SAFE-OS: A Secure and Usable Desktop Operating System

**François Lesueur, Ala Rezmerita, Thomas Hérault,
Sylvain Peyronnet and Sébastien Tixeuil**

`http://safe-os.lri.fr`

LRI, University Paris-Sud, France

Université Pierre et Marie Curie, Sorbonne Universités, France

CRiSIS, October 12 2010

Montréal, Québec, Canada

Security in Operating Systems

Computer security

- Protection : Programming secured software
- Detection : Monitoring vulnerabilities
- Containment : Isolating attacks

Containment of applications

- Mandatory for security purpose (vulnerabilities)
- Full containment is incompatible with usability

Basics of SAFE-OS

Isolation of applications for server systems

- Services hosted on different servers
- Usage of virtualization
- Mostly network interactions

SAFE-OS

- Virtualization security for desktop systems
- Innovative assembly of well-known softwares

Challenges

Interactions among applications

- Editing a downloaded file
- Emailing a locally generated document

⇒ Enable specific interactions between isolated applications

User interface

- Unified user interface
- Usability is the key point

⇒ Provide the same interface as in an ordinary OS

Outline

1. Related Work
2. Architecture
3. Data Transfers
4. Evaluation

Outline

1. **Related Work**
   - Kernel-Based Containment
   - Virtualization-Based Containment
2. Architecture
3. Data Transfers
4. Evaluation

Kernel Security

Security policies

- DAC policies : no isolation of a corrupted application
- MAC policies (SELinux, TOMOYO, AppArmor) : complex policies for each application

Vulnerability to kernel attacks (SECUNIA : 435 vulnerabilities against Linux 2.6.x since 2004 [1])

[1] http://secunia.com/advisories/product/2719/?task=statistics

Virtualization for desktop OS

Usages

- Protection of sensitive data (SVFS, Storage Capsules)
  ⇒ only for files, no protection for interactions (i.e., bank sessions)
- Complete isolation (NetTop)
  ⇒ full containment, no interactions between VMs
- Desktop solutions (Bitfrost, Qubes OS)
  ⇒ several VMs, unified interface, some interactions, but no fine grained control on VMs

SECUNIA : 17 vulnerabilities against Xen 3.x since 2007 [2]

[2] http://secunia.com/advisories/product/15863/?task=statistics

SAFE-OS

SAFE-OS

- Desktop OS using virtualization
- Protects interactions of applications (i.e., bank sessions)
- Allows necessary communications between VMs
- Fine-grained control on VMs capabilities

Outline

1. Related Work
2. **Architecture**
   - Containment through Virtualization
   - Interfaces
   - Appliances
3. Data Transfers
4. Evaluation

Virtualization characteristics

Different VMs on a single machine

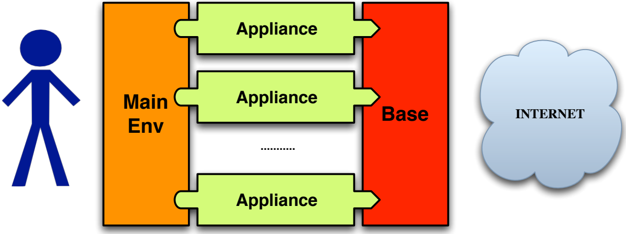
- Virtualized hardware (memory, hard disk, network card, . . .)
- Each VM runs its own OS
- Total isolation among VMs

Containment of attacks

- VMs are isolated
- Corruption of 1 VM does not allow to corrupt others
- 0-day / Kernel vulnerabilities are contained in the attacked VM

For instance, an 0-day targeting a web browser in a VM cannot alter a mail reader in another VM.

SAFE-OS Architecture



- Applications are run in VMs *Appliances*
- Network access is controlled by the VM *Base*
- User interactions is achieved through the VM *Main Env*

Base : VM/World communication enforcer

- Communication policy among VMs
- Communication policy between appliances and internet
- Applicative firewall with specific hooks

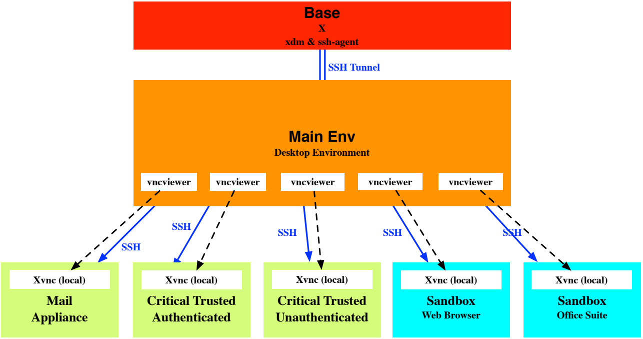
- Xen *dom0*
- Only VM connected directly to internet
- Every communication goes through the Base (filtering)
- Invisible to the user

Main Env : VM/User communication center

- Interface between appliances and user
- Only VM the user has access to
- Control and display of every appliance
- Abstraction of the different appliances

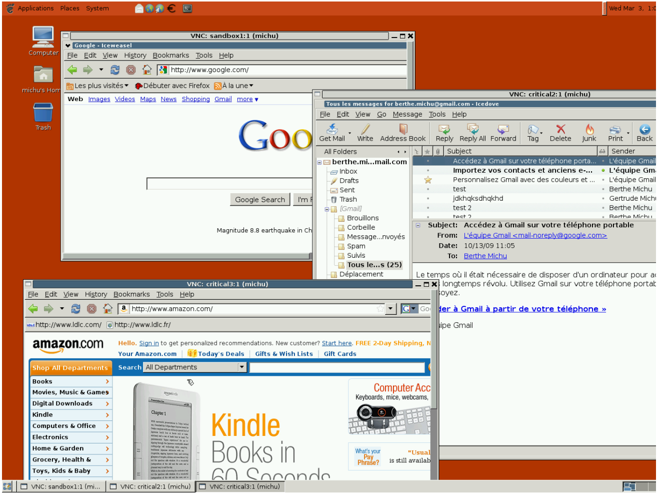
⇒ The user has no knowledge of the underlying complexity

Control and display of applications



- SSH is used to launch applications/Xvnc inside other VMs
- VNC is used to display and interact with applications

SAFE-OS user interface


Applications Places System
Wed Mar 3, 1:0
Computer
michu's Hom
Trash
VNC: sandbox1:1 (michu)
Google - Iceweasel
File Edit View History Bookmarks Tools Help
http://www.google.com/
Les plus visités ▾ Débuter avec Firefox À la une ▾
Web Images Videos Maps News Shopping Gmail more ▾
Goo
Google Search I'm F
Magnitude 8.8 earthquake in Ch
VNC: critical2:1 (michu)
Tous les messages for berthe.michu@gmail.com - Icedove
File Edit View Go Message Tools Help
Get Mail Write Address Book Reply Reply All Forward Tag Delete Junk Print Back
All Folders
berthe.mi...mail.com
Inbox
Drafts
Sent
Trash
[Gmail]
Brouillons
Corbeille
Message...nvoyés
Spam
Suivis
Tous le...s (25)
Déplacement
Subject
Sender
VNC: critical3:1 (michu)
File Edit View History Bookmarks Tools Help
http://www.amazon.com/
http://www.ldlc.com/ http://www.ldlc.fr/
amazon.com
Hello. Sign in to get personalized recommendations. New customer? Start here. FREE 2-Day Shipping, N
Your Amazon.com Today's Deals Gifts & Wish Lists Gift Cards
Shop All Departments Search All Departments
Books
Movies, Music & Games
Digital Downloads
Kindle
Computers & Office
Electronics
Home & Garden
Grocery, Health &
Toys, Kids & Baby
Kindle
Books in
60 Seconds
Computer Acc
Keyboards, mice, webcams,
What's your Pay Phrase?
"Usual
is still availab
VNC: sandbox1:1 (mi... VNC: critical2:1 (michu) VNC: critical3:1 (michu)

Subject	Sender
Accédez à Gmail sur votre téléphone porta...	L'équipe Gmail
Importez vos contacts et anciens e-...	L'équipe Gm
Personnalisez Gmail avec des couleurs et ...	L'équipe Gmail
test	Berthe Michu
jdkhqksdhqkhd	Gertrude Mich
test 2	Berthe Michu
test 2	Berthe Michu

Subject: Accédez à Gmail sur votre téléphone portable
From: L'équipe Gmail <mail-noreply@google.com>
Date: 10/13/09 11:05
To: Berthe Michu

Le temps où il était nécessaire de disposer d'un ordinateur pour a
longtemps révolu. Utilisez Gmail sur votre téléphone portab
soyez.

der à Gmail à partir de votre téléphone »

iipe Gmail

Appliances : User service providers

- Each appliance provides a specific service
- Autonomous VM running a minimalistic OS
- Plugged into the Base (security module)
- Plugged into the Main Env (shortcuts, display)

- Execution is contained in appliances : attacks too
- Control and display through the Main Env
- Internet communications through the Base

Preconfigured appliances

Critical appliances

- Mail
- Trusted authenticated websites, only `https` (taxes, bank)
- Trusted but unauthenticated websites, `https+http` (e-selling)

Sandboxes

- Untrusted websites
- Office applications

Mail Appliance 1/3

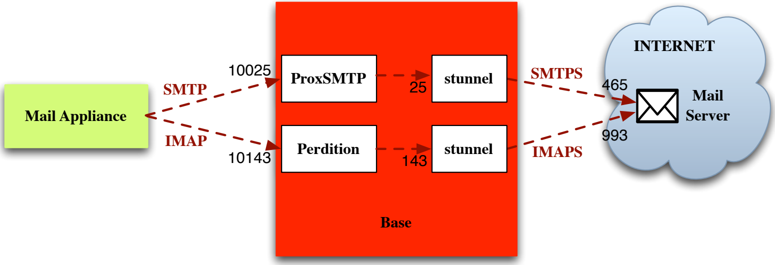
Aim : no information leakage even if corrupted

- Only allowed to access mail services
- Tightened to the user's IMAP account
- Sent mail were explicitly allowed by the user

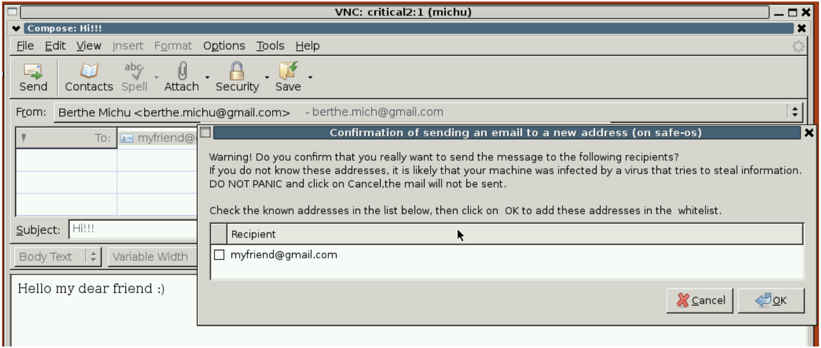
Solution : dom0 applicative firewall (*security module*)

- Runs in *dom0*
  ⇒ Protected from corruptions originating in mail appliance
  ⇒ Can filter every communication from mail appliance
- Allows only IMAPS/SMTPS to configured server with configured username
- Asks the user whether he indeed sent a mail to the recipients

Mail Appliance 2/3



Mail Appliance 3/3


VNC: critical2:1 (michu)
Compose: Hi!!!
File Edit View Insert Format Options Tools Help
Send Contacts Spell Attach Security Save
Body Text Variable Width
Cancel OK

From: Berthe Michu <berthe.michu@gmail.com> - berthe.mich@gmail.com

To: myfriend@

Subject: Hi!!!

Hello my dear friend :)

Confirmation of sending an email to a new address (on safe-os)

Warning! Do you confirm that you really want to send the message to the following recipients?
If you do not know these addresses, it is likely that your machine was infected by a virus that tries to steal information.
DO NOT PANIC and click on Cancel,the mail will not be sent.

Check the known addresses in the list below, then click on OK to add these addresses in the whitelist.

	Recipient
□	myfriend@gmail.com

Trusted Authenticated Websites Appliance

Aim : Communicate only with trusted servers

- Only `https` with *valid* certificates
- Connects only to some whitelisted websites (taxes, banks)

Solution : Whitelisting proxy and *dom0* firewall

- Proxy runs in the appliance
  ⇒ Only connects to trusted servers so remains clean
- Firefox tweaked to deny security exceptions
- *dom0* firewall only allows `https` and `DNS`

Trusted but Unauthenticated Websites

Appliance

Aim : Communicate only with trusted servers, *best effort*

- Some websites require `http` before `https` (e-selling)
- Connects only to some whitelisted websites
- Vulnerability during the `http` part

Solution : Whitelisting proxy and *dom0* firewall

- Proxy runs in the appliance
  ⇒ Only connects to trusted servers so remains clean
- Firefox tweaked to deny security exceptions
- *dom0* firewall only allows `https`, `http` and `DNS`

Sandboxes

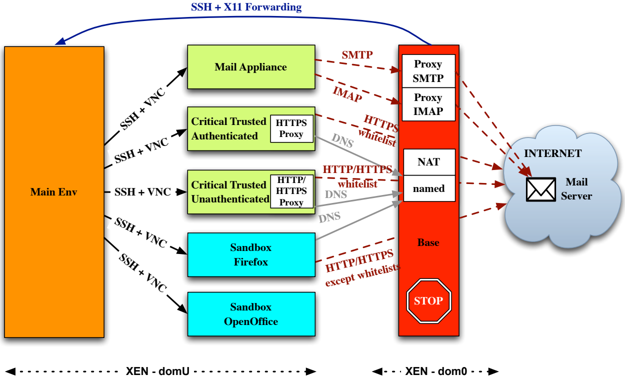
Untrusted websites

- `http`, `https` and `DNS` access to everywhere
- Easy restoration to initial state

Office applications

- OpenOffice.org, xpdf, . . .
- No internet access at all
- Easy restoration to initial state

Communication details



Outline

1 Related Work

2 Architecture

3 **Data Transfers**
- Problem
- Proposed solution

4 Evaluation

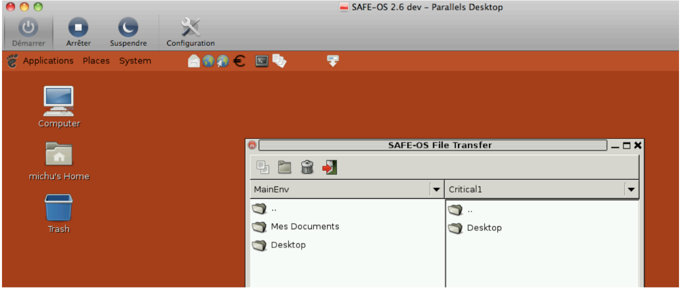
Limitations of virtualization

- Each application runs in its own VM
- Each VM has its own filesystem

⇒ The user must be able to share documents between applications

A data transfer tool

- Graphical tool to copy files between appliances
- Executed in the Main Env
- Uses `sftp` to do the actual transfers
- Only copies what user explicitly asks to !



Outline

1. Related Work
2. Architecture
3. Data Transfers
4. **Evaluation**

Security

Interactions between VMs

- Xen : careful design, less code than a Linux kernel
- VNC : only used to *display* applications
- SSH : highly secured software

Resilience

- Base (dom0) runs few services
- Base can restore all other VMs to a safe state

Benchmarking

	Reference	SAFE-OS
Boot time (seconds)	42.6	107.3
Cold Firefox launch (seconds)	5.9	11.4
Warm Firefox launch (seconds)	1.5	5.2
CSS (ms)	53.3	54
SunSpider (ms)	3821	3859

- Some optimizations needed at boot time
- Applications are not noticeably slowed down

SAFE-OS

Characteristics of SAFE-OS

- Secure desktop OS
- Security based on Xen virtualization
- Interface similar to the one of a standard OS

Composition

- Base : Communication policy
- Main Env : Interactions with the user
- Appliances : Isolation of applications

Available online !

- Developped for the French ANR challenge SEC&SI
- Image files at `http://safe-os.lri.fr`

SAFE-OS: A Secure and Usable Desktop Operating System

François Lesueur, Ala Rezmerita, Thomas Hérault,
Sylvain Peyronnet and Sébastien Tixeuil

`http://safe-os.lri.fr`

LRI, University Paris-Sud, France

Université Pierre et Marie Curie, Sorbonne Universités, France

CRiSIS, October 12 2010

Montréal, Québec, Canada