

Using Model-Checking to Reveal a Vulnerability of Tamper-Evident Pairing

Rody Kersten¹ Bernard van Gastel² Manu Drijvers¹
Sjaak Smetsers¹ Marko van Eekelen^{1,2}

¹Radboud University Nijmegen, The Netherlands

²Open University of the Netherlands, The Netherlands



May 14, 2013





Wi-Fi Protected Setup



- Setup WPA2 without remembering passphrases
- PIN method
- Push-Button Configuration (PBC)





PBC vulnerabilities

- **Collision** - The adversary jams the legitimate message, preventing the receiver from decoding it, then sends his own message instead
- **Capture effect** - The adversary transmits a message at the same time as the legitimate sender, but at significantly higher power
- **Timing control** - The adversary impersonates the receiver by continuously occupying the medium after the sender sends his key, preventing the actual receiver to send his key, but sending his own instead



Tamper Evident Pairing (TEP)



Shyamnath Gollakota, Nabeel Ahmed, Nickolai Zeldovich, and Dina Katabi. Massachusetts Institute of Technology.

Secure In-Band Wireless Pairing.

Usenix Security, 2011



Tamper Evident Pairing (TEP)

- The IEEE 802.11 standard requires Wi-Fi hardware to sense the wireless medium for energy
- Sending a packet of fixed (large) length, means energy on channel
- Not sending a packet means no energy, unless others are transmitting
- On/Off slots
- Can be used as bits



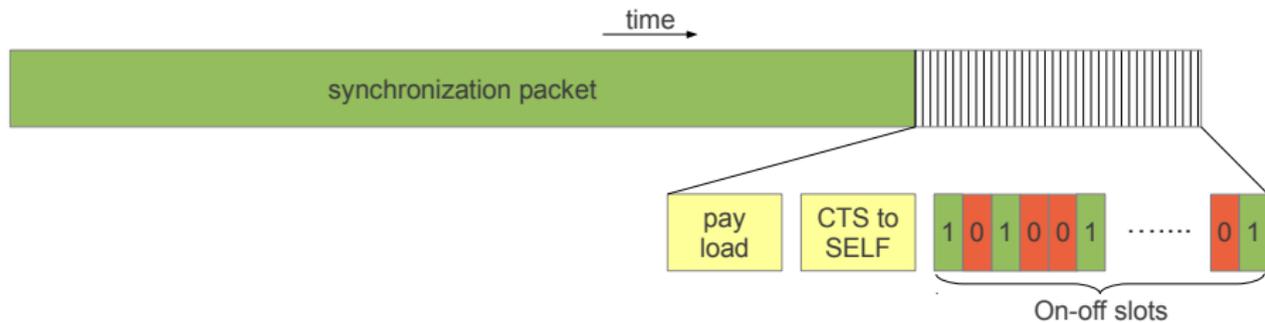
Attacker Model

An adversary, trying to launch a man-in-the-middle attack, has the following capabilities:

- Overwrite data packets
- Introduce energy on the wireless medium



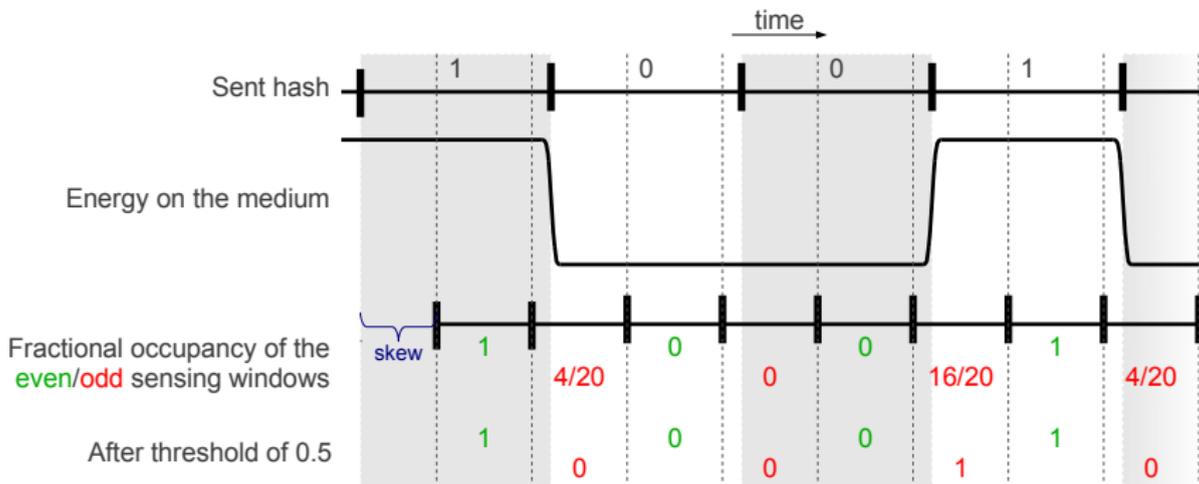
Tamper Evident Announcement (TEA)



Slots are “bit-balanced”!



Receiving the Slots





Model Parameters

Several parameters were underspecified, these have become parameters to the Spin model:

- Hash length
- Number of measurements per sensing window
- Sensing window threshold
- Skew



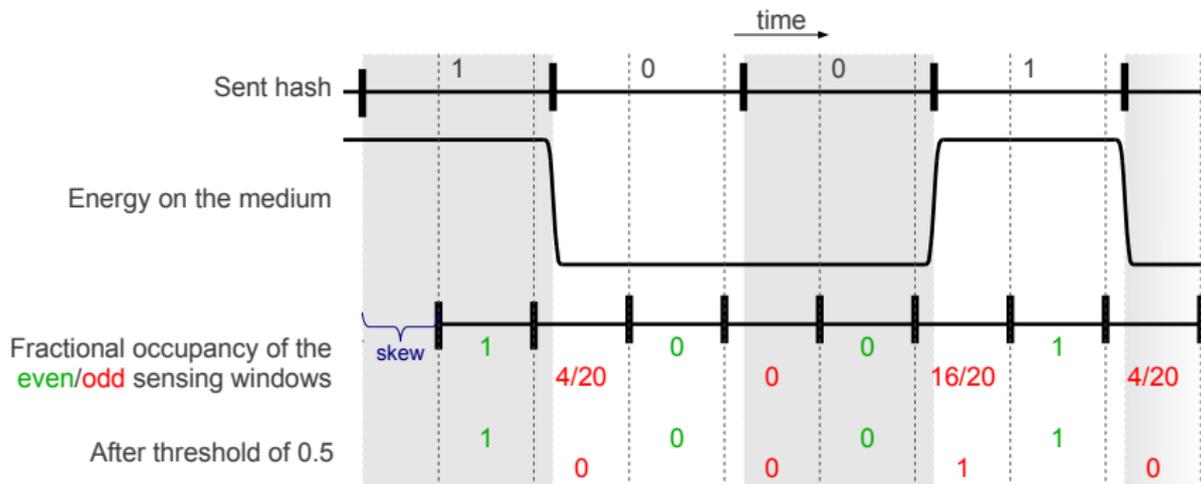
Processes

- Clock
- Sender
- Receiver
- Adversary

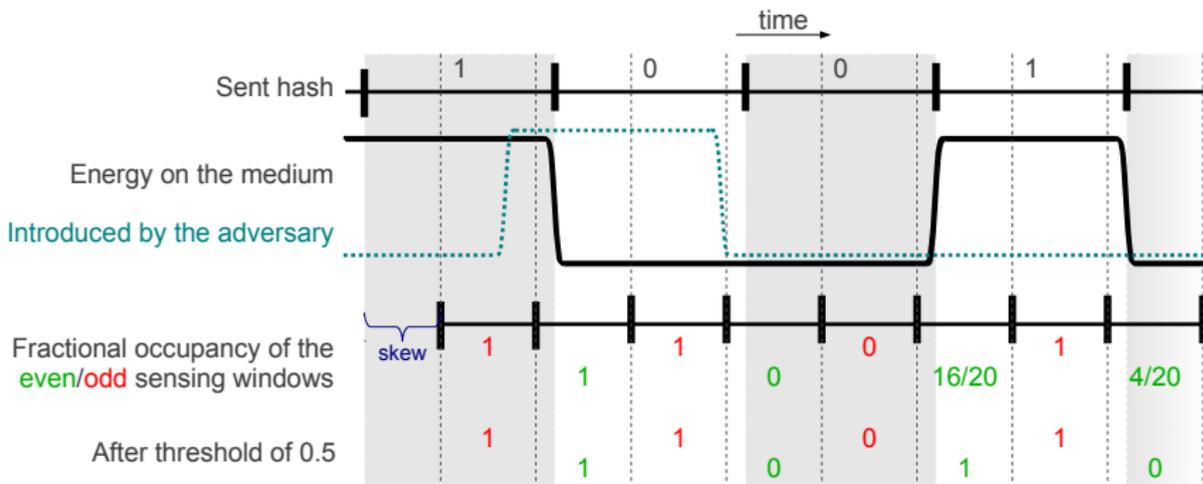
```
1 proctype adversary () {  
2   end :  
3   do  
4     :: mediumAdversary = 1;  
5     mediumAdversary = 0;  
6   od  
7 }
```



Revealed Vulnerability in the TEA



Revealed Vulnerability in the TEA





Varying the Values of the Model Parameters

threshold = 3

		<i>skew</i>										
		0	1	2	3	4	5	6	7	8	9	10
<i>sw_meas.</i>	4	+	-	-	-	-	-	-	-	-	-	-
	5	+	+	-	-	-	-	-	-	-	-	-
	6	+	+	+	-	-	-	-	-	-	-	-
	7	+	+	+	+	-	-	-	-	-	-	-
	8	+	+	+	+	+	-	-	-	-	-	-
	9	+	+	+	+	+	+	-	-	-	-	-
10	+	+	+	+	+	+	+	-	-	-	-	

threshold = 5

		<i>skew</i>										
		0	1	2	3	4	5	6	7	8	9	10
<i>sw_meas.</i>	6	+	-	-	-	-	-	-	-	-	-	-
	7	+	+	-	-	-	-	-	-	-	-	-
	8	+	+	+	-	-	-	-	-	-	-	-
	9	+	+	+	+	-	-	-	-	-	-	-
	10	+	+	+	+	+	-	-	-	-	-	-

threshold = 7

		<i>skew</i>										
		0	1	2	3	4	5	6	7	8	9	10
<i>sw_meas.</i>	8	+	-	-	-	-	-	-	-	-	-	-
	9	+	+	-	-	-	-	-	-	-	-	-
	10	+	+	+	-	-	-	-	-	-	-	-

threshold = 9

		<i>skew</i>										
		0	1	2	3	4	5	6	7	8	9	10
<i>sw_meas.</i>	10	+	-	-	-	-	-	-	-	-	-	-

$$\textit{skew} \geq \textit{sw_measurements} - \textit{threshold}$$



Summary

- Modeled the Tamper-Evident Announcement in Spin
- Several parameters were not adequately specified by the authors of TEP
- Model-Checking revealed a serious vulnerability for certain values of these parameters
- An adversary aiming to initiate a man-in-the-middle attack can evidently tamper with the received hash