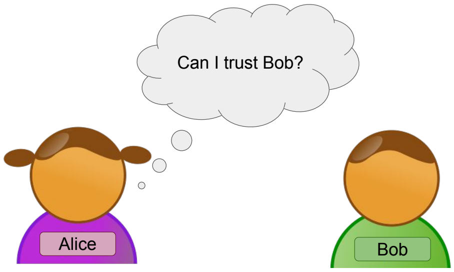
OS Security

COMP 435
Fall 2017
Prof. Cynthia Sturton

Trust Terminology

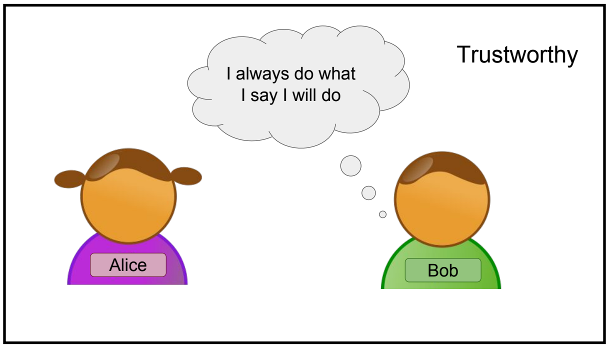
- Trust
- Trusted system
- Trustworthiness
- Trusted Computing Base

Trust

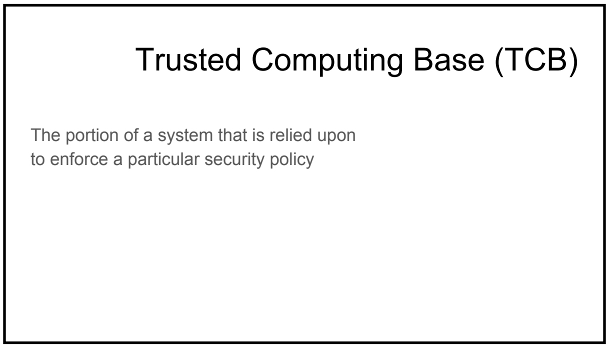


Trusted System

A system believed to enforce a security specification
to a given level of assurance

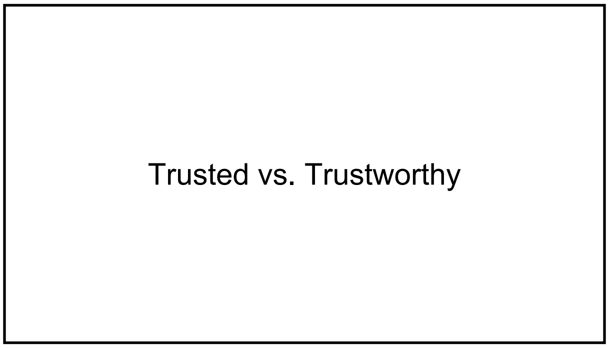


Trustworthy

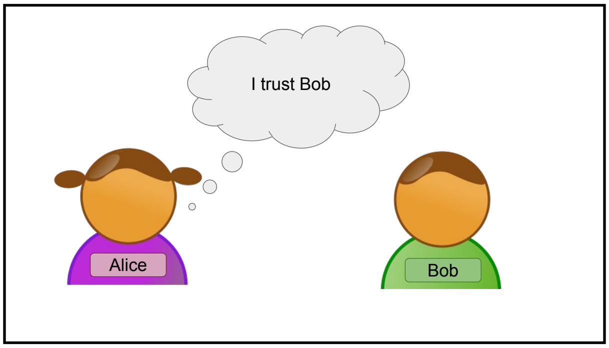


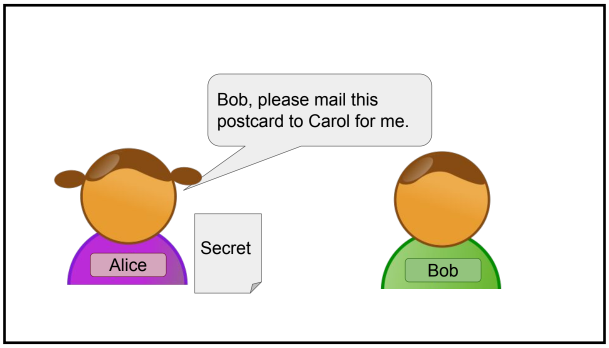
Trusted Computing Base (TCB)

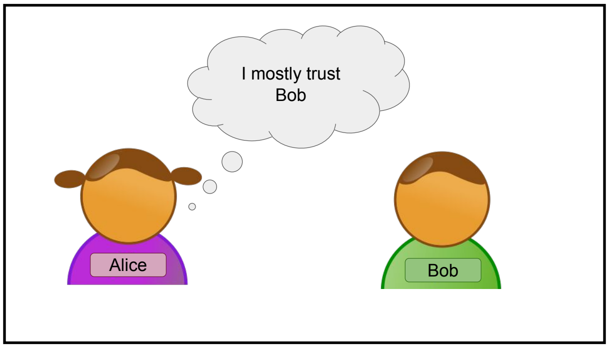
The portion of a system that is relied upon
to enforce a particular security policy

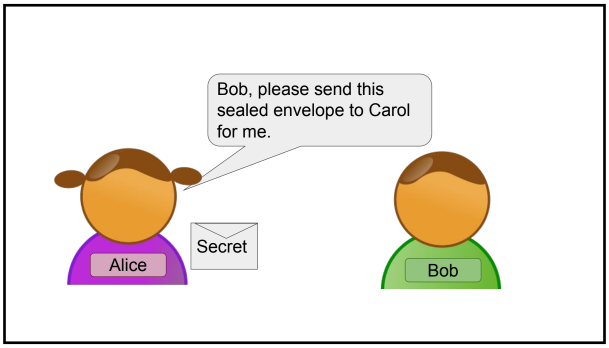


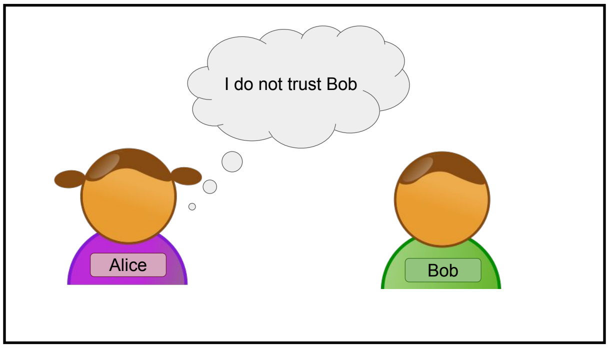
Trusted vs. Trustworthy

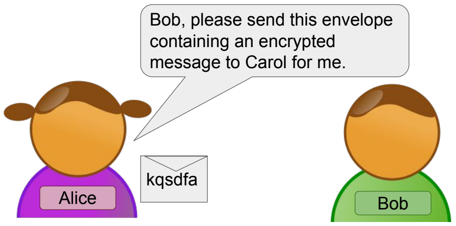



Bob, please mail this postcard to Carol for me.
Secret
Alice
Bob

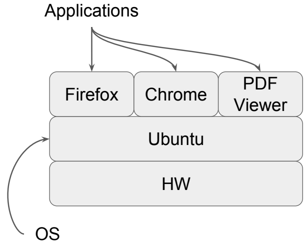

I mostly trust Bob
Alice
Bob


Bob, please send this sealed envelope to Carol for me.
Secret
Alice
Bob


I do not trust Bob
Alice
Bob


Bob, please send this envelope containing an encrypted message to Carol for me.
kqsdfa
Alice
Bob

Trusted Computing Base (TCB)

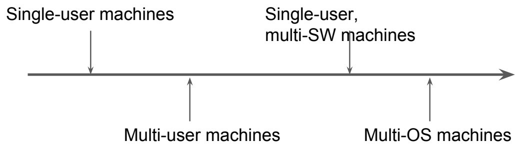


Operating Systems

OS Responsibilities

- Provide HW interface
- Manage resources
- Mediate interprocess communication
- Protect itself
- Provide user authentication

Timeline of OS Requirements



Single-user machines

Multi-user machines

Single-user,
multi-SW machines

Multi-OS machines

Separation

- Physical
- Temporal
- Logical
- Cryptographic

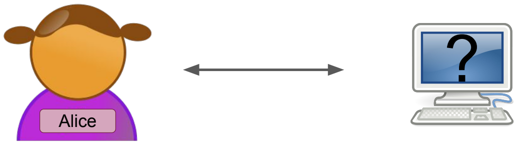
Memory Protection

- Fence
- Base--Bounds registers
- Tagged architecture
- Virtual memory
  - Segmentation
  - Paging

Trusted Path

Trusted line of communication between user and application

Trusted Path



Secure Startup

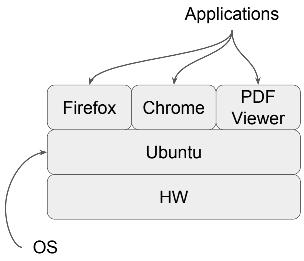
System must start from a known secure point

Virtualization

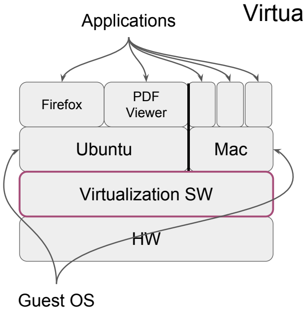
Virtualization

- Non-interference
- Simulation
- Sandboxing
- Honeypots

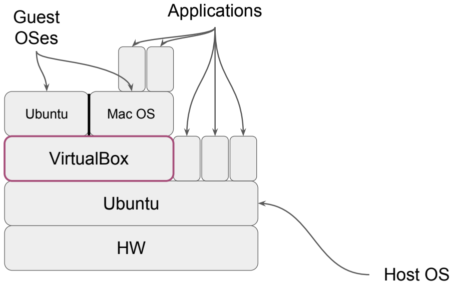
My Machine



Virtual Machines: Bare Metal



Virtual Machines: Hosted



Rootkits

Rootkit

Script that obtains privileges of root

Root

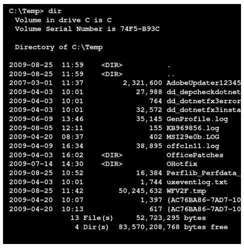
Most privileged subject in a Unix-like operating system

Rootkit

- Take control early
- Remain permanent
- Hook into OS subroutines

Hook into OS subroutines

```
C:\> dir
```

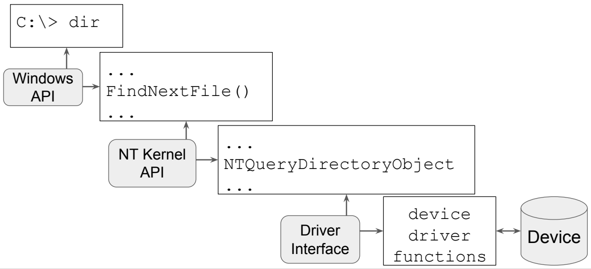


```
C:\Temp> dir
 Volume in drive C is C
 Volume Serial Number is 74F5-B93C

 Directory of C:\Temp

2009-08-25  11:59    <DIR>          .
2009-08-25  11:59    <DIR>          ..
2007-03-01  11:37         2,321,600 AdobeUpdater12345
2009-04-03  10:01            27,988 dd_depcheckdotnet
2009-04-03  10:01               764 dd_dotnetfx3error
2009-04-03  10:01            32,572 dd_dotnetfx3insta
2009-06-09  13:46            35,145 GenProfile.log
2009-08-05  12:11               155 KB969856.log
2009-04-20  08:37               402 MSI29e0b.LOG
2009-04-09  16:34            38,895 offcln11.log
2009-04-03  16:02    <DIR>          OfficePatches
2009-07-14  14:30    <DIR>          OHotfix
2009-08-25  10:52            16,384 Perflib_Perfdata_
2009-04-03  10:01             1,744 uxeventlog.txt
2009-08-25  11:42        50,245,632 WFV2F.tmp
2009-04-20  10:07             1,397 {AC76BA86-7AD7-10
2009-04-20  10:13               617 {AC76BA86-7AD7-10
              13 File(s)     52,723,295 bytes
               4 Dir(s)  83,570,208,768 bytes free
```

Hook into OS subroutines



C:\> dir

Windows API

...
FindNextFile()
...

NT Kernel API

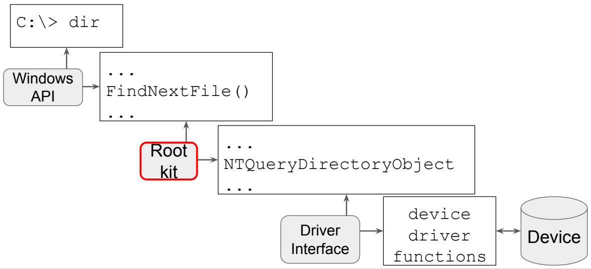
...
NTQueryDirectoryObject
...

Driver Interface

device
driver
functions

Device

Hook into OS subroutines



C:\> dir

Windows API

...
FindNextFile()
...

Root kit

...
NTQueryDirectoryObject
...

Driver Interface

device
driver
functions

Device

Hook into OS subroutines

```
C:\WINNT\APPS> dir
```

```
EXPLORER.SCF
mal_code.exe
PTDOS.EXE
regedit.exe
TASKMAN.EXE
UNINST32.EXE
```

→

```
EXPLORER.SCF
PTDOS.EXE
regedit.exe
TASKMAN.EXE
UNINST32.EXE
```

External Rootkit

Insert a layer of virtualization under the OS!

Rootkit Countermeasures

- Rootkit revealer
- Secure boot
- Trusted path