

Improving Unix Network Security Through Host Rings

Geoff Halprin

The SysAdmin Group Pty. Ltd.

SecureCon, Melbourne, February 2005



© Copyright 1995-2005, The SysAdmin Group Pty. Ltd. All Rights Reserved.

The Problem

- Firewalls provide an effective “choke point” between networks.
 - They suffer from one basic assumption: that the good guys are on the inside, and the bad guys are on the outside.
- Another model is required for use within a client-server LAN.



Scope, Assumptions, Limitations

1. There is a group of core hosts providing services to large number of desktops/laptops (“clients”).
2. Mission critical environments, where centralised policy and practices can be controlled.
3. Single administrative domain.

3

2005-02-03

Improving Unix Network Security Through Host RIngs

The
SysAdmin
Group

A Word About Security

- It's always a trade-off:
Security vs. Convenience
- Several Types of Security:
 - Confidentiality
 - Integrity
 - Availability
- One Size Does Not Fit All!
 - There are several categories of service, and hence security.
 - e.g. A desktop is not the same as a mission-critical server!



4

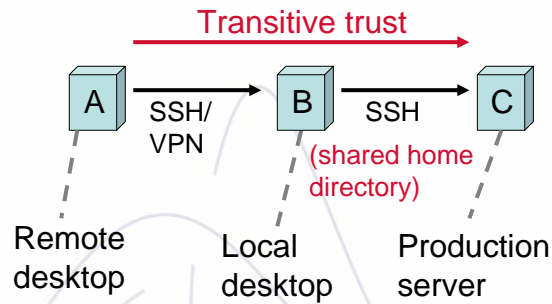
2005-02-03

Improving Unix Network Security Through Host RIngs

The
SysAdmin
Group

The Present Situation

- The Web of Trust
 - Problems of transitive, hidden trust



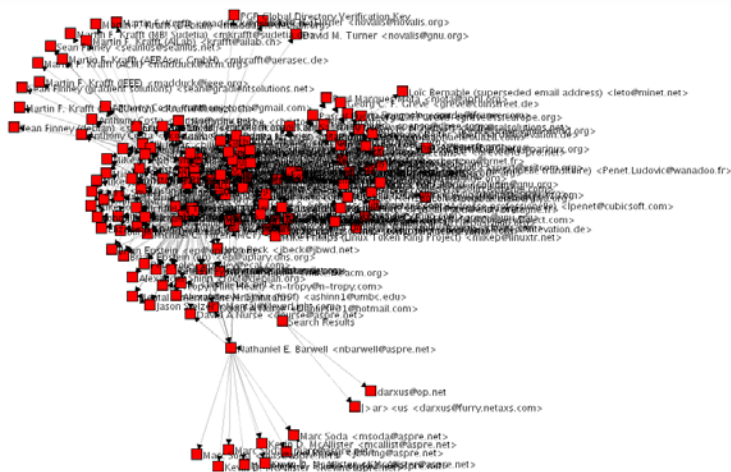
5

2005-02-03

Improving Unix Network Security Through Host RIngs

The SysAdmin Group

Visualising the Web of Trust



Source: http://e170.ex.com/handouts/final/nathande-cobelenski_paper.doc

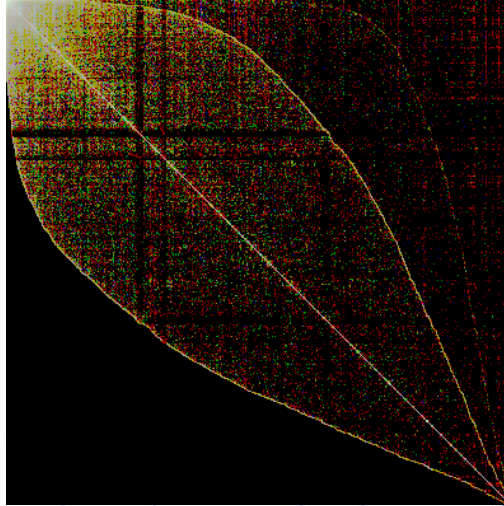
6

2005-02-03

Improving Unix Network Security Through Host RIngs

The SysAdmin Group

The PGP Leaf of Trust



Source:<http://www.lysator.liu.se/~jc/wotsap/leafoftrust.html>

7

2005-02-03

Improving Unix Network Security Through Host RIngs

The
SysAdmin
Group

A Formal Security Model – Why?

1. Establish a Benchmark
 - Analyse and rate the services we provide.
 - This determines infrastructure costs.
2. Proactive Security Management
 - Analyse security implications before we provide the service!
3. Quality Assurance
 - Better predictability of system behaviour.
 - Better repeatability and consistency.

8

2005-02-03

Improving Unix Network Security Through Host RIngs

The
SysAdmin
Group

Host Categorisation

- Example host categories (highest to lowest risk):
 - **Mission Critical.** Company loses revenue for each minute this host off offline.
 - **Business Critical.** Company cannot operate in some significant capacity.
 - **Business Sensitive.** Staff are not able to perform all business functions. i.e. Reduced service levels.
 - **General.** Individual desktops and general service hosts.
 - May be further divided (e.g. dev hosts).
 - **Qualification Platforms.** Identical to production platforms. Used to verify correct behaviour.
 - **Test Hosts.** The first layer. Should identify showstoppers.

9

2005-02-03

Improving Unix Network Security Through Host RIngs

The
SysAdmin
Group

The Hierarchy of Services

- There exists a natural hierarchy of services and hosts:
 - Administrative Services
 - Production Application Services
 - Development Services
 - General Purpose Hosts
 - Internet Related Hosts
 - The Unwashed Desktop

10

2005-02-03

Improving Unix Network Security Through Host RIngs

The
SysAdmin
Group

What's Old is New Again!

- **Multics** introduced the concepts of **execution domains** and **protection rings** for process security.
 - Processes were allocated into rings.
 - The operating system was the most trusted service ring.
 - Processes called inner rings through well-defined interfaces ("**gateways**").
- This same concept can be applied to networks of hosts, rather than hosts of processes.

11

2005-02-03

Improving Unix Network Security Through Host Rings

The
SysAdmin
Group

Host Rings

- Uni-directional, Layered model of trust
- The Rules of the Rings
 1. Each host trusts those hosts in a more inner ring than itself.
 2. No host trusts any host in a more outer ring than itself.
 3. Each host *may* trust those hosts in the same ring as itself.
- Calling an Inner Ring
 - Occasionally there is a need to request a service of an inner host.
 - This is achieved by placing a secure call through a "service gate".
 - All data and authentication is checked and logged.

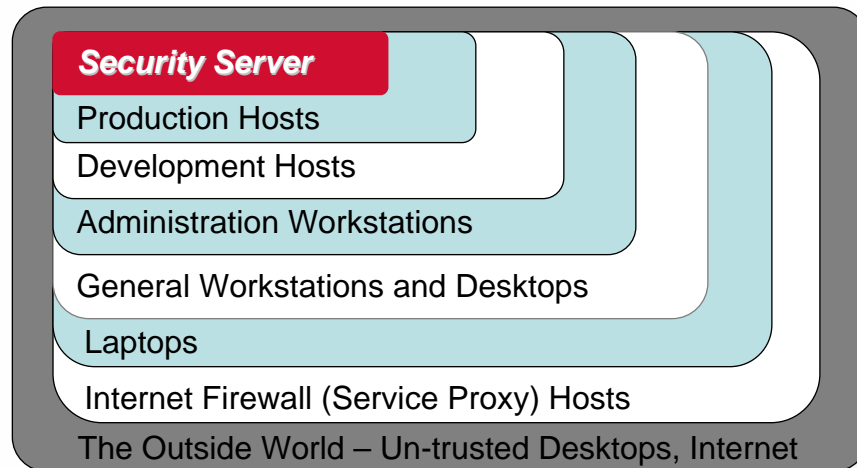
12

2005-02-03

Improving Unix Network Security Through Host Rings

The
SysAdmin
Group

Example Scenario #1



13

2005-02-03

Improving Unix Network Security Through Host Rings

The
SysAdmin
Group

A Walk Through The Rings

- Ring 0 - The Security Server
 - The RDIST Master
 - The Map Server
 - Other Centralised Administration
 - Hardened. Does not provide production services. Only sysadmin users.
 - Secure login channel across the network (ssh)

14

2005-02-03

Improving Unix Network Security Through Host Rings

The
SysAdmin
Group

A Walk Through The Rings (cont.)

- Production Hosts
 - Production Application Services.
 - Restricted Login. Only sysadmin users.
 - Secondary DNS/NIS for resilience.
- Staging Hosts
 - Production (Staging) must “pull” an upgrade from Staging (Development). This protects against rogue upgrades by people who do not have privileges on the Production hosts.
- Development Hosts
 - Lower security/availability requirements.

15

2005-02-03

Improving Unix Network Security Through Host Rings

The
SysAdmin
Group

A Walk Through The Rings (cont.)

- System Administration Workstations
- General Workstations and Desktops
- Remote Access Host
 - For access to internal network from Internet
 - Lower ring than most hosts, hence can't progress further in.
 - Higher ring than Spool host, so can read mail, etc.
- Internet Services Spool Host
 - Mail/News/Web Cache Host
 - This is primary target of attack through server software bugs (which pass through firewall), hence not trusted by most other hosts.
 - Typically NFS exports spool directories to more trusted hosts.

16

2005-02-03

Improving Unix Network Security Through Host Rings

The
SysAdmin
Group

Example Scenario #2

<i>Ring - Description</i>	
<i>Ring 0 - Security Servers</i>	
<i>Ring 1 - Central Production Servers</i>	
<i>Ring 2 - Site Production Servers</i>	AB AS BR CO ME PR SY
<i>Ring 3 - Development and Test</i>	AB AS BR CO ME PR SY
<i>Ring 4 - Support Workstations</i>	CO
<i>Ring 5 - General Workstations</i>	AB AS BR CO ME PR SY
<i>Ring 6 - The Unwashed Masses</i>	AB AS BR CO ME PR SY
<i>Ring 7 - Internet Service Spool</i>	
<i>Ring 8 - Customers Access Platforms</i>	
<i>Ring 9 - Firewall/Security Perimeter</i>	

17

2005-02-03

Improving Unix Network Security Through Host RIngs

The SysAdmin Group

Service Questions

- Does this host require user accounts?
- What services does this host provide?
- What services does this host require?

18

2005-02-03

Improving Unix Network Security Through Host RIngs

The SysAdmin Group

Implementation Details

- SSH provides the transport and host authentication layer.
 - Defends against man-in-the-middle attacks.
- TCPD is the basic access-control/audit tool.
 - TCPD authenticates/audits each in-bound call.
 - Netgroups can be used to define which hosts are in which ring.
- RDIST controls the deployment.
 - The Security Server uses RDIST to distribute `/etc/hosts.allow` and other files.

19

2005-02-03

Improving Unix Network Security Through Host Rings

The
SysAdmin
Group

Observations

- Hard to retrofit - things break.
 - Careful, gradual migration of old services.
 - Easier to fit to new services.
- Initial benefits come from change of mindset.
 - Formal analysis of service requirements.
 - Set policy per ring.
- A useful addition to the toolkit.

20

2005-02-03

Improving Unix Network Security Through Host Rings

The
SysAdmin
Group

New Threats, New Opportunities

Part II

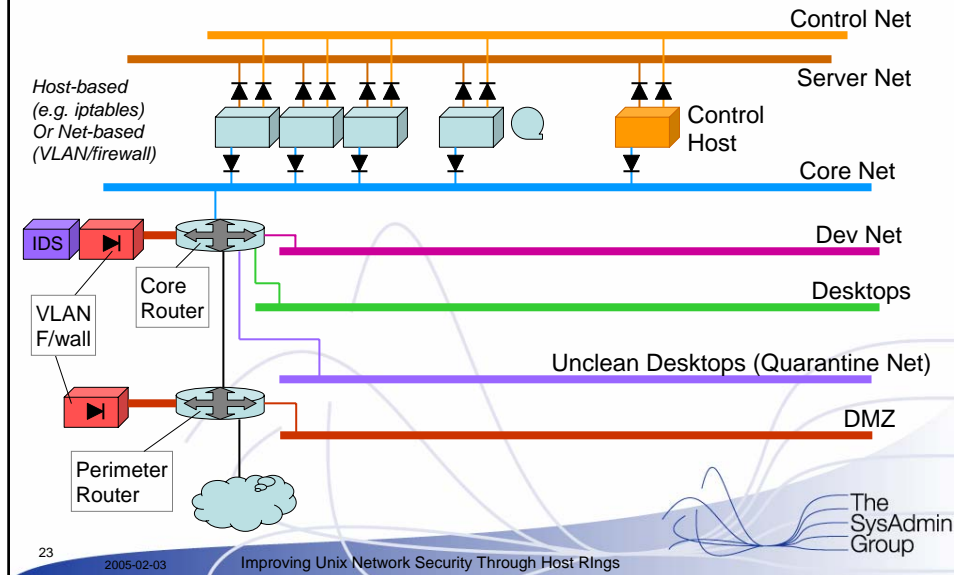
The
SysAdmin
Group

Network Rings

- New threats have emerged since this paper was first written (1996):
 - 30% of all systems are infected at any time.
 - Wireless networks defeat physical security.
 - VPNs side-step firewalls.
- You can no longer trust most machines on the network.
- The same technique (trust rings) can be used to segment a network to enforce a more restrictive trust model.
 - These boundaries are also a great place to locate IDS systems.

The
SysAdmin
Group

Something Like This...



Questions?

geoff@sysadmin.com.au