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 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.

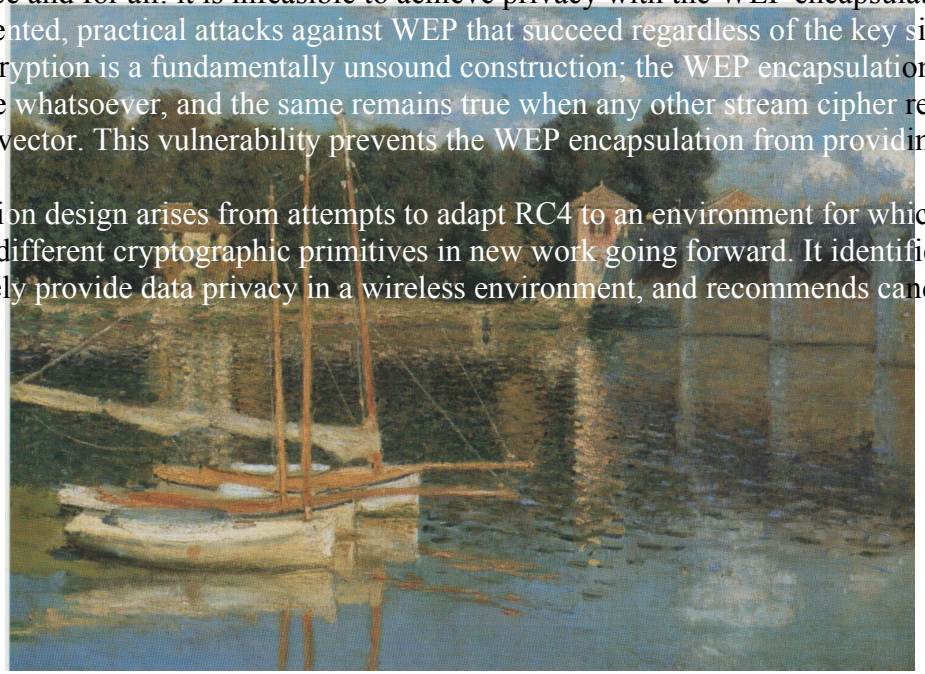
This report seeks dispel this notion once and for all: it is infeasible to achieve privacy with the WEP encapsulation by simply increasing key size. The submission reports easily implemented, practical attacks against WEP that succeed regardless of the key size or the cipher. In particular, as currently 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 [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.

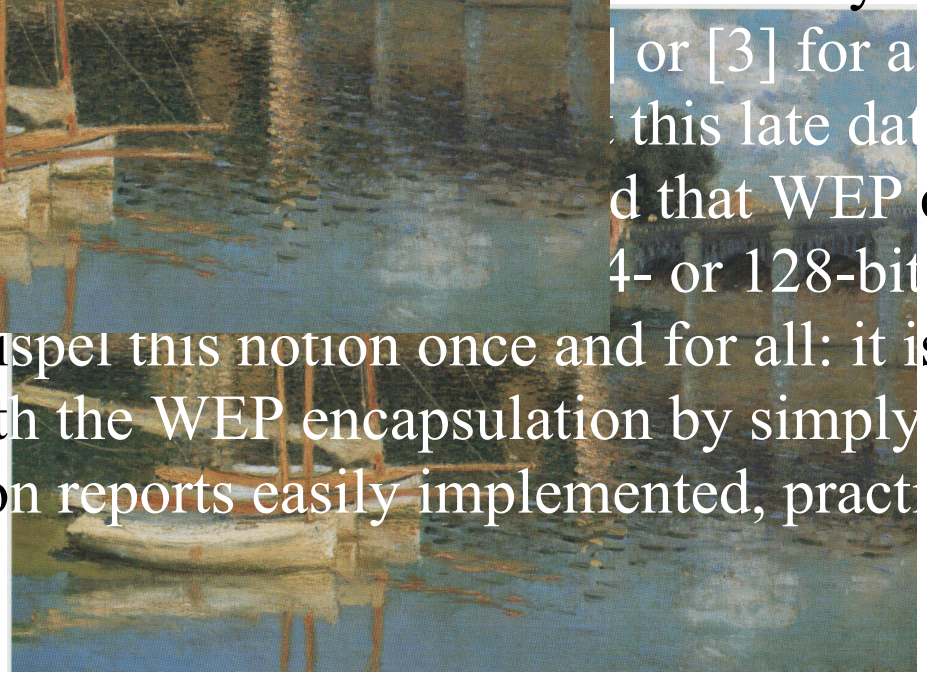
The 802.11 design community generally concedes that the WEP encapsulation fails to meet its design goal, but widely attributes this failure to WEP's use of 40-bit RC4 (see [2] or [3] for a description of RC4) as its encryption mechanism. Even at this late date, it is still repeatedly suggested, asserted, 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 IEE Wired Equivalent Privacy, or
WEP, e . The goal of WEP is to
provide network.
The 802 ncedes that the WEP
encapsu but widely attributes this
failure t or [3] for a description of
RC4) as this late date, it is still
repeated d that WEP could meet its
design g 4- 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, pract



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

<table>
<tr><td></td><td colspan="3">Questa cella è ottenuta unendo celle contigue sulla stessa riga</td></tr>
<tr><td rowspan="2">Questa cella è ottenuta unendo celle contigue sulla stessa riga</td><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td>Queste celle sono ottenute dividendo una singola cella</td><td>Queste celle sono ottenute dividendo una singola cella</td><td></td></tr>
</table>