

Esercitazione di Microsoft Word/2

Alcune funzioni avanzate



XXVII°
Campionato



di

Triathlon

Specialità ***IRONMAN***



Monet

The IEEE 802.11 standard [1] defines the Wired Equivalent Privacy, or WEP, encapsulation of 802.11 data frames. The goal of WEP is to provide data privacy to the level of a wired network.

The 802.11 design community generally concedes that the WEP encapsulation fails to meet its design goal, but widely attributes this failure to WEP's use of 40-bit RC4 (see [2] or [3] for a description of RC4) as its encryption mechanism. Even at this late date, it is still repeatedly suggested, asserted, and assumed that WEP could meet its design goal by migrating from 40-bit to 104- or 128-bit RC4 keys instead.



This report seeks dispel this notion once and for all: it is infeasible to achieve privacy with the WEP encapsulation by simply increasing key size. The submission reports easily implemented, practical attacks against WEP that succeed regardless of the key size or the cipher. In particular, as currently defined, WEP's usage of encryption is a fundamentally unsound construction; the WEP encapsulation remains insecure whether its key length is 1 bit or 1000 or any other size whatsoever, and the same remains true when any other stream cipher replaces RC4. The weakness stems from WEP's usage of its initialization vector. This vulnerability prevents the WEP encapsulation from providing a meaningful notion of privacy at any key size.

The deficiency of the WEP encapsulation design arises from attempts to adapt RC4 to an environment for which it is poorly suited. This submission accordingly argues to replace RC4 by different cryptographic primitives in new work going forward. It identifies the characteristics needed by any encryption algorithm that can effectively provide data privacy in a wireless environment, and recommends candidate replacement algorithms and a replacement encapsulation.

The IEEE 802.11 standard [1] defines the Wired Equivalent Privacy, or WEP, encapsulation of 802.11 data frames. The goal of WEP is to provide data privacy to the level of a wired network.

The 802.11 design community generally concedes that the WEP encapsulation fails to meet its design goal, but widely attributes this failure to WEP's use of 40-bit RC4 (see [2] or [3] for a description of RC4) as its encryption mechanism. Even at this late date, it is still repeatedly suggested, asserted, and assumed that WEP could meet its design goal by migrating from 40-bit to 104- or 128-bit RC4 keys instead.

This report seeks dispel this notion achieve privacy with the WEP key size. The submission reports attacks against WEP that succeed cipher. In particular, as currently is a fundamentally unsound encapsulation remains insecure 1000 or any other size whatsoever, other stream cipher replaces RC4. usage of its initialization vector. This encapsulation from providing a key size.

The deficiency of the WEP attempts to adapt RC4 to an suited. This submission accordingly cryptographic primitives in new characteristics needed by any effectively provide data privacy in a recommends candidate replacement encapsulation.



once and for all: it is infeasible to encapsulation by simply increasing easily implemented, practical regardless of the key size or the defined, WEP's usage of encryption construction; the WEP whether its key length is 1 bit or and the same remains true when any The weakness stems from WEP's vulnerability prevents the WEP meaningful notion of privacy at any

encapsulation design arises from environment for which it is poorly argues to replace RC4 by different work going forward. It identifies the encryption algorithm that can wireless environment, and algorithms and a replacement

The IEEE 802.11 standard [1] defines the Wired Equivalent Privacy, or WEP, encapsulation of 802.11 data frames. The goal of WEP is to provide data privacy to the level of a wired network.

The 802.11 design community generally concedes that the WEP encapsulation fails to meet its design goal, but widely attributes this failure to WEP's use of 40-bit RC4 (see [2] or [3] for a description of RC4) as its encryption mechanism. Even at this late date, it is still repeatedly suggested, asserted, and assumed that WEP could meet its design goal by migrating from 40-bit to 104- or 128-bit RC4 keys instead.



This report seeks to dispel this notion once and for all: it is infeasible to achieve privacy with the WEP encapsulation by simply increasing key size. The submission reports easily implemented, practical attacks against WEP that succeed regardless of the key size or the cipher. In particular, as currently defined, WEP's usage of encryption is a fundamentally unsound construction; the WEP encapsulation remains insecure whether its key length is 1 bit or 1000 or any other size whatsoever, and the same remains true when any other stream cipher replaces RC4. The weakness stems from WEP's usage of its initialization vector.

This vulnerability prevents the WEP encapsulation from providing a meaningful notion of privacy at any key size.

The deficiency of the WEP encapsulation design arises from attempts to adapt RC4 to an environment for which it is poorly suited. This submission accordingly argues to replace RC4 by different cryptographic primitives in new work going forward. It identifies the characteristics needed by any encryption algorithm that can effectively provide data privacy in a wireless environment, and recommends candidate replacement algorithms and a replacement encapsulation.

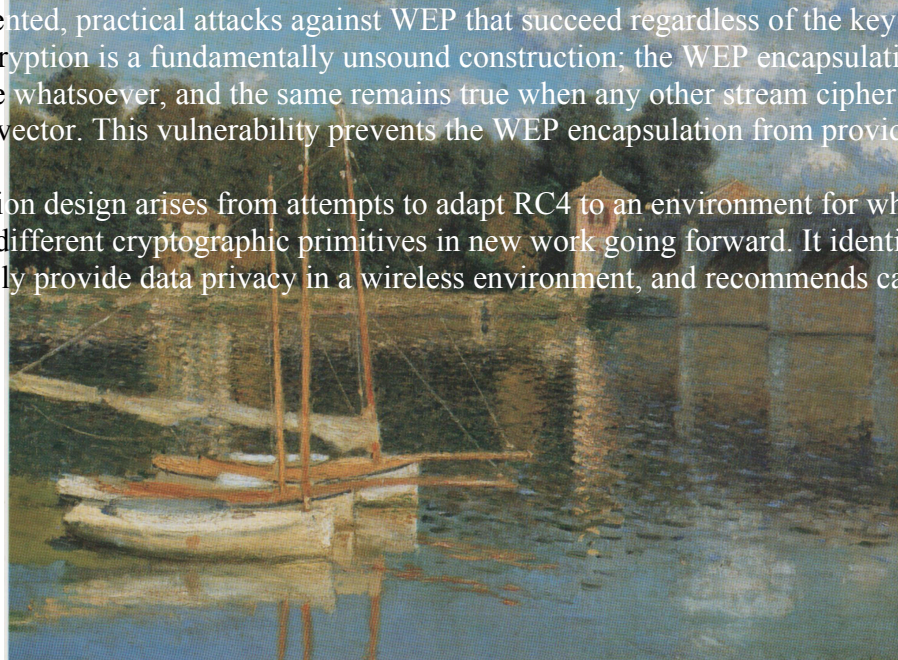
The IEEE 802.11 standard [1] defines the Wired Equivalent Privacy, or WEP, encapsulation of 802.11 data frames. The goal of WEP is to provide data privacy to the level of a wired network.

The 802.11 design community generally concedes that the WEP encapsulation fails to meet its design goal, but widely attributes this failure to WEP's use of 40-bit RC4 (see [2] or [3] for a description of RC4) as its encryption mechanism. Even at this late date, it is still repeatedly suggested, asserted, and assumed that WEP could meet its design goal by migrating from 40-bit to 104- or 128-bit RC4 keys instead.

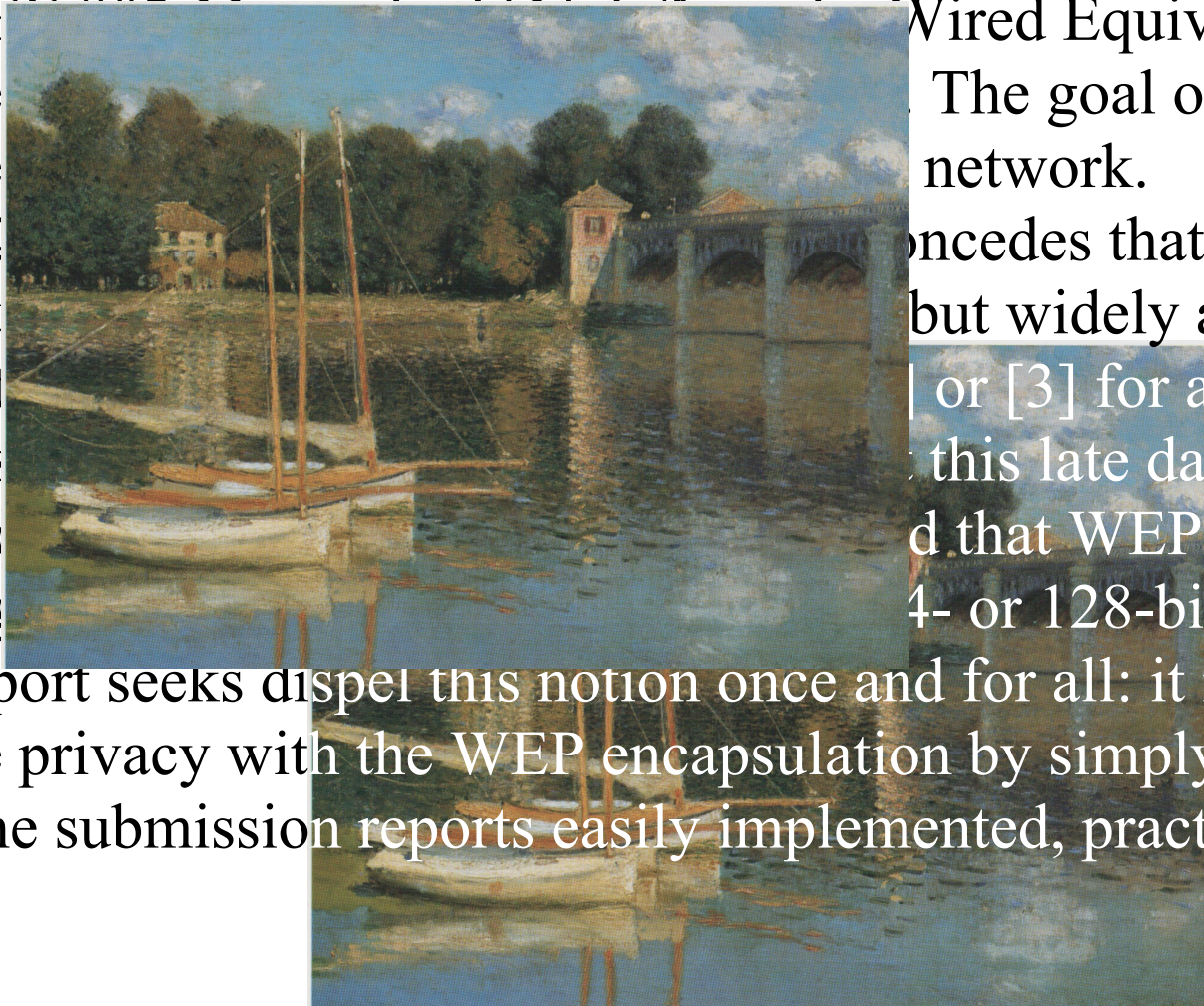
This report seeks dispel this notion once and for all: it is infeasible to achieve privacy with the WEP encapsulation by simply increasing key size.

The submission reports easily implemented, practical attacks against WEP that succeed regardless of the key size or the cipher. In particular, as currently defined, WEP's usage of encryption is a fundamentally unsound construction; the WEP encapsulation remains insecure whether its key length is 1 bit or 1000 or any other size whatsoever, and the same remains true when any other stream cipher replaces RC4. The weakness stems from WEP's usage of its initialization vector. This vulnerability prevents the WEP encapsulation from providing a meaningful notion of privacy at any key size.

The deficiency of the WEP encapsulation design arises from attempts to adapt RC4 to an environment for which it is poorly suited. This submission accordingly argues to replace RC4 by different cryptographic primitives in new work going forward. It identifies the characteristics needed by any encryption algorithm that can effectively provide data privacy in a wireless environment, and recommends candidate replacement algorithms and a replacement encapsulation.



The IEEE 802.11 standard defines WEP, and provides a mechanism for providing confidentiality. The 802.11 standard defines WEP encapsulation (using RC4) as a means of providing confidentiality. The standard repeatedly states that WEP is designed to provide confidentiality.



This report seeks to dispel this notion once and for all: it is infeasible to achieve privacy with the WEP encapsulation by simply increasing key size. The submission reports an easily implemented, practical attack on WEP that can be used to recover the plaintext of any WEP-encrypted packet.

Wired Equivalent Privacy, or WEP. The goal of WEP is to provide confidentiality over a network. The standard concedes that the WEP standard is flawed, but widely attributes this flaw to the RC4 algorithm. For a description of the RC4 algorithm, see [3]. At this late date, it is still surprising to find that WEP could meet its goal of providing confidentiality with 4- or 128-bit RC4 keys instead.

Questa è una cella				
Questa cella è orientata in verticale	Questa cella è orientata in verticale	Questa cella è allineata in alto	Questa cella è allineata al centro	Questa cella è allineata in basso

	Questa cella è ottenuta unendo celle contigue sulla stessa riga			
Questa cella è ottenuta unendo celle contigue sulla stessa riga				
		Queste celle sono ottenute dividendo una singola cella	Queste celle sono ottenute dividendo una singola cella	