

---

<b>5</b>	<b>Addressing leaks through networking</b>	<b>21</b>
	Scenario 0: An air-gapped system (no network) . . . . .	22
	Scenario 1: A closed network of trusted peers . . . . .	23
	Scenario 2: Tor-ified or VPN-ed open Internet . . . . .	24
	Scenario 3: Unconstrained Internet access? . . . . .	25
<b>6</b>	<b>(Un)trusting firmware and the host OS</b>	<b>27</b>
	Firmware considerations . . . . .	27
	Host OS considerations . . . . .	28
	Reconsidering BIOS and ME (un)trusting? . . . . .	28
<b>7</b>	<b>Addressing Evil Maid Attacks</b>	<b>30</b>
<b>8</b>	<b>Select implementation considerations</b>	<b>32</b>
	SPI Flash emulation challenges . . . . .	32
	Host OS implementation considerations . . . . .	33
	User partition encryption considerations . . . . .	34
	Temper-resistance considerations . . . . .	34
<b>9</b>	<b>Alternative solutions?</b>	<b>36</b>
	ARM-based platforms? . . . . .	36
	FPGA-based, true open source processors and platforms? . . . . .	37
<b>10</b>	<b>Summary</b>	<b>38</b>
	<b>Credits</b>	<b>39</b>
	<b>Contacting the author</b>	<b>40</b>
	<b>References</b>	<b>41</b>