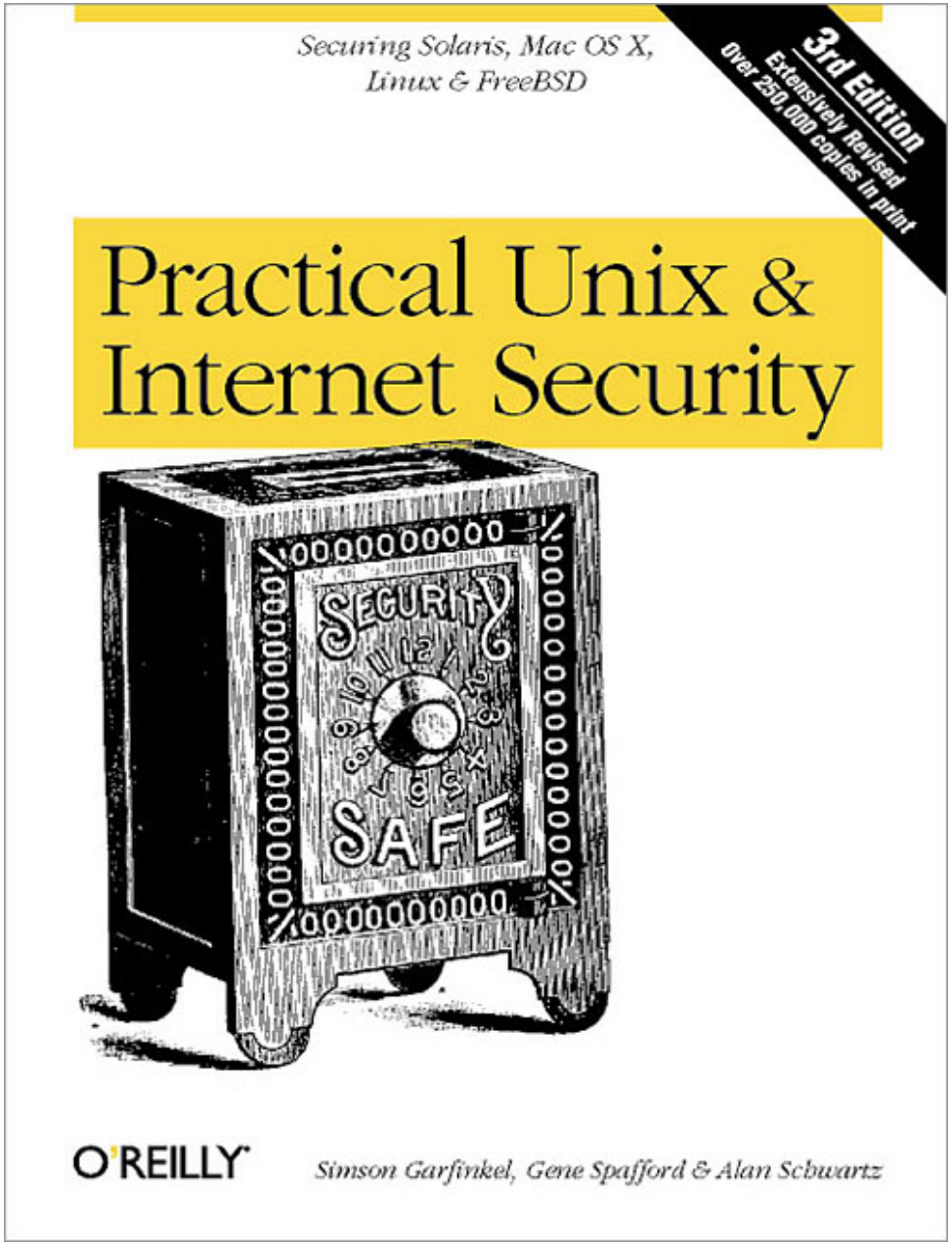
A better security metaphor

Et al.

27. Dezember 2016

The safe as metaphor



The safe as metaphor

The safe as metaphor Resembles mainframe/early UNIX computing environment

- it's self-contained
- material enters/leaves only with consent and on purpose
- material in environment can be inspected
- personell controls environment
- need specialized knowledge
- attacks are noticeable, because security is mostly physical

The safe as metaphor

The safe as metaphor Resembles mainframe/early UNIX computing environment

- it's self-contained
- material enters/leaves only with consent and on purpose
- material in environment can be inspected
- personell controls environment
- need specialized knowledge
- attacks are noticeable, because security is mostly physical

The safe as metaphor

The safe as metaphor Resembles mainframe/early UNIX computing environment

- it's self-contained
- material enters/leaves only with consent and on purpose
- material in environment can be inspected
- personell controls environment
- need specialized knowledge
- attacks are noticeable, because security is mostly physical

The safe as metaphor

The safe as metaphor Resembles mainframe/early UNIX computing environment

- it's self-contained
- material enters/leaves only with consent and on purpose
- material in environment can be inspected
- personell controls environment
- need specialized knowledge
- attacks are noticeable, because security is mostly physical

The safe as metaphor

The safe as metaphor Resembles mainframe/early UNIX computing environment

- it's self-contained
- material enters/leaves only with consent and on purpose
- material in environment can be inspected
- personell controls environment
- need specialized knowledge
- attacks are noticeable, because security is mostly physical

The safe as metaphor

The safe as metaphor Resembles mainframe/early UNIX computing environment

- it's self-contained
- material enters/leaves only with consent and on purpose
- material in environment can be inspected
- personell controls environment
- need specialized knowledge
- attacks are noticeable, because security is mostly physical

Modern Standard Environment (OS+Network+Browser)

- not contained (Content pulled from network into Browser generates network traffic . . .)
- material can enter without consent (ads, cookies, webappsstore, malvertising)
- material can be siphoned off without consent (browser tracking, location data)
- at least in MS/Apple products, users cannot inspect internals
- environment is remotely controlled (auto-updates, Windows 10 EULA, botnet admins)
- only perceived way to cleanup a compromised system is complete wipeout+re-install
- nobody knows what goes on in the system (dozens of undocumented services . . .)
- **but it is convenient!**
- everbody can use it
- So what would be a better metaphor?

Modern Standard Environment (OS+Network+Browser)

- not contained (Content pulled from network into Browser generates network traffic . . .)
- material can enter without consent (ads, cookies, webappsstore, malvertising)
- material can be siphoned off without consent (browser tracking, location data)
- at least in MS/Apple products, users cannot inspect internals
- environment is remotely controlled (auto-updates, Windows 10 EULA, botnet admins)
- only perceived way to cleanup a compromised system is complete wipeout+re-install
- nobody knows what goes on in the system (dozens of undocumented services . . .)
- **but it is convenient!**
- everbody can use it
- So what would be a better metaphor?

Modern Standard Environment (OS+Network+Browser)

- not contained (Content pulled from network into Browser generates network traffic . . .)
- material can enter without consent (ads, cookies, webappsstore, malvertising)
- material can be siphoned off without consent (browser tracking, location data)
- at least in MS/Apple products, users cannot inspect internals
- environment is remotely controlled (auto-updates, Windows 10 EULA, botnet admins)
- only perceived way to cleanup a compromised system is complete wipeout+re-install
- nobody knows what goes on in the system (dozens of undocumented services . . .)
- **but it is convenient!**
- everbody can use it
- So what would be a better metaphor?

Modern Standard Environment (OS+Network+Browser)

- not contained (Content pulled from network into Browser generates network traffic . . .)
- material can enter without consent (ads, cookies, webappsstore, malvertising)
- material can be siphoned off without consent (browser tracking, location data)
- at least in MS/Apple products, users cannot inspect internals
- environment is remotely controlled (auto-updates, Windows 10 EULA, botnet admins)
- only perceived way to cleanup a compromised system is complete wipeout+re-install
- nobody knows what goes on in the system (dozens of undocumented services . . .)
- **but it is convenient!**
- everbody can use it
- So what would be a better metaphor?

Modern Standard Environment (OS+Network+Browser)

- not contained (Content pulled from network into Browser generates network traffic . . .)
- material can enter without consent (ads, cookies, webappsstore, malvertising)
- material can be siphoned off without consent (browser tracking, location data)
- at least in MS/Apple products, users cannot inspect internals
- environment is remotely controlled (auto-updates, Windows 10 EULA, botnet admins)
- only perceived way to cleanup a compromised system is complete wipeout+re-install
- nobody knows what goes on in the system (dozens of undocumented services . . .)
- **but it is convenient!**
- everbody can use it
- So what would be a better metaphor?

Modern Standard Environment (OS+Network+Browser)

- not contained (Content pulled from network into Browser generates network traffic . . .)
- material can enter without consent (ads, cookies, webappsstore, malvertising)
- material can be siphoned off without consent (browser tracking, location data)
- at least in MS/Apple products, users cannot inspect internals
- environment is remotely controlled (auto-updates, Windows 10 EULA, botnet admins)
- only perceived way to cleanup a compromised system is complete wipeout+re-install
- nobody knows what goes on in the system (dozens of undocumented services . . .)
- **but it is convenient!**
- everbody can use it
- So what would be a better metaphor?

Modern Standard Environment (OS+Network+Browser)

- not contained (Content pulled from network into Browser generates network traffic . . .)
- material can enter without consent (ads, cookies, webappsstore, malvertising)
- material can be siphoned off without consent (browser tracking, location data)
- at least in MS/Apple products, users cannot inspect internals
- environment is remotely controlled (auto-updates, Windows 10 EULA, botnet admins)
- only perceived way to cleanup a compromised system is complete wipeout+re-install
- nobody knows what goes on in the system (dozens of undocumented services . . .)
- **but it is convenient!**
- everbody can use it
- So what would be a better metaphor?

Modern Standard Environment (OS+Network+Browser)

- not contained (Content pulled from network into Browser generates network traffic . . .)
- material can enter without consent (ads, cookies, webappsstore, malvertising)
- material can be siphoned off without consent (browser tracking, location data)
- at least in MS/Apple products, users cannot inspect internals
- environment is remotely controlled (auto-updates, Windows 10 EULA, botnet admins)
- only perceived way to cleanup a compromised system is complete wipeout+re-install
- nobody knows what goes on in the system (dozens of undocumented services . . .)
- **but it is convenient!**
- everbody can use it
- So what would be a better metaphor?

Modern Standard Environment (OS+Network+Browser)

- not contained (Content pulled from network into Browser generates network traffic . . .)
- material can enter without consent (ads, cookies, webappsstore, malvertising)
- material can be siphoned off without consent (browser tracking, location data)
- at least in MS/Apple products, users cannot inspect internals
- environment is remotely controlled (auto-updates, Windows 10 EULA, botnet admins)
- only perceived way to cleanup a compromised system is complete wipeout+re-install
- nobody knows what goes on in the system (dozens of undocumented services . . .)
- **but it is convenient!**
- everbody can use it
- So what would be a better metaphor?

Modern Standard Environment (OS+Network+Browser)

- not contained (Content pulled from network into Browser generates network traffic . . .)
- material can enter without consent (ads, cookies, webappsstore, malvertising)
- material can be siphoned off without consent (browser tracking, location data)
- at least in MS/Apple products, users cannot inspect internals
- environment is remotely controlled (auto-updates, Windows 10 EULA, botnet admins)
- only perceived way to cleanup a compromised system is complete wipeout+re-install
- nobody knows what goes on in the system (dozens of undocumented services . . .)
- **but it is convenient!**
- everbody can use it
- So what would be a better metaphor?

The now security paradigm

Conclusion

The portaloo

- is **convenient**
- most users are locked out at any time
- is not owned by its users
- only way to a clean one is complete re-install
- **Nobody would store anything important in a portaloo!**

Conclusion

The portaloo

- is **convenient**
- most users are locked out at any time
- is not owned by its users
- only way to a clean one is complete re-install
- **Nobody would store anything important in a portaloo!**

Conclusion

The portaloo

- is **convenient**
- most users are locked out at any time
- is not owned by its users
- only way to a clean one is complete re-install
- **Nobody would store anything important in a portaloo!**

Conclusion

The portaloo

- is **convenient**
- most users are locked out at any time
- is not owned by its users
- only way to a clean one is complete re-install
- **Nobody would store anything important in a portaloo!**

Conclusion

The portaloo

- is **convenient**
- most users are locked out at any time
- is not owned by its users
- only way to a clean one is complete re-install
- **Nobody would store anything important in a portaloo!**