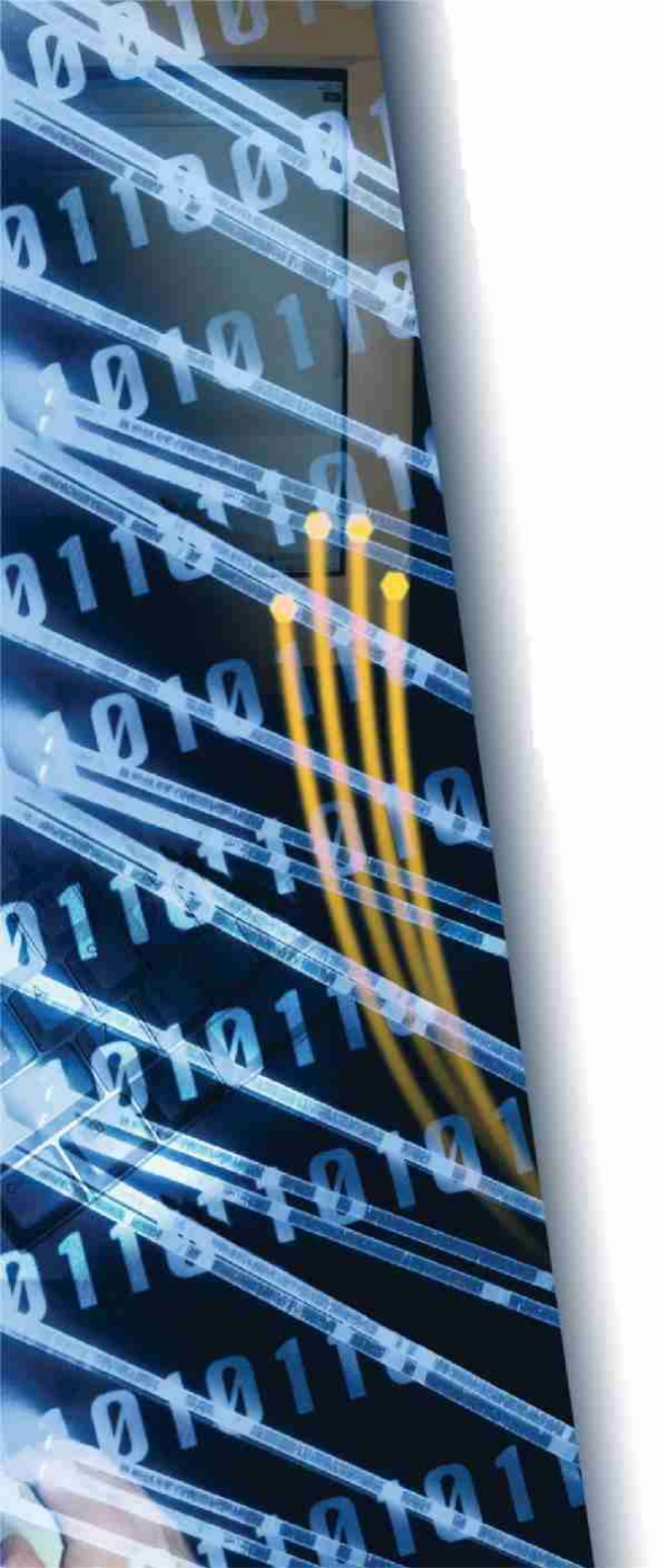


A Network of IDS-Sensors for Attack-Statistics

Till Dörges
Olaf Gellert
Klaus-Peter Kossakowski

PRESECURE®

Outline / ToC

- Outline / ToC
- Introduction
- Realisation
- Operation
- Statistics
- Conclusion / Perspectives
- Closing Remarks

PRESECURE®

Introduction: History

- **Current project evolved from eCSIRT.net**
  - Funded by European Commission
  - Improve Collaboration between European CSIRTs
  - Raise Public Awareness through Attack-Statistics
  - http://www.ecsirt.net/
- **Realisation of Distributed IDS**
  - Gather Information about Internet Attacks
  - Acquire “holistic” View

PRESECURE®

Introduction: Distributed IDS

- **Single IDS only have limited View**
  - 1 Sensor
  - Single Host
  - Single Network
- **Distributed IDS get bigger Picture**
  - n Sensors + m Managers
  - Technology / Software available
  - Problem: Deployment across administr. Domains
    - Different / Incompatible Policies
    - Trust

PRESECURE®

Outline / ToC

PRESECURE®

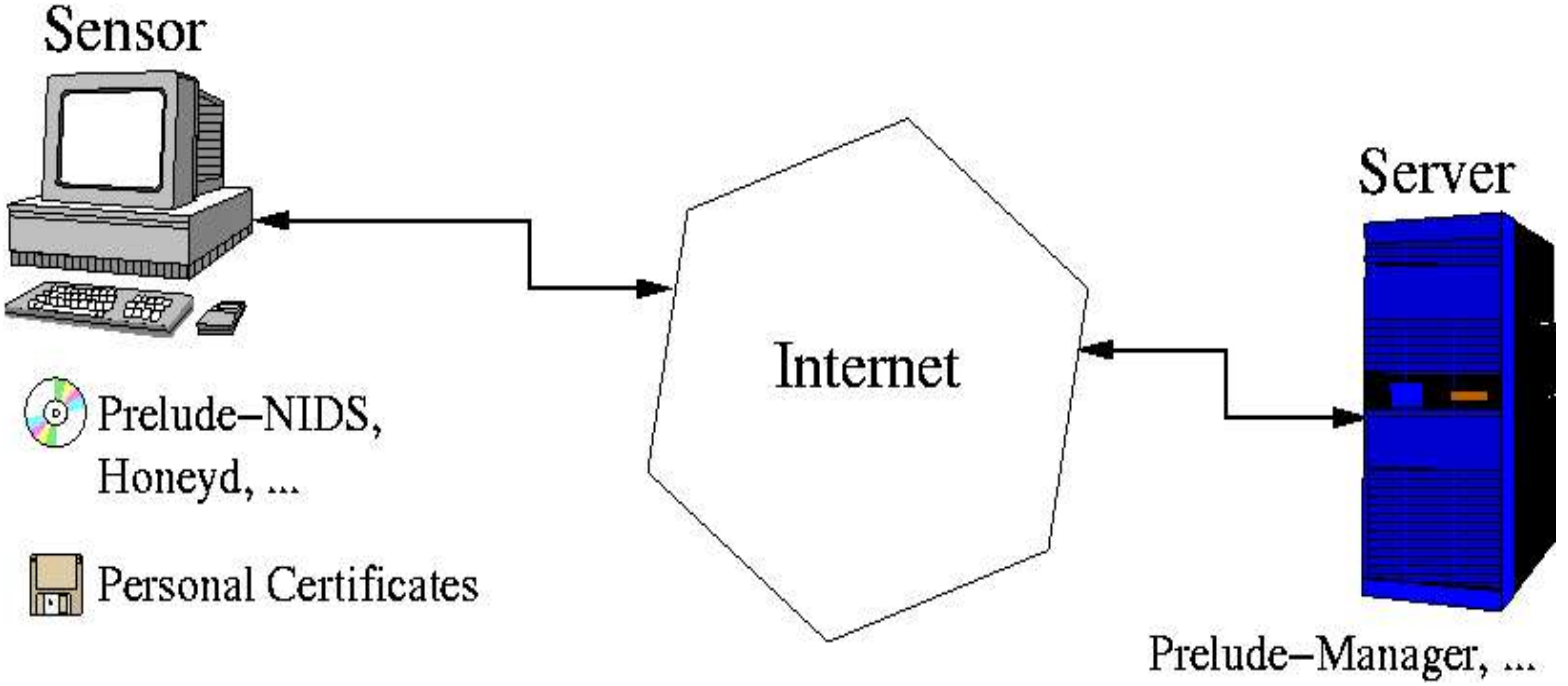
Realisation: Policy & Trust

- **Each Sensors is assigned 1 IP-Address**
- **Other IP-Addresses must not be listened to**
- **Communication between Sensor and Manager**
  - Encrypted
  - Authenticated
- **Trust-Relation between all participating Parties**
  - Common Code of Conduct
  - Strongly based on Trusted Introducer (TI)
    - http://ti.terena.nl/

PRESECURE®

Realisation: Architecture

- **Main Component:**
  Prelude (http://www.prelude-ids.org)



Realisation: Software

- **Sensors**
  - Primary Objective: Plug 'n Play
    - Simple Setup Menu
  - CDROM based on Knoppix (http://knoppix.org/)
    - Prelude-NIDS
    - Crypto-NTPD
    - Honeyd
  - Floppy containing Credentials
- **Manager**
  - Prelude-Manager
  - Crypto-NTPD

PRESECURE®

Realisation: Honeyd

- **Sensors: No “Eavesdropping” due to Policy**
  - Honeyd to help out (http://www.honeyd.org)
- **Honeyd provides attackable Services**
  - FTP TCP/21
  - SSH TCP/22
  - TELNET TCP/23
  - SMTP TCP/25
  - HTTP TCP/80
  - POP3 TCP/110
- **Problem: No complete Simulation**

Outline / ToC

PRESECURE®

Operation

- **Smooth Operation of all Components**
- **Current Sensor-Network**
  - Netherlands (2 Sensors)
  - Germany (2 Sensors)
  - Great Britain
  - Spain (2 Sensors)
  - Denmark
  - Japan
- **More Sensors always welcome!**
  - No Geographic Restrictions

Outline / ToC

PRESECURE®

Analyses: Prelude Webfrontend I

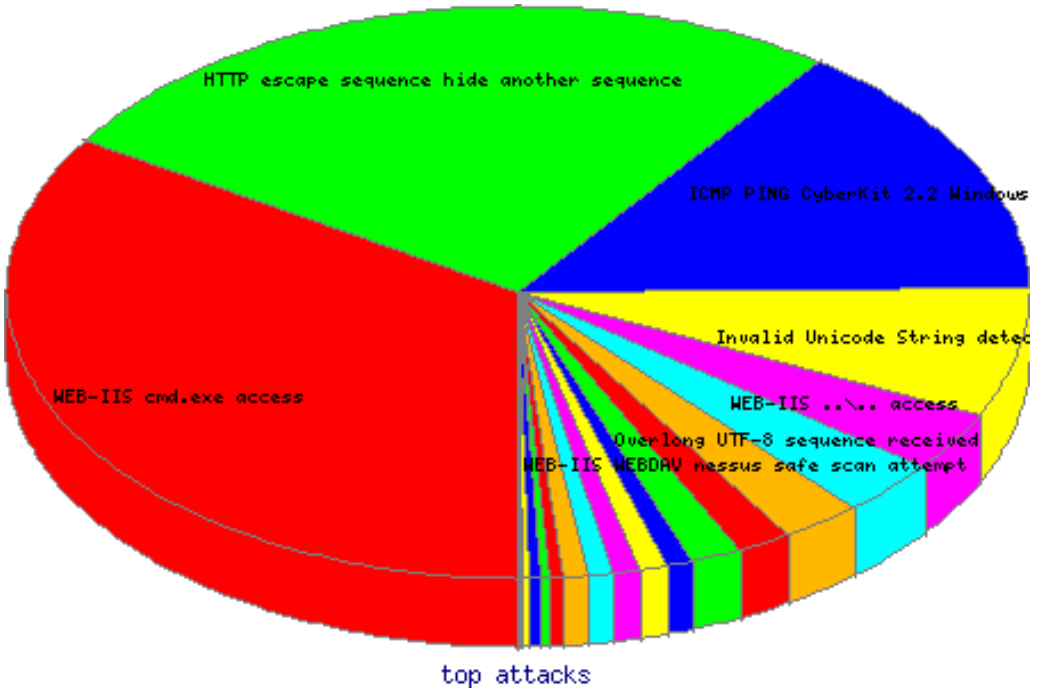
■ Top Attacking Sites

AttackNb	AttackTypeNb	TargetNb	Score	Address	Country	Host name
15681	12	1	1306.75	**213.131.73.**[redacted]	EG	[redacted].link.com.eg
6871	17	2	202.088235294118	**194.249.177.**[redacted]	SI	n/a
6617	17	1	389.235294117647	**213.136.117.**[redacted]	CI	n/a
6613	10	11	60.1181818181818	**127.0.0.1**	Unk.	localhost
6401	17	1	376.529411764706	**192.204.188.**[redacted]	US	n/a
6291	17	1	370.05882352941 2	**194.209.168.**[redacted]	CH	n/a
6282	17	1	369.529411764706	**199.6.51.**[redacted]	US	n/a
6160	20	2	154	**219.106.**[redacted]	JP	[redacted].co.jp
5597	12	1	466.416666666667	**212.0.138.**[redacted]	SD	n/a
5137	15	3	114.155555555556	**80.108.86.**[redacted]	SE	[redacted].25.11.vie.surfer.at
4894	5	3	326.266666666667	**210.212.89.**[redacted]	IN	n/a
4362	14	1	311.571428571429	**80.142.231.**[redacted]	DE	[redacted].dip.t-dialin.net
3674	5	2	367.4	**62.117.102.**[redacted]	RU	n/a
3346	10	1	334.6	**82.37.219.**[redacted]	GB	[redacted].cable.ubr07.dudl.blueyonder.co.uk
3149	17	1	185.235294117647	**211.38.233.**[redacted]	KR	n/a
2984	8	4	93.25	**61.189.240.**[redacted]	CN	n/a
2532	12	1	211	**217.255.191.**[redacted]	DE	[redacted].dip.t-dialin.net
2486	11	1	226	**80.142.231.**[redacted]	DE	[redacted].dip.t-dialin.net
2477	12	1	206.416666666667	**80.142.233.**[redacted]	DE	[redacted].dip.t-dialin.net
2460	12	1	205	**217.255.181.**[redacted]	DE	[redacted].dip.t-dialin.net

PRESECURE®

Analyses: Prelude Webfrontend II

- **Top Attacks (May 21, 2004)**
  - Most Attacks Target WWW-Services



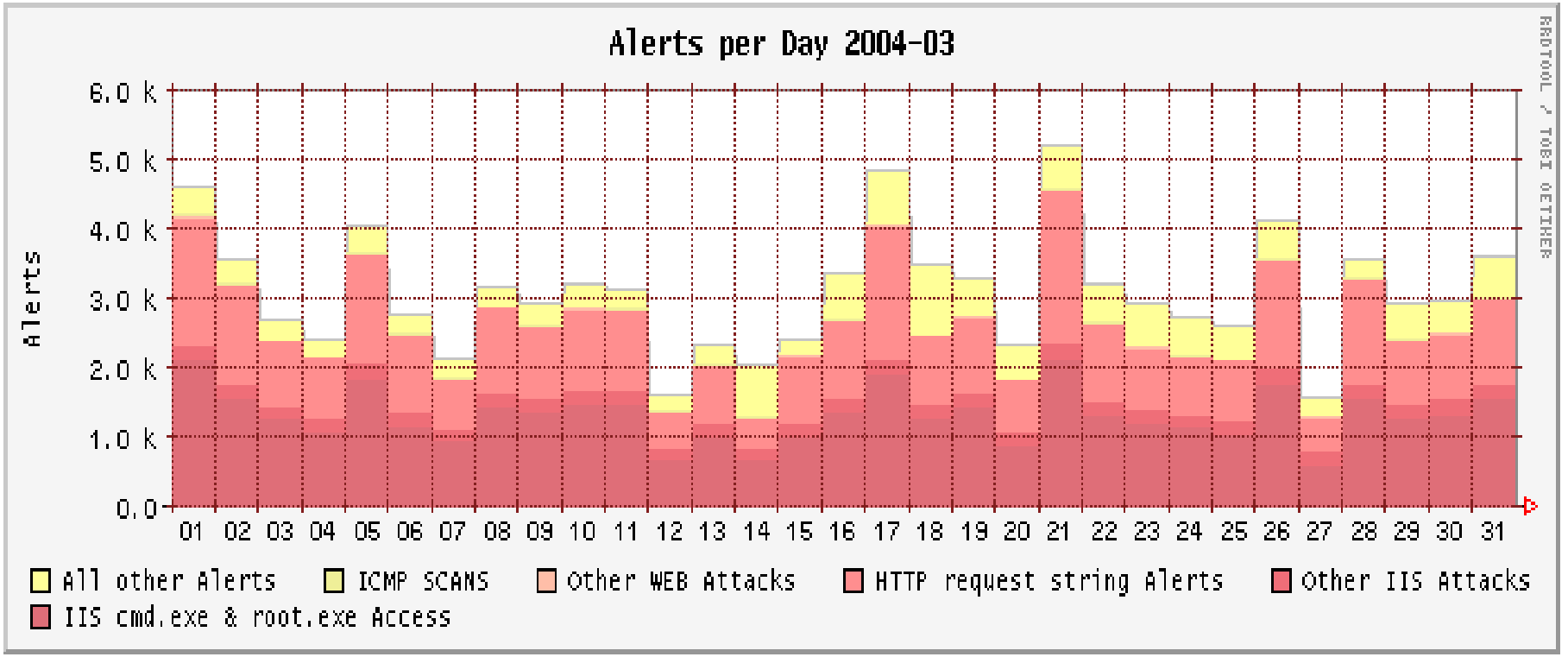
Analyses: Overviews

- **Overviews generated**
  - Daily
  - Monthly
  - Complete
- **Grouped into the these Classes**
  - IIS Access (`cmd.exe` & `root.exe`)
  - HTTP Request String Alerts
  - Other IIS Attacks
  - Other WEB Attacks
  - ICMP Scans
  - All Others

PRESECURE®

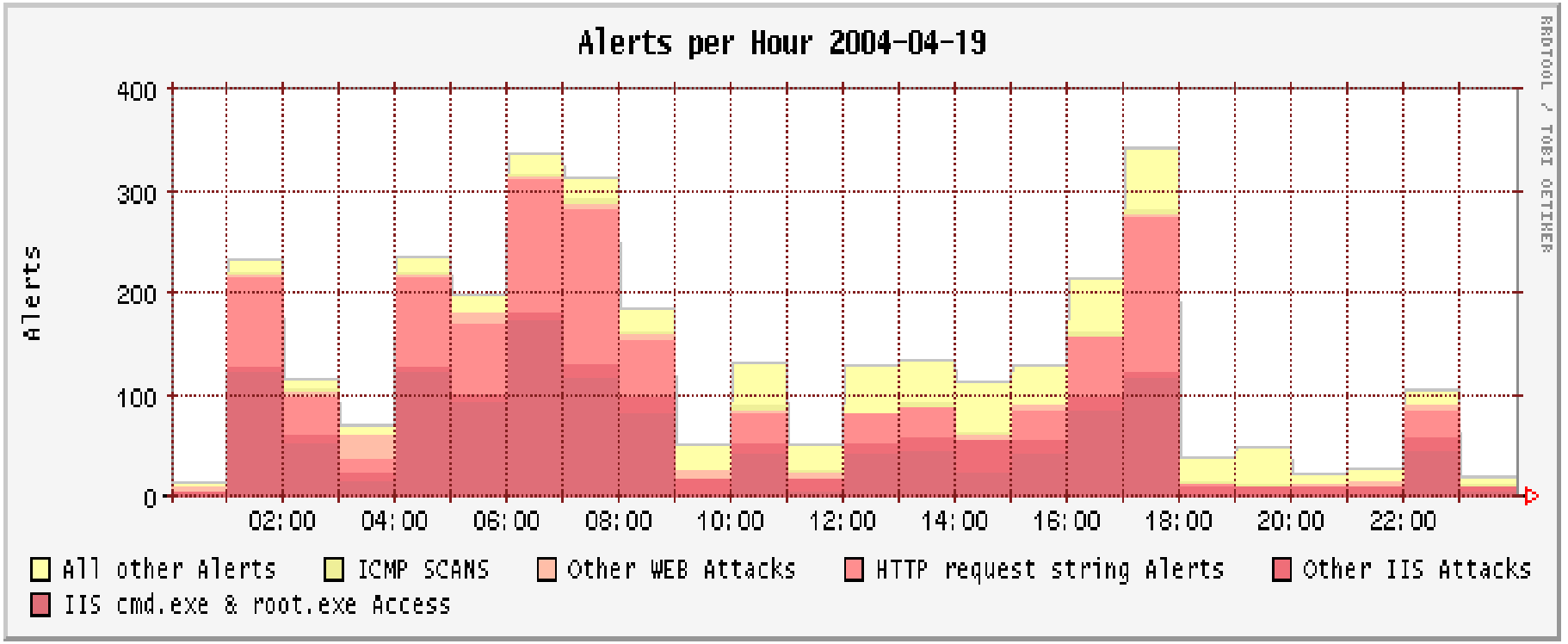
Analyses: Overviews: Example I

- Monthly Overview, Alerts per Day



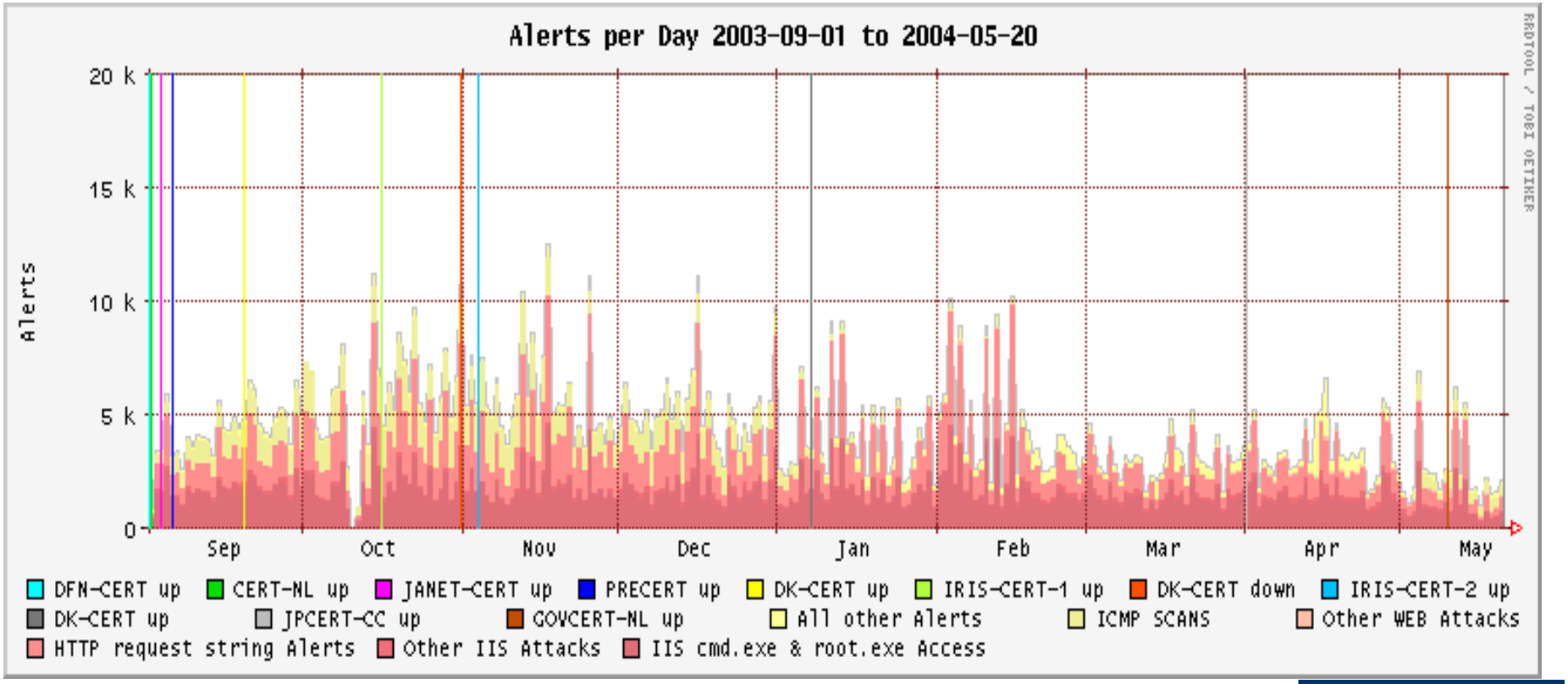
Analyses: Overviews: Example II

■ Daily Overview, Alerts per Hour



Analyses: Overviews: Example III

- Complete Overview, Alerts per Day



Analyses: Argus vs. Prelude I

- **Problem: Prelude only sees, what it knows**
  - Prelude-NIDS is a Signature-Based IDS
  - Most Attacks Require Answers from Victim
- **Argus for Different Perspective**
  - http://www.qosient.com/argus/
  - Records Connections / Statistics
- **Comparison for PRESECURE-Sensor**
  - Prelude: “Alert” (Match against Rule)
  - Argus: “Connection” (SYN-Packet)

Analyses: Argus vs. Prelude II

■ Access by Ports for PRESECURE-Sensor

Port	Argus (PS)		Prelude (PS)		Prelude (Total)	
21/tcp (h)	**10091**	*8,87%*	**1333**	*2,61%*	**8073**	*0,87%*
22/tcp (h)	**182**	*0,16%*	**20**	*0,04%*	**55**	*0,01%*
23/tcp (h)	**137**	*0,12%*	**1**	*0,00%*	**17**	*0,00%*
25/tcp (h)	**400**	*0,35%*	**1**	*0,00%*	**52**	*0,01%*
80/tcp (h)	**23407**	*20,58%*	**45131**	*88,53%*	**887597**	*95,32%*
110/tcp(h)	**47**	*0,04%*		*0,00%*	**14**	*0,00%*
135/tcp	**47883**	*42,11%*		*0,00%*	**5**	*0,00%*
137/udp	**4065**	*3,57%*		*0,00%*	**3**	*0,00%*
139/tcp	**2302**	*2,02%*		*0,00%*		*0,00%*
445/tcp	**5704**	*5,02%*		*0,00%*	**4**	*0,00%*
1080/tcp	**600**	*0,53%*	**1022**	*2,00%*	**3416**	*0,37%*
1434/udp	**2015**	*1,77%*	**1983**	*3,89%*	**8939**	*0,96%*
Not Incl.	***16879***	*14,84%*	***1488***	*2,92%*	***22997***	*2,47%*
Total	**113712**		**50979**		**931172**	

Analyses: Different Attacks

■ Attackers try more than 1 Attack

# Attacks	1	2	3	4	5	6	...	143	159	235
2003-09	13381	2393	1260	107	656	26	...			
2003-10	13547	3311	210	165	581	94	...			
2003-11	14027	3508	50	46	561	42	...	1		
2003-12	16472	6234	38	32	573	50	...			
2004-01	3595	1239	1363	60	502	51	...			
2004-02	3399	689	1381	56	465	41	...		1	1
2004-03	5831	474	1080	59	464	42	...			
2004-04	8475	625	871	40	383	38	...			
Total	**78727**	**18473**	**6253**	**565**	**4185**	**384**	**...**	**1**	**1**	**1**

Analyses: Different Sensors Attacked

- **Attackers attack different Sensors**

# Sensors	1	2	3	4	5	6
2003-09	17543	267	32	6		
2003-10	17426	360	109	48	42	1
2003-11	17995	211	37	9		
2003-12	23192	175	33	20		
2004-01	6459	319	34	12	7	
2004-02	5705	305	22	20	8	
2004-03	7629	280	31	18	17	
2004-04	10074	312	38	12	6	13
Total	**106023**	**2229**	**336**	**145**	**80**	**14**

Analyses: Mean Time Between Attack(er)s

- **~ 14000 Attackers per Month (Sep 03 – Mar 04)**
- **~ 2000 Attackers per Month per Sensor**
- **~ 3 Attackers per Hour per Sensor**
- **Average System Connected to Internet**
  - ~ 20 Minutes between Attackers
- **Only very Cautious Estimation**
  - Attackers try ~ 1.5 Different Attacks
  - Prelude doesn't see all Attacks

PRESECURE®

Outline / ToC

PRESECURE®

Conclusion / Perspectives

- **Successful Operation for over 10 Months**
- **Interesting Data Gathered**
- **Analyses (somewhat) limited**
- **Number of Sensors still increasing**
- **Active Development of Sensor-Technology**
  - Automatic Updates of Signatures
  - Argus to be Included
- **Participants Welcome**

PRESECURE®

Outline / ToC

PRESECURE®

Contacting the Authors

- **Till Dörges**
  - td@pre-secure.de PGP-Key: 0x22A13E69
  - 2226 8447 3251 F6BE F8DC 6D4D 2F54 E55F
- **Olaf Gellert**
  - og@pre-secure.de PGP-Key: 0x799241C1
  - 6C6D E613 BEE4 1D6D B14B D266 2383 A735
- **Klaus-Peter Kossakowski**
  - kpk@pre-secure.de PGP-Key: 0x38B56E3D
  - 5B21 A75D 0820 1A93 835C 6EE3 4D1B F050

The End (of the Beginning...)

More Participants / Sensors are Welcome!

Thank You for Your Attention!

Questions?

PRESECURE®