CS 5438: Security and Privacy: Practice and Case Studies Homework #2

Due: Before class on 30 Apr. 2016

Instructors: Ari Juels and Vitaly Shmatikov

Each question is worth 10 points. The total assignment is worth 130 points.

1. Cryptocurrencies, Blockchains, and Smart Contracts

   (a) The company 21 Inc. purportedly planned to offer free 15W toasters that doubled as Bitcoin miners and computed at around 125 Gigahashes per second. Assume the following: (1) Electricity costs 12 cents per kilowatt-hour; (2) The Bitcoin network has a hash rate of 1.25×10^{18} hashes / sec; (3) A block is mined exactly every 10 minutes; and (4) The current 25 BTC block reward is worth $10,000. Would you use the 21 Inc. toaster under these assumptions? Why or why not?

   (b) Recall Duncan Goldie-Scot's lecture, which included a discussion of Bitpesa, which uses Bitcoin for remittances. Why is Bitcoin beneficial for this purpose?

   (c) Why has Bitcoin made ransomware more pervasive and profitable?

   (d) How might the owner of a Bitcoin address prove her ownership off-chain, i.e., without performing a transaction?

   (e) Transactions and smart contracts executed on (decentralized) blockchains are publicly visible. Give an example of a smart contract (which may be hypothetical) for which this feature could be problematic, and explain what the problem is.

(f) Name two threats to the long-term viability of the Bitcoin network, i.e., why might Bitcoin fail in the end to see broad adoption—or even survive?

(g) Write a smart contract in pseudocode that implements a highest-price auction for a domain name DN. For simplicity, you may use the notation "Assign(DN, P)" to denote the assignment of DN to account holder $\mathcal{P}$. You may use the notation from the relevant lecture notes (which may be found on Piazza).

2. Internet surveillance and censorship.
   Find three different tools that claim to help users evade surveillance and censorship.

   (a) How did you find these tools?

   (b) What promises do these tools make to their users? Do these promises differ between tools?

   (c) How do you think each tool works?

3. TLS and certificates

   (a) Explain the differences between an HTTPS session protected using a regular certificate and an HTTPS session protected using an extended-validation certificate.

      i. What does the browser do differently?

      ii. What is the difference from the viewpoint of a "Web attacker," i.e., someone who controls a malicious website and wants to impersonate a legitimate site?

      iii. What is the difference from the viewpoint of a "network attacker," i.e., someone who controls a malicious router or Wi-Fi access point?

   (b) Sotirov et al. used MD5 hash collisions to forge a rogue SSL certificate for the name "MD5 Collisions Inc." This certificate can be used to issue additional fraudulent certificates for arbitrary Web domains, such as gmail.com

      i. Why would anyone believe that "MD5 Collisions Inc." is authorized to issue certificates for other domains?

ii. The forged "MD5 Collisions Inc." certificate is not one of the root certificates stored by the Web browser. Would the browser accept a gmail.com certificate issued using the forged certificate? Why or why not?

(c) How can Web browsers protect users from ...

i. forged certificates?

ii. compromised certificate authorities?

iii. malicious "re-signing" certificates installed by Komodia, PrivDog, and similar tools?