

Siemens PLM Connection

Security at the Edge

2008

Siemens
PLM Connection



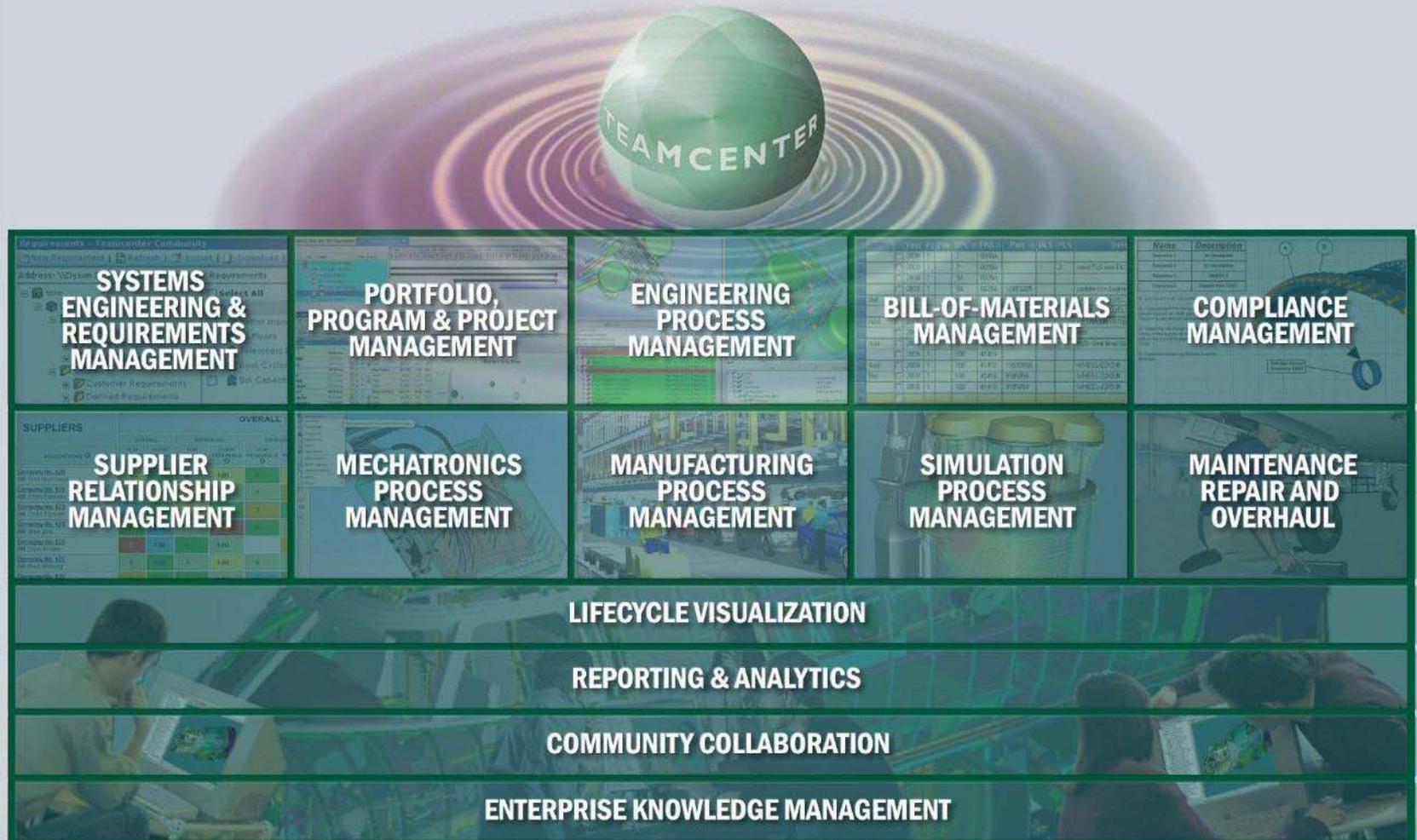
Americas 2008

PLM Software

Answers for industry.

SIEMENS

Teamcenter Digital Lifecycle Management Solutions



Agenda

- With 4-tier deployment Teamcenter can now take advantage of modern infrastructures based on the use of http. Http makes connection to the outside world easier. More complex configurations are possible with standard , but not necessarily supported, hardware. This all makes it possible to include external supplier access via the Internet.
- But with it comes more risk. The first line of defence for any application is the Operating system security, the following applies to both Teamcenter and the OS. But when the accessor is remote via Http you need more than your local OS to protect you.
 - Security issues – evaluating the risks
 - Defence in depth
 - Authentication
 - Reverse Proxy/Forward Proxy/Load Balancer
 - HTTPS and Wi-Fi



Security Considerations

Property

- Site location
- Site perimeter
- Computer rooms
- Environmental facilities
- Disaster recovery

People

- Outsiders (consider ADA)
- Users
- Disaster recovery

http://www.sans.org/reading_room/whitepapers/awareness/416.php

Risk assessment



Assessing Asset Values

Primary factors	Annual value
Overall value to the organization Web site, runs 24/7, \$2,000/hr revenue	\$17,520,000
Immediate financial impact of loss Unavailable for six hours: 0.0685% per year (Example ignores time of day, day of week, season, marketing campaigns)	-\$12,000
Indirect business impact of loss Attack: \$10,000 to counteract negative publicity; 1% lost annual sales: \$175,200	-\$185,200

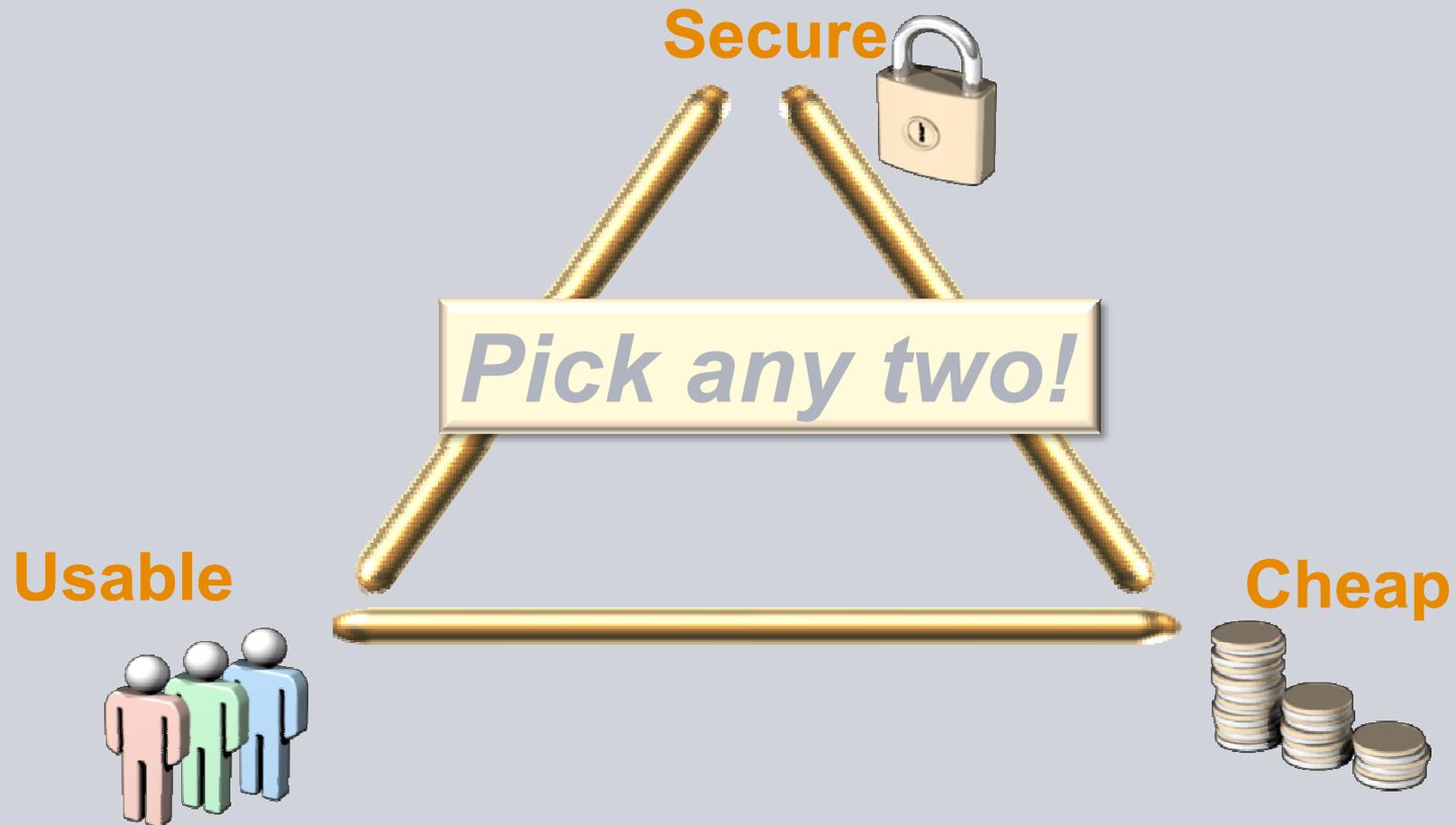
DREAD

Damage potential	How great is the damage if the vulnerability is exploited?
Reproducibility	How easy is it to reproduce the attack?
Exploitability	How easy is it to launch the attack?
Affected users	As a rough percentage, how many users are affected?
Discoverability	How easy is it to find the vulnerability?

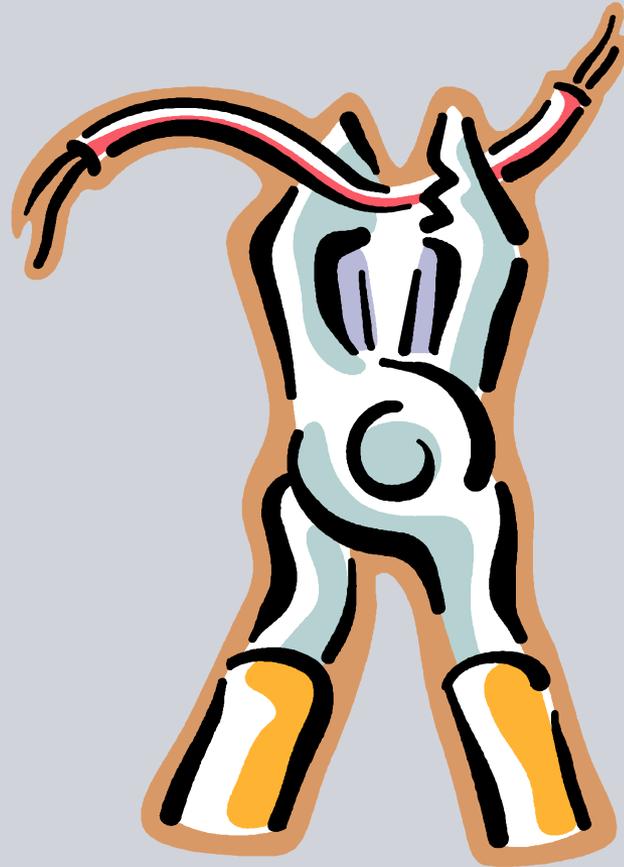
Sample threat ratings

Rating	High (3)	Medium (2)	Low (1)
Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content	Leaking sensitive information	Leaking trivial information
Reproducibility	The attack can be reproduced every time and does not require a timing window	The attack can be reproduced, but only with a timing window and a particular race situation	The attack is very difficult to reproduce, even with knowledge of the security hole
Exploitability	A novice programmer could make the attack in a short time	A skilled programmer could make the attack, then repeat the steps	The attack requires an extremely skilled person and in-depth knowledge every time to exploit
Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use	The bug is obscure, and it is unlikely that users will work out damage potential

Take Your Pick



Total Security?



Security Strategies

Defence in Depth – Layered Defence

Defense in depth was originally a military strategy that seeks to delay, rather than prevent, the advance of an attacker by yielding space in order to buy time. A castle's defence relies on a series of obstacles.



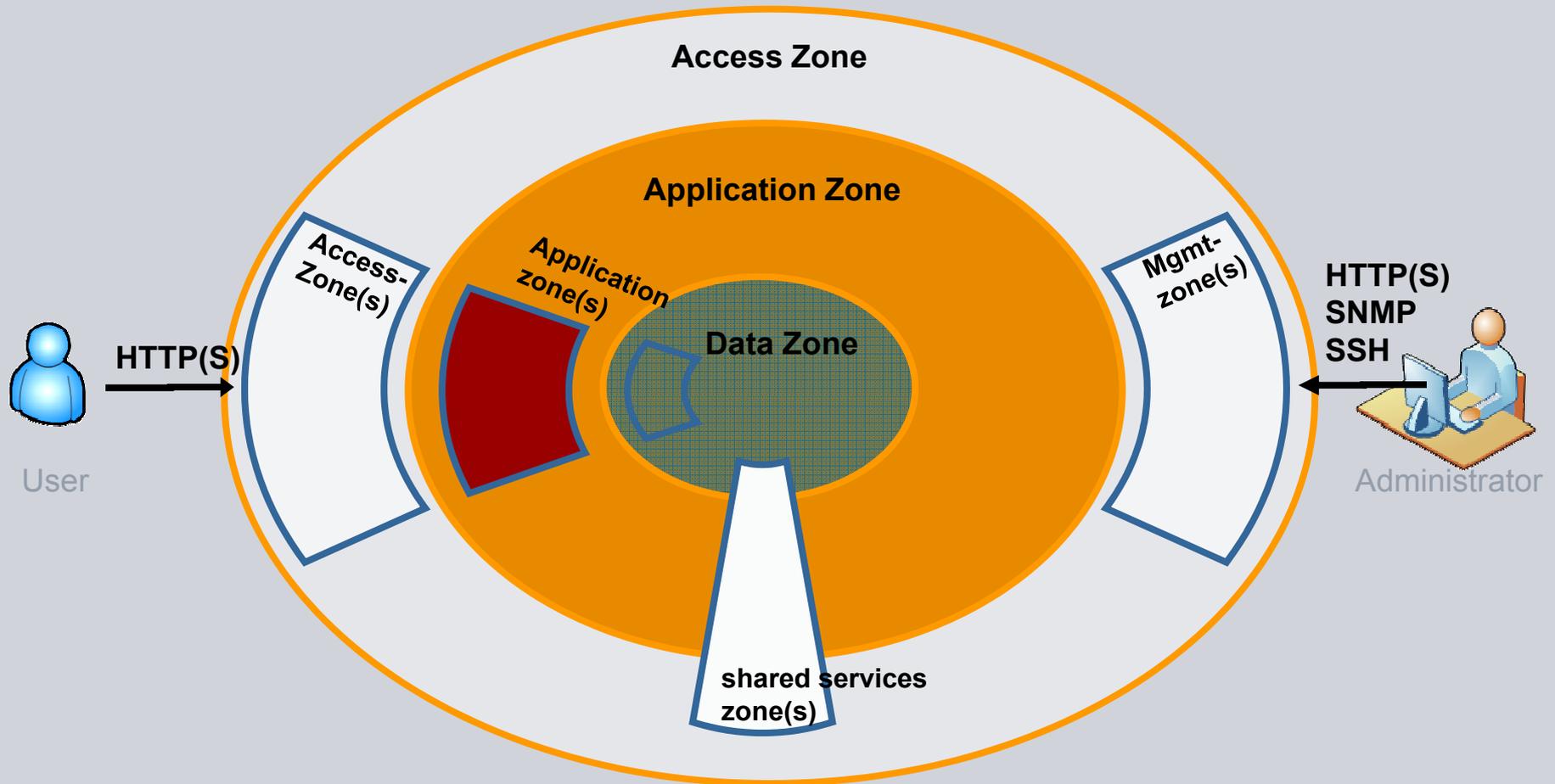
Defence in depth - IT

The creation of layers of protection i.e. more than one method of preventing intrusion could include any of the following:

- Physical Security (e.g. dead bolt locks)
- Authentication and password security
- Antivirus software
- Firewalls (hardware or software)
- DMZ (Demilitarized zones)
- IDS (Intrusion Detection Software)
- Packet filters
- Routers and Switches
- Proxy servers
- VPN(Virtual private networks)
- Logging and Auditing
- Biometrics
- Timed access control

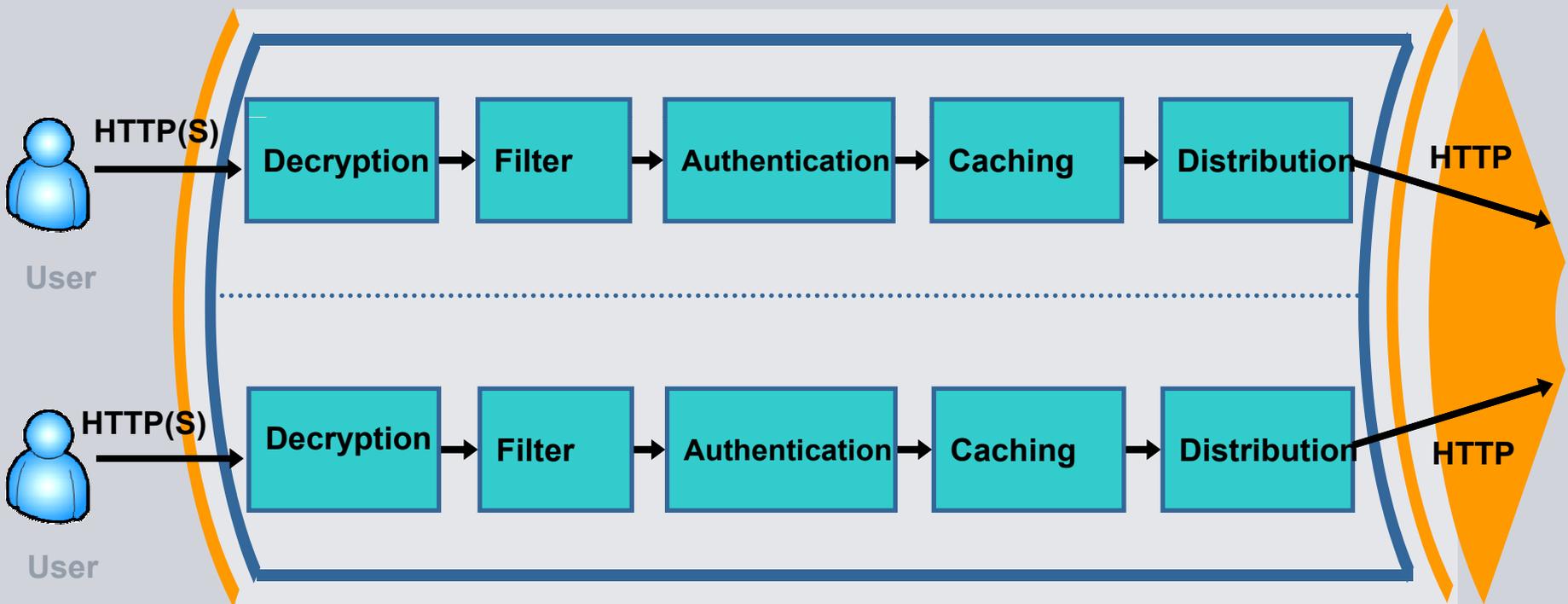
Defence in Depth measures should not only prevent security breaches, but also buys an organization time to detect and respond to an attack, mitigating the impact of a breach.

A Zoned Approach



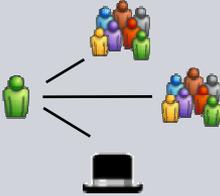
Typical Access Zone

Access zone(n)



Some of the functions that can take place in the Access zone

Authentication

<p>Authentication</p>		<p>Process of determining whether someone or something is, in fact, who or what it is declared to be. In TC this is the initial login, various third party authentication systems can be used. This is a subject in its own right.</p>
<p>Authorization</p>		<p>Designates user access to various system resources based on the user's identity. Authorization is typically defined through the use of categories such as groups, roles and project membership. It may now also include possession of the right license such as an ITAR TAA (Technical Assistance Agreement). Some of these can be defined by TC or synchronized from an external system such as LDAP. Again another subject.</p>
<p>Entitlement</p>		<p>Determining whether a participant has the rights/privileges to access specific functionality or information within a system at a given point in time. This is usually accomplished through the execution of business rules against the authorization defined for the entity. This is the subject of these slides. In general we refer to Entitlement as Access Control.</p>

Authentication

**At the basic level this is simple a password to access Teamcenter.
In general this is adequate protection but you should have good policies**

Poor, weak passwords have the following characteristics:

- The password contains less than fifteen characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "<Company Name>", "sanjose", "sanfran" or any derivation.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Passwords

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9
- Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Policy Resource: <http://www.sans.org/resources/policies>

Password and Authentication Management

Typically passwords management is by a central system e.g. Active Directory.

Teamcenter Security Services supports integration into these system via LDAP.

If you need to integrate into this environment you should seek Siemens Services Assistance.

When Passwords aren't enough



But....

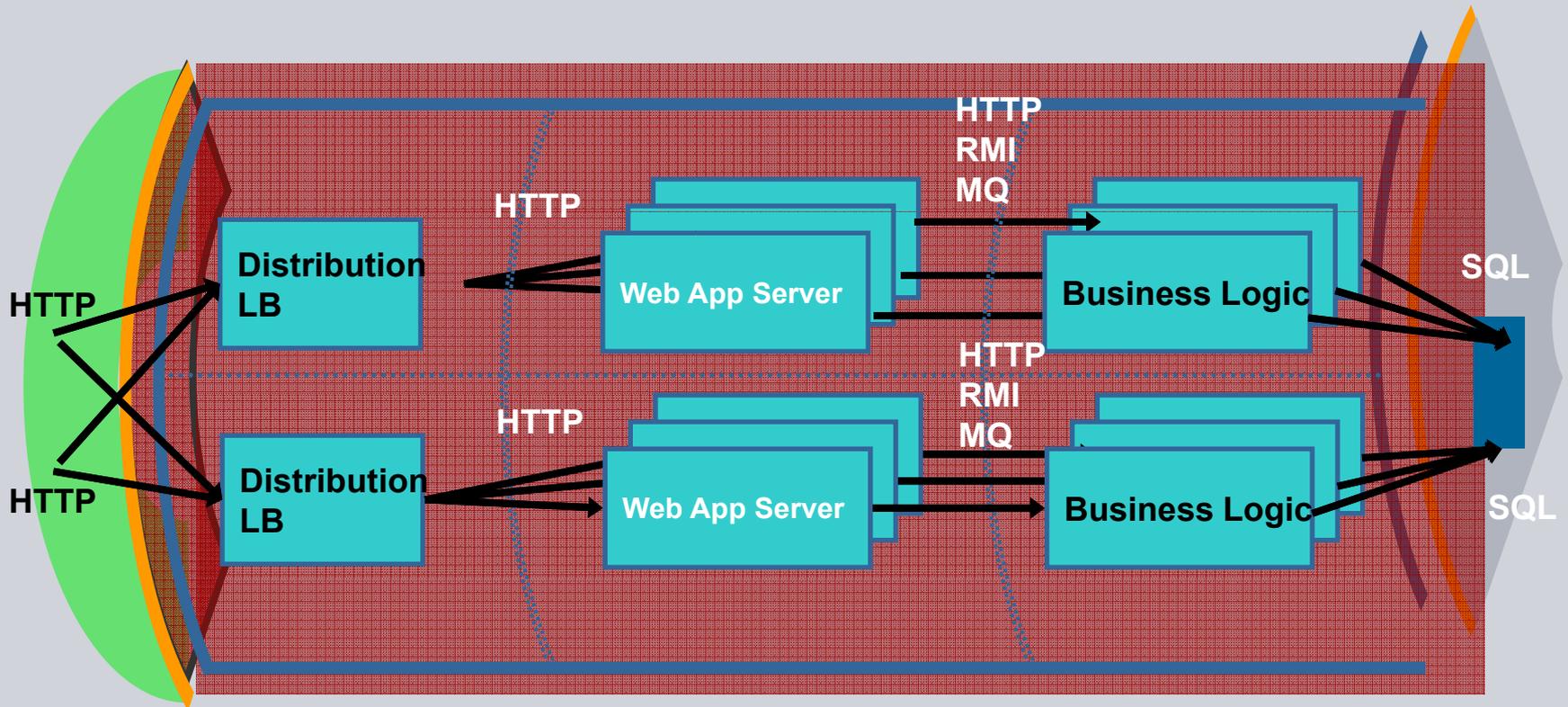
Single Sign On

Commercial SSO such as Site Minder and WebSEAL provide support for various authentication method including RSA.

Teamcenter Security Services can be integrated into this environment but there are many possible configuration options many of which are not supported.

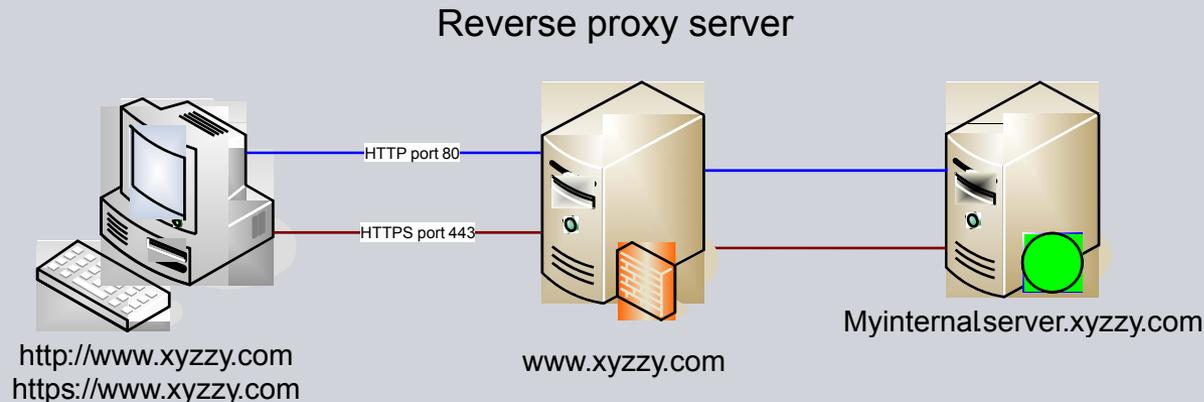
If you need to integrate into this environment you should seek Siemens Services Assistance.

Typical Application Zone



Reverse proxy servers

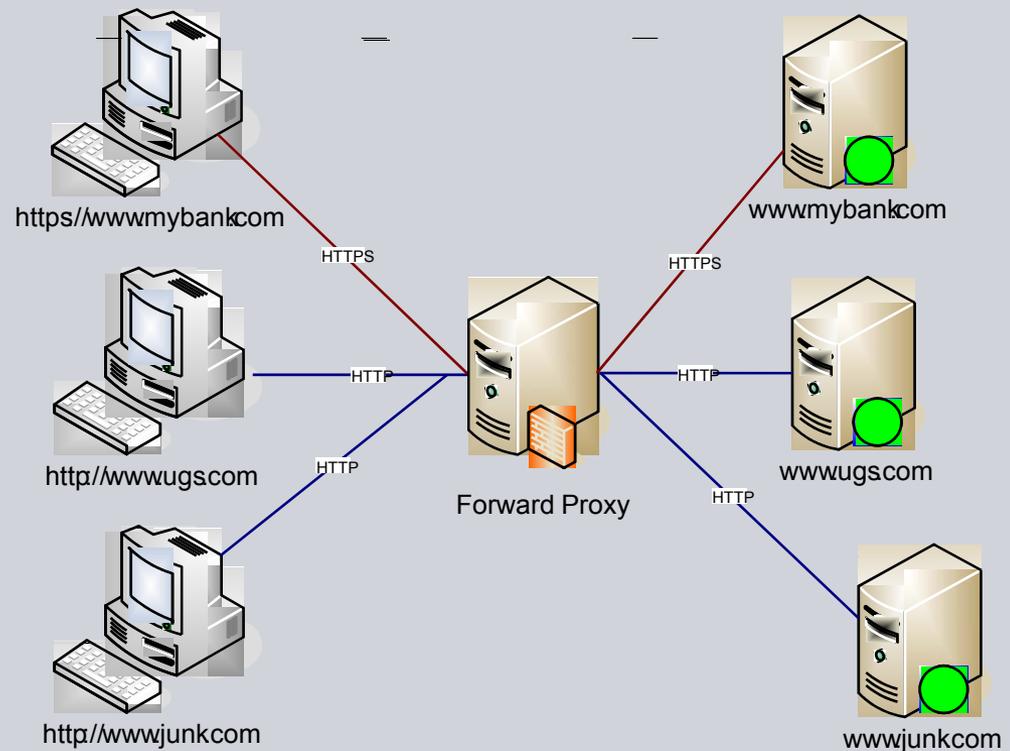
Teamcenter provides support for Reverse Proxy servers and hardware load balancers (form of RP). But configuration of the various types can be complex and often problematic depending on the type. *Assistance should be sort from Siemens Services.*



Forward Proxy

Forward Proxy are often use to manage access to the Internet.

Teamcenter provides limited support for Forward Proxy servers and under some circumstances basic authentication. But configuration of the various types can be complex and often problematic depending on the type. Assistance should be sort from Siemens Services.



HTTPS and Wi-Fi

You should use HTTPS where traffic is exposed to attack e.g. the Internet.

Internally switched networks prevent network capture with Wireshark etc., and the risk is minimal.

However you need to be careful with your use of Wi-Fi make sure you do not leak.

Tools like AirSnort makes Wi-Fi cracking easy.



Take a look at <http://www.wigle.net/> is your company on it? Is your home on it?

Teamcenter supports the use of HTTPS. Configuration can be fun and a wise person uses a trusted certificate

The Enemy within

Teamcenter 2007 includes ITAR/IP access controls and when used with NX it support access control by user type.

Where does it fit?

- It allows external or low clearance users to work on your system but restricts the users access.

Information digital rights management is also available from some suppliers (Microsoft, Adobe) and is supported by some applications e.g. Word, PDF. It uses a license manager that allows access to data even off site for specific period. It is generally intended to prevent the unauthorized use (such as industrial or corporate espionage or inadvertent release) of proprietary documents.

Where does it fit?

- It is intended to allow you to control access to data sent to a supplier out side of your control. Currently it is only inconvenient i.e. it can be broken.

Don't forget

Security is all about money

Save money...

- Identify and mitigate real risk
- Ensure compliance (e.g. ITAR)

Make money...

- Translate annoyances into differentiators

Select the trade-offs that balance security with business goals

Just because you can doesn't mean you have to.

Resources

Teamcenter Security Services documentation

Advance Deployment White Paper.

SANS Institute <http://www.sans.org/resources/policies>

Steve Riley: www.protectyourwindowsnetwork.com

Contact

David Howe
Senior Technical Consultant
Teamcenter Development Consulting

Parker's House
46 Regent Street
Cambridge
CB2 1DP
UK

Phone: +44 (0)1223 371532
Fax: +44 (0)1223316931
Mobile: +44 (0)7870 238886

E-mail: dave.howe@siemens.com

www.siemens.com/plm