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/VIIC traffic with SSH2
- IIS and NT 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 Internet Information Server 5.0 Security Configuration Guide

May 2005
Contrasted with OASIS

OASIS Standards

- Application Vulnerability Description Language (AVDL) v1.0
- Common Alerting Protocol v1.0
- Extensible Business Integration Architecture (EBI) 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 Reliable Interoperability (WS-Reliability) v1.0
- Web Services Security v1.0 (WS-Security 2004)
- Web Services Security SAML Token Profile v1.0 and REL Token Profile v1.0
- WSUML Management Using Web Services v1.0 (WSUML-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

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

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

<table>
<thead>
<tr>
<th>Year</th>
<th>Encrypted</th>
<th>Unencrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>6%</td>
<td>94%</td>
</tr>
<tr>
<td>2002</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003</td>
<td>41%</td>
<td>59%</td>
</tr>
<tr>
<td>2004</td>
<td>49%</td>
<td>51%</td>
</tr>
<tr>
<td>2005</td>
<td>100%</td>
<td>0%</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>WS-Policy</td>
<td>WS-Trust</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **WS-Security**
  - XML Signature, XML Encryption, XML Key Management Services (XKMS)
  - Foundation Web Standards: WSDL, SOAP, XML, HTTP, HTML

### Key
- **WSSG** – published
- **Liberty Alliance** – published
- **OASIS** – published

- **WSSG** – unpublished
- **Liberty Alliance** – unpublished
- **OASIS** – unpublished

**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 ?