Cybersecurity for Future Presidents

Lecture 13:
DEBATE #5:

Debate 5: Resolved: Bitcoin transactions are better for consumers than credit card transactions.

Any Questions?

My office hours:
Wed. afternoon, 12-3pm, 442 RH. Signup sheet circulating

- About previous lecture?
- About homework? (debate questions)
- About reading? (Bitcoin and credit card payment processing)

Reading for next week: 3 papers on cyberattack/cyberwarfare

1. Berson, T.A. and Denning, D.E. "Cyberwarfare,.
2. National Research Council, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyb erattack Capabilities. Chapter 1, pp. 9-23. (Up to Section 1.8).
3. Sanger, David. "U.S. Directs Cyberweapons at ISIS for First Time." New York Times, p. 1, 25 August 2016. (available on Canvas)

Exercise for next week:
Questions related to the reading and earlier course topics

Cybersecurity events from the past week of interest to future (or current) Presidents:

- Update on $81M theft from Bengladeshi central bank
  - BAE Systems reports that malware was installed on SWIFT client software to allow thieves to prevent printing of transfer records and to erase records of transfers
  - http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR
- NYT reports on cyberattacks on ISIS
  - Implants reportedly placed on command & control networks
  - No reports of physical damage
  - http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?ref=world
- FBI purchase of iPhone zero-day exploit said to cost $1.3M (=7*$186,000)

Coming up: … ?

Today's Debate

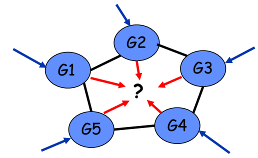
DEBATE #5:
Resolved: Bitcoin transactions are better for consumers than credit card transactions.

Byzantine Generals (aka Byzantine Agreement)

- 1982 paper by Lamport, Shostak, and Pease
- The scenario: A set of generals, each with his own troops, surround an enemy city. The generals need to agree on a common plan of attack, but some of the generals are traitors and may try to prevent the loyal generals from reaching consensus
- Desired properties of solution:
  - All loyal generals agree on the same course of action
  - A small number of traitors cannot cause the loyal generals to adopt a bad plan
- Where this problem came from:
  - Need to provide automated control (e.g. of an airplane) when some components may be faulty, and fail in arbitrarily bad ways
  - Replicated components (e.g. sensors, actuators) correspond to the generals
- How it relates to Bitcoin;
  - Bitcoin needs consensus among miners to agree on which blockchain fork is the right one to build on

A little more motivation for the problem…

- Suppose you have several replicated computers and several replicated sensors
- Each computer gets input from several sensors (e.g., "hot" or "cold")
- Computers send messages to each other to try to generate consensus on sensor readings
- Consensus used to instruct actuator (e.g. move up or move down)
- If a computer fails in a bad way, it may send false messages about its sensor readings (inputs) to other computers (and it may "lie" – i.e., tell one computer "hot" and another "cold") = "Byzantine" fault

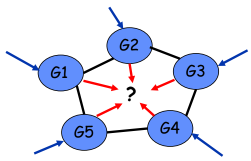


Blue arrows = input
Black arrows = comms
Red arrows = output

Key parameter: m = # of traitorous generals

Some other parameters for the problem:

- Messages are sent among generals:
  - Synchronous / asynchronous / other?
  - Oral (corruptible) or non-oral
- All loyal generals following same protocol?
- Can messages be undetectably modified by adversary?
- . . .



Some Basic Results on Byzantine Agreement

- With synchronous oral messages, you need at least 3m+1 generals to tolerate m traitors
  - Hence it is impossible to solve this problem with only three generals (= 3 processors)
- So to tolerate one traitor, you need at least 4 generals total
- The problem is much-studied (fun for computer scientists) and there are many different parameters to twiddle

- Bitcoin miners look a bit like the Byzantine generals
  - There might be incentives to be a traitor
- Communications are flooded in the bitcoin P2P network (or they are supposed to be)
- Messages are signed, so not as vulnerable as "oral messages" to corruption, but false messages might be introduced
- Bottom line: bitcoin protocol is not a clean abstraction, it's a real protocol. There are informal arguments about its properties but not mathematical proofs, as far as I know.

Bitcoin "multisig" – not really threshold crypto

- You may not want to trust your entire private key to your own machine (what if it gets hacked?)
- How can you safely share the key with another machine?
- There are "secret sharing" schemes developed in cryptography that enable this kind of behavior
- Bitcoin has implemented something called "multi-sig" that supports this kind of function (e.g., two of three must agree for a transaction to go ahead (or 5 of 6 or other possibilities)
- But this apparently is more like requiring a tuple of signatures on the transaction rather than splitting a secret key into parts and sharing the parts

Backup slides follow

Computing with encrypted data

Zero knowledge proofs (not profs!)

ZKP – a form of interactive proof between a prover and a verifier in which the verifier learns nothing about a specific solution but is convinced the the prover has the information (eg. solution to a Sudoku) in question