External Threats

Information Security

Hans Georg Schaathun

University of Surrey

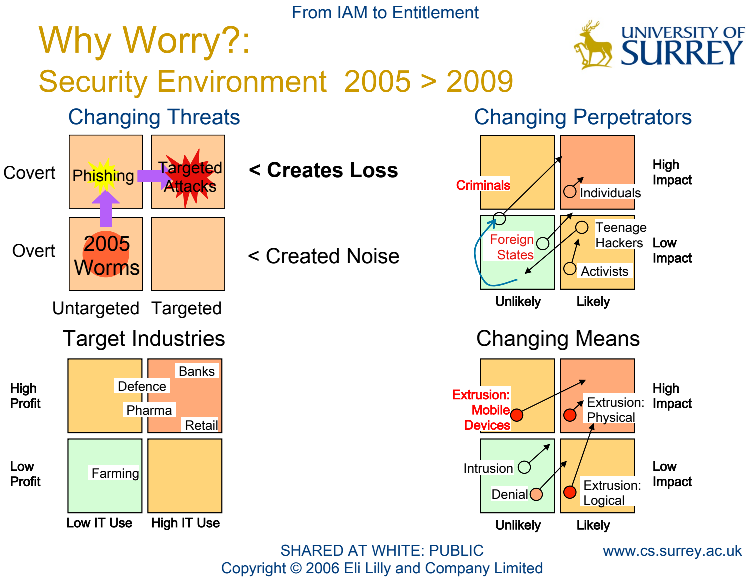
Autumn 2011 – Week 11

Outline

Session objectives

After this session, the student will

- have an overview of external threats and associated vulnerabilities.
- be familiar with the operation of intrusion detection systems



From IAM to Entitlement

Why Worry?:

Security Environment 2005 > 2009

UNIVERSITY OF SURREY

Changing Threats

Covert: Phishing → Targeted Attacks — < **Creates Loss**

Overt: 2005 Worms — < Created Noise

Untargeted | Targeted

Changing Perpetrators

High Impact: Criminals, Individuals

Low Impact: Foreign States, Teenage Hackers, Activists

Unlikely | Likely

Target Industries

High Profit: Defence, Banks, Pharma, Retail

Low Profit: Farming

Low IT Use | High IT Use

Changing Means

High Impact: Extrusion: Mobile Devices, Extrusion: Physical

Low Impact: Intrusion, Denial, Extrusion: Logical

Unlikely | Likely

SHARED AT WHITE: PUBLIC

www.cs.surrey.ac.uk

HØGSKOLEN I ÅLESUND
Aalesund University College

Outline

Demilitarised Zone (DMZ)

What do we mean be a Demilitarized Zone? Firstly, non-IT case.

- Demilitarized – not actively controlled by any party
- Buffer zone.
  - pull back to defend core realm
  - keep away from border to avoid provocation

Demilitarised Zone (DMZ)

What do we mean be a Demilitarized Zone? Firstly, non-IT case.

- Demilitarized – not actively controlled by any party
- Buffer zone.
  - pull back to defend core realm
  - keep away from border to avoid provocation

DMZ on a network

What is a DMZ in an IT (network) context?

- Network segment under limit security control
- *Why* do we have a DMZ?
- Need to offer public services
  - thus requiring reduced controls
- Placing such services in DMZ,
  - we can maintain tight controls on main LAN.
- Classic perimeter thinking
  - Inner castle walls, for invitees only
  - Outer courtyard is a public place
    - just monitored and guarded

DMZ on a network

What is a DMZ in an IT (network) context?

- Network segment under limit security control
- *Why* do we have a DMZ?
- Need to offer public services
  - thus requiring reduced controls
- Placing such services in DMZ,
  - we can maintain tight controls on main LAN.
- Classic perimeter thinking
  - Inner castle walls, for invitees only
  - Outer courtyard is a public place
    - just monitored and guarded

DMZ on a network

What is a DMZ in an IT (network) context?

- Network segment under limit security control
- *Why* do we have a DMZ?
- Need to offer public services
  - thus requiring reduced controls
- Placing such services in DMZ,
  - we can maintain tight controls on main LAN.
- Classic perimeter thinking
  - Inner castle walls, for invitees only
  - Outer courtyard is a public place
    - just monitored and guarded

DMZ on a network

What is a DMZ in an IT (network) context?

- Network segment under limit security control
- *Why* do we have a DMZ?
- Need to offer public services
  - thus requiring reduced controls
- Placing such services in DMZ,
  - we can maintain tight controls on main LAN.
- Classic perimeter thinking
  - Inner castle walls, for invitees only
  - Outer courtyard is a public place
    - just monitored and guarded

Risk analysis versus DMZ

What role would DMZ take in a risk model/risk analysis?

- Different risk profiles
- DMZ
  - very exposed – high probability of loss
  - limited assets – limited loss magnitude
- inner LAN
  - unexposed – limited probability of loss
  - all assets are present – very high potential loss magnitude

Why not have more than two profiles?

Risk analysis versus DMZ

What role would DMZ take in a risk model/risk analysis?

- Different risk profiles
- DMZ
  - very exposed – high probability of loss
  - limited assets – limited loss magnitude
- inner LAN
  - unexposed – limited probability of loss
  - all assets are present – very high potential loss magnitude

Why not have more than two profiles?

Risk analysis versus DMZ

What role would DMZ take in a risk model/risk analysis?

- Different risk profiles
- DMZ
  - very exposed – high probability of loss
  - limited assets – limited loss magnitude
- inner LAN
  - unexposed – limited probability of loss
  - all assets are present – very high potential loss magnitude

Why not have more than two profiles?

Outline

Intrusion detection systems

- Intrusion Detection Systems (IDS)
  - passive devices – monitors and alerts
- Network-based IDS (NIDS)
  - monitors all traffic on a subnet or across a boundary
- Host-based IDS (HIDS)
  - monitors data and processes on a single host
- Intrusion Prevention Systems (IPS)
  - active devices
  - IDPS : detection and prevention

Outline

Where is the device?

Network-Based IDS (NIDS)

- A NIDS is usually a dedicated device on the network.
- Could it alternatively run on a router or gateway?
- Independent passive device is invisible to attackers.
- Controls on a router might be vulnerable to attacks on the router

Where is the device?

Network-Based IDS (NIDS)

- A NIDS is usually a dedicated device on the network.
- Could it alternatively run on a router or gateway?
- Independent passive device is invisible to attackers.
- Controls on a router might be vulnerable to attacks on the router

Location in the network

Where do you place the device to control your network?

- Most obvious choice is close to gateway
- Monitoring all traffic into and out of the LAN
- May also need monitoring of internal

Location in the network

Where do you place the device to control your network?

- Most obvious choice is close to gateway
- Monitoring all traffic into and out of the LAN
- May also need monitoring of internal

Location in the network

Where do you place the device to control your network?

- Most obvious choice is close to gateway
- Monitoring all traffic into and out of the LAN
- May also need monitoring of internal

How do you connect the device?

Network-Based IDS (NIDS)

How do you place your NIDS to monitor all traffic?

- Problem : Switches.
- Switches do not flood the network
  - a NIDS connected directly to a switch will be in the dark
- Some switches have a monitoring port for this purpose
  - but may not be able to keep up with all the traffic
  - yet, it may be the best solution.
- It is easier with a hub ...

How do you connect the device?

Network-Based IDS (NIDS)

How do you place your NIDS to monitor all traffic?

- Problem : Switches.
- Switches do not flood the network
  - a NIDS connected directly to a switch will be in the dark
- Some switches have a monitoring port for this purpose
  - but may not be able to keep up with all the traffic
  - yet, it may be the best solution.
- It is easier with a hub ...

How do you connect the device?

Network-Based IDS (NIDS)

How do you place your NIDS to monitor all traffic?

- Problem : Switches.
- Switches do not flood the network
  - a NIDS connected directly to a switch will be in the dark
- Some switches have a monitoring port for this purpose
  - but may not be able to keep up with all the traffic
  - yet, it may be the best solution.
- It is easier with a hub ...

What can we look for?

TCP/IP

Application

Link/Physical Layer

You might need multiple devices to manage all of it ...

What can we look for?

TCP/IP malformed protocol stacks

Application

Link/Physical Layer

You might need multiple devices to manage all of it ...

What can we look for?

TCP/IP	malformed protocol stacks
Application	unexpected behaviour, imporper use, excessive fragmentation
Link/Physical Layer	

You might need multiple devices to manage all of it ...

What can we look for?

TCP/IP malformed protocol stacks

Application unexpected behaviour, imporper use, excessive fragmentation

Link/Physical Layer wireless: scanners, rogue devices, misconfigured devices, impersonation, DoS, unusual use

You might need multiple devices to manage all of it ...

Advantages of NIDS

- Good control with few devices (and careful placement)
- Passive devices causing little or no disruption
- Not usually susceptible to direct attack; may not even be detectible

Limitations of NIDS

- May be overwhelmed by traffic and miss attacks
- Difficult to achieve complete monitoring (because of switches)
- Cannot analyse encrypted contents
- Can hardly distinguish between successful and failed attacks
- Some attacks are difficult to detect (such as packet fragmentation)

Outline

What can be detected?

Host-based IDS

- Changes is most straight-forward
- Monitor the system state
  - system files, executable files
- Report all changes
  - manual review to filter authorised changes
- Basic integrity check

What can be detected?

Host-based IDS

- Changes is most straight-forward
- Monitor the system state
  - system files, executable files
- Report all changes
  - manual review to filter authorised changes
- Basic integrity check

Colour Coding

Red system registry, OS config, OS kernel, application software

Yellow device drivers; other relatively important files

Green user data

What is special about the red files compared to green ones?

Advantages of HIDS

- Detects local events — some would elude the NIDS
- Can access traffic after decryption
- Never kept in the dark by switches
- Can detect incosistencies after the network traffic is complete; e.g. a Trojan horse

Disadvantages of HIDS

- Most be managed host by host
- Vulnerable to attacks
  - direct attacks
  - attacks on the host
  - some DoS attacks
- Sees only a single host; no multi-host awareness
- Performance overhead and disk usage

Outline

Signature Based

- Searches for characteristics *known* attacks
- Maintains a database of such signatures or patterns
- Reliable detection of known attacks
- Poor or no detection of new and unknown attacks

Statistical Anomaly

- Builds a statistical model of normal activity
- Flags events which do not fit the model
- No information about known attacks is used
  - unknown attacks are detected as well as known ones

Stateful Protocol Analysis

- Observe execution of network protocols (e.g. FTP)
- What do we mean by stateful?
- Stateless analysis considers individual messages
  - can detect malformed messages
  - but not messages out of place
- Stateful analysis follows the protocol
  - messages out of place may be detected

Note! State is a concept worth spending time on.

Stateful Protocol Analysis

- Observe execution of network protocols (e.g. FTP)
- What do we mean by stateful?
- Stateless analysis considers individual messages
  - can detect malformed messages
  - but not messages out of place
- Stateful analysis follows the protocol
  - messages out of place may be detected

Note! State is a concept worth spending time on.

Stateful Protocol Analysis

- Observe execution of network protocols (e.g. FTP)
- What do we mean by stateful?
- Stateless analysis considers individual messages
  - can detect malformed messages
  - but not messages out of place
- Stateful analysis follows the protocol
  - messages out of place may be detected

Note! State is a concept worth spending time on.

Outline

Response strategies

- Attack detected — now what?

  What would you suggest?

Alert system administrator

- Email message
- Pop-up windows
- Phone/SMS
- Audible/visual alarm
- Log entry

Reconfigure gateway/firewall

- Drop external link — last resort only
  - what happens in the event of a DoS attack?
- Add packet filtering (port/IP/structure/contents)
  - complex task in the event of distributed attacks
- Close session (TCP close)

Other countermeasures

- No limitation
  - Arbitrary programs may be run
  - Arbitrary messages to other devices
- Start more sophisticated IDS (in spite of overhead)
- Collect evidentiary documentation
- Counterattack
  - Trace or criple
  - Could very well be illegal
  - Could also harm an innocent third party

Outline

Questions

- What is a honey pot?
- Why do we use them?

Honey pots

- Decoy systems
- Attract attackers to dummy assets
- May allow
  - Diverting an attack from the real system
  - Collect information about attacks and attackers
  - Trace attackers and possibly respond
- The attacker cannot know that it is not the real system

Padded cells

- Tandom of a hardened honey pot and an IDPS
- When IDPS detects an attack
  - divert it into a dummy replica of the system

Padded Cells

Advantages

- Attacker diverted – can do know harm
- Buys time to decide on response
- Monitoring refines the threat analysis
- Effective against snooping insiders

Padded cells

Disadvantages

- Unclear legal position
- Not yet proved themselves – commercial tools are very recent
- May provoke attacks or aggravate attacks
- Expert sys admin required

Outline

Summary

- Three technologies covered
  - DMZ
  - IDPS
  - Honey pots
- Especially DMZ and IDPS are becoming standard