Slide 3/4  Attacking the certification model.

The big challenge, and achievement in the paper, is forging the rogue CA certificate; the black one in the diagram.

This is done by using a MD5 collision attack, which is why it bears 'exactly the same signature' as the blue, valid certificate.

From there, it is then fairly easy to construct a bogus certificate of the website you want to attack—the red one—and it can be verified using the black certificate. Since the black and blue costs are the same, the browser will accept the black, which then verifies the red certificate, and you 'win'—the browser is redirected to the malicious copy site.

Hash Functions: Understanding distinction between Second Preimage Resistance and Collision Resistance. Collision resistance involves a top-down approach using H; Second preimage involves using an already decoded m.

MD5 compression details: page 6-7 in Paper.

Armour begins to crack—write on board using 'one step' of MD5 diagram.

\[ E \xrightarrow{H} JHV \]
- Describe fundamental flaw of MO construction. Chum by chunk (odd/even) iteration.<

Chosen - Prefix Collision:

More steps expand upon previous chalkboard drawing.

\[ \text{prefix} = \text{prefix} \]

At this point, "birthdaying" has caused IHVs to be close, but not equal.

Use series of "near-collision" blocks to massage the IHVs to be near the same.

Before transitioning.

Birthday bits: biggest computational obstacle. \(2^{3^{1/2}} \) times needed 200 PS3 game consoles for computation.

Estimated around \(2^{30}\) MOS compression calls w/30 GB of memory takes "a little more than a day" for a single attempt.