Melior Inc.

Perfectionists At Work

CyberWarfare Defense Solutions

Patented Technology

Applied against dDoS & PenTest attacks

iSecure

CyberWarfare Defense

A New Layer of Network Security

Hello Lockheed Martin!

Matt Gair
COO and Co-Founder
Melior, Inc.
www.dDoS.com

USA/HQ: Dallas/Texas
Germany: Dortmund & Stuttgart
India: New Dehli

Melior Inc.
Perfectionists At Work

Presentation Overview

1. About Melior, Inc.
2. The Threats: Penetration Testing & dDoS Attacks - a quick overview
3. iSecure Technology – Overview of Core System
4. iSecure applied: Penetration Testing Defense, v3.2
5. iSecure applied: dDoS Defense, v3.2
6. iSecure Developments: dDoS and eDoS
7. Practical Applications in current production
8. More Information, White Paper, Demonstrations

About Melior, Inc.

- Start-up company with a global focus
- Founded in 1996
- iSecure Development started in the late 1990’s
- iSecure started European patent process as an appliance (not Software patent!) in 2001; the Swiss patent was granted in April 2004, and is now applied in many countries through PCT
- We are “the” dDoS company: with the first working product efficiently defending against Denial-of-Service

iSecure Product Launch

- iSecure products started shipping (launch with the RSA Show in San Francisco in February, and Berlin/Germany in May)
- Product evaluations and dedeployments in progress at many sites, mostly in the US and EU
- Both dDoS and PenTest products are shown this week at Networld + Interop in Tokyo, Japan

Melior, Inc. Product Impact

- We host and protect London/UK-based Spamhaus successfully against dDoS and PenTest attacks - since Fall 2003
- Showcase demonstrating the effect of large-scale Denial-of-Service attacks
- MyDoom Virus written specifically to launch dDoS attacks against Spamhaus and other anti-Spam organizations

Melior, Inc. – Product Impact

- By protecting Spamhaus against dDoS Attacks, all of their customers can still utilize their anti-Spam databases
- Spamhaus’ SBL and XBL allows customers to eliminate 30%-40% of Spam
- Without our iSecure dDoS CyberWarfare Defense solution, this valuable resource would have been gone since September 2003

CyberWarfare Defense ™

These Spamhaus customers have anti-Spam protection because of iSecure:

Allegiance Telecom, Ameritech (SBC), AON, Boeing, Cable & Wireless,
Charter Communications (chartercom.com), Citigroup, City of New York, County of San Bernardino, Cox Communications, DaimlerChrysler, Deutsche Bank, Deutsche Telekom AG, Ericsson, ESPN, FAA, GoAmerica, Hawaii Online, Hotmail/MSN, Hughes, Intel, Internap, **Lockheed Martin**, Lufthansa, Macmillan Publishing, Message Labs, Morgan Stanley, Mosaic Communications, MSN Disney, MTV Networks /Viacom, Inc., NASA, NEC, Nortel, Novell, Oracle, Porsche, Schlund, SGI, Stanford University (and many other Universities world-wide), Symantec, Toshiba, UPS, Verio/NTT, Vodafone

The Threat

Penetration Testing & dDoS Attacks

- Ongoing IP Scans to determine & exploit vulnerabilities
- Penetration Testing provides the “road map” for subsequent attacks
- dDoS attacks often take advantage of vulnerabilities
- dDoS cause wide-spread outages and damages (economically, politically, etc).

Defense against Penetration Testing?

- No defense tool on the market is geared towards this purpose
- Firewalls limit TCP/UDP ports, but leave those open which need to pass traffic (Web, E-Mail, FTP, SSH, ...)
- Scanning Tools (NMAP, Nessus, etc.) can map routers, firewalls, and all systems behind a firewall through open ports, determine Hardware, OSs, Configuration

Existing Defense Approaches?

- ALL existing solutions are re-active:
- Signature-based traffic comparison / matching – finds only known attacks
- Bandwidth Averaging: requires “learning”, applies QoS methods, which cut off valid traffic spikes and aid dDoS attacks by “drowning out” the good traffic
- Often requires major infrastructure changes

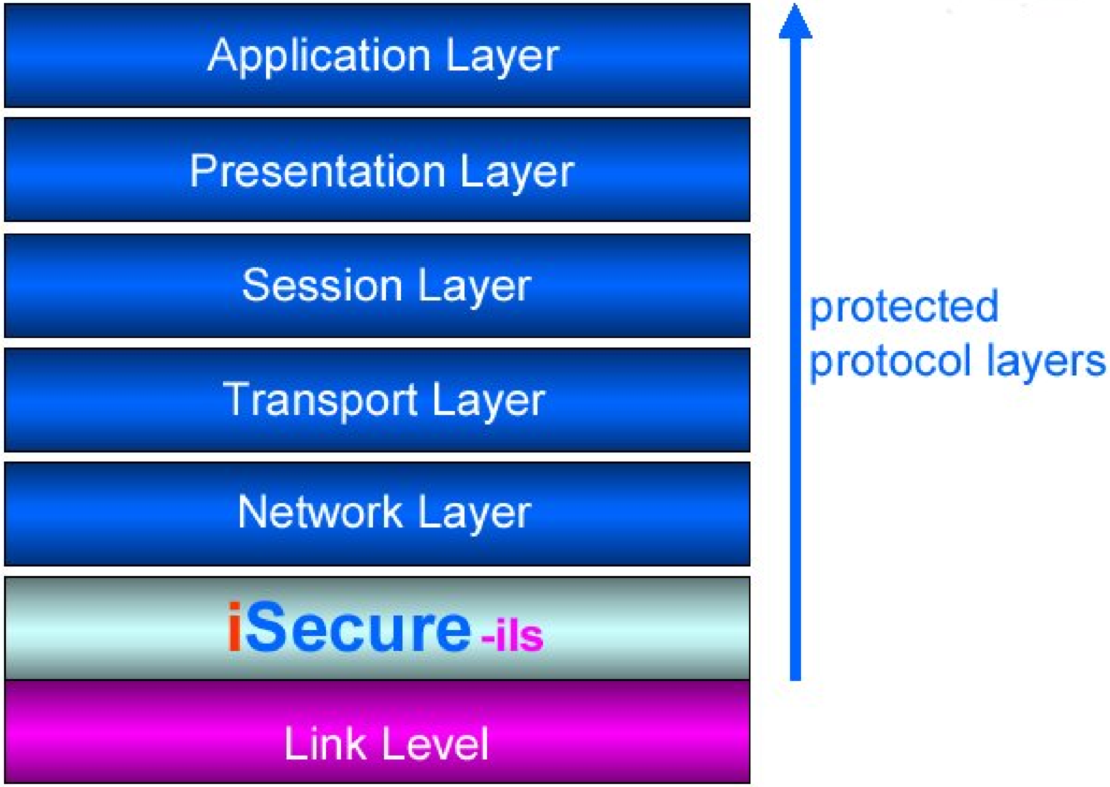
Existing Defenses? (Cont’d)

- Router ACL modification works only against definable traffic, is very slow, and may require manual SysAdmin interaction – while dDoS damage is done within seconds
- ICMP port blocking defends against some attacks, but application-level attacks share bandwidth with valid traffic, so port blocking does not help

The iSecure CORE Technology

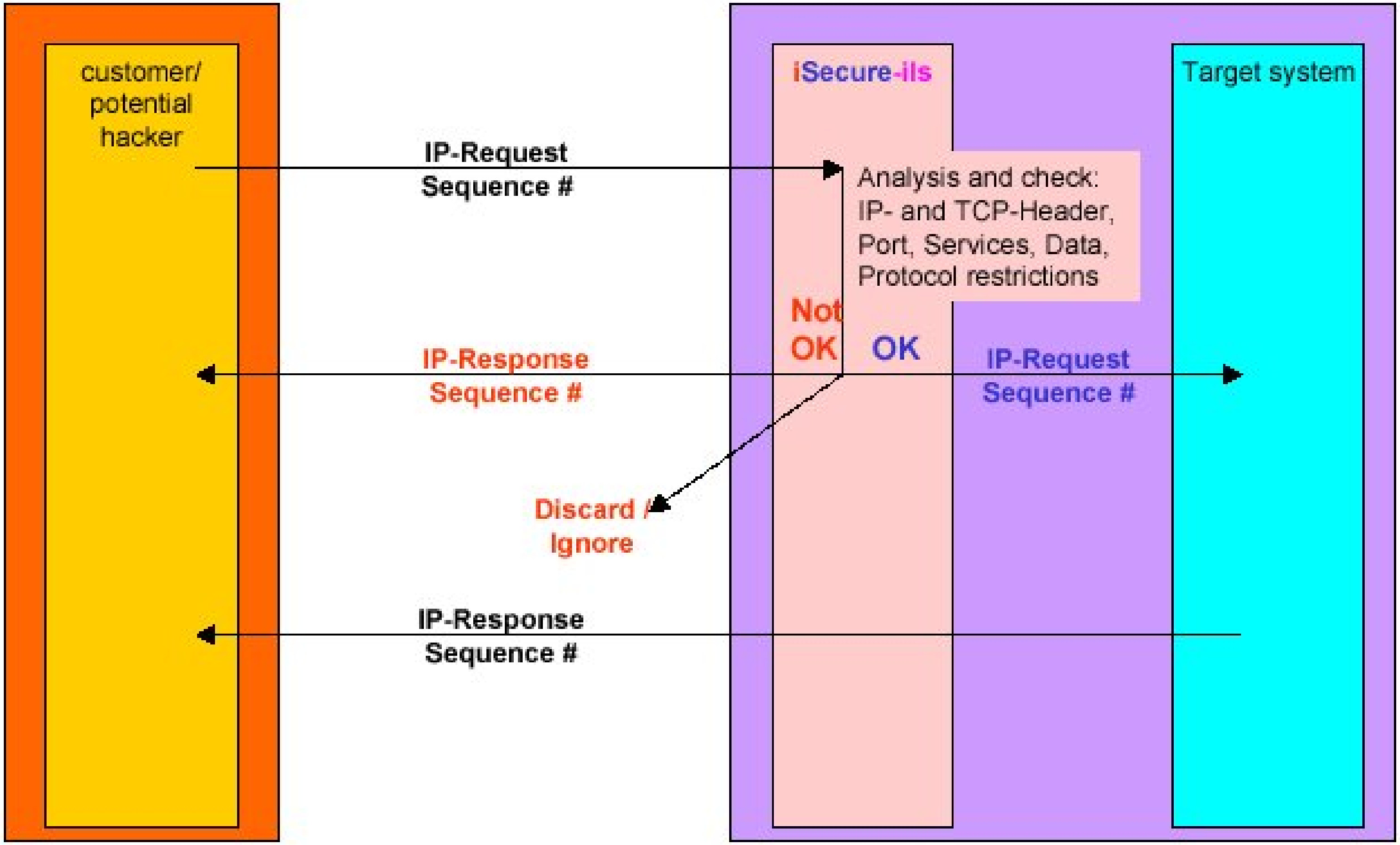
- Real-time Performance (6ns to 6ms)
- Signature-free (!) – never an update
- No Configuration, defends instantly
- Undetectable (mirrors attacker’s OS and ads a randomized response)
- Cannot be compromised
- No MAC address / No IP Number

Defending at Layer 2

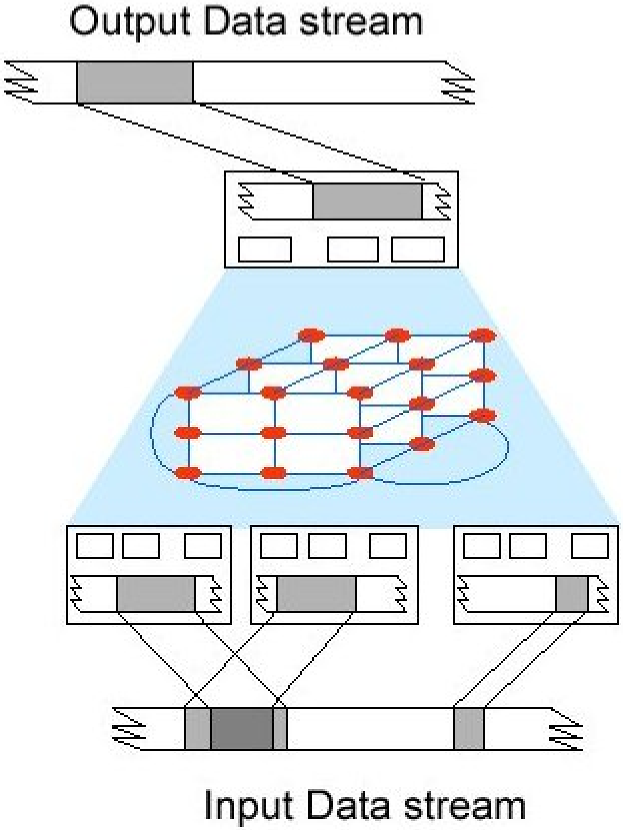


Melior Inc.
Perfectionists At Work

Works as In-Line-Scanner



Real-Time Decisions



Bit-Stream Engine “prepares” and slices Data for parallel Processing.

Decision Engine applies the iSecure algorithm

Melior Inc.
Perfectionists At Work

iSecure Technology Applied:

- Penetration Testing Defense (“Infrastructure Cloaking”)
- Distributed Denial-of-Service Defense (dDoS)

In Development:

- iSecure eDoS: e-Mail Denial-of-Service (Spam & Virus Defense)

Penetration Testing Defense

- Recognizes & Intercepts Penetration Testing (PenTest) probes across more than one port or with high volume on single port
- Reports all ports as “open”
- Provides no Hardware/OS/Configuration
- “Mirrors” the Attacker’s own OS back
  (plus random response)
- NMAP OS Guessing Score always the highest: 9,999,999 (if the attacker turns this option on)
- Attacker does not know what the infrastructure looks like, and cannot target an attack or explore specific vulnerabilities

Denial-of-Service Defense

- iSecure recognizes “good” from “bad” traffic, discards the bad, and allows the good traffic to go through (currently TCP traffic only)
- Defends against all three types of dDoS attacks: bandwidth flooding, TCP/IP stack attacks, application-level attacks
- Defends against KNOWN and UNKNOWN dDoS attacks, incl. Synk4, etc.
  (i.e. includes “zero-day” attacks)

Common Product Features

- Does not require a learning curve, i.e. works right out of the box
- Admin Interface GUI allows for optional “fine-tuning” in legacy environments; UDP port blocking, ICMP configuration beyond default settings
- Easy to deploy (no changes to existing infrastructure required)

iSecure™ **PenTest** Defense

- **PenTest Defense Stand-Alone v3.2**
- Available in Standard (1U) or High-Availability (2U)
- Network Interfaces fail open or close in HA configuration
- True 100 Mbit/s throughput

iSecure™ **PenTest & dDoS Defense**

- **Full Product: PenTest and dDoS Defense v3.2**
- Available in Standard (1U) or High-Availability (2U)
- Network Interfaces fail open or close in HA configuration
- True 100 Mbit/s throughput

New Product: **iSecure Gigabit**

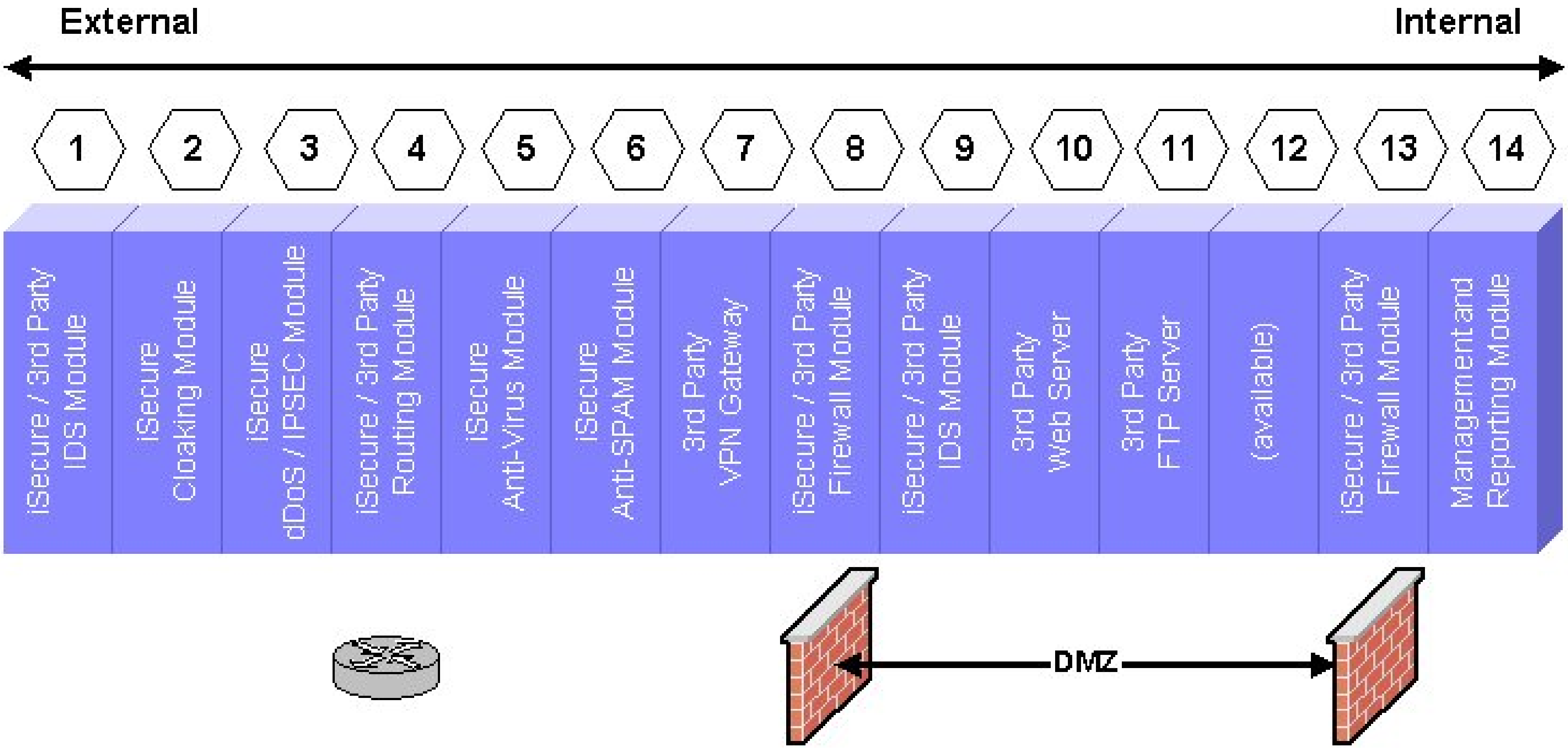
- Announced in Berlin/Germany (May):
  - iSecure PenTest and dDoS scalable to 1 Gigabit/s
  - Load-balanced (two-way) across up to 10 iSecure 100 Mbit/s units, starting with 200 Mbit/s (pay only for the bandwidth protection the customer needs), and upgradeable in 100 Mbit/s increments

Product Improvements:

- We plan to include in PenTest/dDoS v4.0:
  - UDP protection
  - ARP protection
  - Migration from the current Windows-based GUI to a platform-independent central Admin/Report interface via 3rd network port
  - Ability to report to a central monitoring system via 3rd network port (syslogd)
  - Improved reporting capabilities
  - Ability for higher bandwidth in one system

In Development: iSecure "TIPS"

True Intrusion Prevention System



1 iSecure / 3rd Party IDS Module

2 iSecure Cloaking Module

3 iSecure dDoS / IPSEC Module

4 iSecure / 3rd Party Routing Module

5 iSecure Anti-Virus Module

6 iSecure Anti-SPAM Module

7 3rd Party VPN Gateway

8 iSecure / 3rd Party Firewall Module

9 iSecure / 3rd Party IDS Module

10 3rd Party Web Server

11 3rd Party FTP Server

12 (available)

13 iSecure / 3rd Party Firewall Module

14 Management and Reporting Module

Other Production Examples:

- eCommerce Hosting Provider
  - Under constant dDoS attacks, web site unavailable for days
  - iSecure deployment instantly defended against the dDoS attacks; web site has been always available since (over 1 year now, starting with Pilot product tests)
- Federal Credit Union
  (pilot with one of 18,000 nationwide in the USA)
  - Successfully deployed PenTest defense from Pilot-Program through production version
- Successfully Tested at Commerzbank AG, Frankfurt/Germany

Melior Inc.
Perfectionists At Work

More Information & Demo Units

www.dDoS.com

Demo Units

Available in the US
and our German offices

White Paper

per request

Demonstrations

Live on the Internet
Or On-Site

Melior F.I.R.E CD

For live comparison
and product testing

Demo-Video

Live on the Internet
At www.dDoS.com
Or as DVD per
request