New technologies and future security challenges

Chris Mitchell
Royal Holloway, University of London
http://www.isg.rhul.ac.uk/~cjm
Goals

- Examine two key issues for future cyber security:
  - **Technology trends** – what do they mean for future cyber security?
  - **Conflicting requirements** – security/privacy requirements versus economic and technological pressure.
1. Technology trends

- We look at four key emerging technology trends with serious security and privacy implications:
  - Ubiquitous/ambient computing;
  - Clouds/proxies/Grids;
  - Growing system and component complexity;
  - Integrated peripherals.
Ubiquitous computing

• The advent of always connected devices is already with us (mobile phones, wireless PC connectivity, RFID, ...).
• Systems have evolved piecemeal – no overall security architecture.
• Network access protocols offer very limited security (device authentication of network is sometimes non-existent):
  – ‘fake network’ attacks (GSM, 802.11, ...);
  – compromised access points (either by software or hardware attack).
• Similarly, pair-wise device authentication is sometimes not robust.
• Growing risk of widespread malware attacks, as devices become more ‘smart’ and flexible.
• Apart from poor security fundamentals, privacy is a major issue – device tracking is far too simple.
There is growing trend to move data and processing to the cloud.

Security and privacy concerns are widely documented – especially as the cloud providers offer very little guarantees about security, privacy and availability.

This is just one part of a long-term trend to outsource IT provision.

Users of outsourced services need to start asking deep questions about security and availability.
Complexity

• Another long-term trend is that towards increasing complexity, covering:
  – hardware of individual devices;
  – software running on devices (e.g. move towards general purpose OSs on special purpose devices);
  – system itself – growing interconnectivity adds huge complexity.

• Long known that complexity is the enemy of assurance.

• A lot of wishful thinking about emergent properties permeates the industry ...
Ubiquitous peripherals

- Ubiquitous computing devices come equipped with growing numbers of external interfaces – cameras, microphones, biometric readers, ...
- Who controls these?
- Do you trust all your applications running on all your devices not to misuse these functions?
- These peripherals represent a huge threat to personal and organisational security and privacy.
- Ubiquitous sensors pose a related threat.
Other issues 1

• Privacy technology – requirements for providing anonymity will make it more difficult to trace attacks.

• We can expect continued growth in orchestrated attacks, by governments or other organisations (e.g. terrorist groups, criminal gangs, protesters, ...).

• New and unexpected types of malware are bound to emerge. Also, malware will spread across multiple platform types – e.g. rootkits on mobile phones ...

• Security threats to embedded devices pose an ever-increasing safety threat through their control of physical devices (e.g. vehicle control systems, radio power control and battery management systems in mobiles, ...).
Other issues II

• Provenance of software/hardware has become almost impossible to determine – how do we know our systems do not incorporate deliberately engineered vulnerabilities?

• Automatic updating of complex software is both very helpful and a huge risk – e.g. through ownership/influence of large corporates and foreign governments.

• User authentication techniques are not getting any better – still overwhelmingly rely on passwords (tokens, public keys, etc. are still not widely used).
2. Growing conflicts

- **Requirements:**
  - High robustness – because of criticality of IT;
  - Privacy protection – growing legal frameworks and user interest.

- **Economic/technological factors:**
  - Increasing complexity (inevitable technological drift) directly threatens robustness;
  - Increased use of third parties (outsourcing) makes privacy and security assurance very hard.
  - Smarts everywhere (flexibility) also threatens robustness.
Efficiency versus robustness

• Efficiency pressures:
  – use of third party providers;
  – integration across sectors;
  – just in time issues (minimise IT investment);
  – green/environmental issues.

• Robustness requirements:
  – avoid reliance on systems outside of direct control and single points of failure;
  – avoid possibility of cascading failures;
  – redundancy (multiple systems, …).
Efficiency versus diversity

• Efficiency pressures:
  – minimise number of types of platform/system to reduce maintenance and purchasing costs;
  – minimise number of suppliers (economies of scale).

• Diversity requirements:
  – reduce impact of vulnerabilities by using diverse systems;
  – spread risk through diversity.
Complexity versus reliability

- Complexity pressures:
  - hardware and software development more and more removed from human understanding – more complex – more intermediary layers (libraries, CAD tools, …).

- Reliability requirements:
  - the simpler a system is, the easier it is to make it reliable.
Flexibility versus stability

• Flexibility pressures:
  – re-use of a standard platform (e.g. a PC), even in embedded applications, reduces cost;
  – end users want flexibility to gain maximum benefit from their investment.

• Stability requirements:
  – keeping things simple increases assurance;
  – flexibility vastly increases the attack surface.
3. Are we all doomed?

• Conclude by highlighting some areas in which we might discern security-positive events:
  – growing diversity of platform types (e.g. games platforms as IT platforms);
  – better software;
  – growing awareness of seriousness of security threats;
  – possible future in ‘locked down’ devices.