NIST Wireless Security Guidance SP 800-48

December 4, 2002

Special Publication 800-48

The document examines the benefits and security risks of 802.11 WLAN, Bluetooth Ad Hoc Networks, and PDAs.

The document also provides practical guidelines and recommendations for mitigating the risks associated with these technologies

Over 30,000 downloads from over 50 countries

http://csrc.nist.gov/publications/nistpubs/index.html

Federal Information Processing Standard (140-2)

- FIPS 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for federal agencies that have determined that certain information be protected via cryptographic means.

- As currently defined, the security of neither 802.11 nor Bluetooth meets the FIPS 140-2 standard.

- Must employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport-Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms.

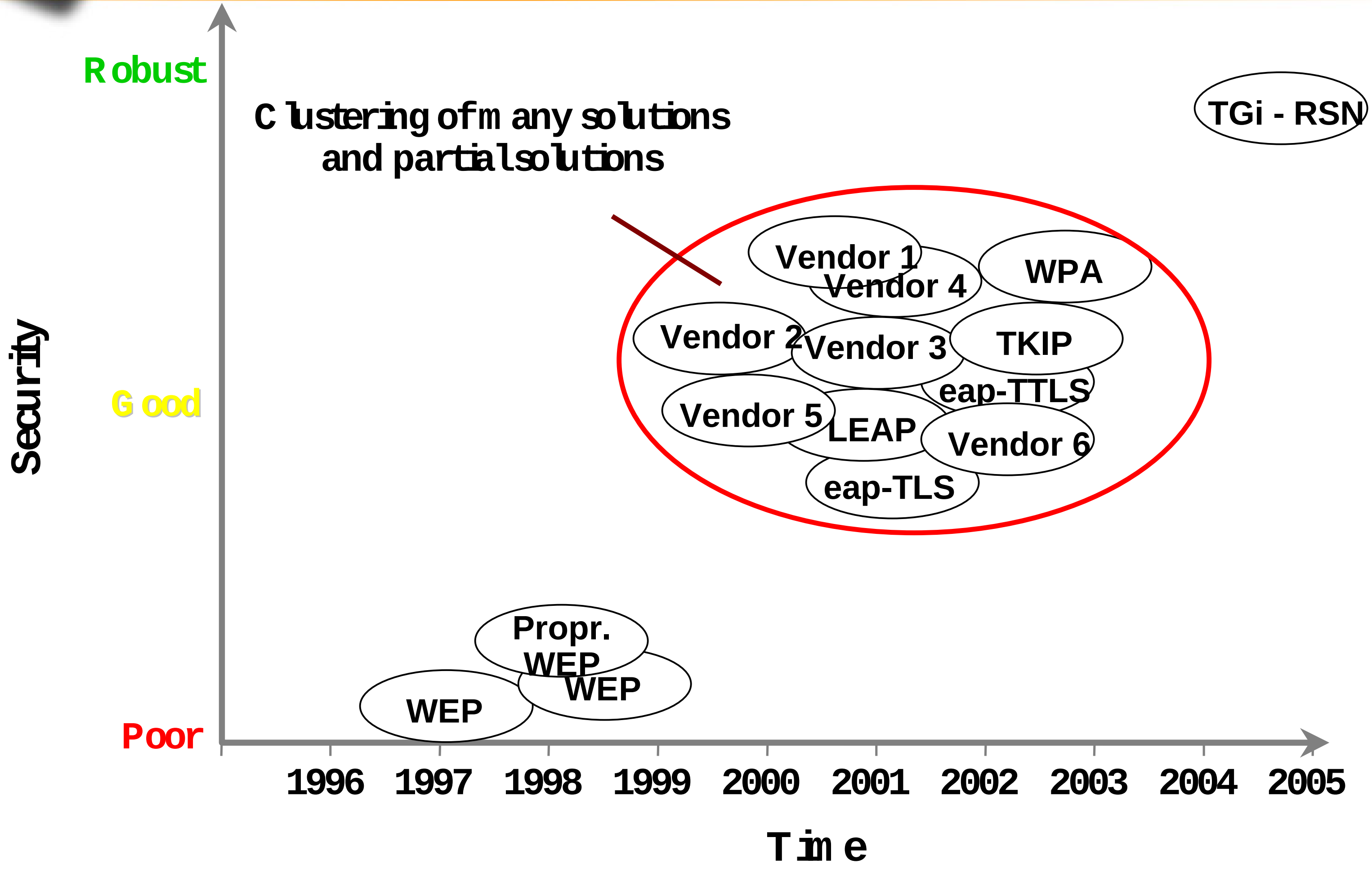
SP 800-48 Recommendations

- (FIPS) 140-2 *Security Requirements for Cryptographic Modules*
- Security is an ongoing process
- Understand Risks before wireless systems are deployed
- Understand technical and security implications
- Carefully plan deployment of these technologies
- Security management practices and controls are critical
- Physical controls are especially important
- Enable, use, and test security features

NIST - Industry

- Help Industry
- Guidance to Federal Agencies
- Standards
- Interoperability
- Security
- Open Process
- Public Review
- Vendor Neutrality

WiFi Security Evolution



Lessons for Wireless

- We must learn from our past
- Security must be built-in from the beginning
- Good cryptography is essential
- The right people must be applied to the security problem
- Key management cannot be ignored
- The development process cannot be rushed or security will suffer
- Vigilance is required from concept to operations

NIST Optimistic Plans

- Development of wireless security guidance documents
- Emerging wireless standards participation
- Wireless security research
- Empirical analysis in wireless Lab
- Explore impacts of technology convergence
- Technology assessments and secure architectures

Contact Information

- **Tom Karygiannis**

  National Institute of Standards and Technology

  karygiannis@nist.gov

  Telephone: 301-975-4728