Everything I have Managed To Learn About Computer Security

Marcus J. Ranum
Tenable Network Security, Inc.

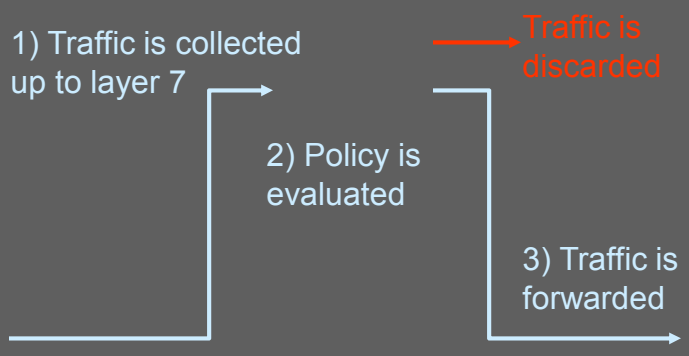
Some Stuff

- This is kind of a grab-bag; there is no consistent central narrative
  - I am telling you this so you don't waste brain-cycles trying to find one
- I occasionally worry that these ideas are all aspects of one big underlying idea
  - I just haven't figured that one out, yet

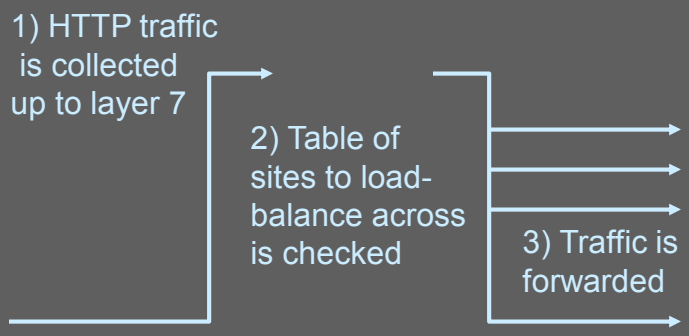
We Keep Repeating Ourselves!

- Virtually all the doo-dads we recognize as “security technologies” overlap in principle

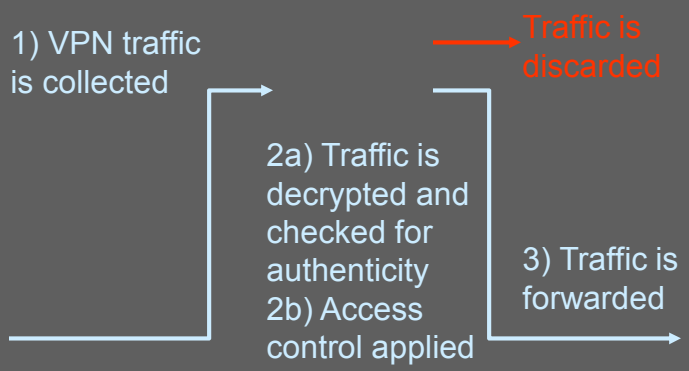
A Firewall



A Load Balancer



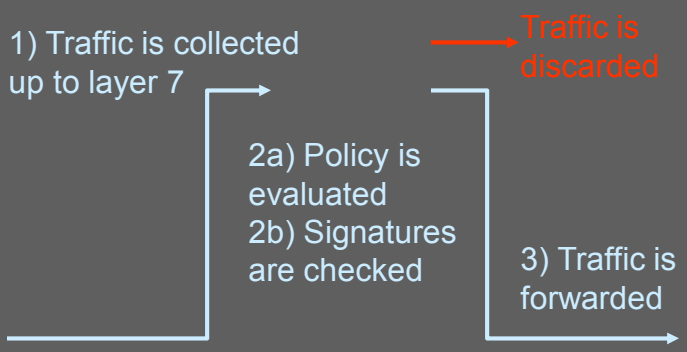
A VPN Gateway



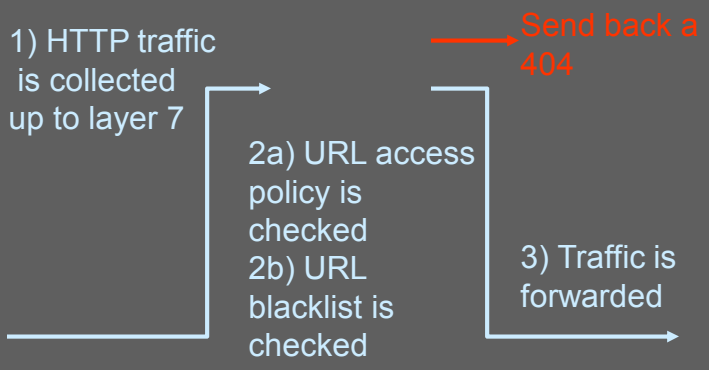
An IDS


1) Traffic is collected up to layer 7
3) Traffic is discarded
2) Signatures are checked

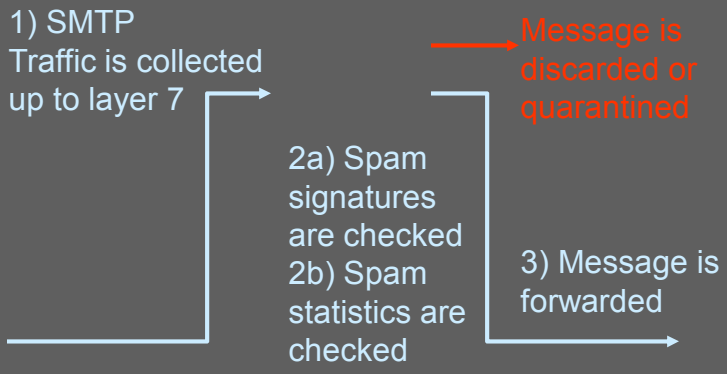
An IPS


1) Traffic is collected up to layer 7
Traffic is discarded
2a) Policy is evaluated
2b) Signatures are checked
3) Traffic is forwarded

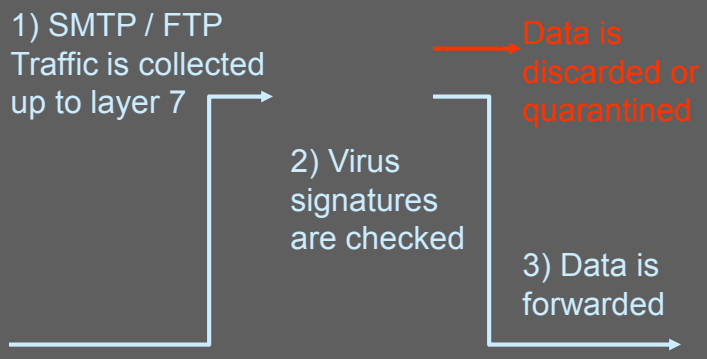
A Web Security Gateway



A spam blocker



A border A/V gateway



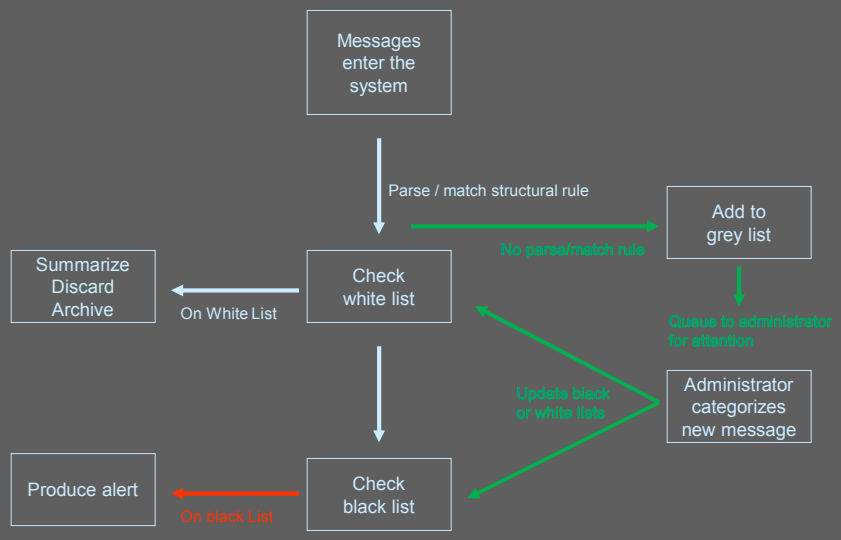
Now Let's Talk Algorithms

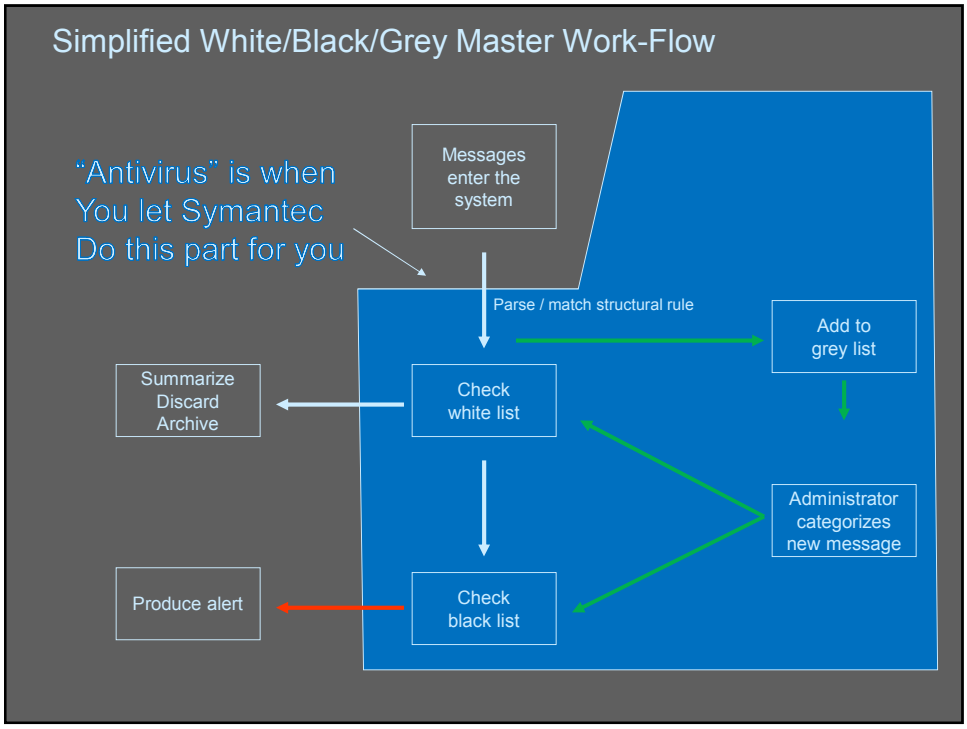
- How do security systems do what they do?

White/Black/Grey

- It turns out that there is really only one work-flow in all of security; it reduces down to this
  - Your task is to decide what parts of it *you* do and what parts you let a *vendor* or *service provider* do
  - If you are missing a part, you will fail

Simplified White/Black/Grey Master Work-Flow





Signatures

- You have no doubt heard that signatures are bad from various vendors
  - Here's another way of thinking of signatures!
- A "signature" is a matching rule attached to a diagnosis

Signatures *(cont)*

- In other words, a signature is an epistemological device:
  - "If you see *this* or *that* or *this+that* then it's an instance of a *wossname*"
- This is how humans *know* what a wossname *is*

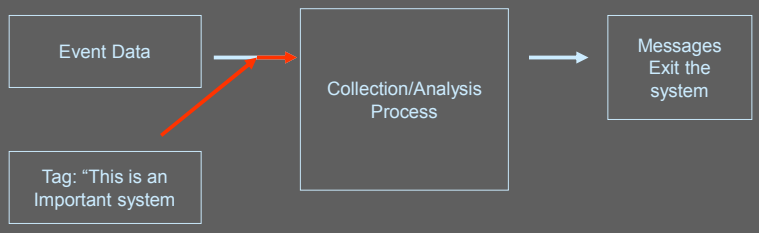
Signatures *(cont)*

- A system without signatures is a system that cannot convey knowledge
  - Which is probably what you want it to do
- "XYZ is under a denial of service attack (LOIC)"
- "The ratio of SYN to FIN packets from XYZ is 3 std deviations off norm"

Presorting Data

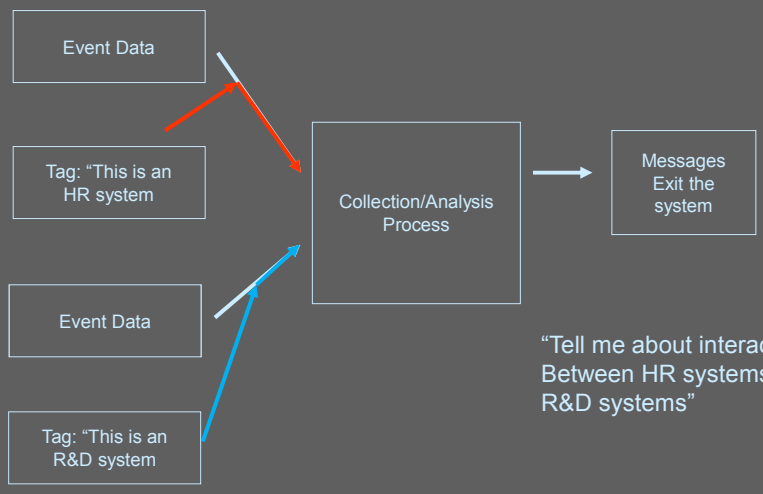
- When you are having trouble sorting through all your data:
  - Apply a tag to the input that lets you sort the output
  - I also call this “shaping your data” or “management overlays” depending on the context

Presorting Data: Significance Tagging



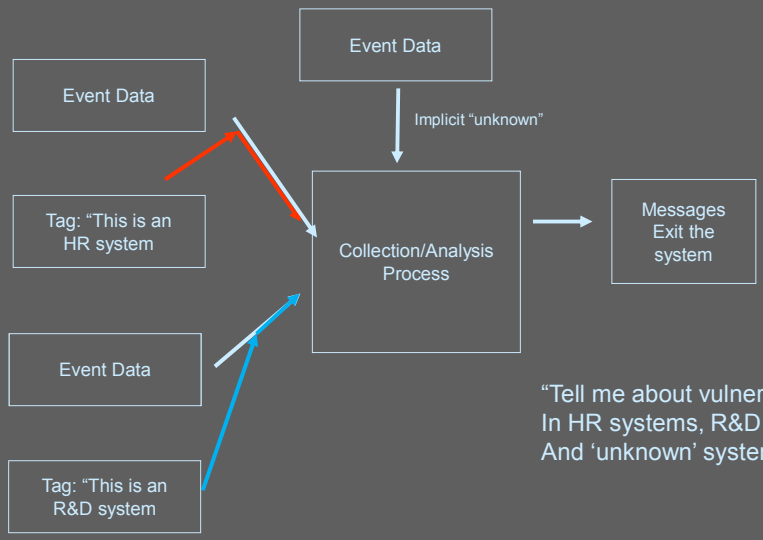
“Tell me about “important systems”

Presorting Data: Management Overlays



"Tell me about interactions Between HR systems and R&D systems"

Presorting Data: Metrics



"Tell me about vulnerabilities In HR systems, R&D systems And 'unknown' systems"

Y Be Normal

- What ***is*** "abnormal {traffic | event | configuration | file | process | user activity}"?
- This is ***the*** question in computer security, for many applications/problems
- It is the core issue behind detection

What is Abnormal?

- There is only ***one way to do this***

1. Define "normal"
2. Take everything that happens
3. Subtract "normal" from it
4. Everything else that's left is "abnormal"

What is Abnormal? (cont)

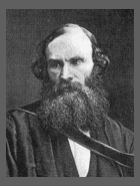
- If you think about it for a second, you'll realize that's the algorithm I described on my white/black/grey slide !!
- You can use statistics or whatever to prune "normal" out of the event-cloud but your idea of "abnormal" is never anything but what's left over

What is Abnormal? (cont)

- One rather weird point:
  - Your signatures are part of your definition of ***"normal"!***
    - Because signatures are ***expected*** conditions
  - Unfortunately signatures don't prune enough from "everything" to give you a small enough set of left-overs

A Word on Metrics

- "Yes"



"To measure is to know."
- William Thomson (Lord Kelvin)

The mandatory Cloud Content →

Cloud

- If your current security sucks
  - Cloud will be an improvement
- But, because you have allowed your current security to suck
  - You can be sure you won't use Cloud correctly either
  - i.e.: you will make your Cloud security suck

Partial Conclusion

- The good news is:
  - The stuff I have talked about here is easy! It's not computationally difficult at all
  - It just requires that you know what "good" means for you

Partial Conclusion (cont)

- The inevitable conclusion I reach from all this is that computer security, as a field, ought to be subsumed as a focus-point in configuration management
  - Corollary: organizations that don't do CM have bad security