

Melior^{Inc.}

Perfectionists At Work

CyberWarfare Defense
against Penetration Testing and
distributed Denial-of-Service Attacks



The Foundation of Network Security

Stand-alone (ISP/Carrier – Server Farm) modular “TIPS” for Perimeter Defense




We brought a prototype for you!

Presentation Overview

1. Penetration Testing & dDoS Attacks
- a quick overview
2. iSecure Technology – Overview of Core System
3. iSecure applied: Penetration Testing Defense
4. iSecure applied: dDoS Defense
5. iSecure Development: anti-Virus, anti-SPAM
6. Practical Applications in current production
7. More Information, White Paper, Demonstrations


The Threat

Penetration Testing & dDoS Attacks

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




Defense against Penetration Testing?

- None 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

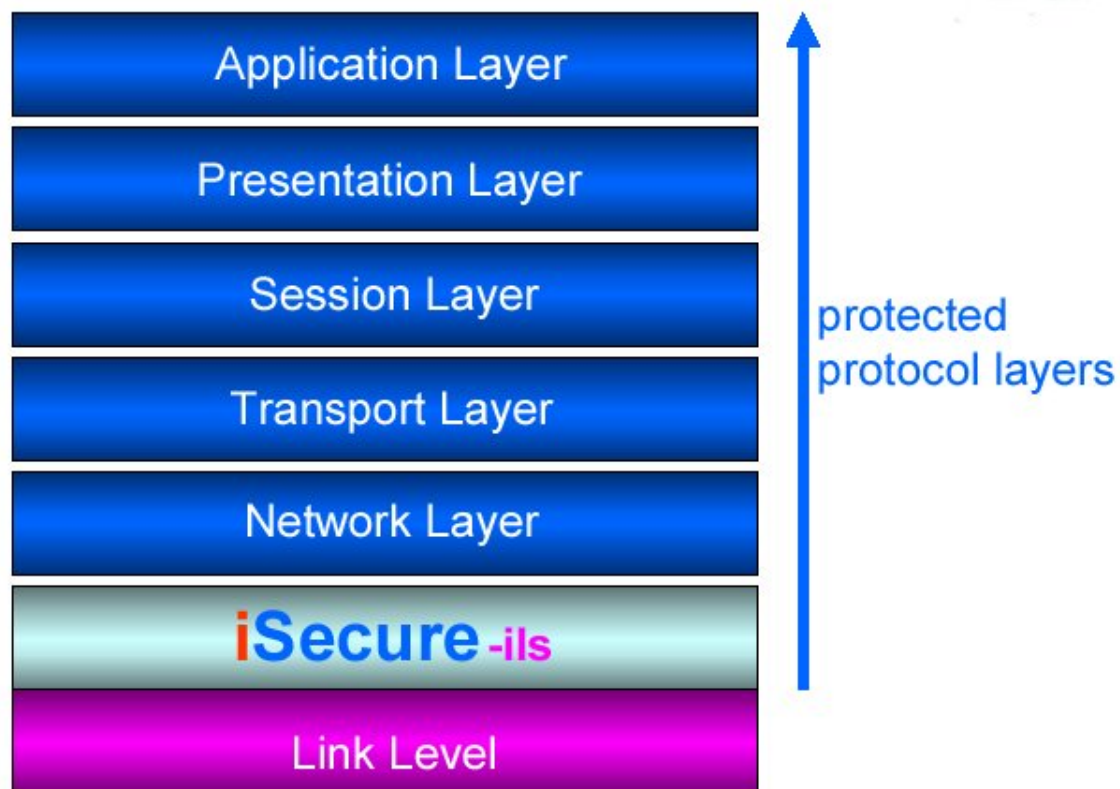
Existing Defenses? (Cont'd)

- Router ACL modification works only against definable traffic, very slow, may require manual SysAdmin interaction – 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
- 

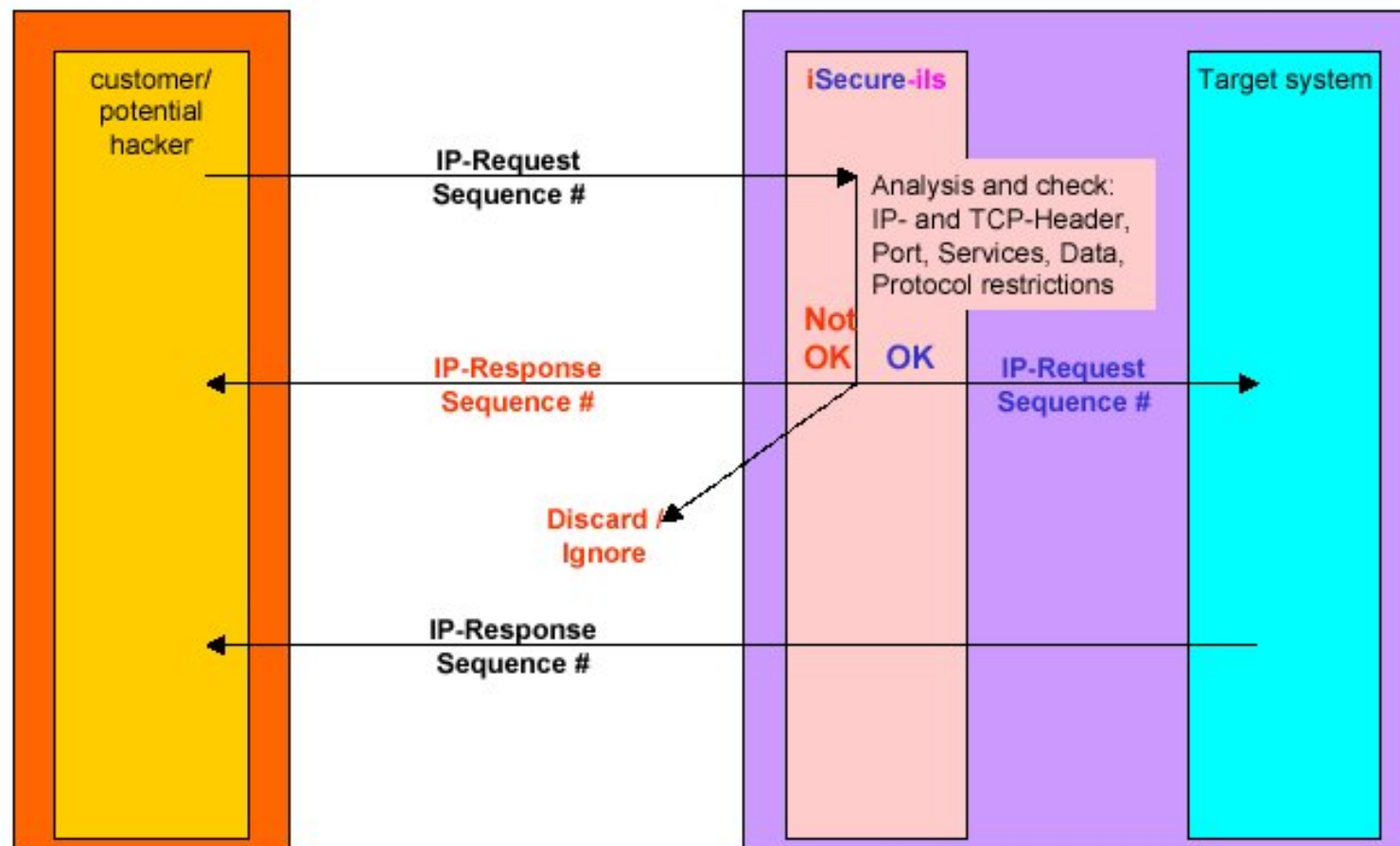
The iSecure CORE Technology

- Real-time Performance (6ns to 6ms)
- Signature-free
- No Configuration, defends instantly
- Stateless (!) – no attackable tables
- Undetectable
- Cannot be compromised
- No MAC address / No IP Number

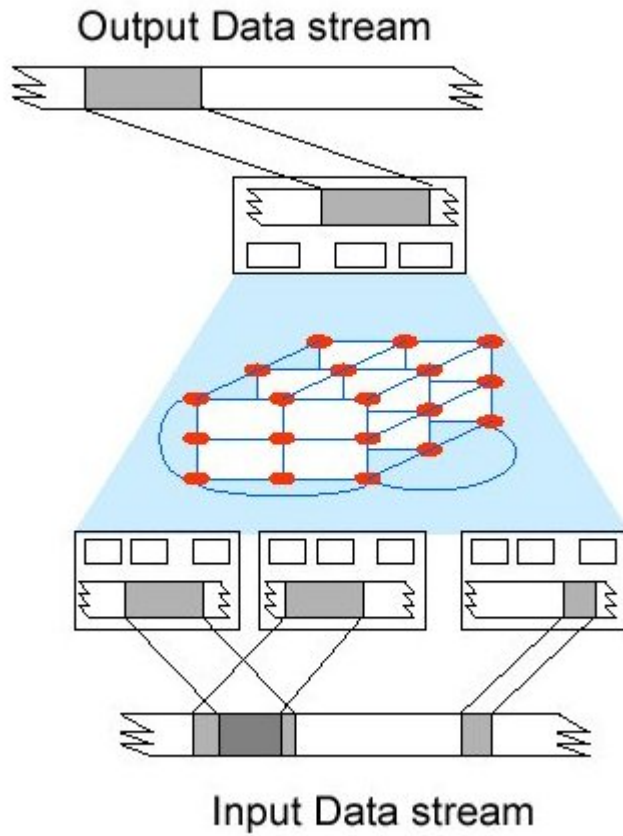
Defending at Layer 2



Works as In-Line-Scanner



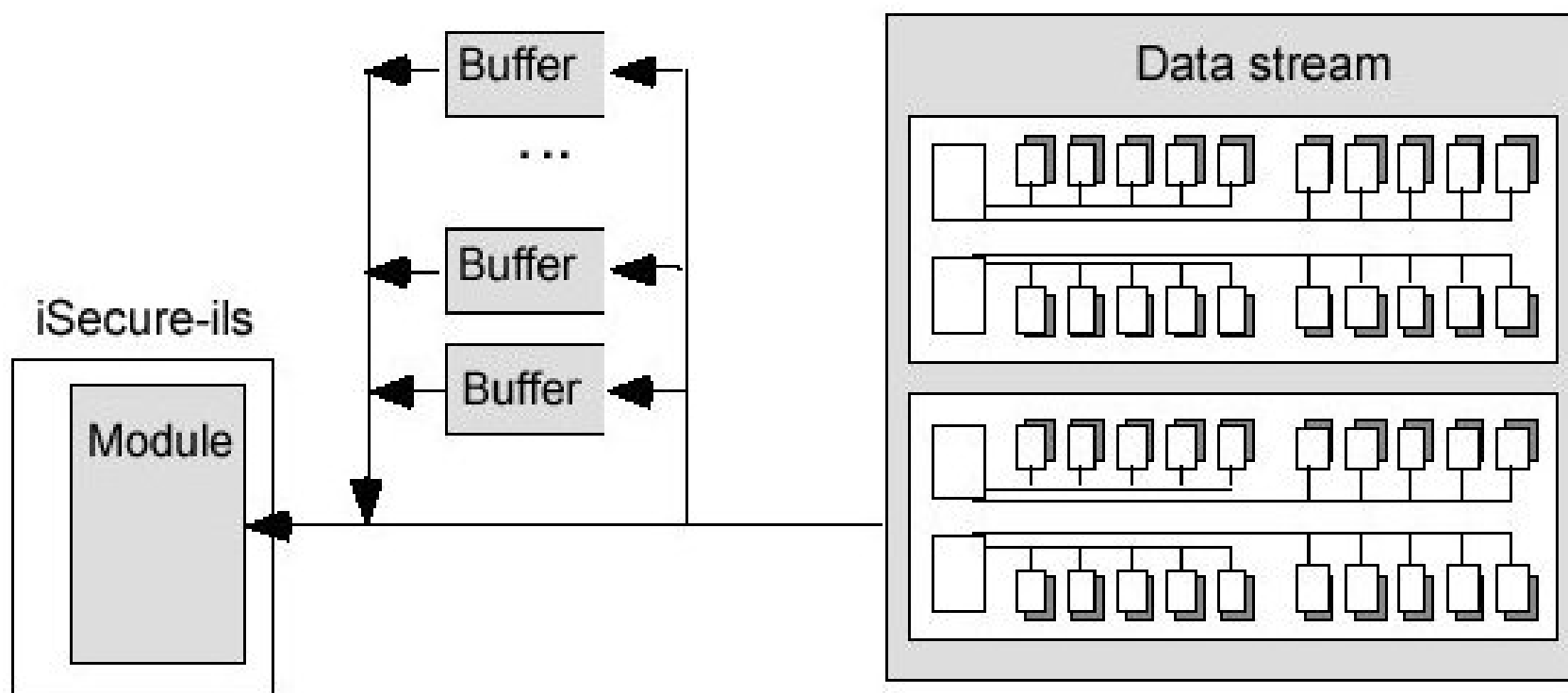
Real-Time Decisions



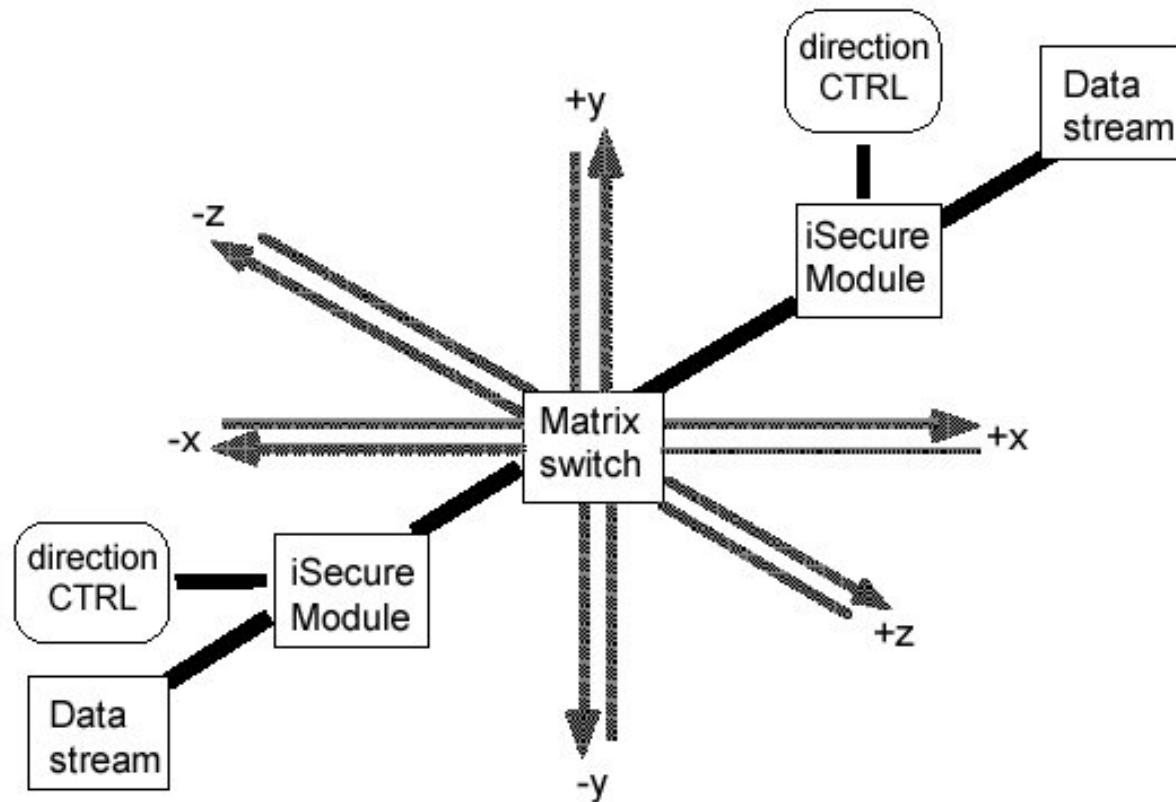
Bit-Stream Engine
“prepares” and slices
Data for parallel
Processing.

Decision Engine
applies the iSecure
algorithm

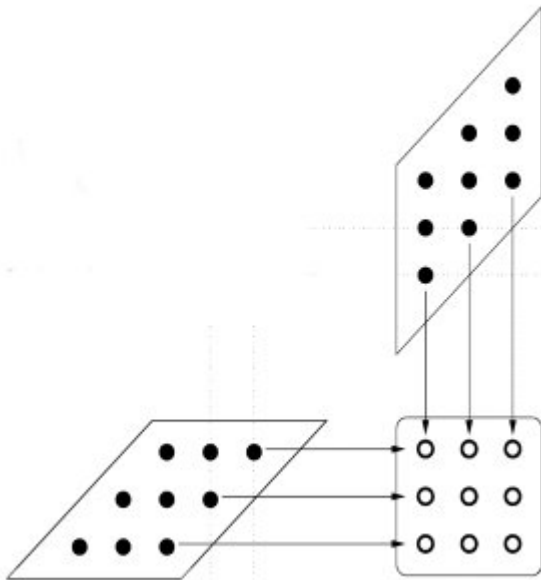
Prepared Data “Slices” are fed to the Decision Engine



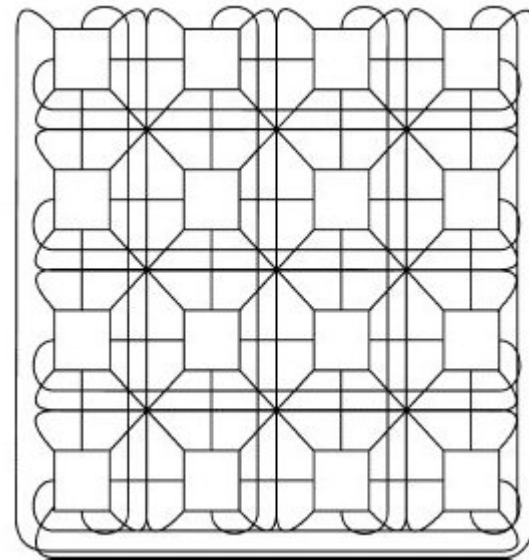
iSecure Decision Engine applies algorithm



iSecure Algorithm “tags” data slices based on 3-dimensional model

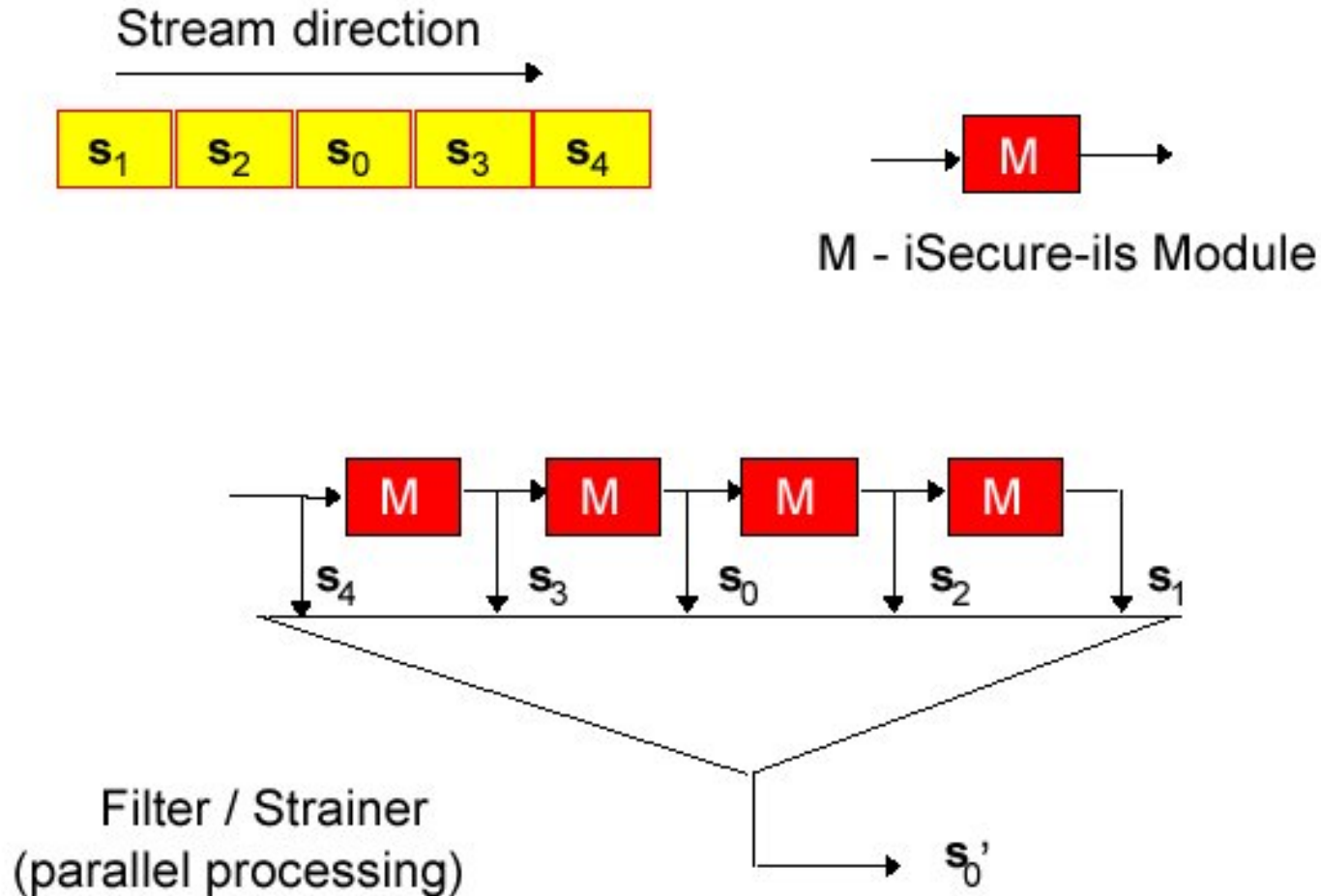


2-dimensional model

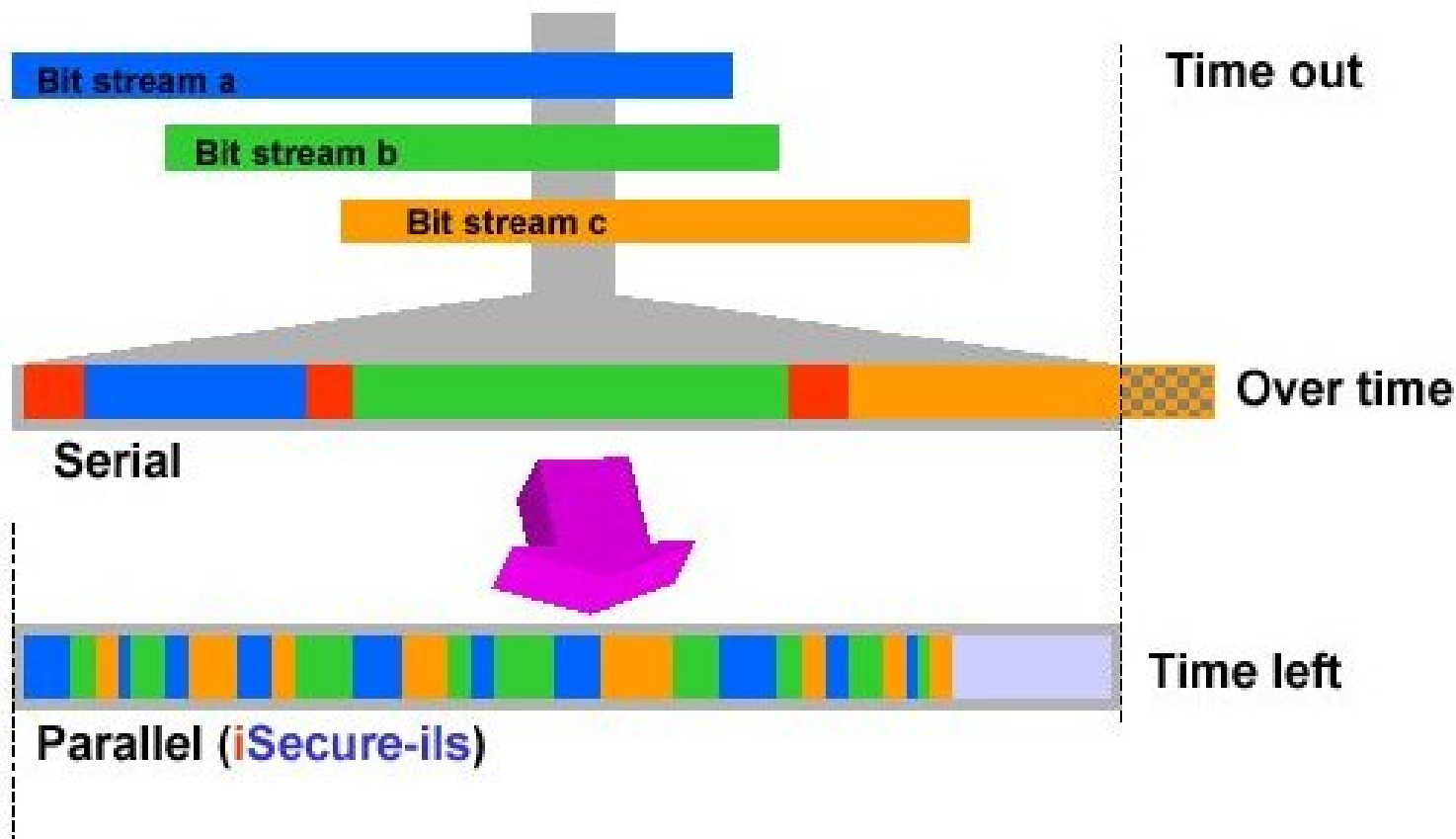


Slice of the decision matrix

Re-Assembly of Data Slices



Parallel Processing of Streams



iSecure Technology Applied:

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

In Development:

- iSecure Anti-Virus
- iSecure Anti-SPAM (UCE) E-Mail

Penetration Testing Defense

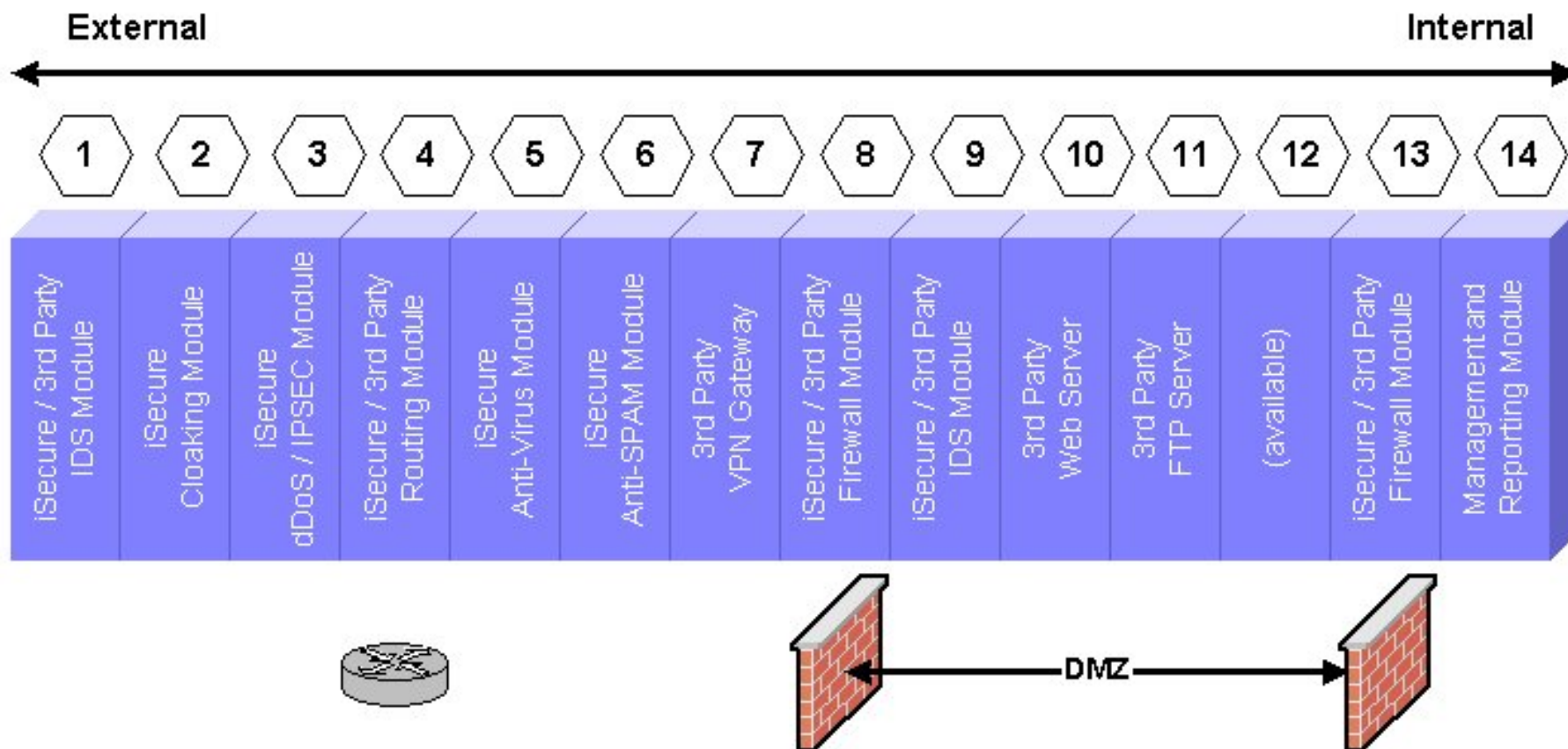
- Recognizes & Intercepts Penetration Testing probes
- Reports all ports as “open”
- Provides no Hardware/OS/Configuration
- “Mirrors” the Attacker’s own configuration back
- NMAP OS Guessing Score always the highest: 9,999,999
- Attacker does not know what the infrastructure looks like, and cannot target 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
- 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.

iSecure "TIPS"

True Intrusion Prevention System



Current Production Example: eCommerce

- eCommerce Hosting Provider
 - Under constant dDoS attacks, web sites unavailable for days
 - iSecure deployment instantly defended against the dDoS attacks; web sites have been always available since

Current Production Example Keeping E-Mail Flowing

- SPAM Blacklist Provider OsiruSoft permanently shut down, resulting in e-mail outages for FTC and many other users
- All other blacklist providers under dDoS attacks (SORBS, EazyNet, DSBL)
- SoBig.F linked to Spam Blacklist attacks, exploiting the network of compromised machines

Attacks on BlackList ISPs

- iSecure systems are being deployed at SORBS in Brisbane, Australia, and Connecticut
- Defending against dDoS attacks, keeping anti-SPAM blacklist providers on the net
- Allowing Government and Corporate E-Mail systems to check against Blacklists to eliminate Spam

More Information & Demo

www.dDoS.com

WHITE PAPER
per request

Melior F.I.R.E CD
For live comparison
and product testing

Demonstration
S
Live on the Internet
Or On-Site

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

