NORTEL NETWORKS

AES and Beyond
The IETF and Strong Crypto

Marcus Leech

[IETF logo here]

IETF OVERVIEW

Chartered by IAB to deliver current technical standards for Internet protocols

Divided into AREAS, with AREA DIRECTORS for each area:

TRANSPORT - Scott Bradner-Harvard U, Vern Paxson-LBL

- TCP, UDP, RTP, etc

- ROUTING - Rob Coltun-CIENA, David Oran-Cisco
  - OSPF, BGP, IS-IS, etc
- INTERNET - Erik Nordmark-SUN, Thomas Narten-IBM
  - ARP, PAR, MPLS, IP-over-foo, etc
- O&M - Randy Bush-, Bert Wijnen-IBM
  - DNS, SNMP, etc
- APPLICATIONS - Ned Freed, Patrik Falstrom-SWIP.net
  - HTTP, and a zillion others
- GENERAL - Fred Baker-Cisco (also IETF chair)
- USER SERVICES - April Marine-Internet Engines - GRIP, SSH
- SECURITY - Jeff Schiller-MIT, Marcus Leech-Nortel
  - Working groups exist under a particular area
- IETF URL: www.ietf.org

[Nortel Networks logo here]

[IETF logo here]

SECURITY AREA OVERVIEW

Security Area Working Groups:

- IPSEC - Ted T’so - VALinux Systems
  - IP layer security: AH, ESP, IKE
- IPSP - Luis Sanchez-BBN, Hillary Orman-ARPA
  - IPSEC Policy (how to describe ACLs, crypto policy, etc)
- IPSRA - Sara Bitan-Radguard, Paul Hoffman-VPN Consortium
  - IPSEC Remote Access
- PKIX - Steve Kent BBN, Warwick Ford-Verisign
  - Public-key infrastructure (X.509, etc)
- S/MIME - Russ Housley-SPYRUS
- OPENPGP - John Noerenberg-Qualcomm
- AFT - Wei Lu (used to be Marcus Leech)-NEC

[Nortel Networks logo here]

[IETF logo here]

Security Area Overview (contd)

- CAT - John Linn-RSA Security
  - GSS-API (security API)
- SECSH - Bill Sommerfeld - Sun Microsystems
  - Secure Shell; standardization of SSH protocol
- IDWG - Michael Erlinger-Harvey Mudd College, Stuart Staniford-Chen UC Davis
  - Intrusion Detection exchange format
- STIME - Tim Polk-NIST, Patrick Cain-BBN
  - Secure version of NTP
- KINK - Derek Atkins, Telcordia
  - Kerberos-based key exchange for IPSEC

[Nortel Networks logo here]

[IETF logo here]

IETF and Crypto algorithms

- General approach has historically been to mandate the strongest algorithms that are standard, reasonable, and widely available.
- Not to preclude the use (among consenting adults) of other algorithms with different properties (stronger, or weaker than the mandated algorithms, for example).
- In most cases, this has meant DES as mandatory, and as DES became vulnerable, 3DES as mandatory, or a strong SHOULD.
- This position upset some whose local laws made it awkward to export products that were fully compliant with IETF protocol standards. Mandating AES isn’t likely to win the IETF any friends in the export-challenged countries.

[Nortel Networks logo here]

[IETF logo here]

IPSEC OVERVIEW

- **IPSEC**
  - Designed to provide strong confidentiality, integrity, and authentication at the IP (Network) layer.
- **Two architectural elements:**
  - *IKE* - does session key management
    - Key exchange with either RSA or D-H
    - Session protected with DES or 3DES
  - *AH* and *ESP* transforms - carries user data, protected under keys/algorithms negotiated during *IKE*
    - Integrity provided by either HMAC-MD5 or HMAC-SHA1
    - Confidentiality provided by either DES or 3DES
- **Moving to AES and SHA-2**
  - Shiela Frankel (NIST) has produced an Internet-Draft describing the use of AES within ESP. This document will be on the STANDARDS TRACK shortly.
  - IANA assignments for both AES and SHA-2 were issued on October 4.
  - Latest NETBSD snapshot includes support for AES, with correct IANA numbers.

TLS (RFC2246,2712)

- Provides Transport Layer Security--usually between application and TCP
- Originated external to IETF, as SSLV3. Most WEB browsers today speak SSLV3, and will soon speak TLS instead.
- Growth of the WEB has driven growth in deployment of SSLV3, and TLS.
- SSLV3 has almost completely obliterated SET (MasterCard/VISA secure transaction initiative).
- Other application protocols starting to be secured with SSLV3/TLS:
  - IMAP
  - POP3
  - TELNET
  - FTP
- Flexible with respect to “crypto suites”. Replacing current DES/3DES-based suites with AES-based suites is both trivial, and already underway.

[Nortel Networks logo here]

[IETF logo here]

SECSH

- Based on original SSH by Tatu Ylonen/SSH Communications
- Provides a secure terminal-emulator channel (TELNET-like), and secure “connection forwarding”.
- Also provides secure file copy.
- Many enterprises use SSH to securely management various network and security elements (firewalls, VPN gateways, Certification Authorities, web servers, etc).
- Must consider secure management of elements of VPN, if you manage it yourself.
- Extremely flexible with respect to selected crypto algorithms, blocksizes, etc. Adding AES should be trivial.

[Nortel Networks logo here]

[IETF logo here]

SNMPV3 (RFC2573,2574,2575,2570,2571,2572)

- First version of SNMP to provide reasonable security and access control for SNMP objects. Previous versions relied on keeping the COMMUNITY string "secret"-- which is pretty hard in large networks.
- Adding AES support should be trivial.

[Nortel Networks logo here]

[IETF logo here]

S/MIME

- Secure e-mail layered on top of MIME standards
- Adding AES support should be trivial
- Tim Polk (NIST) already working up necessary OIDs to assist in support of AES and SHA-2 both for S/MIME and PKIX

[Nortel Networks logo here]

[IETF logo here]

KERBEROS

- Application-layer security that predates TLS by quite a few years.
- New work in IETF to standardize a number of useful “hacks” to KERBEROS that the community has developed over the years.
- Timing is good to integrate AES into IETF Kerberos work.
- Flexible crypto structure makes integration of AES fairly straightforward.
- “Kerberized” applications automatically “inherit” AES support in underlying Kerberos.

[Nortel Networks logo here]

[IETF logo here]

VOIP (SIP, MGCP, RTP, …)

- Various VoIP initiatives are using various IETF protocols
- PACKETCABLE currently using MGCP, with RC4 for "bearer channel" encryption
- Move afoot to change from stream cipher to AES, since AES is at least as fast as stream cipher

[Nortel Networks logo here]

[IETF logo here]

OPEN ISSUES

- Not clear what appropriate key lengths are for key-exchange/key-agreement mechanisms, for AES key lengths >128 bits.
- AES is fast even at key length of 256 bits--providing a matching key agreement (RSA and D-H) will be SLOW!

[Nortel Networks logo here]

[IETF logo here]

Conclusions

- Most IETF protocols that use encryption are naturally "AES Ready"
- Most of the important protocols will be mandating AES over the next year, while the rest will phase it in over the next two or three years.
- DES will remain for backwards compatibility for some time--likely two to three years.

[Nortel Networks logo here]

[IETF logo here]