Prolog to Lecture 5
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

The SHA-1 Crack

- Google recently (2017) “cracked” SHA-1
- What’s that actually mean?
- What are the implications?
- Should you be worried?

What Does It Mean?

- SHA-1 is a secure hashing algorithm
- A number of bad things can happen to secure hashing algorithms
- One is collisions
  - Where two different data patterns hash to the same thing
  - Especially bad if you can find a second data pattern with same hash as a given pattern’s

That’s What Happened to SHA-1

- Google found two PDFs that SHA-1 hashed to the same thing
- Worse, two very similar PDFs
  - https://shattered.io/static/shattered-1.pdf
  - https://shattered.io/static/shattered-2.pdf
- Essentially the same document, with a different color banner

What Are the Implications?

- An attacker could substitute one document with another
- If identity of first document was secured via SHA-1,
- The switch wouldn’t be noticed
- Could change contracts, scientific data, who knows what?

What Bad Things Could Happen?

- Cryptographic hashes are very widely used
- To secure web transactions
- To set up VPNs
- To distribute keys
- Lots of other stuff
- So possibly wide-ranging effects

A Few Relevant Details

- The attack found a match for <u>one</u> document
  - Would need to repeat it for others
- The attack cost $100,000 in compute resources
  - 110 years of a single GPU’s computations
  - Actually done in parallel on many machines

Not Really a New Attack

- Attack method was discovered some years ago
- Google was simply the first to (publically) perform the attack
- Pretty much anyone with sufficient resources could do the same

Should You Be Worried?

- Mostly not
- The attack is still very expensive
  - So few will perform it
  - *But attacks always get cheaper*
- SHA-1 was deprecated many years ago
  - Not used in modern software
  - *But still in some old legacy systems*