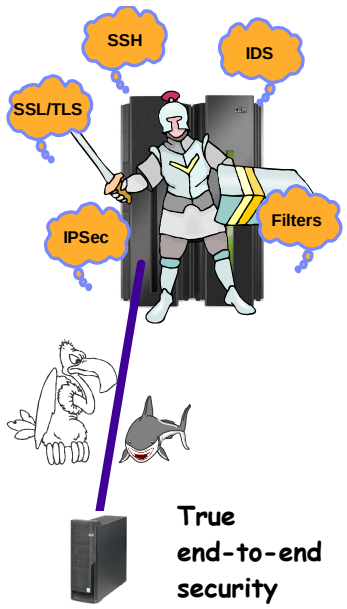
This presentation will give you an overview of the enhancements to the Communications Server in z/OS V1R11 for security.

Security

- IPSec enhancements
- AT-TLS enhancements



There are two main groups of enhancements to the z/OS Communications Server networking security functions in this release. The AT-TLS function is enhanced with support for many new SSL features. IPSec is enhanced within the network management area.

IKEv1 enhancements for IPSec

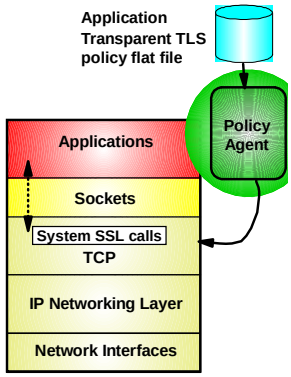
- **The Internet Key Exchange (IKE) daemon has been updated:**
  - Retransmission scheme has been updated to better conform to some of the points in RFC 2408.
    - Rather than using fixed intervals for IKE message retransmission, the daemon now uses a geometrically increasing retransmission interval.
- **In addition, several fine-grained attributes are now reported through:**
  - The ipsec command reports
  - The Network Management Interface (NMI)
  - The System Management Facility (SMF) records

The Internet Key Exchange (IKE) version one protocol handling is updated to better conform with the latest standards with respect to how retransmissions are done.

In addition, several detailed management data is being made available by way of the various network management interfaces that are supported by z/OS Communications Server: ipsec command, NMI, and SMF.

AT-TLS enhancements

- **AT-TLS to support System SSL functions that have been added since z/OS V1R7**:
  - TLS V1.1
  - Using RFC3280 to validate a certificate
  - Negotiation and use of a truncated HMAC
  - Negotiation and use of a maximum SSL fragment size
  - Negotiation and use of handshake server name indication
  - Setting the CRL LDAP server access security level



- **AT-TLS is also updated to address FIPS 140-2 requirements for applications that use AT-TLS to provide secure connections**.
- **AT-TLS performance enhancements for short-lived connections**

ATTLS was initially developed and implemented in z/OS V1R7. Since then, System SSL has added support for new features and protocol extensions. The ATTLS support is in this release enhanced to allow those features to be configured by way of the Configuration Assistant and for ATTLS to exploit these new features.

Among the more obvious ones is support for an updated TLS protocol – the TLS version 1.1 protocol level.

In combination with System SSL, ATTLS is also enhanced to aid in addressing FIPS 140-2 requirements – allowing such system SSL capabilities to be configured and used.

Trademarks, copyrights, and disclaimers

IBM, the IBM logo, ibm.com, and the following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

z/OS

If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of other IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

Other company, product, or service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.