Defending Computer Networks
Lecture 22: Public Key Encryption

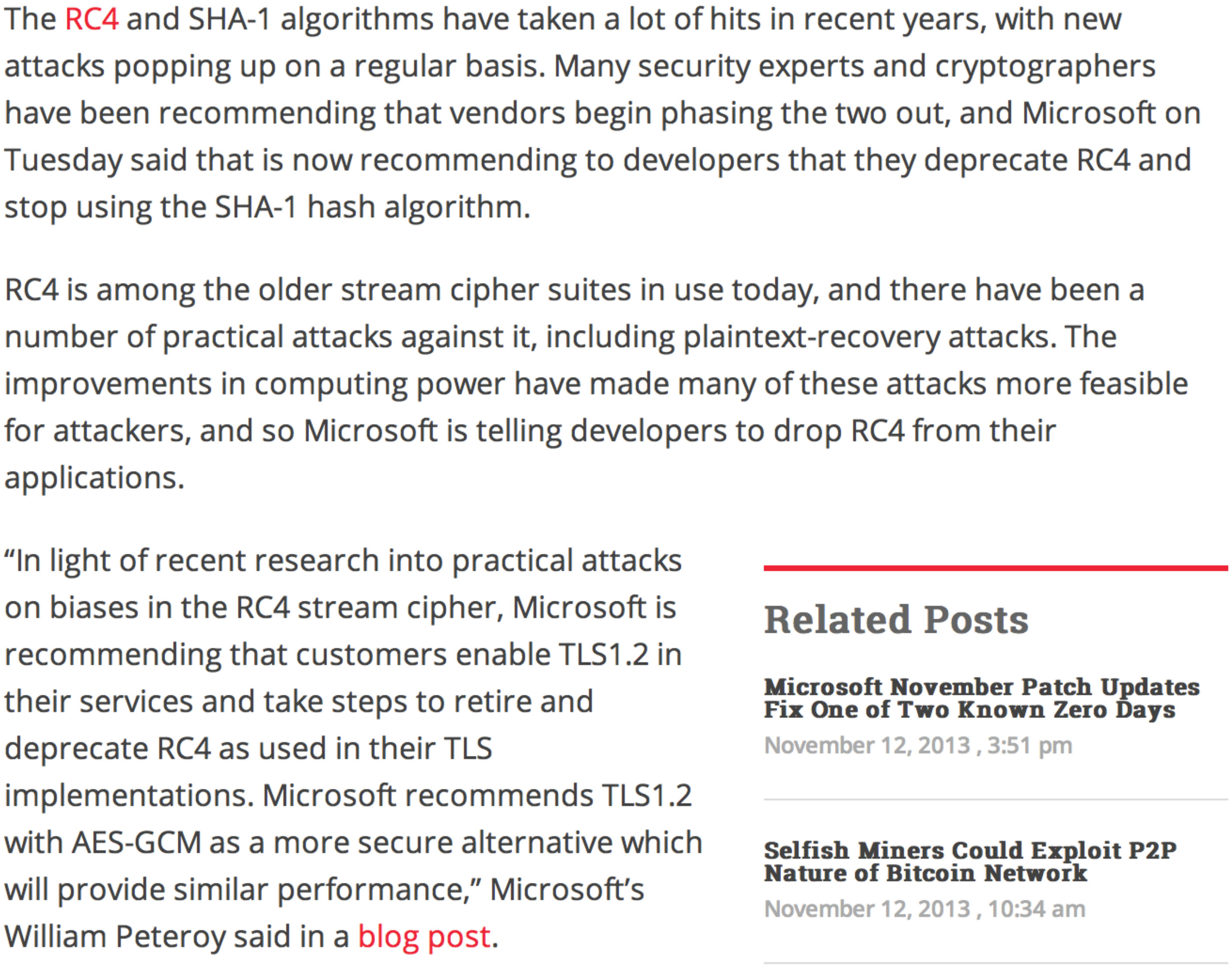
Stuart Staniford

Adjunct Professor of Computer Science

Logistics

- Quiz 2
- Guest lecture next Thursday

Latest News



The RC4 and SHA-1 algorithms have taken a lot of hits in recent years, with new attacks popping up on a regular basis. Many security experts and cryptographers have been recommending that vendors begin phasing the two out, and Microsoft on Tuesday said that is now recommending to developers that they deprecate RC4 and stop using the SHA-1 hash algorithm.

RC4 is among the older stream cipher suites in use today, and there have been a number of practical attacks against it, including plaintext-recovery attacks. The improvements in computing power have made many of these attacks more feasible for attackers, and so Microsoft is telling developers to drop RC4 from their applications.

“In light of recent research into practical attacks on biases in the RC4 stream cipher, Microsoft is recommending that customers enable TLS1.2 in their services and take steps to retire and deprecate RC4 as used in their TLS implementations. Microsoft recommends TLS1.2 with AES-GCM as a more secure alternative which will provide similar performance,” Microsoft’s William Peteroy said in a blog post.

Related Posts

Microsoft November Patch Updates Fix One of Two Known Zero Days

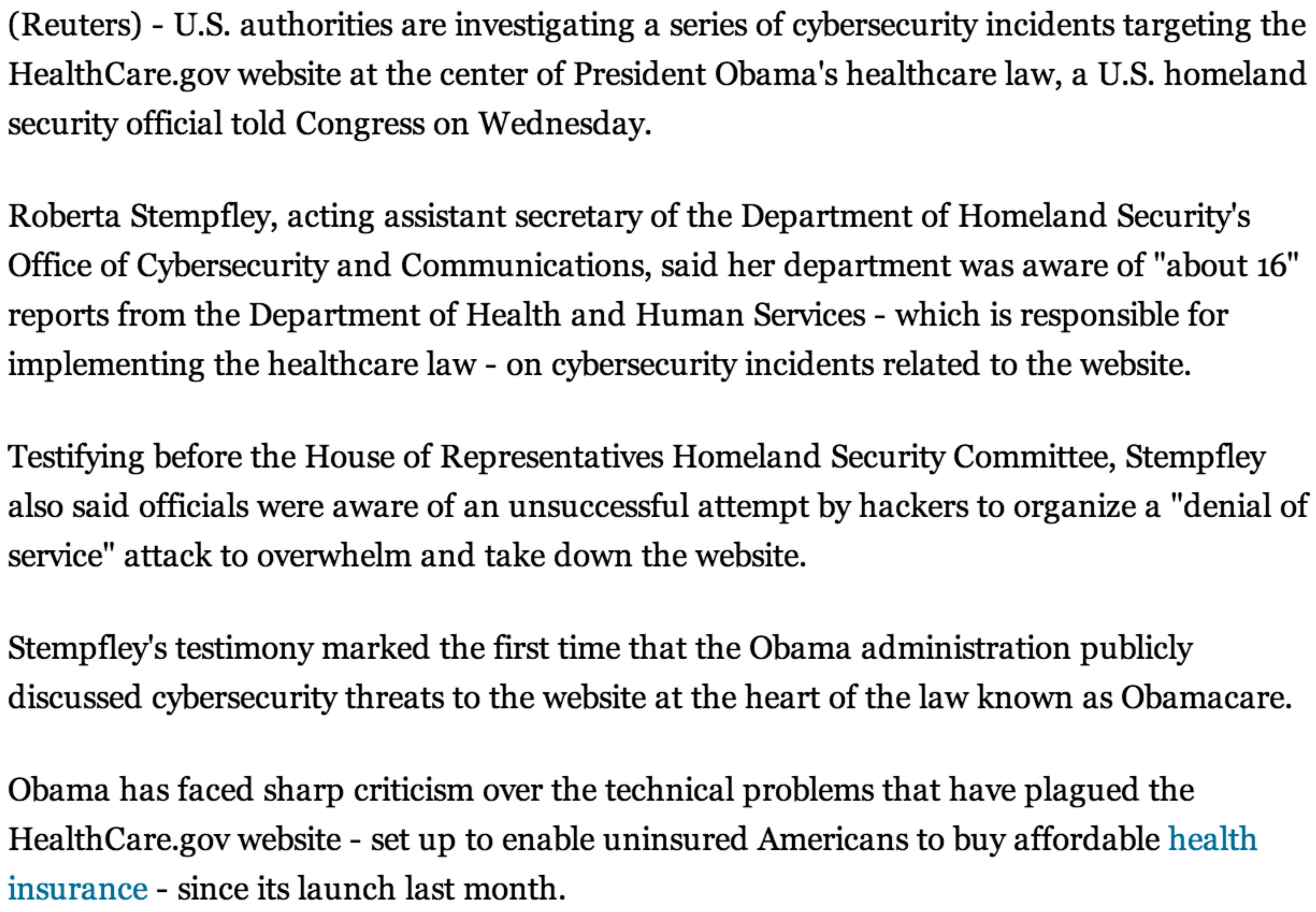
November 12, 2013 , 3:51 pm

Selfish Miners Could Exploit P2P Nature of Bitcoin Network

November 12, 2013 , 10:34 am

http://threatpost.com/microsoft-warns-customers-away-from-sha-1-and-rc4/102902

More News



(Reuters) - U.S. authorities are investigating a series of cybersecurity incidents targeting the HealthCare.gov website at the center of President Obama's healthcare law, a U.S. homeland security official told Congress on Wednesday.

Roberta Stempfley, acting assistant secretary of the Department of Homeland Security's Office of Cybersecurity and Communications, said her department was aware of "about 16" reports from the Department of Health and Human Services - which is responsible for implementing the healthcare law - on cybersecurity incidents related to the website.

Testifying before the House of Representatives Homeland Security Committee, Stempfley also said officials were aware of an unsuccessful attempt by hackers to organize a "denial of service" attack to overwhelm and take down the website.

Stempfley's testimony marked the first time that the Obama administration publicly discussed cybersecurity threats to the website at the heart of the law known as Obamacare.

Obama has faced sharp criticism over the technical problems that have plagued the HealthCare.gov website - set up to enable uninsured Americans to buy affordable health insurance - since its launch last month.

http://www.reuters.com/article/2013/11/13/us-usa-healthcare-security-idUSBRE9AC16M20131113

Main Focus of Today

- Public/Private Key Cryptography

Public Key Cryptography

- Also known as Asymmetric Cryptography
    - To distinguish from symmetric cryptography
        - shared secret
- Instead of shared key, keys come in pairs
    - Public key used to encrypt data
    - Private key used to decrypt data
    - Not feasible to infer private key from public key

Main Advantage

- Enormously simplifies key management
  - Imagine large group that need to communicate by shared key schemes
    - Share one key amongst many and risk losing everything
    - Or keep track of n^2 keys
- With public key crypto, I give out my public key, everyone can know it.
  - Anyone can send me a message
  - Only I can read those messages
  - I only have to worry about one secret key (mine)
  - Don’t have to share my secret (private) key with anyone

History

- Invented in the seventies
- 1973, secretly, by GCHQ (British intel)
- 1976 Diffie Hellmann Key exchange
- 1977 RSA public/private key exchange
  - Rivest, Shamir, Adleman
- Many more schemes since then
- RSA still in wide practical use
  - 1024 bit keys considered weak, but longer ok

RSA

- Underlying base is difficulty of factoring very large numbers
- Will sketch algorithm while again skipping worst of math details
- We choose two large primes *p*, *q*
  - hundreds of digits each
  - Modulus, *n = pq*
  - Size of *n* in bits is the key length
  - Then choose an exponent, *e* that
    - Has no common factors with *(p-1)(q-1)*
- Public key is *n* and *e*
- Private key can be computed from *p* & *q*

Encryption

- Take the text and turn blocks of text into numbers. Say M is number for some block
- Then take M^e mod n
- Toy example
  - http://www.woodmann.com/crackz/Tutorials/Rsa.htm
  - p = 43, q = 59 (both prime)
  - n = 43*59 = 2537
  - e = 13 (no common factor with 42 or 58)

Encryption Example

- Message is ST OP
- Encode as 1819 1415
  - $1819^{13} \bmod 2537 = 2081$
  - $1415^{13} \bmod 2537 = 2182$
  - Ciphertext is 2081 2182

Decryption

- Find decryption exponent d such that
- *de* mod *(p-1)(q-1) = 1*
- Ie *d* is the multiplicative inverse of *e*,
  - modulo *(p-1)(q-1)*
  - Tractable algorithms for this are known
- Then plaintext P can be computed from C
  - $P = C^d \bmod n$

Decryption Example

- Suppose ciphertext is 0981 0461
- d = 937 for our previous example
- 937*13 mod 2436 = 12181 mod 2436 = 1
- 0981^{13} mod 2537 = 0704
- 0981^{13} mod 2537 = 1115
- Message was HE LP

Applicability of Public Key

- Typically public key algorithms are computationally expensive.
- Not practical to apply to long messages
- Therefore generally used in the process of establishing a temporary symmetric key
  - Session key
    - Encrypted by public key crypto for transfer
    - Then used to encrypt lengthy communication session
    - Then thrown away

Let’s Try It

- openssl genrsa -out private_key.pem 1024
- more private_key.pem
- openssl rsa -in private_key.pem -text -noout
- openssl rsa -pubout -in private_key.pem -out public_key.pem
- more public_key.pem