



Altus

clear thinking for Financial Services

Security Assessment

Your business needs efficient access to reliable information. The right people need access to the right data at the right time, and need to have confidence in the answers they get. You are dealing with more customers, suppliers and partners. You have more data and more applications, accessed via more channels, and must comply with an increasing array of corporate policies and legislative requirements. A technology-driven security design – “don’t worry, it’s SSL-secured” – cannot meet all these business demands.

At Altus we believe that technology decisions should be driven by business needs. Our approach to security is to begin by working with business stakeholders to identify and model exposures to security threats, and only then work with technical groups to understand how the system design should respond to those threats. By understanding the real business security needs, we can help you ensure that you get real protection, not just buzzword compliance and a false sense of security.



The Issue

Companies, particularly in the Financial Services sector, are under increasing threat from phishing, trojan, man-in-the-middle and identity-theft attacks. They cannot afford to ignore the opportunities presented by new channels such as internet and mobile phone, but neither can they afford to ignore the security risks. The threat from internal attacks hasn't gone away either.

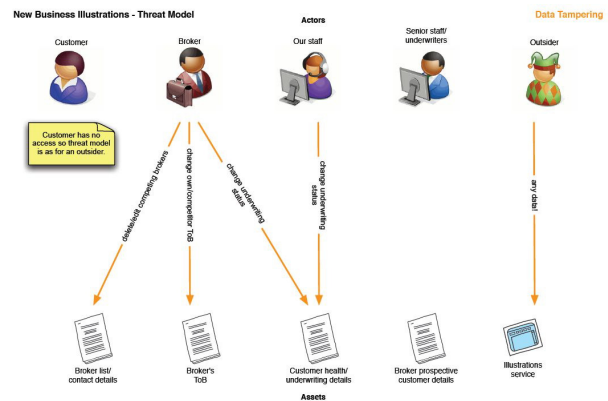
Meanwhile, systems are ever more complex. Service Oriented Architectures (SOA) bring together disparate systems, often built using many different architectures and technologies, some of them from outside the organisation. Authentication becomes a multi-faceted problem, identifying not just the user, but also the customer and each of the systems involved.

Technical solutions are legion: directory services, trust networks, firewalls, role-based or capability-based authorisation, intrusion detection systems, client and server certificates, PKI, digital signatures, biometric authentication, data and channel encryption, VPNs, code access security, and privilege separation.

But a technical solution is useless if the security system is not both manageable and usable. Systems must encourage users to do the right thing rather than the wrong thing, and must ensure that potential attacks are noted and acted upon.

And just like any critical system functionality, security must be tested; a non-trivial undertaking as system security is often dependent on the configuration of the test environment. Both testing and deployment must be carefully planned to ensure testing truly reflects live use.

Threat Model Example



The Altus Approach

At Altus, we believe that technology decisions should be driven by business needs. We start by working with the business to identify and model the proposed system's exposure to security threats. We consider the likelihood of each threat occurring, the impact on the business, and the duration of the exposure.

We then work with technical groups to understand how the system design responds to those threats. We review the system architecture and design for potential security issues, and for compliance with corporate security policies.

Our review covers not just the basics of channel access, authentication and authorisation, but also investigates how data in the system is used, and evaluates the basis for the trust placed in its accuracy. We evaluate the systems' vulnerability to, and potential to act as a vector for, identity-theft attacks.

We look not just at perimeter defences such as firewalls, but also for layered security systems providing secure auditing, defence-in-depth and avoiding common-mode failures.



The Altus Approach (cont.)

Finally, we consider the “real-world” implications of the security design. There is little point employing digital signatures if none of your customers have the means to verify them.

We also assess plans for ongoing review and testing of security elements to ensure that the finished system implements the design, and for key management, deployment, go-live, and post-live support processes to ensure that security is maintained as the system moves into production.

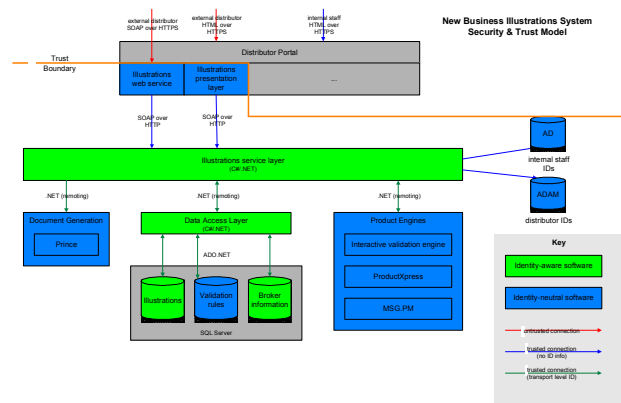
Based on our review, we will recommend necessary system or process changes, and can help plan and coordinate the necessary steps to reach the agreed solution.

The Deliverables

The outputs of our work will be:

- A specification of the security objectives in meaningful business terms;
- A visual presentation of the security threats to which the system is exposed;
- Proposed business process and system security controls;
- Security architecture diagrams and documentation high-lighting actual and potential problems;
- Specific recommendations for system security architecture and design changes;
- Recommendations for security testing to be performed on the completed system.

Security and Trust Model Example



The Benefits

By understanding the real business security needs, we will help you ensure that you get real protection, not just buzzword-compliance and a false sense of security.

By documenting those in a form that can be understood by both technical and IT staff, we help you avoid mistakes before they are made, and provide a model to guide implementation and testing.

And by targeting effort on the security controls that best meet your business needs, we will help you minimise project costs.

You will also get the confidence of an independent, well-documented review of your project against legislative, regulatory, corporate policy or other minimum security standards, providing a sound basis for proceeding with development.

Finally, by involving both business and IT staff in the assessment process, communication across the organisation on security issues will be improved, leading to better understanding and a more consistent approach across projects.




clear thinking for Financial Services

Altus understand Financial Services - the products, the processes, the people and the systems that make the whole thing tick. With years of experience in complex change programmes, we understand that successful solutions begin with the business.

Altus Limited

1 Widcombe Crescent, Bath, BA2 6AH

 +44 (0)1225 472830

 enquiries@altus.co.uk

 www.altus.co.uk