Glossary

1G - First Generation
2G - Second Generation
3DES - Triple DES
3G - Third Generation
8PSK - 8-Phase Shift Keying
A3 - Cryptographic Authentication Algorithm
A5 - Encryption Algorithm
A8 - Session Key Generation Algorithm
AES - Advanced Encryption Standard
AGCH - Access Grant Channel
AMPS - Advanced Mobile Phone System
ASN.1 - Abstract Syntax Notation Language
AuC - Authentication Center
BCCH - Broadcast Control Channel
BSS - Base Station Subsystem
BSSAP+ - Base Station System Application Part +
BTS - Base Transceiver Station
CCH - Common Control Channel
CCS - Common Channel Signaling
CDMA - Code-Division Multiple Access
COI - Communities of Interest
CSD - Circuit Switched Data
CSCF - Call Server Control Function
DCA - Direct Channel Allocation
DES - Data Encryption Standard
DoS - Denial of Service
DDoS - Distributed Denial of Service
DMZ - De-Militarized Zone
DTX - Discontinuous Transmission
EDGE - Enhanced Data Rates for GSM Evolution
EGPRS - Enhanced GPRS (a.k.a. EDGE)

EGSM - Extended GSM
EIR - Equipment Identity Register
ESME - External Short Messaging Entity
ESN - Electronic Serial Number
EV-DO - Enhanced Version - Data Optimized
EV-DV - Enhanced Version - Data and Voice
FDMA - Frequency-Division Multiple Access
GGSN - Gateway GPRS Support Node
GPRS - General Packet Radio Service
GSM - Global System for Mobile Communication
GTP - GPRS Tunneling Protocol
HSCSD - High Speed Circuit Switched Data
HLR - Home Location Register
HSN - Hopping Sequence Number
HSS - Home Subscriber Server
IAM - Initial Address Message
IETF - Internet Engineering Task Force
IKE - Internet Key Exchange
IMEI - International Mobile Equipment Identity
IMSI - International Mobile Subscriber Identity
IMS - IP Multimedia Subsystem
IN - Intelligent Network
ISDN - Integrated Services Digital Network
ISUP - ISDN User Part
ITU - International Telecommunications Union
K_c - Symmetric Session Key
K_i - Client Symmetric Key
LA - Location Area
MAP - Mobile Application Part
MAPsec - Mobile Application Part Security
MCEF - Mobile Capacity Exceeded Flag
MD5 - Message Digest algorithm 5
MMS - Multimedia Messaging Service
MMUSIC - Multiparty Multimedia Session Control
MO - Mobile Originated
MS - Mobile Station
MSISDN - Mobile Subscriber Integrated Services Digital Network Number
MSRN - Mobile Station Routing Number
MT - Mobile Terminated
MSC - Mobile Switching Center
MTP - Message Transfer Part
NANP - North American Numbering Plan
NCS - National Communications System
NDS - Network Domain Security
NIST - National Institute of Standards and Technology

NPA - Numbering Plan Area
NSA - National Security Agency
NSP - Network Services Part
NXX - Numbering Plan Exchange
P-TMSI - Packet Temporary Mobile Subscriber Identity
PACCH - Packet Associated Control Channel
PAGCH - Packet Access Grant Channel
PBCCH - Packet Broadcast Control Channel
PCH - Paging Channel
PCM - Pulse Code Modulation
PDCH - Packet Data Channel
PDP - Packet Data Protocol
PDTCH - Packet Data Traffic Channel
PKI - Public Key Infrastructure
PM - Protection Mode
PPCH - Packet Paging Channel
PRACH - Packet Random Access Channel
PSTN - Public Switched Telephone Network
QoS - Quality of Service
RA - Routing Area
RACH - Random Access Channel
RAI - Routing Area Identity
RED - Random Early Detection
RPE-LTE - Regular Pulse Excitation - Long Term Prediction
RTCP - RTP Control Protocol
RTP - Realtime Transport Protocol
SCCP - Signaling Connection Control Point
SCP - Signaling Control Point
SDCCH - Standalone Dedicated Control Channel
SGSN - Serving GPRS Support Node
SHA-1 - Secure Hash Algorithm 1
SID - Silence Descriptor
SIM - Subscriber Identity Module
SIP - Session Initiation Protocol
SIPS - Secure SIP
SMPP - Short Messaging Peer Protocol
SMS - Short Messaging Service
SMSC - Short Messaging Service Center
SRP - Static Resource Provisioning
SRTCP - Secure RTCP
SRTP - Secure RTP
SS7 - Signaling System Number 7
SSL - Secure Sockets Layer
TACS - Total Access Communication System
TBF - Temporary Block Flow

TCAP - Transaction Capabilities Application Part
TCH - Traffic Channel
TDMA - Time-Division Multiple Access
TFI - Temporary Flow Identifier
TMSI - Temporary Mobile Subscriber Identity
TRX - Transmission Channel
UMTS - Universal Mobile Telecommunication System
UHF - Ultra-High Frequency
URI - Uniform Resource Identifier
VAD - Voice Activity Detection
VLR - Visitor Location Register
VoIP - Voice over IP
WCDMA - Wide-band CDMA
WFQ - Weighted Fair Queuing
WRED - Weighted Random Early Detection
ZRTP - Media Path Key Agreement for Secure RTP

References

1. Computer Emergency Response Team. http://www.cert.org/.
2. National Institute of Standards and Technology. http://www.nist.gov/.
3. OpenSSL. http://www.openssl.org/.
4. Young prefer texting to calls'. http://news.bbc.co.uk/2/hi/business/2985072.stm, June 2003.
5. 3G Americas, LLC. 3G Americas::Unifying the Americas through Wireless Technology. http://www.3gamericas.org.
6. 3rd Generation Partnership Project. Comfort Noise Aspects for Full Rate Speech Traffic Channels. Technical Report 3GPP TS 06.12 v8.1.0.
7. 3rd Generation Partnership Project. Discontinuous Transmission (DTX) for Full Rate Speech Traffic Channels. Technical Report 3GPP TS 06.31 v8.0.1.
8. 3rd Generation Partnership Project. Full rate speech; Processing functions . Technical Report 3GPP TS 06.01 v8.0.1.
9. 3rd Generation Partnership Project. Full rate speech; Substitution and muting of lost frames for full rate speech channels. Technical Report 3GPP TS 06.11 v8.0.1.
10. 3rd Generation Partnership Project. Full rate speech; Transcoding. Technical Report 3GPP TS 06.10 v8.2.0.
11. 3rd Generation Partnership Project. General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control/Medium Access Control (RLC/MAC) protocol. Technical Report 3GPP TS 44.060 v7.6.0.
12. 3rd Generation Partnership Project. General Packet Radio Service (GPRS); Overall description of GPRS radio interface; Stage 2. Technical Report 3GPP TS 03.64 v8.12.0.
13. 3rd Generation Partnership Project. General Packet Radio Service (GPRS); Service description;. Technical Report 3GPP TS 03.60 v7.9.0.
14. 3rd Generation Partnership Project. GSM/EDGE Radio Access Network; General PAcket Radio Service (GPRS); Overall description of the GPRS radio interface; Stage 2. Technical Report 3GPP TS 43.064 v7.2.0.
15. 3rd Generation Partnership Project. Organization of subscriber data. Technical Report 3GPP TS 03.08 v7.5.0.
16. 3rd Generation Partnership Project. Physical layer on the radio path; General description. Technical Report 3GPP TS 05.01 v8.9.0.

17. 3rd Generation Partnership Project. Physical layer on the radio path; General description. Technical Report 3GPP TS 04.18 v8.26.0.
18. 3rd Generation Partnership Project. Radio Access Network; Radio transmission and reception. Technical Report 3GPP TS 05.05 v8.20.0.
19. 3rd Generation Partnership Project. Technical realization of the Short Message Service (SMS). Technical Report 3GPP TS 03.40 v7.5.0.
20. 3rd Generation Partnership Project. Technical Specification Group Core Network and Terminals; Mobile Application Part (MAP) specification. Technical Report 3GPP TS 29.002 v8.1.0.
21. 3rd Generation Partnership Project. Technical Specification Group GSM/EDGE, Radio Access Network; Channel coding. Technical Report 3GPP TS 45.003 v7.1.0.
22. 3rd Generation Partnership Project. Technical Specification Group GSM/EDGE Radio Access Network; Multiplexing and multiple access on the radio path. Technical Report 3GPP TS 05.02 v8.11.0.
23. 3rd Generation Partnership Project. Technical Specification Group Radio Access Network; Medium Access Control (MAC) protocol specification (Release 7). Technical Report 3GPP TS 25.321 v7.2.0.
24. 3rd Generation Partnership Project. Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; MAP application layer security . Technical Report 3GPP TS 33.200 v7.0.0.
25. 3rd Generation Partnership Project. Technical Specification Group Terminals; Alphabets and language-specific information. Technical Report 3GPP TS 23.038 v7.0.0.
26. 3rd Generation Partnership Project. Voice Activity Detection (VAD). Technical Report 3GPP TS 06.32 v8.0.1.
27. A. Abutaleb and V. O. Li. Paging strategy optimization in personal communication systems. *Wireless Networks*, 3(3):195–204, 1997.
28. American District Telegraph (ADT). Frequently Asked Questions (FAQ's). `http://www.adt.com/wps/portal/adt/customer_service/?wgc=for_your_home/cellular_radio_monitoring_faqs`, 2007.
29. P. Amrein. BMD Wireless Announces Commercial Availability of Application SMSC and High Speed Messaging Platform. `http://www.intradoemea.com/main.php?content=newsflash_08200201`, 2002.
30. R. Anderson. Usenet Group uk.telecom: A5 (Was: HACKING DIGITAL PHONES). `http://groups.google.com/group/uk.telecom/msg/ba76615fef32ba32`, 1994.
31. F. Andreasen, M. Baugher, and D. Wing. RFC 4568: Session Description Protocol (SDP) Security Descriptions for Media Streams. `http://tools.ietf.org/html/rfc4568`, 2006.
32. Antenna Systems & Solutions, Inc. Tactical Response Cell Phone Jammer (TRJ) - Antenna Systems & Solutions. `www.antennasystems.com/cellular/trj-89_cellphonejammer.htm`, 2008.
33. J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman. RFC 3830: MIKEY: Multimedia Internet KEYing. `http://tools.ietf.org/html/rfc3830`, 2004.
34. A. Arpaci-Dusseau and R. Arpaci-Dusseau. Information and Control in Gray-Box Systems. In *Proceedings of Symposium on Operating Systems Principles (SOSP)*, 2001.

35. AT&T Wireless. Picture & Video Messaging and Frequently asked questions. http://www.wireless.att.com/learn/messaging-internet/messaging/faq-multimedia-messaging.jsp, 2007.
36. Audacity Development Team. Oreka: Audio streams recording and retrieval. http://oreka.sourceforge.net/, 2007.
37. S. Axelsson. The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection. *Proceedings of the 6th ACM Conference on Computer and Communications Security*, 1999.
38. E. Barkhan, E. Biham, and N. Keller. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. In *Proceedings of the Annual International Cryptology Conference (CRYPTO)*, 2003.
39. M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman. RFC 3711: The Secure Real-time Transport Protocol (SRTP). http://tools.ietf.org/html/rfc3711, 2004.
40. S. Bellovin. Security problems in the TCP/IP protocol suite. *Computer Communications Review*, 19(2):32–48, April 1989.
41. E. Biham and O. Dunkelman. Cryptanalysis of the A5/1 GSM Stream Cipher. In *Proceedings of INDOCRYPT*, 2000.
42. E. Biham, O. Dunkelman, and N. Keller. A Related-Key Rectangle Attack on the Full KASUMI. In *Proceedings of ASIACRYPT*, 2005.
43. A. Biryukov, A. Shamir, and D. Wagner. Real Time Cryptanalysis of A5/1 on a PC. In *Proceedings of the Fast Software Encryption Workshop*, 2000.
44. B. Branden, D. Clark, J. Crowcroft, B. Davie, S. Deering, D. Estrin, S. Floyd, V. Jacobson, G. Minshall, C. Partridge, L. Peterson, K. Ramakrishnan, S. Shenker, J. Wroclawski, and L. Zhang. RFC 2309: Recommendations on Queue Management and congestion Avoidance in the Internet. http://tools.ietf.org/html/rfc2309, 1998.
45. S. Buckingham. What is GPRS? http://www.gsmworld.com/technology/gprs/intro.shtml#5, 2000.
46. N. Burnett, J. Bent, A. Arpaci-Dusseau, and R. Arpaci-Dusseau. Exploiting Gray-Box Knowledge of Buffer-Cache Management. In *Proceedings of USENIX Annual Technical Conference*, 2002.
47. R. Buskey, H. Chen, T. La Porta, J. Larson, S. Mizikovsky, and P. Traynor. Cellular Networks Security Panel. USENIX Security Symposium, 2007.
48. S. Byers, A. Rubin, and D. Kormann. Defending Against an Internet-based Attack on the Physical World. *ACM Transactions on Internet Technology (TOIT)*, 4(3):239–254, August 2004.
49. H. Choi, H. Song, G. Cao, and T. La Porta. Mobile Multi-Layered IPsec. In *Proceedings of IEEE INFOCOM*, 2005.
50. A. Choong. Wireless Watch: Jammed. http://asia.cnet.com/reviews/handphones/wirelesswatch/0,39020107,39186280,00.htm, September 7, 2004.
51. Cisco Systems Whitepaper. A study in mobile messaging: The evolution of messaging in mobile networks, and how to efficiently and effectively manage the growing messaging traffic. Technical report, 2004.
52. D. Clark, J. Wroslawski, K. Sollins, and R. Braden. Tussle in Cyberspace: Defining Tomorrow's Internet. In *Proceedings of ACM SIGCOMM*, 2002.
53. G. Combs. Wireshark. http://www.wireshark.org/, 2007.
54. Computer Security: Art and Science. *Matt Bishop*. Addison-Wesley, Reading, MA, 2003.

55. C. Cortes, D. Pregibon, and C. Volinsky. Communities of Interest. In *Proceedings of the International Conference on Advances in Intelligent Data Analysis (IDA)*, 2001.
56. Cryptome. Interception of GSM Cellphones. `http://cryptome.org/gsm-spy.htm`, 2005.
57. A. Demers, S. Keshav, and S. Shenker. Analysis and Simulation of a Fair Queueing Algorithm. In *Proceedings of ACM SIGCOMM*, pages 3–12, 1989.
58. D. Eastlake and P. Jones. US Secure Hash Algorithm 1 (SHA1). Internet Engineering Task Force RFC 3174, Sept. 2001.
59. C. M. Ellison and B. Schneier. Ten Risks of PKI: What You're Not Being Told About Public-Key Infrastructure. *Computer Security Journal*, 16(1):1–7, 1999.
60. J. Elwell. RFC 4916: Connected Identity in the Session Initiation Protocol (SIP). `http://tools.ietf.org/html/rfc4916`, 2007.
61. W. Enck, P. Traynor, P. McDaniel, and T. F. La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the ACM Conference on Computer and Communication Security (CCS)*, November 2005.
62. F-Secure Corporation. F-Secure Virus Descriptions : Cabir.H. `http://www.f-secure.com/v-descs/cabir\_h.shtml`, December 2004.
63. F-Secure Corporation. F-Secure Virus Descriptions : Duts.1520. `http://www.f-secure.com/v-descs/dtus.shtml`, 2004.
64. F-Secure Corporation. F-Secure Virus Descriptions : Commwarrior. `http://www.f-secure.com/v-descs/commwarrior.shtml`, 2005.
65. F-Secure Corporation. F-Secure Virus Descriptions : Mabir.A. `http://www.f-secure.com/v-descs/mabir.shtml`, April 2005.
66. F-Secure Corporation. F-Secure Virus Descriptions : Skulls.A. `http://www.f-secure.com/v-descs/skulls.shtml`, January 2005.
67. D. Farber, L. Dignan, and D. Berlind. Why the FCC's 700Mhz auction matters. `http://blogs.zdnet.com/BTL/?p=5807`, 2007.
68. Federal Communications Commission. Year 2000 Biennial Review Amendment of Part 22 of the Commissions Rules to Modify or Eliminate Outdated Rules Affecting the Cellular Radiotelephone Service and Other Commercial Mobile Radio Service, 2000.
69. Federal Communications Commission. FCC: Wireless Services: Broadband PCS: Operations: Blocking & Jamming. `http://wireless.fcc.gov/services/index.htm?job=operations_1&id=broadband_pcs`, 2002.
70. Federal Communications Commission. Auction 73: 700 MHz Band. `http://wireless.fcc.gov/auctions/default.htm?job=auction_summary&id=73`, 2008.
71. S. Floyd and V. Jacobson. Random Early Detection Gateways for Congestion Avoidance. *IEEE/ACM Transactions on Networking*, 1(4):397–413, August 1993.
72. Gateway to Russia. Mobile networks facing overload. `http://www.gateway2russia.com/st/art_187902.php`, December 31, 2003.
73. General Electric. GE Security. `http://www.gesecurity.com/portal/site/GESecurity`, 2007.
74. General Motors. OnStar Car Safety Device and Vehicle Security System. `http://www.onstar.com`, 2007.
75. I. Goldberg, D. Wagner, and M. Briceno. GSM Cloning. `http://www.isaac.cs.berkeley.edu/isaac/gsm.html`, 1998.

76. D. M. Goldschlag, M. G. Reed, and P. F. Syverson. "Onion Routing for Anonymous and Private Internet Connections. *Communications of the ACM*, 42(2), February 1999.
77. J. D. Golic. Cryptanalysis of Alleged A5 Stream Cipher. In *Proceedings of EuroCrypt*, 1997.
78. M. Grenville. Operators: Celebration Messages Overload SMS Network. `http://www.160characters.org/news.php?action=view&nid=819`, November 2003.
79. GSM World. Brief History of GSM & the GSMA. `http://www.gsmworld.com/about/history.shtml`, 2007.
80. GSM World. GSM Operators, Coverage Maps and Roaming Information - Countries/Areas. `http://www.gsmworld.com/roaming/gsminfo/index.shtml`, 2007.
81. GSM World. GSM Security Algorithms. `http://www.gsmworld.com/using/algorithms/index.shtml`, 2008.
82. C. Guo, H. J. Wang, and W. Zhu. Smart Phone Attacks and Defenses. In *Proceedings of Third ACM Workshop on Hot Topics in Networks (HotNets-III)*, 2004.
83. D. Hanluain. They Be Jammin' in France. `http://www.wired.com/culture/lifestyle/news/2002/03/51273`, 2002.
84. D. Harkins and D. Carrel. The Internet Key Exchange. *Internet Engineering Task Force*, November 1998. RFC 2409.
85. Hewlett-Packard. HP to Drive Mobile Connectivity Around the Globe with Vodafone. `http://www.hp.com/hpinfo/newsroom/press/2006/060706b.html`, 2006.
86. M. Hines. Attackers Get Chatty on VOIP. `http://www.pcworld.com/businesscenter/article/132389/attackers_get_chatty_on_voip.html`, May 2007.
87. Intel Whitepaper. SMS Messaging in SS7 Networks: Optimizing Revenue with Modular Components. Technical report, 2003.
88. International Electrotechnical Commission. Audio recording - Compact disc digital audio system. Technical Report IEC 60908.
89. International Telecommunications Union. H.261 : Video codec for audiovisual services at p x 64 kbit/s. Technical Report ITU-T Recommendation H.261.
90. International Telecommunications Union. ITU: Committed to connecting the world. `http://www.itu.int/`.
91. International Telecommunications Union. Narrow-band visual telephone systems and terminal equipment. Technical Report ITU-T Recommendation H.320.
92. International Telecommunications Union. Packet-based multimedia communications systems. Technical Report ITU-T Recommendation H.323.
93. International Telecommunications Union. Pulse code modulation (PCM) of voice frequencies. Technical Report ITU-T Recommendation G.711.
94. International Telecommunications Union. Transmission performance characteristics of pulse code modulation channels. Technical Report ITU-T Recommendation G.712.
95. Internet Engineering Task Force. Session Initiation Protocol (sip). Technical report.
96. J. Ioannidis and S. Bellovin. Implementing Pushback: Router-Based Defense Against DDoS Attacks. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*, February 2002.

97. ITFacts. Mobile Usage: 2.7% of Americans downloaded a mobile game. http://www.itfacts.biz/index.php?id=P6428, 2006.
98. iTnews. Record calls, text again expected for NYE. http://www.itnews.com.au/newsstory.aspx?CIaNID=17434, December 31, 2004.
99. R. Jain. Myths about congestion management in high speed networks. *Internetworking: Research and Experience*, 3:101–113, 1992.
100. L. Johansen, K. Butler, M. Rowell, and P. McDaniel. Email Communities of Interest. In *Proceedings of the Conference on Email and Anti-Spam (CEAS)*, 2007.
101. D. Johnson, C. Perkins, and J. Arkko. RFC 3775: Mobility Support in IPv6. http://tools.ietf.org/html/rfc3775, 2004.
102. A. Juels and J. G. Brainard. Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks. In *Proceedings of Network and Distributed System Security Symposium (NDSS)*, 1999.
103. D. Kahn. *The Codebreakers*. Macmillan Publishing Co., 1967.
104. C. Kaufman, R. Perlman, and M. Speciner. *Network security: private communication in a public world*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2nd edition, 2002.
105. S. Kent and R. Atkinson. IP Authentication Header. RFC 2402, Nov. 1998.
106. S. Kent and R. Atkinson. IP Encapsulating Security Payload. RFC 2406, Nov. 1998.
107. S. Kent and R. Atkinson. RFC 2401: Security Architecture for the Internet Protocol. http://tools.ietf.org/html/rfc2401, 1998.
108. A. Keromytis, V. Misra, and D. Rubenstein. SOS: Secure Overlay Services. In *Proceedings of ACM SIGCOMM*, 2002.
109. G. Kim, S. H. Lee, S. C. Lee, H. G. Lee, and O. Kwon. MONETA Services of SK Telecom: Lessons from Business Convergence Experiences for Ubiqu itous Computing Services. In *Proceedings of the 2nd IEEE Workshop on Software Technologies for Future Embedded and U biquitous Systems (WSTFEUS'04)*, 2004.
110. K. Kotapati, P. Liu, and T. La Porta. CAT - A Practical Graph & SDL Based Toolkit for Vulnerability Assessment of 3G Networks. In *Proceedings of the IFIP International Information Security Conference, Security and Privacy in Dynamic Environments*, 2006.
111. B. Krebs. Research May Hasten Death of Mobile Privacy Standard. http://blog.washingtonpost.com/securityfix/2008/02/research_may_spell_end_of_mobi.html, 2008.
112. B. Krishnamachari, R.-H. Gau, S. B. Wicker, and Z. J. Haas. Optimal sequential paging in cellular wireless networks. *Wireless Networks*, 10(2):121–131, 2004.
113. D. R. Kuhn, T. J. Walsh, and S. Fries. Security Considerations for Voice Over IP Systems. Technical Report Special Report 800-58, National Institute of Standards and Technology (NIST), 2005.
114. G. Kunene. Perimeter Security Ain't What It Used to Be, Experts Say. *DevX.com*, 2004.
115. J. LeClaire. Malware Writers Exploit Skype Hype. http://www.technewsworld.com/story/voip/46802.html, October 18, 2005.
116. C. Lepschy, G. Minerva, D. Minervini, and F. Pascali. GSM-GPRS radio access dimensioning. In *IEEE Technology Conference (VTC Fall)*, 2001.

117. G. Lorenz, T. Moore, G. Manes, J. Hale, and S. Shenoi. Securing SS7 Telecommunications Networks. In *Proceedings of the IEEE Workshop on Information Assurance and Security*, 2001.
118. Lucent Technologies. 5ESS(R) 2000 - Switch Mobile Switching Centre (MSC) for Service Providers. `http://www.lucent.com/products/solution/0,,CTID+2019-STID+10048-SOID+824-LOCL+1,00.html`, 2006.
119. K. Maney. Surge in text messaging makes cell operators :-). `http://www.usatoday.com/money/2005-07-27-text-messaging_x.htm`, July 27 2005.
120. S. Marwaha. Will Success Spoil SMS? `http://wirelessreview.com/mag/wireless_success_spoil_sms/`, March 15, 2001.
121. P. McDaniel, S. Sen, O. Spatscheck, J. V. der Merwe, B. Aiello, and C. Kalmanek. Enterprise Security: A Community of Interest Based Approach. In *Proceedings of the Network & Distributed System Security Symposium (NDSS)*, 2006.
122. J. Mirkovic and P. Reiher. A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2):39–53, 2004.
123. G. S. Mobile. Services and Facilities to be provided in the GSM System. Technical Report GSM Doc 28/85, Revision 2, June 1985.
124. T. Moore, T. Kosloff, J. Keller, G. Manes, and S. Shenoi. Signaling System 7 Network Security. In *Proceedings of the IEEE 45th Midwest Symposium on Circuits and Systems*, 2002.
125. Motorola Corporation. Motorola GSM Solutions. `www.motorola.com/networkoperators/pdfs/GSM-Solutions.pdf`, 2006.
126. C. Mulliner and G. Vigna. Vulnerability Analysis of MMS User Agents. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, 2006.
127. R. Mullner, C. F. Ball, K. Ivanov, and H. Winkler. Advanced quality of service strategies for GERAN mobile radio networks. In *IEEE Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2004.
128. J. Nagle. RFC 896: Congestion Control in IP/TCP Internetworks. `http://www.ietf.org/rfc/rfc896.txt`, 1984.
129. J. B. Nagle. On Packet Switches with Infinite Storage. *IEEE Transactions on Communications*, COM-35(4), April 1987.
130. National Bureau of Standards. Data Encryption Standard. *Federal Information Processing Standards Publication*, 1976.
131. National Communications System. SMS over SS7. Technical Report Technical Information Bulletin 03-2 (NCS TIB 03-2), December 2003.
132. National Security Agency. Recommended IP Telephony Architecture. Technical Report I332-009R-2006, Systems and Network Attack Center (SNAC), 2006.
133. P. Neumann. Cause of AT&T network failure. *The Risks Digest*, 9(62), 1990.
134. NIST. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher. Special Publication 800-67, 2004.
135. Nyquetek, Inc. Wireless Priority Service for National Security. `http://wireless.fcc.gov/releases/da051650PublicUse.pdf`, 2002.
136. J. Pearce. Mobile firms gear up for New Years text-fest. `http://news.zdnet.co.uk/communications/networks/0,39020345,39118812,00.htm`, December 30, 2003.

137. J. Peterson. RFC 3853: S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP). http://tools.ietf.org/html/rfc3853, 2004.
138. S. Petrovic and A. Fuster-Sabater. An Improved Cryptanalysis of the A5/2 Algorithm for Mobile Communications. In *Proceedings of Communication Systems and Networks*, 2002.
139. Phone Jammer: Cell Phone Jammer Specialists. Cell Phone Jammer, Low Power Mobile Phone Jammers, Blocker Stopper - Buy Here - Cool ! http://phonejammer.com/, 2008.
140. G. Platform. Implementations: Mobile Telecom. http://www.globalplatform.org/, March 2008.
141. V. Prevelakis and D. Spinellis. The Athens Affair. *IEEE Spectrum*, pages 18–25, July 2007.
142. R. Racic, D. Ma, and H. Chen. Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery. In *Proceedings of the IEEE International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2006.
143. A. Ramirez. Theft Through Cellular 'Clone' Calls. *The New York Times*, April 7, 1992.
144. J. Rao, P. Rohatgi, H. Scherzer, and S. Tinguely. Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards. In *Proceedings of the IEEE Symposium on Security and Privacy (OAKLAND)*, 2002.
145. M. Reardon. ThinkPads to support Cingular 3G technology. http://news.com.com/ThinkPads+to+support+Cingular+3G+technology/2100-1034_3-6017968.html, 2006.
146. M. Reardon. Sprint unveils WiMax plans. http://www.news.com/Sprint-unveils-WiMax-plans/2100-1039_3-6170672.html, 2007.
147. D. Reed, J. Saltzer, and D. Clark. Active Networking and End-To-End Arguments. *IEEE Network*, 12(3):67–71, May/June 1998.
148. Research In Motion. Blackberry. http://www.blackberry.com/, 2006.
149. F. Ricciato. Unwanted Traffic in 3G Networks. In *ACM SIGCOMM Computer Communication Review*, 2006.
150. M. Richtel. Yahoo Attributes a Lengthy Service Failure to an Attack. *The New York Times*, February 8 2000.
151. M. Richtel. Devices Enforce Silence of Cellphones, Illegally. *The New York Times*, November 4, 2007.
152. R. Rivest. The MD5 Message Digest Algorithm. *Internet Engineering Task Force*, April 1992. RFC 1321.
153. R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.
154. A. B. Roach. RFC 3265: Session Initiation Protocol (SIP)-Specific Event Notification. http://tools.ietf.org/html/rfc3265, 2002.
155. Roam Secure. 17 Counties & Cities in Washington, DC Region deploy Roam Secure Alert Network. http://www.roamsecure.net/story.php?news_id=52, September 2005.
156. R. Rosenbaum. Secrets of the Little Blue Box. *Esquire Magazine*, pages 117–125 and 222–226, October 1971.

157. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. RFC 3261: SIP: Session Initiation Protocol. http://tools.ietf.org/html/rfc3261, 2002.
158. J. H. Saltzer, D. P. Reed, and D. D. Clark. End-To-End Arguments In System Design. *ACM Transactions on Computer Systems*, 2(4):277–288, 1984.
159. SANS Institute. The GSM Standard (An Overview of Its Security). http://www.sans.org/rr/papers/index.php?id=317, 2001.
160. S. Savage, D. Wetherall, A. Karlin, and T. Anderson. Practical network support for IP traceback. In *Proceedings of ACM SIGCOMM*, pages 295–306, October 2000.
161. F. B. Schneider, editor. *Trust in Cyberspace*. National Academy Press, 1999.
162. M. Schwartz. Addison-Wesley Publishing Company, 1987.
163. J. Serror, H. Zang, and J. C. Bolot. Impact of paging channel overloads or attacks on a cellular network. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, 2006.
164. G. Shannon. Security Vulnerabilities in Protocols. In *Proceedings of ITU-T Workshop on Security*, May 13-14 2002.
165. M. Sherr, E. Cronin, S. Clark, and M. Blaze. Signaling Vulnerabilities in Wiretapping Systems. *IEEE Security & Privacy*, 3(6):13–25, November/December 2005.
166. Skype Limited. Skype - Internet Calls. http://www.skype.com/, 2007.
167. R. Sparks. RFC 4320: Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction. http://tools.ietf.org/html/rfc4320, 2006.
168. S. Staniford, V. Paxson, and N. Weaver. How to 0wn the Internet in Your Spare Time. In *Usenix Security Symposium*, pages 149–167, 2002.
169. Start Corp. http://www.startcorp.com, 2005.
170. Tamara Neale. VDOT LAUNCHES NEW 511 EMAIL ALERT SERVICE. http://www.virginiadot.org/infoservice/news/newsrelease.asp?ID=CO-511-06, February 2006.
171. S. Telecom. Moneta Stock. http://www.sktelecom.com/, March 2008.
172. Telecommunication Industry Association/Electronic Industries Association (TIA/EIA) Standard. Short Messaging Service for Spread Spectrum Systems. Technical Report ANSI/TIA/EIA-637-A-1999.
173. The 104th Congress of the United States. The Telecommunications Act of 1996. http://www.fcc.gov/Reports/tcom1996.txt, 1996. Pub. LA. No. 104-104.
174. The Internet Engineering Task Force. IETF Home Page. http://www.ietf.org/.
175. The Internet Engineering Task Force. RFC 2460: Internet Protocol, Version 6 (IPv6) Specification. http://www.ietf.org/rfc/rfc2460.txt, 1998.
176. The Signal Jammer. TheSignalJammer.com: Cellular and GPS Jamming Products. http://www.thesignaljammer.com/, 2008.
177. The Tor Project. Tor: anonymity online. http://tor.eff.org/, 2007.
178. Third Generation Partnership Plan 2 (3GPP2). Developing the Next Generation of cdma2000 Wireless Communications. http://www.3gpp2.org.
179. Third Generation Partnership Plan (3GPP). Shaping the future of mobile communication standards. http://www.3gpp.org.
180. Tom's Hardware. How To: Building a BlueSniper Rifle. http://www.tomsnetworking.com/Sections-article106.php, March 2005.

181. P. Traynor. *Characterizing the Impact of Rigidity on the Security of Cellular Telecommunications Networks*. PhD thesis, The Pennsylvania State University, 2008.
182. P. Traynor, W. Enck, P. McDaniel, and T. La Porta. Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the Twelfth Annual ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2006.
183. P. Traynor, W. Enck, P. McDaniel, and T. La Porta. Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks. *IEEE/ACM Transactions on Networking (TON)*, To Appear.
184. P. Traynor, W. Enck, P. McDaniel, and T. La Porta. Exlopiting Open Functionality in SMS-Capable Cellular Networks. *Journal of Computer Security (JCS)*, To Appear 2008.
185. P. Traynor, P. McDaniel, and T. La Porta. On Attack Causality in Internet-Connected Cellular Networks. In *Proceedings of the USENIX Security Symposium*, 2007.
186. P. Traynor, V. Rao, T. Jaeger, P. McDaniel, and T. La Porta. From Mobile Phones to Responsible Devices. Technical Report NAS-TR-0059-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, 2007.
187. Trifinite. BlueBug. `http://trifinite.org/trifinite_stuff_bluebug.html`, 2004.
188. United States Census Bureau. United States Census 2000. `http://www.census.gov/main/www/cen2000.html`, 2000.
189. Verizon Wireless. Verizon Wireless Picture & Video Messaging. `http://www.vzwpix.com/pri/composer/guestCreate.do?sortField=-creationDate&category=Stuff+to+Send%2CE-Cards`, 2007.
190. Vonage Marketing, Inc. Vonage - A Better Phone Service For Less. `http://www.vonage.com/`, 2007.
191. X. Wang, S. Chen, and S. Jajodia. Tracking Anonymous Peer-to-Peer VoIP Calls on the Internet. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2005.
192. X. Wang, S. Chen, and S. Jajodia. Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems. In *Proceedings of the IEEE Symposium on Security and Privacy (OAKLAND)*, 2007.
193. B. Waters, A. Juels, J. Halderman, and E. Felten. New client puzzle outsourcing techniques for DoS resistance. In *Proceedings of ACM Conference on Computer and Communications Security (CCS)*, pages 246–256, 2004.
194. J. Wexler. WiMax service hits Seattle. `http://www.techworld.com/mobility/features/index.cfm?featureid=1434`, 2005.
195. WiMAX Forum. Welcome to the WiMAX Forum. `http://www.wimaxforum.org/home/`, 2007.
196. C. Wright, L. Ballard, S. Coull, F. Monrose, and G. Masson. Spot me if you can: Uncovering spoken phrases in encrypted VoIP conversations. In *Proceedings of IEEE Symposium on Security and Privacy (OAKLAND)*, 2008.
197. C. Wright, L. Ballard, F. Monrose, and G. Masson. Language Identification of Encrypted VoIP Traffic: Alejandra y Roberto or Alice and Bob? In *Proceedings of the USENIX Security Symposium*, 2007.

198. M. Wright, M. Adler, B. N. Levine, and C. Shields. Passive Logging Attacks Against Anonymous Communications. *ACM Transactions on Information and Systems Security (TISSEC)*, To appear, 2008.
199. W. Yu, X. Fu, S. Graham, D. Xuan, and W. Zhao. DSSS-based Flow Marking Technique for Invisible Traceback. In *Proceedings of IEEE Symposium on Security and Privacy (OAKLAND)*, 2007.
200. R. Zhang, X. Wang, X. Yang, and X. Jiang. Billing Attacks on SIP-Based VoIP Systems. In *Proceedings of the USENIX Workshop on Offensive Technologies (WOOT)*, 2007.
201. Y. Zhang and B. Singh. A Multi-Layer IPsec Protocol. In *Proceedings of the USENIX Security Symposium*, 2000.
202. P. Zimmermann, A. Johnston, and J. Callas. ZRTP: Media Path Key Agreement for Secure RTP. `http://zfoneproject.com/docs/ietf/draft-zimmermann-avt-zrtp-04.html`, 2007.

Index