Imperfect Forward Secrecy by J.Alex Halderman

This was quite an interesting talk. They started off by saying NSA breaks a lot of crypto algorithms and that they spy on communications. He stated that an attacker could try two methods to crack widely used crypto. The attacker either attacks the implementation by finding vulnerabilities or adding backdoors or attacks the crypto algorithms themselves. The only difference between these methods is if the attacker attacks the implementations then the attacker has to make a big investment in the hardware and the piece of software that the attacker is trying to compromise. He also states that the public key cryptography is most likely to be targeted than symmetric key cryptography.

They explained a little about the RSA algorithm. First, they started off with the textbook RSA and said that the only reason this algorithm is considered strong is because factoring a given number is not easy. Then they explained a method called the number field sieve that has multiple stages and helps in factoring a number. A table containing the accurate amount of time that would be taken to factor different sized keys using this method was put up showing that it is easy to factor a 512 bit size prime number.

After this they talked about the diffiehellman key exchange algorithm. They stated that it provided perfect forward secrecy as long as a fresh random value was generated for each session. They also said that the diffie hellman cryptanalysis was difficult because calculating discrete logs is hard, i.e, given g^a mod p it would be very difficult to obtain a. Also, they pointed out that in the number field sieve algorithm, all the stages except the last stage depends on the prime number 'p'. Therefore, if many communications use the same 'p' we could precompute all these stages which make it easier to crack the security of communications. Therefore, this makes it easy for NSA to crack 512 bit connections. Also, back in the 90's the US restricted the cipher suites on export goods to a limited subset called export grade cipher suites which was a list of crypto algorithms that exported products can use outside the US. According to the speaker, this was done to allow NSA to eavesdrop on communications.

Even today this export grade cipher suite is used which only allows a maximum of 512 bits. There are two attacks that can exploit this vulnerability. The connections are downgraded to this cipher suite and after which 512 bits are factored and all communications can be broken. These two attacks are the FREAK attack and logjam attack. They explained what happens in the logjam attack and how the attacker modifies the messages to downgrade the connection to an export grade DH and perform a man-in-the-middle attack. From their research they presented certain statistics which showed that 97% of hosts use one of three 512 bit primes. This was a result of these primes being hardcoded onto the machines or servers. So they had performed precomputations for these using the number field sieve method and found that it took only 70 seconds to break the connections after having the precomputations. To defend against the

logjam attack the internet explorer, chrome and firefox browsers started accepting only 1024 bits. After this, they talked about how the government could use this attack for massive surveillance and about NSA being able to decrypt VPN connections. Overall the talk was very insightful and interesting. At the end of the talk I strongly felt that people who said, “anything could be broken” are all correct.