RELIABILITY TESTING OF COTS SECURITY-BASED SOFTWARE APPLICATIONS

Dr. W. W. Everett

SPRE, Inc

wwe@SPRE-Inc.Com
Tel (505) 890-7773

Jim Widmaier, COTR

Motivation

"*Can Reliability Testing add value in the assurance of security-based software applications?*"

Premise: The fields of Reliability and Security have different approaches to establishing assurance of products. Leveraging these differences of approaches may provide higher levels of assurance of security-based products.

Approach: Follow the steps for doing software reliability engineering (SRE) as documented in [Musa98] with selected security-based software applications.

Motivation (cont'd)

- Security Approach to Assurance
  - Focus on how the product is built
  - E.g. Common Criteria, NIAP Certification Testing.
- Reliability Approach to Assurance
  - Focus on how product is used
  - Provide a numerical value that statistically defines the period of time for which software will run failure free under stated operating conditions.

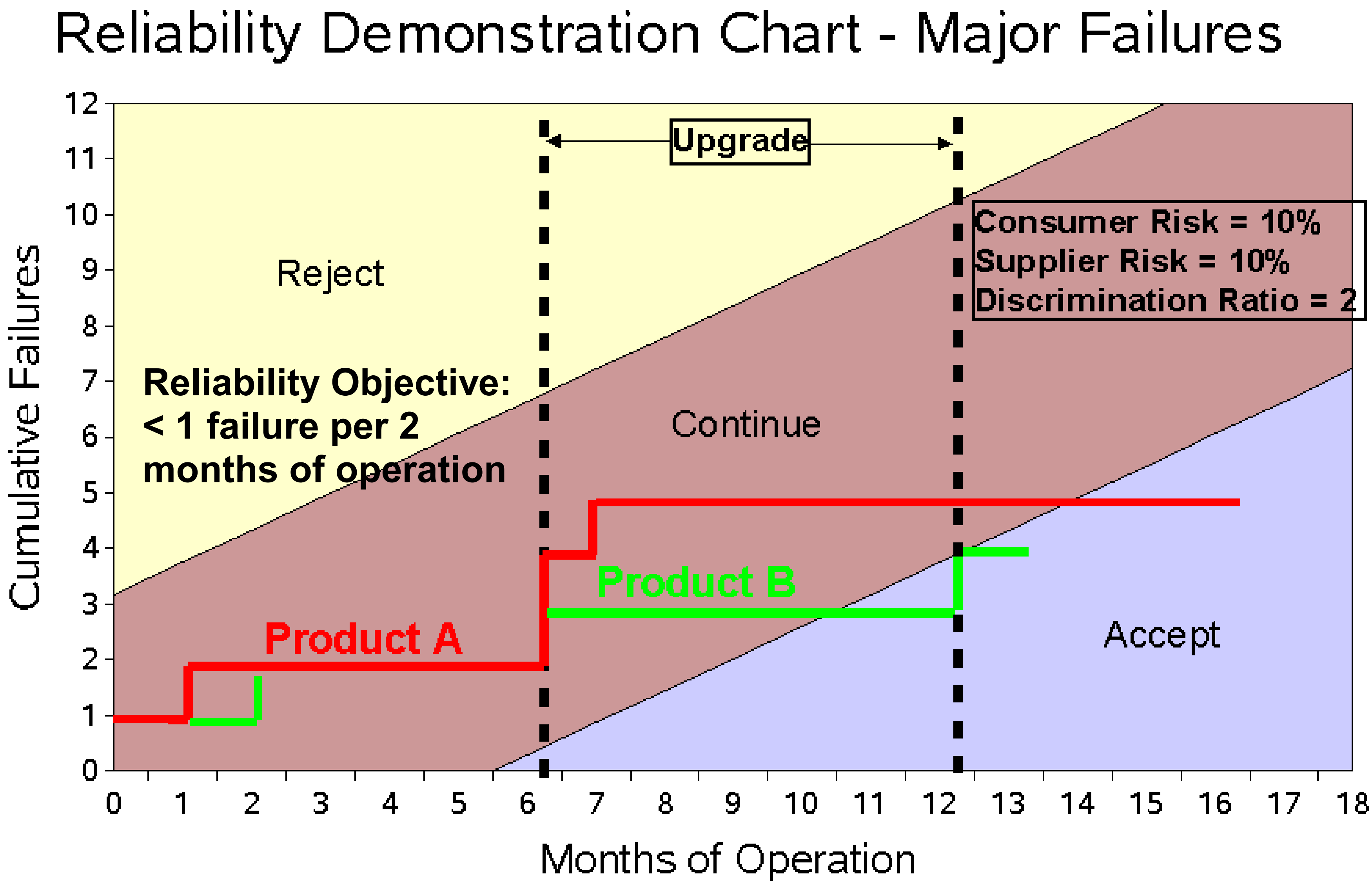
In a Nutshell

- Objective
  - Demonstrate Reliability Testing
    - Two Commercial Firewall products under NIAP certification
- Approach
  - Identified candidate products
    - Those being certified via NIAP Evaluation Scheme
  - Defined Reliability Requirements
    - Defined operational modes
    - Set reliability objectives by failure severity category
    - Established operating conditions (Operational Profile) under which objectives are to be met.
  - Set up a test environment
    - Defined test scripts mimicking operating conditions
    - Established a test bed, test automation tools, test acceleration methods.
  - Executed reliability testing
    - Logged failure events
    - Tracked measured reliability against objectives

In a Nutshell

- Results
  - Simulated between 13 to 16 months of field activity
  - No severe failures observed
  - Observed 7 major failure events
    - No failures compromised the security of protected systems.
  - Produced quantified results showing progress in meeting reliability objectives
  - Observations
    - Operational Profile made sure we focused on how products are used.
    - Need to consider all users of system. Nearly all failures were associated with provisioning or administering the system.
    - Most failures were "multi-event" type failures.
    - Our opinion: "Failure proneness of products like this lie in the ability of **individuals** to manage the complexity to provision and administer these products."

In a Nutshell



Briefing Overview

- Project Objectives, Scope, Risk Mgt.
- Candidate Selection
- Reliability Requirements
- Test Environment
  - Test Bed
  - Test Drivers
- Reliability Testing
- Observed Failures
- Results
- Recommendations

Project Objectives

2.1.The contractor shall choose and follow the “standardized” software testing and reliability measurement methodology defined by John Musa …….

…… calculation of the functional reliability, R, of specified COTS security products.

2.2.1. Model two software based security products (COTS) in state machine representation.

2.2.2. Define three failure categories for classifying the failures expected during testing and verify with users that they are appropriately defined.

2.2.3. Define identical operational profiles for the selected systems using J. Musa’s technique ………

2.2.4. Generate statistically significant sets of test data for each operational profile. Target 90% degree of confidence levels in determining test set size for reliability estimations.

3.1 Standard software testing procedure descriptions which include discussions on modeling and reliability estimation.

3.2 Test suites for each operational profile and for each NIAP system under test.

3.3 Reliability and Mean Time Between Failure estimation calculations in report for for each system under test.

Project Scope, Risk Management

- Staffing
  - Senior Mathematician – 35 staff days
  - Senior Electronics Technician – 35 staff days
- Schedule
  - 9 months, April – December 2001
- Budget
  - Fixed price, $10,000 allocated for acquiring candidate products and test bed equipment
- Risks
  - Limited materials budget
  - Limited staff background with Firewalls
- Risk Management
  - Face-to-face project review meetings every 6 weeks
  - Adjust scope when needed.

Candidate Selection

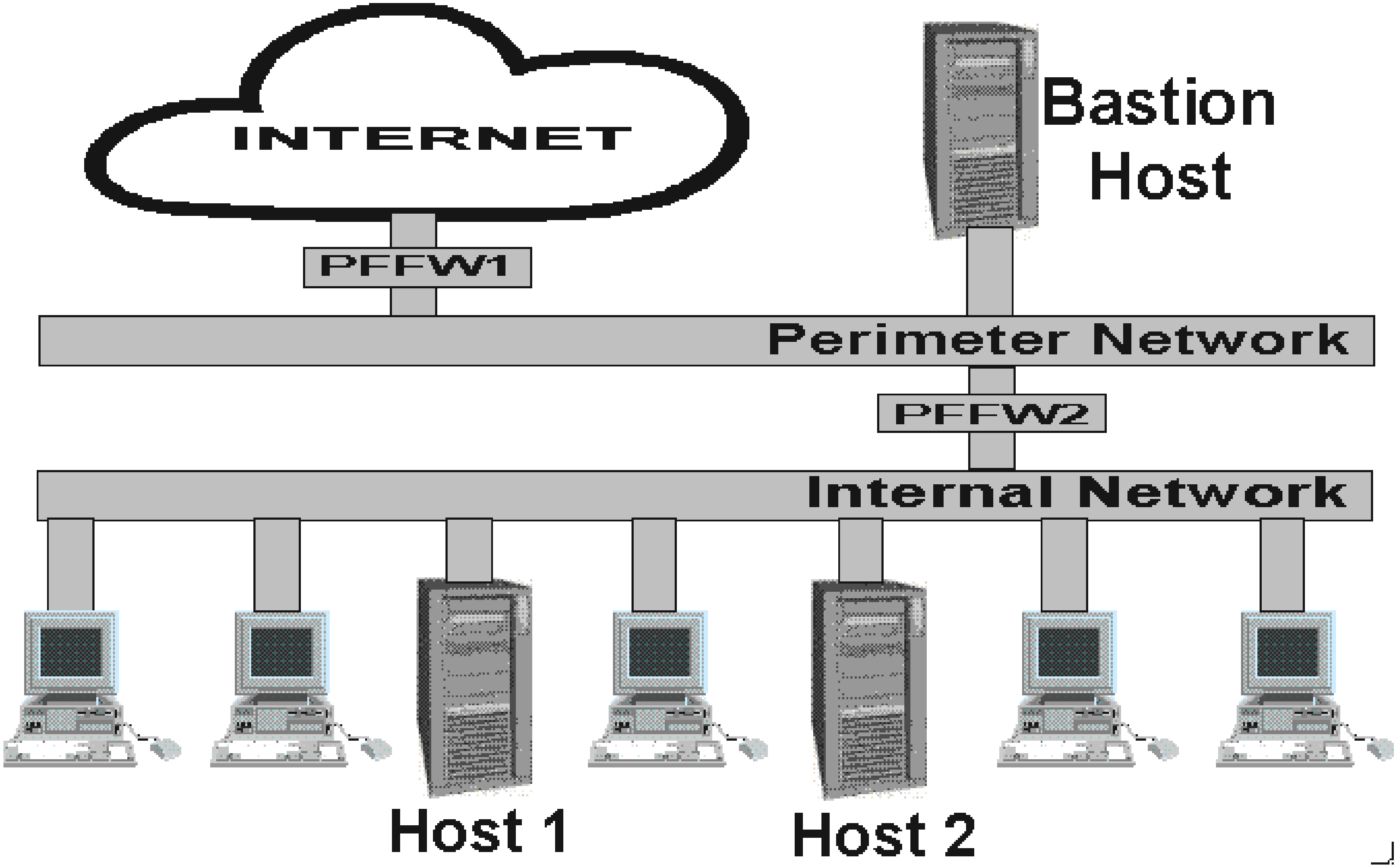
- Criteria
  - Candidates certified (or under certification) with respect to NIAP Common Criteria Evaluation for Packet Filter FireWalls (PFFW) protection profiles.
  - At least two candidates be selected.
  - Cost of acquiring the products fit project materials budget.
- Candidates
  - Cisco PIX 520 (certified EAL 2)
  - ☞ Gauntlet (under certification at EAL 4*)
  - Checkpoint (certified EAL 2)
  - ☞ Sidewinder (under certification at EAL 4)

*** vendor withdrew from certification after we selected it.**

Reliability Requirements

- Modelled on a particular agency organization
  - Interviewed the organization to obtain information
- Operational Profile
  - Operational Configuration
  - Packet Filter Rules
  - Operational Modes
    - Four Modes defined
    - Activity by Type
    - Activity by Hour of the Day
- Failure Modes
  - Based in part on PFFW Protection Profile
- Failure Severity Classes
- Reliability (Failure Rate) Objectives

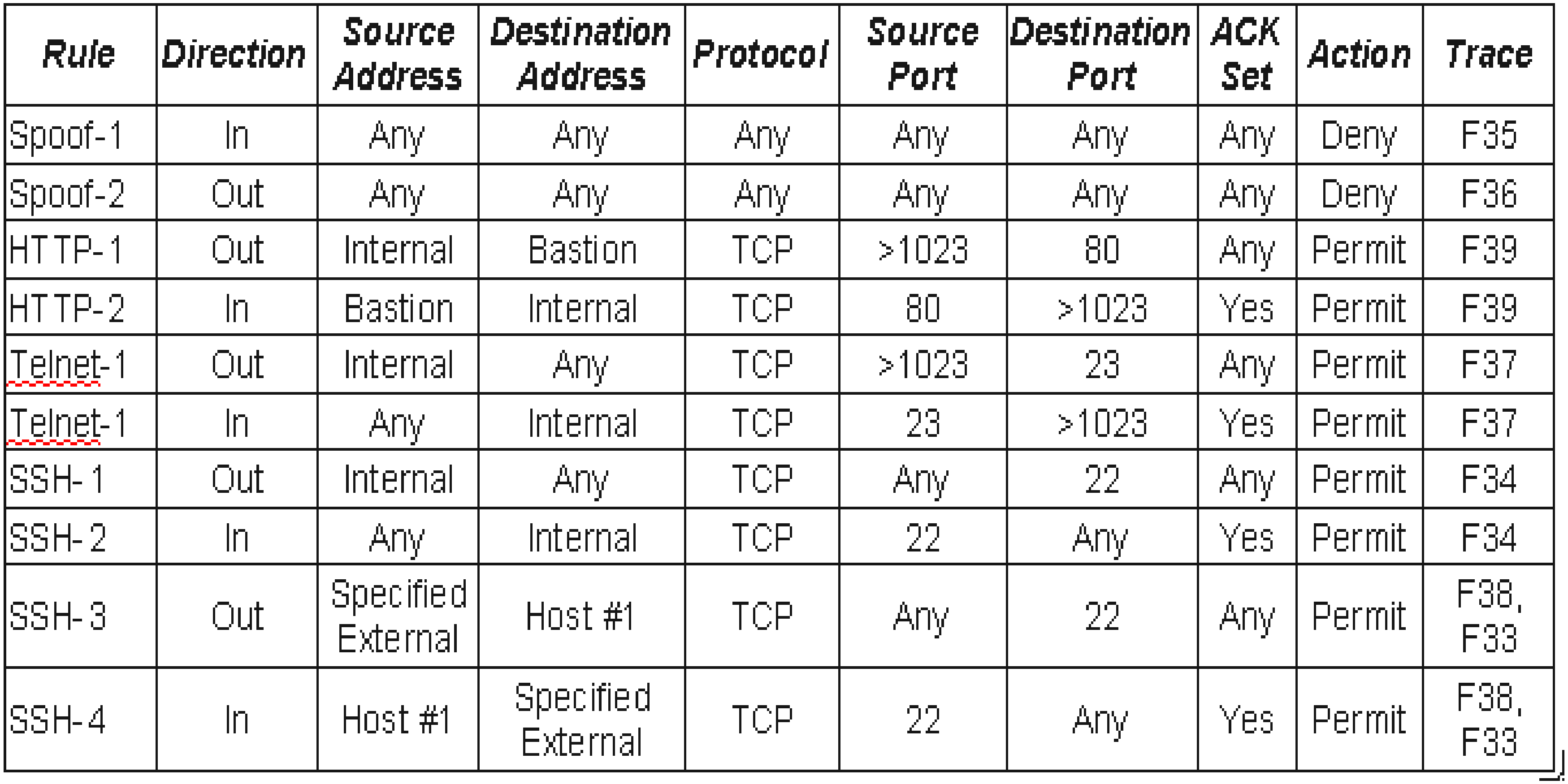
Operational Configuration



Machine Configuration

- Client machines
  - 100 on internal network.
  - Trusted clients on external network
- Bastion Host (Sun Solaris 2.7)
  - A public information website, proxy electronic mail, file transfer, internet web access (via http)
  - A DNS server that masks internal machines names.
- Internal Host 1 (WinNT Server)
  - A special information server (SIS)
- Internal Host 2 (Win2000 Server)
  - Electronic mail exchange service, an internal DNS, other internal-only services
- External Web Servers

Packet Filter Rules

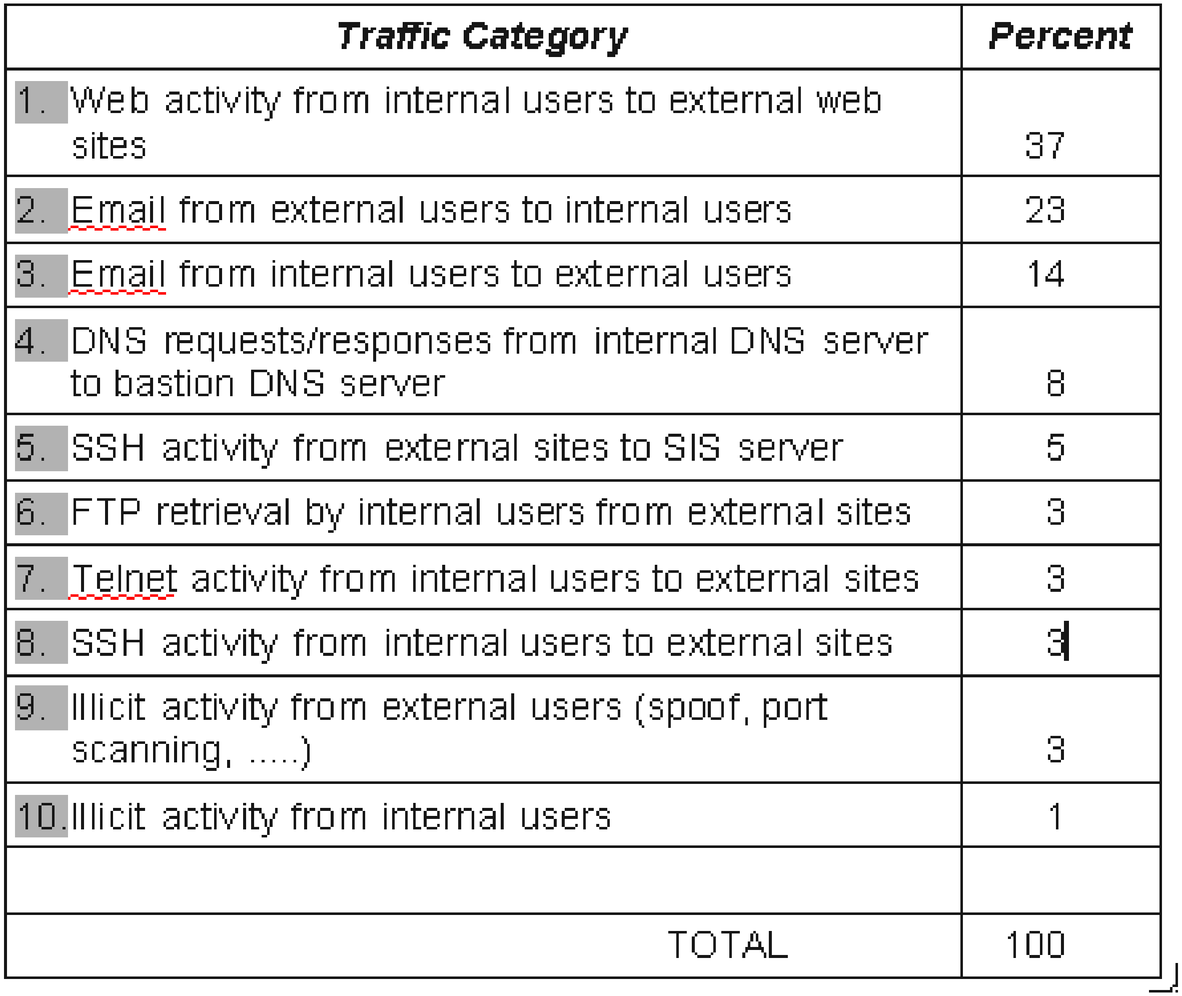


Rule	Direction	Source Address	Destination Address	Protocol	Source Port	Destination Port	ACK Set	Action	Trace
Spoof-1	In	Any	Any	Any	Any	Any	Any	Deny	F35
Spoof-2	Out	Any	Any	Any	Any	Any	Any	Deny	F36
HTTP-1	Out	Internal	Bastion	TCP	>1023	80	Any	Permit	F39
HTTP-2	In	Bastion	Internal	TCP	80	>1023	Yes	Permit	F39
Telnet-1	Out	Internal	Any	TCP	>1023	23	Any	Permit	F37
Telnet-1	In	Any	Internal	TCP	23	>1023	Yes	Permit	F37
SSH-1	Out	Internal	Any	TCP	Any	22	Any	Permit	F34
SSH-2	In	Any	Internal	TCP	22	Any	Yes	Permit	F34
SSH-3	Out	Specified External	Host #1	TCP	Any	22	Any	Permit	F38, F33
SSH-4	In	Host #1	Specified External	TCP	22	Any	Yes	Permit	F38, F33

Operational Modes

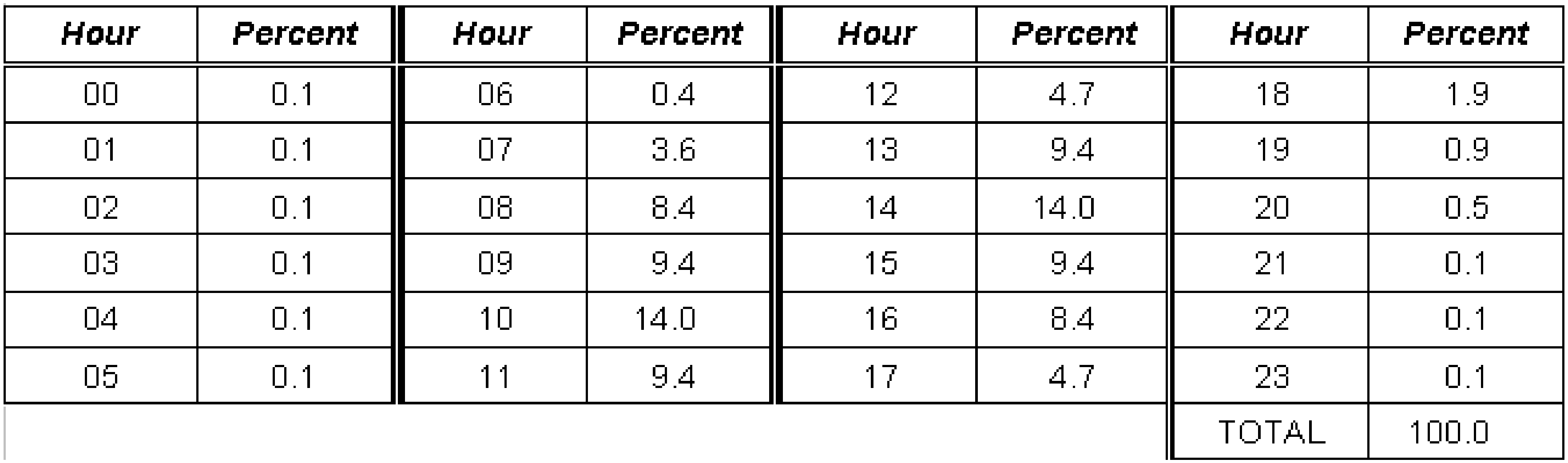
- Installation/Configuration
  - Once every 6 months
- Power-down/Restart
  - Once per month
- Power-loss/Recover
  - Once every 2 months
- Regular Operation
  - Average Workday
    - 500MB out, 40MB in, 1KB packet size
    - 540,000 packets per day
  - Weekend/Holiday
    - 5% of Average Workday
  - Peak Day
    - 125% of Average Workday

Activity by Type



Traffic Category	Percent
1. Web activity from internal users to external web sites	37
2. Email from external users to internal users	23
3. Email from internal users to external users	14
4. DNS requests/responses from internal DNS server to bastion DNS server	8
5. SSH activity from external sites to SIS server	5
6. FTP retrieval by internal users from external sites	3
7. Telnet activity from internal users to external sites	3
8. SSH activity from internal users to external sites	3
9. Illicit activity from external users (spoof, port scanning, ...)	3
10. Illicit activity from internal users	1
TOTAL	100

Activity By Hour of Day*



Hour	*Percent*	*Hour*	*Percent*	*Hour*	*Percent*	*Hour*	*Percent*
00	0.1	06	0.4	12	4.7	18	1.9
01	0.1	07	3.6	13	9.4	19	0.9
02	0.1	08	8.4	14	14.0	20	0.5
03	0.1	09	9.4	15	9.4	21	0.1
04	0.1	10	14.0	16	8.4	22	0.1
05	0.1	11	9.4	17	4.7	23	0.1
						TOTAL	100.0

*** In terms of packets transmitted/received through FireWall**

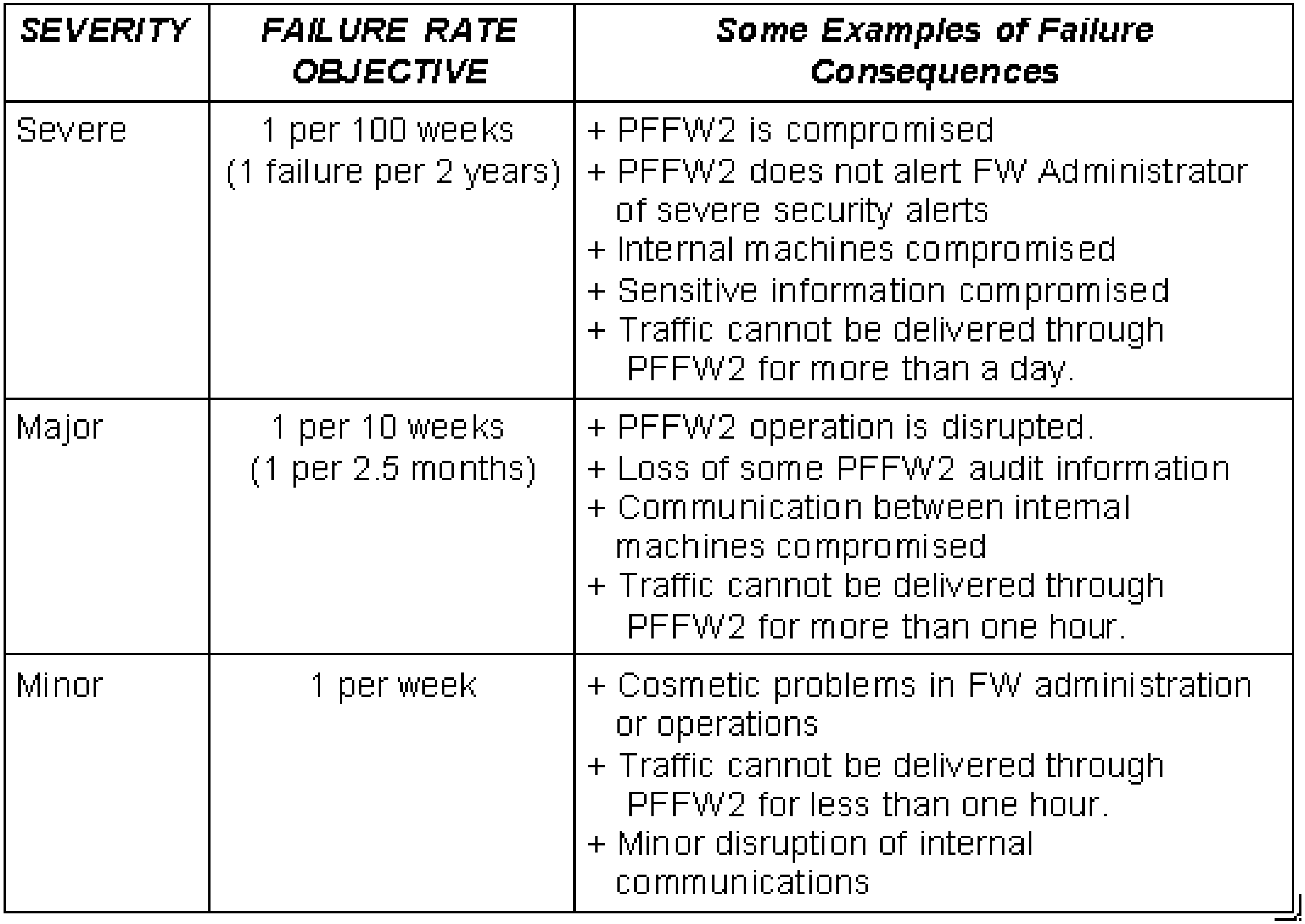
Failure Modes

- The PFFW2 is down for more than 1 hour, 1 day, several days so no traffic can flow through the firewall.
- The security capabilities of PFFW2 are not functioning correctly after a recovery from a power outage. from a normal reboot.
- An unauthorized person gains access and use to functions provided by PFFW2.
- The firewall administrator is not alerted to an unauthorized person repeatedly guessing authentication data in order to use this information to launch attacks on the PFFW2.
- An unauthorized person on the external network by-passes the information flow control policy of PFFW2 by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on the internal network.
- An unauthorized person sends impermissible information through PFFW2 which results in the exploitation of resources on the internal network.

Failure Modes (cont'd)

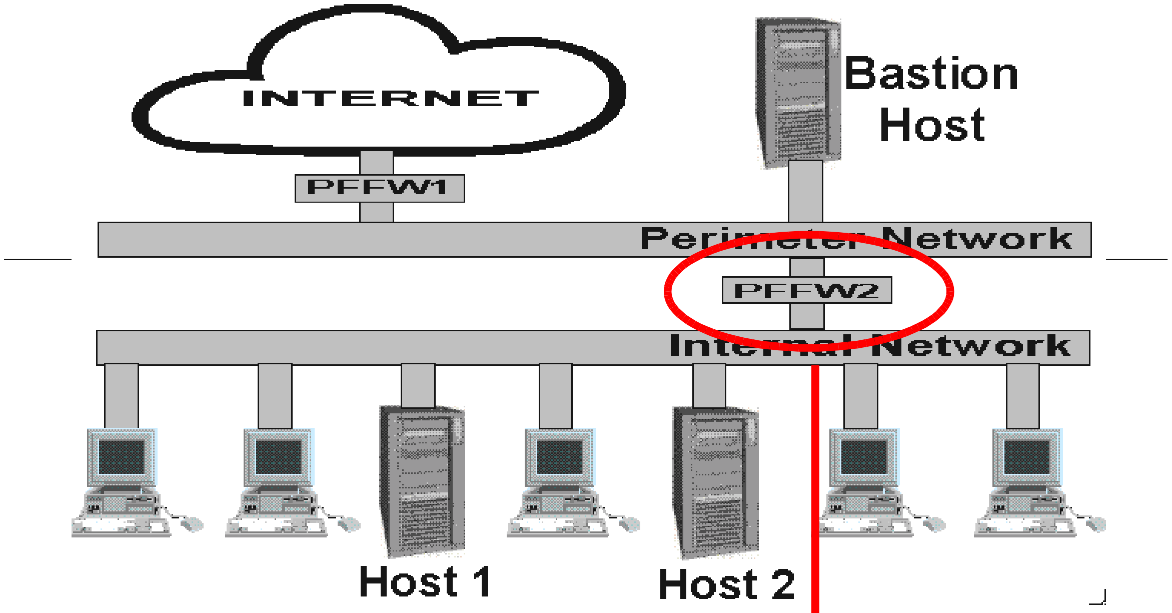
- The PFFW2 software or hardware cannot be installed or configured.
- Because of a flaw in PFFW2, an unauthorized person gathers residual information from a previous information flow or internal PFFW2 data by monitoring the padding of the information flows from PFFW2.
- The PFFW2 audit records are incomplete or lost resulting in persons not being accountable for the actions that they conduct.
- An unauthorized person can read, modify, or destroy security critical configuration data in PFFW2.
- An unauthorized person causes audit records to be lost or prevents future records from being recorded by taking actions to exhaust audit storage capacity in PFFW2, thus masking an attackers actions.
- PFFW2 allows a skilled attacker with moderate attack potential to bypass security features to gain access to PFFW2 or the assets it protects.
- PFFW2 may be inadvertently configured, used and administered in a insecure manner by either authorized or unauthorized persons

Failure Severity Classes and Failure Rate Objectives

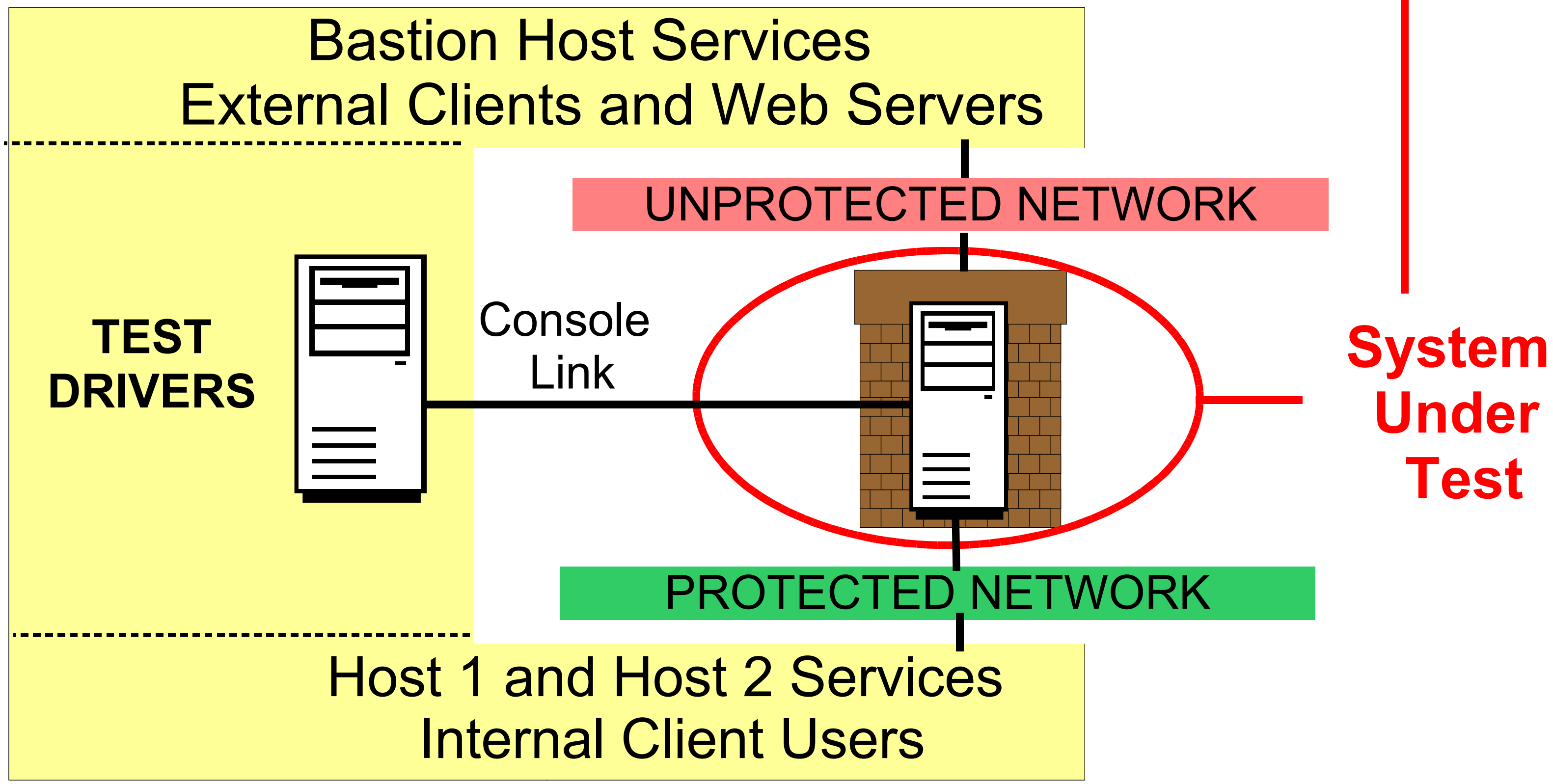


SEVERITY	*FAILURE RATE OBJECTIVE*	***Some Examples of Failure Consequences***
Severe	1 per 100 weeks (1 failure per 2 years)	+ PFFW2 is compromised + PFFW2 does not alert FW Administrator of severe security alerts + Internal machines compromised + Sensitive information compromised + Traffic cannot be delivered through PFFW2 for more than a day.
Major	1 per 10 weeks (1 per 2.5 months)	+ PFFW2 operation is disrupted. + Loss of some PFFW2 audit information + Communication between intemal machines compromised + Traffic cannot be delivered through PFFW2 for more than one hour.
Minor	1 per week	+ Cosmetic problems in FW administration or operations + Traffic cannot be delivered through PFFW2 for less than one hour. + Minor disruption of internal communications

Test Environment



SPRE06
SUN ULTRA 5



Bastion Host Services
External Clients and Web Servers

UNPROTECTED NETWORK

TEST DRIVERS

Console Link

System Under Test

PROTECTED NETWORK

Host 1 and Host 2 Services
Internal Client Users

Test Drivers

- Can simulate over 100 IP addresses
- Use NAT* to route traffic between subnets
- Packet generator
  - Create listener/transmitter pair with arbitrary source/destination IP addresses and ports.
  - Open a TCP session and exchange a specified number of packets
- Traffic generator
  - Simulate HTTP, telnet, ftp, SSH, DNS session activity at specified rates, log activity and results
- Port probing of FireWall
  - Simulated some hacking activity
    - TCP Ping, connect, SYN, FIN, Xmas scans

* **Network Address Translation**

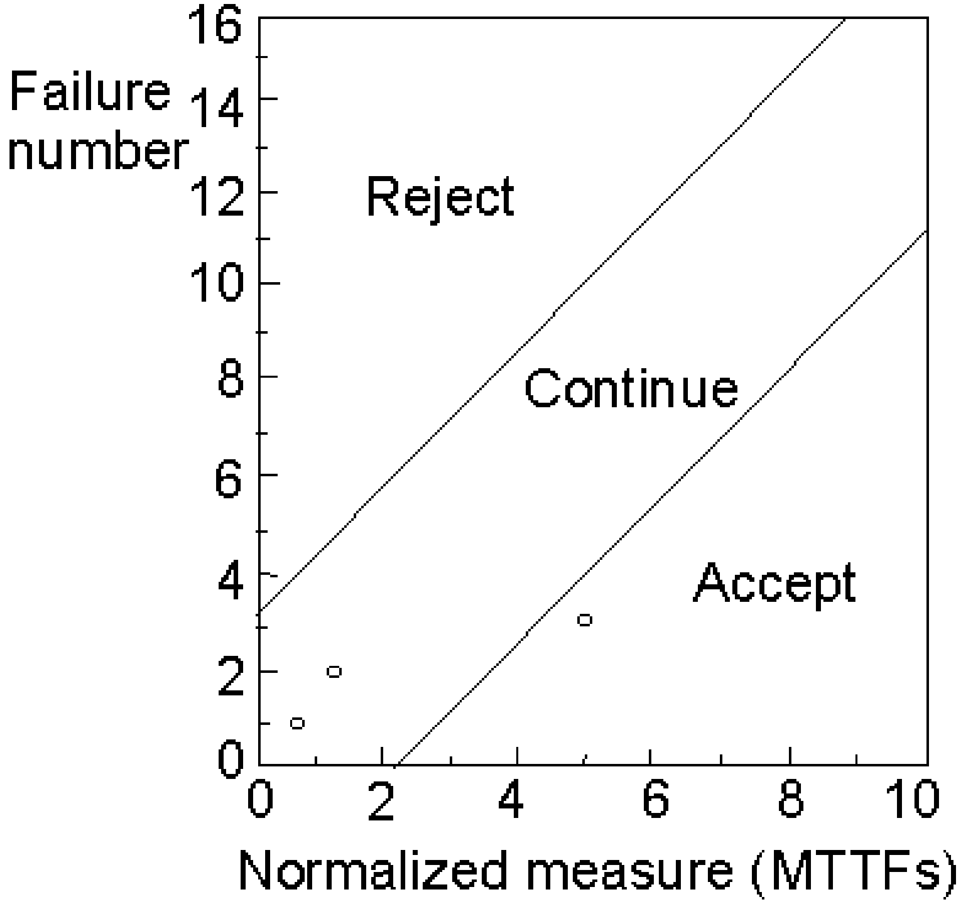
Reliability Testing

- Executed test cases with frequency dictated by the Operational Profile
- Automated
  - Normal operation
  - Accelerated testing
    - Reduced packet size
    - Could transmit 540,000 packets/hour = 1 workday activity
    - Run 4-6 hour sessions over 1 to 3 day period.
- Manual Test
  - Installation/configuration
  - Backup/restore
  - Power outage/restore
  - Interleaved results with Normal Operation

Observed Failures

- Failure descriptions
  - Configuration conflict between application and OS/hardware on installation
    - wrong "media" for hardware/OS version
    - wrong directory permissions for email delivery.
  - Administrative reporting of certain system events
    - failure to do "clean" file system check after a power restore
    - alerting when the maximum user limit specified by the license is reached.
  - Other
    - conflict between telnet packet filter rules and telnet proxy server application
    - IP address interpretation (192.168.1.**047** vs 192.168.1.**47**)

Used Reliability Demo Charts to Track Testing progress



Fail. No.	Mcalls at Failure	Number of MTTFs
1	0.1875	0.75
2	0.3125	1.25
3	1.25	5

Failure intensity objective:
4 failures / Mcalls

Use when no repair activity is underway, e.g. during field operation.

Results

- Observations
  - Field of Use
    - The differences in observed reliability between the two products can be explained in part by differences in the intended use of each product and the architectures adopted to meet the intended use.
  - Configuring a FireWall is a complex task, open to human error.
    - Weakest Link – capability of a person to configure and administrate a Firewall.
    - The vendors for both products sold separately support coverage for provisioning/administering their products.
  - Balance security with usability
    - Analogy – a perfectly safe aircraft has so many safety interlocks that the aircraft will never take off. Buttttt, you would never run an airline with it.

Recommendations

- Include Reliability Testing in EAL Matrix
  - I.e., for which EAL levels should Reliability Testing be specified.
- Special considerations in the Reliability Testing of Security-based products.
  - Administration/Provisioning/Maintenance Activities
    - Can we automate them more so we can focus more and varied test activity on them?
    - Establish better guidelines on counting repeated failures or not, interleaving results with normal activity.
    - Can we exploit test acceleration with other operational modes?
  - Normal Operation
    - How do we include "hacking" activity in the Operational Profile?
    - Can we automate testing for other Protection Profiles, e.g. Application FW PP, Switch/Router PP, Biometric PPs.

References

Musa, John. 1999. **Software Reliability Engineering.** McGraw-Hill,New York, NY. ISBN: 0-07-913271-5

Zwicky, Elizabeth, Simon Cooper, and Brent Chapman. 2000. **Building Internet Firewalls Second Edition.** O'Reilly & Associates. Sebastopol,CA. ISBN: 1-56592-871-7

Department of Defense, **Final – Traffic-Filter FireWall Protection Profile For Medium Robustness Environments,** Version 1.4, 1 May 2000, http://www.iatf.net/protection_profiles/firewalls.cfm

Department of Defense, **FireWall Protection Profiles Frequently Asked Questions,** 19 December 1997.

McClure, Stuart, Joel Scambray, and George Kurtz. 2001. **Hacking Exposed Third Edition**. McGraw-Hill, New York, NY. ISBN: 0-07-219381-6