Security Challenges on the Road Ahead

Tim Mather, CISO

How Information Security Should Not Be Perceived

How Information Security Should Not Be Engaged

Rain on the FIRST “Parade” – No

FIRST Best Practice Guide Library

Public Guides

Must not be copied or distributed without prior consent of FIRST

- **Checking Microsoft Windows Systems for Signs of Compromise**
- **Checking UNIX/LINUX Systems for Signs of Compromise**
- **CSIRT Case Classification (Example for enterprise CSIRT)**
- **Guide to Tunneling Windows NT VNC traffic with SSH2**
- **IIS and NTS 4.0 Hardening Guide**
- **Online Forensics of Win32 System Guide**
- **Secure BGP Template**
- **Secure BIND Template**
- **Secure IOS Configuration Template**
- **SSH Public Key Configuration Windows NT/2000/XP Guide**
- **Windows 2000 / IIS 5.0 DMZ Hardening Guide**
- **Windows 2003 / IIS 6.0 DMZ Hardening Guidelines**

FIRST Members-only Guides

Restricted to FIRST Members and must not be redistributed outside of FIRST

- Personal Digital Assistant (PDA) Security Configuration Guide
- Red Hat LINUX Security Configuration Guide
- Solaris 7 / 8 - Secure Configuration Guide
- Windows 2000: Certificate Services Security Configuration Guide
- Windows 2000 Internet Information Server 5.0 Security Configuration Guide
- Windows 2000 Security Configuration Guide
- Windows 2000: Terminal Services Security Configuration Guide

May 2005

Contrasted with OASIS

OASIS Standards

- Application Vulnerability Description Language (AVDL) v1.0
- Common Alerting Protocol v1.0
- ~~Darwin Information Typing Architecture (DITA) v1.0~~
- Directory Services Markup Language (DSML) v2.0
- DocBook v4.1
- ebXML Collaborative Partner Profile Agreement (CPPA) v2
- ebXML Message Service Specification v2.0
- ebXML Registry Information Model (RIM) v2.0
- ebXML Registry Information Model (RIM) v3.0
- ebXML Registry Services Specification (RS) v2.0
- ebXML Registry Services Specification (RS) v3.0
- Extensible Access Control Markup Language (XACML) v1.0
- eXtensible Access Control Markup Language TC v2.0 (XACML)
- ~~OpenDocument Format for Office Applications (OpenDocument) v1.0~~
- Security Assertion Markup Language (SAML) v1.0
- Security Assertion Markup Language (SAML) v1.1
- Security Assertion Markup Language (SAML) V2.0
- ~~Service Provisioning Markup Language (SPML) v1.0~~
- Universal Description, Discovery and Integration (UDDI) v2.0
- Universal Description, Discovery and Integration (UDDI) v3.0.2
- Universal Business Language (UBL) v1.0
- Universal Business Language Naming & Design Rules v1.0 (UBL NDR)
- WS-Reliability (WS-R) v1.1
- ~~Web Services for Remote Portlets (WSRP) v1.0~~
- Web Services Security v1.0 (WS-Security 2004)
- Web Services Security SAML Token Profile v 1.0 and REL Token Profile v1.0
- ~~WSDM Management Using Web Services v1.0 (WSDM-MOWS)~~
- WSDM Management Using Web Services v1.0 (WSDM-MOWS)
- XML Common Biometric Format (XCBF) v1.1

May 2005

FIRST Conference 2005 Theme

"The theme for the 2005 conference is 'Join The Global Computer Security Network,' where the emphasis is on collaborative and cooperative approaches to the multiple disciplines involved in computer and network security incident response."

It is not about security for security's sake

It is about solving real-world business challenges

FIRST Press Release

“CALL TO ARMS FOR CORPORATE CHIEFS TO ATTEND ‘CRITICAL’ CYBER CONFERENCE

LONDON - April 27, 2005. Corporate executives from around the world were today being urged to attend a special conference on risk, to be staged this June in Singapore by FIRST, the world's premier force in the battle against cyber crime, sabotage and terrorism, and leading adviser to corporations and governments on internet security and stability.

Executives will be given a unique opportunity in closed sessions to focus with expert advice on aspects of risk which derive from and threaten the fast-evolving virtual cores of modern commerce.”

Tearing Down Firewalls

“We need technologies that won't impede our Internet use.

This is probably the most open secret in infosecurity that you don't want your CEO to discover: Ahem...those large, expensive border firewalls with those overpriced managed service contracts really aren't doing much to secure your enterprise. In fact, they are doing little more than inhibiting your business.

Gasp? Don't be so quick to dismiss this notion. Let's examine the facts.

As a security manager, you insist that your business units make connections through the perimeter firewall or a dedicated proxy on the DMZ. You delay projects until you can craft and test firewall rules, making sure they don't conflict with the 200 other rules already in place. And, you de-grade throughput and performance for marginal security gains.

Where does all of this get you? Despite perimeter firewalls, enterprises worldwide are struck by worm after worm – Slammer, Blaster, Sasser, MyDoom, …”

Paul Simmonds, CISO of Imperial Chemical Industries; member of the Jericho Forum Management Board
© *Information Security* magazine, March 2005

Participants

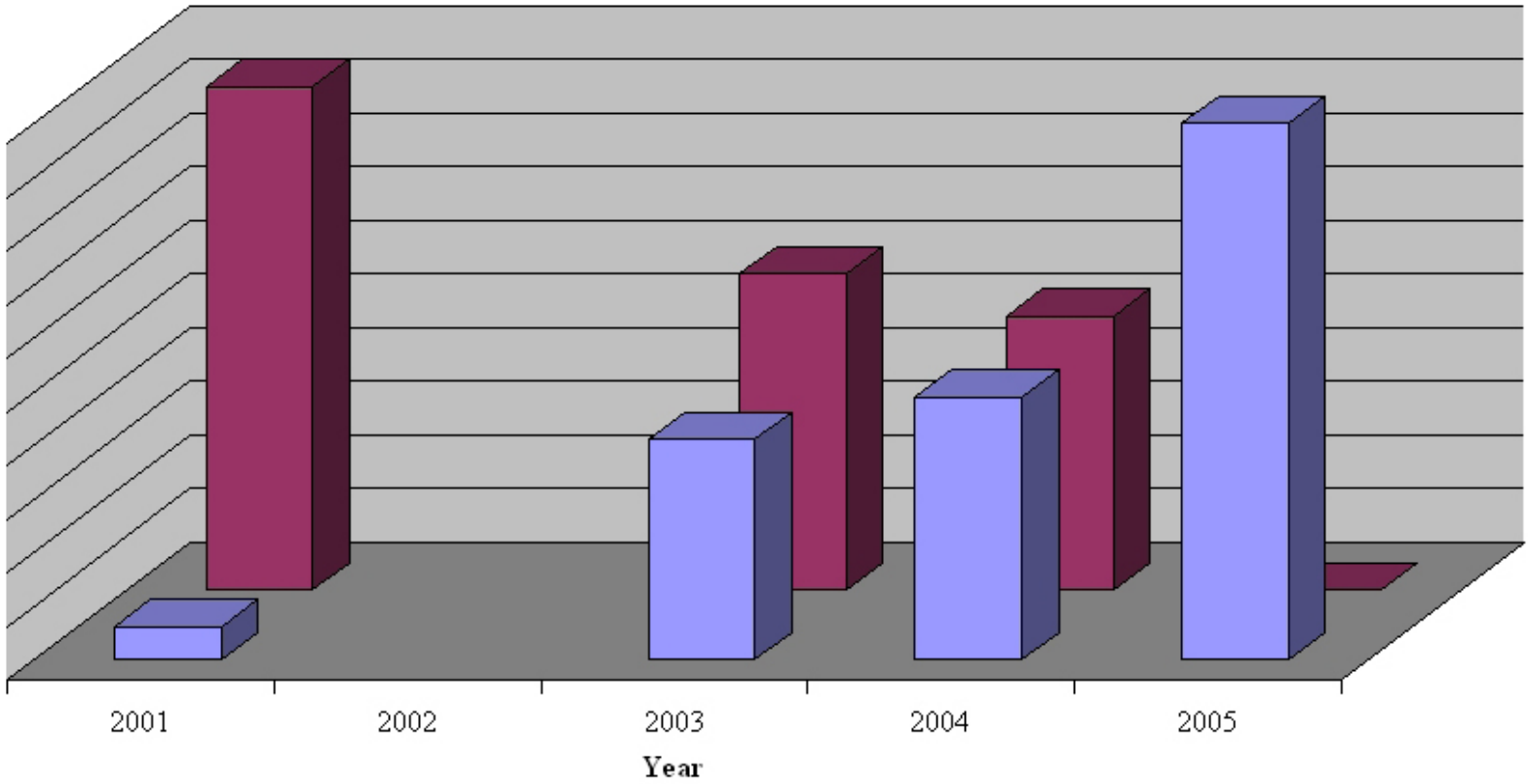
Abbot Laboratories	Eli Lilly	PA Consulting
ABN AMRO Bank	Ernst & Young LLP	Pfizer
Airbus	Geisinger Health System	Procter & Gamble
BAPLA	GlaxoSmithKline	Qantas
Barclays Bank	HBOS	Reuters
BAE SYSTEMS	HSBC	Rolls-Royce
Boeing	ICI	Romeike
British Broadcasting Corporation	ING	RBS
BP	Iron Mountain	Royal Dutch/Shell
Cabinet Office	JPMorgan Chase	Royal Mail
Cable & Wireless	KPMG LLP (UK)	Standard Chartered Bank
Clearstream	Lloyds TSB	The Open Group
Credit Agricole	Lockheed Martin	UBS Investment Bank
Credit Suisse First Boston	MBNA Europe Bank	UKCeB (Council for e-Business) Task Force
Deloitte	National Australia Bank Group (Europe)	Unilever
Deutsche Bank	Northern Rock	University of Kent Computing Laboratory
Dresdner Kleinwort Wasserstein	Olswang Solicitors	YELL

March 2005

Increasing Utilization of Encryption in Transit

- IPSec
- SSH
- SSL/TLS:
  - SMTP Service Extension for Secure SMTP over TLS
  - HTTPS 443
  - NNTPS 563
  - LDAPS 636
  - FTPS-Data 989
  - FTPS 990
  - TelnetS 992
  - IMAPS 993
  - IRCS 994
  - POP3S 995
  - TFTPS 3713

Increasing Utilization of Encryption in Transit



	2001	2002	2003	2004	2005
Encrypted	6%		41%	49%	100%
Unencrypted	94%		59%	51%	0%

Security and Mobile IP – v4 and v6

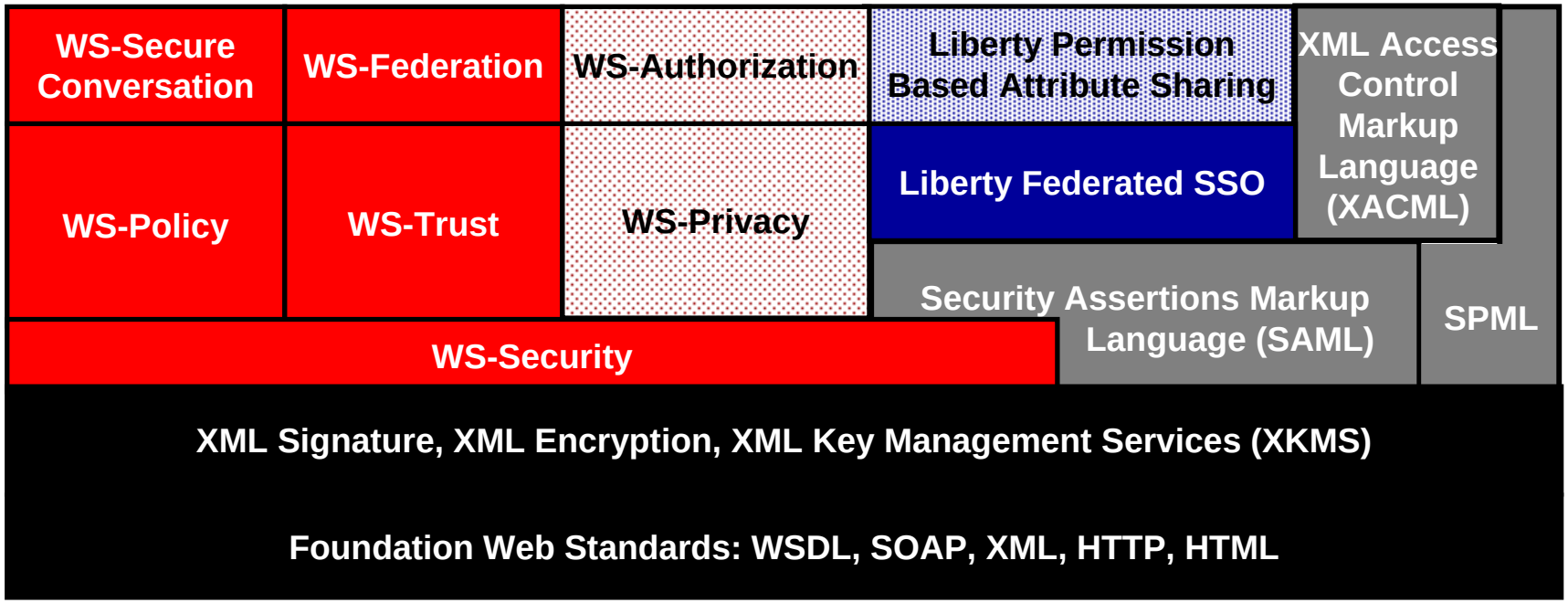
"…without a NAT, the care-of address in the registration request will be directly used by the HA [host address] to send traffic back to the MN [mobile node] (or the FA [firewall address]), and the care-of address is protected by the MN-HA (or FA-HA) authentication extension. When communicating across a NAT, the effective care-of address from the HA point of view is that of the NAT, which is not protected by any authentication extension, but inferred from the apparent IP source address of received packets. This means that by using the mobile IP registration extensions described in this document to enable traversal of NATs, one is opening oneself up to having the care-of address of a MN (or a FA) maliciously changed by an attacker."

RFC 3519 - Mobile IP Traversal of Network Address Translation (NAT) Devices

Security and VoIP

- "Traditional" security attacks directed against VoIP
  1. Underlying OS attacks against VoIP devices
  2. Infrastructure attacks against VoIP devices
- "New" concerns directed against VoIP
  3. Attacks against VoIP protocol implementations
  4. Configuration weaknesses in VoIP devices
  5. Application-level attacks against VoIP devices

Security and Web Services



KEY

SPML = Service Provisioning Mark-up Language
WSSG = Web Service Security Group: IBM, Microsoft, VeriSign

Problems that Need Solving

Computing on Ciphertexts – 2DNF

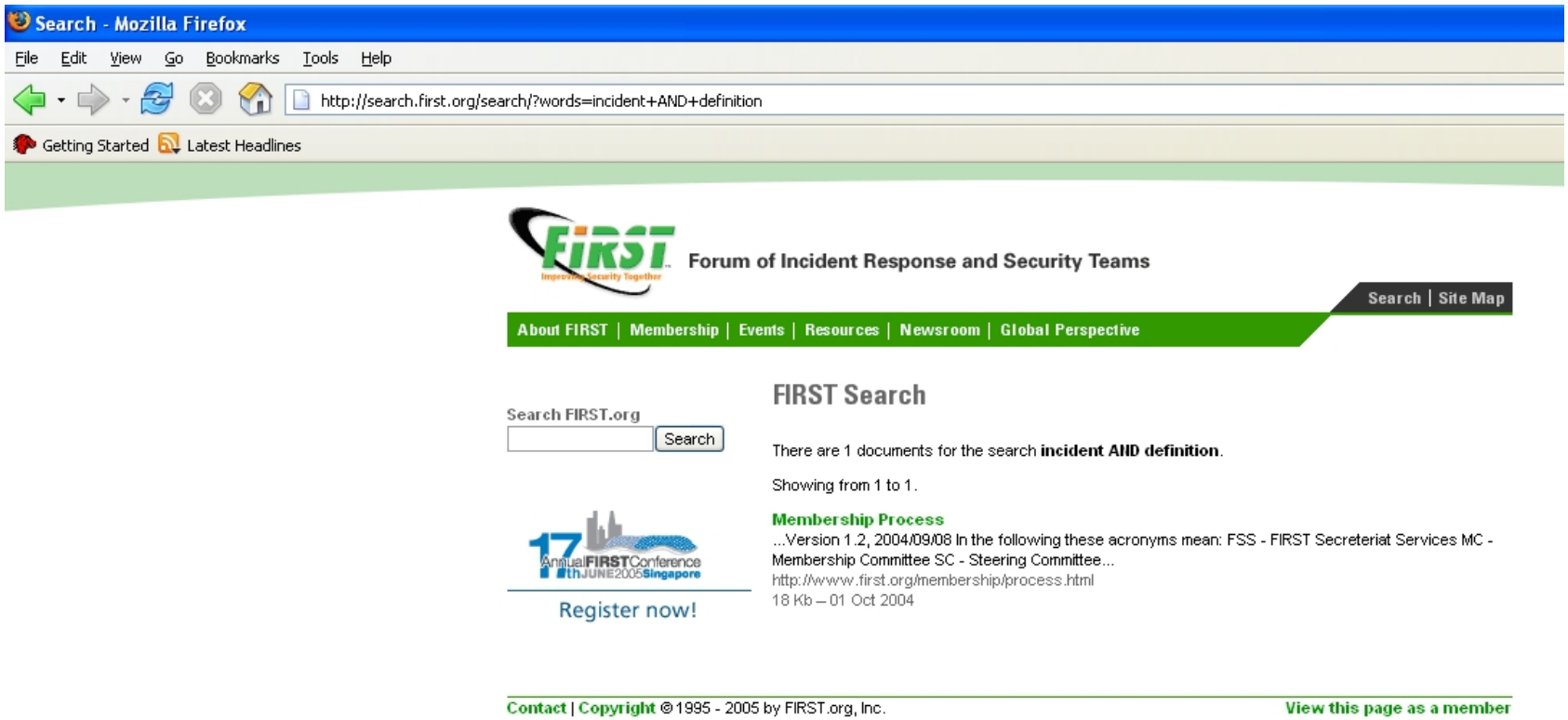
ABSTRACT:

An encryption scheme is additively (respectively multiplicatively) homomorphic if given the encryption of a message A and the encryption of B, anyone can compute the encryption of A+B (respectively AxB). Known homomorphic encryption schemes are either only additively or multiplicatively homomorphic, but not both. Ideally, we want an encryption scheme that is homomorphic to both addition and multiplication; such a scheme is called doubly homomorphic. Any logical function can be computed on ciphertext created using a doubly homomorphic encryption scheme. Applications of a doubly homomorphic encryption scheme include privacy preserving computations on encrypted databases and distributed computing on sensitive data.

Unfortunately, the construction of a doubly homomorphic encryption scheme is a long standing open problem dating from 1978. We have recently made some progress on this problem, developing an additively homomorphic encryption scheme with an additional limited multiplicative homomorphism (only a single multiplication). Even with such limitations, our encryption scheme allows us to evaluate on encrypted inputs useful formulas such as 2-DNFs, dot products, and polynomials of total degree at most two.

Eu-Jin Goh, PhD Candidate, Computer Science Dept., Stanford University

Problems that Need Solving



Thank you ?