Biztonságos desktop megoldás: Qubes OS

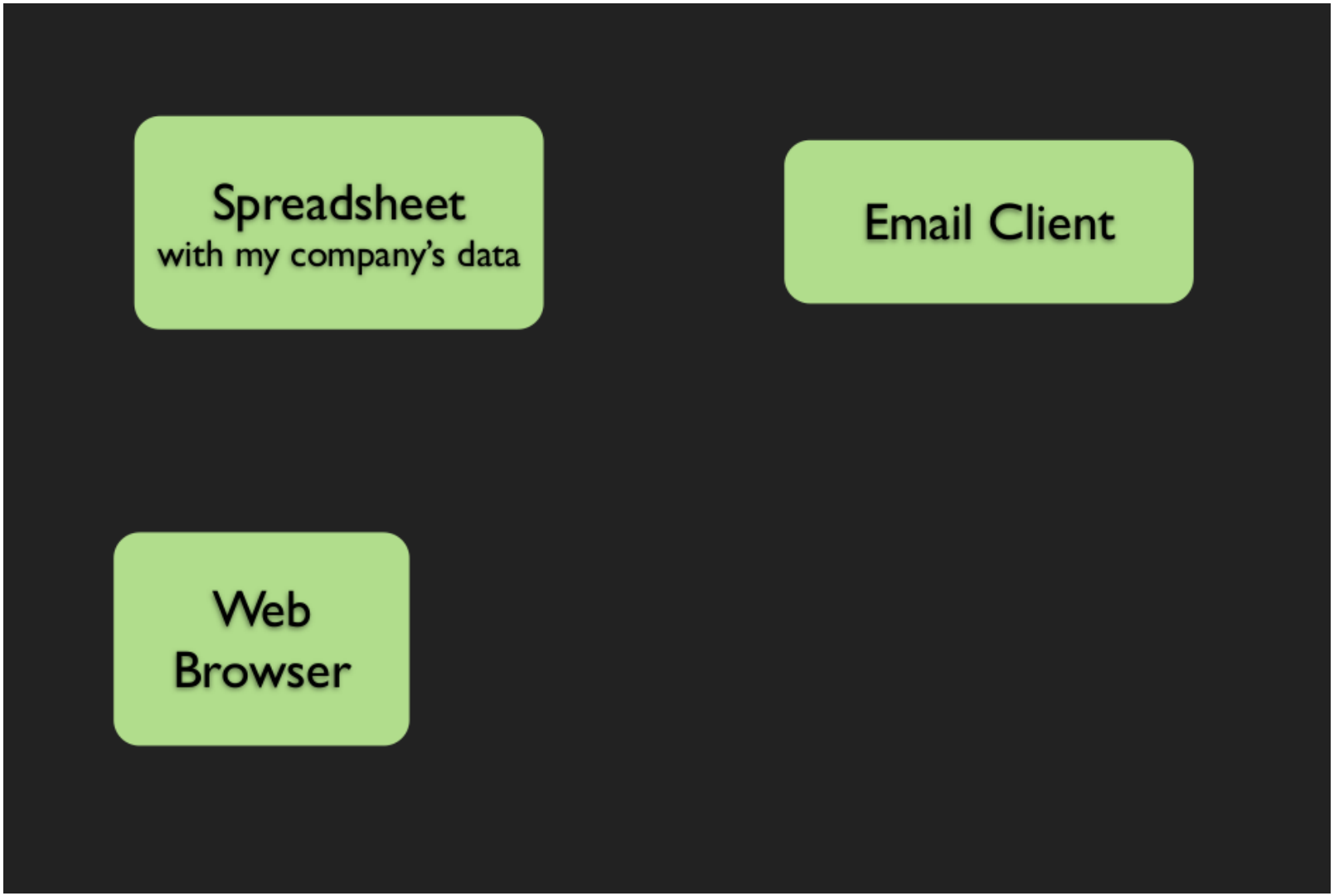
Zrubecz.Laszlo@andrews.hu

Andrews IT Engineering Kft.

A probléma

avagy, miért nem jók a mostani operációs rendszerek

Képzeljünk el egy hagyományos operációs rendszert (Windows, Linux, Mac)


Spreadsheet
with my company's data
Email Client
Web
Browser

Természetesen mindenki más és más alkalmazásokat használ, és várhatóan többet is egyszerre.

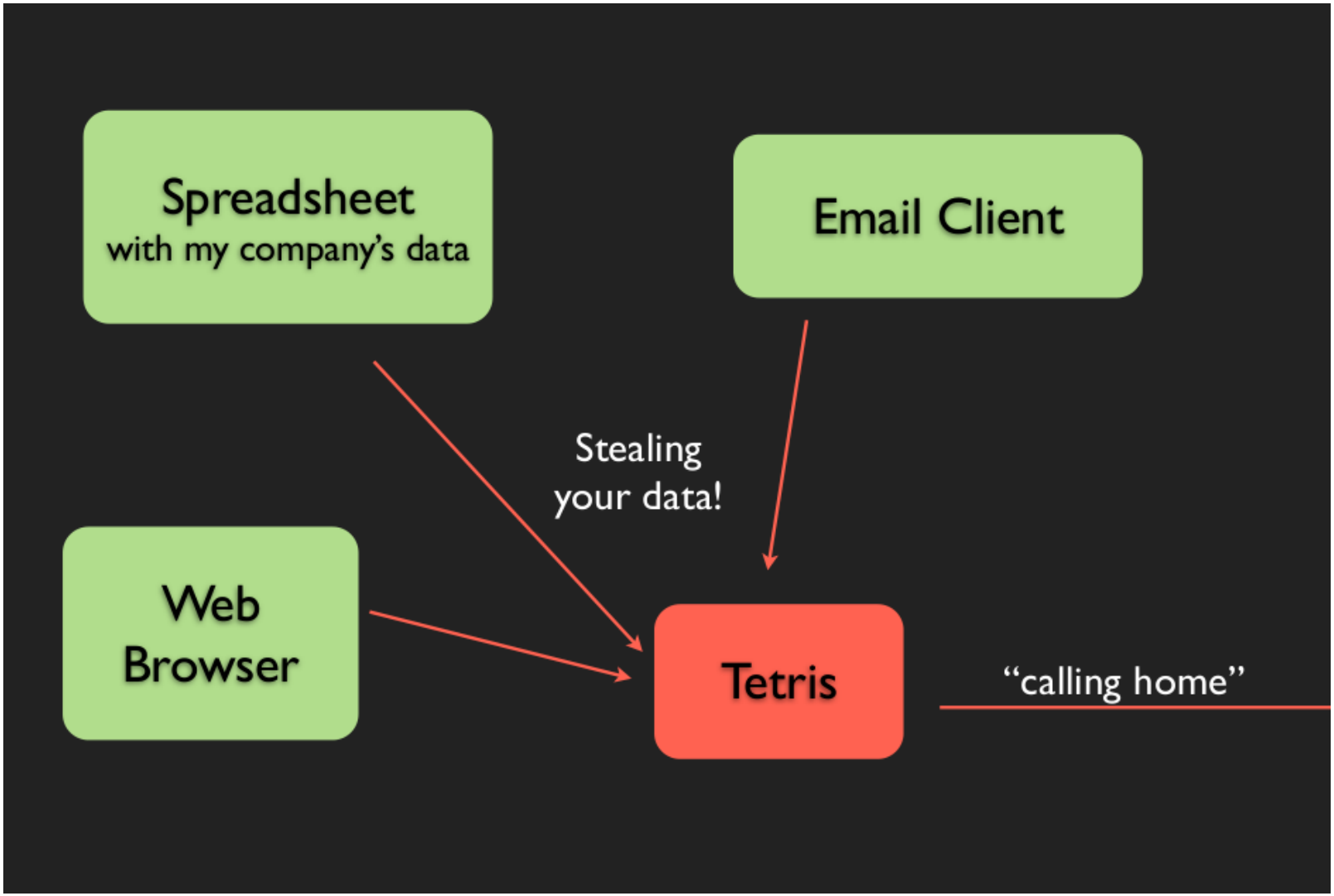
Dehát erre való egy számítógép, nem?

De mi van akkor, ha az egyik alkalmazás mást is csinál, mint amit mond magáról?

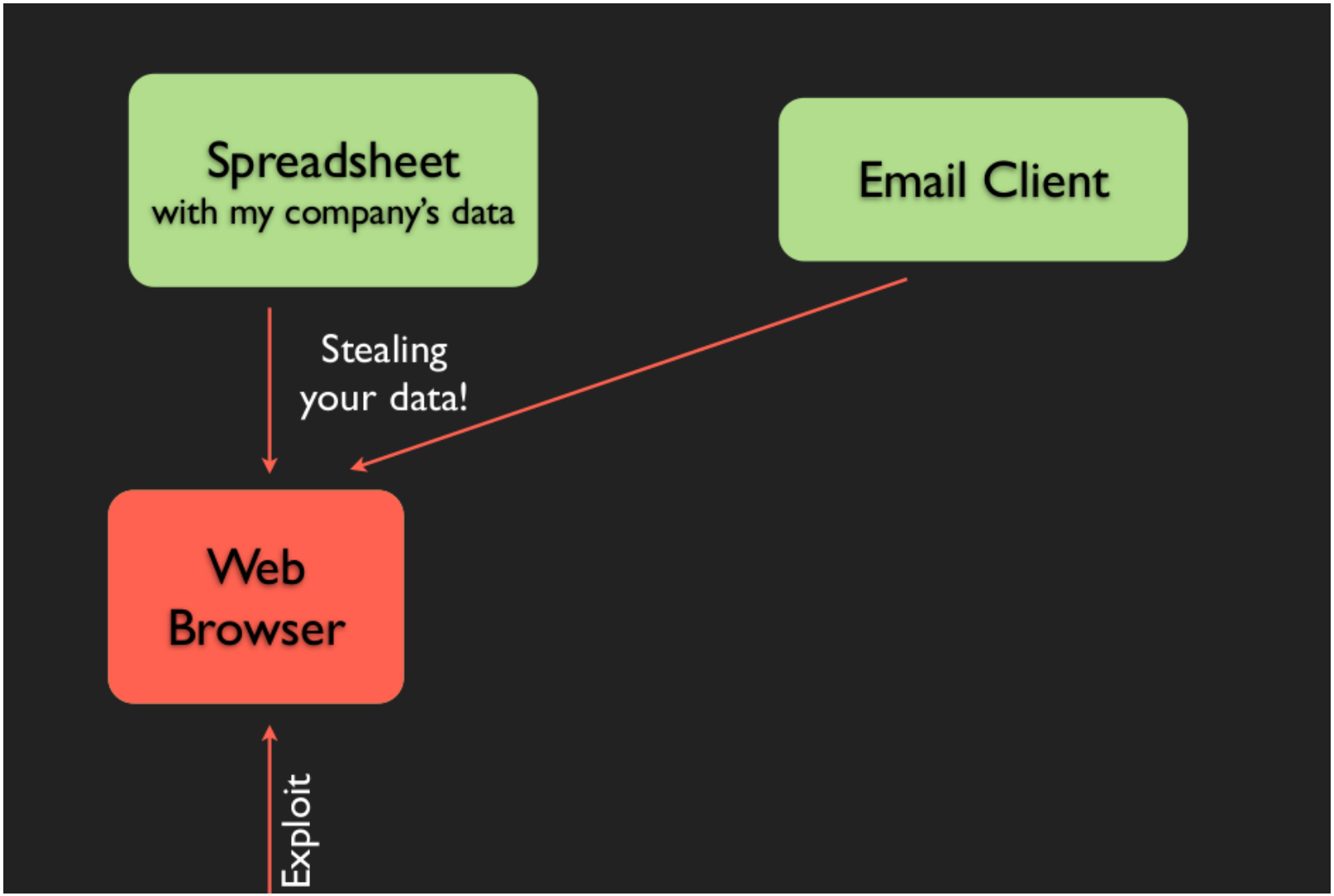
Természetesen mindenki más és más alkalmazásokat használ, és várhatóan többet is egyszerre.

Dehát erre való egy számítógép, nem?

De mi van akkor, ha az egyik alkalmazás mást is csinál, mint amit mond magáról?


Spreadsheet
with my company's data
Email Client
Stealing
your data!
Web
Browser
Tetris
"calling home"

Vagy, ha az egyik jól ismert alkalmazásunk mondjuk egy vírussal fertőzött?


Spreadsheet
with my company's data
Email Client
Stealing
your data!
Web
Browser
Exploit

Hát, ez gáz!

Mi lehet a megoldás?

- Hibátlan kód? ;)
- Izoláció!

- Fejlesztők oktatása
- Kód audit
- Tesztelés
- ISO szabványok

- Fejlesztők oktatása
- Kód audit
- Tesztelés
- ISO szabványok

- Fejlesztők oktatása
- Kód audit
- Tesztelés
- ISO szabványok

- Fejlesztők oktatása
- Kód audit
- Tesztelés
- ISO szabványok

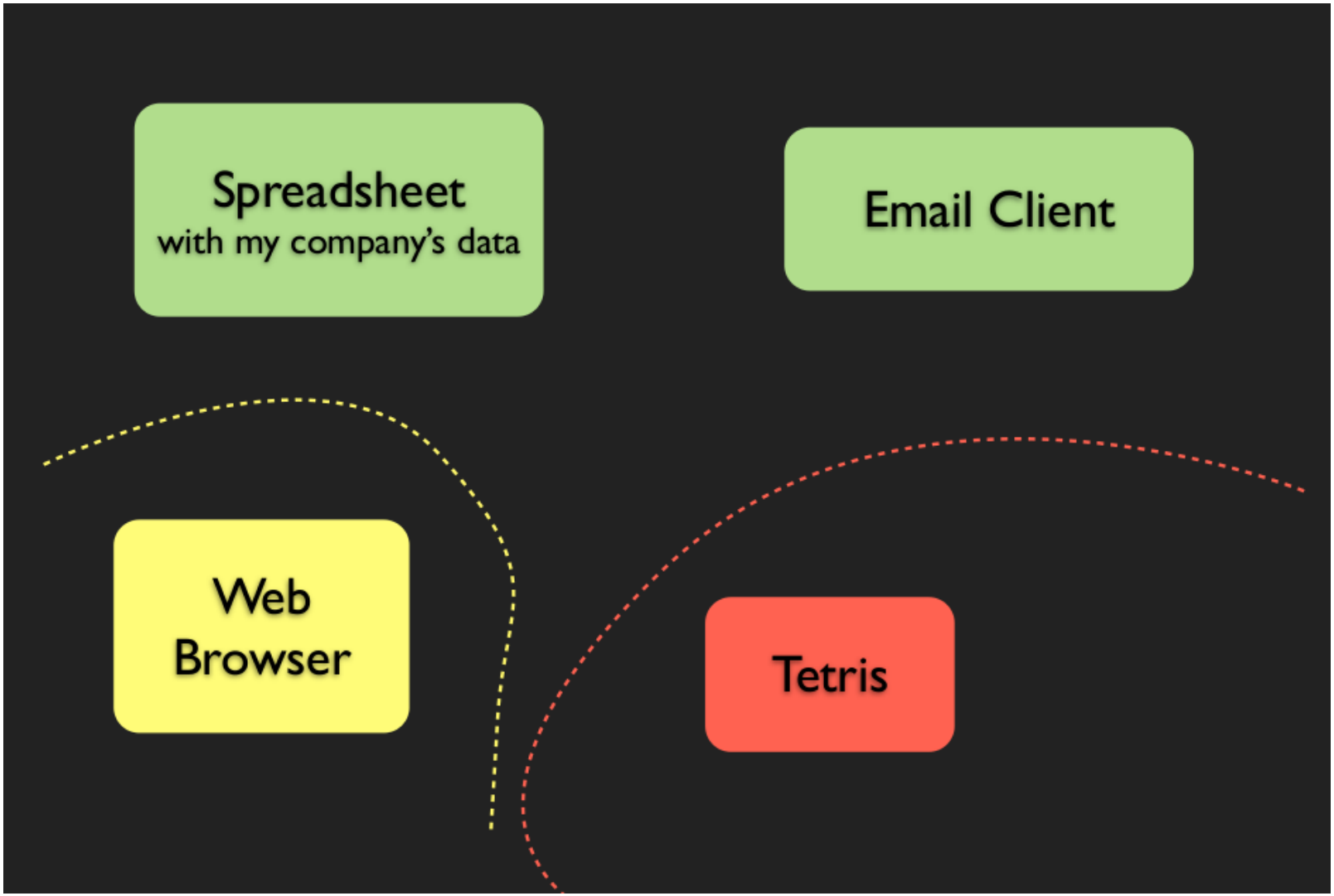
Ez mind szép és hasznos dolog...

...de a gyakorlatban nem működik!

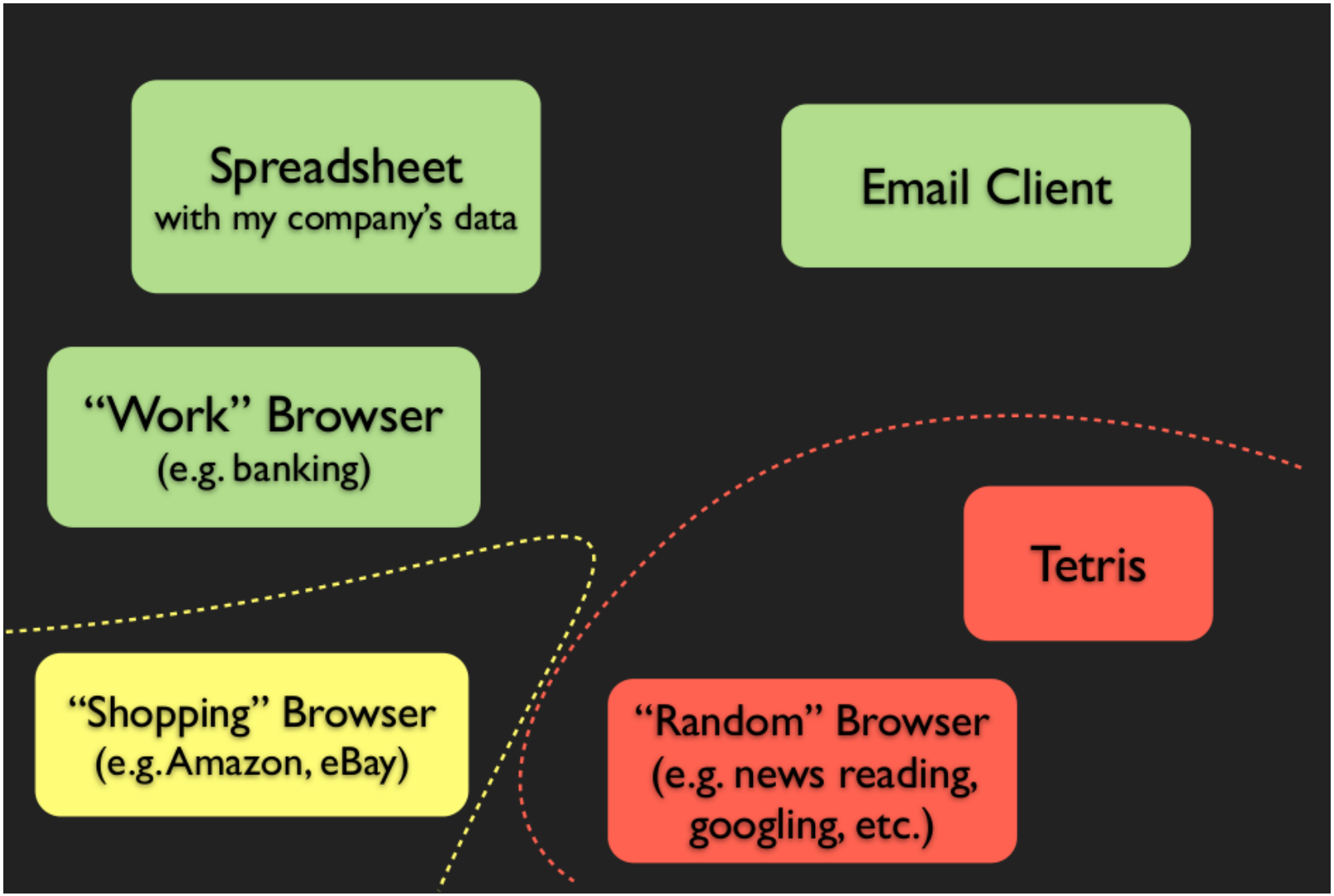
Ez mind szép és hasznos dolog...

...de a gyakorlatban nem működik!

Mi azt várnánk el egy operációs rendszertől, hogy a lehető legjobban elválassza el az alkalmazásokat egymástól, mert biztosan van közöttük nem megbízható vagy akár fertőzött/feltört is...


Spreadsheet
with my company's data
Email Client
Web
Browser
Tetris

Sőt, ha ennél is messzebb megyünk, vannak olyan alkalmazások, amiken belül további szeparációra lenne szükség...


Spreadsheet
with my company's data
Email Client
"Work" Browser
(e.g. banking)
Tetris
"Shopping" Browser
(e.g. Amazon, eBay)
"Random" Browser
(e.g. news reading,
googling, etc.)

Jogosan merülhet fela a kérdés, hogy:

A mai modern operációs rendszerek mindegyike támogat valamilyen szintű izolációt, nem?

- Address space isolation
- User account isolation
- Advanced ACL-ek
- Kernel/User mode separation

Mi is a baj akkor ezekkel?

Ezek sajnos nem működnek a gyakorlatban.

Azért nem, mert mindegyik egy monolitikus kernel-re épül, ami önmagában sem megbízható, és főleg nem hibamentes!

Nem is lehet hibamentes, ha akár több száz külső drivert is tartalmazhat!

Egyetlen bug elég a kernelben, ami megboríthatja az operációs rendszer összes biztonsági mechanizmusát!

Ezek sajnos nem működnek a gyakorlatban.

Azért nem, mert mindegyik egy monolitikus kernel-re épül, ami önmagában sem megbízható, és főleg nem hibamentes!

Nem is lehet hibamentes, ha akár több száz külső drivert is tartalmazhat!

Egyetlen bug elég a kernelben, ami megboríthatja az operációs rendszer összes biztonsági mechanizmusát!

Ezek sajnos nem működnek a gyakorlatban.

Azért nem, mert mindegyik egy monolitikus kernel-re épül, ami önmagában sem megbízható, és főleg nem hibamentes!

Nem is lehet hibamentes, ha akár több száz külső drivert is tartalmazhat!

Egyetlen bug elég a kernelben, ami megboríthatja az operációs rendszer összes biztonsági mechanizmusát!

Ezek sajnos nem működnek a gyakorlatban.

Azért nem, mert mindegyik egy monolitikus kernel-re épül, ami önmagában sem megbízható, és főleg nem hibamentes!

Nem is lehet hibamentes, ha akár több száz külső drivert is tartalmazhat!

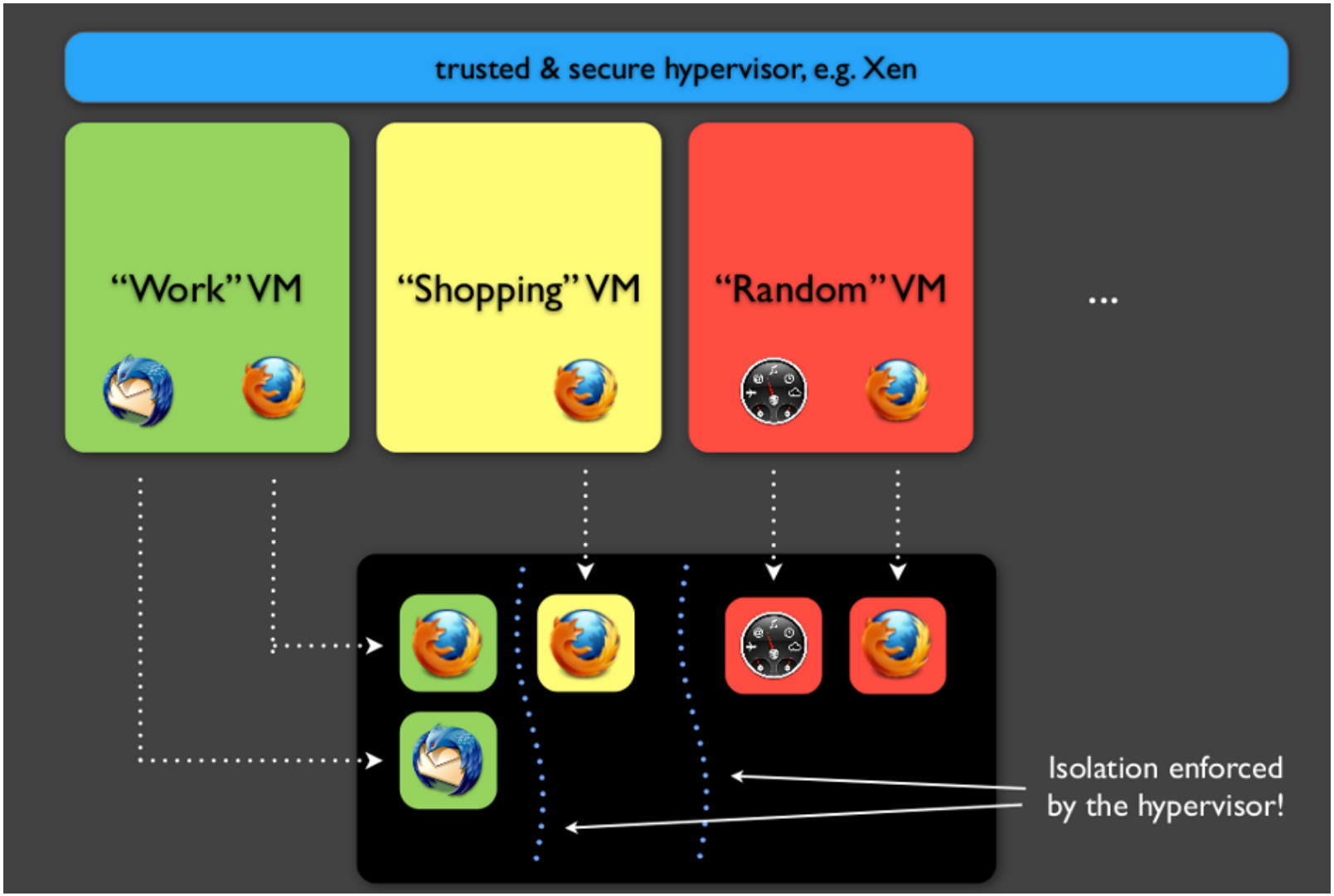
Egyetlen bug elég a kernelben, ami megboríthatja az operációs rendszer összes biztonsági mechanizmusát!

Nekünk valami ennél sokkal jobb megoldás kell!

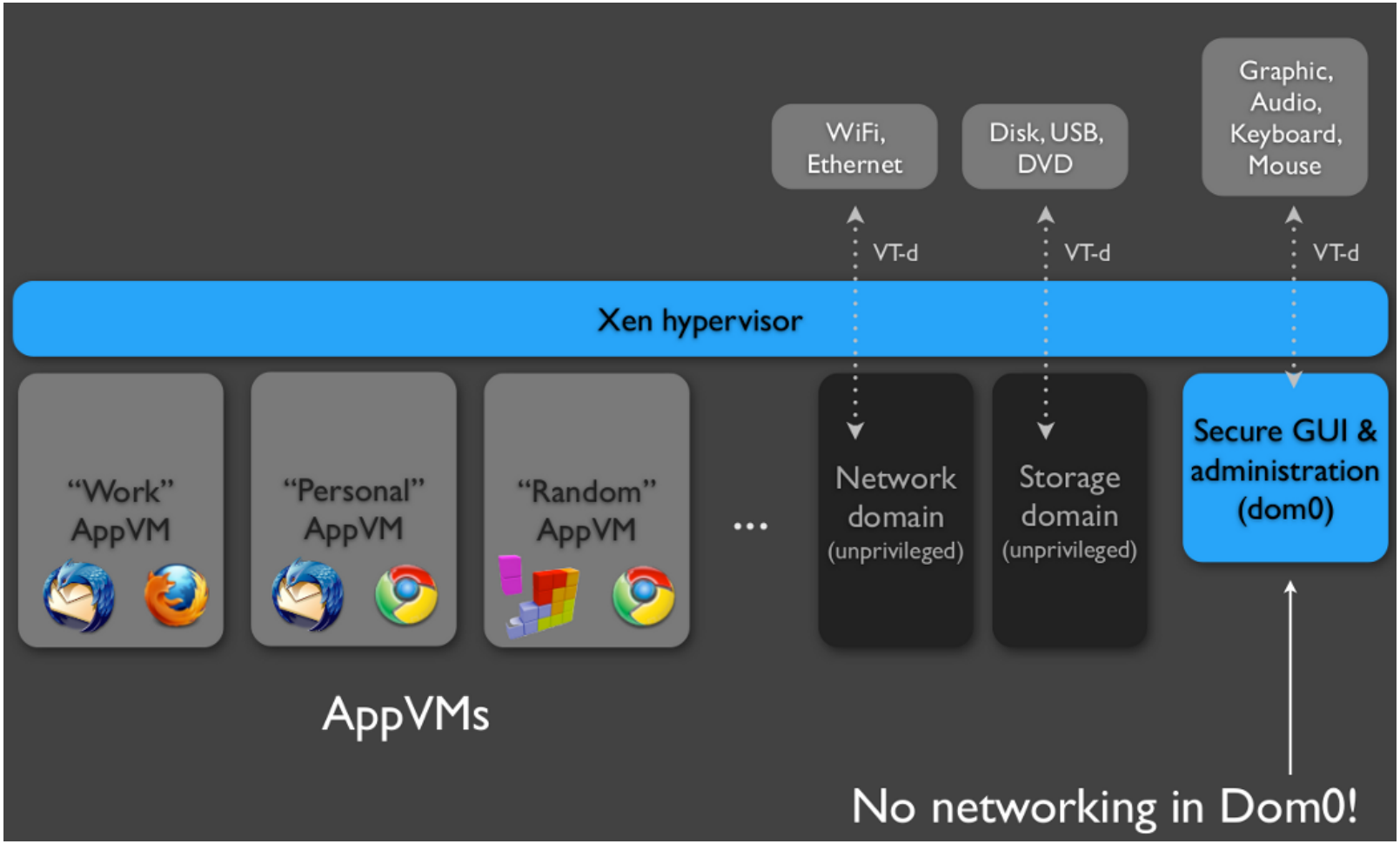
Qubes OS

Válaszuk el az operációs rendszer kerneleit az izolációt biztosító kódtól!

Qubes OS


trusted & secure hypervisor, e.g. Xen
"Work" VM
"Shopping" VM
"Random" VM
...
Isolation enforced
by the hypervisor!

Qubes OS


WiFi, Ethernet
Disk, USB, DVD
Graphic, Audio, Keyboard, Mouse
VT-d
VT-d
VT-d
Xen hypervisor
"Work" AppVM
"Personal" AppVM
"Random" AppVM
...
Network domain (unprivileged)
Storage domain (unprivileged)
Secure GUI & administration (dom0)
AppVMs
No networking in Dom0!

http://qubes-os.org

Köszönöm a figyelmet

http://qubes-os.org

Köszönöm a figyelmet