Upcoming information security threats
- an end-user perspective -

Roland Rieke, Fraunhofer Institute for Secure Information Technology

FORWARD workshop, April 17-18, 2008

ICT infrastructure security and resilience have become ever more important considering the latest attacks including fast-flux networks and malware such as the Storm worm. The development of future ICT infrastructures will boost the evolution of information security related attacks such as denial-of-service attacks, identity and information theft, phishing, spam attacks, spit (spam over IP telephony). Besides economic damages caused by ICT attacks, social effects cannot be ignored. For instance, news reports about these attacks and people's identity being stolen reduces citizens trust and confidence in e-government services and e-commerce activities.

In contrast to end-systems connected to networks of enterprises and public organisations, the majority of home users' end-systems are much more vulnerable to security threats because they are set up by non-expert users.

Attacks and malware will exploit the increasing availability of mobile networking technology. This allows attackers to not only target the traditional network stack, but also spread through communication vectors such as personal area networks (IrDA, Bluetooth), wireless wide-area phone networks (e.g., GSM, GPRS), or wireless local-area networks (e.g., 802.11, WiFi). Furthermore, attackers will exploit the increasing numbers of mobile devices, and the fact that they are often resource-constrained makes it difficult to install adequate defence solutions. Moreover, mobile devices can simply be used as carriers that leverage syncing mechanisms and USB connections to infect multiple hosts and the media they have access to.

Attackers will also target novel types of services that are deployed. Such services include services over mobile networks (e.g. MMS), but also novel services over traditional networks (such as VoIP or TV over IP). Novel malware spreading and control mechanism such as botnets based on voice oriented and encrypted protocols can easily cross firewalls and will be very difficult to detect. TV over IP malware could reach millions of end-users all of a sudden.

New large-scale ICT infrastructures will be deployed in sectors currently not vulnerable to Internet threats. One example are the upcoming e-health infrastructures. One problem is that the transmitted information such as genetic data and psychological or medical treatment is still sensible after many years. This opens opportunities for novel, very long-dated threat patterns such as eavesdropping encrypted data and storing the data for many years until decryption is possible. Vehicular ad hoc networks provide another new platform for new kinds of threats. Attackers will try to spread malware using physical transportation, to trace vehicle movement and possibly to trigger accidents.

Challenges.

- To *understand the general principles* of systemic intervention, disruption and infection in highly interconnected complex ICT systems. and to *predict the effects* of threat prevention, detection, and mitigation strategies in current and future attack scenarios.
- To develop novel concepts, tools and mechanisms to *prevent and mitigate malware epidemics* enabling efficient and adequate countermeasures and offering assistance to the affected end-users.
- To improve *usability of security*. End-users' *legal responsibility* for unintentional attacks requires that the current situation and the impact of possible courses of actions is fully understood.
- *Not to sacrifice privacy for security* (e.g. in forensic analysis).

Solution approaches. There are many concepts to build trusted dependable subnetworks for specific purposes using software/hardware based solutions such as VPN, PKI, digital identity, TPM to support authentication of partners, integrity of software systems and confidentiality of communication channels or communicated information. Examples are secure VoIP for emergency response teams, special hw/sw solutions for TV over IP distribution, building automation systems, in-car communication, middleware for networked embedded systems.

Increasingly, the weakest link in the overall picture appears to be the users PC or smartphone that might be part of a botnet or have a malicious rootkit installed performing unauthorised tasks without the home-user even being aware of it. Moreover, recent attacks such as those in Estonia indicate that the identification of source of attacks and mitigating the contagion through launching successful protective or counter measure strategies must include SMEs and home-users to secure network reliability and dependability. Most current connection devices between end-user systems and the Internet use unidirectional protection (protect the user against attacks from the Internet). These connection devices could be replaced by trusted security devices that provide (1) *accurate security analysis* and (2) *bidirectional security enforcement*. These systems themselves will be subject to attacks and thus have to be secured (e.g. by trusted computing technology).

To support (1) and to increase the shared situational awareness for better orchestrating defense against cyber attacks these security systems should collaborate. Analysis of distributed events and local and distributed reasoning using e.g. operational models, security and plausibility measures and behaviour based anomaly detection will enhance detection of malware spreading and botnet control structures. Self-adaptation to changing context will be an important challenge. An anomaly of today might be normal behaviour tomorrow, so the same algorithm at different times, might and should come to different judgements.

To support (2) a temporary and adequately adjusted quarantine solution for large-scale ISP networks that deal with infected end-systems is one means to secure the Internet from botnet controlled attacks using end-user resources. Countermeasures have to be accompanied with user-intuitive remedy solutions adjusted to the situation to guide fixing the problem.