

광통신시스템의 취약성 : 광신호 탭핑의 역할

UMOH, GABRIEL ETIM
전기/전자/ICT 엔지니어링 대학
엔지니어링 학과, 아크와 이봄 주립 대학
IKOT AKPADEN, MKPAT ENIN LGA
아크와이봄 주, 나리지리아
E-mails: gabriel.umoh5@gmail.com

AKPAN, ANIEFIOK OTU
물리학 대학
자연 과학 및 응용 과학 학과,
아크와 이봄 주립 대학
IKOT AKPADEN, MKPAT ENIN, L.G.A.
아크와이봄 주, 나리지리아
E-mails: aniefiokotu@gmail.com

초록

오늘날 공공 및 사설의 광 네트워크에 설치된 광 탭핑 장치는 모든 광섬유 세그먼트를 통해 전송되는 모든 통신 및 정보에 제한 없는 접근을 허용하게 한다. 전 세계적으로 수 많은 제조사가 법적으로 문제 없이 그리고 저렴하게 광섬유 탭을 공급하고 있으므로, 이것은 매일 매일 사용되고 있는 표준적인 네트워크 유지 장비이다. 광신호 탭이 불법적으로 사용되게 되면 이것은 실제로 탐지될 가능성이 없이 음성 및 데이터 통신을 가로챌 수 있는 탁월한 방법을 제공하게 된다. 그러므로 침입자는 잡힐 수 있는 위험이 거의 없이, 보상금이나 혹은 관련 정보라는 보상을 받게 될 것이다. 광 네트워크 장비 제조사는 현재 그러한 네트워크 침해를 실시간으로 감시하기 위해서 그들의 플랫폼에 적절한 예방 및 탐지 기술을 통합하고 있지 않다. 그래서 네트워크 운용사는 그들의 네트워크 상에 있는 광 신호를 보호할 수 없고, 그러므로 민감한 데이터 및 통신의 유출을 방지할 수 없다. 한편, 정부 네트워크는 분명히 더 안전하지만, 더 발전된 수동 및 능동 탭핑 방법 중 어떤 유형에는 여전히 취약하다. 이 배경 논문은 오늘날의 현대적 광 네트워크의 취약성에 대해 전반적인 개요를 제공하고; 그러한 문제를 다루는 방법을 설명하고; 그리고 광 보안, 감시, 침입 탐지 및 침해 위치 발견 솔루션을 소개한다.

검색어 : 광섬유, 광신호 탭핑, 스플리터, 커플러, 광펄스시행기(Optical Time Domain Reflector: OTDR), 오이스터 오픈스.

1.0 서론

광통신 시스템은 모든 현대의 통신 네트워크의 중추를 구성하고 있다. 음성, 데이터, 동영상, 팩스, 무선, 이메일, TV 혹은 다른 것이던 간에, 1억 8천만 마일의 광케이블이 계속 증가하는

다양한 정보 및 통신의 대부분을 전 세계적으로 전송하고 있다. 현대의 경제 및 사회가 정상적으로 그리고 효율적으로 기능하기 위해서는 중요한 광네트워크 기반 시설이 가용한지, 이것에 대한 기밀성이 유지되는지, 그리고 이것이 완전한지에 달려 있다.

광통신 시스템에 대한 최초의 소개는 광섬유 기반의 전송은 본질적으로 안전하다는 믿음과 함께 이루어졌다. 그 이후로 광섬유 시스템은 구리 기반의 통신 시스템 보다 더 탭핑하기 간단하다는 것이 증명되었다. 더욱이 탭핑된 광 네트워크는 훨씬 더 많은 관련 정보를 더욱 더 정돈되고 디지털화된 방식으로 누설하게 된다. 사실 많은 광섬유 탭은 전 세계의 통신 운용사에 의해서 매일 사용되고 있는 표준적인 네트워크 정비 장비이다. 하지만 이 장비들이 불법적으로 사용되게 되면, 이 장비들은 거의 탐지될 가능성이 없거나 전혀 탐지될 가능성 없이 광섬유 플랜트에 있는 모든 음성 및 데이터 통신의 유출을 가능하게 한다.

2.0 방법론

케이블 속에 있는 빛이 전송되는 신호 속에 있는 모든 정보를 담고 있고, 시장에 있는 보통의 탭핑 장비로 그 빛을 쉽게 포획할 수 있고, 해석할 수 있고, 조정할 수 있기 때문에 이것이 이루어질 수 있다. 오늘날 사설 및 공공 네트워크는 광신호 탭을 탐지하기 위한 방법을 포함하고 있지 않고 있기 때문에 침입자가 비교적 안전한 데이터 추출 계획을 세울 수 있게 한다. 광통신 시스템은 광섬유 속에서 대량의 데이터를 빛으로 전송하기 때문에, 그러한 방법은 정보를 수집하는 위험이 낮은 방법으로 선호되고 대량의 정보에 대한 접근을 가능하게 한다. 도청 및 스파이 행위의 관점에서 보면, 그것의 이점은 명확하다.

오늘날 우리는 회사 스파이 행위가 국제적인 스포츠가 되어 버린 사회에 살고 있다. 광섬유를 이용한 통신이 점점 더 어디에나 존재하는 것이 되었기 때문에, 불법적인 비밀 정보 및 상업적으로 민감한 데이터의 탭핑과 도둑질도 또한 어디에서나 벌어지는 것이 되었다. 미국 회사에만 국한하더라도, 2000년에 순수하게 기술적인 수단으로 2백억 달러의 손실이 있는 반면에 회사 스파이 행위에 의해 천억 달러가 넘는 금액의 손실이 있었다고 추정이 된다. 국제적으로 100 개가 넘는 외국의 정부 기관들이 회사들에 대한 민감한 정보를 정기적으로 획득하여 그들의 국내 회사에 제공하고 있다. 사실 가장 최근의 **미 연방 정보국 및 컴퓨터 보안 기관**의 “2002 컴퓨터 범죄 및 보안 조사”에서 주요한 미국 회사들 및 기관들은 그들에 대한 가장 가능성 있는 공격 소스는 미국의 경쟁사, 외국의 회사 및 외국 정부들이 일으키는 결합된 스파이 행위라고 언급하였다. 독립적인 해커들 및 불만이 많은 종업원들은 반드시 적절하게 관리되어야만 하는 상시적인 위협이지만 스파이 행위의 결합된 위협에 이어서 두 번째와 세 번째의 순위가 되었다. 최근의 사례로는 프랑스가 영국 무선 네트워크를 탭핑하여 경쟁 입찰 상황에 있는 임원들의 대화를 도청한 것; 대한 범죄자들에 의해 네덜란드 경찰 네트워크에 설치된 탭 ; 이전의 동독 비밀 경찰 (STASI)에 의해 서 베를린과 서독 사이의 광 링크에 설치된 광신호 탭 ; 그리고 심지어는 보스턴에 있는 주요한 금융 기관 한 곳의 광케이블에 대한 최근의 탭핑 등이 있다.

특히, 문제가 심각한 것은 광신호 탭의 대다수가 완전히 탐지되지 않은 채 지속되고 있고, 오늘날 대부분의 기업들이 그들의 광 네트워크에 있는 데이터를 감시하고, 탐지하고 보호하기 위한 적절한 기술들을 채용하고 있지 있다는 점이다. 분명히 그러한 환경에서는, 현대 사회에서 모든 통신과 데이터 전송의 생명소인 광네트워크는 진정한 공격 목표가 된다

전통적으로 시스템에 대한 불법적인 침입은 통신 시스템에 대한 탭핑을 통해서이거나 혹은 무선 전송을 가로채는 것을 통해서 이루어졌다. 하지만 최근 수 년간에는 일반 대중들은 컴퓨터 해킹에 훨씬 더 초점을 맞추고 있다. 해커들은 다른 목표를 가지고 있고 그들의 침입 성공 업적에 대해 대중들이 잘 알아주기를 원하는 경향이 있다. '서비스 거부' 공격 혹은 "아이 러브 유" 바이러스와 같은 그러한 주의를 끌려고 하는 공격은 많은 미디어의 주의를 끌게 된다. 그것들이 희생자에 대하여 금전적으로 어떤 간접적인 영향을 끼치지 않는 반면에, 그것들은 오랜 기간 동안 유지될 수 있고 시설들, 건물, 캠퍼스 혹은 어느 특정 지역 간에 전송되고 수신되는 모든 회사의 정보 및 통신에 대해 접근할 수 있게 하는 장기간의 형태의 탐지되지 않는 광섬유 탭에서 발생하는 대량의 손실에 비교해 보면 점점 미약해 진다.

비교해 보면, 전문가들은 탐지되거나 혹은 붙잡히지 않는 목표를 가지고 특정한 재무적인 혹은 정치적인 이득을 위해 가능한 한 오랫동안 가능한 한 많은 정보를 빼 내기를 원하기 때문에 매우 다른 작업 방식을 가지고 있다. 그들의 불법적인 정보 수집 도구의 참고에서 광섬유 탭은 아주 유용한 방법을 제공한다.

그 결과, 대중의 믿음과는 반대로, 광통신시스템은 탭핑에 극도로 취약하고, 그들의 네트워크가 '탭 프리' 혹은 광 탭핑 방법으로부터 심지어 최소한으로라도 방지 수단을 가지고 있다고 주장할 수 있는 사실 네트워크 운용사 혹은 공공 네트워크 운용사는 거의 없다.

3.0 광통신

광섬유는 빛을 제한하는 데 사용되는 유전체 도파 장치이다. 이러한 케이블은 전형적으로 피복에 둘러 쌓인 실리카 글라스 코어로 제작되고, 이것은 그 다음에 외피에 의해 보호된다. 피복은 전형적으로 또한 실리카 글라스로 제작되지만, 어떤 용도에는 플라스틱이나 혹은 "도핑된" 실리카를 활용한다. 그 소재에 관계 없이, 내부의 굴절과 광섬유를 통한 빛의 전파를 위해 피복의 굴절률은 스넬의 법칙을 충족시키기 위해서 반드시 중심부 보다 낮아야 한다. 외피의 기본적인 기능은 광섬유가 손상되지 않도록 보호하는 것이다.

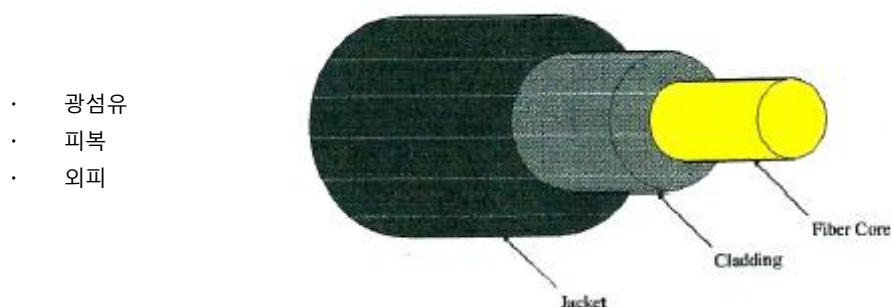


그림 1 : 광섬유에 대한 표준적인 단면 형상

광섬유를 이용하는 통신은 다른 통신 시스템에 비해 여러 가지의 매력적인 특징 및 장점을 가지고 있다. 이러한 장점으로서는 다음과 같다:

- 더 넓은 대역폭 및 용량

- 전기적인 격리
- 낮은 에러율
- 외부의 영향에 대한 더 큰 면역력
- 간섭 및 크로스워크에 대한 더 큰 면역력

광통신시스템은 그들의 높은 대역폭으로 인하여 예를 들면 초기에 하나의 광케이블에 대하여 일천 개의 구리 와이어의 비율로 교체할 수 있게 하기 때문에, 통신 시스템에서 점점 더 많이 전개되고 있다. DWDM에 있어서의 발전은 추가적인 파장 및 채널을 통해서 그 비율을 지속적으로 더욱 더 향상시킬 수 있게 하고 있다.

그러한 인기 있는 특성을 가지고 있기 때문에 광섬유가 통신 시스템을 통해 정보를 전송하는 수단 중에서 가장 활용할 수 있고 효율적인 수단이 되는 것이 전혀 놀라운 일이 아닐 것이다.

전체적인 대역폭이 증가된 용량을 가지게 되고 성장하기 때문에 무선 네트워크, 인터넷, 회사의 광역 네트워크, 데이터 저장 공간 네트워크 등과 같은 다른 통신 매체가 굉장히 많이 발전할 수 있게 되었다. 이 모든 것들은 모두 광섬유 코어를 사용하고 있다. 그래서 광섬유 기반 통신 시스템은 실제로 중심부에서 모든 이전의 통신 시스템의 유형을 교체해 왔다. 그리고 그것이 계속 네트워크의 가장자리로 확장하고 있기 때문에 광섬유가 거의 모든 데스크 톱 컴퓨터 및 대부분의 가정에 도달하는 것은 진짜로 단지 시간 문제일 것이다. 모든 광 스위치에 있어서의 더 이상의 발전 및 심지어는 광 프로세서 및 버스에 있어서의 초기 개발도 모든 광학적인 육상 네트워크 기반 시설에 대한 미래의 풍부함을 약속하고 있다.

4.0 광통신시스템의 취약성

현대의 광네트워크는 전 세계적으로 1억 8천만 마일에 걸쳐서 광섬유를 전개하고 있다. 이 네트워크는 대량의 데이터 및 정보가 한 지점에서 다른 지점으로 저렴하게 그리고 쉽게 전송되게 하고, 극도로 중요하고 기밀적인 정보를 전송하고 있다. 비록 처음에는 이 광섬유 시스템이 본질적으로 안전하다고 생각되었지만, 광섬유로부터 정보를 빼 내는 것이 비교적 간단하고, 표준적인 시험 및 정비 장비가 점점 더 정교해지고 사용 가능해짐으로써 도움을 받게 되었다.

광섬유 탭핑 방법에는 여러 가지가 있다. 하지만 대부분의 방법들은 아래의 주요한 범주에 속하게 된다:

- 스플라이스
- 스플리터 혹은 커플러 (가변적)
- 비 접촉 방법 (수동 및 능동)

4.01 스플라이스 :

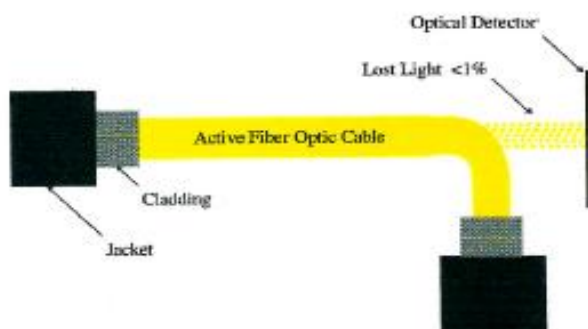
탭핑에 대한 가장 간단한 방법은 광섬유를 간단히 합쳐 이어서 장비를 삽입하여 신호가 최종의 사용자에게 전송이 되게 하면서, 한편으로는 침입자가 가로챌 수 있게 하는 것이다. 광학적인 스플라이스는 광섬유가 운영되지 않는 동안에 순간적인 데이터의 소실을 초래한다. 하지만 망 운용사는 광섬유 파손의 위치를 실시간으로 파악할 수 있는 능력을 가지고 있지 않아서, 그렇게 되면 보통은 트럭과 기술자들을 보내서 추가적인 외부 장비를 삽입해야 한다.

그러므로 만약 중단 시간이 짧으면, 많은 망 운용사는 그 장애가 네트워크의 작은 고장 때문이라고 생각하고 데이터의 전송을 계속하게 하고 탭이 설치된 것을 인식하지 못한다. 하지만 오늘날 대부분의 시장에 나와 있는 탭핑 장비들은 신호를 가로채지 못하고, 그래서 스플라이싱 방법은 선호되지 않는다.

4.02 스플리터 및 커플러 (가변적) :

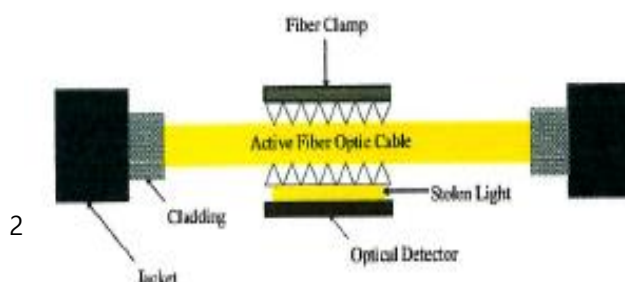
그러한 방법은 실제적으로 광섬유를 파손하거나 혹은 데이터 흐름을 중단 시키지 않고 하나의 광섬유에 대한 탭핑을 가능하게 한다. 광섬유에 대한 덜 알려진 특성 중 하나는, 특히 그 광섬유가 마이크로 밴드 혹은 리플이 그 표면에 형성되는 방식으로 굽혀 지거나 집게로 잡을 경우에, 광섬유의 외피 및 피복 두 가지 모두로부터 빛이 쉽게 손실될 수 있다는 것이다. 아마도 그러한 현상에 대한 가장 단순한 사례는 만약 한 사람이 그 손에 광섬유를 들고 있으면 그 사람이 하나의 광섬유 안에서 빛을 볼 수 있는 것이다. 단순히 한 사람이 그 빛을 보는 것과 같은 식으로 (사람의 눈은 결국 생물학적인 광학 탐지기이기 때문에), 그 장비는 그것을 해석할 수 있게 설계된다. 실제로는 광섬유를 통해서 이동하는 모든 정보를 빼 내기 위해서 요구되는 모든 것은 길이 방향으로 어떤 지점에서 그 광섬유에 약간의 굽힘을 주거나 그것에 클램핑을 하는 것이다. 그러면 빛의 광자는 침입자의 수신기로 누출되어 들어간다.

- Optical Detector : 광 탐지기
- Loss light : 손실된 빛 < 1%
- Active Fiber Optic Cable : 통신중인 광케이블
- Cladding : 클래드(빛차단 층)
- Jacket : 피복



(a)

- Fiber Clamp : 광섬유 클램프
- Active Fiber Optic Cable : 통신중인 광케이블
- Cladding : 클래드(빛차단 층)
- Jacket : 피복
- Stolen Light : 새어나온 빛



(b)

그림 2 : 광섬유로부터 빛이 새어나오는 두가지의 간단한 탭 방법

사실 많은 광시험 기기들은 이러한 사실을 이용할 수 있도록 특별하게 설계되어 있다. 예를 들면, 아래는 보통 사용할 수 있는 광섬유 식별기이다. 이것은 외피를 제거할 필요 없이 하나의 광 신호의 방향을 측정하기 위해 사용된다. 기타 수동형으로는, 비침입성 탭핑 장치들이 있다..



3(a)



3(b)



3(c)



3(d)

그림 3(a-d) : 신호 방향을 측정하기 위하여 상업적으로 구할 수 있는 광 신호 탭핑 장치 3(a), 분극화를 유지하는 가변 비율 에바네센트 웨이브 커플러 3(b), 마이크로 벤드 클램핑 탭핑 장치 3(c), 그리고 매크로 벤드 탭핑 장치 3(d).

기본적인 탭에 대해서는 신호의 존재 및 방향을 식별하기 위해서는 오직 0.2 dB의 광학적

세기가 필요하다. 그래서 전체적인 광 신호를 수집하기 위해서 더 민감한 광 탐지기와 추가적인 전자 기술을 활용하는 것은 꽤 단순하다. 일단 이것이 달성되면, 하나의 광네트워크 분석기는 수많은 회사에서 제조되는 일반적으로 구할 수 있는 시험 기기이고, 이것을 사용하여 통신 프로토콜을 판단하고 정보를 해석할 수 있다.

심지어는 단지 0.1 dB (~2%) 미만의 신호가 누출되는 경우에도 그것은 여전히 각 광자에 의해 전송되는 모든 정보를 담고 있게 될 것이다. 반대 편에 있는 사용자는 그들의 통신에 대해 명확하지 않은 간섭만을 경험할 것이기 때문에 그들의 정보가 위태롭게 되는 것을 절대 알지 못할 것이다.

4.03 네트워크 붕괴 :

사실 어떤 탭핑 장치는 단지 수동적 탭핑만을 위해서 활용된 것은 아니고 능동적 탭핑을 위해서 활용될 수 있다. 능동적 탭핑에서는 정당한 정비, 혹은 심지어는 위험한 네트워크 붕괴 및 공격과 같은 다양한 용도를 위해서 신호가 광섬유 플랜트로 주입되는 현상이 발생한다. 그러한 기술은 잘못된 정보를 소개하기 위해서나 혹은 기존의 정보 흐름을 훼손하기 위해서 사용될 수도 있다. 그러한 능력은 회사 스파이 행위의 허위 정보에서부터 중요한 통신 기반 시설에 대한 테러리스트의 파괴 행위까지 광범위한 악용을 가능하게 한다. 광 케이블을 절단하는 것과 같은 네트워크 기반 시설에 대한 노골적인 물리적 공격과 다르게, 오늘날의 네트워크에서 파괴의 목적으로 사용되는 광학적 탭은 그 성격에서 민감하고 실시간으로는 탐지될 수 없으며 그 위치를 발견하기가 어렵고 기반 시설의 완전성과 유효성에 대한 혼란을 가져오게 한다.

4.04 비 접촉 방법 (수동 및 능동) :

실질적으로 광섬유에 접촉할 필요 없이 광섬유를 탭핑하거나 혹은 광섬유 플랜트에서 빛을 "훔치는" 수 많은 방법이 있다. 어떤 방법들은 십 년 이상 동안 주위에 있었지만 최근에야 공공의 영역에서 발표가 되었고, 현재는 전 세계적으로 인터넷 연결에 접근할 수 있는 어떤 사람에 의해서나 접근될 수 있다. 도이치 텔레콤에 발행된 최근의 한 미국 특허 (6,265,710) 및 유럽 특허 (0 915 356)에서는 "어떠한 탐지 가능한 간섭의 발생 없이, 특히 유리 섬유를 통해 전파되는 신호가 어떠한 전송 손실도 경험하지 않게, 유리 섬유로부터 신호를 빼 내는 방법 혹은 장치...", 에 대해 상세하게 설명하고 있다.

- 이 특정한 실행 사례가 최대 비트 전송률에 있어서 제한이 있지만, 다른 덜 알려진 방법도 또한 존재한다. 이것은 훨씬 더 높은 비트 전송률의 광신호 탭을 가능하게 한다. 더욱 더 주목할 만한 것은 비록 현재는 그러한 탐지가 안 되는 광신호 탭을 위해서 시장에서 구할 수 있는 기존 장비를 구입할 수가 없을지라도, 그 특허 서류는 선호되는 방법과 어떻게 그러한 장치가 제작되고 작동되는지를 명확하게 설명하고 있다.

더 발전된 비 접촉식 능동 탭은 그 반대로 추가적인 빛을 광섬유 플랜트에 주입하고, 그 둘 사이의 어떠한 상호 작용을 측정함으로써 기본적인 광 신호를 도출할 수가 있다. 그러한 비 접촉식 탭은 기본적으로 탐지될 수가 없고, 그래서 적절한 물리적 층으로 된 광 신호 보호가 적용되지 않으면, 데이터는 네트워크 운용사 혹은 최종 사용자가 알아 채지 못한 상태에서 무한대로 가로채 질 수 있다.



그림 3(e) 실험실 설정에서 네트워크 파괴 혹은 시각적으로 볼 수 있는 신호의 저하 없이 10 킬로미터 간격에 걸친 실시간 화상 회의에 대한 탭핑의 사례. 두 개의 랩톱 사이에서 가로채진 화상 회의가 세 번째 랩톱에서 실시간으로 재생됨

5.0 정부 대 상업 네트워크

그들을 가능하게 하는 상업적 광네트워크 및 장비는 광 탭핑 방법에 대한 종합적인 보호 메커니즘을 통합하고 있지 않다. 상업적인 네트워크에 광신호 탭을 활용하는 침입자들은 그들이 그들의 불법적인 행위를 통해 망 운용사 혹은 망 운용사의 법인 고객에 의해 적발될 확률이 거의 없거나 전혀 없이 풍부한 량의 목표하는 정보를 잘 정렬되고 디지털화된 형식으로 얻을 수 있다는 것을 알고 그렇게 하고 있다.

하지만 정부 네트워크는 일반적으로 탭핑 방법에 대항해서 더 단단한 보호 장치를 통합하고 있다. 그러한 노력은 네트워크의 유형, 전송되는 데이터의 중요도 및 그 적용의 특성에 따라 달라진다. 예를 들면, 많은 정부 네트워크는 전송하는 많은 정보나 혹은 전송하는 모든 정보를 신중하게 암호화한다. 이와 같이, 어떤 정부 네트워크는 가능한 탭핑 행위에 대한 광섬유 건강 지표에 있어서의 가능한 변화를 찾기 위해서 매일 임의로 광학 시간 도메인 반사율계 ("OTDR") 스캔을 사용할 것이다. 그러한 경우에는 비 접촉식 수동 및 능동 탭핑 방법을 이용하면 정부 네트워크는 여전히 도청, 스파이 행위 및 파괴에 취약하게 만들게 된다. 비용이 중요한 문제가 아닌 극단적인 상황에서는 강화 콘크리트 도관 혹은 가스가 채워진 패키징과 같은 더 강렬한 수단이 또한 사용될 수도 있다.

모든 경우에 정부 네트워크는 광 탭핑 방법에 대항하여 보호하려고 노력하고 있다는 것을 알아야 한다. 그렇지 않으면 그러한 보호 수단을 먼저 채택하는 이유가 없을 것이다.

6.0 정보의 보호

위에서 언급한 증거에 근거해서 보면, 통신 산업계에서 널리 구할 수 있는 비교적 저렴한 광전자 부품을 사용함으로써 광섬유를 탭핑에 대한 효과적인 탐지기를 설치할 수 있고 혹은 미리 조립된 것을 쉽게 구매할 수 있다는 결론을 내는 것은 쉽다. 이것은 광통신시스템을 사용하는

사람들, 특히 연구 및 개발 시설, 글로벌 제조사, 정부 기관 및 다른 기관뿐만 아니라 금융 기관, 거래소, 보험 회사 및 건강 관리 회사와 같은 민감한 데이터를 가진 사람들에게 대해서는 심각한 보안에 대한 함축적인 의미를 가지게 된다.

전형적으로 민감한 정보는 군대 및 외무부와 같은 매우 높은 보안 조직의 영역에 있는 것으로 믿어진다. 하지만 경쟁이 심한 글로벌 시장에서는 상업적인 조직이 그들의 생존에 핵심적인 통신 및 정보를 보유하고 교환하고 있다. 이러한 데이터 중 많은 것은 엄격한 비밀 하에 그들의 고객, 파트너 혹은 글로벌 자회사와 교환되고 있거나 혹은 그들에게 공급되고 있다. 그러한 조직은 몇 개만 예를 들자면 회계 회사, 연구 및 개발 조직, 정부 규제 기관 및 보험 회사 등을 포함하고 있다.

모든 공공 및 사설 네트워크 운용사 및 그들 각각의 고객들은 그들의 임무에 중요한 통신 및 정보의 탭핑 및 도난에 완전히 취약하게 되어있다. 크게는 공급자, 운용사 및 사용자가 그 심각한 위협을 이해하지 못하였기 때문에, 그리고 최근까지 그러한 사건의 발생에 대응하기 위해 사용할 수 있는 효과적인 해결책이 없었기 때문에, 전 세계적인 광학 통신 기반 시설에 대한 기본적인 취약성은 지금까지 공개적으로 거론되지 않아 왔다. 더욱이 공급자 및 운용사는 광 보안 기술을 아직까지 통합하지 않았고, 그래서 탭핑 사고는 거의 탐지되지 않는다. 그리고 브랜드 보호 및 위험 경감이라는 명백한 이유 때문에 절대 공개되지 않았다. 오늘날의 대중은 전형적인 광섬유는 통신을 위한 안전한 수단이라는 잘못된 생각을 가지고 있다. 이것은 간단하게 말하면 잘못된 생각이다.

광 네트워크는 특히 국선 및 접근 루프에서 그리고 공공 영역 혹은 약점의 선택 지점에 있는 광섬유에 침입자가 접근할 수 있는 큰 기회를 가질 수 있는 어느 곳에서건 취약하다 예를 들면, 광케이블에 대한 접근은 전형적으로 국선 광섬유 루프에서 고객 사유지와 첫 번째 스위칭 센터 사이뿐만 아니라 고객의 사유지에서 그리고 그 주변에서 많이 발생한다. 만약 첫 번째 스위칭 센터 이전에서 접근 되면, 모든 음성 및 데이터 통신의 100%가 고객 혹은 망 운용사가 모르는 사이에 전형적으로 가로채지고 빼 내어질 수 있다. 광 탭핑을 위해 요구되는 장비는 또한 국선 및 접근 루프에서 덜 비싸고 덜 복잡하다. 이 부분에서는 속도와 망 접속 형태를 관리하기가 더 쉽다.

대도시 및 금융 센터에서 고층 빌딩과 같은 여러 층으로 된 건물 및 여러 세입자가 있는 건물에서는 사용자가 인접하지 않은 여러 층을 사용하고 있는 경우가 종종 있는데, 이런 곳에 있는 시스템에 대한 광 네트워크의 취약성은 특히 확대된다. 통신 시설에 연결된 광 케이블은 전형적으로 수직관이나 혹은 승강기 통을 통해 전개되는데, 그곳에는 기존의 감시 혹은 보안 장치가 설치되어 있지 않다. 조직들은 그냥 그들의 정보 및 통신이 그렇게 쉽게 접근할 수 있는 공용 지역에 쉽게 설치될 수 있는 탭을 통해서 빼 내질 수 있다는 것을 깨닫지 못하고 있다.

전화 클로짓, 케이지, 도관, 수직관, 샤프트, 주차장, 맨홀, 지하철, 전신주 및 많은 다른 모든 부분에는 광섬유 탭을 설치하기 위해 접근할 수 있다. 회사들이 더 경쟁적이 되고 덜 친숙한 외국에 진출하면서, 더 광범위한 세계화를 향한 트렌드는 단지 문제를 추가하기만 한다.

7.0 해결책

사전 예방과 사후 대응: 오늘날의 대부분의 보안 수단은 특성상 사후 대응적인 것이다. 즉,

그것들은 암호화 같은 수단을 통해서 네트워크에 침입하려고 하는 침입자의 행위를 늦추게 하거나 방해하기 위한 것이다. 그러한 사후 대응적인 기술로 많은 침입자를 저지하는데 성공할 수 있을지 모르지만, 그러한 방법으로 모든 침입자를 저지하지 못할 뿐만 아니라 침입자의 실질적인 정보 빼내기를 허용하지도 않는다. 그래서 침입자들은 잡히지 않고 미래에 다시 그러한 시도를 하는 것을 멈추게 할 수도 없다.

하지만 사전 예방적인 보안 수단은 침입 사건에 대한 즉각적인 판단을 가능하게 하고 실시간으로 광섬유 플랜트에서의 침입자의 정확한 위치를 파악할 수 있게 할 수 있다. 그러므로 사법 당국 및 국토 안보국은 침입 시도가 벌어지는 중에 침입자를 탐지하고 그 위치를 파악할 수 있는 효과적인 도구를 가지게 되고, 또한 범인이 미래에 네트워크 공격을 하는 것을 멈추게 할 수 있다. 그러므로 전체적인 광섬유 운용사의 신호가 요청되는 것을 방지할 뿐만 아니라 또한 침입자의 가로채기를 허용하는 사전 예방적인 그리고 사후 대응적인 보안 방법의 종합적인 조합이 아주 바람직하다.

오이스터 옵틱 주식회사는 현재의 글로벌한 광 네트워크를 위한 획기적인 광 보안, 감시, 침입 탐지 및 침입 위치 파악 솔루션을 개발하고 그것에 대해 특허를 받았다. 그 회사의 기술은 암호 없는 (하지만 암호 호환이 되는), 프로토콜에 독립적인 것이고, 이미 존재하는 광 기반 시설에 대해 가장 높은 수준의 보안을 제공한다. 물리적인 전송 층이 완전히 보안되어 있기 때문에 모든 높은 수준의 네트워킹 층 및 데이터 유형들도 또한 보호가 된다. 오이스터 옵틱은 그들의 기술을 통신 장비 공급사들 및 방위 산업체들이 공공 및 사설 네트워크에 설치할 수 있게 라이선스 하고 있다. 극도로 안전한 정부의 적용처 및 네트워크를 위한 특별 구성도 가능하다. 오이스터 옵틱은 또한 고객 맞춤형 디자인, 엔지니어링 및 지원 서비스를 제공하고 있다.

모든 종류의 회사 스파이 행위는 광네트워크의 탭핑이 침입자가 모든 회사의 음성 및 데이터 통신을 어떤 시간이라도 접근할 수 있게 하면서 증가하는 추세에 있다. 오프 사이트 코로케이션, 호스팅, 백업, 재앙 복구 및 SAN 시설은 이러한 경향을 가중시키고, 보안 유지가 되지 않고 개방된 공공 도메인을 통해서 오프 프레미스 네트워크 와인딩의 안전으로부터의 침입자가 회사의 중요한 정보에 접근하는 기회를 훨씬 더 많이 주게 된다. 오늘날의 일반적인 보안 기술은 간단하게 말하면 물리적 전송 층을 잠그지도 못하고 광 네트워크에 걸쳐서 적절한 보안도 제공하지 못한다.

통신망 운용사 및 정부 네트워크를 위한 광학 장비에 통합된 오이스터 옵틱의 기술은 현재 사용할 수 있는 가장 강력한 네트워크 보안을 제공한다. 그렇게 함으로써 광 탭핑 기술을 활용하는 적대적 혹은 원치 않는 침입자가 모든 데이터, 음성, 비디오, 영상 및 다른 정보를 절대 복구할 수 없게 한다. 침입 탐지 및 침입 위치 파악 기술은 광섬유 플랜트에 대한 침입과 정비 실시 건을 실시간으로 감시하고, 그렇게 함으로써 특정 자원의 파견이 이루어질 수 있게 한다. 글로벌 표준 1000 회사들, 금융 기관들, 연구 및 개발 시설 및 정부 기관들은 지리적으로 떨어진 그들의 시설을 서로 같이 연결할 때, 그러한 것을 보장할 수 있는 방법을 찾아야 한다. 이러한 것에 대해 조치를 부족하게 하면, 침입자들이 잘 알려진 네트워크의 취약점을 이용할 수 있게 공개적으로 문을 열어주는 것과 같다.

오이스터 옵틱의 기술은 광 음성 및 데이터를 기존의 광네트워크를 통해 안전하게 전송될 수

있게 한다. 광 캐리어 위에 있는 데이터에 표식을 찍기 위해서 특허 받은 광 신호의 보안 페이지 모듈레이션의 방법을 사용함으로써, 데이터는 오직 전원 가동 시에 전송된 것과 동기화된 특별한 오이스터 옵틱의 수신기에 의해서만 복구될 수 있다. 각 오이스터 옵틱의 활성화된 송신기 및 수신기는 논쇄도 랜덤 제조 과정을 통해서 진짜로 독특하다. 그래서 그것은 복제가 불가능하다. 그래서 광 패킷을 탭핑하는 전통적인 방법 및 암호화된 데이터를 해독하는 전통적인 방법은 오이스터 옵틱 기술로 보호된 광섬유를 탭핑하는 시도에서는 소용이 없다. 추가적으로, 오이스터 옵틱의 특허 받은 보안 페이지 모듈레이션 기술을 이용하여 전송된 광 신호의 본질적 특성으로 인하여, 오이스터로 보호된 광섬유에 대한 탭핑 시도 및 광섬유 플랜트에 대한 탭 설치 시도는 매우 민감한 침입 감지 기술을 통해 즉각적으로 네트워크 운용사에게 발각된다. 그래서 광 신호는 도청 시도로부터 완벽하게 안전하고, 또한 보증한 바와 같이 자동적으로 또 다른 안전한 오이스터로 보호된 광섬유 경로로 다시 보내어 진다.

오이스터 옵틱의 특허 받은 전송 방법은 광 보안, 침입 감지 및 정비의 분야에 있어서 새로운 진보를 가능하게 한다. 네 가지의 기본적인 방법이 같이 결합되면, 이것은 광네트워크에 대한 모든 광 탭핑 기술에 대응하는 비할 데 없는 수준의 보안을 제공할 수 있다:

1. **물리 층 보안** : 데이터가 실제로 복구될 수 없게 하고 판독될 수 없게 하는 완벽하게 안전한 광섬유 전송 층 (0, 1)
2. **침입 탐지** : 미세하게 조정할 수 있는 임계치를 가진 다양한 침입 및 정비 실시 건에 대한 매우 민감한 감시는 네트워크 침입 시도에 대한 즉각적인 경보를 가능하게 한다.
3. **침입 위치 파악** : 실시간으로 광섬유를 따라 그러한 사건의 정확한 위치를 계산. 사전 예방적인 통합적 수단에 의해서 범인에 대한 법 집행 실시가 이제 처음으로 가능하다. 정비 및 수리 행위는 또한 더욱 더 목표를 겨냥하게 되고 효과적이다.
4. **출력물 최적화** : 소프트웨어 관리를 통해서 전체적으로 광섬유 플랜트에서 사용할 수 있는 빛을 정확한 광섬유 경간 길이로 제한한다. 허용할 수 있는 신호 대비 소음 비율 및 비트 오류 비율을 소프트웨어로 프로그램 할 수 있고, 한편으로는 광섬유 플랜트에서 전형적으로 발견되는 불필요한 빛을 제한하면서 단단한 광 링크를 가능하게 한다. 그 불필요한 빛은 제한하지 않으면 광신호 탭을 통한 악용을 위한 추가적인 수단을 제공하게 된다.

8.0 결론 및 권고 사항

오늘날의 현대적인 정보 기술 및 서비스에 기반한 경제에서는 통신은 필수적인 요소이다. 전 세계적인 상업은 중요한 통신 기반 시설에 의존하고 있고, 데이터 및 음성 전송의 사용 가능 여부, 기밀성 및 완전성에 의존한다. 공공 및 사설 네트워크로부터 빼 내어진 불법적인 민감한 통신 및 정보는 금전적, 정치적 혹은 다른 이득을 위해 불법적으로 사용될 수 있다. 회사 스파이 행위는 그러한 행위 뒤에 있는 주여 동기로서 정부 스파이 행위를 초과하게 되었다. 전 세계의 경쟁사들은 그러한 비도덕적인 수단을 통해서 점점 더 경쟁 우위를 추구하고, 비밀 정보, 금전적인 이득 및 가치가 있는 개인 소유의 시장 정보를 찾고 있다. 전 세계의 조직들이 점점 더 정교한 공격 수단을 활용하고 있기 때문에, 중요한 통신 기반 시설의 완전성과 유효성을 붕괴시키거나 혹은 파괴하는 것을 통한 테러리즘에 대해 고려하여야 한다.

광 네트워크는 대량의 정보를 저렴하고 효율적으로 전 세계에 전송하는 것에 아주 적절한

것으로 증명되어 왔다. 오늘날의 모든 유형의 통신 네트워크는 중심부에 있는 광네트워크와 주변으로 퍼져 나가는 것으로 구성되어 있다. 더 많은 기술적인 발전 및 가격 인하로 인하여 광섬유는 대부분의 회사 건물에 존재하게 되고, 시간이 지나면서 데스크탑 컴퓨터로, 혹은 심지어는 더 부유한 거주자 동네 및 주거지로, 네트워크의 최종 말단을 향하여 그 길을 가고 있다. 오늘날의 회사들은, 그리고 그들이 지지하고 있는 경제는 진짜로 광 네트워크가 제공하는 통신 서비스에 아주 많이 의존하고 있다.

광신호 탭핑 방법은 광섬유 위에서 전송되는 대량의 음성 및 데이터를 빼낼 수 있게 하고 분류할 수 있게 한다. 모든 유형의 미디어는 필수적으로 디지털화되고, 조직화되고 잘 문서화된 표준 프로토콜을 통해 광 네트워크를 통해서 전송된다. 광섬유에 대한 본질적인 위험성, 그리고 그것들이 정말 안전하다는 믿음은 아마도 오늘날의 통신 산업계에서 가장 큰 오해일 수도 있다. 이러한 보이지 않는 위험을 무시하기로 한 회사, 정부 및 다른 조직들은 잠재적으로 상당한 손실, 과도한 노출 및 장기간의 브랜드 희석에 직면하고 있는 것이다. 통신망 운용사도 또한 이러한 노골적인 네트워크 취약성에 대해 반드시 대응해야 하고, 광신호 탭에 대응한 보호와 계약적인 보증을 그들의 고객에게 제안하여야 한다. 정부는 모든 유형의 광신호 탭으로부터 그들의 네트워크를 더 잘 보호하여야 하고, 사전 예방적으로 그러한 방법을 불법적으로 활용하는 사람들을 사전 예방적으로 추적해야 하고 탐지해야 하고, 그러한 위험에 대하여 조직들과 시민들을 교육하고 힘을 실어 주는 것을 도와야 한다. 광신호 탭핑 기술을 둘러싼 문제들을 다루고 그런 문제를 바로 잡을 준비가 안된 그룹들은 금융적 및 위험 노출의 관점에서 장기적으로 분명히 경쟁 열위를 갖게 될 것이다.

참고 문헌

- Alwayn, Virek. "광섬유 뒤에 있는 물리학". *광섬유 기술*. 2004년 4월 23일.
- ARC Electronics. "구리 케이블에 대비한 광케이블의 장점에 대한 간단한 개요". *광케이블에 대한 기본 사항 - 지도서*. 일자 불명.
- Book, Elizabeth. "정보 기술 산업은 다양한 위협을 겨냥하고 있다. 네트워크 취약성에 대한 두려움이 향상된 보안 시스템에 대한 시장을 활성화 시키고 있다". 2002년 8월.
- Corning Incorporated. "광섬유에 대한 기본 원칙", *코닝 케이블 시스템*. 저자 미상. 2005년.
- 광섬유 협회. "광섬유 통신에 대해 이해하기". 2004년.
- Goff, David R. "광섬유 기술에 대한 간략한 연혁", *광섬유 참조 가이드*, 제 3판. Focal Press: 2002년.
- LightSpeed MBPS, Inc. "광섬유 101". 일자 미상.
- 오이스터 옵틱스 주식회사. "광 탭핑 방법에 대응한 광섬유 통신의 보안", *광신호 탭 및 다양한 솔루션에 대한 백서*. 2002-2003년.
- Poole, Craig D. "완전한 반사 표면을 가진 광섬유 탭 및 그것을 만드는 방법". *미국 특허 6,535,671*. 2003년 3월.
- Snawerdt, Peter, "페이지 모듈레이티드 광통신시스템". *미국 특허 6,469,816*. 2002년 10월.
- Svoboda, Elizabeth. "광자 기반의 시스템에 의해 명칭하게 된 암호 해독자" *디스커버*, 2005년 1 월.

33 vol. 26, No. 1

Tapanes, E. and Carroll, D. "탐핑에 대응한 광섬유 통신 링크에 대한 보안", *광섬유 보안 링크 - 백서*. 일자 미상.

Walter, Herbert, "유리 섬유로부터 신호를 빼내기 위한 방법 및 장치" *미국 특허 6,265,710*. 2001년 7월.

< 作成日 > 2015年.11月.3日

< 翻譯者 > 김 준 형

- 韓國貿易協會 通翻譯 專門委員 5 期
- IT, 電子, 保安裝備 製造社 海外營業 本部長 歷任
- 綜合商社 海外支社長 : 機械, 플랜트, 電子 , IT, 石油製品 輸出入

< 監修者 > 吳 成 根

- 大韓民國産業現場教授(情報通信)