SECURE360

Network Security: Reloaded

Marcus J. Ranum

mjr@ranum.com

Speaking only for himself

Agenda

- Introductions
- Reinventing Security by Redesigning It
- Overlapping Controls
- The Eight-legged Platform
- Making It Stand
- Synergy
- Takeaways/Q&A
- Resources

SECURE360

But First: A Digression Regarding Metrics

- None of this stuff will be as valuable if you don't have a metrics program in place first
  - Metrics allow you to
    1. Measure outcomes
    2. Propose interventions
    3. Measure outcomes
    4. Hypothesize about the effectiveness of interventions
  - Since this is all one big proposed intervention you should not undertake any of this unless you intend to be able to argue that it was worthwhile
    - The dark ages of security, when we sold ideas based on FUD, they are over

SECURE360

Metrics and Enclaves

- The enclave model allows you to do some process analysis
  - What does this enclave do and why?
  - What security-related measurements might we do well to capture about this enclave's outcomes?
  - What measurements should we already be capturing?
    - Hint: incident rates are the basic public health-meter of security
    - What is a proxy for incident rates, if you don't have that information? Reimaging rates? Downtime?

SECURE360

Metrics and Automation

- If you automate your metrics collection (you should) then you'll have some baseline data before you start making changes
  - Do interventions and report on changes to the baseline
  - Tie the change to the intervention and the cost of the intervention
  - Now, you are measuring security effectiveness in terms of staffing or $$

SECURE360

Reinventing Security By Redesigning It

- If you look at what's happening in security, there are only two things:
  - Fads
  - Old techniques that work but are "hard"
- In this session, we're going to examine a way of re-integrating the old techniques in a way that provides more predictable and better security than the fads
  - If you've been trying the "fad diet" model of security and keep getting owned by malware, you will understand why, by the time this session is done
- The security industry does not actually exist to secure your systems
  - That's your job
  - Their job is to get your money

SECURE360

The Doctrine of Overlapping Controls*

- Each security control should broadly influence a class of systems
- Each security control should help backstop/reinforce or detect flaws or policy violations in one or more others
- Each security control should fail correctly by design:
  - Sometimes open
  - Sometimes closed
  - Always trigger a warning and provide the best possible diagnosis
- Every security control probably overlaps in purpose to a certain degree
  - Why?
  - Why do we ignore that?

*This is not “suspenders and a belt”

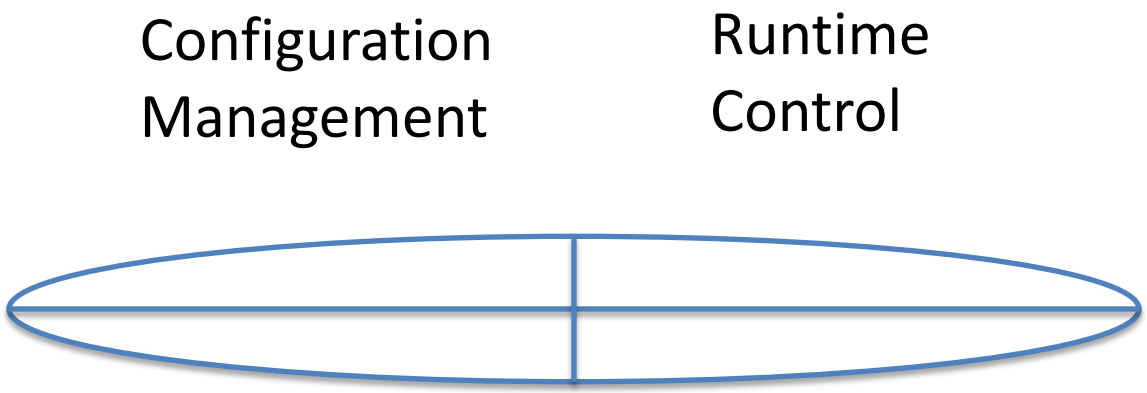
The Doctrine of Overlapping Controls

(Continued)

- A simple example:
  - Your configuration management is a primary capability for:
    - System configuration
  - Your configuration management is a secondary capability for:
    - System variance detection
    - Configuration policy variance detection
    - Business resumption/emergency repair/disaster recovery
    - Field-expedient software (runtime) control
- Given all that, why would you buy a 1u rackmount “malware detection system?”

The Landscape

SECURE360



SECURE360

The Eight-Legged Platform*

- Runtime Control
- Desktop Configuration Doctrines
- Configuration Management
- Edge Vehicles/Log Collection and Management
- File Share/Attachment Management
- Segmentation
- Privilege Management
- Policy Violation Detection

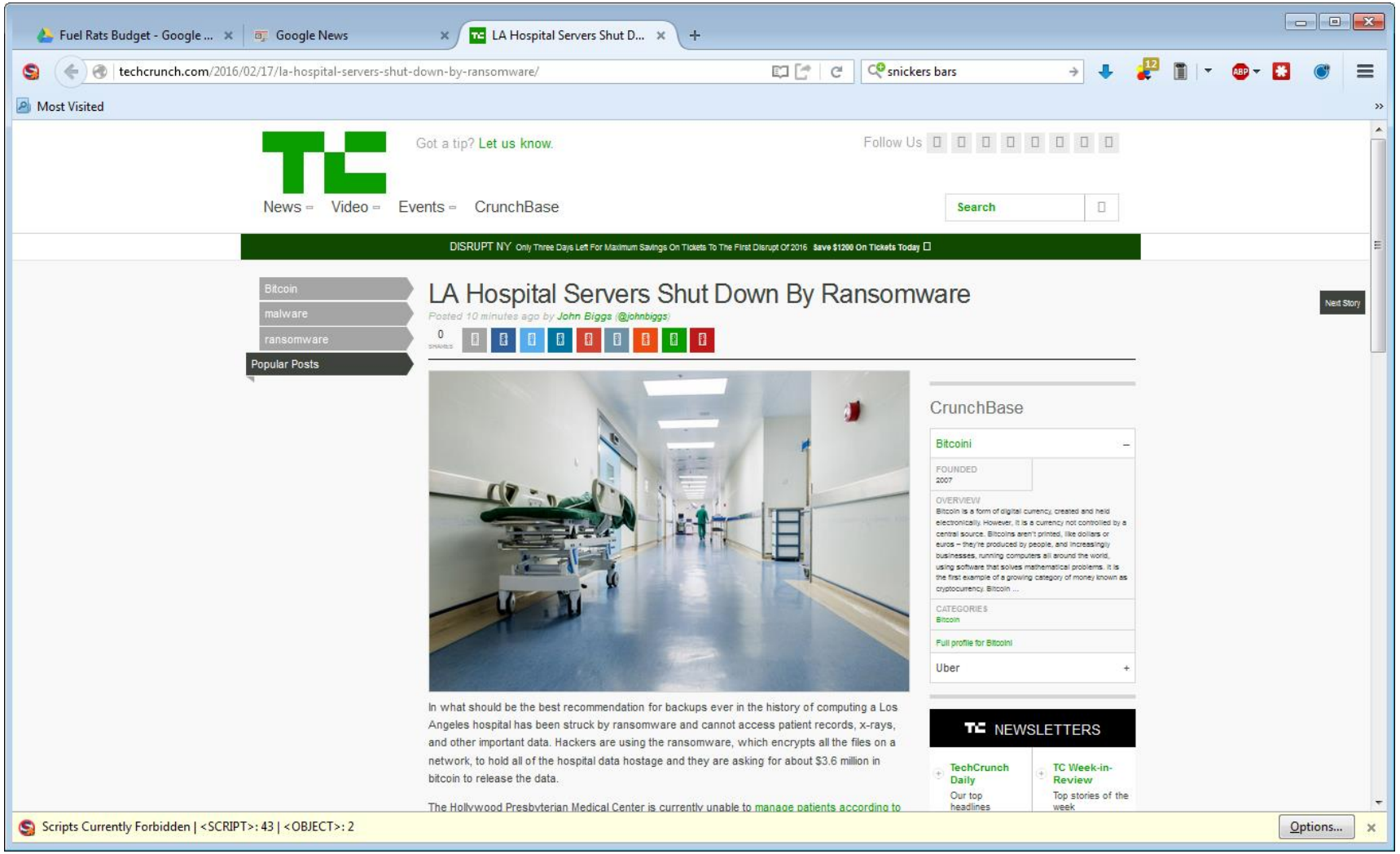
*No, it will not stand on just 2 legs

Runtime Control

- Technology: Bit-9, Lumension, Applocker (Windows 7+), Apple OS, UNIX
- Application whitelisting on low change-rate systems
  - This encounters tremendous resistance, generally
  - Start with systems like:
    - Office automation/temp workers
    - Security Guard stations
    - Kiosks
  - Then move to:
    - Legal
    - Executive
- High change-rate systems go in their own segments, it's either/or
  - High change-rate systems are subject to more in-depth analysis and logging

SECURE360

Runtime Control



SECURE360

Runtime Control

- Random extras:
  - Service-level agreement (“We will approve/deny an executable within 12hr”)
  - IT has a workstation in their system administration/CM practice that installs all new software then whitelists are updated before most users get the update
  - Metrics are reported to management about software licenses in use
    - Figuring out what machines are licensed for X but never run X can save potentially large amounts of money
    - Use that to help justify process
  - Enterprise-wide can disable suspicious executables; make malware vanish anywhere and everywhere, enterprise-wide from a central console
- Lab/Swamp/unmanaged clusters; give them their own whitelisting ruleset and let them manage their own machines

SECURE360

Desktop Configuration Doctrines

- Tech: SAN, AD, Windows, BitLocker (Windows 7+) Configuration Management
- Configuration Management is used to control users' experience on desktops
  - No software installs
  - No local admin
  - Local hard drive has a "temporary" directory users can stick things in
    - Cleaned automatically every month
  - Users' data goes onto a SAN, using a BitLocker-encrypted volume for each user as well as a business unit/group-encrypted volume for each business unit/group
    - SAN file-level accesses are all logged
- Browsers come preconfigured with a script blocker and ad blocker
- Security outcomes are tracked between "managed desktops" and "unmanaged desktops" and reported to exec. management

SECURE360

Desktop Configuration Doctrines

- Random extras:
  - Data on SAN in containers allows potential user mobility without having to deal with desktop data
  - Desktops are disposable and fast; execution is local, executables are local, the hard drive is basically a cache
  - Desktops do not need to be backed up; this saves tremendous amount of work and expense
  - Call it a “file cloud” and sprinkle “cloud fairy dust” on it

SECURE360

Configuration Management

- Tech: SCCM, Configuresoft, (optionally Vmware) “gold releases”
- Systems are either under CM or they are in separate “unmanaged” segments
  - There are no systems that IT is both responsible for and that are not under CM
  - If the business units want unmanaged machines, they manage them
    - And those machines are firewalled off from the main network
    - There are “core services” (Web-based attachment sharing, email) and everything else is treated as being on the internet
  - This is the “BYOD” policy also! (that’s your BYOD strategy right there)
- IT populates systems and keeps control over them
- CM/QA process is used to help update whitelists
- CM process collects metrics about administrative effort expended per business unit

Configuration Management

- Random extras:
  - CM cross-trained with security/vulnerability management process
  - CM variance data goes into SIEM
    - Variances get whitelisted or suppressed
  - CM practice has a network-based “boot to green field install” so that systems can be recovered to correct state without IT intervention

SECURE360

Edge Vehicle/Log Collection

- Syslog-ng, Kiwi syslogd, or possibly Splunk or a SIEM (can do cluster file systems)
- Collects data and splits it:
  - Data that gets forwarded to the SOC
  - Data that gets preserved locally and rotated out automatically
- Edge Vehicle (for example) gets full load-balancer logs, which means it is not necessary to get Web server logs
  - Some stuff gets summarized
- The Edge Vehicle's value is that nobody can complain about it sucking up performance
- Edge Vehicle has an interface on the "green network" (private network to SOC and SIEM)
  - Back-hauling data is security's problem and doesn't interfere with performance

Edge Vehicle/Log Collection

- Stuff to collect:
  - AD logs
  - DHCP logs
  - Firewall logs
  - SAN server logs
  - CM logs
  - Execution control/runtime logs

- Stuff to analyze and look for weirdness in:
    - DNS logs

Edge Vehicle/Log Collection

- Random Extras:
  - The Edge Vehicles sometimes produce summaries of certain types of activity
    - Only summary goes to SOC (summary gets syslogged)
  - A typical Edge Vehicle is not very expensive (use a standalone CPU not a VM so you can just beat on it)
  - The Edge Vehicle exists for collection/analysis as well as for incident/response
    - Keep 3-4 months of data
    - In the event things go wrong, you know which EV will have the critical stuff

SECURE360

File Share/Attachment Management

- Tech: Accellion, FileCloud (can be done with something like Dropbox)
- File sharing between segments is ONLY through a service that scans for and sequesters executable content
  - Includes an Outlook plug-in that strips and manages attachments
  - Includes a mappable folder (similar to Dropbox, etc.)
  - All attachments are logged
    - Can identify “patient zero” in a phish attack
    - Metrics and usage are kept
  - Includes sharing outside the organization and is Internet reachable
    - Users can create a share and email a link out to someone else, with various authentication options, SSL-enabled or Google authenticate

SECURE360

File Share/Attachment Management

- Random extras:
  - Emails coming in with attachments normally get stripped and pushed to server
  - Metrics kept regarding which business units get most targeted by phishing attacks
    - This really helps “sell” the system to management
  - Employees can build a share folder with themselves and use it to transfer work files to home systems

    … it’s just all tracked and recorded

Segmentation

- Tech: NG-FW “bump in a wire” mode, VLANs, copper separation
- Firewalls are implemented as a layer between the core switching layer in HA/fail open pairs
  - Running a central policy for Internet access as well as internal<->internal
  - Most internal<->internal is disabled except for core resources:
    - SAN
    - Database server(s)
    - File-sharing server
    - Internally hosted infrastructure

SECURE360

Segmentation

- Random extras:
  - The firewall's "malware detection" engines aren't utterly useless
    - May as well use them!
  - The firewall's categorization engines (for sites, apps, users) are very useful
    - Look for "unknown" in the firewall logs
      - If you have an unknown user going to an unknown site with an unknown certificate: it's malware
  - Can be used for rule-based packet collection during an incident response
    - Connection to the "green network" for logging and collection
  - Can be used with "overlay" rules to provide group- or zone-based monitoring
    - E.g., permit and permit-and-log

Privilege Management

- Tech: CyberArk, Thycotic, many options, build-your-own “jump box”
  - Ask your pen tester: The first thing they go after is AD credentials
  - Administrative credentials aren’t good enough via legacy AD; use a jump box
    - Segment firewalls can permit traffic from the jump box(es) to anywhere
    - Not just for admins
  - Logging
  - Do not try to “boil the ocean” – start with a few servers/services and keep locking them down as you go

Privilege Management

- Random extras:
  - Good for provider access as well!
    - Many PAM systems support Google authenticate or Duo, with self-enrollment
    - Providers can enroll and provide the credential to enable in the PAM solution
    - All access is logged

Policy Violation Detection

- Tech: Firewall rules in the NG-FW
- Your segments should match zone maps in your firewalls
  - Now you can put deny/log or permit/log rules in to collect information about attempts to go between zones
  - Engineering -> Office of the CFO: Deny and log
  - The SIEM then becomes a significant malware exploration detector
  - May wish to create a zone called “admin’s machines” and then you can look for attempts to connect to the jump box by non-admin machines (almost certainly a hacker or a pen tester)
  - May wish to create a port-map for AD servers and flag attempts to do port enumerations on AD servers or specific feature probes
    - Most NG-FWs are very programmable in the L7 matching engines

SECURE360

DNS Tracking

- Malware frequently gives itself up in DNS queries
- The easiest way to catch it is to have a caching nameserver (a good idea for performance and reliability, anyway!)
  - Analyze server logs
  - Any system that is making 10 times more DNS queries than the admin’s machine on a typical day has probably got malware

Fringe Benefits: Incident Response Depth

- All the data collected throughout the system is designed to allow rapid determination and categorization of “patient zero” in outbreaks
- The CM practice can be used to retrieve copies of questionable data
- The SAN can be used to sequester/back up copies of potentially damageable data
- In the event of an active outbreak, the firewalls are in place to collect detailed trace information
  - Or to globally inject a blocking rule after you are sure what traffic you want disabled

Fringe Benefits: Business Resumption/Recovery

SECURE360

- The configuration management practice can be used to:
  - Revert systems
  - Relocate systems
  - Replicate systems
  - Sequester crucial data off systems
    - E.g., use the CM console to remotely make a user's files write-protected

Fringe Benefits: Data Leakage Control and Audit

- Since attachments go through the attachment server and all other transactions with the outside go through the firewall:
  - Combined firewall+attachment server logs make a very good baseline for data movement
  - SAN logs combined with the above allow audit of what files a user may have moved when and where
  - It ought to be possible to capture files using the firewalls (will require additional infrastructure or a larger Edge Vehicle)

SECURE360

Yes, This Stuff Is Hard

WHAT ABOUT BEING OWNED

CONSTANTLY

IS SO

!&*  !#(&!&

EASY?

SECURE360

Miscellaneous

- Marcus Ranum blogs on freethoughtblogs as ‘stderr’
  (Content warning: politics, anarchism, criticism of military procurement and spending, moral nihilism, and extreme snark)
- Some articles on metrics by Marcus at SecurityWeek:
  http://www.securityweek.com/authors/marcus-ranum
- Marcus’ interview column on SearchSecurity:
  http://www.techtarget.com/contributor/Marcus-J-Ranum
- Marcus occasionally “Tweets” as @mjranum