



Computer Science Department

Computer Security and Forensics Group



Security Assessment in WLAN 802.11, Bluetooth, & GPRS

Patel, M. & S. H. Courellis
CS Dept., California State Univ., Fullerton

Description: Evaluation of the level of security and the algorithms employed in the three most prolific wireless communications technologies: WLAN IEEE 802.11, Bluetooth (IEEE 802.15), and GPRS.

WLAN 802.11

	WEP	WPA	WPA2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24 bit IV	48 bit IV	48 bit IV
Packet Key	Concatenated	Mixing Function	Not needed
Data Integrity	CRC-32	Michael Algorithm	CCMP
Message Integrity	None	Michael Algorithm	CCMP
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP Based	EAP Based

Bluetooth

Unit A: $LK_{K_s} = E_{K_s}(RAND, BD_ADDR_s, C_s + LK_RAND, (DOR) K)$

Unit B: $LK_{K_s} = E_{K_s}(LK_RAND, BD_ADDR_s, C_s + LK_RAND, (DOR) K)$

Unit A: $LK_{K_s} = C_s (DOR) K$
 $LK_{K_s} = E_{K_s}(LK_RAND, BD_ADDR_s, C_s + LK_RAND, (DOR) K)$
 $P_{s+1} = LK_{K_s} (DOR) LK_{K_s} + P_s$

Unit B: $LK_{K_s} = C_s (DOR) K$
 $LK_{K_s} = E_{K_s}(LK_RAND, BD_ADDR_s, C_s + LK_RAND, (DOR) K)$
 $P_{s+1} = LK_{K_s} (DOR) LK_{K_s} + P_s$

Authentication

Verifier (Unit A): $AU_RAND_s, BD_ADDR_s, Link Key$ → E_s → $SRES$ → ACC → $SRES$ (Verify)

Claimant (Unit B): $AU_RAND_s, BD_ADDR_s, Link Key$ → E_s → $SRES$ → ACC

GPRS

Mobile: MS → Auth Req (1) → Rand (4) → SGIN → HLR/AUC → Rand → SRES (5) → Encrypted Data → Key K_s (7)

Radio: MS → SRES (5) → ? → Pass/Fail Authentication (6)

Network: SGIN → HLR/AUC → Rand → SRES (5) → Encrypted Data → Key K_s (7)

Applications

- Understand the level of protection associated with each technology
- Identify strengths/weaknesses and areas for potential improvement

Focus

Computer Security, Network Security, Intrusion Detection, Firewalls, Distributed Systems Security, Embedded, & Wireless Systems Security, Computer & Network Forensic Techniques, Forensic Analysis and Incident Response.

Proposed Courses

- Data Security & Encryption Techniques
- Computer Forensics & Incident Response
- Computer Security & Forensic Analysis
- Network Security & Forensic Analysis
- Adv. Computer Security & Forensics

Group Members

S. Barua, N. Chen, J. Choi, B. Cong, S. Courellis, D. Falconer, A. Holliday, F. Holliday, D. Huizinga, C. Jo, D. Kastner, B. Laguna, D. Michalopoulos, M. Molodowitch, T. Ryu, X. Wang

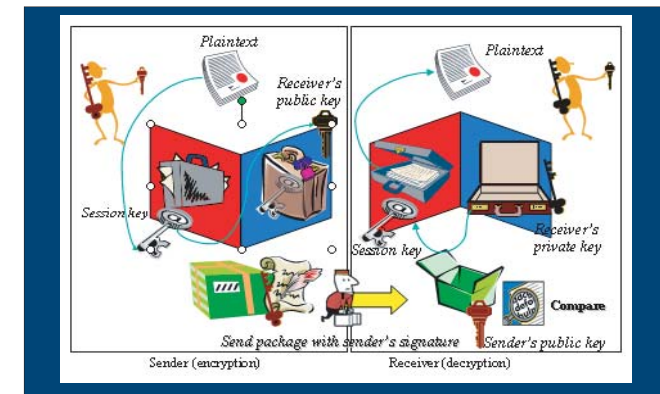
Collaborating Groups

- Data Mining and Bioinformatics
- Embedded, Wireless, & Mobile Computing
- Multimedia, Computer Games, & Digital Animation
- Software Engineering
- Web & Internet Technologies

Enhancing Security Design in Wireless Ad-Hoc Networks

Li, S. T. & X. Wang
CS Dept., California State Univ., Fullerton

Description: Performance and fault tolerance improvement in IEEE 802.11 wireless adhoc networks through the integration of the dynamic route discovery mechanism with a distributed security approach.



Applications

- Secure wireless workgroup business communication
- Secure home area networks and personal area networks.