White Paper

Enterprise Architecture for Data Security in a BYOD World

WP0123 | January 2014

Karl Schulmeisters

Karl Schulmeisters is Technology Advisor for the Carver Global Health Group where he provides expert leadership in Business Process Architecture, Enterprise Architecture and Cloud Computing. Karl's current emphasis is on the impact and integration of disruptive technologies into traditional enterprise IT organizations: Cloud, Mobility, Consumerized IT, Machine Learning/Big Data and Social Media.

Karl Schulmeisters is an internationally recognized speaker – his most recent speaking engagement was at the Congress on the Future of Engineering Software in St. Petersburg Russia. He welcomes your comments at *karl.schulmeisters@cg-hg.com*

This white paper will look at ways in which the rapidly expanding use of "Bring Your Own Device" (BYOD) technology is changing how security fits into the Enterprise Architecture practice. It will also look at some approaches that Enterprise Architects should consider as they design and re-architect systems.

Security should be part of Enterprise Architecture

It is almost a tautology to state that Information Security should be part of Enterprise Architecture. After all Security is an aspect of systems behavior and the Enterprise Architecture discipline is specifically focused on identifying, planning and managing the span between required, implemented and needed behaviors of information systems. Guy Sereff has already covered the high level aspects of this in his two excellent white papers: *Information Security Integration within the Enterprise Reference Architecture Model: Part I and Part II*[i]. In those papers he puts forth the CORAS Model Based Risk Assessment methodology and the Carnegie Mellon Security Quality Requirements Engineering methodology (SQUARE). To this I would like to add STRIDE for reasons that I will cover below.

As a quick recap, CORAS' approach incorporates[ii]:

- Context Identification
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment

SQUARE's approach is a 9 step program[iii]:

1. Agree on Definitions
2. Identify Assets and Security Goals
3. Develop Artifacts to Support Security Requirements Definitions
4. Perform Risk Assessment
5. Select Elicitation Techniques
6. Elicit Security Requirements
7. Categorize Requirements by Level (System Software, Application Software etc.) and by type of Constraint/Requirement
8. Prioritize Requirements
9. Inspect Requirements

These are both abstract models for integrating security into architectural frameworks. While there are a variety of frameworks in use, particularly when it comes to security, TOGAF® 9 (which Orbus Software's iServer supports[iv]) is more process driven than some of the other frameworks and this enables codifying the Security standards into the architectural patterns being used[v]. As this white paper is aimed somewhat more tactically, I would like to add to the above security frameworks, a more tactical approach known as STRIDE. STRIDE is a mnemonic for a tactical approach Microsoft advocates in using when analyzing computer security threats[vi]. The STRIDE mnemonic stands for

- **S**poofing of user identity
- **T**ampering
- **R**epudiation
- **I**nformation disclosure (privacy breach or Data leak)
- **D**enial of Service (D.o.S)
- **E**levation of privilege

While from an Enterprise Architecture perspective the ideal approach is to identify the types of risks being evaluated, to specifically discuss the practical differences that Bring Your Own Device (BYOD) imposes on an Enterprise Architecture we need a more tangible framework than the first two.

One of the key things to recognize in any security effort is that security is fundamentally a cost minimization function. When first presented this sounds somewhat heretical. After all, don't we seek ideal security wherever possible? To which the answer is no. Because "security" at its most fundamental is about denying access to data or tools to a class of users. Any denial process means that accessing the information by those who should have access is made more cumbersome and hence more

expensive. And that additional expense must be weighed against the costs associated with a potential loss. You would never buy a $10,000 safe to secure a $10 bill. Nor would you leave $10,000 in a $1.00 paper bag sitting on your desk. The correct amount of security in each case is different as both the risk of loss, and the cost of the loss are different.

The same applies to information security.

Too often Security is not part of Base Architecture Design

Unfortunately, historically, too often security has not been part of the base systems architecture. Some of this is due to historic patterns of data usage. When applications were being developed for stand-alone personal computers, data security meant locking up your floppy disks in your desk drawer. Some of this was due to a lack of an Enterprise Architecture discipline being applied to the design or deployment of systems. An example of this is the infamous SQL Slammer Virus[vii] which infected many deployed systems at Microsoft even though Microsoft had released a patch to address the problem 6 months earlier. Lastly we have the problem that as systems became more interconnected and become complex, we are presented with new threat vectors that require us to go back and revisit our security implementations and architecture.

I would posit that BYOD fits into this latter category.

Does BYOD Change Things?

As far back as 1997 we began seeing predictions that there would be a blurring between the Internet and the Intranet[viii], and of course we still have firewalls and intranets. But with the advent of Gmail, and tools like Dropbox, more and more of this prediction is finally starting to come true. Employees are using these tools to accomplish business tasks that are inhibited by the security policies that have not remained current with current ways of working. If I am working on an extended team that includes outside parties, organizing meetings by exposing our mutual calendars via Gmail is as easy as adding a rule to forward all my calendar invites to Gmail. And if I have to share an image or a series of scanned documents that exceeds my per message email limit – Dropbox is there to give me the ability to share large files for a low $10.00 fee.

So our intranets are becoming less and less effective. And various vendors are recognizing this: Yahoo, Twitter and Microsoft have all announced plans to begin encrypting their Cloud based data of their clients. And Microsoft in its Windows 7 and Server 2012 version of Windows implemented a feature that allows end-to-end encryption of

a Remote Access connection to servers inside of an intranet without allowing other servers to be visible[ix].

But all of those approaches face a more insidious challenge: The lowly USB key! And the USB Key is a great model for understanding the problems that BYOD brings to our Existing Enterprise Architectures.

As we learned during the summer of 2010, the Stuxnet virus had been introduced into the Iranian secure military system through a lowly USB drive[x]. Essentially bypassing all the network firewalls because some engineer brought in a drive and connected it to a machine inside the firewall of the organization. The approach taken by most Enterprise Architecture security implementations has been one where if the attacker has access to the physical machine, we can at best delay the inevitable. We need to change this approach. Because Stuxnet isn't the only problem:

- Dropbox pushes our data out into the wider world;
- Smartphones/tablets, which are easily lost, contain reams and reams of corporate emails, passwords and documents;
- Viruses like Stuxnet and the more recent CryptoLocker (http://en.wikipedia.org/wiki/CryptoLocker) can ride into the intranet on BYOD Laptops.
- Firesheep http://www.pcworld.com/article/209333/how_to_hijack_facebook_using_firesheep.html) allows a BYOD device to snoop on the wireless devices accessing your corporate network (laptops, tablets) if your corporate standard is Firefox
- BYOD Laptops

So what are the risk exposures here? Well let's use the STRIDE model to assess them:

- Spoofing – where the identity of the originator of a data stream is misrepresented as someone else
    - Dropbox – not much risk since you still have to log into the Dropbox site. But it is possible to snoop on some of the data packets if you catch the user in the process of an upload
    - Smartphones/Tablets – spoofing can be used to send a text or email to smartphone from "a friend" that then refers the user to download content that can compromise the Smartphone and gain access to the contents
    - CryptoLocker et. al. – CryptoLocker uses referral spoofing to get users to open content that installs the virus on the home system
    - Firesheep and other snoopers – these use spoofing to capture the data streams they copy and generate
    - BYOD Laptops – infected with a virus can send messages masquerading as other corporate users and the messages originate internally

- Tampering (with data)
    - Dropbox – not much risk other than a corporate document "in the wild" might be modified in a way that misrepresents the corporate position
    - Smartphone/tablets – if the data or the applications are tampered with, many smartphones can be root-kitted and thus all data compromised
    - CryptoLocker – by definition this tampers with your data on our hard drives and encrypts that data thereby destroying it
    - Firesheep – as the link above describes Firesheep can be used to tamper with the content being sent
    - BYOD Laptops – Corporate data downloaded onto such a laptop can be tampered with – we have seen cases like these both from government agencies as well as corporations where unauthorized data was found downloaded onto laptops

- Repudiation
    - Dropbox – because the data being transferred in and out of DropBox is not authenticated in any way, the sender can repudiate having sent it. As in: - no idea where you got that file from but that was not the price we were agreeing to.
    - Smartphones/tablets – if lost and physically in someone else's hands – commitments can be made, messages sent on behalf of the owner who lost the phone. Particularly a problem if the phone is linked to corporate email or other apps
    - Viruses typically are not involved in repudiation attacks
    - Firesheep – again by tampering with the message content – hijacking the message stream via cookie authentication, message can be sent on behalf of the person who's account got hijacked
    - BYOD Laptops – not much risk

- Information Disclosure
    - Dropbox – clearly there is a risk here. No longer is access to the document controlled by corporate security policies or data retention policies
    - Smartphones/tablets – with gigabytes of corporate email and documents, the potential for information disclosure is immense
    - Viruses stealing data, passwords, financial account information are all part and parcel
    - Firesheep – snooping is by definition information disclosure
    - BYOD Laptops – if lost or not properly recycled can send corporate data into the wide world very easily

- Denial of Service
    - Dropbox – not much risk
    - Smartphones/tablets – not much risk except as vectors of distributing the malware
    - Viruses – this is one of the key attack vectors of Viruses
    - Firesheep - hijacking one message stream is tampering, hijacking a thousand can become a DoS
    - BYOD laptops – again as with Smartphones – the threat here is as a vector of infection

- Elevation of Privilege
    - DropBox – not much risk since DropBox is not being run on the corporate environment
    - Smartphones – only as vectors of infection
    - Viruses – typically exploit some form of elevation of privilege. In the Stuxnet case, the act of bringing the infected drive behind the firewall “elevated” the “privilege” of that drive to one of a peer corporate asset
    - Firesheep – if a password can be captured – then it applies
    - BYOD Laptops – again as with the SmartPhone, primarily limited to being a vector of infection

So to summarize, what does a STRIDE analysis of these new “BYOD” technologies tell us?

1. Data being viewed outside of the authorized execution context can lead to Spoofing, Tampering, Repudiation as well as the more obvious Information disclosure problems
2. Left uninspected, BYOD devices can act as vectors of infection within the corporate environment
3. Data stored on BYOD devices can easily be tampered with, repudiated and disclosed.

So What to Do?

When taking this information back into the SQUARE and CORAS analytic realms, the question becomes what should the risk mitigation be? The common thread here is data compromise. So the Enterprise Architecture approach would be to begin a review of the data security policies, standards and risks that BYOD brings. Some implementation tools that can be brought to bear include:

- Tighter security of data on a per data-object basis.
- Implementation of virtualized remote desktops for accessing corporate data and applications from BYOD devices
- Implementing IPSEC on intranet networks and using that to create quarantine environments for any device newly connected to the corporate network. Only upon passing the quarantine inspection is the device given access to the broader network.

Direct Data Issues are Only the Beginning

Direct data access issues are only the beginning of the security challenges Bring Your Own Devices requires Enterprise Architecture to address. Precisely because these devices are mobile and interact with the Internet directly, there is other data that is collected (cell tower connectivity, GPS location) that can be analyzed using Big Data techniques to extract crucial information.

Dumpster Diving has been called the “No Tech Hacking” approach to “social engineering” which can be seen as a way past security. The modern equivalent is to use machine learning techniques to analyze the Big Data stream of “data exhaust” that mobile and consumer devices produce. When the mobile device contains corporate data or is used in a corporate setting, meta-data relevant to the systems, processes and information infrastructure of the corporation will also be gathered and analyzed.

Conclusion

As we have seen in previous papers, security can be made a consistent part of an Enterprise Architecture discipline. If you use a process based methodology like TOGAF 9, the integration of security into the process templates can itself be a selling point of the value of an Enterprise Architecture approach.

However, as powerful as the various Security Frameworks can be, without insight into how new and disruptive technologies impact security, it is possible to fail to properly account for the risks new technology imposes. This is where taking a concrete look at the implementation impacts of the new technology using a more tactical approach like STRIDE can help.

Once the new types of risks are identified, the patterns can be updated and a thorough re-review of the consequences of those updates can be done.

Failure to do that leaves huge potential vulnerabilities, and particularly in this new BYOD world, where users expect to be able to see their corporate email and their personal communications on a single device, security is an area that needs a thorough revisit.

References

i Sereff, Guy. Information Security with the Enerprise Reference Architecture Model: Part I and Part II
http://www.orbussoftware.com/downloads/white-papers/information-security-integration-within-the-enterprise-reference-architecture-model-part-1/
http://www.orbussoftware.com/downloads/white-papers/information-security-integration-within-the-enterprise-reference-architecture-model-part-2/

ii Dahl, Heidi. The CORAS method for Security Risk Analysis
http://coras.sourceforge.net/documents/080828TheCORASMethod.pdf

iii Mead, Nancy et. al. Incorporating Security Quality Requirements Engineering (SQUARE) into Standard Life-Cycle Models
http://resources.sei.cmu.edu/asset_files/TechnicalNote/2008_004_001_14933.pdf
http://www.orbussoftware.com/enterprise-architecture/solutions/togaf-9

iv Ertaul, L, Movasseghi, A, Kumar,S.. Enterprise Security Planning with TOGAF 9
http://www.mcs.csueastbay.edu/~lertaul/Enterprise%20Security%20Planining%20with%20TOGAF.pdf

v Hernan, Shawn, et. al. Uncover Security Design Flaws Using The STRIDE Approach
http://msdn.microsoft.com/en-us/magazine/cc163519.aspx

vi CERT® Advisory CA-2003-04 MS-SQL Server Worm
http://www.cert.org/advisories/CA-2003-04.html

vii Secure Internet makes Intranet redundant, says research
http://www.v3.co.uk/v3-uk/news/1984104/secure-internet-makes-intranet-redundant-research-225

ix Direct Access http://technet.microsoft.com/en-us/network/dd420463.aspx

x Malcho, Jurja et. al. Stuxnet Under the Microscope
http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

Orbus Software
3rd Floor
111 Buckingham Palace Road
London
SW1W 0SR
United Kingdom

+44 (0) 870 991 1851
enquiries@orbussoftware.com
www.orbussoftware.com

orbus software