Towards a security and privacy model for the IoT

Saša Radomirović

University of Luxembourg

Motivation

Model security and privacy in the IoT.

Motivation

Model security and privacy in the IoT.

What are the dangers to look out for in the IoT?

Motivation

Model security and privacy in the IoT.

What are the dangers to look out for in the IoT?

How do we recognize early signs of something that might go wrong?

Approach

1. Look at past developments.
2. Study current situation.
3. Extrapolate.

Internet of Things (IoT)

- communication network
- extends the present Internet
- includes everyday items and sensors

Internet of Things (IoT)

- communication network
- extends the present Internet
- includes everyday items and sensors

Technologies used:

- *Radio Frequency Identification* (RFID) tags attached to cheap and disposable objects
- more powerful radio signal transmitters/receivers integrated into large and valuable objects

Simplistic Timeline of the Internet

Time	Network	Events
1980s		PCs are widespread
early 90s	dial-up connections	BBSs are popular
mid 90s	Internet is popular	BBSs reachable from Internet
	(0.4% of world pop.)	E-commerce starts
early 00s	broadband	E-commerce takes off
	(4.1% of world pop.)	Amazon makes profit
late 00s	wireless	cloud applications
	(26% of world pop.)	

Phase transitions

- significant size of Internet → E-commerce becoming possible
- switch to broadband → Cloud apps, social networking, TV

Simplistic Timeline of the Internet and Malware

Time	Network	Events
1980s		Trojans and viruses on floppy discs
early 90s	dial-up connections	Malware spreading through BBSs
mid 90s	Internet is popular	E-commerce starts
	(0.4% of world pop.)	Website defacement
early 00s	broadband	Internet worms, viruses, botnets
	(4.1% of world pop.)	E-commerce takes off
		XP SP2 with software firewall
late 00s	wireless	Internet black market
	(26% of world pop.)	cloud applications

Phase transitions

- significant size of Internet → E-commerce becoming possible
- switch to broadband → Cloud apps, social networking, TV

Phase transitions

- significant size of Internet → E-commerce becoming possible
- switch to broadband → Cloud apps, social networking, TV

But also:

- before E-commerce: viruses, worms as pranks
- after E-commerce: malware for profit

Phase transitions in malware

Transitions caused by combination of honeymoon effect and low-hanging fruit.

Phase transitions in malware

Transitions caused by combination of honeymoon effect and low-hanging fruit.

Example of a phase transition:

- Exploits before XP SP2: trivial (open ports).
- Exploits after XP SP2: client-side exploits, larger effort required

Phase transitions in malware

Transitions caused by combination of honeymoon effect and low-hanging fruit.

Example of a phase transition:

- Exploits before XP SP2: trivial (open ports).
- Exploits after XP SP2: client-side exploits, larger effort required

Note: Large number of identically vulnerable devices.

Internet story so far

- Several vulnerable objects (home PCs) exist.
- Exploits don’t seem interesting, are only created for amusement.
- Context change (e-commerce).
- Exploits blow up.

Present developments

1. Shift from computer application exploits to hardware exploits.

Present developments

1. Shift from computer application exploits to hardware exploits.

   Examples:

   - Cars can be remotely controlled due to wireless communication between components.
   - Firmware of Network cards can be “easily” changed, could thus be infected by malware.
   - Printers can be “easily” hacked, fuser temperature can be increased.

Present developments

1. Shift from computer application exploits to hardware exploits.

   Examples:

   - Cars can be remotely controlled due to wireless communication between components.
   - Firmware of Network cards can be "easily" changed, could thus be infected by malware.
   - Printers can be "easily" hacked, fuser temperature can be increased.

2. Loss of privacy.

   - Long list of fingerprinting and profiling techniques.

     Short story: Everything is "fingerprintable" (typing cadence, browser configuration, sensor noise patterns, ...)

   - Data collection sites are mushrooming.

     Examples: cvgadget.com, dirtsearch.com, mylife.com, pipl.com, rapleaf.com, spokeo.com, wink.com, ...

Present developments

1. Shift from computer application exploits to hardware exploits.

   Examples:

   - Cars can be remotely controlled due to wireless communication between components.
   - Firmware of Network cards can be “easily” changed, could thus be infected by malware.
   - Printers can be “easily” hacked, fuser temperature can be increased.

2. Loss of privacy.

   - Long list of fingerprinting and profiling techniques.

     Short story: Everything is “fingerprintable” (typing cadence, browser configuration, sensor noise patterns, ...)

   - Data collection sites are mushrooming.

     Examples: cvgadget.com, dirtsearch.com, mylife.com, pipl.com, rapleaf.com, spokeo.com, wink.com, ...

Other developments?

Outlook for IoT: Infrastructure

Today: VANets (car-to-car networks), wireless road pricing, sensor networks, RFID tickets, biometric scanners, ...

Outlook for IoT: Infrastructure

Today: VANets (car-to-car networks), wireless road pricing, sensor networks, RFID tickets, biometric scanners, ...

Near future: same technologies, increasing density, interoperability.

Outlook for IoT: Infrastructure

Today: VANets (car-to-car networks), wireless road pricing, sensor networks, RFID tickets, biometric scanners, ...

Near future: same technologies, increasing density, interoperability.

(Distant?) future: phase transition, context change.

Outlook for IoT: Security and Privacy

- IoT technologies fall into hardware exploits category.
- Cheap mass production implies shoddy security design.
  There will be a plethora of vulnerable devices.
- Wireless communication is cheap and ubiquitous.
  → Advertising pamphlets, gifts, purchased equipment may contain Trojan devices. (Trust issues...)

Mitigation

- Defense against discovered vulnerabilities in devices: Proactive mitigation (cf. Firefox’ plugin check). Compare own devices with list of known vulnerabilities.

Mitigation

- Defense against discovered vulnerabilities in devices: Proactive mitigation (cf. Firefox’ plugin check). Compare own devices with list of known vulnerabilities.
- Defense against Trojan devices: Scan every incoming and outgoing item.

Mitigation

- Defense against discovered vulnerabilities in devices: Proactive mitigation (cf. Firefox' plugin check). Compare own devices with list of known vulnerabilities.
- Defense against Trojan devices: Scan every incoming and outgoing item.

Note: OS security analogy.

Towards Modeling: Formal aspects

- Consider symbolic formal model (perfect crypto abstraction).
  Standard approach for network security models.

Towards Modeling: Formal aspects

- Consider symbolic formal model (perfect crypto abstraction). Standard approach for network security models.
- Abstract away from type of communication devices and tokens. Simplification analogous to perfect crypto abstraction.

Towards Modeling: Formal aspects

- Consider symbolic formal model (perfect crypto abstraction).
  Standard approach for network security models.
- Abstract away from type of communication devices and tokens.
  Simplification analogous to perfect crypto abstraction.
- Adversary has corruption capabilities.
  Through strong hardware exploits, Trojan devices.
- Adversary has fingerprinting capabilities.
  Through weak hardware exploits, Trojan devices.

Towards Modeling: Formal aspects

- Consider symbolic formal model (perfect crypto abstraction).
  Standard approach for network security models.
- Abstract away from type of communication devices and tokens.
  Simplification analogous to perfect crypto abstraction.
- Adversary has corruption capabilities.
  Through strong hardware exploits, Trojan devices.
- Adversary has fingerprinting capabilities.
  Through weak hardware exploits, Trojan devices.
- Asynchronous communication under control of Dolev-Yao adversary.
  Through Trojan devices, hardware exploits, cheap ubiquitous wireless communication.

Towards Modeling: Formal aspects

- Consider symbolic formal model (perfect crypto abstraction).
  Standard approach for network security models.
- Abstract away from type of communication devices and tokens.
  Simplification analogous to perfect crypto abstraction.
- Adversary has corruption capabilities.
  Through strong hardware exploits, Trojan devices.
- Adversary has fingerprinting capabilities.
  Through weak hardware exploits, Trojan devices.
- Asynchronous communication under control of Dolev-Yao adversary.
  Through Trojan devices, hardware exploits, cheap ubiquitous wireless communication.
- Define Security and Privacy properties.
  Well-known: secrecy, authentication, untraceability (location privacy). New: unlinkability of digital crumbs.

Specific Privacy issue: Digital Crumbs

Motivation for Unlinkability of Digital Crumbs:
The Internet cannot forget.

Specific Privacy issue: Digital Crumbs

Motivation for Unlinkability of Digital Crumbs:
The Internet cannot forget.

At present: Intentionally uploaded personal content to social networking apps.

Specific Privacy issue: Digital Crumbs

Motivation for Unlinkability of Digital Crumbs:
The Internet cannot forget.

At present: Intentionally uploaded personal content to social networking apps.

IoT: Your (precise) location, typical travel route, equipment, (contents of fridge) on a given day at a given time, health indicators.

These are all digital crumbs that are unavoidable to be leaked to specific entities.

Specific Privacy issue: Digital Crumbs

Motivation for Unlinkability of Digital Crumbs:
The Internet cannot forget.

At present: Intentionally uploaded personal content to social networking apps.

IoT: Your (precise) location, typical travel route, equipment, (contents of fridge) on a given day at a given time, health indicators.

These are all digital crumbs that are unavoidable to be leaked to specific entities.

Privacy property requirement: Two digital crumbs created by the same entity should not be linkable.

Conclusion

- Technological advancement gives rise to profound socio-economical changes.
- A consequence for the IoT is that legacy devices may become a security and privacy liability. Security vulnerabilities of devices should therefore be proactively monitored.
- It might be useful to consider a set of devices in the IoT as a fusion of an OS and a communication network.

Future Work

- Develop phase transition theory.
- Complete the formal model.
- Work out unlinkability of digital crumbs and other privacy properties.

Thank you!