Freescale Semiconductor

White Paper

Freescale and Kaspersky® Accelerated Antivirus Solution Platform for OEM Vendors

Overview

Accelerated Antivirus (Accelerated AV) is a high-performance network antivirus solution platform jointly offered by Kaspersky® Lab and Freescale Semiconductor, Inc. to OEM vendors. Accelerated AV is based on Freescale's MPC8572E PowerQUICC™ III processor built on Power Architecture™ technology and Kaspersky's SafeStream signatures database. The platform enables the rapid development of competitive, high-performance, cost-effective network AV devices that are highly effective in the mitigation of the impact of dangerous and widespread malware (viruses, worms and trojans) and malware outbreaks.

Contents

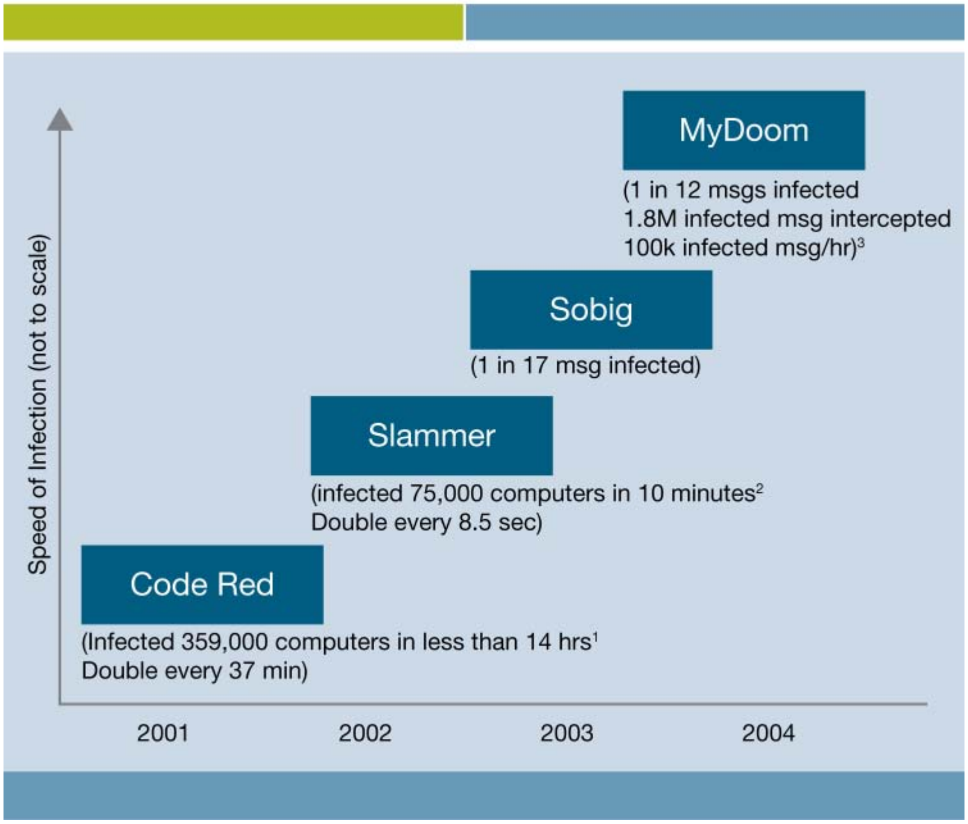
1 Network Antivirus Landscape and Trends

The damage caused by computer malware is very significant. Today, most computers in enterprises are protected by antivirus software to minimize the damage potentially caused by malicious programs.

According to CERT®, "The speed at which viruses are spreading is increasing … we have seen worm propagation times drop from hours to minutes."

The graph illustrates the speed of infection of major malware outbreaks in recent years.[1, 2, 3]

Speed of Major Malware Outbreaks



Unfortunately, it may take days, if not weeks, to apply software patches and malware signature updates to all PCs and servers in a large enterprise to defend against a new malware. Meanwhile, the malware is already invading the enterprise network.

A network-based solution is inherently more effective than a host-based solution to control malware propagation—applying updates to the much fewer number of network AV devices takes less time (and consumes less network bandwidth). A suitably positioned network-based AV device stops malware before it gets to the host computers. Most enterprises are therefore using network-based AV solutions to mitigate the impact of malware outbreaks to complement a host-based AV solution for in-depth defense.

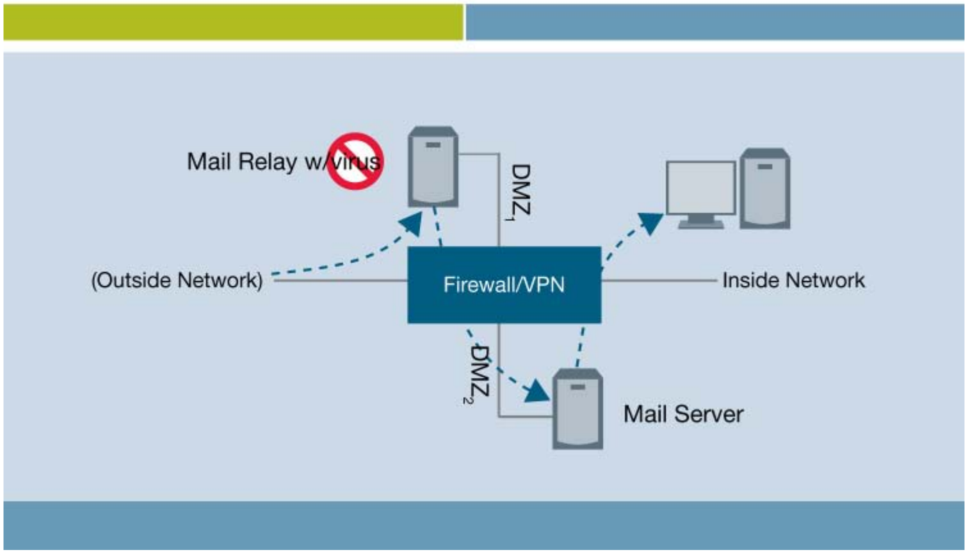
[1] CAIDA. "Analysis of Code Red." http://www.caida.org/analysis/security/code-red/

[2] David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford and Nicholas Weaver. "The Spread of the Sapphire/Slammer Worm." http://www.cs.berkeley.edu/˜nweaver/sapphire/

[3] www.messagelabs.com

Traditional network AV is proxy based. In a typical deployment scenario, the mail relay receives the complete e-mail, invokes the antivirus function and forwards the e-mail on to the mail server if it is checked out to be clean. This is a store-and-forward operation. Real time is not a primary concern. Only e-mail traffic—a fraction of the total traffic going into or out of the enterprise network—goes through the mail relay. If there is a delay of a few seconds or even a few minutes, the end-user does not notice.

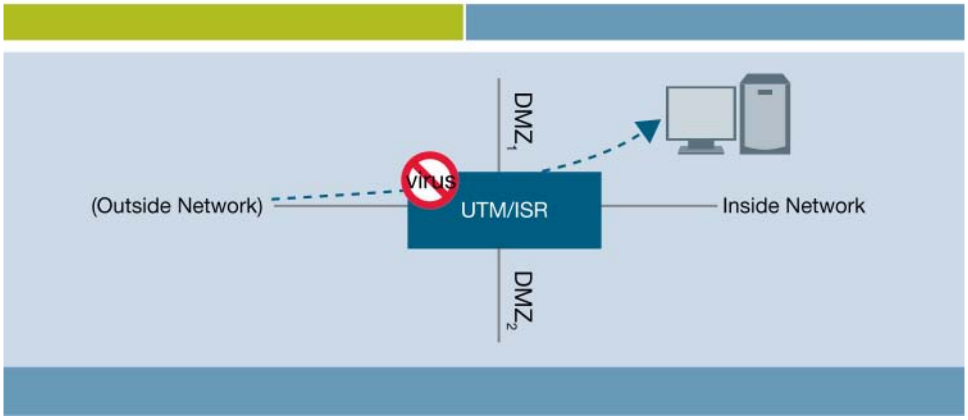
Traditional Network AV Deployment



However, malware is not only carried by e-mails—it can be propagated by a variety of protocols including those used in real-time sensitive Web and multimedia messaging applications.

There is also a trend towards Universal Threat Management (UTM) or Integrated Services Router (ISR) to reduce cost and simplify operation. This is a single network device with routing, firewall, IDS/IPS, antivirus, anti-spam and content filtering functions.

Network AV Deployment in UTM/ISR



Compared with the e-mail relay, there is a lot more traffic—different types of traffic, including e-mail—streaming through the UTM/ISR. The throughput performance has to be high or else the AV device will bottleneck network traffic. The latency has to be low or else time-sensitive applications like VoIP, Instant Messenger and the Web will be affected.

2 Design Challenges

OEM vendors are faced with a number of design challenges in order to develop and support an effective product to win in the network-based antivirus marketplace. These include:

- High performance
- High accuracy
- Cost effectiveness
- Guaranteed, continual, timely availability of accurate malware signatures coupled with fast, in-service, incremental updates of signatures

As an inline networking device, the network AV system should perform at line-rate with minimal delay in order to avoid slowing down traffic. To be able to detect malware accurately—i.e. no false positives, no false negatives—is the prerequisite of a high-quality AV system.

The combination of Gbps line rate performance and accurate detection of malware is particularly challenging. While a purely software-based detection mechanism can be made to be very accurate, the performance achievable with today's technology is only a hundred Mbps or so. Simple string matching hardware can provide the speed required, but places a limit on the sophistication of signatures and hence the ability to detect complex viruses. Today, accurate Gbps virus detection implies the use of hardware pattern matching technology with powerful, regular-expression (RegEx) capabilities.

To compete successfully in the market, the network AV device has to be cost effective. A device built from several discrete processors and hardware components may achieve the performance and accuracy required, but the bill of materials and development costs will likely become too high for the marketplace.

Even if all the challenges regarding speed, accuracy and cost are met with regard to building the network AV device, there are still additional challenges. To complete the story on accuracy and speed, a set of sophisticated, hardware-friendly malware signatures is required to populate the pattern matching hardware in the network AV device. This is not a one-time activity; to stay effective in stopping malware propagation, the Pattern Matcher needs to be updated in a timely manner with the latest signatures that match the new malware. This translates to two distinct requirements:

- The continual, guaranteed, timely availability of accurate signatures to combat malware outbreaks
- The capability to compile and load new signatures quickly while the network AV device is in service

Switching back to performance, as more and more signatures are added to detect newer malware, the real-time performance of the device should not degrade. These requirements cannot be taken for granted. The OEM vendor must ensure that the chosen platform can meet all of these requirements.

3 Accelerated AV Solution Platform

The Accelerated AV solution platform is jointly offered by Kaspersky and Freescale to OEM vendors. The platform enables the rapid development of competitive, high-performance and cost-effective network AV devices, including Universal Threat Management (UTM) and Integrated Service Router (ISR).

The solution platform consists of components from Freescale and Kaspersky.

3.1 Freescale Components

The solution platform components available through Freescale or its distributors include the following:

- MPC8572E PowerQUICC™ III processor with integrated pattern matcher
- Associated software
- Associated documentation

Software includes drivers and board support packages that are typical of Freescale processors. In addition, specific to the MPC8572E and other future processors with a built-in Pattern Matcher, it also includes Pattern Matcher-specific software for Linux®:

- Pattern management software:
  - RegEx compiler
  - Stateful rule compiler
  - Linker loader
  - Sample Pattern Matcher management application
- Pattern Matcher driver
- Sample Pattern Matcher data scan application

With these, the OEM will be able to develop its product hardware and software.

3.2 Kaspersky Components

The solution platform components available through Kaspersky are:

- Kaspersky SafeStream signatures database in binary Freescale Pattern Matcher format
- Regular daily updates and urgent (in case of malware outbreaks) updates of Kaspersky SafeStream signatures database, also in binary Freescale Pattern Matcher format

In other words, before delivery to the OEM, native Kaspersky SafeStream signatures are:

- Pre-converted to Freescale format
- Pre-compiled to Freescale binary format
- Verified to work with Freescale's Pattern Matcher

3.3 OEM Responsibility

It is the responsibility of the OEM to develop the following:

- Proprietary system hardware powered by the MPC8572E PowerQUICC III
- Proprietary management and scanning software utilizing the Pattern Matcher
- Mechanism to deliver the signatures in Freescale binary format to its customers, who will link and load the signatures into the network AV device. It is the OEM's choice whether to incorporate the linking and loading of signatures into its security policy management framework.

The OEM may choose to use products and services from other ODMs to develop the complete solution.

3.4 MPC8572E PowerQUICC III Processor Overview

The MPC8572E is an advanced PowerQUICC III processor purposely built to meet the requirements of high-performance application-aware networking and content security. It is based on—and an enhancement to—the highly successful PowerQUICC system-on-chip (SoC) platform, well-proven in traditional networking; with further incorporation of new hardware optimized to process application content at high speeds.

The MPC8572E consists of dual e500 cores built on Power Architecture™ technology at clock speeds from 1.2 GHz to 1.5 GHz. The CPU cores, each with 32 KB I-Cache and 32 KB D-Cache, share 1024 KB of integrated L2 cache. For memory, the MPC8572E includes two integrated 64-bit DDR2/DDR3 SDRAM controllers.

To further speed up processing while keeping power dissipation down, the MPC8572E integrates powerful engines: a security engine that accelerates crypto operations in IPSec and SSL/TLS; a pattern-matching engine to handle regular expression matching; a deflate engine to manage file decompression; and two table look-up units (TLU) that manages complex table searches and header inspections.

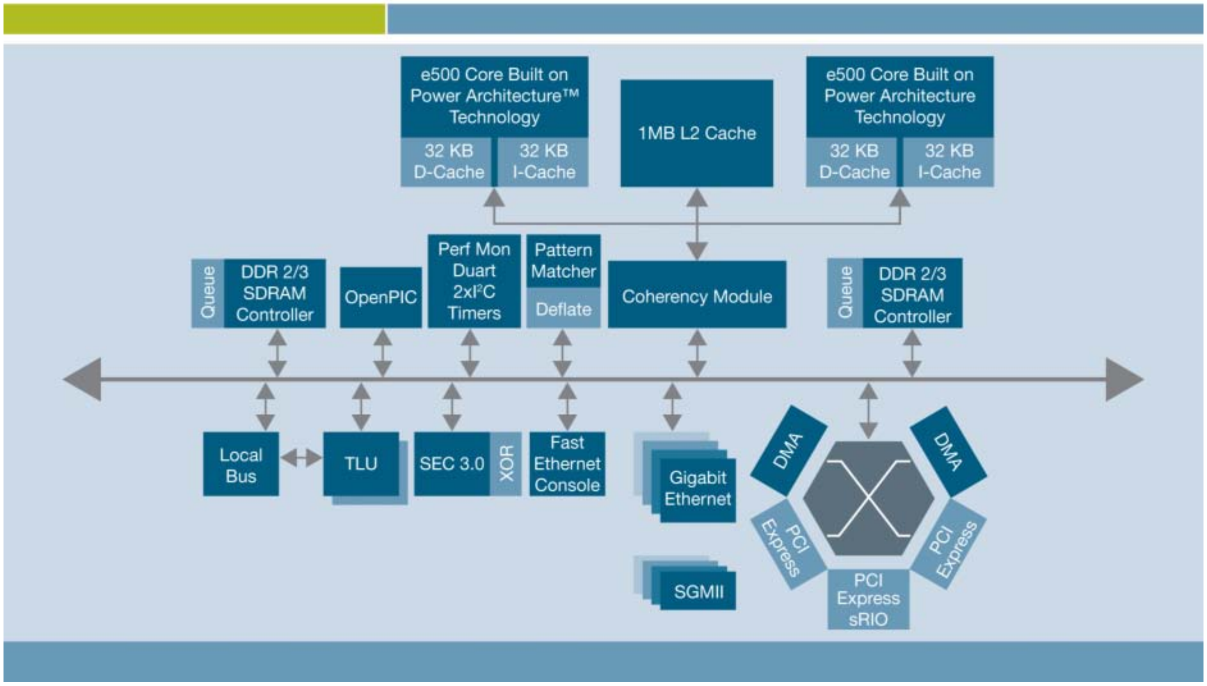
The MPC8572E offers a combination of network interfaces, including 4 integrated enhanced Triple-Speed Ethernet Controllers (eTSEC). These controllers accelerate packet I/O by offloading checksum calculation. They also provide QoS support with eight Rx queues and eight Tx queues to accelerate traffic management.

For high-speed connectivity to other devices, the MPC8572E supports PCI Express®, Serial RapidIO® and DMA interfaces.

The major processing and I/O elements are integrated into the MPC8572E with a highly optimized internal interconnect architecture to ensure high bandwidth, low latency and efficient pipeline operation, balancing processing performance with I/O system throughput.

Based on Freescale's 90 nm silicon-on-insulator (SOI) copper interconnect process technology, the MPC8572E is designed to deliver higher performance with lower power dissipation.

MPC8572E PowerQUICC III



3.4.1 Pattern Matcher

The Pattern Matcher is an integrated hardware block inside the MPC8572E with the following capabilities:

- High performance, feature-rich hardware pattern matching of compressed and uncompressed data
  - Patterns expressed in RegEx with significant capabilities beyond that provided by the RegEx language
  - Stateful rule—correlates multiple pattern matches and maintains state between matches
- Improvements over other pattern matching technologies:
  - No pattern “explosion” to support “wildcarding” or case-insensitivity
  - Fast compilation of pattern database
  - Fast incremental additions to pattern database
  - Live pattern database update
  - Patterns stored in main DDR DRAM, not SRAM or FCRAM
- On-chip hash tables for low system memory utilization, removing need for costly low-latency memory technologies
- Pattern matching across data “work units” (e.g. can match patterns split across TCP segments)

3.5 Kaspersky SafeStream Overview

Kaspersky SafeStream is dedicated for:

- Detection of the most dangerous and widespread malware (viruses, worms, trojans as well as spyware) threats
- Performing low latency detection at wire speed with help of hardware acceleration
- Provisioning appropriate level of protection for almost all kinds of networking and security devices independently of software and/or hardware used

Kaspersky SafeStream signatures database contains signatures of dangerous and widespread viruses, trojans, worms as well as spyware. Using these signatures the network AV device can block malware threats before they reach the host computers in the network.

The Kaspersky SafeStream signatures database allows high-performance malware filters to be implemented on platforms where, due to limitations in architecture, processing power or memory, traditional antivirus software is not operable. The database includes signatures compatible with common pattern-matching engines as well as regular expressions (RegEx) matching engines, software or hardware-based.

The Kaspersky SafeStream signature database is updated every day at a fixed time—“daily updates” and additional “urgent updates” can be issued several times a day during a malware outbreak. “Urgent updates” are created on the same time frame as “urgent updates” for standard Kaspersky Lab products.

The Kaspersky SafeStream signatures database, when coupled with a third-party RegEx pattern-matching engine, can be used as a stream-based malware scanning solution where, unlike in a traditional proxy-based malware scanning solution, network traffic is processed packet by packet. The scanning process therefore requires very little additional memory for packet sequencing and reassembly. Likewise, the solution does not affect throughput and its operation is not dependent from object size, which slows down scanning in conventional antivirus engines. Malware scanning based on Kaspersky SafeStream, when combined with an appropriate hardware acceleration platform, provides excellent speed and throughput. This approach delivers efficient gateway-level protection from dangerous malware threats and outbreaks.

This solution is not meant to protect against all malware—the emphasis is rather on ensuring the highest possible performance while providing protection from the most dangerous and widespread threats. It is meant to be used in high-performance network-based AV solutions to mitigate the impact of new outbreaks to complement a host-based AV solution for defense-in-depth solutions.

To sum up, the key features and benefits of SafeStream are:

- Unparalleled performance
    - Hardware acceleration compatibility
    - Throughput is independent of processing object sizes
    - Minimal added latency even during malware outbreaks
    - Possibility to achieve wire speed malware scanning
- Maximum compatibility
    - Hardware and software platform agnostic
    - Possible integration into embedded systems
    - Perfect for solutions with limitations in the architecture, processing power or memory
- Protection against most dangerous and wide-spread malware
    - Timely response to the most dangerous viruses, worms, trojans as well as spyware programs
    - Based on real-time malware spreading statistics gathered by Kaspersky Lab
    - Regular daily updates and urgent updates in case of malware outbreaks

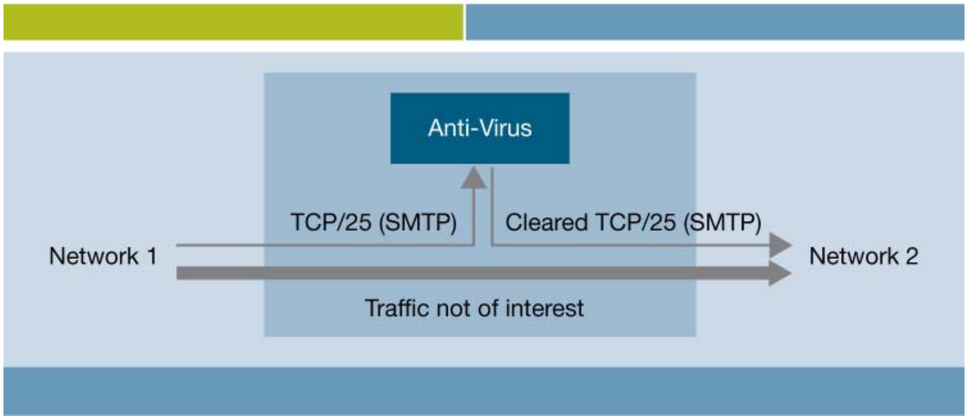
4 Designing Network-Based AV with the Accelerated AV Platform

4.1 Network AV Operations

In order to understand what an ideal network AV platform looks like, let’s examine the key operations performed in a typical network AV device. Note that while SMTP is used in the example, other application protocols carrying the file/object to be inspected are also applicable. The Accelerated AV solution is independent of the application protocol.

4.1.1 Data Path

Typical Network AV Operation



The key data path operations in a typical network AV device are as follows:

- Allow traffic not of interest to flow through transparently
- Reassemble (with or without transparent TCP termination) traffic of interest—SMTP is used in the above diagram, but other traffic such as HTTP and FTP are also applicable
- Observe end-to-end SMTP protocol exchange and capture e-mails on the fly
- MIME decode, separate e-mail into component parts, e. g. attachments
- Additional unpacking/decompression (for example, unzipping) processing of message’s attachments
- Compare e-mail body and attachments against the configured malware signatures
- Delete, modify, quarantine bad e-mail as required
- Forward safe e-mail to destination

Four key types of processing are involved:

1. Packet I/O and processing, for both “interesting” and “non-interesting” traffic
2. Application protocol processing for the “interesting” traffic
3. MIME decode and unpack/decompress for messages of interest
4. Match suitable parts of the processed messages against malware signatures

By far, the most time-consuming operations are decode and unpack/decompress processing, as well as matching of e-mail body and attachments against malware signatures.

4.1.2 Control Path

The key operation of concern is populating the device with malware signatures so that during the runtime datapath, the device can determine whether network traffic is infected by matching it against the configured signatures.

The process after a new malware sample is discovered is as follows:

1. The team of antivirus experts creates accurate signature(s) that would match the new malware sample and possibly its variants
2. The new signature is converted to a format that is native to the Pattern Matcher used in the AV platform
3. The converted signature is compiled to a binary, machine-readable format
4. The binary signature is (linked and) loaded into the AV hardware platform

Depending on the design of the Pattern Matcher and the overall system, the steps involved may differ, and only some of the steps are performed by the network AV device:

- Compilation time: it may take a fraction of a second or hours to compile and link a new signature
- Incremental update: the new signature may be incrementally added or the complete set of signatures has to be loaded again
- Live update: loading may be done while the system is up or the system has to be taken down

4.2 Network AV Operations Using Accelerated AV

In an Accelerated AV-based network device, the operations are executed on the MPC8572E and the malware signatures provided by Kaspersky are pre-compiled to the Freescale format, and pre-tested on the Freescale hardware platform.

Network AV operations are well suited to the Asymmetric Multi-Processing (AMP) usage model on the dual-core MPC8572E:

- Control Path runs on dedicated CPU Core2, interacting with the Pattern Matcher to link and load the new signatures incrementally while the system is up and running
- Data Path for “non-interesting” traffic forwarding runs on CPU Core1 with the TLU used to accelerate flow table lookup and eTSEC, network I/O
- Data Path for “interesting” traffic:
    - Packet I/O: runs on CPU Core1 with the TLU used to accelerate flow table lookup and eTSEC, network I/O
    - Reassemble/terminate TCP, application protocol processing, MIME-decode, decompress, matching of application data against signatures: execute on CPU Core2 with the help of the Pattern Matcher and Deflate Engine

4.2.1 Performance Advantage—Data Path

The MPC8572E, with its powerful e500 CPU cores, acceleration hardware blocks (TLU), I/O elements (eTSEC) and highly efficient interconnect architecture, supports multi-Gbps line rate packet I/O processing. For details, please see related white paper.[4]

The advanced integrated Pattern Matcher and Deflate Engine, coupled with the e500 core, enable application protocol processing, MIME-decoding, decompressing and matching of sophisticated malware signatures at line rate.

Specifically, a powerful e500 core is used for application protocol processing and decoding. The Deflate Engine can be called upon to accelerate and offload decompression if required. The integrated Pattern Matcher with its powerful RegEx and Stateful Rule capability enable very sophisticated signatures be designed and hence enable highly accurate

[4] Freescale white paper entitled “Designing Firewall/VPN with the PowerQUICC™ III MPC8572E”

detection. Its rated raw performance at 2.4 Gbps throughput and about 5 microsecond latency remain essentially constant with the number of patterns configured. Furthermore, the Deflate Engine and the Pattern Matcher operate in a pipeline, minimizing interaction with the CPU core, resulting in increased performance.

4.2.2 Performance Advantage—Control Path

The key advantage of using the Accelerated AV platform for the Control Path is that the network AV device can start using the accurate SafeStream signatures to stop new threats early:

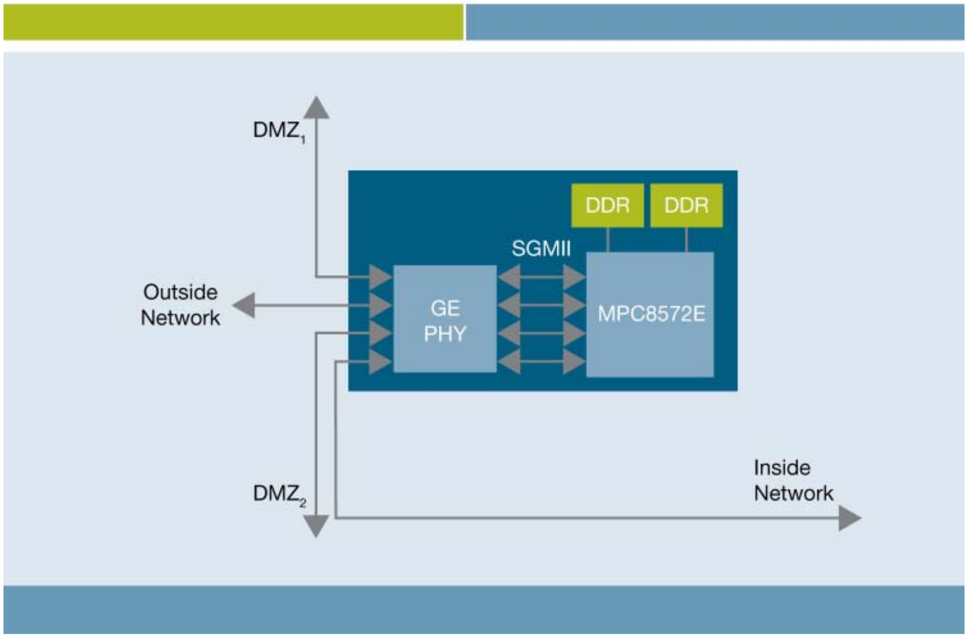
- New updates of the SafeStream signatures database matching new malware are provided on a daily basis, further augmented with emergency updates if required
- Compilation of a pattern is fast—one to a few seconds depending on the number of patterns—unlike some Pattern Matchers in the market
- The signatures delivered to the OEM are already in the compiled binary format, ready to be linked and loaded into the network AV device
- The Pattern Matcher supports a fast, live incremental signature update in a matter of seconds

4.3 Network AV Hardware Platform Design with the MPC8572E

As seen in Section 4.1.1, the AV device is a networking device with high packet rate, with part of the traffic requiring further examination for malware detection.

The simplified block diagram below shows the essence of a 4-port network security appliance, illustrating how easy a system design based on the MPC8572E can be. With suitable software, the appliance can be turned into a network AV device.

4-Port Security Appliance



4.3.1 Cost Advantage

The very simple system design—a direct result of the exceptional integration in the MPC8572E—enables significantly lower system cost and shorter time to market.

There is no separate pattern matching hardware to complicate the design and add additional cost. Similarly, there is also no separate expensive low latency memory—the MPC8572E's built-in Pattern Matcher does not need it for high performance, unlike other Pattern Matchers in the market.

5 Summary

The Accelerated AV solution platform jointly offered by Freescale Semiconductor, Inc. and Kaspersky Lab enables OEMs to deliver quickly to the market high-performance, cost-effective network-AV devices that are highly effective in the mitigation of malware outbreaks.

Effective malware outbreak mitigation is a result of:

- Kaspersky's team of antivirus experts who continuously monitor the world for new malware and quickly create accurate signatures (daily plus emergency updates) to detect them
- Freescale's advanced pattern matching technology that supports fast, live compile and incremental signature updates within seconds

High performance is achieved through the use of the MPC8572E, the engine of the network AV device. Its dual e500 cores provide CPU cycles and flexibility to perform various packet and application protocol processing. The MPC8572E's integrated hardware blocks—eTSEC, TLU, Deflate Engine and Pattern Matcher in particular—accelerate operations that are highly CPU-intensive with low power dissipation. Furthermore, the processor's highly optimized internal interconnect architecture ensures high bandwidth, low latency and efficient pipeline operation.

The MPC8572E PowerQUICC III processor—with all major processing and I/O elements included—enables very simple, elegant system design, with low system cost and a short design cycle. Contributing further to cost-effectiveness is the Pattern Matcher's use of DRAM instead of expensive low-latency SRAM or FCRAM.

As a result, OEMs can count on using the Accelerated AV solution platform to deliver highly competitive network AV products to the marketplace.

How to Reach Us:

Home Page:
www.freescale.com

e-Mail:
support@freescale.com

USA/Europe or Locations Not Listed:
Freescale Semiconductor
Technical Information Center, CH370
1300 N. Alma School Road
Chandler, Arizona 85224
1-800-521-6274
480-768-2130
support@freescale.com

Europe, Middle East and Africa:
Freescale Halbleiter Deutschland GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
support@freescale.com

Japan:
Freescale Semiconductor Japan Ltd.
Headquarters
ARCO Tower 15F
1-8-1, Shimo-Meguro, Meguro-ku,
Tokyo 153-0064, Japan
0120 191014
+81 3 5437 9125
support.japan@freescale.com

Asia/Pacific:
Freescale Semiconductor Hong Kong Ltd
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate,
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@freescale.com

For Literature Requests Only:
Freescale Semiconductor
Literature Distribution Center
P.O. Box 5405
Denver, Colorado 80217
1-800-441-2447
303-675-2140
Fax: 303-675-2150
LDCForFreescaleSemiconductor@hibbertgroup.com

Information in this document is provided solely to enable system and software implementers to use Freescale Semiconductor products. There are no express or implied copyright license granted hereunder to design or fabricate any integrated circuits or integrated circuits based on the information in this document.

Freescale Semiconductor reserves the right to make changes without further notice to any products herein. Freescale Semiconductor makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does Freescale Semiconductor assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters which may be provided in Freescale Semiconductor data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including “Typicals” must be validated for each customer application by customer’s technical experts. Freescale Semiconductor does not convey any license under its patent rights nor the rights of others. Freescale Semiconductor products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which the failure of the Freescale Semiconductor product could create a situation where personal injury or death may occur. Should Buyer purchase or use Freescale Semiconductor products for any such unintended or unauthorized application, Buyer shall indemnify and hold Freescale Semiconductor and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Freescale Semiconductor was negligent regarding the design or manufacture of the part.

Document Number: KASPERSKYWP
REV 1