



www.embeddedforecast.com

EMF's Guide to Embedded Security for Communications Systems

What vendors, OEMs and developers need to know about embedded security

Jerry Krasner, Ph.D., MBA

Table of Contents

EMF’s Guide to Embedded Security for Communications Systems.....	5
Introduction	5
Executive Summary	5
Encryption (or lack of)	6
Lack of Certified Encryption	7
The Federal Information Processing Standards (FIPS): Why embedded vendors, OEMs and developers need to incorporate FIPS 140-2.....	7
Improper Application of Encryption	9
Using Strong Encryption, Weakly.....	9
Key Size Disparities	9
Using “Pretend” Encryption.....	11
Unproven Protocol Implementations	11
SNMP.....	12
TCP/IP.....	12
OpenSSL-derivatives	12
Inevitable Conclusion	13
Protecting the Wrong Things	13
Lack of Management & Monitoring Abilities	14
Painful & Expensive Patch Management with Minimal Accountability	15
Embedded Limitations At Odds with Security Requirements & Existing Security Standards	16
Requirements of SSL	17
Requirements of SSH.....	18
Requirements of IP-Sec	19
When SSL, SSH, and IP-Sec Are Overkill.....	20

Lack of Vendor- or Industry-Originated Best Practices	20
Insecure by Default	21
Ambiguous Responsibilities	21
Summary	22
Appendix A – A Brief Introduction to FIPS 140	23
What Is FIPS 140?	23
Why is FIPS 140 Important?	23
I've never heard of FIPS 140, So How Important Can It Be?.....	24
How is FIPS 140 different from the Common Criteria certification?	25
How is FIPS 140 different from SSL or IP-sec?	25
If I have FIPS 140 certification, does that mean my system is secure? ...	25
How can I get FIPS 140 certification?.....	25
Appendix B – Integration of FIPS 140-certified Modules into Embedded Solutions	27
Embedded Systems Support.....	27
Insufficient Flexibility.....	27
Unacceptable Pricing, Licensing Terms	28
Out Of Date Certifications	29
Available Toolkits.....	29
Integrating FIPS 140 into New and Existing Embedded Systems.....	29
An SSL Implementation	30
An IP-Sec Implementation	30
A Proprietary Product with Existing Encryption Capabilities	30
A Proprietary Product without Existing Encryption Capabilities	31
RTOS CONSIDERATIONS.....	31

Appendix C – A Survey of Embedded Security Products.....	32
IP-Sec Implementations	32
TeamF1 V-IPSecure	32
Elmic Systems Voyager IPsec/IKE	33
InterPeak IKE.....	33
InterPeak IP-sec	33
SSL Implementations	34
TeamF1 SSLimSecureSecure	34
Interpeak Embedded SSL.....	34
Accelerated Technology Nucleus SSL.....	35
SSH Implementations	35
TeamF1 SSHield	35
Interpeak Embedded SSH	36
Proprietary Encrypted Communication Tools	36
TeamF1 SSMartSecure	36
Embedded Management Technologies	37
Interpeak Embedded SNMP	37
FIPS 140 Certified Encryption Toolkits	37
Certicom SecurityBuilder GSE.....	37
Cryptos Mobile Systems TACHYON-Crypt.....	38
Atmel AT97SC3201	38
Appendix D – “Why Does FIPS Matter?”	39

Copyright 2009 by American Technology International, Inc, 1257 Worcester Road #500, Framingham, MA 01701. All rights reserved. No part of this report covered by copyright hereon may be reproduced or copied in any manner whatsoever. Every effort has been made to provide accurate data. To the best of the editor’s knowledge, data is reliable and complete, but no warranty is made for this.