

Introduction and Security Threats

Dr Stephen Hailes, UCL

May 10th

INET 2004 Barcelona



Security for the pervasive computing world



Introduction

- ▲ Security – isn't it all solved?
- ▲ Conventional threats
- ▲ Wireless systems now
- ▲ A vision of the future
- ▲ Protection now
- ▲ Protection in the future

So what's the big problem?

- ▲ We have firewalls and IDS – so we're safe from attack from the outside

- ▲ VPNs, RADIUS, SSH, etc. allow secure remote access

- ▲ PKI can be used in authentication

- ▲ S/MIME or PGP protects mail

- ▲ SSL/TLS protects web access

- ▲ Virus scanning is effective

- ▲ Security patches can be applied centrally – SMS

- ▲ and it's always sunny outside, the pink flopsy bunnies play happily in the streets and everyone is kind to old ladies

UK DTI survey 2002

<http://www.security-survey.gov.uk/>

▲ 70% UK businesses have a website (18% transactional)

▲ 76% businesses believe they have critical info

▲ 44% suffered malicious breach in past year

▲ Avg. cost of breach €45K; some €750K

▲ 83% businesses use anti-virus software

▲ 27% businesses have written security policy

▲ BS7799 – only 15% security officers aware

▲ 33% have software to detect intrusion

▲ For large businesses: 48% most serious attacks internal

▲ 68% security officers believe they catch all breaches

▲ 30% businesses evaluate ROI for security

▲ 27% spend > 1% of their IT budget on security

Why is there a problem?

- ▲ Lots of money + intellectual property (=money)
- ▲ Hostile environment (motivations for attack vary)
- ▲ Lack of security consciousness
- ▲ Lots of potential points of attack
- ▲ Policies are often seen as unacceptable
- ▲ No regulatory framework
- ▲ Legal aspects unclear

Other Threats

- ▲ Physical attack

- ▲ Trojan Horses, viruses, worms, logic bombs

- ▲ Passwords

- ▲ Loopholes

- ▲ Collusion

- ▲ Accidental access

- ▲ Tempest

- ▲ Social Engineering

Cost effective protection

Absolute security?

GIVE UP ON THE IDEA OF CERTAINTY
– IT'S FICTIONAL

Security = delay = cost to an attacker.

But security costs implementer too.

So compromise on level of security

- Evaluate risks
- Evaluate cost of losses
- Don't spend more than this
- Hard --
 - ▲ don't know motivation of attacker
 - ▲ don't know value of information or goodwill

Wireless systems

Oh and then it all gets decidedly worse. And the culprits?...



Toys!
aka 'empowering the workforce'



© 2003 CNET Networks, Inc.

New problems

- ▲ Infrastructure doesn't protect data
- ▲ Applications can't be trusted to secure data
- ▲ New forms of virus?
- ▲ Security in mobile devices not standardised (many OS)
- ▲ Devices easy to lose (or steal) or break
- ▲ Radio is a broadcast medium
- ▲ Most mobile devices come with security disabled
- ▲ Data loss is painful; the more so the more one relies on it

So what's to be done?

▲
▲
▲
▲
▲ Play Luddite?

▲ ■ Too late

▲ Wireless nodes will always be resource scarce compared to equivalent wired nodes

▲ Actually, there is (going to be) a LOT of heterogeneity in this space

▲ ■ Low mobility high b/w devices (802.11)

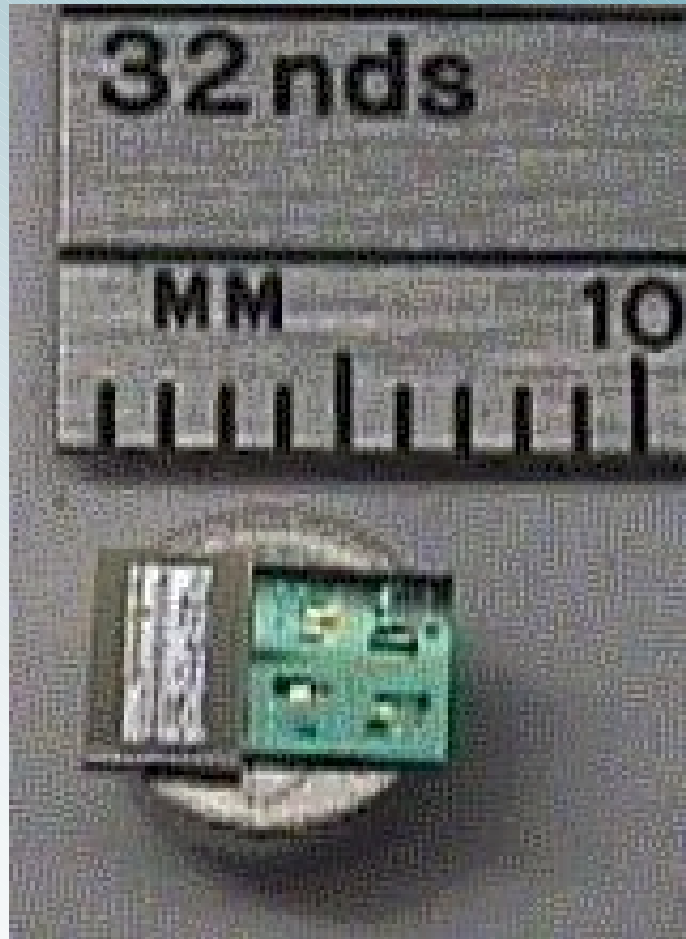
▲ ■ High mobility low b/w devices (cell phones all the way down to RFID tags)

▲ And the UIs will not be getting significantly better (au contraire)

▲ And there's battery lifetime to consider (new DoS attacks)

▲ And not all of it is going to look anything like it does currently...
▲
▲
▲
▲
▲

Gratuitous picture of neat technology



Security Issues

Same as ever – robustness

- Authentication
- Confidentiality
- Integrity
- Non-repudiation
- Access control (authorisation)
- Accounting/billing

But

- Focus is on ‘certainty’ – and it’s not clear we can have that
- Resource poverty – processing power/bandwidth
- Actuators can kill people
- Lawful interception

Security issues

- ▲ Encryption, signatures etc. affected by resources
- ▲ VPNs and PKI work OK in principle (to the same extent as wired systems)
- ▲ So does application level security
- ▲ Malicious code – no ubiquitous approach
- ▲ Overly rigid security procedures also dangerous
 - Users will try to circumvent controls
 - Important facilities may be unavailable, which can be expensive and damaging
 - More insecure procedures may be adopted
 - ▲ E.g. taking home sensitive documents rather than accessing remotely with careful security procedures
 - ▲ E.g. not permitting secure Voice/IP, IP multicast and IP conferencing, and using insecure voice, data and fax instead.

Traditional approach to securing systems

If we want to secure a system, then we need to follow a number of principles:

■ Prevention is *never* 100% effective – so:

- ▲ Need defence in depth – several different mechanisms
- ▲ Mechanisms for detecting and responding to attacks, preferably in real time, are essential:
 - Detect – get to know you're being attacked.
 - Localise – determine what's being attacked.
 - Identify – determine who the attacker is.
 - Assess – why are they doing this?
 - Respond – depends on all of above.
 - Recover – Have a plan better than 'go find a new job'
- ▲ Compartmentalise – don't put all of your data in one basket
- ▲ Start by securing the weakest link
- ▲ Mediocre security now is better than great security never
- ▲ Take your users with you

What changes in this?

- ▲ Ambient computing = invisible computing
- ▲ But heterogeneity in infrastructure, network protocols, etc.
- ▲ Issues of scale mean that human intervention is largely impracticable
 - need autonomic mechanisms
 - need new models of trust
 - need to abandon the simple certainties of conventional security
- ▲ Mobility in the system means changing physical connectivity and logical context
 - Need different types of policies; ones that can capture context
 - Need to have those policies implemented in a context dependent way
 - Need a flexible architecture to allow for composition of appropriate components
 - Need some assurance about how this will perform
- ▲ There are big privacy issues

What's necessary

Security at present just about works

- But it is a bolt on – it has been a painful process to get here
- But security yesterday <> security tomorrow – this is a war zone

Vision of future

- systems of huge scale,
- with huge heterogeneity,
- and a bigger impact on our lives than ever before
- abandon the attempt to get a 'perfect' system

Need R&D urgently to

- think about what security means in these environments
- build security in to these systems from day 1

Need a public debate about impacts on society

SEINIT is an EU and Swiss funded Framework 6 Integrated Project (IP)

- Aim is to address security issues in ambient environments across heterogeneous platforms
- IPv6 oriented
- €5M over 24 months, started 1/12/03

13 partners: **Thales Communications** (France-Coordinator), Alcatel (Fr), BT (UK), ENST (Fr), IABG (Ge), Kyos (CH), T-Systems (Ge), Telscom (CH), Thales Research and Technology (UK) Ltd, University College London (UK), University of Murcia (ES), Waterford Institute of Technology (IRL), and ISOC (Int'l).

Aims:

- Defining new trust, security models and security policies, maintaining an adequate security level without infringing a user's right to privacy.
- Devising an architecture that allows the realisation of these policies across heterogeneous platforms in systems of considerable dynamicity
- Specifying components that are composed to form the infrastructure, under the control of the architecture.
- Assessing the performance of this framework in different settings
- Porting applications to this framework as proof of concept.

For more information see <http://www.seinit.org>