

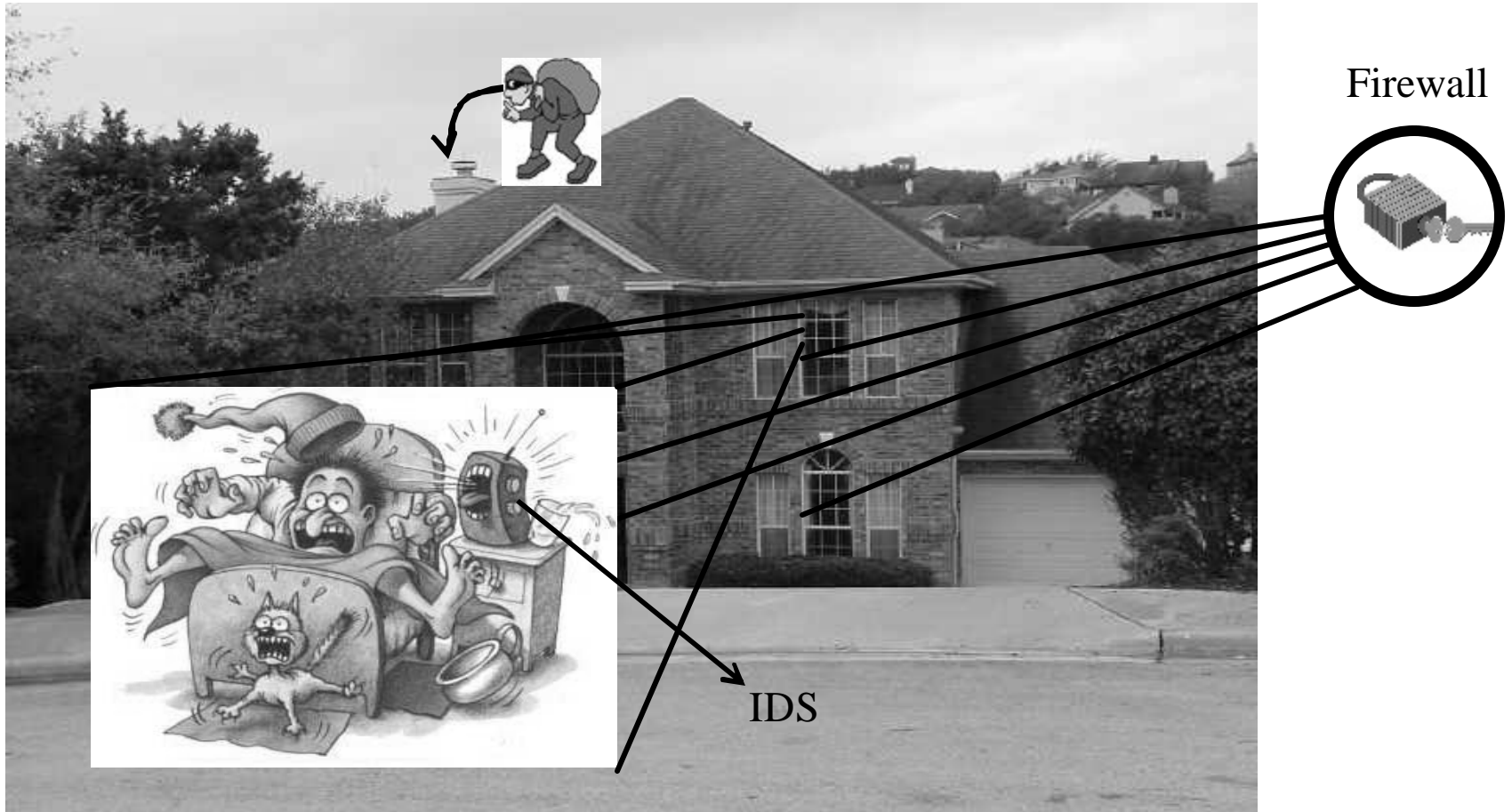
Firewalls and IDS

Sumitha Bhandarkar
James Esslinger

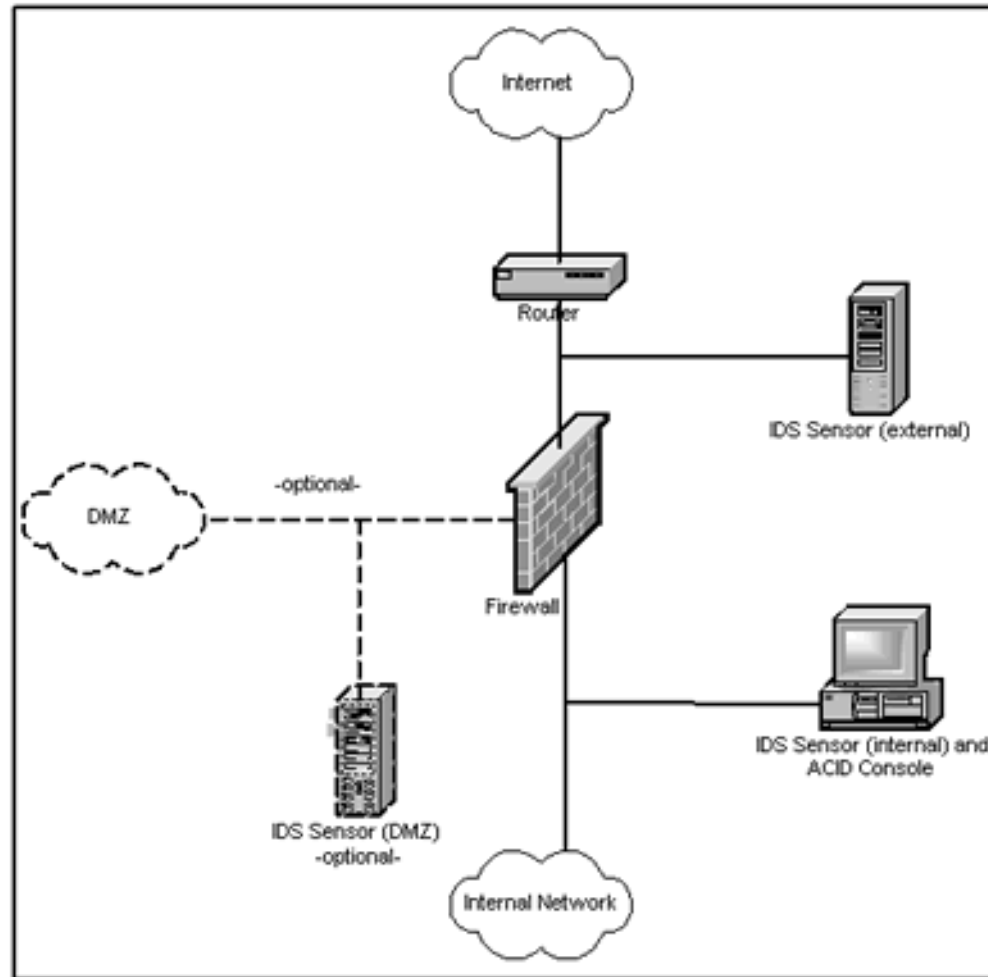
Outline

- Background
 - What are firewalls and IDS ?
 - How are they different from each other ?
- Firewalls
 - Problems associated with conventional Firewalls
 - Distributed Firewalls
 - Some of the implementations of distributed firewalls
- IDS
 - Types of IDS and uses
 - Granidt – A hardware based NIDS
 - Honeynets
- Conclusions

Background



Background (Cont.)



Conventional Firewalls

Characteristics

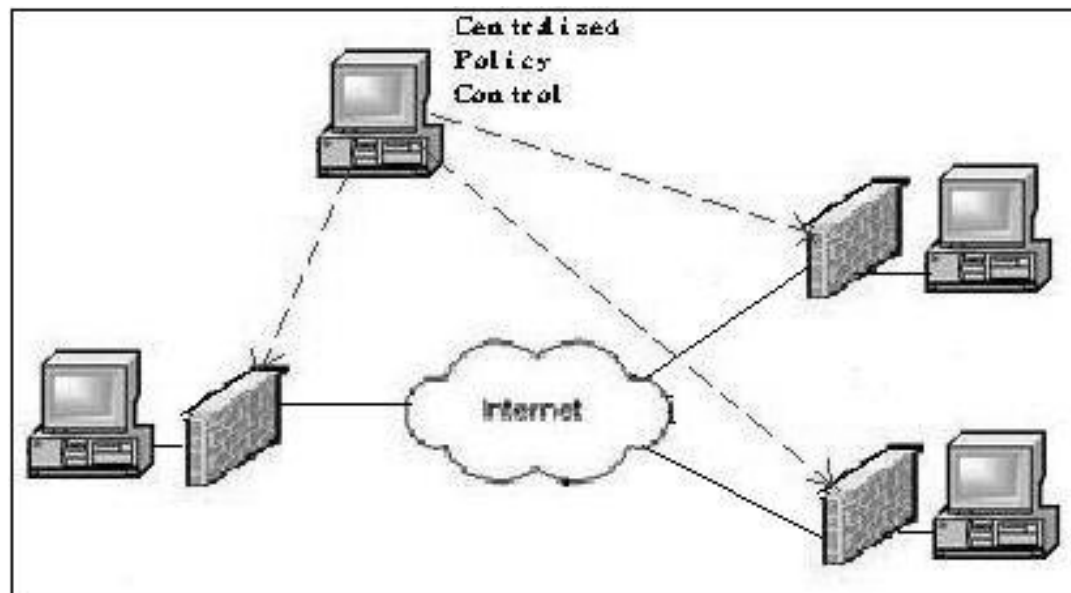
- Topology dependent
- Choose between “triangle routing” or “lowered security”
- Do not protect from internal attacks
- Problematic to handle end-to-end encrypted packets
- Application level proxies needed for applications like FTP and RealAudio
- Single point of failure
- Can become network bottleneck

*But they offer **centralized** policy control !*

Distributed Firewalls

Framework

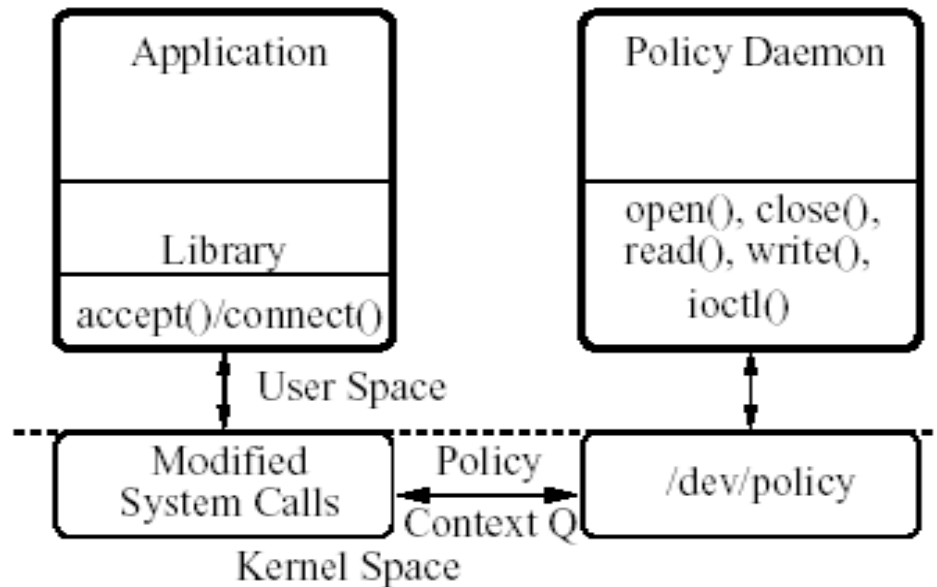
- Centralized Policy control / Distributed Policy enforcement
 - (a) Security policy language
 - (b) Policy Distribution Scheme
 - (c) Authentication and Encryption Mechanism



Distributed Firewalls

Prototype

- Software implementation on OpenBSD platform
- *Keynote* used as the policy language
- IPsec used for distribution, authentication and encryption
- Filtering : focus on TCP traffic ; operates at connection level



Distributed Firewalls

Prototype

- Software implementation: user level or kernel level?
 - User-level code is easy to tamper
 - Kernel level code requires the kernel to be rebuilt for upgrades
- Additional “latency” while policy daemon verifies the credentials
 - Will overhead be too high if implementation is packet-based instead of connection-based?
- Additional context switching between kernel and userspace for policy verification (in current implementation)
- Application level (FTP, Real Audio etc) filtering can be handled easily

Distributed Firewalls

Alternate Design

Autonomic Distributed Firewall (ADF) - “Embedded Firewall”

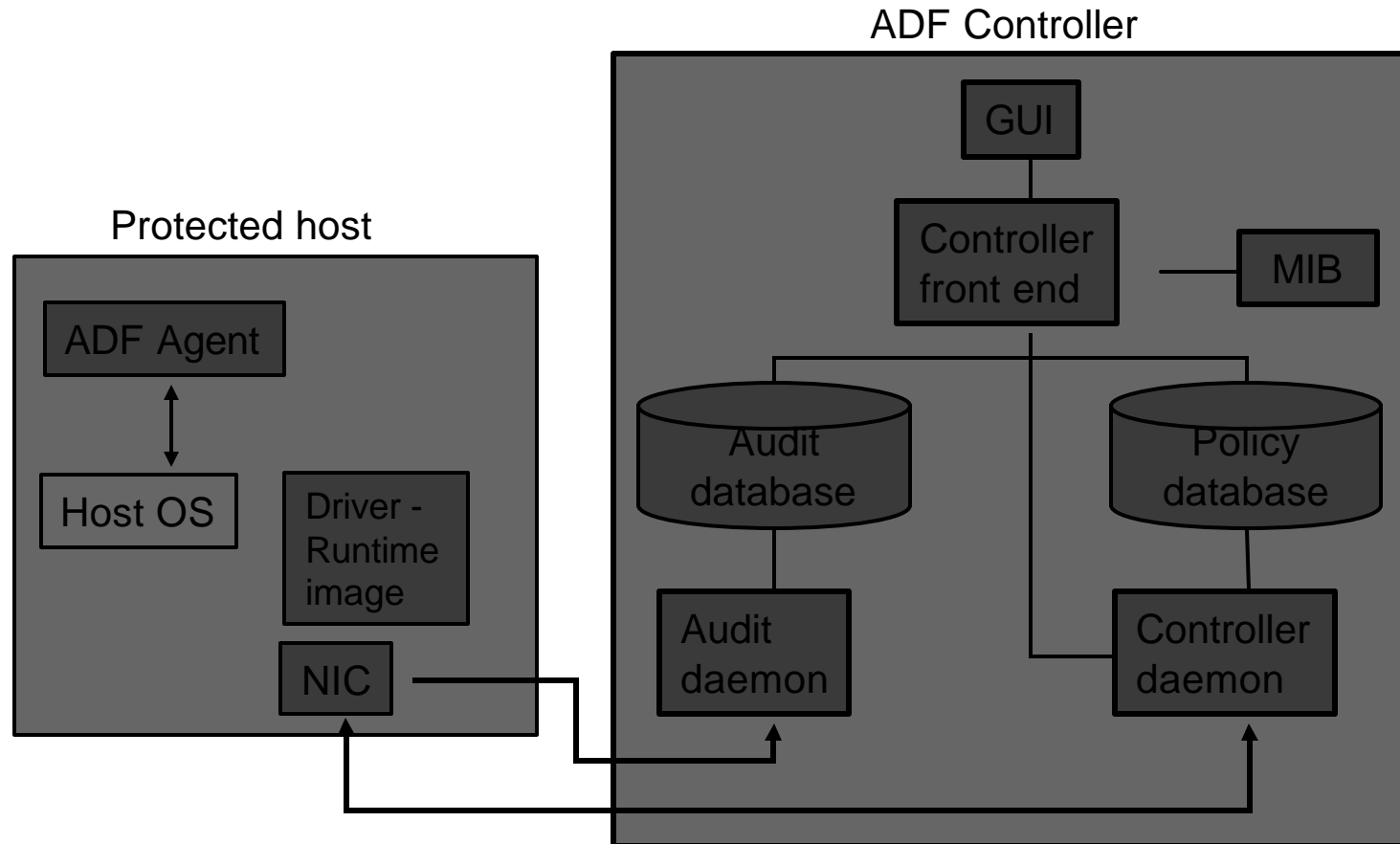
- DARPA funded project built by Secure Computing using 3com NIC
- Processor/Memory/Encryption engine embedded on NIC
- Embedded firewall provides protection against vulnerabilities in the OS
- Uses master-slave architecture to provide scalability & centralized security policy management
- Hybrid solution - the ADF to be used to *complement* conventional perimeter firewall and *NOT replace* it.
- No sniffing; No spoofing; Audit request can be tagged with individual rules; Emergency rule set can be used for controlling the behavior of all the NICs using the push of a single button.

1. <http://www.blackhat.com/presentations/bh-usa-01/JelattisPapps/bh-usa-01-Jelattis-Pappas.ppt>.

2. Charles Payne, Tom Markham, "Architecture and Applications for a Distributed Embedded Firewall", 17th Annual Computer Security Applications Conference, December 2001.

Distributed Firewalls

Alternate Design (Cont.)



1. <http://www.blackhat.com/presentations/bh-usa-01/JelattisPapps/bh-usa-01-Jelattis-Pappas.ppt>.

2. Charles Payne, Tom Markham, "Architecture and Applications for a Distributed Embedded Firewall", 17th Annual Computer Security Applications Conference, December 2001.

Distributed Firewalls

Alternate Design (Cont.)

Autonomic Distributed Firewall (ADF) - “Embedded Firewall”

- Simple test by PC Magazine showed 3COM embedded firewall to be better than conventional software firewalls.
- Reduces CPU load by offloading firewall/VPN/IPSec functionality to NIC.
- Scaleable, transparent, (largely) tamper-resistant solution.
- Application filtering is hard.
- Limited memory on the NIC allows only 64 policy rules.
- Solution is not as cost-effective as claimed (Policy server prices at ~ 300USD, each NIC ~100 - 250 USD).
- No gigabit support (yet).

1. <http://www.blackhat.com/presentations/bh-usa-01/JelattisPapps/bh-usa-01-Jelatis-Pappas.ppt>.

2. Charles Payne, Tom Markham, "Architecture and Applications for a Distributed Embedded Firewall", 17th Annual Computer Security Applications Conference, December 2001.

Intrusion Detection Systems (IDS)

- The ultimate goal of IDS is to identify all attacks while not identifying regular activity as an attack.
- Two types of IDS
 - Host-based
 - Has the ability to interact with applications to provide more information than a network-based IDS.
 - Can report intrusions that would not normally cause any external anomalies.
 - Network-based
 - Can collect data for all traffic on the network.
 - Central point of failure.
- Anomaly based detection
- Signature based detection

-
1. John McHugh, Alan Christie, Julia Allen, "Defending Yourself: The Role of Intrusion Detection Systems," IEEE Software, pp. 42-51. October 2000.
 2. Gerald Tripp, "An Intrusion Detection System for Gigabit Networks," University of Kent, 2003.

Network IDS

(NIDS)

- Another level of defense to be employed along with firewalls.
- Can provide administrators with information such as if the firewall is working as intended.
- Will have to monitor all packets that arrive with the headers and content being examined.
- This is computationally expensive and software implementation may not be able to handle the load.
- As data transmission rates increase, packets may get past the NIDS and thus a system that can handle the load is needed.
- Software NIDS maxes out on approximately a 100 Mb/s link.

Gigabit Networks

- Software implementations of NIDS will not be of any use on high bandwidth networks.
- Hardware implementations are being researched to help detect intrusions on gigabit networks.
- Non-Deterministic Finite Automata and Deterministic Finite Automata can be used to help increase the speeds at which regular expressions are matched.
- IDS can be used on each host which helps to mitigate the problem, but does not allow for network-based IDS.
- Granidt is a work in progress that is a NIDS that is made from hardware and software.

1. Gerald Tripp, "An Intrusion Detection System for Gigabit Networks," University of Kent, 2003.

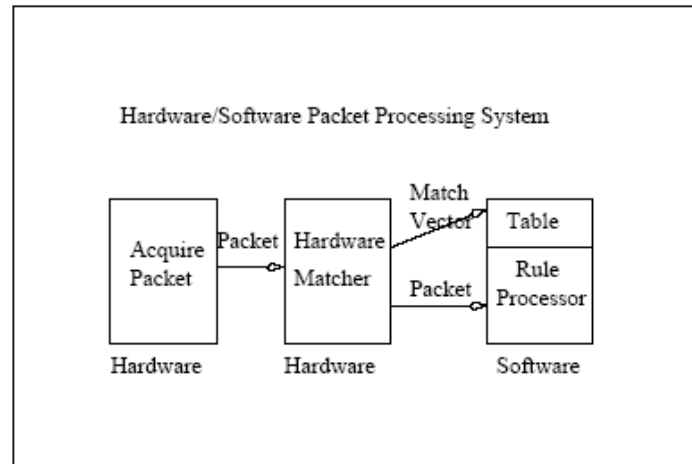
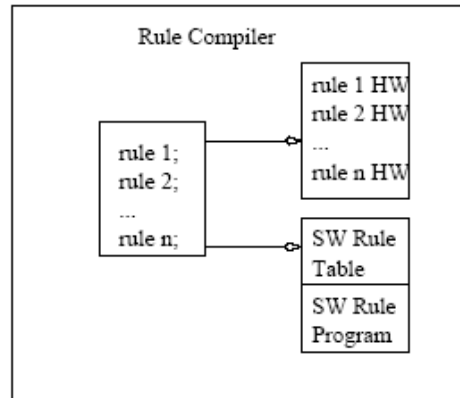
2. Maya Gokhale, Dave Dubois, Andy Dubois, Mike Boorman, Steve Poole, Vic Hogsett, "Granidt: Towards Gigabit Rate Network Intrusion Detection Technology," Los Alamos National Laboratory, 2002.

Granidt

Hardware NIDS

- Uses Field Programmable Gate Arrays (FPGAs) to compare packets against a database which is based on a subset of Snort rules.
- Two sets of logic circuits employed to compare data.
 - One compares the packet headers.
 - Another to compare the packet content to known packet content strings.
- Once a packet is successfully detected, the packet is sent to software for processing.
- The FPGAs are flexible and allow new rules to be added without the need of recompiling the hardware.
- The rules are stored in Content Addressable Memories.
- The FPGAs search for matches in the CAMs and then pass successful matches to software.

Granidt



1. Maya Gokhale, Dave Dubois, Andy Dubois, Mike Boorman, Steve Poole, Vic Hogsett, "Granidt: Towards Gigabit Rate Network Intrusion Detection Technology," Los Alamos National Laboratory, 2002.

What is a HoneyNet?

- Intrusion Detection Systems can be used to go on the offensive.
- Allows real data to be collected on the threats existing on the network.
- A collection of honeypots which is intended to attract potential intruders.
- The honeypots have no productive value and are only used to gather information of the types of threats present.
- The honeypots must report the data collected over some medium other than that of the public network.

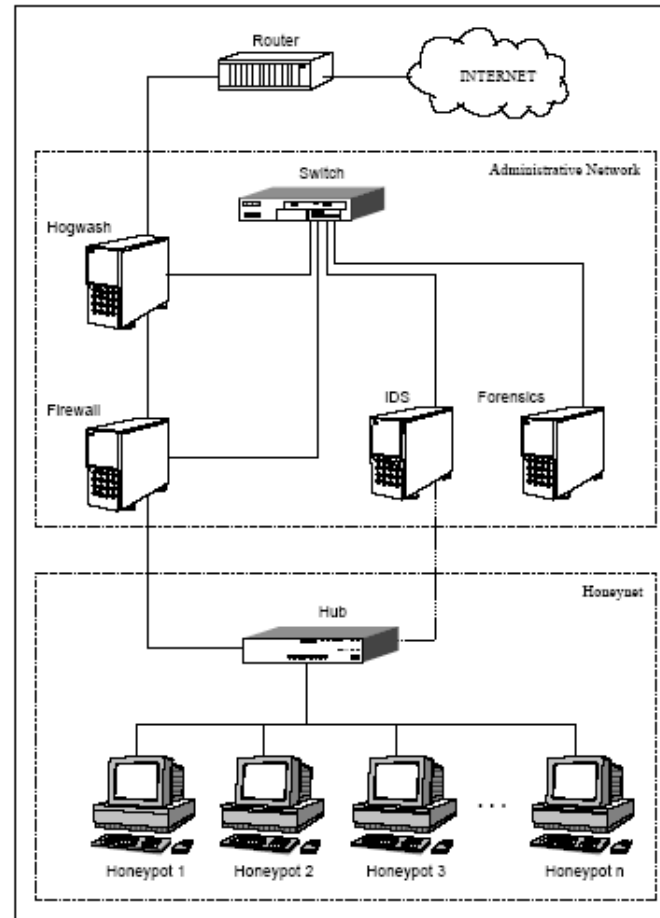
Honeypots?

- A system that is created as a decoy to deceive intruders into attempting a break-in.
- Each honeypot must run a host-based IDS in order to collect data which can be later examined for potential threats.
- Must appear as a productive system, without actually being productive.



-
1. Honey.net.org, "Know Your Enemy: Honeynets," November 2003.
<http://www.honey.net.org/papers/honey.net/index.html>.
 2. Image courtesy of <http://www.machaon.ru/pics/pooh/winni.jpg>

Diagram of a Honeyynet



1. Image courtesy of <http://www.nbso.nic.br/docs/papers/hnbr-first2003.pdf>

Honeynets

Risks

- Systems that are part of the Honeynet can be potentially used to attack systems that are not part of the Honeynet.
- Once the Honeynet is detected by an attacker, the value of the Honeynet is reduced.
- If the functionality of the Honeynet is disabled, attacks may proceed without the administrators knowledge.
- There is the risk that the compromised machines may be used for criminal activity and the Honeynet owner could be held responsible.

Honeynets

Effectiveness

- In order for a Honeynet to be effective, it has to must appear real to potential intruders.
- If the machines are comprised easily then the IDS could be comprised as well, leaving the administrator with little or no information.
- The honeypots should not be interacted with by normal users.
- If no interaction occurs, any activity on these systems can be considered to be potentially malicious and should be reviewed.

Honeynets

- The integration IDS and multiple honeypots is a tool for administrators to gain real data of the threats existing on the network.
- There are risks involved when deploying Honeynets. A risk threshold must be maintained and a course of action must be taken when this threshold is reached, such as shutting the Honeynet down.
- A reverse firewall should be used of the Honeynet to reduce the risk of attacks originating from within the Honeynet.
- Legalities of Honeynets?

Conclusion

- The technologies are very useful in securing networks when used correctly.
- Hardware and software solutions are available for IDS and Firewalls – select what suits your needs best.
- It is up to the administrators to stay one step ahead of adversaries and these technologies help them do so.

References

1. Frank Neugebauer, “Intrusion Detection : Knowing when someone is knocking on your door”
<http://www.linux-tip.net/workshop/ids-snort/ids-snort.htm>
2. Steven M. Bellovin, “Distributed Firewalls”, ;login:, pp. 37-39, November 1999.
3. Daniel Wan, “Distributed Firewall”, GSEC Practical Assignment Version 1.2c.
4. Sotiris Ioannidis, Angelos D. Keromytis, Steve M. Bellovin and Jonathan M. Smith, “Implementing a Distributed Firewall”, Proceedings of the 7th ACM Conference on Computer and Communications Security, November 2000, Athens, Greece
5. <http://www.blackhat.com/presentations/bh-usa-01/JelattisPapps/bh-usa-01-Jelatis-Pappas.ppt>
6. Charles Payne, Tom Markham,”Architecture and Applications for a Distributed Embedded Firewall”, 17th Annual Computer Security Applications Conference, December 2001.
7. Gerald Tripp, “An Intrusion Detection System for Gigabit Networks,” University of Kent, 2003.
8. Maya Gokhale, Dave Dubois, Andy Dubois, Mike Boorman, Steve Poole, Vic Hogsett, “Granidt: Towards Gigabit Rate Network Intrusion Detection Technology,” Los Alamos National Laboratory, 2002.
9. Honey.net.org, “Know Your Enemy: Honeynets,” November 2003.
<http://www.honey.net.org/papers/honey.net/index.html>
10. John McHugh, Alan Christie, Julia Allen, “Defending Yourself: The Role of Intrusion Detection Systems,” IEEE Software, pp. 42-51. October 2000.

Questions?