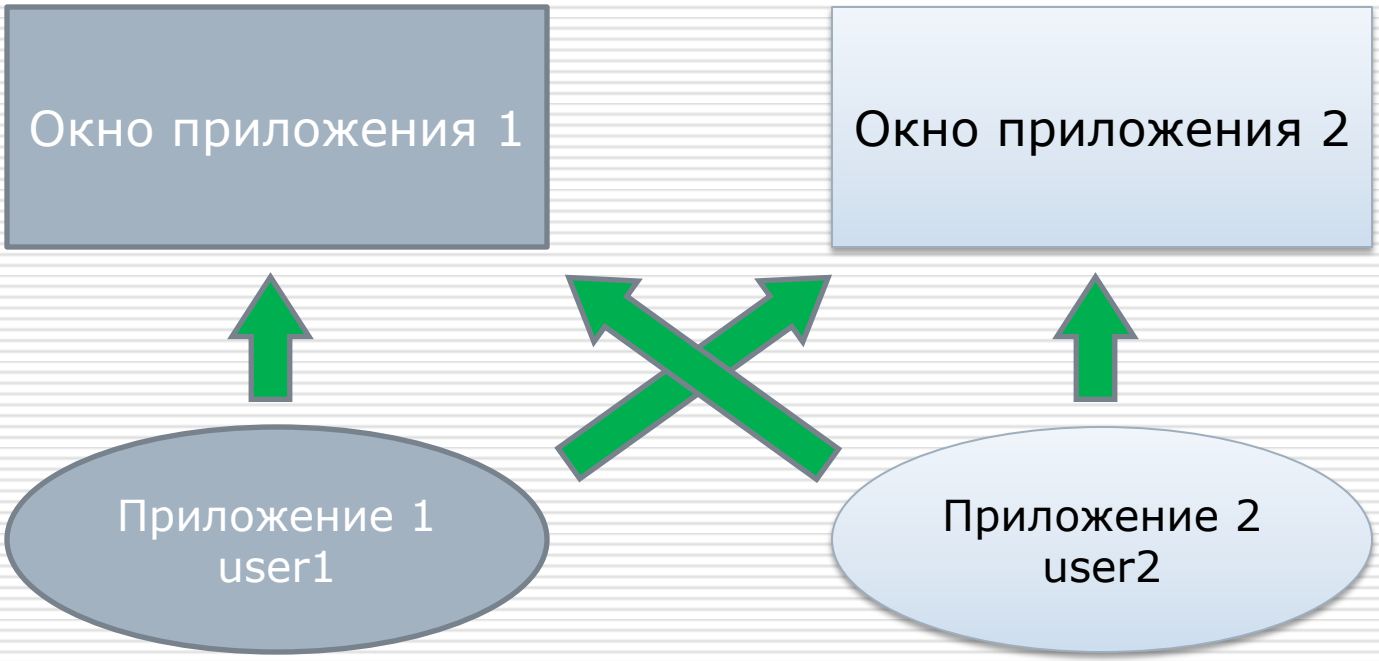
Новый подход к защите графических подсистем рабочих станций Linux

Проскурин Вадим Геннадьевич
к.т.н., доцент
vadim_proskurin@hotmail.com
vadim_proskurin@mail.ru

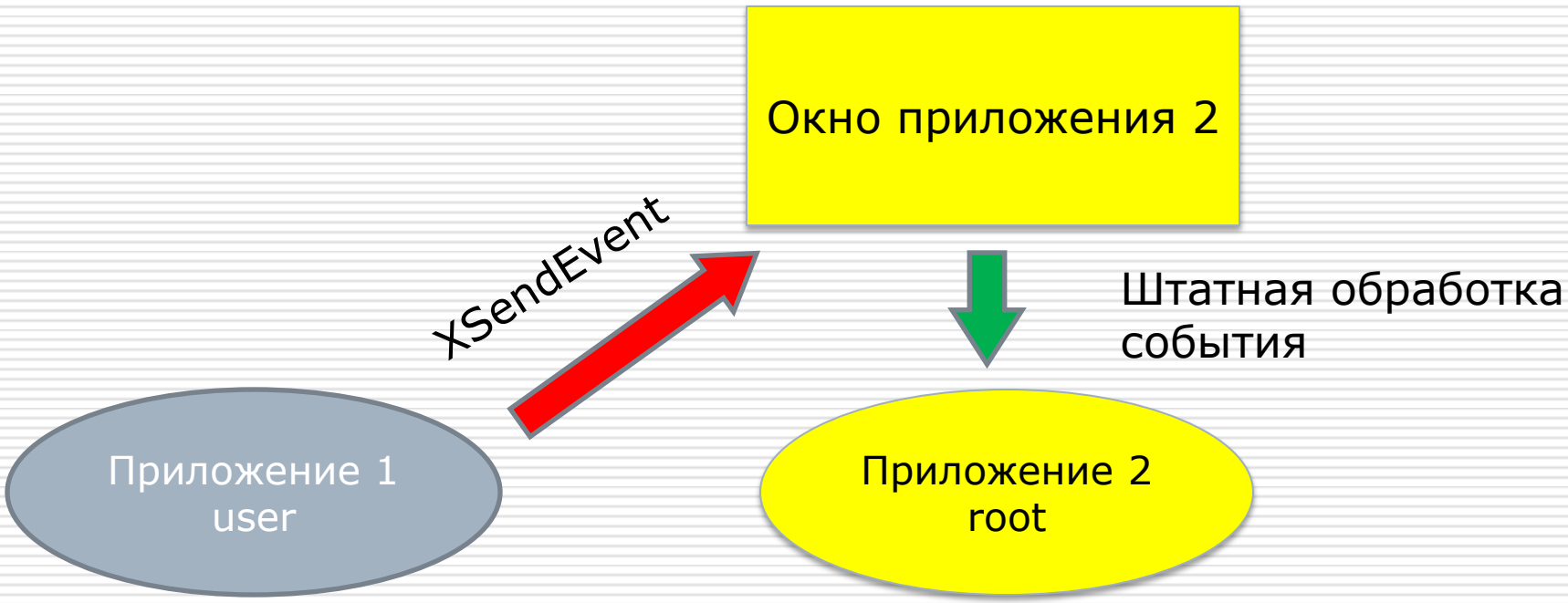
Смирнов Александр Юрьевич
к.т.н.
a.smirnov@rusbitech.ru

Отсутствие управления доступом в X Window System

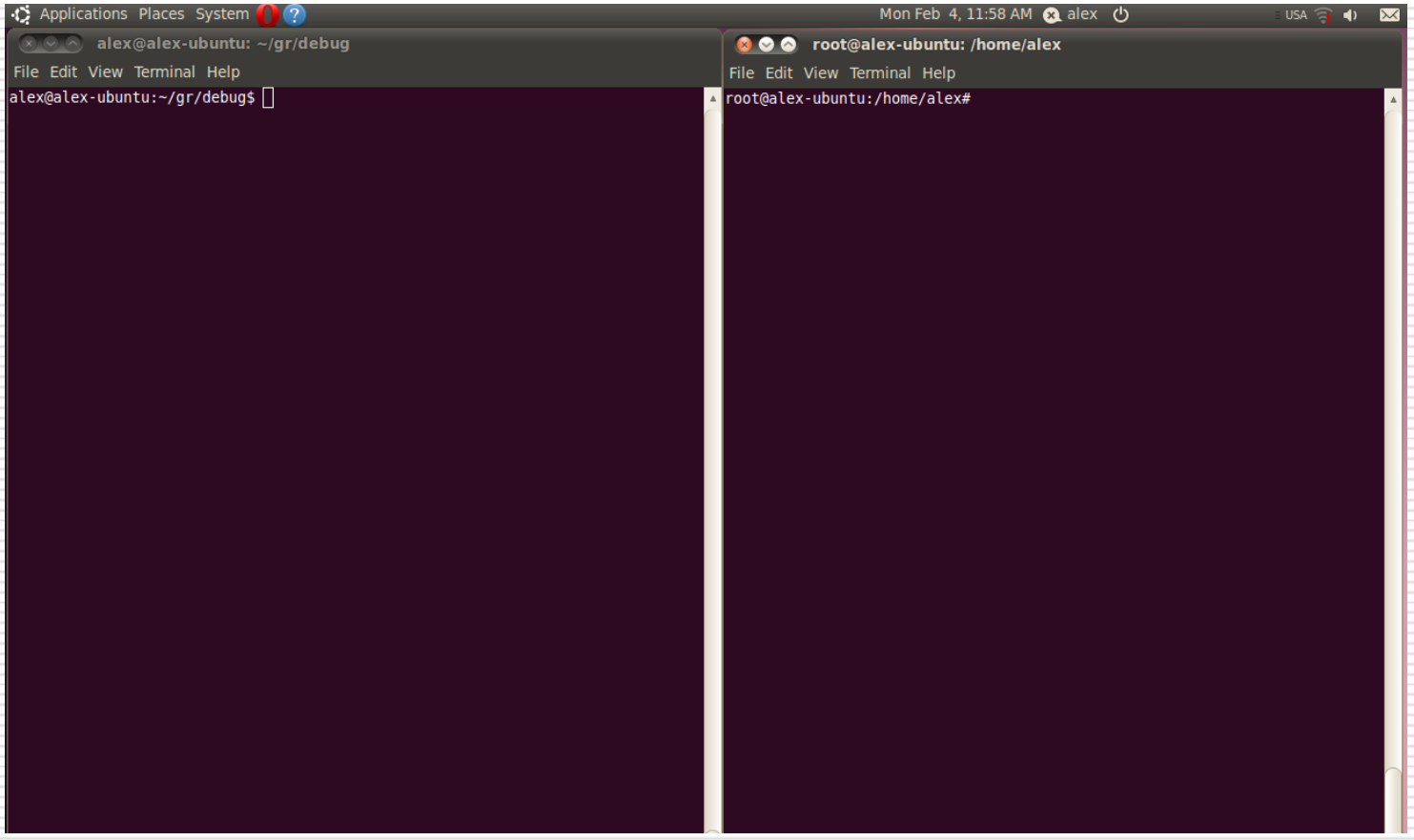


Любой доступ любого приложения к любому окну разрешен (за редкими исключениями)

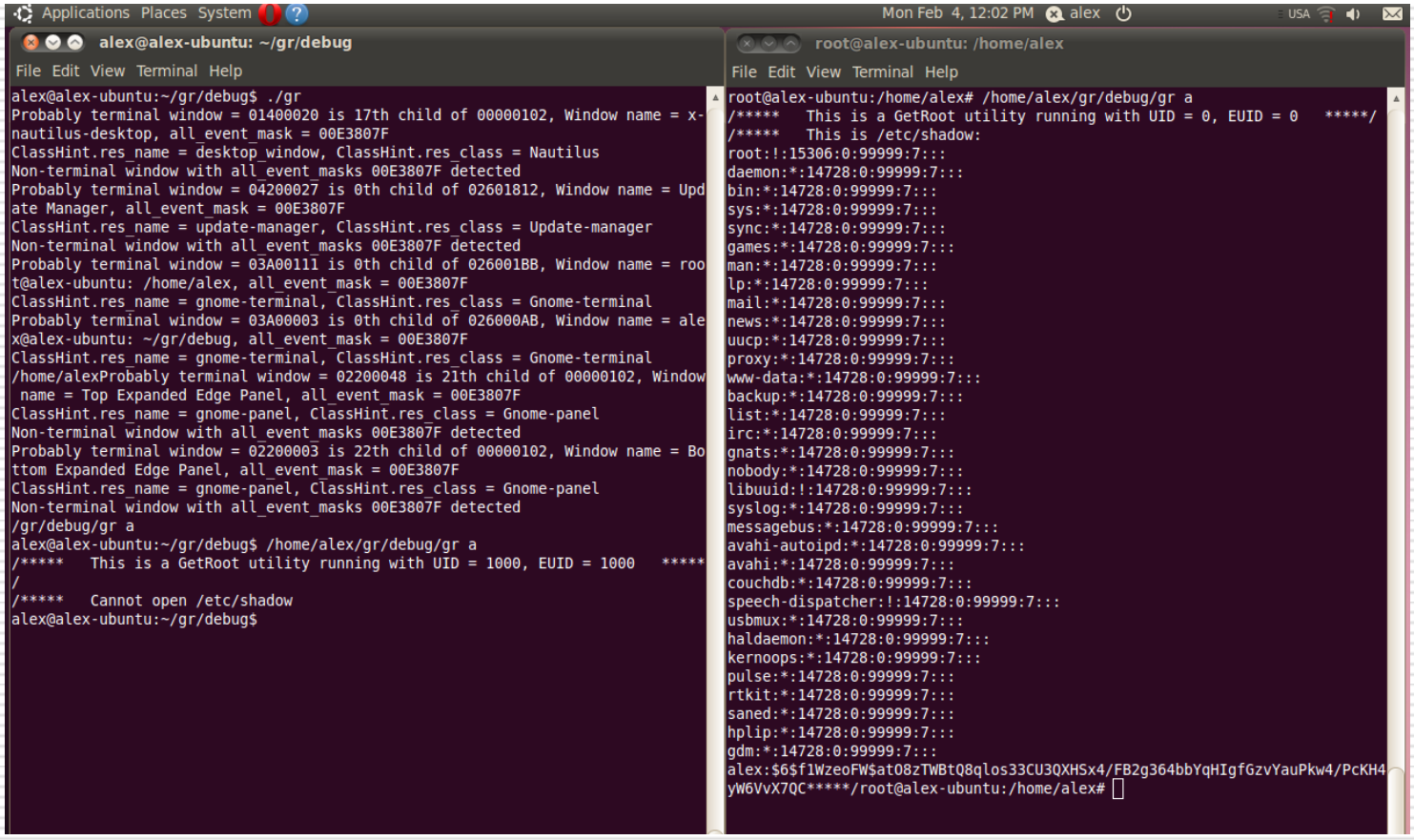
Уязвимость 1
Навязывание оконных событий окнам привилегированных процессов



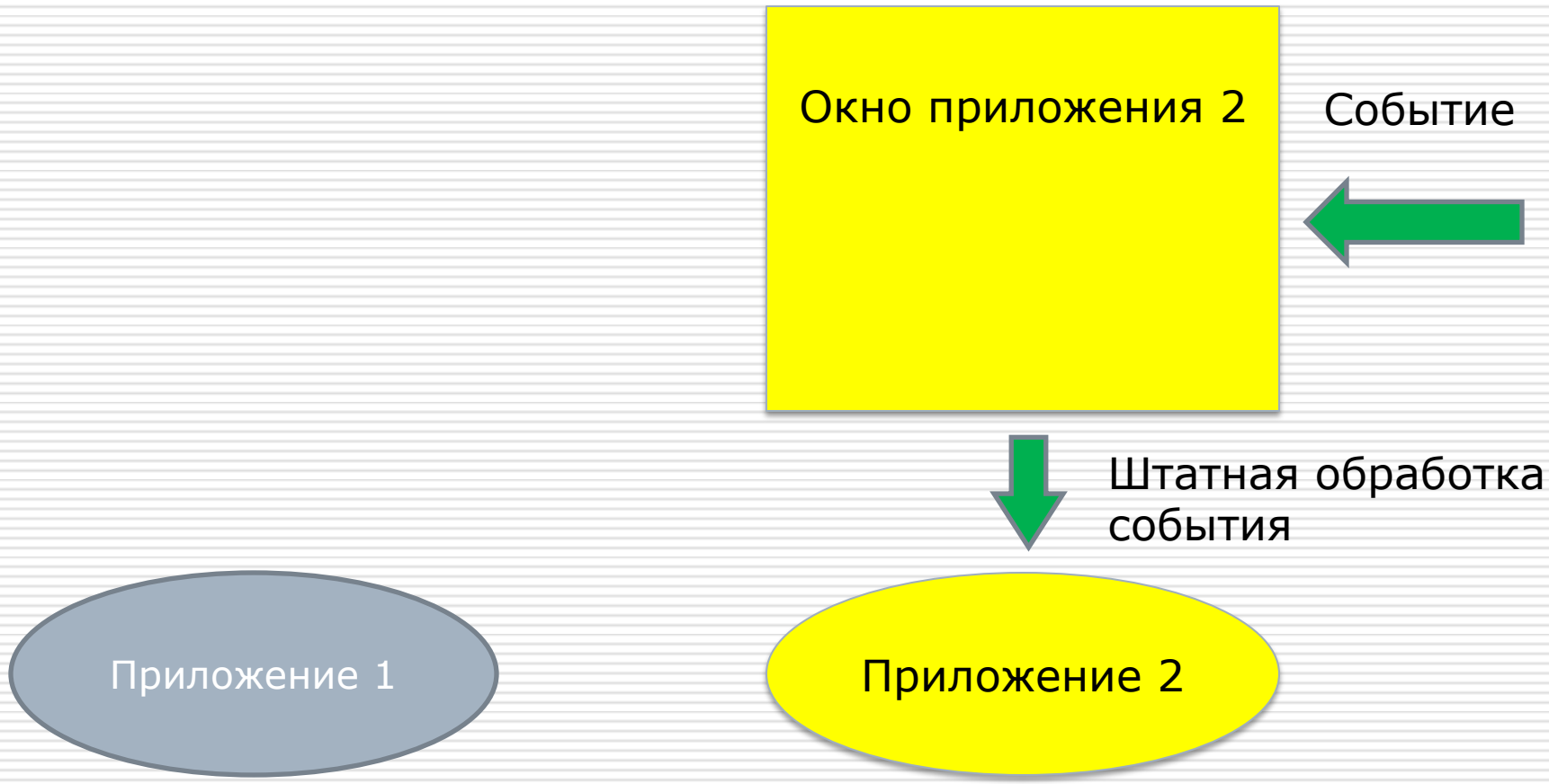
Уязвимость 1
Навязывание оконных событий окнам привилегированных процессов



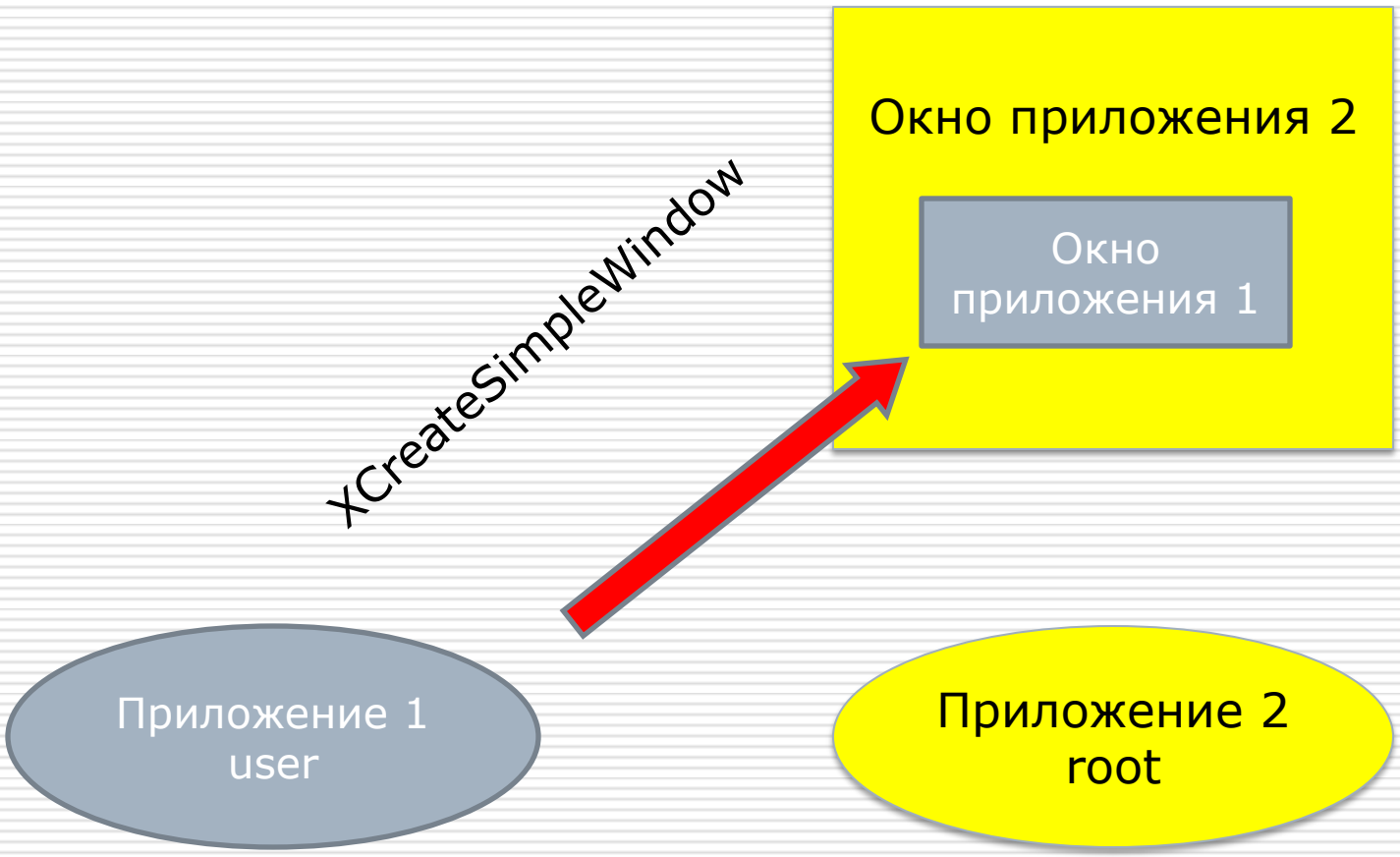
Уязвимость 1
Навязывание оконных событий окнам привилегированных процессов



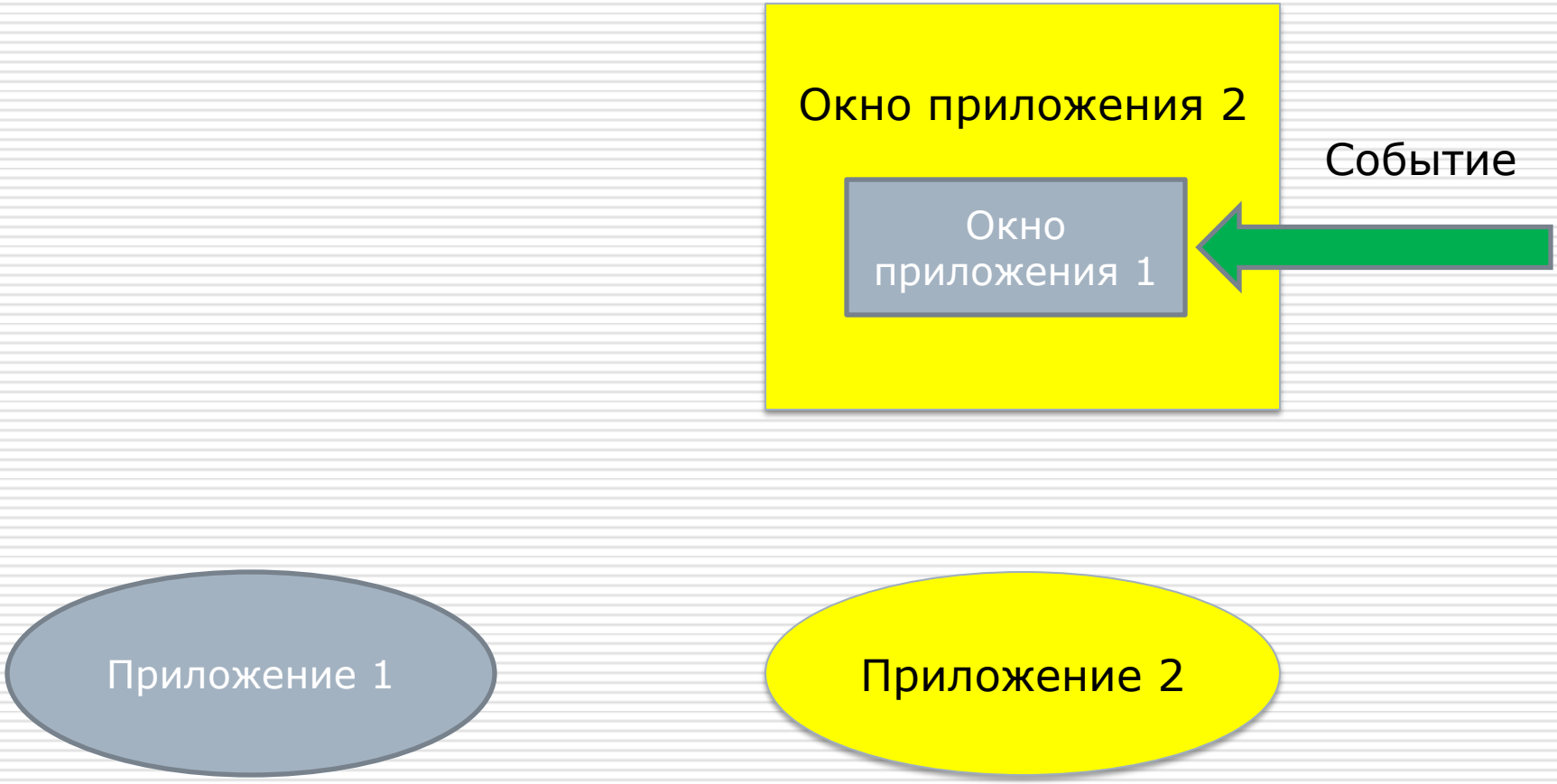
Уязвимость 2
Внедрение дочернего окна в чужое родительское окно



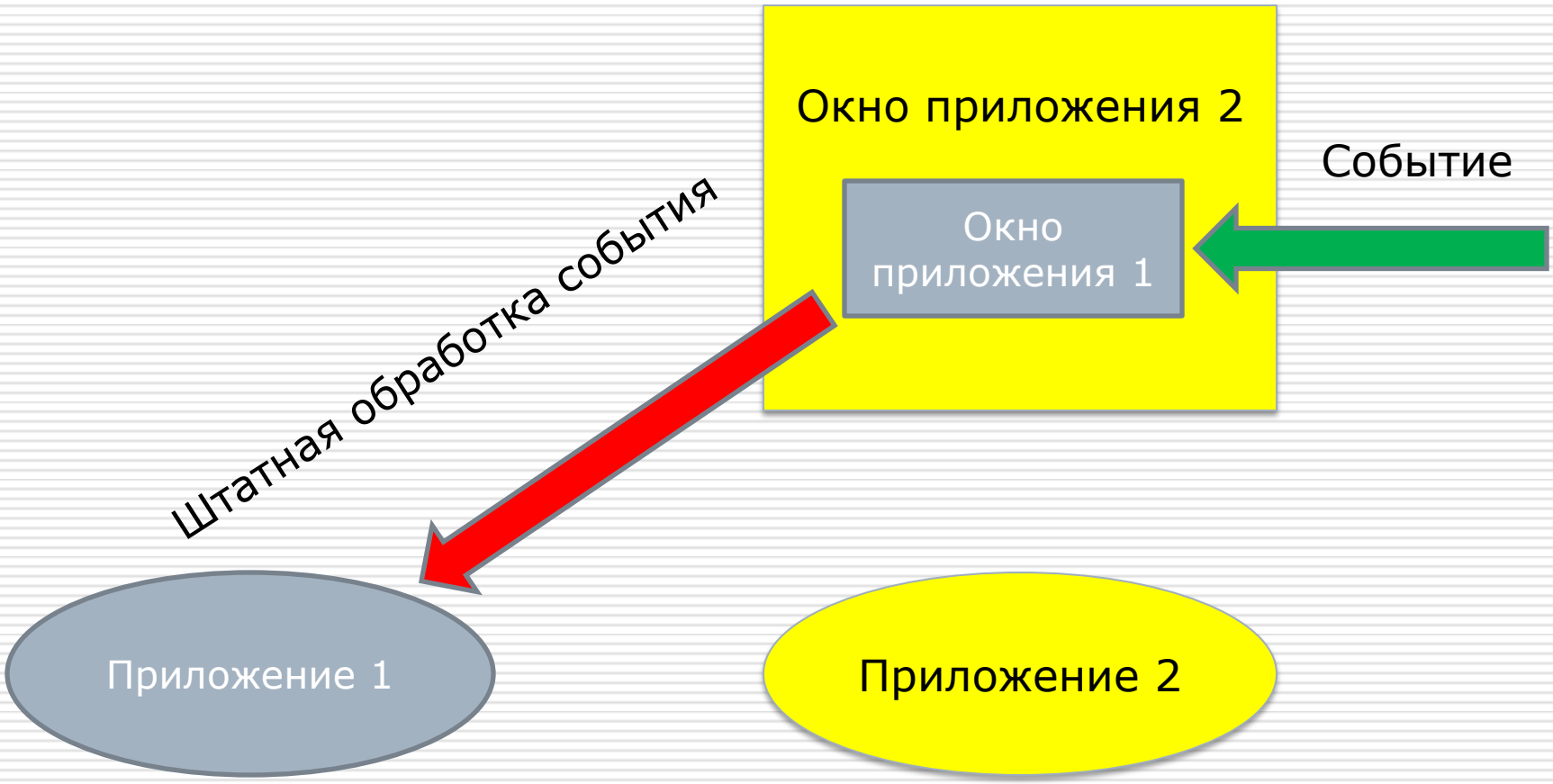
Уязвимость 2
Внедрение дочернего окна в чужое родительское окно



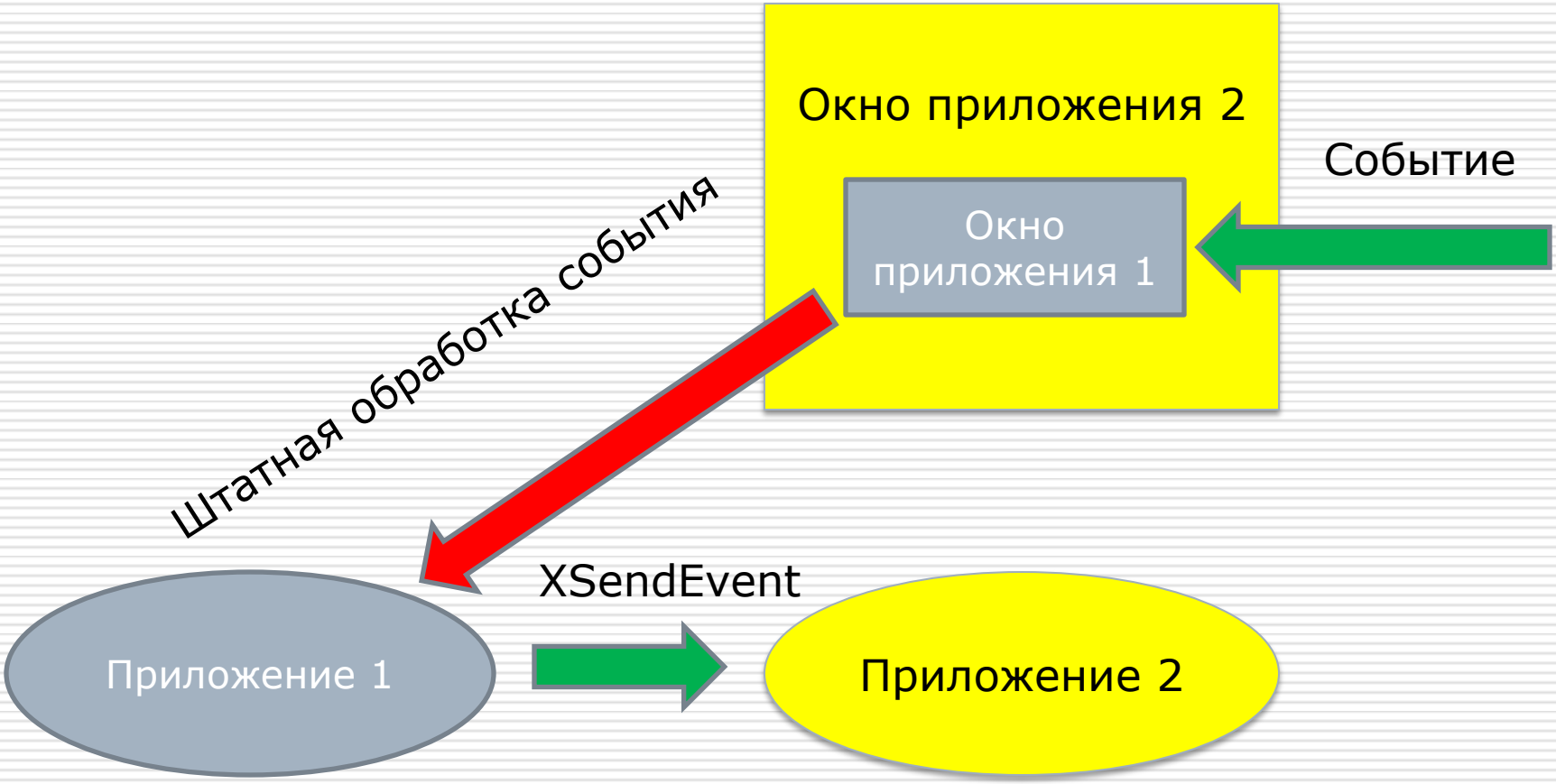
Уязвимость 2
Внедрение дочернего окна в чужое родительское окно



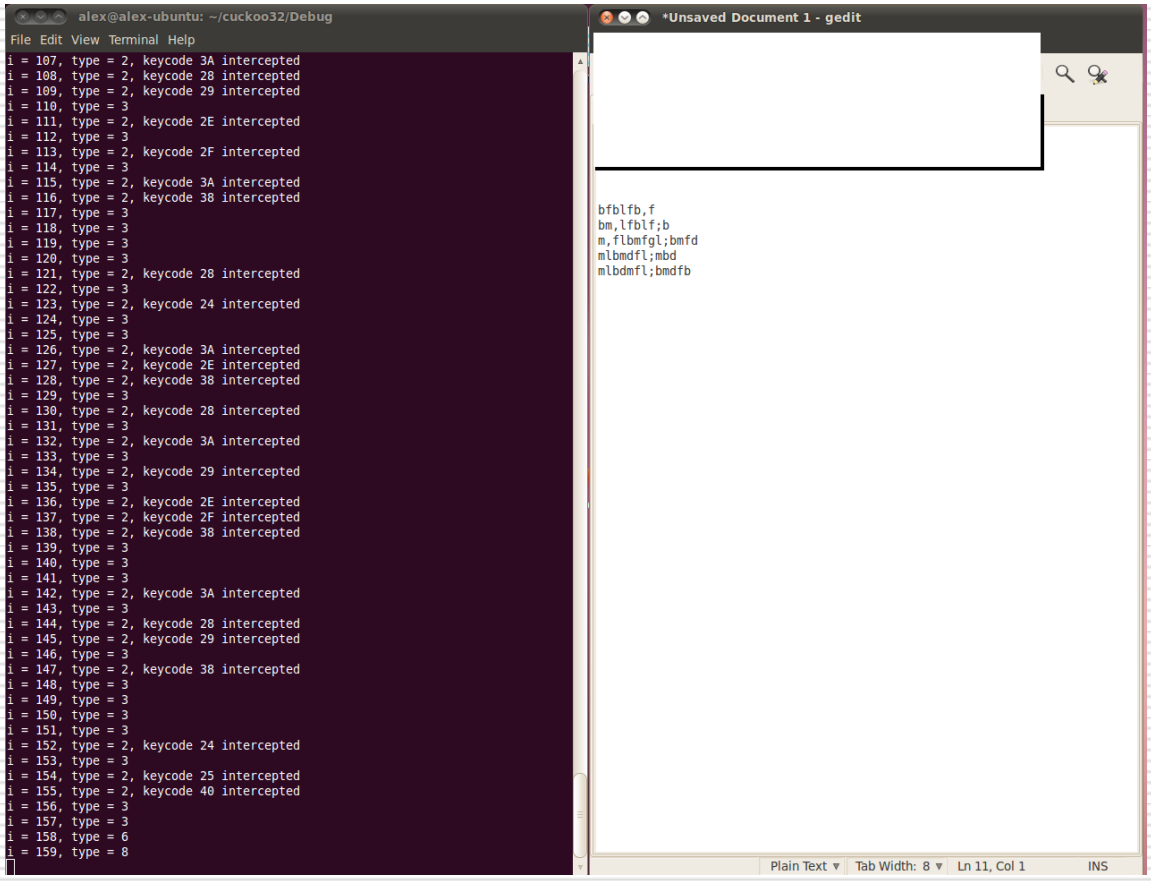
Уязвимость 2
Внедрение дочернего окна в чужое родительское окно



Уязвимость 2
Внедрение дочернего окна в чужое родительское окно



Уязвимость 2
Внедрение дочернего окна в чужое родительское окно



Новый подход к управлению доступом в графической подсистеме Linux

- включает в себя мандатное управление доступом (опционально) и мандатный контроль целостности
- основано на МРОСЛ ДП-модели
- конфиденциальность или целостность дочернего объекта не могут быть выше, чем у объекта-родителя
- не содержит произвольно задаваемых дискреционных правил

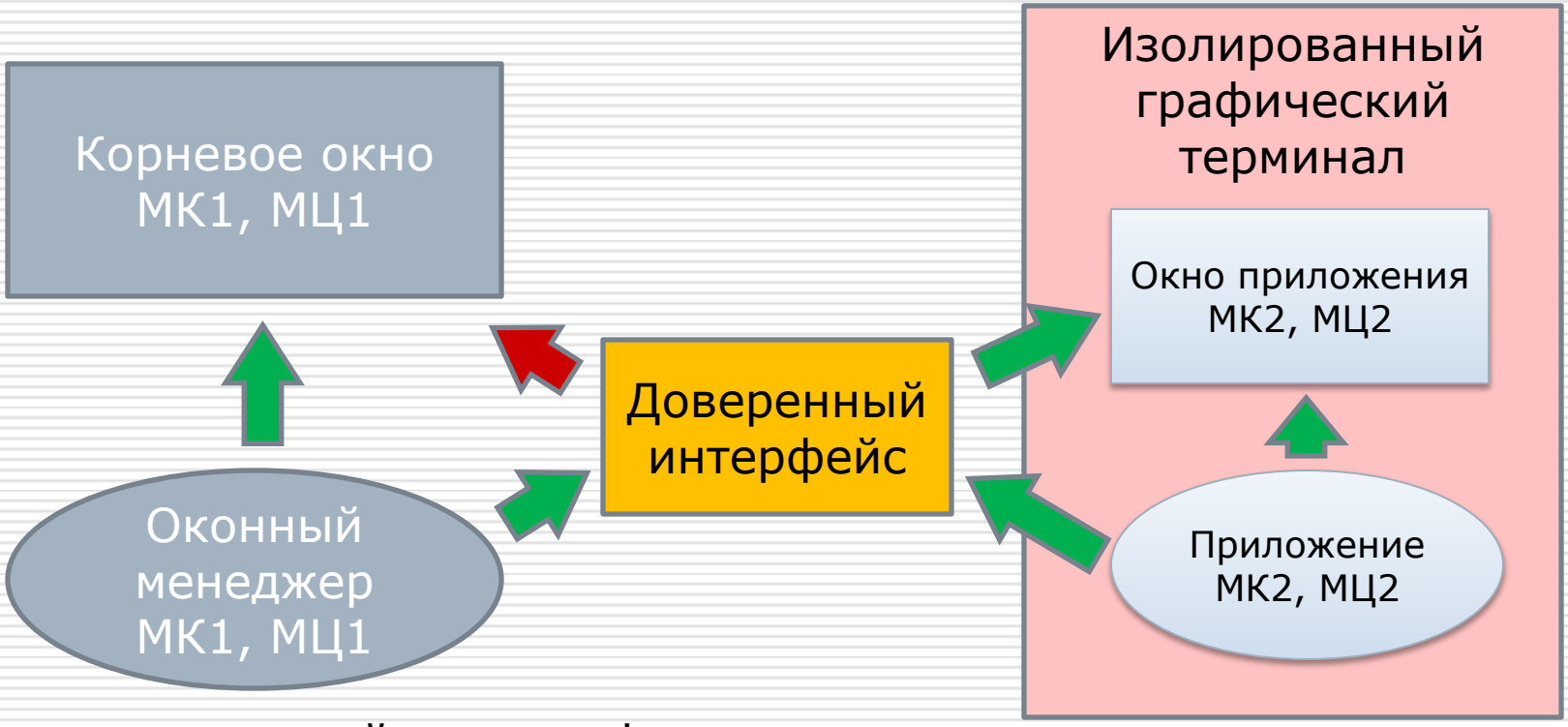
Почему не используется SELinux

- трудно обосновать корректность и полноту реализуемых функций, требуется определенная степень доверия разработчику (АНБ США)
- многие приложения нуждаются в тонкой настройке на конкретную версию SELinux
- средства описания конкретных политик безопасности крайне неудобны
- реализация мандатного контроля целостности требует отдельных исследований

Управление доступом в графической подсистеме Linux

Окна приложений, чья конфиденциальность и целостность совпадают с конфиденциальностью и целостностью оконного менеджера, не изолируются от корневого окна

Управление доступом в графической подсистеме Linux



Окна приложений, чья конфиденциальность или целостность не строго ниже, чем у оконного менеджера, инкапсулируются в изолированный графический терминал

Спасибо
за внимание
Вопросы?