Insecurity in ATM-based passive optical networks

Stephen Thomas
Wave7 Optics
Email: sthomas@w7optics.com

David Wagner
University of California at Berkeley
Email: daw@cs.berkeley.edu

***Abstract*— We consider the security of an ITU standard for ATM-based passive optical networks. First, we show that the standard's encryption algorithm, called churning, has an effective 8-bit key length and thus is trivial to break with exhaustive keysearch. Second, we show that the authentication mechanisms have significant weaknesses. The conclusion is that these measures should not be relied upon to provide security.**

***Index Terms*—APON, ATM, passive optical networks, churning, encryption, authentication, security.**

I. Introduction

ATM-based passive optical networks (APON) are high-speed, optical access networks for voice, video, and data traffic. APONs are emerging as a viable technology for connections to homes and businesses. In the United States, deployments and trials by BellSouth, Qwest, and SBC are underway now or beginning shortly [4].

APONs are shared media networks. Packets transmitted to any subscriber are actually broadcast simultaneously to multiple subscribers, with addressing information in each packet indicating the intended recipient. Just as for other shared media technologies such as DOCSIS cable modems and IEEE 802.11 wireless networks, the security of data transmission is critical in protecting the privacy of users and confidentiality of their communications. The current APON standards specify a new encryption technique, known as *churning*, to provide "the necessary function of data scrambling" and to offer "protection for data confidentiality" [2].

Unfortunately, churning has many critical, even fatal, flaws, and it is trivial to defeat. We show easy passive attacks on churning. These flaws are not merely theoretical: defeating churning is well within the capabilities of would-be eavesdroppers today, and APON sniffer tools could easily incorporate methods for automated real-time cryptanalysis of churning at essentially no performance impact.

APON users are at a high risk of having their presumed private communications exposed to adversaries. Even users that employ other security techniques—Secure Sockets Layer (SSL) encryption, for example—may still inadvertently disclose information such as the identity of Web servers with which they communicate. Furthermore, many applications supported by APONs (e.g. ATM-based telephony) do not normally provide any security services on their own, assuming, instead, that individual links are secure.

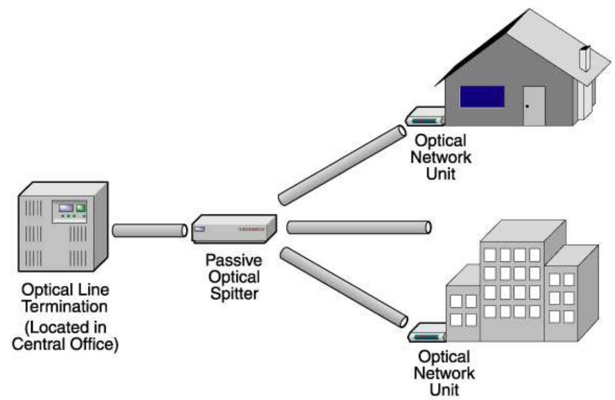

Fig. 1. Architecture of an ATM-based passive optical network.

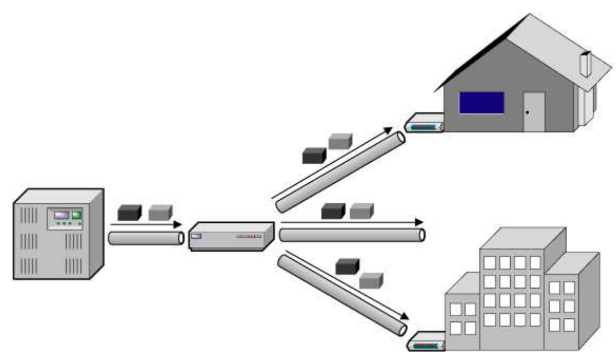

Fig. 2. Packets from the central office are broadcast to all customers on the same network segment.

II. APON Networks

ATM-based passive optical networks rely solely on fiber optic cabling to connect communications networks to homes and businesses. From the central office (or equivalent facility) a single fiber optic cable extends 10 km or more into a neighborhood. As Figure 1 shows, a passive optical device splits the signal into several individual fibers to individual subscribers. The APON device in the central office is known as an optical line termination device, or OLT. The system at the customer's premises is an optical network unit (ONU).

Figure 2 highlights a key characteristic of APON technology. Packets transmitted from the OLT to any ONU are broadcast, and the splitter delivers them to all ONUs simultaneously. Addressing information in each packet identifies its intended destination; other ONUs are supposed to ignore the packet. Because APONs use broadcast transmission in this manner, they are a shared media network. Note, however, that the splitter is a one-way device. Packets transmitted by any ONU are delivered only to the OLT; other ONUs do not see these packets.

A. Authentication

APON networks support a primitive form of password-based authentication. The mechanism allows the OLT to query any ONU for its password. The standards explicitly allow the OLT to avoid maintaining a database of ONU passwords. If an OLT does not maintain a password database, it is expected to simply trust the first password it receives from an ONU and use that password for future authentication! The serious security risks inherent in this scheme should be self-evident. Furthermore, even this weak authentication scheme is optional [2, §8.3.5.7], and press reports [3] indicate that not all vendors support it.

B. Encryption

APON networks use a very low grade encryption mechanism known as churning to provide confidentiality for packets broadcast from the OLT. Churning is a simple substitution cipher operating on 4-bit nibbles. The substitution scheme is a non-linear function that uses 8-bit keys; the upper and lower nibbles of each byte use separate keys. The specific plaintext-to-ciphertext mapping does not change until the key is updated. Key updates are supposed to occur at least once every second. However, at APON data rates of 622 Mbit/s, even one second of data provides a significant amount of ciphertext for the cryptanalyst.

Churning is used only on the downstream link, to encrypt packets broadcast by from the central office. We note that, because the downstream link is a broadcast channel, it is easy for a customer to intercept all packets destined for any other customer on the same network; physical layer issues such as clocking and ATM frame synchronization are not a barrier to passive eavesdropping on ciphertext sent via the downstream link. Data sent upstream to the OLT is transmitted in the clear, on the assumption that eavesdropping on a fiber optic link is likely to be difficult due to the physical properties of the medium.

C. Definition of the churning cipher

The ITU standard describes the churning cipher as a mapping from 8-bit plaintexts to 8-bit ciphertexts that operates under the control of a single 24-bit key. We refer to the standard for the official description of the cipher [2].

Instead, we give here an equivalent description as a mapping that transforms a 4-bit plaintext into a 4-bit ciphertext under the control of an 8-bit key $k = \langle k_1, \ldots, k_8 \rangle$. The specific choice of function is not especially relevant to our analysis, but we describe it here to allow others to verify the correctness of our equivalent description. Define a controlled swap function σ given by $\sigma_b(x_0, x_1) = \langle x_b, x_{1-b} \rangle$, and let τ denote the parallel-swap function defined by $\tau_{b,b'}(x, x') = \langle \sigma_b(x), \sigma_{b'}(x') \rangle$. Also, define a bit permutation π by $\pi(x_0, x_1, x_2, x_3) = \langle x_0, x_2, x_1, x_3 \rangle$, and write $x \oplus y$ for the XOR of x and y. Then the churning cipher is given by

$$S_k(x) = \tau_{k_7,k_8}(\pi(\tau_{k_1,k_2}(x)) \oplus \langle k_3, k_4, k_5, k_6 \rangle),$$

which defines a permutation S_k on the set of 4-bit values. Finally, S_k is applied to the 4-bit nibbles of the cipher. The high nibbles use one 8-bit key, and the low nibbles use another 8-bit key.

Note that the key schedule is presented slightly differently here than in the standard[1], but both formulations turn out to be equivalent. In particular, the standard claims to use a 24-bit key, but the designers seem to have overlooked that there are large key equivalence classes, and so the effective key length is at most 16 bits, a fact that follows immediately from our description.

III. Attacks

A. Exhaustive keysearch

Because the nibble-substitution cipher uses only an 8-bit key, it is easy to try all possibilities for the key through exhaustive search. Given some intercepted ciphertext, one can try decrypting this ciphertext under each possible key and looking for a decryption that appears meaningful. It will not be hard to recognize the correct key value: there is likely to be a great deal of known plaintext (for instance, from TCP/IP headers), and at 622 Mbit/s, one second gives plenty of data to work with. By repeating the attack once for the high nibble and then again for the low nibble, we are sure to recover the key after at most 2^9 trial decryptions.

Even when known plaintext is not available, we expect that the decidedly non-uniform statistics of typical network traffic will allow easy recognition of correct guesses at the key value. For instance, one common case is ASCII text, where the high bit of every byte is always zero; as a consequence, if we find a packet containing several dozen consecutive characters each of which decrypt under some guess at the key to bytes with their high bit zero, then we can safely conclude that we have found the right key value.

B. Re-keying

The standard calls for the churning key to be changed once every second. The new key is transmitted in the clear from the ONU (the customer) to the OLT on the non-broadcast upstream link, and thus is not susceptible to easy eavesdropping by other customers. This re-keying was apparently introduced in an attempt to harden the standard. However, these key changes do not provide effective protection against our exhaustive keysearch attacks, because it is easy to repeat the keysearch attack every time the key is changed.

[1] We give a few equations to help in converting between our notation (namely, k) and the notation of the standard (namely, $P1, \ldots, P16, K1, \ldots, K10$). The low nibble uses $k = \langle K1 \oplus P1, K1 \oplus P3, K3, K4, K5, K6, K2 \oplus P2, K2 \oplus P4 \rangle$. Also, the high nibble uses $k = \langle K1 \oplus P5, K1 \oplus P7, K7, K8, K9, K10, K2 \oplus P6, K2 \oplus P8 \rangle$ [2, §8.3.5.6].

C. Other flaws

There are numerous other defects that could be exploited. For instance, the churning key schedule has flaws that could be used to speed up exhaustive keysearch: if k, k' denote the two 8-bit keys used to encipher both nibbles, then the relation $k_3 = k_4 = k_5 = k_6 = k'_3 = k'_4 = k'_5 = k'_6$ holds with probability 1/2, due to the way that these keys are generated in the standard.

As another example of alternative attacks on churning, instead of using exhaustive keysearch, one can easily apply classical techniques for cryptanalysis of simple substitution ciphers [1]. Moreover, the churning function is entirely linear—for any fixed key k, we can write it in the form $S_k(x) = Mx$ for some non-singular 4×4 matrix M over GF(2)—and consequently we can break it using linear algebra given just 4 known input-output pairs $(a_i, S_k(a_i))$ for S_k.

We did not study these alternative attacks in depth: because searching an 8-bit keyspace is so easy, there seemed to be little reason to look for other attacks. However, it seems clear we can conclude that, in short, the churning cipher is robustly weak.

IV. Discussion

A. Countermeasures

Fortunately, there are some partial steps that users of ATM-based passive optical networks can take to alleviate the risk of eavesdropping. A natural countermeasure is to use end-to-end encryption (such as SSL or IPSec) or a Virtual Private Network (VPN) to protect the content from eavesdropping. The major drawback of this approach is that deploying encryption at every endpoint has significant administrative costs. For this reason, a better solution may be to seek an improved link-layer encryption scheme to replace churning.

B. Lessons

The attacks in this paper serve to demonstrate a fact that has been well-known in the cryptography community: the design of secure cryptographic algorithms is very difficult, requires special expertise beyond that acquired in designing network protocols, and should not be attempted without considerable experience in the subject.

It is tempting to design one's own encryption algorithm, optimized specially for the particular setting of ATM-based passive optical networks. However, such a strategy is fraught with peril. Historically, the field is strewn with the debris of self-designed ciphers that have been found to be seriously broken, and the APON churning scheme is merely one more unfortunate example of this risk.

Designing secure encryption algorithms is very challenging, especially when under strict performance constraints (as was apparently the case with the APON standards). Even the most experienced of security professionals can make serious errors. Due to this risk, the accepted practice is to rely on the collective expertise of others to design suitable cryptographic primitives. Two important ways to do this are to reuse past designs and to offer new designs for public reviews.

Past encryption algorithms should be reused whenever possible. A common tenet of cipher design is "Don't do it." General-purpose ciphers such as 3DES and AES have been thoroughly studied in the cryptographic literature, allowing us to gain significant confidence in their security. If past designs are inadequate, it seems sensible to seek the assistance of the cryptographic research community in identifying better solutions. One way to begin this process is to articulate the design requirements and challenge cryptographers to find a satisfactory design. We believe that there is a strong opportunity for productive interactions between the optical networking and cryptographic communities, and we hope that this direction will be explored further in the future.

In any case, no matter how one arrives at an encryption algorithm, public review is also of great importance: open review is a last resort for finding vulnerabilities before they can cause harm. In the case of the APON churning design, we feel confident that public review by the cryptographic community would have made a big difference. We believe that the flaws of the churning cipher are so strikingly self-evident to one trained in cryptanalysis that if the churning cipher had been examined by the cryptographic community before it was enacted into an international standard, its flaws would have been quickly identified in time to avoid its inclusion in the standard. While we applaud the fact that the APON standard is open, this alone is not always sufficient: in the future, it would appear to be prudent for any working group developing a new encryption algorithm to proactively invite the security community to analyze it.

V. Conclusion

The security mechanisms in the APON standard are trivial to defeat, and should not be relied upon. Consequently, we recommend that APON should not be counted on to provide strong link-level security, and that additional precautions be taken to protect network traffic. We hope that our discoveries will motivate a redesign of the APON churning cipher to address the vulnerabilities that we found. We also hope that this paper will expose important security principles and design practices to a wide audience, and that the lessons we identify will benefit future designers of both APON and other communications security systems.

References

[1] H.F. Gaines, *Cryptanalysis: a study of ciphers and their solution*, Dover Publications, Inc., New York, 1956.

[2] ITU Recommendation G.983.1E, "Broadband Optical Access Systems Based on Passive Optical Networks (PON)," October 1998.

[3] R. Kirby, "Passive Optical Networking Brings DSL to the Masses," *Network Magazine*, 5 November 2000.

[4] C. Wilson, "A Market Downturn Turns Into a Rout," *The Net Economy*, 2 July 2001.