

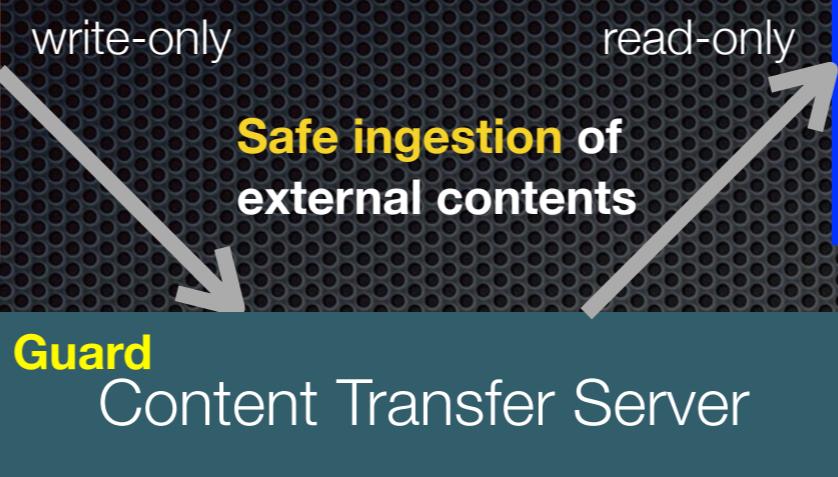
# Securing networks through compartmentalisation

Considerations for various approaches

What is  
compartmentalisation?

Internet Zone

Intranet Zone



Past

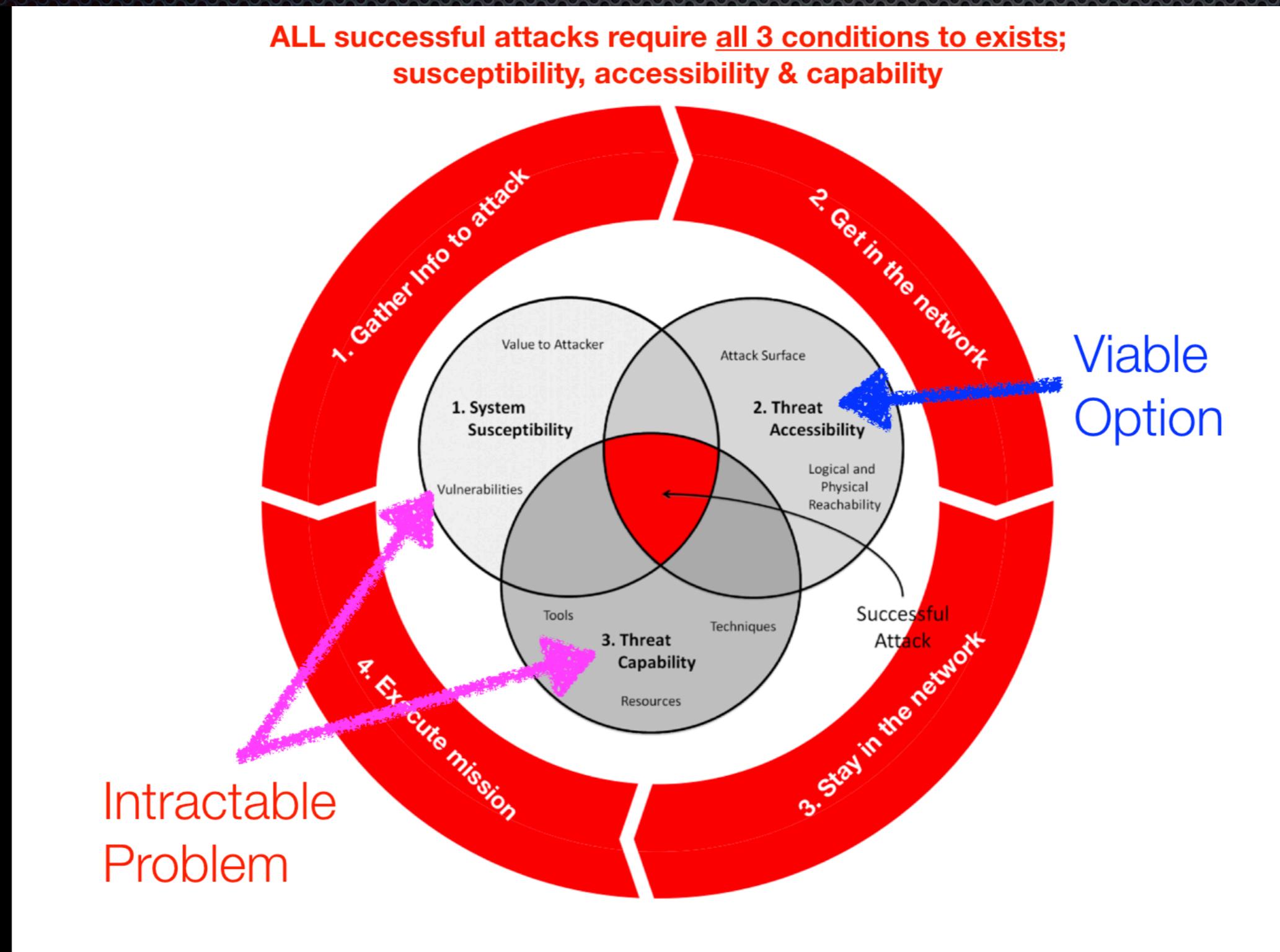


Present

Future



# Why Compartmentalise?



# 3 Requirements of Attack easily met in most environments

- Attackers have **free tools** found on Internet (eg. Github for malware source-code, Youtube for tutorials, Forums for support)
- Modern Operating Systems & Applications are **complex** & have too much functionalities to attackers' advantage
- **Susceptible devices have two paths**; one to the Internet (attackers use to reach us) and other to Intranet (every device becomes a pivot point)

# Why Limiting Threat Accessibility is viable?

- When devices have dual paths, attacks just need to get it right once but your security products & posture needs to constantly keep up with existing & new vulnerabilities
- Compartmentalisation when implemented right, increases cost-of-attack; have to get nearer to the target environment instead of remotely launching attacks; harder to exploit existing vulnerabilities directly

# What good is the Internet?

Do **ALL** users need Internet & for what?

- Receive contents from external partners
- Assimilate useful public contents (eg. Text, Graphics) into internal work
- Access some cloud-based services
- External communications (eg. Web conferences)

# Why is Compartmentalisation better?

- **Isolation** from Internet; increase cost-of-attacks eg. planting backdoors, malicious infections
- Limits damages from intrusions, **if Internet Zone only holds public contents.** Nothing much to steal if attackers are stuck within Internet zone
- Limits illegitimate flow of information out of intranet (eg. Insider Threats)

# Considerations for Type 2 Hypervisors Isolation

# What is Type 2 Hypervisor?

- Runs **V**irtual **M**achine within another interactive Host **O**perating **S**ystems like Windows & MacOS
- **Savvy** home users surf with Internet VM to keep malware out
- **Versus Type 1 hypervisor which has better isolation but need server class machines**
- Good for home use, not suitable for Enterprise setting
- Why?

# Key Considerations

- Usability for non-technical users
- Type 2 hypervisor vulnerability management
- File transfer monitoring
- Shift of work-space => more sensitive contents in VM

# How about non-techie users?

- Not every user is tech-savvy
- Storage management for snap-shots  
(forget to snap-shot, running out-of-space...)



# How about vulnerability management?

■ More than one machine to manage

**EXPLOIT DATABASE**

Home    Exploits    Shellcode    Papers    Google Hacking Database    Submit    Search

## Search the Exploit Database

Search the Database for Exploits, Papers, and Shellcode. You can even search by **CVE** and **OSVDB** identifiers.

virtualbox

I'm not a robot

reCAPTCHA  
Privacy - Terms

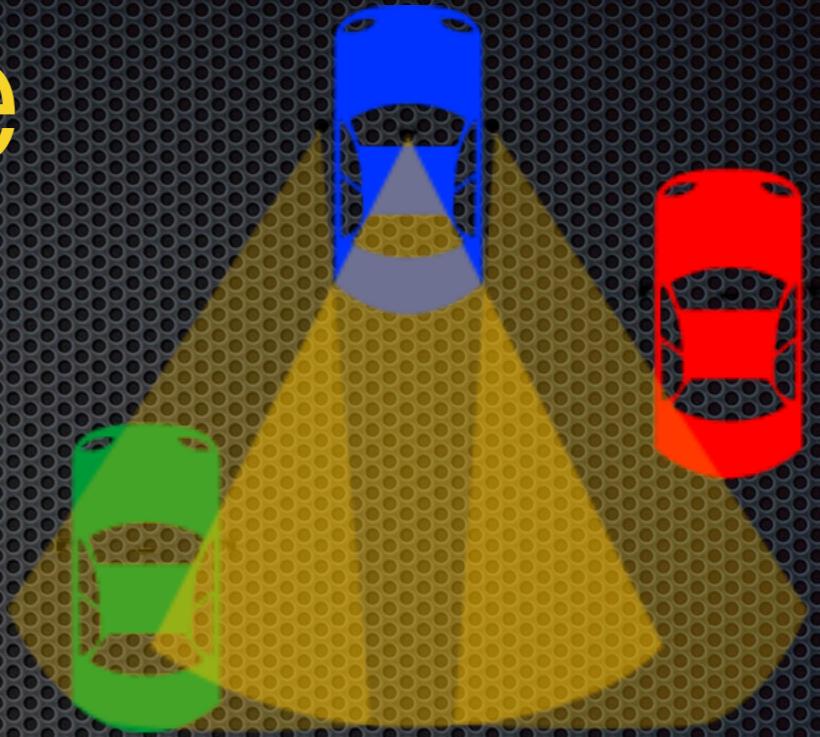
Search

More Options

20 total entries

Date	D	A	V	Title	Platform	Author
2017-08-03	⬇️	-	✓	VirtualBox 5.1.22 - Windows Process DLL Signature Bypass Privilege Escalation	Windows	Google Secu...
2017-08-03	⬇️	-	✓	VirtualBox 5.1.22 - Windows Process DLL UNC Path Signature Bypass Privilege Escalation	Windows	Google Secu...
2017-04-25	⬇️	-	✓	Oracle VirtualBox Guest Additions 5.1.18 - Unprivileged Windows User-Mode Guest Code...	Multiple	Google Secu...
2017-04-20	⬇️	-	✓	Oracle VM VirtualBox 5.0.32 r112930 (x64) - Windows Process COM Injection Privileg...	Win_x86-64	Google Secu...
2017-04-20	⬇️	-	✓	Oracle VM VirtualBox - Environment and ioctl Unprivileged Host User to Host Kernel...	Multiple	Google Secu...
2017-04-20	⬇️	-	✓	Oracle VM VirtualBox - 'virtio-net' Guest-to-Host Out-of-Bounds Write	Multiple	Google Secu...
2017-04-20	⬇️	-	✓	Oracle VM VirtualBox 5.1.14 r112924 - Unprivileged Host User to Host Kernel Privileg...	Linux	Google Secu...
2017-04-20	⬇️	-	✓	Oracle VM VirtualBox - Guest-to-Host Privilege Escalation via Broken Length Handling in...	Multiple	Google Secu...
2017-03-13	⬇️	-	✓	Oracle VM VirtualBox - Cooperating VMs can Escape from Shared Folder	Linux	Google Secu...
2017-01-27	⬇️	-	⌚	Oracle VM VirtualBox < 5.0.32 / < 5.1.14 - Privilege Escalation (PoC)	Linux	Wolfgang Ho...
2016-10-21	⬇️	-	✓	Oracle VM VirtualBox 4.3.28 - '.ovf' Crash (PoC)	Windows	sultan alba...
2014-08-14	⬇️	📅	✓	Oracle VM VirtualBox 4.3.6 - 3D Acceleration Virtual Machine Escape (Metasploit)	Win_x86-64	Metasploit
2014-08-13	⬇️	⌚	✓	Oracle VM VirtualBox Guest Additions 4.3.10r93012 - 'VBoxGuest.vsd' Privilege Escalation	Windows	Metasploit

# How to monitor file transfers?



- Freeware are **not** enterprise ready
- No logging; drag-&-drop **convenient** for users but night-mare for security monitoring operations
- No central management to enforce **control-policies**
- Malware infection (dragged-out of VM) & Data leakage (dragged-into VM) becomes harder to detect with extra loop-holes via VMs

# Sensitive contents creation in Internet VM?

- More flexibility within Internet VM means higher chance of doing all the work there
- Back to square one



# Considerations for Two Separate Fleets

# Two separate fleets/zones

- One for Internet usage, the other for Intranet
- Better isolation than VMs
- Also has unintended consequences

# Key Considerations

- File transfer between zones
- Management & monitoring of two or more zones
- Usability, logistics & other hidden costs

# File Transfer Challenge



- End up with more USB storage
- Are whitelisted USB drives are “clean”?
- How about losing USB drives with sensitive contents?



# Managing & Monitoring Internet Zone

- More flexibility within Internet VM means higher chance of creating contents; defeats the purpose...
- Need to harden, patch...



# Usability, Logistics & Hidden Costs

- More USB devices, patching, hardening & logging configuration
- **K**eyboard **V**ideo **M**ouse switches for multiple sets of monitors, mouse & keyboard
- Multiple devices **cumbersome** for mobile/traveling executives

# Desirable Properties

## Desirable Properties

Strong Isolation without hassle of logistics & hidden costs

Centrally managed policies, supports security monitoring

Personal Internet kiosk, safe content consumption only

User-friendly, controlled & monitored content transfers

Insider Threat Deterrence

## Black-PC/Laptop

Type 1 hypervisor + hardware based isolation 

Central management & logging 

Hardened, read-only Internet VM that is roll-back friendly 

User-friendly safe content transfers between zones 

Hardware monitoring 