CSci 5271
Introduction to Computer Security
Day 26: Student Project Presentations #1

Stephen McCamant

University of Minnesota, Computer Science & Engineering

Outline

Announcements

Exercise set 4 debrief

Bitcoin experience (cont'd)

Social network tracking 1:18

Evasive JavaScript malware 1:36

Smartphone messaging DoS 1:54

Project reports and meetings

- Final individual report due 11:55pm tonight
- Meetings scheduled for this week

Exercise set 5 due Thursday

- Final exercises due 11:55pm 12/5
- Plan to return both it and HW2 before final

Turn in presentation slides

- After presentation, send copy of slides to Stephen
  - PDF format preferred if possible
- Evaluation comments by email

Presentation logistics

- Main presentation/demo: 12 minutes
  - Save most questions until the end
  - I stand up → time to finish up
- Audience Q&A: 3 minutes
  - Ideal: insightful but not too hostile
  - I may have questions if no students do

Outline

Announcements

Exercise set 4 debrief

Bitcoin experience (cont'd)

Social network tracking 1:18

Evasive JavaScript malware 1:36

Smartphone messaging DoS 1:54

Seeding a PRNG

- Entropy required for unpredictability
- Black-box attacks easy, reverse engineering also possible
- Bad ideas:
  - `time()`
  - Process ID
  - Time XOR PID
- How to do better?

Web server false alarms

- Attack is unlikely to appear in benign traffic
  - Illegal UTF-8 rep. of path traversal
- Best way to inject false positives?
  - IP spoofing not easy for TCP
- Takeaway: FP/FN rates depend on attacker

ViruSniff

- Can you have no FNs without solving the halting problem?
- Mimicry attack against ViruSniff
- Countermeasures

DoS protection: Sly's scheme

- Requests get delayed bit if not first in queue from their IP
- Delayed requests re-queued until a second has passed
- Can an attacker still deny service?

DoS protection: Carl's scheme

- When overloaded, redirect traffic to previous clients
- Can attackers still deny service?
- What else can go wrong?

Outline

Announcements

Exercise set 4 debrief

Bitcoin experience (cont'd)

Social network tracking 1:18

Evasive JavaScript malware 1:36

Smartphone messaging DoS 1:54

Bitcoin mining trends

- Exponentially increasing rates
- CPU → GPU → FPGA → ASIC
- Specialized hardware eclipsing general purpose
  - Including malware and botnets
- Recent price trends suggest continuing investment

Enforcing consistency

- Structure of network very resistant to protocol change
  - Inertia of everybody else's code
- Changes unpopular among miners will not stick
- Minor crisis in March: details of database lock allocation cause half of network to reject large block

Stealing bitcoins

- Bitcoins are a very tempting target for malware
  - Private keys stored directly on client machines
  - Theft is non-reversible
  - Much easier than PayPal or identity theft
- Standard recommendation is to keep keys mostly offline

Bitcoin (non-)anonymity

- Bitcoin addresses are not directly tied to any other identity
- But the block chain is public, so there's lots of information
  - List of largest balances on Wikipedia, academic research
  - `http://eprint.iacr.org/2013/782`
- Real unlinkability is a research topic

Outline

Announcements

Exercise set 4 debrief

Bitcoin experience (cont'd)

Social network tracking 1:18

Evasive JavaScript malware 1:36

Smartphone messaging DoS 1:54

Outline

Announcements

Exercise set 4 debrief

Bitcoin experience (cont'd)

Social network tracking 1:18

Evasive JavaScript malware 1:36

Smartphone messaging DoS 1:54

Outline

Announcements

Exercise set 4 debrief

Bitcoin experience (cont'd)

Social network tracking 1:18

Evasive JavaScript malware 1:36

Smartphone messaging DoS 1:54