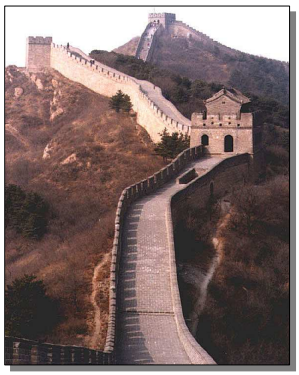
Welcome to 21st century!
Do you know where your data is?

Franjo Majstor
Sr. Technical Director - EMEA
CipherOptics Inc.
franjo@cipheroptics.com

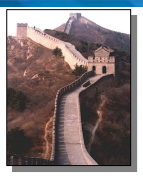
CIPHEROPTICS

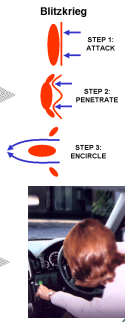
Q: What Do These Things Have in Common?



CIPHEROPTICS

A: They all inspired "bad guy innovation"





CIPHEROPTICS

Defending your perimeter

Suddenly, a heated exchange took place between the king and the moat contractor.

The Far Side by Gary Larson

CIPHEROPTICS

Does This Keep The Bad Guys Out?

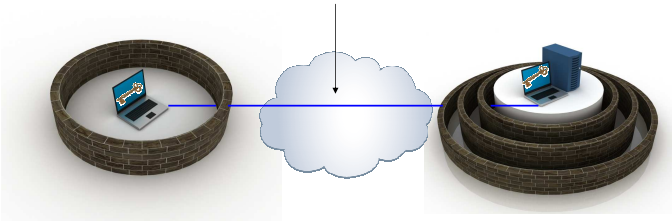
Perimeter Security

Defense in Depth

CIPHEROPTICS

Where is your data NOT protected

What is your security solution for here?



Perimeter Security

Defense in Depth

CIPHEROPTICS

Protecting Data "Between the Rings"

The Limitations of Perimeter Defense

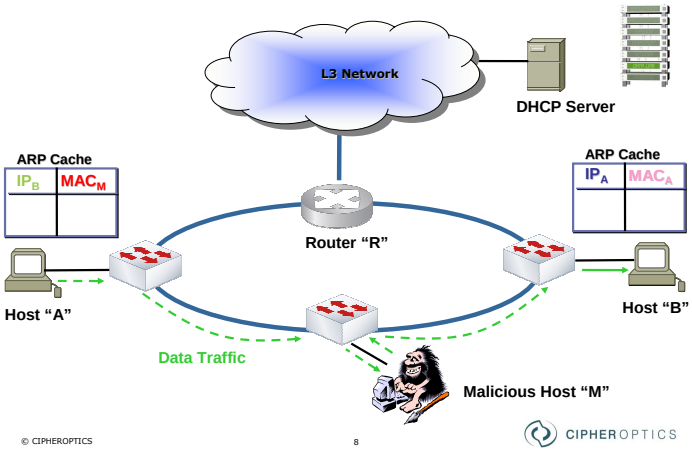
- Data is pretty secure inside your firewall/perimeter defense
- You see all users and control access to resources and storage locations, but…
- Data Thieves, and Foreign Governments can wait patiently for you to send data beyond your perimeter defenses

The Perimeter is Crumbling!

- Your data moves beyond the reach of your security solutions all the time (you can't do business confined to your perimeter).
- Many of the the bad things that happen to data occur "between the rings" because that is where it is most vulnerable

CIPHEROPTICS

MitM Attack - Only stealing a Password?



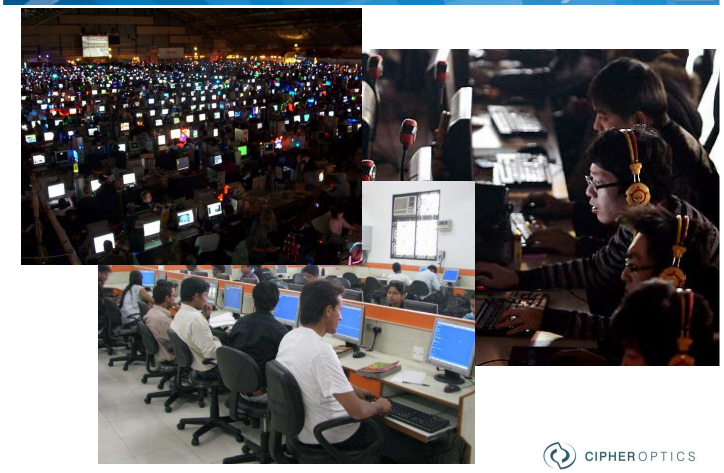
CIPHEROPTICS

MitM Attack - Recording the VoIP call…

- After intercepting a network connection, packets containing G.711 voice data are collected and the phone conversation is recorded and then replayed
- Demonstrated live to senior executives in their network
- Tools are publicly available with GUI and bi-directional spoofs
- Easily taught in 5 minutes
- Neither the victim nor the default gateway is aware of the attack!

CIPHEROPTICS

Who is it we are defending against?

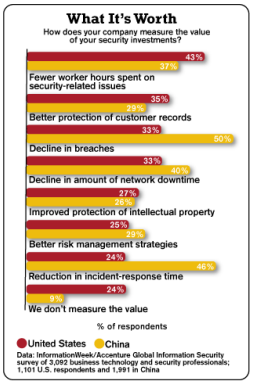


CIPHEROPTICS

Where to put your efforts?

Ideally you should make investments that yield the greatest reduction in risk

- **Options**
  - Perimeter Security
  - Information control (white lists)
  - Intrusion Detection/Prevention
  - WAN Encryption
  - Others
- **Which of these will give you the biggest reduction in RISK?**



CIPHEROPTICS

Do Not Recommend This Strategy!

"We don't pay much attention to information security. We're hoping our competitors will steal our ideas and become as unsuccessful as we are."

CIPHEROPTICS

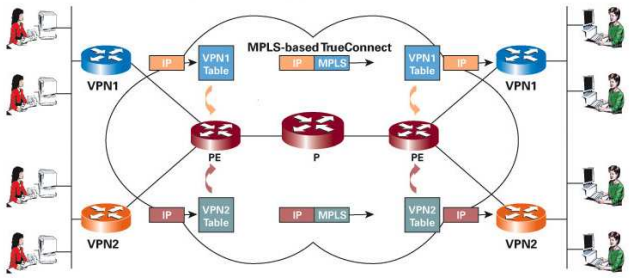
We use a "Private Network"

The SP says the network *is secure...*

- Traffic streams are kept separate
- There are controls around provisioning and management
- There are gateways between the Public Internet and the MPLS
- Because they have Netflow to identify "malicious" activity

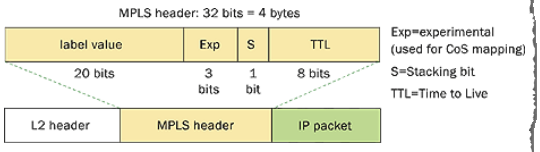
CIPHEROPTICS

When Privacy was Equal to Security



CIPHEROPTICS

Where is the security?



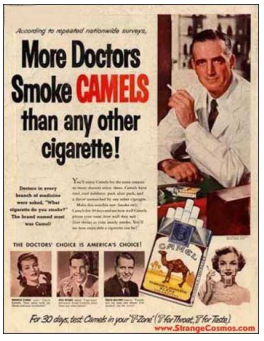
CIPHEROPTICS

We use a "Private Network"

People say the network *is secure*

In a podcast dated April 2009 a Product Director said security was "built in" to MPLS based on the following:

- Traffic streams are kept separate
- There are controls around provisioning and management
- There are gateways between the Public Internet and the MPLS
- Because they have Netflow to identify "malicious" activity



CIPHEROPTICS

The Truth about MPLS "Security"

Black Hat Conference 2009

One of the breakout sessions and downloadable whitepapers provide a "cook book" approach to sniffing and redirecting MPLS traffic

- Traffic streams are kept separate
  - The very mechanism used to separate traffic is what the data thieves are exploiting
- There are controls around provisioning and management
  - Provisioning and management are to data security what traffic lights are to bank robbers
- There are gateways between the Public Internet and the MPLS
  - Traffic is not accidentally leaking out to the Internet, it is being stolen right off the MPLS backbone
- Because they have Netflow to identify "malicious activity"
  - Post event notification is not a substitute for prevention

CIPHEROPTICS

What is it that they are after?

INTERNATIONAL Herald Tribune

Arrests of 20 widen Telecom Italia

By Eric Sylvers
Thursday, September 21, 2006

The Italian police have arrested 20 people in se
scandal involving a senior Telecom Italia execu
official.

Although the investigation is not connected with
break-up of the company, which resulted in the
a dispute with the prime minister, it is another b
companies in Italy.

Those arrested Wednesday included the forme
Italia; the current head of security of Pirelli, whi
owner of a private investigation agency; and m
other police forces, according to the official, wh
he was not authorized to speak while the inquiry was under way.

The arrested are accused of corruption and of illegally obtaining bank and phone records. It is not clear why the accused were accumulating the data.

www.nytimes.com/2006/09/21/technology/21iht-italia.2690013.html

InfoWorld Home / News / Business / Telecom Italia embroiled in new espionage scandal

JANUARY 19, 2007

Telecom Italia embroiled in new espionage scandal

Cloak-and-dagger story of hacking and spying brings four arrests, including the company's head of information security

By Philip Willan | IDGNS

Print | Add a comment | Like | Be the first of your friends to like this.

Milan magistrates have arrested four Telecom Italia employees for alleged illegal espionage activities, bringing a fresh wave of scandal crashing down onto the former national carrier.

The suspects were identified as Fabio Ghioni, the head of information security at Telecom Italia; his assistant, Rocco Lucia; and Guglielmo Sasinini, a former journalist who had been hired by the company to conduct country risk analyses for the Middle East region, according to a 230-page arrest warrant signed by Judge Giuseppe Gennari and widely cited in newspaper reports Friday.

A fourth warrant was served in prison on Giuliano Tavaroli, the former head of security at Telecom Italia, who had already been incarcerated on illegal espionage charges as a result of a separate investigation.

CIPHEROPTICS

Are Fiber Links secure?

- Organizations must assume that an unauthorized user can eventually access privileged information in transit
- There are tools on the Internet selling for **$100** to hack fiber cables
- It is not a matter of IF, but WHEN

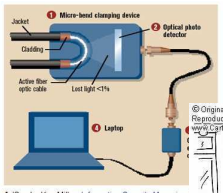


Figure A (Sandra Kay Miller, *Information Security Magazine*,

➢ **Encryption is necessary to eliminate the risk**

CIPHEROPTICS

What's the Security Concern?

➢ **Networking professionals are often sold the myth that because fiber is optical, it's inherently secure. This is not the case.**

ComputerWorld:
"Tapping fiber optic cable without being detected, and making sense of the information you collect, certainly isn't trivial, but has been done for the past seven or eight years."
-- Gartner Group

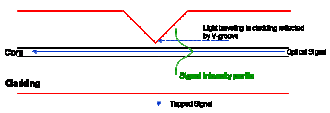
The Wolf Report:
"Security forces in the US discovered an illegally installed fiber eavesdropping device in Verizon's optical network. It was placed at a mutual fund company shortly before the release of their quarterly numbers."

It's even possible, using macrobending techniques, to tap fiber without removing the fiber cable sheathing.

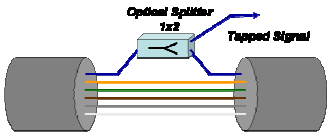
A fiber tap

CIPHEROPTICS

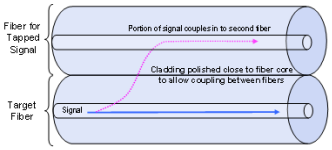
Types of Fiber Taps (Intrusive Methods)



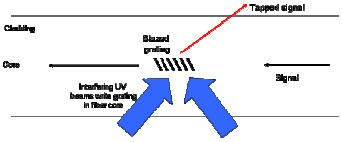
V-Grove Tapping



Splitter Tapping
(Powered & Non-Powered)



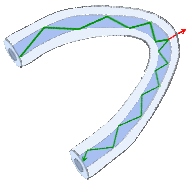
Evanescent Coupling Tap

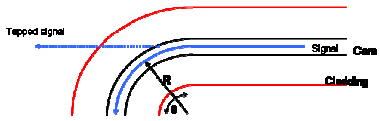


Scattering Tap

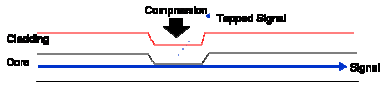
CIPHEROPTICS

Types of Fiber Taps (Non-Intrusive)





Bent Fiber Tapping



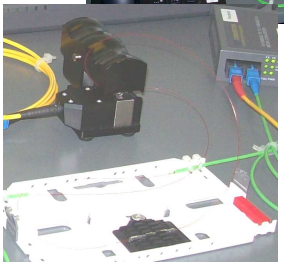
Compression Tapping

CIPHEROPTICS

Have I Done it?

Passive Fiber tapping demo on Infosec show in London 2009.

Low cost equipment and effective VoIP wire tap with a minimum investment, ...just for the show?



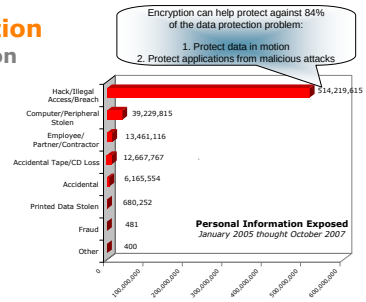
CIPHEROPTICS

Benefits of Network-wide Encryption

Proactive Data Protection

Encryption of data in motion protects against:

- **Data Theft**
  - Hackers
  - Bots
  - Dishonest employees or contractors
- **Data Leakage**
  - Router mis-configurations
  - OS vulnerabilities
  - Application back doors

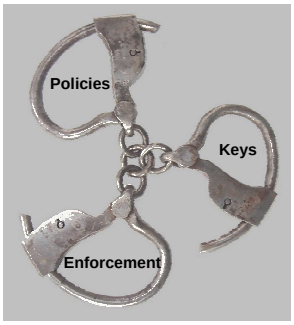


Peace of Mind and Compliance

- **Encryption is the only security solution that keeps working for you after the data has left your control**
- **Even if the SP network is breached, your data remains safe**

CIPHEROPTICS

Why is encryption so hard?



- Encryption has three main components
  - Security Policy creation
  - Key Distribution and management
  - Policy Enforcement
- IKE based IPsec
  - Binds the three components of encryption into a single, monolithic process
  - This turns every network into a point to point network!
- This was fine in the late 90's when everything was point to point
  - It causes a lot of problems today

By de-coupling the three processes from each other you are able to make encryption transparent to both network and applications

CIPHEROPTICS

What Has Changed?

Encryption is finally "enterprise friendly"

- Fast, scalable, reliable, **no user impact**
- Policy-based security **independent** of network policy
- Easy to deploy and can be **centrally managed**
- **Natively supports** any-to-any connectivity required for VoIP and multicast **applications**
- Works on **all topologies**

Network-wide encryption with today's technology allows you to move from detection to prevention.

- **Leverages synergies** of access control and encryption
- Allows **Secure Information Sharing** over ANY network

"Demonstrating that your company is implementing strong privacy safeguards and consistently enforcing information security controls is a strong competitive differentiator."

- John Ho-Chi,
Ernst & Young, Singapore

CIPHEROPTICS

The trade off Performance vs. Security

Modern Networks Require	Traditional Network Encryption
Any to Any Connectivity	Limited to Point to Point connections
Scalability	Exponentially complex with scale
High Speed-Low Latency Performance	Induces latency and chokes throughput
High Availability Architectures (load balancing, DR)	Requires manual fail over procedures
Layer 2-4 Services	Masks Headers

CIPHEROPTICS

Providing Security and Performance

Our Modern Approach to Encryption

Define Polices based on you existing Network or Application Topologies

Topologies	Applications
Mesh	Voice
Hub and Spoke	Video
Multicast	Control Data
Hybrids	FTP or other protocols

Create the Keys needed to support the Policies

CipherEngine uses standards based security protocols
- AES 256
- SHA-1
- IPsec

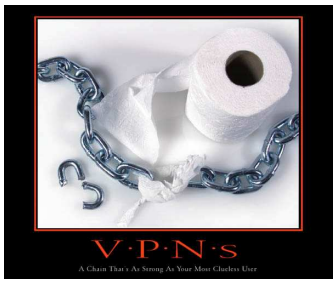
Enforce the policies without creating tunnels

Preserve native routing/switching protocols and paths
- Layer 2 - encrypt by VLAN
- Layer 3 - preserve IP routs and subnets
- Layer 4 - maintain traffic shaping and Netflow/Jflow while encrypting

By designing encryption for modern networks, made it easy to install, transparent and performing you may have a solution in your hands…

CIPHEROPTICS

Instead of the Summary…

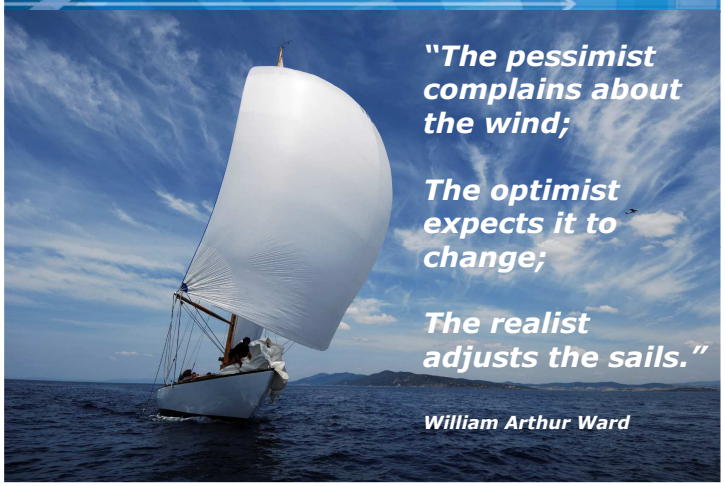


Source: Sourcefire 2004 Network Security Calendar

http://www.ranum.com/security/computer_security/calendar/index.html

CIPHEROPTICS

What will you do?




Networking
Thank You!
CipherOptics.com
Security
CIPHEROPTICS