Cybersecurity

Cryptographic Attacks

CYBER.ORG

Cryptographic Attacks

- Strong encryption helps ensure safe communication between sender and receiver
- Modern encryption methods are based on algorithms that are relatively easy to compute but difficult and time consuming to decrypt without the key
- It's been said encryption has existed in some form for as long as there have been written secrets
- Attempts to break encryption by a third party must be anticipated
- The following attacks are popular methods to cracking

Collisions

- Hashes are very useful in ensure data integrity
- Hash values are supposed to be *unique*
  - Different input values should never create the same output result
- When hashes are the same, this is called a collision

- The MD5 hashing algorithm is a popular method
- Collisions in MD5 can be *generated*.
  - MD5 first published in 1992
  - MD5 Collisions identified in 1996
- MD5 is useful but not safe. New hashing methods used now

Collision example

- Following two large values generate the same MD5 hash

d131dd02c5e6eec4693d9a0698aff95c	d131dd02c5e6eec4693d9a0698aff95c
2fcab58712467eab4004583eb8fb7f89	2fcab50712467eab4004583eb8fb7f89
55ad340609f4b30283e488832571415a	55ad340609f4b30283e4888325f1415a
085125e8f7cdc99fd91dbdf280373c5b	085125e8f7cdc99fd91dbd7280373c5b
d8823e3156348f5bae6dacd436c919c6	d8823e3156348f5bae6dacd436c919c6
dd53e2b487da03fd02396306d248cda0	dd53e23487da03fd02396306d248cda0
e99f33420f577ee8ce54b67080a80d1e	e99f33420f577ee8ce54b6708280d1e
c69821bcb6a8839396f9652b6ff72a70	c69821bcb6a8839396f965ab6ff72a70
MD5 Hash:	MD5 Hash:
79054025255fb1a26e4bc422aef54eb4	79054025255fb1a26e4bc422aef54eb4

- Collisions are bad for secure, trust-worthy encryption!
- Solution is often to make resulting hash values larger

Birthday Problem

- With a group of 30 people, what are the chances that any two individuals share a birthday?
  - Remember, there are 365 possible birthdays (+1 if you count Leap Day)
  - Actually works out to ~70%!
  - Seems crazy, known as the Birthday Problem or Birthday Paradox.
    Chances go up as more people are added to the group.
- This statistical anomaly is basis for The Birthday Attack

Birthday Attack

- Instead of matching birthdays, let's look for matching hash values. (In the cyber world, this is a hash collision)
- Find a collision through brute force
  - Might seem like it'll take a super long time, but Birthday Paradox suggests it might not take as long
- Hacker generates multiple versions of plaintext to hash then check for matching hashes
  - Protect yourself with a large hash output size (e.g. MD5 hashes are only 32 characters long)

Downgrade Attack

- Old cryptographic processes are abandoned for newer, more secure algorithms
- Due to compatibility issues, some older code or systems may use less-than-ideal cryptography
- Forcing one system to downgrade its security weakens the security of the entire system
- Old crypto algorithms are retired for a reason!
  - *Don't use weak crypto!*