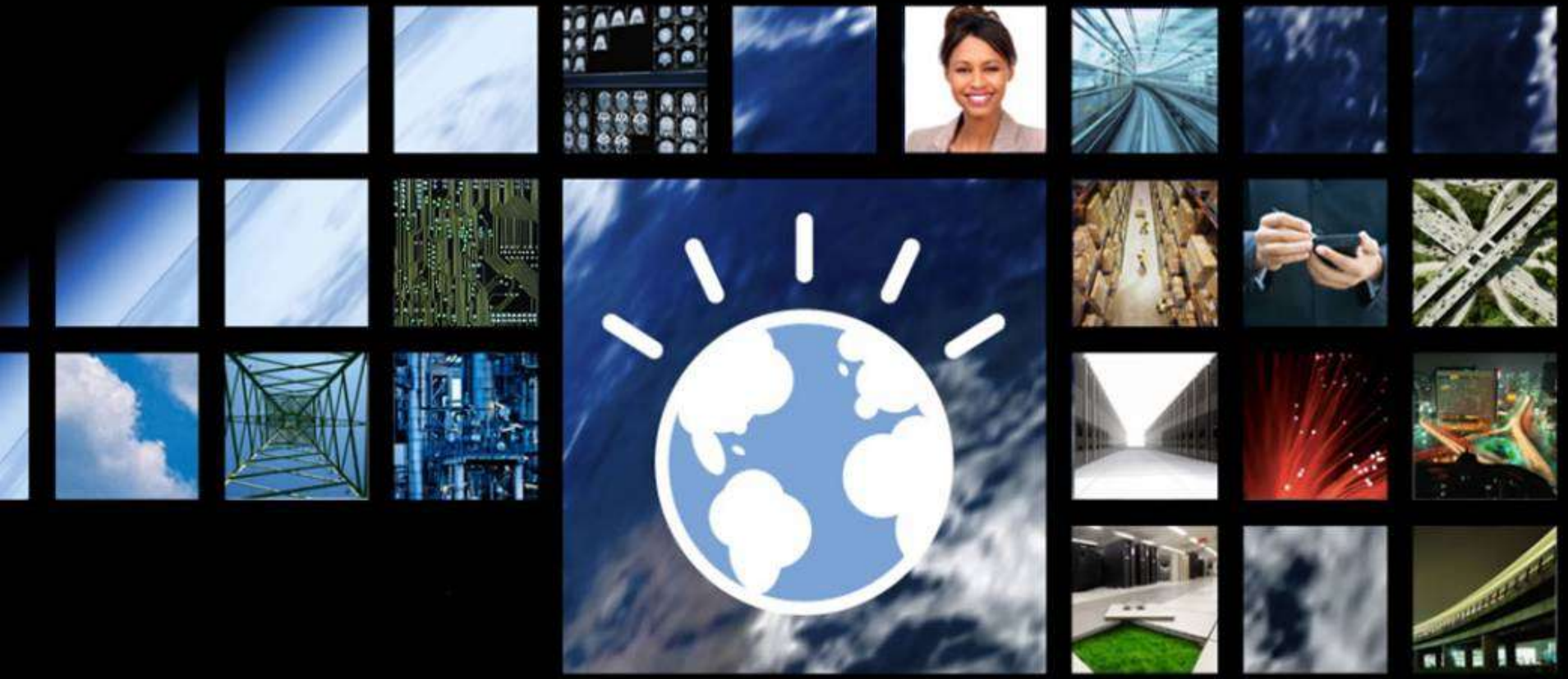
Smart Work for a Smarter Planet



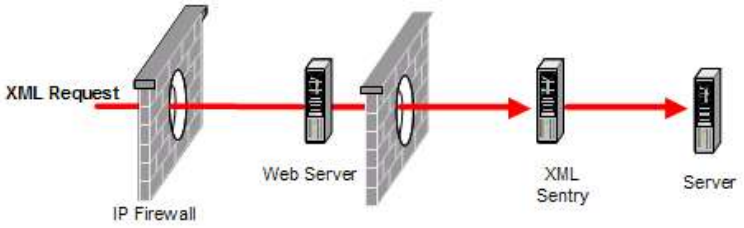
XML의 위협과 WebSphere DataPower

Speaker Name : 지용득 차장
E-Mail : ydji@kr.ibm.com

IMPACT Korea 2009

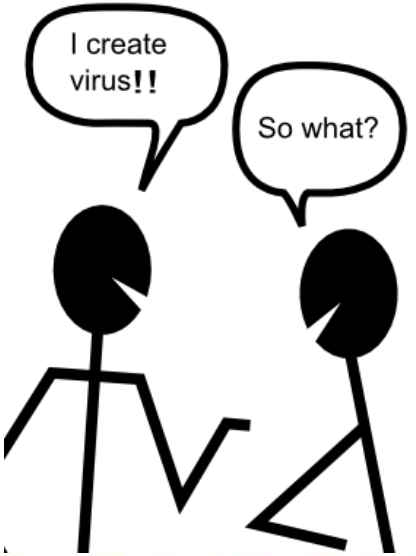
XML과 웹 애플리케이션 공격

- 둘은 유사성이 많음: 사실 많은 XML 기반의 공격은 과거의 공격 형태를 변용한 것
  - 주입(injection), 리플레이(replay), 딕셔너리(dictionary), 서비스 거부(DoS)
- 웹 애플리케이션 공격은 대체로 사람이나 브라우저를 기반으로 함
  - 교차 사이트 스크립팅(cross site scripting), 피싱(phishing)
- 반면 XML 공격은 서버를 직접 겨냥하려는 경향이 있음
  - 파서(parser)나 XML 체제(dialect)를 활용
- 아무튼 둘 다 잘못된 설정, 좋지 못한 절차나 코딩 관행에 의한 보안 상 구멍을 악용하려는 경향이 있음
- 웹 애플리케이션과 관련된 자료는 많음: XML 공격에 초점을 맞춤



새로운 개척 정신

- 전통적인 공격 대상들에 더 이상 흥미를 느끼지 못하게 된 것으로 보임
  - 개선된 프로세스와 보안성이 확보됨
- 신기술은 공격자들에게 더 놀기 좋은 토양이 됨
  - 흥미롭고 미성숙한 대상
  - 악용할 수 있는 버그와 부정확한 설정들이 빈번
- 예측하자면, 악용의 소지가 있는 Web Services 나 SOA의 보안 취약성들이 폭발적으로 발생할 것으로 보입니다.
- 하지만 말하기 꺼려지는 비밀들



XML 기반 공격

- 개체 확장 및 반복 공격
- XML 문서 크기 공격
- XML 문서 폭 공격
- XML 문서 깊이 공격
- XML 정형성 (Wellformedness) 기반 파서 공격
- 점보 페이로드
- 반복 요소
- 메가 태그 – 점보 태그라고도 지칭
- 공용 키 DoS
- XML 플러드
- 리소스 하이재킹
- 딕셔너리 공격
- 메시지 조작
- 데이터 조작
- 메시지 스누핑
- XPath 주입
- SQL 주입
- WSDL 열거(Enumeration)
- 라우팅 우회
- 스키마 포이즈닝(Schema Poisoning)
- 악성 모핑(Morphing)
- Malicious Include –XXE(XML External Entity) 공격이라고도 함
- 메모리 공간 침입(MSB)
- XML 캡슐화
- XML 바이러스
- 위조 메시지
- 리플레이 공격
- 기타

단일 메시지 XML 서비스 거부 (XDoS)

- 점보 페이로드 – 대용량 XML 문서가 파서/JVM/메모리 한도를 고갈
- XML 반복– 반복적인 개체 확장이나 기타 반복적인 처리를 실행하여 서버 리소스를 고갈시키는데 사용할 수 있는 XML 메시지
- 메가–* 요소/속성 이름, Namespaces 등 지나치게 긴 XML 메시지는 버퍼 오버런을 초래
- 강제 파싱 – 컴퓨터의 리소스를 소비하기 위해 특별히 파싱이 어렵도록 작성된 XML 메시지를 통칭
- 공용 키 DoS – 공용 키의 비대칭적 특성을 이용하여 키 길이가 길고 연산이 많이 필요한 디지털 서명을 다수 포함한 메시지를 전송하여 수신 측의 리소스를 고갈시키도록 하는 공격

단일 메시지 XDoS 예시

- Billion Laughs 공격 (반복, 강제, 점보!)
  - 완전히 유효한 정형 XML 문서
  - 파서에 제출될 때 메모리/CPU를 빠르게 고갈
  - 하나의 단일 메시지 = 하나의 단일 애플리케이션 서버 다운

```
<?xml version="1.0"?>
  <!DOCTYPE billion [
  <!ELEMENT billion (#PCDATA)>
  <!ENTITY laugh0 "ha! ">
  <!ENTITY laugh1 "&laugh0;&laugh0;">
  <!ENTITY laugh2 "&laugh1;&laugh1;">
  ...
  <!ENTITY laugh127 "&laugh126;&laugh126;">
  ]> <billion>&laugh127;</billion>
```

```
<billion>
ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha!
ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha!
ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha!
ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha!
ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha! ha!
......
</billion>
```

데모

- Billion Laughs 공격 데모
- Internet Explorer를 다운시키자

다중 메시지 XDoS

- XML 플러드
  - 일반적으로 알려진 방식은 1초에 수천 개의 (악성 또는 일반) 메시지를 전송하여 웹서비스를 방해
  - 단일 메시지 XDoS와 결합하여 타격을 극대화
  - 더 적은 수의 다중 메시지로 수행하는 XDoS 공격은 초 당 수천 개의 메시지를 DoS로 인식하는 네트워크 감시 프로그램의 탐지 범위를 멀리 우회
- 리소스 하이재킹
  - 완료되지 않는 트랜잭션의 일부
  - 대상 서버의 리소스를 잠그거나 예약하는 메시지를 전송하는 공격
  - 예를 들면 리소스에 대해 고의적으로 잠금 경쟁이나 기타 유사한 상황을 강제하는 메시지 (내부 공격)
- 통계에 의하면, 대부분의 공격은 “내부” 지식이 있는 자에 의해 감행

무허가 액세스 공격

- 딕셔너리 공격
  - 딕셔너리 단어를 통한 Brute Force 검색을 사용하여 유효한 사용자 비밀번호를 추측
- 위조 메시지
  - 중간자(Man in the Middle) 공격을 사용하여 유효한 메시지를 획득하고, 이를 변경하여 다른 메시지를 전송하는 등의 방법으로 메시지가 유효한 사용자로부터 수신된 것처럼 위조
- 리플레이 공격
  - 악의적인 의도로 과거에 유효했던 메시지를 재전송하는 공격. 여기서 (보안 토큰과 같은) 메시지의 일부만 재생(replay) 가능
- WSDL 열거(Enumeration)
  - WSDL에 나열된 서비스를 살펴보고 열거되지 않은 서비스를 추측하여 그 이용 권한을 획득
  - ?wsdl을 추가하여 WSDL 요청
  - WSDL은 데이터 유형, 포트 유형, 바인딩, 서비스 정보를 정의

주입(Injection) 공격

- SQL 주입

입력: <q0:employeeLookup><employee>jsmith</employee><fields>mobile_num></fields></q0:employeeLookup>

애플리케이션:

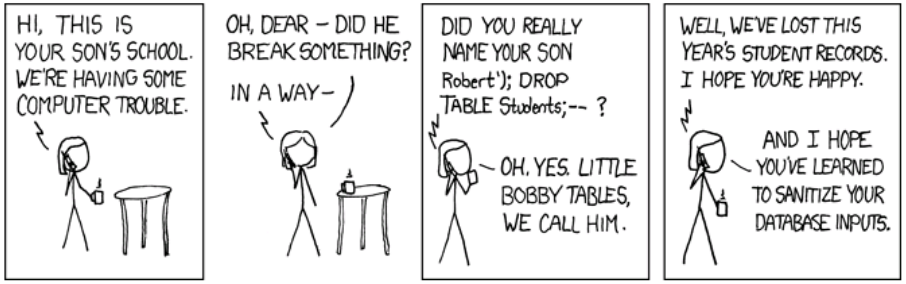
SQLStmt = "SELECT " + fieldString + " FROM corp_employees WHERE username = '" + username + "';"

<employee>*</employee><fields>*</fields> - 전 직원에 대한 모든 열 반환!

<employee>jsmith OR 1=1</employee> - 모든 기록 반환!

<employee>jsmith');DROP TABLE corp_employees;--</employee> - 테이블 삭제!

<employee>jsmith');INSERT INTO db_admins (user_id, passwd, is_admin) VALUES (badguy01, mypwd, true);--</employee> - 관리자 계정 생성!



주입(Injection) 공격

- XPath/XSLT/XQuery/LDAP 주입
  - 애플리케이션 논리에 표현식(Expressions) 주입
  - 새로운 변형에는 공격 감행에 필요한 지식을 줄이는 Blind XPath 주입 공격 등이 있음
  - 신규 XML 데이터베이스를 선호
  - XPath에는 SQL처럼 액세스 컨트롤이 내장되어 있지 않지만 Xquery는 XACML 사용 가능
- 라우팅 우회
  - SOAP 라우팅 헤더를 사용하여 내부 웹서비스를 액세스 (WS-Addressing 등)

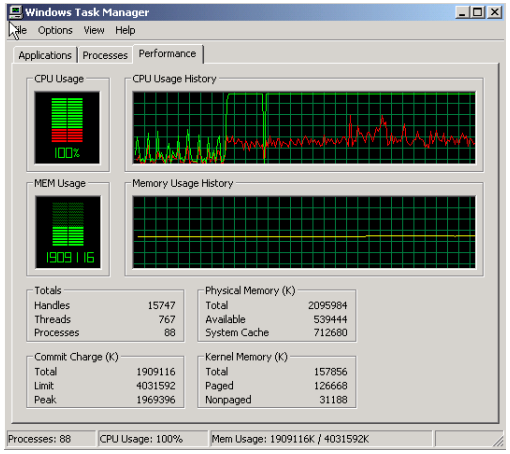
시스템 손상 공격

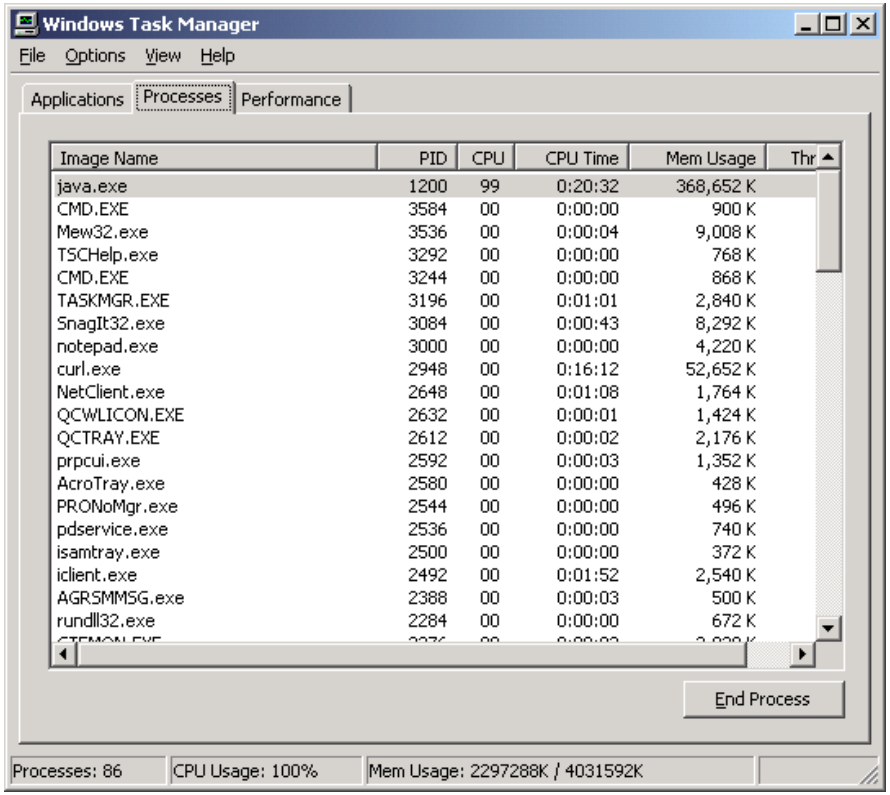
- Malicious Include
  - 웹서비스가 서버 파일 시스템에서 전송된 출력 또는 반환 권한 파일에 유효하지 않은 외부 데이터를 포함하도록 야기하는 공격
  - 예를 들면, 임베디드 "file:" URL을 사용하여 Unix 비밀번호 파일이나 기타 기밀 데이터를 공격자에게 반환
- XML 캡슐화
  - CDATA 태그 등을 통해 XML 페이로드에 시스템 명령을 내장하는 공격
  - CDATA는 XML에 스크립트를 포함한 불법 문자를 포함하는 방법
  - <![CDATA[badCmd = new ActiveXObject (“WScript.Shell”);badCmd.Run(“%systemroot%₩₩SYSTEM32₩₩CMD.EXE /C DEL C:₩₩*.*”);
- XML 바이러스(X -바이러스)
  - SOAP를 첨부파일 또는 기타 첨부 메커니즘과 함께 사용하여 바이러스나 웜 같은 악성 실행 파일을 전송하는 공격

공격 시나리오 예시

- 메가 네임스페이스 공격
  - 매우 단순한 숙련되지 않은 공격
  - 합법 XML – XML 스펙이 네임스페이스를 제한하지 않음

```
<S:Envelope xmlns:S='http://schemas.xmlsoap.org'>
 <S:Body xmlns='http://example.com/'>
 <X
  xmlns:X1='http://www.example.com/x1'
  xmlns:X2='http://www.example.com/x2'
 .....
  xmlns:X9998='http://www.example.com/x9998'
  xmlns:X9999='http://www.example.com/x9999'
 > </X>
 </S:Body>
 </S:Envelope>
```





공격 시나리오 예시

- 20분간의 XDoS 공격 후

- 망연자실한 상황
  - 사용자는 단순한 합법적인 SOAP 메시지를 전송하여 엄청난 양의 컴퓨터 리소스를 소모한 후 서버 전체 다운
  - CPU 이용률이 100%에 달하고 메모리는 포화 상태
  - 유효한 메시지가 전달되지 못함
  - 서버가 정상적으로 종료되지 않음

솔루션이 있다면?

- 기존의 컴포넌트는 사실상 큰 도움을 주지 못합니다
  - 애플리케이션 층의 XML/SOAP에는 네트워크 장비가 제한적
  - 소프트웨어 기반의 방어는 너무 느리고 DMZ에는 적합하지 않음
  - 메시지가 파서에 도달할 경우에는 속수무책
- 그렇다면
  - 최고 수준의 완벽한 보안을 갖춘 전문 초고속 하드에어 애플리케이션이라면?

WebSphere DataPower 소개

WebSphere DataPower 소개

SOA 어플라이언스의 특징

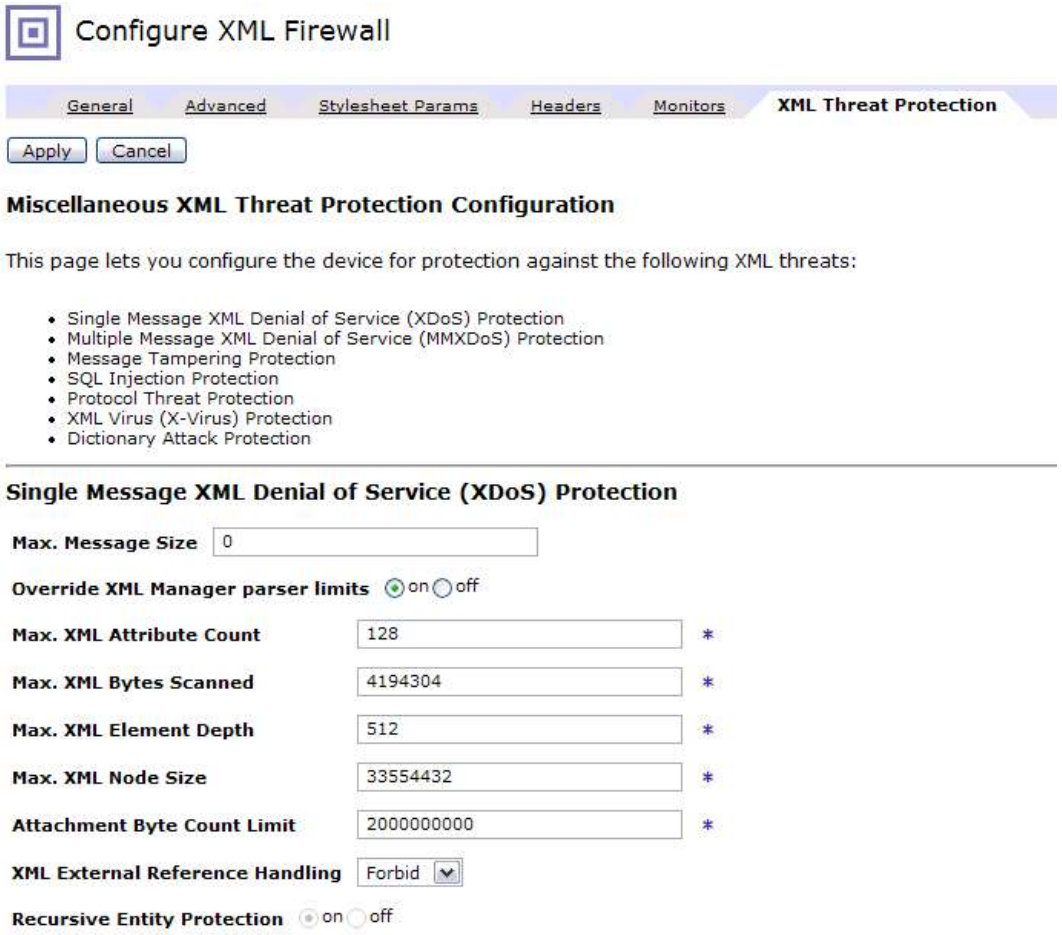
- 네트워크에 상주하는 밀폐된 장치
  - 조작 방지
  - 기본적으로 보안 수준이 높음
- 최적화된 하드웨어, 펌웨어, 맞춤형 임베디드 OS
  - 강력한 보안이 보장된 초고속 XML/ESB/SOA 시나리오를 염두하고 제작
- 서명/암호화된 업그레이드 가능한 단일 펌웨어 이미지
  - 임의로 소프트웨어를 설치할 수 없고, 작은 패치 파일을 사용하여 업데이트
- 보안 취약성의 최소화 (3rd Party 컴포넌트가 거의 없음)
- 암호화 키 하드웨어 스토리지, 감사 로그 잠금
- FIPS 140-2 레벨 3 HSM (옵션)
- XML 및 비 XML 데이터 처리 (COBOL Copybook, EDI 등)
- Java 미사용 (DMZ 친화적)
- 보안, 라우팅, 중개, 변환을 위한 애플리케이션 데이터 형식(XML, SOAP) 이해
- 광범위한 스펙/레벨(예: WS-*)과의 우수한 호환성
- 멀티프로토콜
  - HTTPs, (s)FTP(s), MQ, TIBCO EMS, IMS, TCP, NFS, JMS

DataPower를 이용한 XML 위협 보호

- 몇 가지 간단한 방법부터 시작
  - 초고속이므로 검증 및 암호화(서명/암호화/SSL) 작업에 소요되는 비용의 걱정 없음
  - GETs와 HEADs는 기본적으로 비활성화 (DoS, WSDL 공격)
  - 사용자 정책이 허용하지 않을 경우 메시지는 기본적으로 거부
  - 메시지 트래픽(요청/응답)의 특성 지정
  - SOAP 입력을 지정하면 SOAP가 아닌 것은 전부 거부
  - ACL, SSL/TLS, 백엔드 가상화를 폭넓게 지원
  - 프로토콜 레벨 보호 (즉 HTTP 1.1 미만 사용 금지, FTP CCC 명령 불허)

DataPower 단일 메시지 XDoS 보호

- 모든 DataPower 서비스 및 프록시에 위협 보호 기능
- 이 페이지에서 예상 트래픽의 특성 지정 가능
- 파라미터는 프록시가 지원하는 애플리케이션의 메시지 메트릭스에 맞게 조정 필요
- 메가*, 대체, 점보 페이로드, 반복 공격 보호



DataPower 단일 메시지 XDoS 보호

- Billion Laughs와 메가 네임스페이스 공격은 기본 설정에 따라 즉시 거부

Billion Laughs

16:58:10	xmlfirewall	warn	132388	e	192.168.1.107	0x80e00056	xmlfirewall (SimpleLoopbackFW): No match from processing policy 'SimpleLoopbackFW' for code '0x00030003'
16:58:10	xmlfirewall	error	132388	e	192.168.1.107	0x00030003	xmlfirewall (SimpleLoopbackFW): XML parser limits exceeded
16:58:10	xmlfirewall	warn	132388		192.168.1.107	0x80e0007d	xmlfirewall (SimpleLoopbackFW): Generated error on URL 'http://192.168.1.130:2048/': <?xml version="1.0" encoding="UTF-8"?> <env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/"><env:Body><env:Fault><faultcode>env:Client</faultcode><faultstring>Malforme content (from client)</faultstring></env:Fault></env:Body></env:Envelope>
16:58:10	multistep	error	132388		192.168.1.107	0x00030003	xmlfirewall (SimpleLoopbackFW): XML parser limits exceeded
16:58:10	multistep	error	132388	>	192.168.1.107	0x80c00008	xmlfirewall (SimpleLoopbackFW): rule (SimpleLoopbackFW_request): implied action Parse input as XML failed: document size limit of 419430 bytes exceeded, aborting
16:58:10	xmlparse	error	132388	>	192.168.1.107		xmlfirewall (SimpleLoopbackFW): document size limit of 4194304 bytes exceeded, aborting
16:58:10	xmlparse	debug	132388	>	192.168.1.107		xmlfirewall (SimpleLoopbackFW): Parsing document 'http://192.168.1.130:2048/'
16:58:10	xmlfirewall	info	132388	>	192.168.1.107	0x80e000b4	xmlfirewall (SimpleLoopbackFW): rule (SimpleLoopbackFW_request): selected via match 'SimpleLoopbackFW' from processing policy 'SimpleLoopbackFW'
16:58:10	xmlfirewall	info	132388	>	192.168.1.107	0x80e00077	xmlfirewall (SimpleLoopbackFW): New transaction(conn use=1): POST http://192.168.1.130:2048/ from 192.168.1.107

메가 네임스페이스

17:19:13	xmlfirewall	warn	433713	e	192.168.1.107	0x80e00056	xmlfirewall (SimpleLoopbackFW): No match from processing policy 'SimpleLoopbackFW' for code '0x00030003'
17:19:13	xmlfirewall	error	433713	e	192.168.1.107	0x00030003	xmlfirewall (SimpleLoopbackFW): XML parser limits exceeded
17:19:13	xmlfirewall	warn	433713		192.168.1.107	0x80e0007d	xmlfirewall (SimpleLoopbackFW): Generated error on URL 'http://192.168.1.130:2048/': <?xml version="1.0" encoding="UTF-8"?> <env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/"><env:Body><env:Fault><faultcode>env:Client</faultcode><faultstring>Malforme content (from client)</faultstring></env:Fault></env:Body></env:Envelope>
17:19:13	multistep	error	433713		192.168.1.107	0x00030003	xmlfirewall (SimpleLoopbackFW): XML parser limits exceeded
17:19:13	multistep	error	433713	>	192.168.1.107	0x80c00008	xmlfirewall (SimpleLoopbackFW): rule (SimpleLoopbackFW_request): implied action Parse input as XML failed: attribute limit of 128 per element exceeded, aborting at offset 6190 of http://192.168.1.130:2048/
17:19:13	xmlparse	error	433713	>	192.168.1.107		xmlfirewall (SimpleLoopbackFW): attribute limit of 128 per element exceeded, aborting at offset 6190 of http://192.168.1.130:2048/
17:19:13	xmlparse	debug	433713	>	192.168.1.107		xmlfirewall (SimpleLoopbackFW): Parsing document 'http://192.168.1.130:2048/'
17:19:13	xmlfirewall	info	433713	>	192.168.1.107	0x80e000b4	xmlfirewall (SimpleLoopbackFW): rule (SimpleLoopbackFW_request): selected via match 'SimpleLoopbackFW' from processing policy 'SimpleLoopbackFW'

DataPower 다중 메시지 XDoS 보호

- 최대 트랜잭션 기간, 트랜잭션 속도 허용
  - 설정할 수 있는 광범위한 SLM(Service Level Management) 정책도 있음

Multiple Message XML Denial of Service (MMXDoS) Protection

Enabling MMXDoS will create duration and count monitors and attach them to this firewall.

Enable MMXDoS Protection	(•) on ( ) off	
Max. Duration for a Request	5000	msec *
Interval for Measuring Request Rate from Host	1000	msec *
Max. Request Rate from Host	10	messages/interval *
Interval for Measuring Request Rate for Firewall	1000	msec *
Max. Request Rate for Firewall	1000	messages/interval *
Block Interval	500	msec *
Log Level	error *	

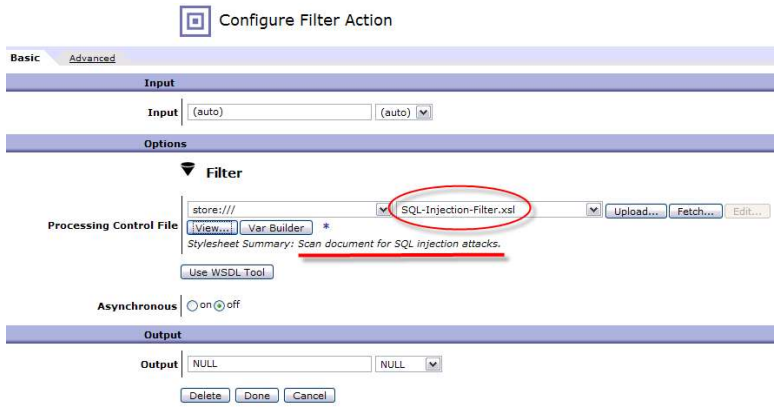
Web Service Proxy SLM

Open tree to: Proxy | WSDLs | Services | Ports | Operations

	Request			Failure			
	Interval (sec)	Limit	Action	Interval (sec)	Limit	Action	Graph
proxy: GSearch			notify			notify	graph
wsdl: GoogleSearch.wsdl			notify			notify	graph
service: {urn:GoogleSearch}GoogleSearchService			notify			notify	graph
port: {urn:GoogleSearch}GoogleSearchPort			notify			notify	graph
port-operation: doGoogleSearch			notify			notify	graph
port-operation: doSpellingSuggestion			notify			notify	graph
port-operation: doGetCachedPage			notify			notify	graph

DataPower를 통해 SQL 주입으로부터 보호

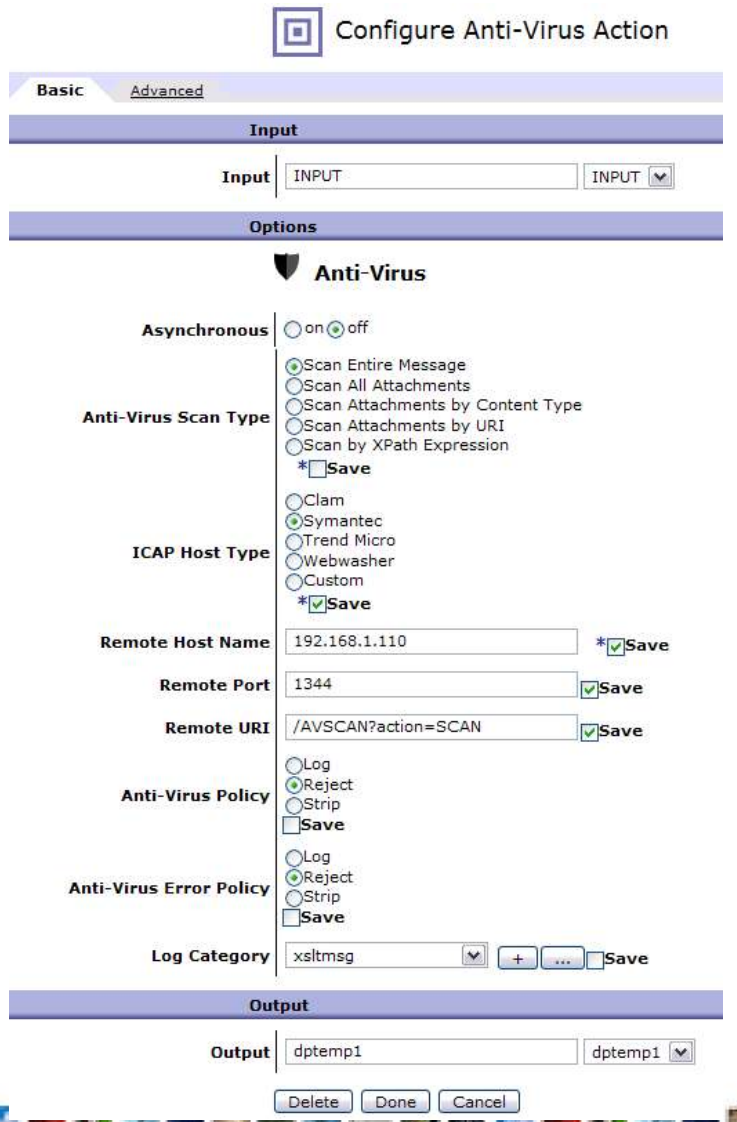
- 내장된 정책 조치 사용 – 구성 및 맞춤화 가능



14:08:29	xmlfirewall	warn	10801	e	192.168.1.102	0x80e000b6	xmlfirewall (XMLThreatTestFirewall): No match from processing policy 'XMLThreatTestFirewall' for code '0x00d30003'
14:08:29	xmlfirewall	error	10801	e	192.168.1.102	0x00d30003	xmlfirewall (XMLThreatTestFirewall): Rejected by filter; SOAP fault sent
14:08:29	xmlfirewall	warn	10801		192.168.1.102	0x80e0007d	xmlfirewall (XMLThreatTestFirewall): Generated error on URL 'http://192.168.1.108:2048/': <?xml version="1.0" encoding="UTF-8"?> <env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/"><env:Body><env:Fault><faultcode>env:Client</faultcode><faultstring>Message contains restricted content (from client)</faultstring></env:Fault></env:Body></env:Envelope>
14:08:29	multistep	error	10801		192.168.1.102	0x00d30003	xmlfirewall (XMLThreatTestFirewall): Rejected by filter; SOAP fault sent
14:08:29	multistep	error	10801	>	192.168.1.102	0x80c00009	xmlfirewall (XMLThreatTestFirewall): request XMLThreatTestFirewall_request #1 filter: 'INPUT store:///SQL-Injection-Filter.xsl' failed: Message contains restricted content
14:08:29	xslt	error	10801	>	192.168.1.102	0x80c00010	xmlfirewall (XMLThreatTestFirewall): Execution of 'store:///SQL-Injection-Filter.xsl' aborted: Message contains restricted content
14:08:29	xsltmsg	error	10801	>	192.168.1.102	0x80000001	xmlfirewall (XMLThreatTestFirewall): ***SQL INJECTION FILTER***: Message from 192.168.1.102 contains possible SQL Injection Attack of type 'SQL LIKE% Match'. Offending content: '%'. Full Message: '<?xml version="1.0" encoding="UTF-8"?> <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"> <SOAP-ENV:Body> <book> <name>Moby Dick;SELECT * FROM BOOK_AUTHORS WHERE AUTHOR_NAME LIKE '%KEROUAC%'</name> <author>Heman Melville</author> </book> </SOAP-ENV:Body> </SOAP-ENV:Envelope>'.
14:08:29	xmlfilter	info	10801	>	192.168.1.102	0x80c00037	xmlfirewall (XMLThreatTestFirewall): Reject set: Message contains restricted content
14:08:29	xmlparse	debug	10801	>	192.168.1.102		xmlfirewall (XMLThreatTestFirewall): Finished parsing store:///SQL-Injection-Patterns.xml
14:08:29	xmlparse	debug	10801	>	192.168.1.102		xmlfirewall (XMLThreatTestFirewall): Parsing document 'store:///SQL-Injection-Patterns.xml'
14:08:29	multistep	debug	10801	>	192.168.1.102		xmlfirewall (XMLThreatTestFirewall): Stylesheet URL to compile is 'store:///SQL-Injection-Filter.xsl'
14:08:29	xmlparse	debug	10801	>	192.168.1.102		xmlfirewall (XMLThreatTestFirewall): Finished parsing http://192.168.1.108:2048/

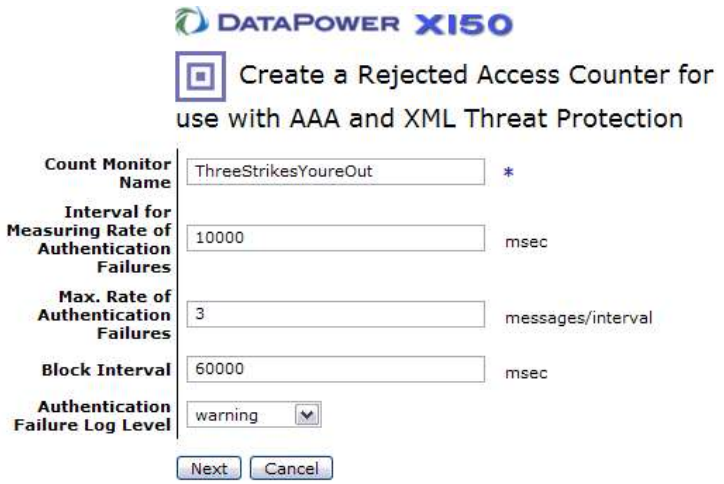
DataPower를 통해 XML 바이러스 차단

- 네트워크 바이러스 스캐너에 메시지 및 첨부파일을 전달하도록 설정할 수 있음
- 첨부 파일을 떼어내고 메시지가 통과할 수 있게 하거나, 전체 메시지를 거부할 수 있는 융통성



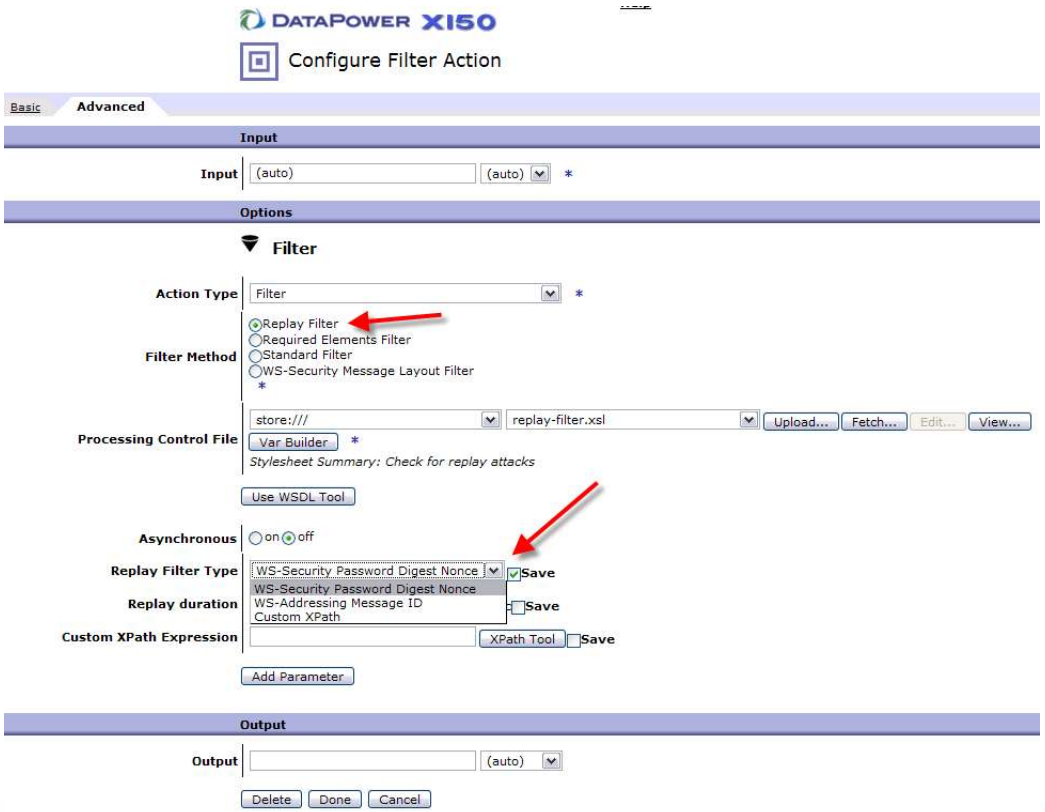
DataPower를 통해 딕셔너리 공격 방어

- 모든 유형의 인증/허가 실패에 대해 "삼진 아웃제"와 같은 정책 설정 가능



DataPower를 통해 Replay 공격 방어

- 마지막으로, WS-Sec 사용자 이름 토큰 안에 임시 정보 및 타임스탬프가 있는지 확인
  - WS-Addressing 헤더와 WS-Sec 메시지 레이아웃에 기반한 리플레이/라우팅 공격 역시 차단



DataPower 제품군

- XA35 XML 처리 가속기
  - XML 프로세스 처리 오프로드
  - XML의 수동식 최적화 불필요

XI50 Integration Appliance
- XML-to-'Any' 변환
- 혁신적인 데이터 지향 처리 아키텍처
- MQ 클라이언트
- 데이터베이스 (ODBC) 클라이언트

XS40 XML 보안 게이트웨이
- 향상된 보안 기능
- 민첩성 – 미래 보장
- 손쉬운 도입

XG4 XML 인식 서브시스템
- XML 기가비트 장벽을 넘어선 최초의 시스템
- 어디든 내장할 수 있는 OEM 솔루션
- 광범위한 용도

XM70 Low Latency Messaging
- 대기 시간이 짧은 대용량 메시지 전송
- 향상된 QoS 및 성능
- LLM에 구성 위주로 간단한 접근 방식
- PUB/SUB 메시지 처리
- 고가용성

XB60 Business to Business (B2B)
- B2B 메시지 처리 (AS2/AS3)
- 거래 파트너 프로필 관리
- B2B 트랜잭션 보기
- 최상의 성능 구현
- 간소화된 관리 및 구성

결론

- XML 기반 공격은 실제적인 위협이며, 조용하게 이루어지고 있음
  - 내부적으로 실행될 때도 있고, 파트너로부터 전송 받은 악성 데이터가 원인일 수도 있음
- 생산 중단은 많은 비용을 초래
  - 공격을 받았다는 소문이 퍼질 경우, 고객과 주주의 신뢰를 잃게 되고 비즈니스에 악영향
- 이와 같은 공격을 방어할 수 있는 실질적인 해법은 처리 능력을 강화하는 방법
  - 분명한 목적을 갖고 제작된 하드웨어 어플라이언스는 프로토콜/스펙/보안 토큰 중개와 백엔드 리소스의 가상화라는 측면에서 큰 도움
  - DMZ에서 문제 차단 필요 (경계 보안의 효과)
  - 유효한 트래픽만 백엔드에 도달할 수 있도록 보장하면 백엔드에서 리소스가 훨씬 효율적으로 사용