



UNIVERSITY
of
GLASGOW



Security Research in Scotland

Prof J Sventek
University of Glasgow
joe@dcs.gla.ac.uk

Outline



- What do I mean by security?
- Who's doing what in Scottish academia?
- Securing the Next Generation Internet

Security



- A system is **secure** if its resources are used and accessed as intended under all circumstances
- Types of security violations:
 - Breach of confidentiality - unauthorized access to data
 - Breach of integrity - unauthorized modification of data
 - Breach of availability - unauthorized destruction of data
 - Theft of service - unauthorized use of resources
 - Denial of service - prevention of legitimate use of the system
- Need to authenticate and authorize principals attempting to access resources.
- I am particularly focused on securing the Internet.

Current Research in Scotland



- Edinburgh
 - Automated Analysis of Security Critical Systems - apply formal tools to the analysis of APIs to hardware security modules used in electronic payment systems
 - Mobile Resource Guarantees - infrastructure needed to endow mobile code with independently verifiable certificates describing its resource behaviour
 - Mobius: Mobility, Ubiquity and Security - use of Proof Carrying Code for establishing trust and security for the next generation of global computers
 - ReQueST: Resource Quantification in e-Science Technologies - attach mechanically checkable certificates of resource consumption to mobile Java applications used in e-Science.
 - Specification and enforcement of security constraints at the XML schema (conceptual) level.

Current Research in Scotland



- Glasgow
 - Intrusion detection systems based upon machine learning - detecting worm variants in the wild
 - GLASgow early adoption of Shibboleth - early adoption of Shibboleth single sign-on infrastructure
 - Dynamic Virtual Organisations in e-Science Education - prototype and apply technologies supporting the dynamic delegation of authority needed to create scalable virtual organisations
 - Virtual Organisations for Trials and Epidemiological Studies - federate data from many sources crossing domains that do not necessarily trust each other
 - Human Factors and security
 - Measurement techniques to facilitate Knowledge Plane



Current Research in Scotland



- Napier
 - Intrusion Detection
 - Framework for Automated Security Abstraction, Modelling and Verification
 - Analysis and Detection of Cruising Computer Viruses
- St Andrews
 - Steganographic covert channels
 - Denial of service
 - Trust in the Dynamic Establishment of Peering Coalitions
 - Measurement Techniques to facilitate Knowledge Plane

Current Research in Scotland



- Stirling
 - Advanced Call Control Enhancing Network Technologies - policy-based management infrastructure for specifying and enforcing obligation and access-control policies
- Strathclyde
 - Secure Environments for Collaboration among Ubiquitous Roaming Entities - application of trust as a means of establishing secure collaborations in highly dynamic computing infrastructures



UNIVERSITY
of
GLASGOW

Securing the Next Generation Internet



- The Internet has grown by 7 orders of magnitude since it was introduced in 1981
- Was built in an era of mutual trust (~200 hosts); no longer merits mutual trust.
- Original Internet was described by 16 specification documents; has accreted several hundred more since.
- Time to reconsider architecture of the Internet to address security and trust issues (among others).
- Securing the Next Generation Internet is a major focus area of the proposed Scottish Informatics and Computer Science Alliance.
- The goals are similar to those espoused by the Team for Research in Ubiquitous Technology (TRUST) science and technology centre operated by Berkeley, Carnegie Mellon, Cornell, Mills, San Jose State, Smith, Stanford, and Vanderbilt
- Some of the following slides have been borrowed from one of their presentations.



UNIVERSITY
of
GLASGOW



Network attacks are growing in sophistication

Slide 2 of

<http://www.truststc.org/publications/presentations/05/trust-intro-2005-07.ppt>



UNIVERSITY
of
GLASGOW



Attack Incidents

[Reports to CERT/CC]

Slide 3 of

<http://www.truststc.org/publications/presentations/05/trust-intro-2005-07.ppt>



UNIVERSITY
of
GLASGOW



The Internet in 1980

Slide 4 of

<http://www.truststc.org/publications/presentations/05/trust-intro-2005-07.ppt>



UNIVERSITY
of
GLASGOW



The Internet Today

<http://cm.bell-labs.com/who/ches/map/gallery/index.html>

Slide 5 of

<http://www.truststc.org/publications/presentations/05/trust-intro-2005-07.ppt>



UNIVERSITY
of
GLASGOW



Bad Code + Big Networks = Problems

Slide 6 of

<http://www.truststc.org/publications/presentations/05/trust-intro-2005-07.ppt>

Our proposed approach



- Revisit the basic network architecture, especially at the IP level, to address masquerading
- Build in required measurement capabilities to facilitate exploit detection and other forms of security monitoring.
- HCI research to enable the average network user to successfully deploy and use the security measures at his/her disposal
- Better understand societal trust relationships and how to map those to the Internet environment.
- Put all of this onto a firm formal basis using network calculi and other formalisms