ENABLING SMARTER CROSS DOMAIN WAYS OF WORKING

MARTIN COOPER – SOLUTIONS ARCHITECT
It's about getting right information, to the right people at the right time to make the right decisions.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>History of Domain Based Separation</td>
<td>1</td>
</tr>
<tr>
<td>Domain Based Security Approaches</td>
<td>2</td>
</tr>
<tr>
<td>Current Cross Domain Solutions</td>
<td>3</td>
</tr>
<tr>
<td>Future of Cross Domain Solutions</td>
<td>4</td>
</tr>
</tbody>
</table>
REASONS FOR ISOLATED NETWORKS

- Differing Security Classification
- Differing Security Policies
- Differing ICT ownership
ISSUES WITH ISOLATED NETWORKS

- Stove-piped
  - Information resides in different networks
  - Information duplicated
  - Information outdated
- Systems not easily/quickly patched
- Not easy/quick to move data between networks
- Impacts on collaboration effectiveness
- Impacts on decision making (potentially outdated information)
- Difficult to get a consolidated view across all domains
- Differing levels of fidelity across the information environment
Attackers aiming to penetrate the network defences to disrupt operations or steal information

Two main concerns are:
- Ingestion of malware and other threat actors into the domain
- Data leakage from the domain
History of Domain Based Separation

Domain Based Security Approaches

Current Cross Domain Solutions

Future of Cross Domain Solutions
SECURITY METHODS

- **Air-Gap**
  - Completely separate physical networks

- **Manual IMPEX Function**
  - User importing and exporting data via CD media or USB devices

- **Intermediate domain**
  - Jump Box – allows connection into and out of an intermediary device
  - Temporarily connect each domain in sequence. Manual/automated physical network switching

- **Firewalls**
  - Next Generation/Application Level Firewalls
  - Unified Threat Management devices
    - IPS, AV, SPAM & Web filtering

- **Guards**
  - Deep content inspection
  - Defined content types

- **Data Diodes**
  - Uni-directional flow enforcement
Perimeter is the first line of defence
- Reduce attack surface, limit protocols
- Multi-layered approach
- Understand what and how data is being transferred
- Dictate secure protocols and formats that can be verified.
- Simplify - The more complex the protocol, data type or solution the more risk of security holes
LEVEL OF CONTROLS

- How do you decide what is needed?
  - Combination of controls within a gateway
- UK NTA (NCSC)
  - Defines concept of Low, Medium and High Threat Gateways depending risk scenario
- NATO
  - Defines concept of Information Exchange Gateways (scenarios A to E depending on risk)
- Published security architectures, patterns and deployment guides available from Nation Technical Authorities.
- In the end it is the Accreditor or Information Security Officer who will decide the level of risk to accept.
RESULT

- Many bespoke gateways
  - Owned and operated by a variety of vendors and organisations
- Difficult to support and maintain
  - Legacy systems, monolithic architectures
- Expensive to create, support and update
- Inflexible
  - Difficult to modify and modernise
INFORMATION SHARING METHODS

INFORMATION SHARING

TRANSFER

ONE-WAY
- DIODE
- NETWORK PUMP

TWO-WAYS
- MANUAL REVIEW
- SECURITY FILTER
- GUARD
- LABELS

ACCESS
Information Transfer
Ask for the data you need, not the document it's wrapped in.
- Transformation Engine
  - Transforms protocol and/or content
- Protocol Break (sender/receiver)
  - Termination of the protocol at all levels of the stack and reconstruction
- Flow Control
  - Control the flow of data inbound and outbound
- Verification Engine
  - Verify that the content conforms to the policy for the domain.
THE ROLE OF EACH STAGE

- **Transformation Engine**
  - Transforms protocol and/or content to normalise or redact/regenerate content
  - Convert the data into a low risk format, to make the verification tasks as easy and secure as possible
  - Remove any unnecessary metadata that could be used for steganography

- **Flow Control**
  - Enforce a unidirectional flow of data to prevent uncontrolled data moving the opposite way
  - Hardware enforcement for higher assurance systems

- **Protocol Break**
  - Can be implemented by proxies, guards or diodes
  - Ensures a vulnerability in one protocol is not enough to compromise the entire system

- **Verification Engine**
  - Performs the Security Enforcing functions to validate the content against the policy for the domain
  - Hardware enforcement for higher assurance systems
Nested content can provide a risk of malware and data leakage.

Embedded content of another format should be un-packed, transformed if required, and verified.

Limit the amount of nesting allowed to prevent vulnerabilities related to recursion.

To prevent masquerading of content (trying to trick the verification engine) content format should be robustly verified.
Capture and Transform
One Way Control & Protocol Break
Data Verification
Regenerate and Deliver

Regenerate and Deliver
One Way Control
Release Control
Capture and Transform Protocol Break [option]
DATA EXPORT

- Reversed pattern with similar controls to data import
- Addition of a Release Control function to verify what is exiting the network
- Types of checks include:
  - Content validation
  - Data leak prevention
  - Signature verification
  - Two-man release
  - Label verification
o Disparate IA approaches and guidance across various nations
o Disparate security policies and postures
o Important to secure your own boundary and control what you ingest and release
o Need for co-operation and definition of information exchange requirements (IERs) between parties
Information Exchange Gateways
INFORMATION EXCHANGE GATEWAYS

Defined and agreed services (IERs)
Guidance Document On The Implementation Of Gateways For Information Exchange Between NATO CIS and External CIS, March 2008
CORE SERVICES

○ User to user
  ▪ Email
  ▪ File
  ▪ Chat
  ▪ Voice

○ Application to application
  ▪ Web Services
  ▪ Mapping data
  ▪ Track data
  ▪ Image data
  ▪ Database synchronisation
Remote Information Access
REMOTE ACCESS

- Access and view the information, do not transfer it.
Swivel Chair Approach
REMOTE ACCESS SOLUTIONS

Provide multi-domain view on a single screen
Remote Access solutions appropriate for “Browse Down” and “Browse Across” scenarios
- Connecting from High domain to Low Domain or at the same level

Not advisable to “Browse Up”
- Connecting from a Low security domain to a high security one.
- Client is in an insecure low trust domain and thus more at risk of compromise.
- If compromised, the attacker has control of the High security domain.
REMOTE ACCESS APPROACHES

- **KVM based**
  - Plug all networks into a segregation device and use a single keyboard, mouse and monitor
  - Automatic KVM video routing solutions available.

- **Remote Desktop based**
  - VDI style infrastructure – allows you to work as a user in the remote domain with a single network to the client
  - Support for multiple thin client protocols (RDP, VNC, PCoIP)
  - Various levels of assurance

- **Browser based**
  - Provides access through a browser and renders content in the browser
  - Connectivity for O365 apps, etc.
  - Will support privately hosted environments

- **Internet cloud based**
  - Data rendered in the cloud
  - Malware analysis performed in the cloud
REMOTE ACCESS BENEFITS

- Reduces the threat of data leakage from high to low.
  - Keyboard and mouse only allowed from high to low

- Reduces the risk of malware from low to high
  - Only allows a remote view of the data, doesn’t ingest the data itself
  - Screen image data only allowed from low to high
  - Data is rendered in the insecure and potentially disposable environment

- Reduced infrastructure at the client
  - Some solutions support ‘zero client’ architecture

- Reduces storage and duplication of data

- Allows users to work across multiple domains at the same time from a single terminal
Single Information Environment
Nirvana

- Easily access and share information securely to enable more effective and efficient collaboration

Implementation using existing capabilities

- Combination of Transfer and Access solutions
  - Transfer solutions - enabling effective, efficient and secure movement of data.
  - Access solutions – providing the ability to securely access information from higher domains

- Allowing for the consolidation of information in a single domain and for the user to effectively work from a single terminal within multiple domains.
BROWSE DOWN, PULL UP ARCHITECTURE
WAYS OF WORKING

- Technology enables the user to work seamlessly in multiple environments
- The risk is moved to the user and their ability to understand the classification of the data
- SOPs and TTPs to ensure secure ways of working
- Making the user understand the risk and giving the data owner the ability to securely mark the data
INFORMATION BASED SECURITY (DATA CENTRIC SECURITY)

Current Domain Based Architecture

System 1
Information objects

(Reasonably) free access

Users

System-defined security measures for Confidentiality, Integrity, Availability

Security boundary

Cross-system access/sharing controls (and supporting measures for Confidentiality, Integrity, Availability in transit)

System 2
Information objects

(Reasonably) free access

Users

System-defined security measures for Confidentiality, Integrity, Availability

Security boundary
INFORMATION BASED SECURITY CONCERNS

- Different assurance concerns
  - How do I trust the security properties are correct?
  - How do I trust that a key can be released for use by identity X?
- Key management
- New technical components
- Different infrastructure requirements
  - IDAM, PKI, Encryption, Decryption
- Security policy evolution
Information is protected:
- Data is encrypted
- Metadata describes security properties
- Information & properties bound together as Information Object

Systems determine security measures dynamically based on:
- Security properties
- User attributes
- Security policy rules

Security controls grant access to information at the point of consumption
ENABLING TECHNOLOGIES

- Encryption and key management
  - Cornerstone of the approach
  - Non trivial

- Content Security
  - Metadata format and binding
  - Confidentiality Labelling - STANAG 4774/4778
  - Trusted Data Format (TDF)

- IdAM
  - Securely verify the client’s identity and role
  - XACML – attribute based access control (ABAC)

- Client Attestation
  - Can you trust the client device and its environment
  - Trusted boot
  - Network Access Control (NAC)
A future vision is to adopt a paradigm where we protect the individual pieces of information we need to work with.

In this vision, system boundaries are no longer an obstacle to information sharing.

Instead, focus moves to managing and maintaining the communities with a need to share this information.
Domain based separation will remain
  - Too much risk and immature technologies.

IBSA technologies will be used to share on a need-to-know basis within a domain.
  - Evolution not revolution

Combination of approaches
  - accredited access and transfer solutions, coupled with attribute based security will provide a consolidated information picture across multiple domains from a single terminal whilst retaining the confidentiality and integrity of the data
Martin Cooper, Nexor
Solutions Architect

✉️ martin.cooper@nexor.com
📞 +44 (0)7712 190 757
🌐 www.nexor.com

Miles Booker, Nexor
Business Development Manager

✉️ miles.booker@nexor.com
📞 +44 (0)7817 980 738
🌐 www.nexor.com