Protect Yourself Against Security Challenges with Next-Generation Encryption

agrieo@cisco.com
mcgrew@cisco.com
How to detect attacks?

- Malware
- Broken encryption
### How to detect attacks?

- **Malware**
  - Host Process Monitoring
  - Network Monitoring
  - Tripwire
  - Antivirus
  - Antimalware
  - Product Security Bulletins
  - Behavioral Analysis

- **Broken encryption**
Next Generation Encryption

- Upgrades all crypto mechanisms
- Designed to meet security and scalability requirements of next two decades
- Standards based
- Available today
Cryptographic Mechanisms

- Encryption
- Data Authentication
- Key Establishment
- Signatures
- Hashing
Using cryptographic mechanisms in IPsec

IKE_SA_INIT  
IKE_AUTH  
CREATE_CHILD_SA  
IKEv2
Using cryptographic mechanisms in IPsec

IKE_SA_INIT
IKE_AUTH
CREATE_CHILD_SA
ESP
ESP
IKEv2
ESP
Authenticated Encryption

Single algorithm provides both confidentiality and authentication in a single pass over data

• More efficient
• More secure
Authenticated Encryption - security issues solved


- **Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS ....**, Vaudenay, EUROCRYPT 2002.

Next Generation Encryption

- Authenticated Encryption: AES-GCM
- Authentication: HMAC-SHA-2
- Key Establishment: ECDH
- Digital Signatures: ECDSA
- Hashing: SHA-2
- Entropy: SP800-90
- Protocols: TLSv1.2, IKEv2, IPsec, MACSec
# Next Generation Encryption

## Suite B

<table>
<thead>
<tr>
<th>Function</th>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticated Encryption</td>
<td>AES-GCM</td>
</tr>
<tr>
<td>Authentication</td>
<td>HMAC-SHA-2</td>
</tr>
<tr>
<td>Key Establishment</td>
<td>ECDH</td>
</tr>
<tr>
<td>Digital Signatures</td>
<td>ECDSA</td>
</tr>
<tr>
<td>Hashing</td>
<td>SHA-2</td>
</tr>
<tr>
<td>Entropy</td>
<td>SP800-90</td>
</tr>
<tr>
<td>Protocols</td>
<td>TLSv1.2, IKEv2, IPsec, MACSec</td>
</tr>
</tbody>
</table>

© 2012 Cisco and/or its affiliates. All rights reserved.
<table>
<thead>
<tr>
<th>Protocol/Algorithm</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>3DES</td>
<td>1GB limit</td>
</tr>
<tr>
<td>HMAC-MD5</td>
<td>Theoretical attacks</td>
</tr>
<tr>
<td>DH, RSA</td>
<td>1024-bit at risk</td>
</tr>
<tr>
<td>RSA, DSA</td>
<td>1024-bit at risk</td>
</tr>
<tr>
<td>MD5, SHA-1</td>
<td>Collision attacks</td>
</tr>
<tr>
<td>Entropy</td>
<td>Inconsistent quality</td>
</tr>
<tr>
<td>TLS1.0, IKEv1</td>
<td>No AE, security issues</td>
</tr>
</tbody>
</table>
Key Strength

Sources: Lenstra and Verheul, NIST
Medium Organization ($300K)
Key Strength

The diagram illustrates the increase in key strength from 1990 to 2030, showing a steady rise from 64 to 128 bits. The NIST logo is prominently featured on the diagram.
Algorithms Never Get Stronger

Sources: FIPS-180-1, Wang, Yin, Yu ‘05, Cochran ‘07
Prevalent

- AES-128-CBC
- DH-1024
- RSA-1024
- SHA-1

© 2012 Cisco and/or its affiliates. All rights reserved.
Next Generation Encryption

128-bit Security Level

- AES-128-GCM
- ECDH-P256
- ECDSA-P256
- SHA-256
NGE higher security levels

- AES-256-GCM
- ECDH-P521
- ECDSA-P521
- SHA-512

- AES-192-GCM
- ECDH-P384
- ECDSA-P384
- SHA-384
ECC Efficiency

Signatures per second

- RSA
- ECC

<table>
<thead>
<tr>
<th>Bit Size</th>
<th>RSA</th>
<th>ECC</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>112</td>
<td>128</td>
</tr>
<tr>
<td>96</td>
<td>160</td>
<td>144</td>
</tr>
<tr>
<td>112</td>
<td>192</td>
<td>176</td>
</tr>
<tr>
<td>128</td>
<td>208</td>
<td>224</td>
</tr>
<tr>
<td>144</td>
<td>240</td>
<td>256</td>
</tr>
</tbody>
</table>
Implementations of NGE
NGE Enabled Encryption Architectures: Available Today

Remote Access VPNs

Site to Site, DMVPN, and FlexVPN

Remote Access VPNs

GETVPN*

MACSec

Supplicant with MACSec

Authenticated User

Data sent in clear

Encrypt

Decrypt

Guest User

MACSec Link
Cisco NGE Enabled Products

- ISRG2 800 Series
- 1900 Series
- 2900 Series
- ISRG2 3900 Series
- ASA 5505
- ASA 5512-X
- ASA 5515-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- ASA 5585 SSP-10
- ASA 5585 SSP-20
- ASA 5585 SSP-40
- ASA 5585 SSP-60
- AnyConnect
- ASA 5505
- ASA 5512-X
- ASA 5515-X
- ASA 5525-X
- ASA 5545-X
- ASA 5555-X
- ASA 5585 SSP-10
- ASA 5585 SSP-20
- ASA 5585 SSP-40
- ASA 5585 SSP-60
- Catalyst 3750-X
- Catalyst 3560-X
- Catalyst 4500x-E w/ Supervisor 7-E
- Catalyst 6500-E
- Nexus 7000
- VPN-ISM
NGE Enabled IPSec VPNs

NGE Capabilities

• Protocols:
  • IPSEC with IKEv2

• Cryptography:
  • AES-GCM (128 and 256 bit keys)
  • ECDSA (256 and 384)
  • ECDH (256 and 384)
  • SHA2 (256 and 384)

• Entropy:
  • Hardware based RNGs

Software Requirements

• For Cisco IOS devices:
  • Cisco IOS releases >15.1(4)M

• For Cisco Adaptive Security Appliance:
  • ASA 9.0 release

• For Cisco AnyConnect Secure Mobile Client:
  • AnyConnect 3.1
NGE Enabled Encryption: High Speed, High Density MACsec

- AES-GCM for per frame encryption and authentication

- Supported at High speeds:
  - Cisco Nexus 7000 Series Modules
    - 2 Port 100 Gigabit Ethernet
    - 6 Port 40 Gigabit Ethernet
    - 24-Port 10 Gigabit Ethernet
    - 48-Port Gigabit Ethernet
## Standards

<table>
<thead>
<tr>
<th>Icon</th>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Lock]</td>
<td>FIPS-197, SP800-38D, SP800-38, RFC5116</td>
</tr>
<tr>
<td>![Key]</td>
<td>RFC2104, RFC4868, FIPS-198</td>
</tr>
<tr>
<td>![Padlock]</td>
<td>RFC6090, SP800-56</td>
</tr>
<tr>
<td>![Microphone]</td>
<td>RFC6090, FIPS-186-3</td>
</tr>
<tr>
<td>![Diameter]</td>
<td>FIPS-180-2</td>
</tr>
<tr>
<td>![Die]</td>
<td>SP800-90</td>
</tr>
<tr>
<td>![Keypad]</td>
<td>IKEv2, IPsec, TLS1.2, IEEE 802.1 AE</td>
</tr>
</tbody>
</table>
NGE Benefits

- Upgrades the entire Crypto Suite
- Efficient at high security levels
  - Addresses escalating threats
- Scalable to high speeds
- USG recommended crypto algorithms
  - Subset of FIPS-140
  - Approved for sensitive information protection by global governments (US Government, UK Government)
- Included in many standards
  - IPsec, TLS, MACSec
Conclusions

Next Generation Encryption

• Highly Secure
• Scalable and Efficient
• Standards Based and Interoperable
• Available Today