Evolution of attacks and Intrusion Detection

AFSecurity seminar
11 April 2012

By: Stian Jahr

mnemonic
- securing your business

Agenda

- Introductions
- What is IDS
- What is IDS in mnemoic
- How attacks have changed by time and how has it changed the IDS-service
- Q&A

mnemonic
- securing your business

Introduction

mnemonic

- securing your business

Who is Stian Jahr?

- Master in information Security from Gjøvik University College
- Worked in mnemonic security services for 6 years
- Mostly doing network and malware analysis

Who is mnemonic?

- mnemonic is the largest provider of IT security services in Scandinavia
  - 7 out of the top 10 companies in Norway use mnemonic services
  - 11 years of service delivery experience
  - Offices in Oslo (HQ), Stavanger and Stockholm
- We have over 100 staff
  - 80 graduate-level consultants
  - Low staff turnover (<5%)
- We deliver consulting services and managed services globally

> *"We use mnemonic as our trusted advisor for IT security because their consultants understand our business and are experts in their field. Our relationship with them is one of true partnership."*
>
> CIO, Public

PCI Security Standards Council™
QUALIFIED SECURITY ASSESSOR

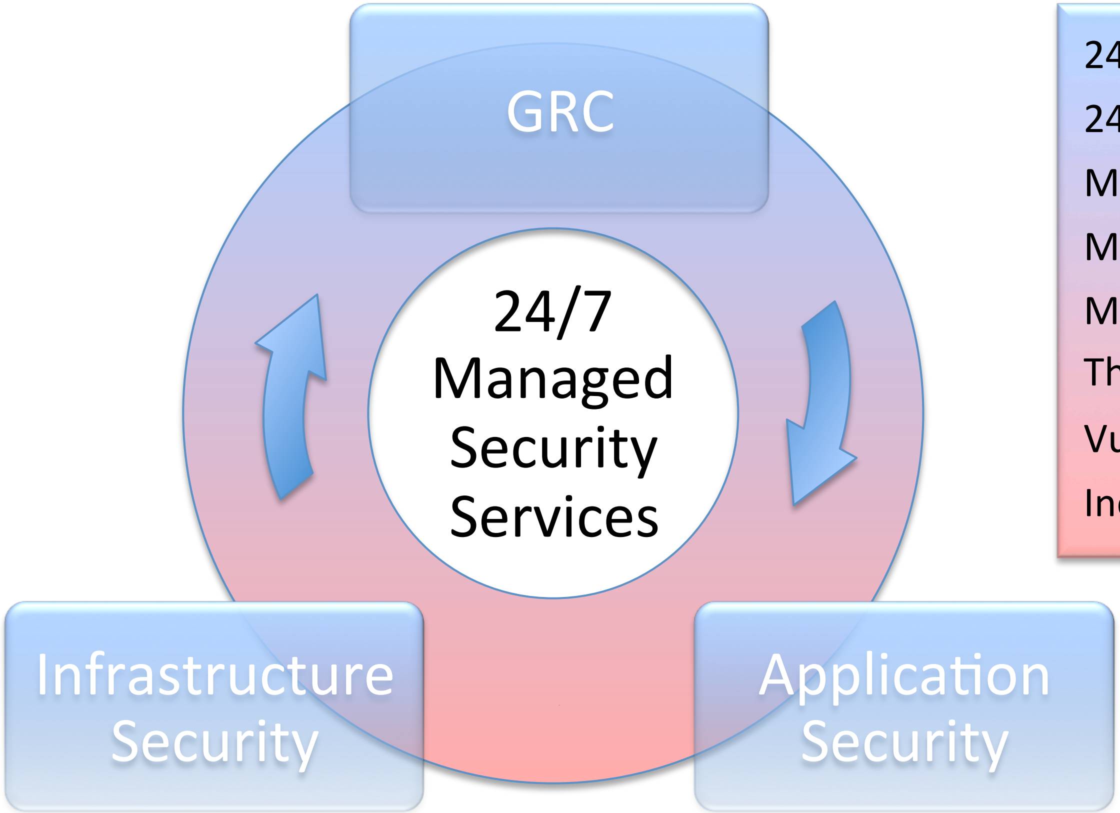
DNV
NORWEGIAN ACCREDITATION
MSYS 003
ISO/IEC 27001 CERTIFIED COMPANY

Miljøfyrtårn®

mnemonic
- securing your business

What does mnemonic do?

We deliver the full range of IT security services to all types of enterprise



24x7 Security Event Monitoring
24x7 Device Management
Managed IDS/IPS Service
Managed Proxy Service
Managed SIEM Service
Threat Intelligence
Vulnerability Assessment
Incident Response

mnemonic
- securing your business

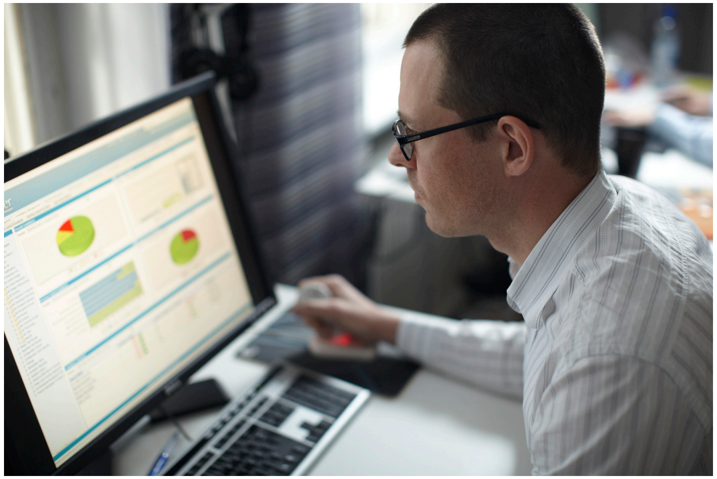
What is IDS

- Software or hardware designed to detect malicious activity on network or systems
- Anomaly / Signature based
- Network / System
- Passive / Reactive
- False positives / false negatives

Argus Managed Security Service System

The Argus MSS system is owned and developed by mnemonic. It features -

- Secure customer portal with rich analysis and reporting functionality
- Integration of multiple services
- Identical incident view for customers and security analysts that eases collaboration
- Automatic failover between Oslo and Stavanger Data Centres
- Scalable, high performance architecture



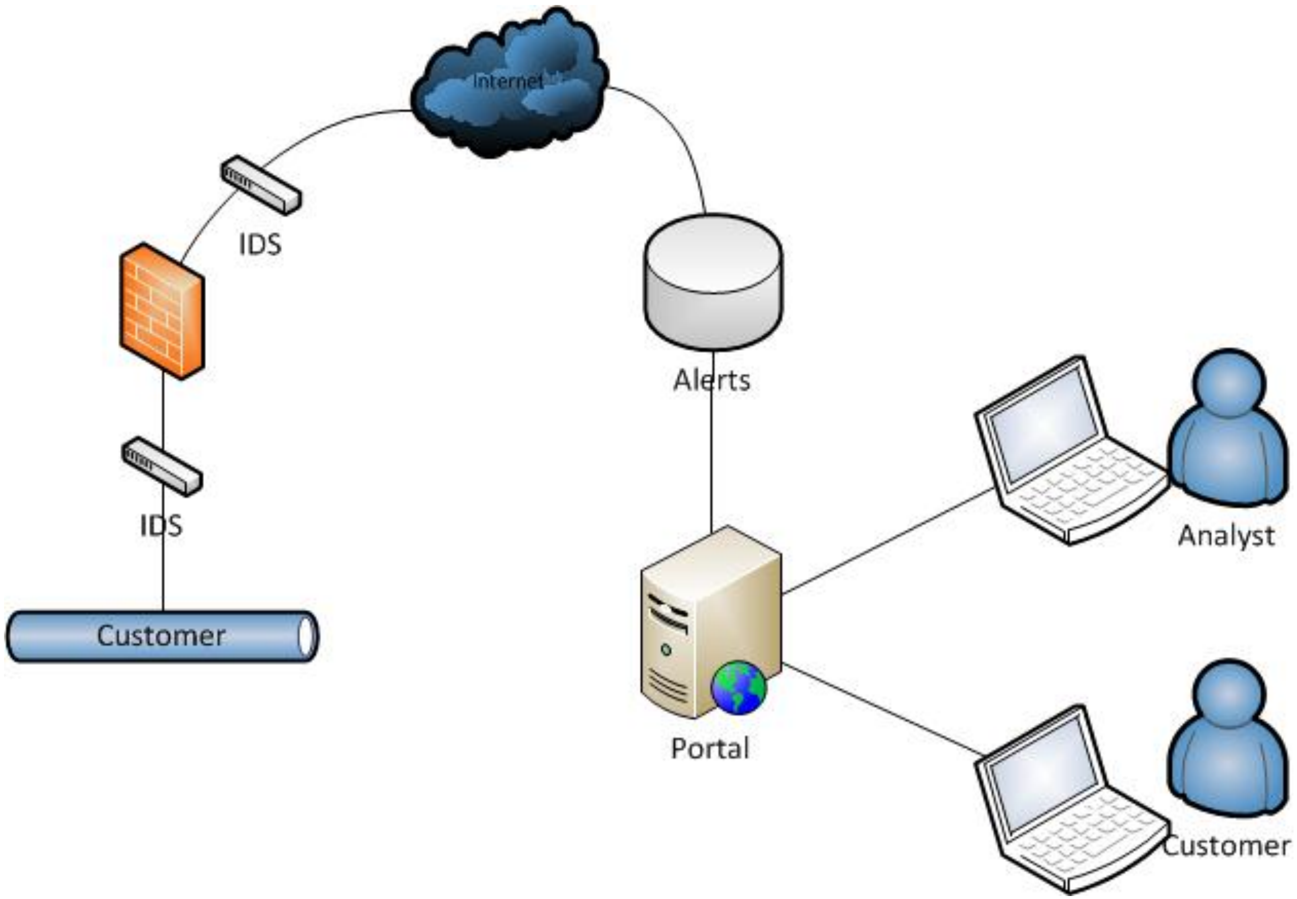
"The real-time reporting capability of the Argus customer portal gives me the information I need when I need it. This helps me demonstrate the value of our security spend"

CISO, Financial Services Business

mnemonic

- securing your business

Argus Managed Security Service System



mnemonic
- securing your business

Evolution of attacks

1990 – 2000 – Type of attacks

- Attacks against network protocols
  - Smurf (ICMP to broadcast)
  - Ping Of Death (Large fragmented ping > 65,535 bytes)
  - Ping flood (many ping packets
  - Teardrop (overlapping IP fragments)
  - WinNuke (SMB)
- Not many break ins and advanced attacks

1990 – 2000 - Attackers

Getty Images

1990 – 2000 - Motivation

1990 – 2000 – IDS coverage

- Not many NIDS-systems at the market
- Antivirus was the protection

2000 – 2005 – Type of attacks

- Worms was hot this period
- I LOVE YOU (spam VBScript)
- Anna Kournikova (spam VBScript)
- Sadmind (Defaced web sites, IIS and Solaris)
- Code Red (Defaced web sites, IIS, DOS whitehouse.gov's IP)
- Nimda (email, smb shares, infected websites, IIS vulnerability and morris/Code Red vulnerabilities, adds guest account and shares c☺
- Beast (Backdoor)
- Slammer (DOS SQL servers)
- Blaster (Spreads through RPC, DoS against windowsupdate.com)
- Netbus
- BackOrfice

2000 - 2005 - Attackers

mnemonic
- securing your business

2000 - 2005 - Motivation

2000 – 2005 – IDS coverage

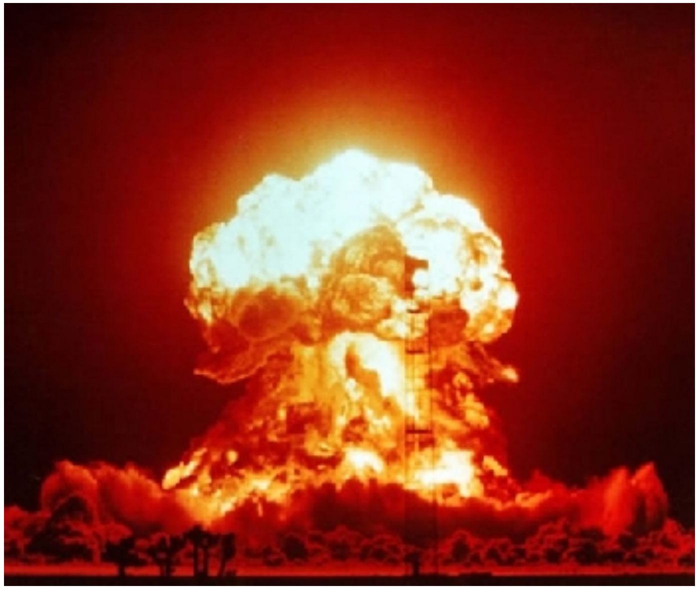
- Signature based IDS
- Some anomaly

2005 – 2010 – Type of attacks

- Metasploit becomes common
- Servers starting to be hard to exploit
- Clients and servers hidden behind firewalls
- Mail filters starting to be good, spam worms become less effective
- Attack vector switching towards clients from web-servers
- More advanced obfuscated attacks
- Exploits against client software (Adobe Reader, Flash, Java, Office)
- Exploits against humans (Fake antivirus)
- Advanced worms and botnets (Stuxnet, Storm, Koobface)
- Starting to see banking trojans (zeus, spyeye)
- Cyber attacks starting to become common criminal act
- Conficker…

2005 – 2010 - Attackers

2005 – 2010 - Motivation



mnemonic
- securing your business

2005 – 2010 – IDS coverage

- Harder to create good signatures due to obfuscation, polymorphism and fast fluxing
- Signatures for obfuscation
- Attack against clients (not only servers)
- Reputation starting to be important due to encryption of control channels

2010 – now - Attacks

- Mass infection of web pages (e.g. wordpress)
- Exploit kits
- More bank trojans (zeus source code was released)
- APT (RSA, Norwegian organisations)
- Anonymous and Lulzsec
- Duqu (stuxnet like)
- MortoA…

2010 – now - Attackers

2010 – now - Motivation

- YOUR money/information
- Political messages
- Destruction
- Espionage
- War

2010 – now – IDS coverage

- Reputation even more important
- NGFW/NGIPS
- More log sources (system logs, firewall logs, proxy logs)
- Correlation of log sources
- Our In-house developed SIEM is starting to get a lot of code to handle all the log sources

Future

- More targeted attacks and “APT”
- Attacks multiple platforms
- More bank trojans and other types of trojans

Q & A

Thanks for your time!

stian@mnemonic.no

mnemonic

– securing your business