

第6讲: 技术驱动下公共到私人的演变

主讲人: Hal Abelson

加密技术

加密技术是如何运作的回顾。我们发现从1980年至2001年, 这一军事、武器上的技术变为平常之用。把加密术看作关系到新技术引进的政策重点。

技术和政策的缺陷:

— “秘密”一词和每个人都有特定关系, 但这些关系都没有涉及到互联网。

— 大约十年前, “电子邮件”这个词没有实际意义, 因为没有人用它。

— 当我们提到电子邮件和加密术时, 他们并不是值得信赖的邮件运送者形象。

机密性—你关心的是, 保证意愿中的接收人收到信息

完整性—你如何知道信息没有被截取和篡改, 不可否认后来你确实收到了信息。

这是一个关于加密术的回顾。

这些被称为数字签名

1. 前历史密码术 (十九世纪七十年代之前):

2. 公共密钥

3. 密码术政策

密码术ca1900BC

这是人们发现最早的成形的密码术—heiroglyphics.

Geoffrey Chaucer 是一个诗人和天文学家, 曾用英文写过第一本科学手册 *Treatise on the Astrolabe*. 他加密了书中的一部分 (class exercise)

他用的形式称为置换密码. 当你用一种方式替换时成为单一字母替换法。

Julius Ceasar 用的替换法是将所有被替代物转化为相同长度进行替换。

在九世纪, Yaqub写了一本频率分析的书(英语字母平均频率图)这是一项始于九世纪的方法。

一千年以后, 令人吃惊的是这种加密术仍在使用。人们仍在使用不可靠的加密方法。不到五年前的互联网上, 一些公司还在都受他们的不可靠甚至极差的加密产品。

\*Vigenere 加密技术

Vigenere 普及了这种加密术, 但确切地说是Alberti创造的。从“a”到“s”, 从“b”到“o” ... 每次替代后循环下去。这是五百年中出现的一次主要突破, 并且被认为是牢不可破的加密方法。事实上, 在十九世纪中期它被超越了。

\*破解 Vigenere

因为英语中语言有特定长度, 所以出现n-different 频率分布问题。

最难的部分是找出算子的长度。

十九世纪二十年代末, 多数国家用数学的black-jammers

chambers 来破解破解 Vigenere

Friedman 发明了破解Vigenere 的代码索引。直到十九世纪二十年代人们才知道Babbage 已经破解了Vigenere代码, 因为他从未对外宣布此事。许多想破解的人并没有得到这项殊荣, 应为他们止步于分类工作。

算子和信息一样长 — 一次一密 (one time pad)

只有被证明为安全密码才是一次一密, 倘若你随机选择算子, 并只用一次。但是人们仍在试图找到更加可靠的办法。

Venona 项目始于1943年。有很多一次一密的例子。

Claude Shannon — 信息理论的英雄, Shannon创造了“bit”这个词, 他也第一次正式定义了可靠加密的定义。

Shannon's 1949年的论文诞生了“绝对保密”概念。

现在最机密的是产生随机pads的方法和途径。找到好的一次一密是非常困难的。

我们现在使用的密码流就是Vigenere的类似品。

DES (数据加密标准)已经过时。NSA (国家安全局)加强了运算法则从而变得更安全。对DES,人们把信息分割成六十四位的许多块,然后进行S-box转换(基于56位算子),最后放在一起。这是非常有效的,因为这只是变得不规则,并容易解码,精巧的设计使之易于复原。数据加密标准的安全性:

唯一破解的办法是原始的尝试所有算子,1965年,  $2^{56}$  是数目巨大的算子,现在算不了什么。

政府强制人们不得使用DES。

NIST (国家技术于标准学会)。

Kerckhoffs 法则:

这与比利时语言学家写的一本关于加密系统优良特性的指导手册有关。原则之一是:仅有极少信息必须安全的设计才是优秀的。安全应该倚仗算子的选择,而不是含糊不清的设计。

Andrew "Bunnie" Huang一破译了关于Xbox的密码.数字Millenium著作权法严禁人们出版散布具有著作权的材料。这些早期的加密术原则并不适合互联网。

伟大的设想:创造一个共享的算子,把他提供给那些从未谋面或从未交流过的人们,并且没有优先的安排。

密码系统

多样的攻击:

选定的纯文本—三百个相同字母。

胶皮管—用胶皮管抽打别人。

这些都不适用于互联网,因为你不得不去满足算子互换。

Diffie是麻省理工的毕业生,他偶遇在斯坦福工作的Marty Hellman, Ralph Merkle 是伯克利的一名毕业生, Merkle对public-key encryption (公共密钥密码)很有见解, Hellman和Diffie编写了运算法则。他们在1976年发表了具有突破进展的论文。仅仅八年前1973-74 Clifford Cocks和Malcolm Williamson在英国情报机构秘密工作时发现的。

Diffie-Hellman-Merkle基本想法:

在任何人能听见相互所说的事情时,如何交换秘密信息呢? Alice会设计只有自己明白地信息, Bob也这样做,结果这里出现了只有Alice和Bob明白的密码。通常是用单项功能的方法,在硬币的一面是一个简单的问题,另一面是需要大量计算的问题。按照以上理论Bob和Alice不在计算这些相同数字,而是用共享的算子进行加密交流,对于那些窃听者来说,他们必须解决离散的编码问题。

数字签名:

我们可以制作一个让别人核对通过的签名,但是这却是很难。生产保证及不被篡改。授权且保证权威。最后你陷入了一个为了获取保证而建立的授权炼中。

基本传输层安全协议(熟知的SSL):

这个协议是客户方的证明, Diffie和Hellman没有关于公共密钥加密的实现方法。不久RSA算法产生了。 RSA可以用在公共密钥和数字签名上。麻省理工和斯坦福都申请专利。RSA是很好的专利,但是公共密钥却相反。麻省理工和斯坦福在公共密钥方面合作并形成协议。他们不对外许可公共密钥专利,除非对方也用RSA专利。公共密钥直到2001年才放开。现在有很多公共密钥编码公诸于世。

十九世纪七十年代末, NSA主管Bobby Ray开始不安起来。过去和现在,加密术都是一项军事武器。NSA开始对外宣布自己的职员撤出。

之后MIT和NSA会谈。MIT很难在校园秘密进行工作。理所当然的,他们把论文和情报送交NSA,随之是代理处和工作人员。Louis Freeh将其变为FBI优先权,1994年,加密术被认为技术中的异类,因为害怕被犯罪分子和恐怖主义利用。

Clipper

公众不愿意使用加密电话。clipper芯片由NSA设计，从而人们可以进行加密通信，这是一种内置的秘密技术。你是如何看待clipper电话？这受到了电化制造业的抵制。这种精密的芯片提高了电话的成本。

算子契约战

—由反复的复杂政策争执构成。

- 各项代理不断的推动议会采用其议程。

答案是出口控制

如果有人做加密软件和产品销售的买卖，那么他会注册为武器经销商。早在1995年前，加密技术就被政府部门划分为军火类。

CIILNKSS – 包括叙利亚，苏丹和利比亚。

有传闻称，1995年NSA有一项监听所有通讯的项目，没有人能说清楚这个秘密项目的缘由。该项目组监听了世界上很多通讯，结果所有的讨论和NIST会谈中止了。建立这些系统其实非常便宜，很多消费者没有意识到这一点。

1996年五月

人们可以拥有自己的加密术，但必须向特定协议注册算子。这是将加密术与电子商业联姻。白宫制定了注册证明的价格并允许电子商业注册算子。

立法，1997年

当时电子业未经注册和没有记录在案的算子很多，这是为了防止议会中断其出口。

在“算子复苏的危险”一文中，认为没有讨论公民自由的余地，文章是在强调阻止犯罪的风险，并从此观点进行了技术性分析。

技术观察：

在政府可以很快介入的情况下，谁还能拥有合法的算子呐，在2000年左右，密码术的法律才变得自由起来，在1994，任何使用软件的个人和团体必须拥有加密许可，这是电子商业压倒工业的结果。

到了2001年九月，Sen. Judd Gregg在国会中提议，应该对加密术采取措施。纳入到1997年立法在法律上是必要的。实际情况已经满足，所以风险已经不再。没有参议员联合拥护此立法，所以到十月份Sen. Gregg不再引介这项法案。

发生了哪些改变呐？

1995年，加密术与电子邮件的关系有些不同，现在加密意味着保护信用卡等，加密变成了消费者的事情。是这个词本身定义了今天的技术与政策。但这可能尚未结束。现在我们不得不对电话安全进行另外的调整。政府拥有什么样的监听权？像Skype之类的网络应用软件又该如何？大家都该遵守CALEA规则吗？在接下来的两年，我们会看到更多变化，也可能网络应用的规则。