Lecture 2: Some Basic Vocabulary of Computer and Network Security and a Brief Review of Classical Encryption Techniques

Lecture Notes on "Computer and Network Security"

by Avi Kak (kak@purdue.edu)

April 30, 2017

10:40am

Goals:

- To introduce the rudiments of the vocabulary of computer and network security and that of encryption/decryption.

- To trace the history of some early approaches to cryptography and to show through this history a common failing of humans to get carried away by the technological and scientific hubris of the moment.

- **Simple Python and Perl scripts that give you pretty good security for confidential communications. Only good for fun, though.**

CONTENTS

2.1: BASIC VOCABULARY TO GET US STARTED

I'll start this section with some basic vocabulary of encryption and decryption, since that's the primary focus of the beginning lectures in this series. Subsequently, I'll also review some of the basic vocabulary of computer and network security more from a systems perspective. For the systems oriented vocabulary, I'll present the definitions in the recently released "Android Security: 2016 Year in Review."

So let's start with encryption and decryption:

plaintext: This is what you want to encrypt

ciphertext: The encrypted output

enciphering or encryption: The process by which plaintext is converted into ciphertext

encryption algorithm: The sequence of data processing steps that go into transforming plaintext into ciphertext. Various parameters used by an encryption algorithm are derived from a secret key. In cryptography for commercial and other civilian applications, the encryption and decryption algorithms are placed in the public domain. [Just think about the consequences of keeping the algorithms secret. First and foremost, a secret algorithm is less likely to be subject to the same level of testing and scrutiny that a public algorithm is. And, assuming that a secret algorithm is used for all communications within an organization, what if a disgruntled employee posted the algorithm anonymously on WikiLeaks?]

secret key: A secret key is used to set some or all of the various parameters used by the encryption algorithm. **The important thing to note is that, in classical cryptography, the same secret key is used for encryption and decryption.** It is for this reason that classical cryptography is also referred to as symmetric key cryptography. **On the other hand, in the more modern cryptographic algorithms, the encryption and decryption keys are not only different, but also one of them is placed in the public domain.** Such algorithms are commonly referred to as asymmetric key cryptography, public key cryptography, etc.

deciphering or decryption: Recovering plaintext from ciphertext

decryption algorithm: The sequence of data processing steps that go into transforming ciphertext back into plaintext. In classical cryptography, the various parameters used by a decryption algorithm are derived from the same secret key that was used in the encryption algorithm.

cryptography: The many schemes available today for encryption and decryption

cryptographic system: Any single scheme for encryption and decryption

cipher: A cipher means the same thing as a “cryptographic system”

block cipher: A block cipher processes a block of input data at a time and produces a ciphertext block of the same size.

stream cipher: A stream cipher encrypts data on the fly, usually one byte at at time.

cryptanalysis: Means “breaking the code”. Cryptanalysis relies on a knowledge of the encryption algorithm (that for civilian applications should be in the public domain) and some knowledge of the possible structure of the plaintext (such as the structure of a typical inter-bank financial transaction) for a partial or full reconstruction of the plaintext from ciphertext. Additionally, the goal is to also infer the key for decryption of future messages.

The precise methods used for cryptanalysis depend on whether the “attacker” has just a piece of ciphertext, or pairs of plaintext and ciphertext, how much structure is possessed by the plaintext, and how much of that structure is known to the attacker.

All forms of cryptanalysis for classical encryption exploit the fact that some aspect of the structure of plaintext may survive in the ciphertext.

key space: The total number of all possible keys that can be used in a cryptographic system. For example, **DES** uses a 56-bit key. So the key space is of size 2^{56}, which is approximately the same as 7.2×10^{16}.

brute-force attack: When encryption and decryption algorithms are publicly available, as they generally are, a brute-force attack means trying