



Designing for Insecurity

Engineering Compartmentalization

Drew Simonis – Drew_Simonis@Symantec.com





Today's Talk

- ▶ Problem Statement
- ▶ Building Business Consensus
- ▶ Solution Discussion
- ▶ Problems
- ▶ Next Steps



Engineering Compartmentalization - Reasoning

- ▶ Problem: ***Software development usually takes place on the least secure systems!***
- ▶ Business Risks:
 - Ship to Market could be delayed due to virus outbreak
 - System compromise could result in disclosure of sensitive information
 - Any question regarding the integrity of the development process would have grave consequences
 - Redundant costs exist due to need for a minimum of two systems per developer
 - Inefficient processes exist exist due to lack of real network interoperability
- ▶ Solution: Drag development out of labs
 - Determine developer system needs
 - Create an environment that is mutually conducive to security and productivity
 - Identify shared development resources



Biosafety Lab Model - Principals



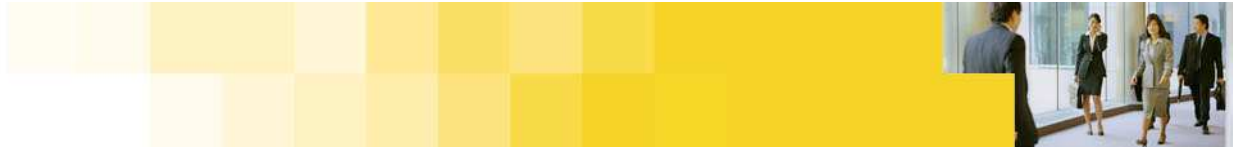
- ▶ Biosafety levels provide
 - Increasing levels of personal and environmental protection
 - Guidelines for working safely in biomedical laboratories
- ▶ Biosafety level guidelines describe
 - Laboratory practices and techniques
 - Safety equipment (primary barriers)
 - Laboratory Facilities (secondary barriers)



Biosafety lab – What makes it work?

- ▶ Biosafety labs have
 - Knowledgeable supervisors
 - Personnel who are
 - aware of the hazards
 - proficient in prevention
- ▶ Biosafety manuals are specific to the lab
- ▶ Biosafety equipment is tailored to each environment
- ▶ Biosafety protection is proportionate to the threat





CDC Biosafety Levels

1. Suitable for work involving well understood agents not known to cause disease in healthy adults and of minimal potential hazard to their surroundings.
2. Applies to moderate-risk organisms that can cause disease in humans, but are generally treatable or preventable by vaccination. Measles virus is an example of a biosafety level 2 agent.
3. Organisms here are infectious agents that can cause serious disease and in most cases can be caught by inhalation. Plague is an example of a biosafety level 3 agent. West Nile virus is also classified at level 3, although it is caught from mosquito bites.
4. Applies to the most serious, highly infectious microorganisms and new diseases where the risks of infection are not known. Examples of biosafety level 4 microbes are Ebola virus and tick-borne encephalitis. Work can only be conducted in purpose-built, airtight laboratories. Workers must wear full body suits with their own air supplies. All equipment, air, water and waste leaving the laboratory must be decontaminated.



Symantec's "Cybersafety" Levels

1. Suitable for every day development tasks such as authoring source code, unit testing, etc. Disparate OS's (e.g., Linux) and server software (e.g., web servers) may be run in this environment, although incoming network connections will not be allowed. Suitable for routine business tasks such as email, expense reporting, etc.
2. Allows for more intensive testing related activities. These may include the running of server systems where clients need to connect to perform testing (e.g., load testing), running of non security compliant builds or related activities. L2 labs would be used by both Dev and QA for integration testing, for example. L2 labs could be logically connected across sites via VPN.
3. L3 labs would house activities that have the potential to impact other hosts on the network segment (e.g., DoS testing, testing exploit code, etc). This lab level would be used to test the active response and detection components of products such as SGS and SNS, but may not be needed by all dev teams.
4. L4 labs would house unknown live viral code or other testing activities well known to have an actual risk.



Engineering Compartmentalization - Desiderata

- ▶ All systems in Level 1 labs conform to security standards standards for client machines
- ▶ Level 1 labs would allow inbound only the minimum necessary services for general client functionality (e.g., domain membership, software distribution, anti-virus)
- ▶ Systems in Level 1 labs have the option of running server OS installations
- ▶ Systems in Level 1 labs are able to run server applications
- ▶ Shared server networks will be located such that the majority of dev servers could reside within them
- ▶ Level 2 labs function much as labs did prior to implementation, ensuring minimal changes to the development lifecycle
- ▶ Activities in Level 2 labs are such that they would not impact the availability of the network, including the shared server network
- ▶ Level 2 labs may interconnect across sites and regions via VPN
- ▶ Level 3 labs are constructed such that they offer sufficient containment for invasive testing
- ▶ Level 4 Labs share no connectivity with other lab levels. These would be, for example, unknown live virus labs.



Cybersafety Lab Model – Level 1

1. Suitable for every day development tasks such as authoring source code, unit testing, etc. Disparate OS's (e.g., Linux) and server software (e.g., web servers) may be run in this environment, although incoming network connections will not be allowed. Suitable for routine business tasks such as email, expense reporting, etc.

▶ **CDC BSL1 barriers include**

- Sinks for hand washing
- Sanitary work areas
- Sturdy furniture
- Windows with fly screens

▶ **Symantec's data analogies**

- AV filtering on inbound network access
- Managed AV on workstations
- Security compliant workstations
- Minimal but effective access control



Cybersafety Lab Model – Level 1 Uses

- ▶ Level 1 Engineering would be composed daily use workstations
- ▶ Inbound access to the Level 1 Engineering networks would be restricted by ACL or equivalent.
- ▶ Since no inbound access is allowed, we tolerate the presence of developer specific alterations. For example, some dev groups need to run web servers or apps servers, etc, on their workstations to conduct even the most basic build testing. The need to run Linux and other Unix platforms is also prevalent.
- ▶ Outbound Activity from a Level 1 Engineering Network would include:
 - Email
 - File/Print access
 - Business systems access (e.g., expense reporting)
 - Outbound HTTP/HTTPS
 - Source repository access
- ▶ Activity that would take place in a Level 1 Engineering Network would include:
 - Source code authoring
 - Build testing
 - “Production” business functions
- ▶ All systems in a Level 1 Engineering would be required to meet the specifications laid out by security, such as the use of managed AV, host firewall and patch management software.



Cybersafety Lab Model – Level 2

2. Allows for more intensive testing related activities. These may include the running of server systems where clients need to connect to perform testing (e.g., load testing), running of non security compliant builds or related activities. L2 labs would be used by both Dev and QA for integration testing, for example. L2 labs could be logically connected across sites via VPN.

- ▶ CDC BSL2 barriers include attention to infection prevention
 - All BSL1 barriers
 - Use of gloves and coats
 - Use of biosafety cabinets when working with infectious agents
- ▶ Symantec Data analogies include the same
 - Near isolation from the Production network
 - Limited access to necessary servers (by destination port/address)
 - Inbound only access from L1 lab



Cybersafety Lab Model – Level 2 Uses

- ▶ Level 2 Engineering networks contain systems running server software which require client connectivity in order to function
 - Load testing
 - User interface testing
 - Etc.
- ▶ All integration and system testing would be conducted in a Level 2 Engineering network
- ▶ Level 2 Engineering networks would also house QA testing activities, although it would be preferable to keep those activities on separate actual networks, regardless of any design similarity
- ▶ Level 2 Engineering networks could be interconnected across sites so that geographically distinct teams could function more efficiently.



Cybersafety Lab Model – Level 3

3. L3 labs would house activities that have the potential to impact other hosts on the network segment (e.g., DoS testing, testing exploit code, etc). This lab level would be used to test the active response and detection components of products such as SGS and SNS, but may not be needed by all dev teams.

▶ CDC BSL3 barriers provide extreme attention to *exposure* prevention

- All BSL1 and BSL2 barriers
- Separate building or isolated zone
- Double door entry
- Directional inward airflow with single pass air
- Enclosures for aerosol generating equipment

▶ Symantec data analogies

- Total isolation from the Production network
- Highly limited access to necessary servers (restricted by both source and destination port/address)
- Inbound only access from L1/L2 labs for remote control



Cybersafety Lab Model – Level 3 Uses

- ▶ Level 3 Engineering network houses all testing activity that would be considered invasive, either actually or potentially.
- ▶ Creating a separate compartment for this activity ensures that any errors do not cause downtime to the rest of the development process.
- ▶ Examples of expected activities include:
 - Using attack tools to test IDS
 - Spyware testing
 - Creating IDS signatures by exploit execution
 - Testing AV



Cybersafety Lab Model – Level 4

4. L4 labs would house unknown live viral code and allow only sufficient connectivity as required for sample submittal.

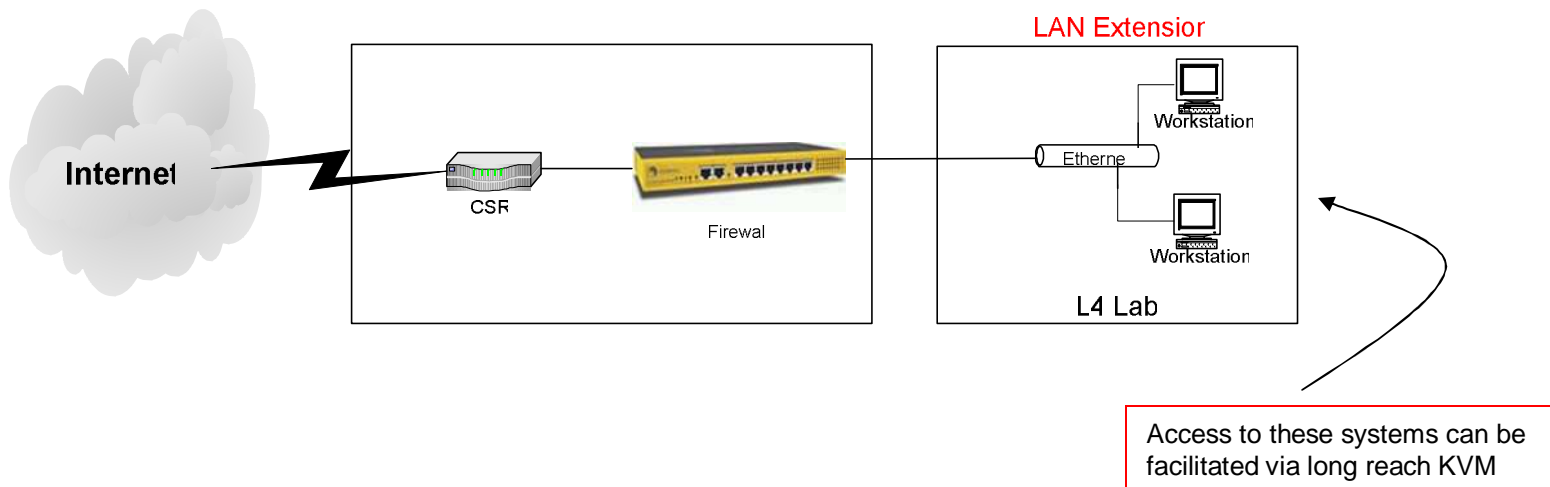
- ▶ BSL4 labs deal with the unknown...
- ▶ This is analogous to Symantec's SARC labs which deal with unknown viral software and other suspected malware.





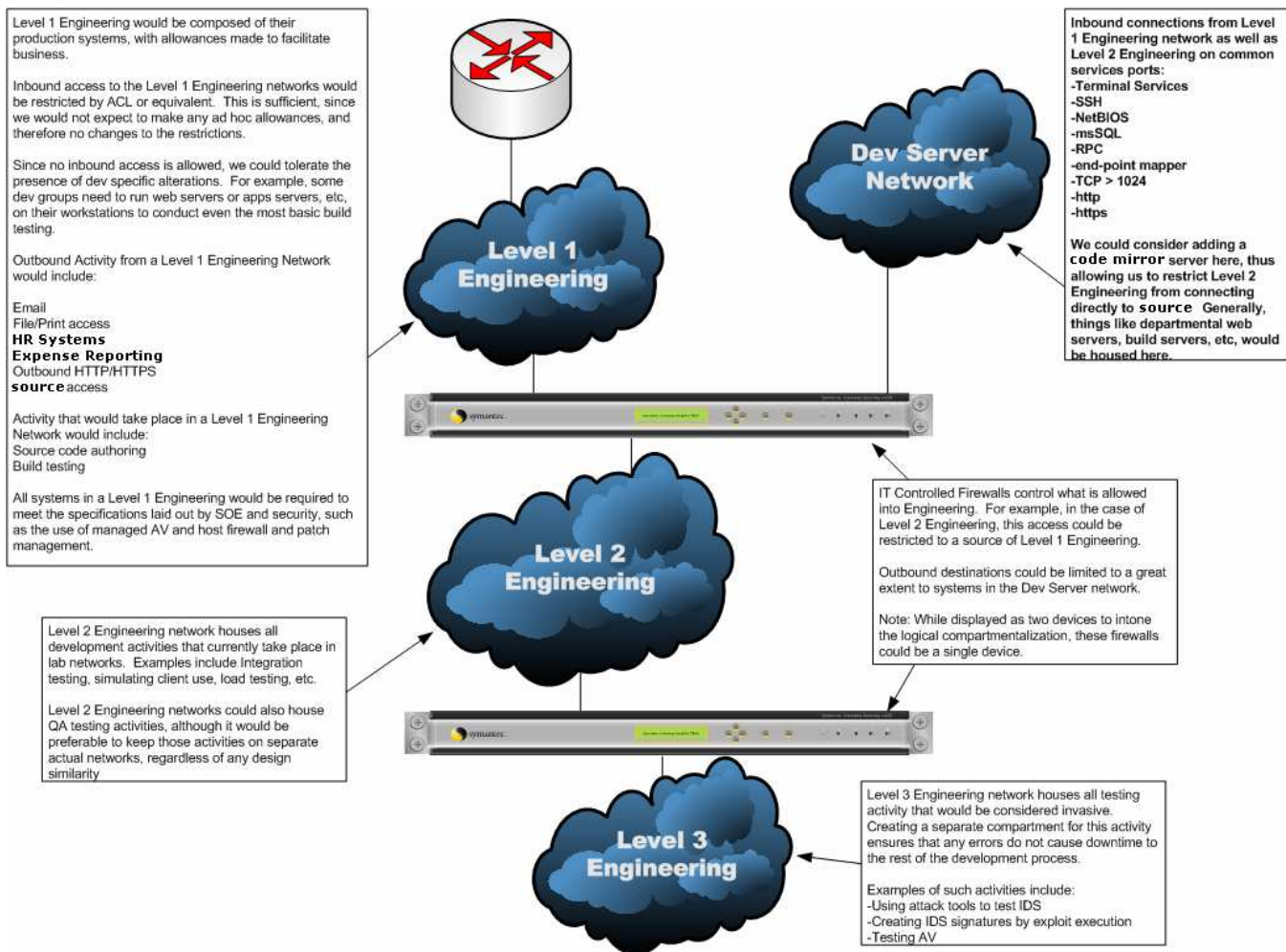
Lab Network Compartmentalization – Technical Design

L4 Networks are “dead enders”:





Lab Network Compartmentalization – Technical Design





Engineering Compartmentalization - Issues

- ▶ **Open Issues:**
 - How to patch disparate OS versions
 - How to track all installed applications
 - Who “owns” the lab infrastructure, IT or development Lab Managers?
 - How to effectively maintain additional infrastructure (e.g., firewalls)
- ▶ Next steps:
 - 802.1x for Dynamic VLAN assignment
 - NAC for compliance control
 - Remote access labs (telework)