`
- keyboard map, mouse map

Remote Font Servers

- provides application-specific fonts for remote app
- does not affect trusted clients


WM
app
X server
browser
security
manager
audio server
security
manager
fw proxy
fw proxy
firewall
xfs
rx app
Web
server
Network connection

Goal met by Broadway security:

can now run applications from anywhere on the Internet